53-1003142-01
27 June 2014

Fabric Watch

Administrators Guide

Supporting Fabric OS v7.3.0

BROCADE

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

Contents

Port Monitoring..65

System Monitoring..87

Fabric Watch Configuration Using Web Tools.. 99

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names Identifies keywords and operands Identifies the names of user-manipulated GUI elements Identifies text to enter at the GUI
italic text	Identifies emphasis Identifies variables and modifiers Identifies paths and Internet addresses Identifies document titles
`Courier font`	Identifies CLI output Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.

Convention	Description
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.

- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and 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. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About This Document

Supported hardware and software

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Fabric OS 7.2.0, documenting all possible configurations and scenarios is beyond the scope of this document.

What's new in this document

- Supported hardware and software on page 11
- No other new content. Bug fixes to the following sections:
- Activating Fabric Watch using a Telnet session on page 35
- Activating Fabric Watch using SNMP on page 36
- E_Port subclass setting guidelines on page 71
- FOP_Port and FCU_Port subclass default settings on page 75
- Recommended port configuration settings on page 83

Fabric Watch

Fabric health

Fabric health refers to the capability of the fabric to route data. A healthy fabric enables effective data transmission between networked devices.

One of the more obvious criteria for fabric health is the condition of the network hardware. A switch or port failure can 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 loss. Receive (Rx) and Transmit (Tx) performance areas are used to monitor the bandwidth utilization to help keep traffic flowing to avoid congestion.

Because of the varied factors involved in determining fabric health, Fabric Watch can help you to 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 overview

Fabric Watch is an optional storage area network (SAN) health monitor that allows you to enable each switch to constantly monitor its SAN fabric for potential faults and automatically alerts you to problems long before they become costly failures.

Fabric Watch tracks a variety of SAN fabric elements and events. Monitoring fabric-wide events, ports, and environmental parameters enables early fault detection and isolation as well as performance measurement. You can configure fabric elements and alert thresholds on an individual-port basis and you can also easily integrate Fabric Watch with enterprise system management solutions.

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 pre-emptive network maintenance, such as trunking or zoning, and avoid potential network failures.

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

Role-based access control

Role-Based Access Control (RBAC) defines the capabilities that a user account has based on the role the account has been assigned. For each role, there is a set of predefined permissions on the jobs and tasks that can be performed on a fabric and its associated fabric elements. Fabric OS v6.1.0 and later use RBAC to determine which commands a user can issue.

Each feature is associated with an RBAC role and you will need to know which role is allowed to run a command, make modifications to the switch, or view the output of the command. To determine which RBAC role you need to run a command, review the section "Role-Based Access Control (RBAC)" of the *Fabric OS Administrator's Guide* .

Fabric Watch licensing

Fabric Watch is an optionally licensed feature of Fabric OS. Refer to the *Fabric OS Software Licensing Guide* for more information about licensing and how to obtain the Fabric Watch license key.

Reasons to customize Fabric Watch settings

Customization is recommended to achieve the following objectives:

- Selecting one or more event settings
- Selecting an appropriate message delivery method for critical and noncritical 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

Before you begin an implementation, make some decisions surrounding the major configuration tasks: monitoring and configuring thresholds, actions, events, time bases, and alerts. These tasks are discussed in the following sections.

Event behavior configuration

You must first use the **fwSetToCustom** command to switch from default to custom settings, and then use the advanced configuration options provided with the **portThConfig**, **thConfig**, and **sysMonitor** commands to configure event behavior, actions, and time bases at the port level.

Alert configuration

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 large numbers of unimportant messages are received, examining the source can identify those classes that need to be reconfigured. To reduce the number of unimportant messages, consider the following reconfiguration options:

- 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. 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.

Brocade recommends using either SNMP trap alerting to your system management console or event log entry in conjunction with syslog forwarding configured on your switches.

Time base configuration

The time base specifies the time interval between two samples to be compared. The **fwSetToCustom** command allows you to switch from default to custom settings. Valid intervals are day, hour, or minute. Refer to Setting Fabric Watch custom and default values on page 43 for more information.

Threshold and action configuration

Before you begin to configure thresholds, decide if you want to have different levels of alerts for E_Ports, FOP_Ports, and FCU_Ports, and configure the ports individually. Always set up thresholds one fabric at a time and test the configuration before you apply the threshold configuration to more switches or fabrics.

NOTE
You cannot configure different thresholds for server and storage ports, because threshold configuration is an area-wide setting and cannot be configured on an element (port).

Monitoring

Do you want to monitor all class areas, or implement the monitoring in incremental stages? If you monitor class areas incrementally, you should configure Fabric Watch to monitor the classes in the following order:

1. Monitor Fabric class areas using the **thConfig** command.

   Refer to Fabric, Security, SFP, and Performance Monitoring on page 47 for details.
2. Monitor Port class areas using the **portThConfig** command.

   Refer to Port Monitoring on page 65 for details.
3. Monitor FRU class areas using the **fwFruCfg** command.

   Refer to System Monitoring on page 87 for details.

NOTE
For each class area, there are setting guidelines and recommendations for whether you should leave the setting at the default or change the settings. If a change is recommended, the reason for the change and the suggested settings are provided in each of the configuration chapters. The default settings are listed in these chapters as well.

Post-processing of messages

After you have configured thresholds and alerts, determine to where the messages will be sent. Then, monitor the messages frequently and take the appropriate actions.

Class, area, and element hierarchy

Fabric elements and events are organized in a hierarchy by class, area, and element. 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.

Here is an example of a very simple Class –> Area –> Element hierarchy:

Port –> Cyclic redundancy check (CRC) –>port 0

Switch monitoring components

Fabric Watch software enables you to monitor the independent components that are listed in this section.

Fabric events monitoring

The Fabric class groups areas of potential problems arising between devices, such as zone changes, fabric segmentation, E_Port down, fabric reconfiguration, domain ID changes, and fabric logins. A Fabric-class alarm alerts you to problems or potential problems with interconnectivity. You can customize Fabric class and area parameters using the **thConfig** command.

For complete information about fabric monitoring, refer to Fabric monitoring guidelines and default settings on page 47.

Performance monitoring

Performance monitoring groups 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.

You can customize Performance Monitor class and area parameters using the **thConfig** command. The **fmConfig** command Manages frame monitor configuration, replacing deprecated advanced performance monitoring commands. Use the **fmConfig** command to configure, install, and display frame monitors across port ranges on a switch. Refer to the *Fabric OS Command Reference* for details.

The Performance Monitor class is divided into the following areas:

- EE (end-to-end) Performance Monitor - Monitors RX and TX performance between two devices.
- Filter Performance Monitor - Measures the number of frames transmitted through a port that match specific values in the first 64 bytes of the frame. Because the entire Fibre Channel frame header and many of upper protocol's header fall within the first 64 bytes of a frame, filter-based monitoring can measure different types of traffic transmitted through a port.

NOTE
Performance Monitoring is not supported on VE_Ports, EX_Ports, and VEX _Ports.

For complete information about performance monitoring, refer to Performance monitoring guidelines and default settings on page 54.

Security monitoring

The Security class monitors different security violations on the switch and takes action based on the configured thresholds and their actions. You can customize Security class and area parameters using the **thConfig** command.

For complete information about security monitoring, refer to Security monitoring guidelines and default settings on page 50.

SFP monitoring

The SFP class groups areas that monitor the physical aspects of an SFP, such as voltage, current, RXP, and TXP for physical ports, E_Ports, FOP_Ports, and FCU_Ports. An SFP class alarm alerts you to an SFP fault. You can customize SFP class and area parameters using the **thConfig** command.

Use the **thMonitor** command to monitor the Brocade 10 Gbps and 16 Gbps SFP modules and 16 Gbps QSFPs. By default, the 10 Gbps SFP and the 16 Gbps SFP and QSFP are disabled. Refer to 16 Gbps SFP and QSFP monitoring on page 58 for more information.

NOTE
SFPs connected to any GbE ports are not monitored by Fabric Watch.

For complete information about SFP monitoring, refer to SFP monitoring guidelines and default settings on page 52.

Port monitoring

Port monitoring monitors port statistics and takes action based on the configured thresholds and actions. You can configure thresholds per port type and apply the configuration to all ports of the specified type using the **portThConfig** command. Configurable ports include physical ports, E_Ports, optical F_Ports (FOP_Ports), copper F_Ports (FCU_Ports), and Virtual E_Ports (VE_Ports).

NOTE
The execution of the **portThConfig** command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to the *Fabric OS Command Reference* for more information and for details about the **portThConfig** command.

For complete information about port monitoring, including configuration examples, port setting guidelines, and default settings, refer to Port Monitoring on page 65.

Port persistence

The data collected in port monitoring can vary a great deal 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.

To set the port persistence time, refer to Setting the port persistence time on page 79.

Port fencing

A port that is consistently unstable can harm the responsiveness and stability of the entire fabric and diminish the ability of the management platform to control and monitor the switches within the fabric. Port fencing is a Fabric Watch enhancement that takes the ports offline if the user-defined thresholds are exceeded. Supported port types include physical ports, E_Ports, optical F_Ports (FOP_Ports), copper F_Ports (FCU_Ports), and Virtual E_Ports (VE_Ports).

NOTE
Port fencing is not enabled by default. You must manually enable port fencing. Refer to Port fencing configuration on page 80 for instructions.

When a port that has exceeded its user-defined thresholds is fenced by the software, the port is placed into the disabled state and held offline. After a port is disabled, the user must manually enable the port for frame traffic to resume on the port.

System resource monitoring

System resource monitoring enables you to monitor your system’s RAM, flash, and CPU. You can use the **sysMonitor** command to perform the following tasks:

- Configure thresholds for Fabric Watch event monitoring and reporting for the environment and resource classes. Environment thresholds enable temperature monitoring, and resource thresholds enable monitoring of flash memory.
- Use the RAM to configure memory or CPU usage parameters on the switch or display memory or CPU usage. Configuration options include setting usage thresholds which, if exceeded, trigger a set of specified Fabric Watch alerts. You can set up the system monitor to poll at certain intervals and specify the number of retries required before Fabric Watch takes action.

For complete information about system resource monitoring, including setting guidelines and default settings, refer to System monitoring using the sysMonitor command on page 89.

Switch policies

Switch policies are a series of rules that define specific health 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, and flash memory.

Refer to Switch status policy planning on page 93 for information on configuring switch policies.

Refer to Fabric Watch reports on page 107 for information on viewing the current switch policies using the Switch Status Policy report.

Logical switch support

Fabric Watch can monitor the switch health on eight logical switches. You can configure thresholds and notifications for ports that belong to a particular logical switch. Each logical switch has its own Fabric Watch configuration and triggers notifications based on its local configuration.

Fabric Watch supports port movement from one logical switch to another. Whenever a port is moved, thresholds associated with the port are deleted from the logical switch from which the port was moved, and created for the logical switch to where the port is moved.

On logical interswitch links (LISLs), Fabric Watch supports state change notifications in the same manner as for normal E_Ports and uses the same threshold values for LISLs as for E_Ports, but does not support threshold areas such as link loss or signal loss.

Threshold monitoring using SNMP tables

Understanding the components of SNMP makes it possible to use third-party tools to view, browse, and manipulate Brocade switch variables remotely. Every Brocade switch and director supports SNMP.

When an event occurs and its severity level is at or below the set value, the Event Trap traps (swFabricWatchTrap), are sent to configured trap recipients.

Once the switch status policy changes, Fabric Watch sends a connUnitStatusChange SNMP trap, and any existing Fabric Watch RASLog is converted into an swEventTrap.

Refer to the Fabric OS release notes, the *Fabric OS Administrator's Guide*, and the MIB files themselves for information about the following:

- Understanding SNMP basics
- How to enable or disable the sending of traps from the various MIBs
- SNMP trap bitmask values
- Loading Brocade Management Information Bases (MIBs)

MIB capability configuration parameters

The **mibCapability** option turns certain MIBs and associated SNMP traps on or off. If a specific MIB is disabled, the corresponding traps are also disabled. If any trap group is disabled, the corresponding individual traps are also disabled.

Refer to the Fabric OS release notes, the *Fabric OS Administrator's Guide*, and the MIB files themselves for detailed information about the following SNMP tables that can be used to manage thresholds:

- swFwClassAreaTable
- swFwThresholdTable

Fabric Watch event settings

Fabric Watch uses two types of settings: factory default settings and user-defined custom settings.

- Factory default settings are automatically enabled. These settings vary depending on hardware platform, and cannot be modified.
- You can create custom configurations to suit your unique environment.

You must first use the **fwSetToCustom** command to switch from default to custom settings, and then use the advanced configuration options provided with the **portThConfig** , **thConfig** , and **sysMonitor** commands to configure event behavior, actions, and time bases at the port level.

Use the advanced configuration option provided with the **portThConfig** , **thConfig** , and **sysMonitor** commands to view and modify custom and default values for specified classes and areas in Fabric Watch. You can customize the information reported by Fabric Watch by configuring event behavior types, threshold values, time bases, and event settings. These area attributes are used to define and detect events in Fabric Watch.

Fabric Watch notification types

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 alarm options.

E-mail alerts

An e-mail alert sends information about a switch event to a one or multiple specified e-mail addresses. An e-mail alert can send information about any error from any element, area, and class (only one e-mail recipient can be configured per class). The e-mail specifies the threshold and describes the event, much like an error message. You can configure multiple e-mail recipients per class using the **fwMailCfg** command. You must separate the e-mail addresses with a comma and include the complete e-mail address. For example, abc@12.com is a valid e-mail address; abc@12 is not.

For a recipient to receive the e-mail alert, you must configure one of the following settings:

- Use the **dnsConfig** command to configure DNS settings to connect the switch to a DNS server.
- In case a DNS server is not available, e-mail alerts can be forwarded through a relay host. You can configure the relay host IP address using the **fwMailCfg** command.

Enabling e-mail alerts for the Changed threshold state in several areas can quickly result in a significant amount of e-mail. Fabric Watch discards e-mail alerts when more than 100 are generated within a minute, which minimizes memory use.

SNMP traps

In environments where you have a high number of messages 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, the Simple Network Management Protocol (SNMP) notifications might be the most efficient notification method. You can avoid having to log in to each switch individually as you would have to do for error log notifications.

SNMP performs an operation called a *trap* that notifies a management station using SNMP when events occur. 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, error messages at that level trigger SNMP traps.

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

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. You can configure SNMP notifications using the **snmpConfig** command and you can configure notifications using Fabric Watch.

For information on configuring the SNMP agent using the **snmpConfig** command, refer to the *Fabric OS Command Reference*.

SNMP trap counters

- When a counter is in the "in-between" state, Fabric Watch sends an informational SNMP trap. Refer to In-between buffer values on page 25 for an explanation of the concepts of "in-between" boundaries and above high, below high, above low, and below low thresholds.
- When a counter is above the high threshold or below the low threshold, Fabric Watch sends a warning SNMP trap except for the power supply area of the environment (ENV), CPU, and Memory classes. The severity of a Fabric Watch SNMP trap for CPU and memory will always be informational.

Refer to Threshold values on page 25 for a more thorough explanation of thresholds.

RASLog for switch events

Following an event, Fabric Watch adds an entry to the internal event log for an individual switch. The RASLog stores event information but does not actively send alerts. Use the **errShow** command to view the RASLog.

Locked port log

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

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

Fabric Watch audit messages

Fabric Watch events caused by configuration value changes are tagged as Audit messages. When managing SANs you may want to filter or audit certain classes of events to ensure that you can view and generate an audit log for what is happening on a switch, particularly for security-related event changes. These events include login failures, zone configuration changes, firmware downloads, and other configuration changes; in other words any critical changes that have a serious effect on the operation and security of the switch.

Important information related to event classes is also tracked and made available. For example, you can track changes from an external source by the user name, IP address, or type of management interface used to access the switch.

NOTE
Audit messages are generated for port fencing configuration changes, whether port fencing is enabled or disabled.

You can set up an external host to receive Audit messages so you can easily monitor unexpected changes. For information on error messages generated by Fabric Watch, refer to the *Fabric OS Message Reference*. For information on configuring an Audit Log, refer to the "Audit Log Configuration" section of the *Fabric OS Administrator's Guide*.

Data values

A data value represents a measured value or a state value, described as follows:

- *Measured value* — The current, measurable value of a fabric or fabric element, such as environmental temperature.
- *State value* — The only qualitative data value information on the overall state of a fabric component. Instead of numerical data, state values contain information on whether components are faulty, active, or in another state.

NOTE
Either measured values or state values can be used; mixed values are not supported.

Fabric Watch compares the 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.

Time bases specify the time interval between two samples to be compared. You can set the time base to day (samples are compared once a day), hour (samples are compared once an hour), or minute (samples are compared every minute). Second samples are not advisable. This configurable field affects the comparison of sensor-based data with user-defined threshold values.

Refer to Time bases on page 27 for more information.

Fabric Watch support in Access Gateway mode

Both the Advanced Performance Monitoring (APM) license and the Fabric Watch license must be installed on the platform configured in Access Gateway (AG) mode to use the frame monitoring and end-to-end (EE) monitoring capabilities. The APM license provides the counters and the Fabric Watch license provides the monitoring and alert mechanisms for these counters. Refer to Setting the high threshold of the RX area of an EE monitor on page 57 for configuration information.

The following classes are not supported in Access Gateway mode:

- Fabric
- Security
- E_Port (Port subclass)
- VE_Port (Port subclass)

Fabric Watch Thresholds

Threshold values

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 because of overheating or freezing.

With Fabric Watch v6.4 and later, there are four threshold categories:

- Above high threshold — Fabric Watch takes this action when the current value is above the high threshold.
- Below high threshold — Fabric Watch takes this action when the current value is between the high and low threshold.
- Above low threshold — This action is only applicable to port classes (physical port, FOP_Port, FCU_Port, and VE_Port). Fabric Watch takes this action when the current value crosses the low threshold towards the high threshold.
- Below low threshold — Fabric Watch takes this action when the current value is below the low threshold.

NOTE
The above low threshold action applies only to the **portThConfig** command. It does not apply to the **thConfig** and **sysMonitor** commands.

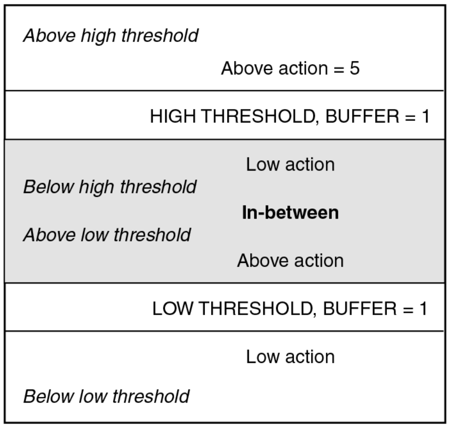
In-between buffer values

The below high threshold is the term used to configure "in between" buffer values, as shown in the figure below.

The following example the high threshold value is 5 and the buffer value is 1. Therefore, the "in-between" boundary value is 4.

```
switch:admin> portthconfig --set port -area crc -highth -value 5 -trigger below -
action raslog -buffer 1
```

FIGURE 1 In-between buffer values



Threshold triggers

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 affects event triggering.

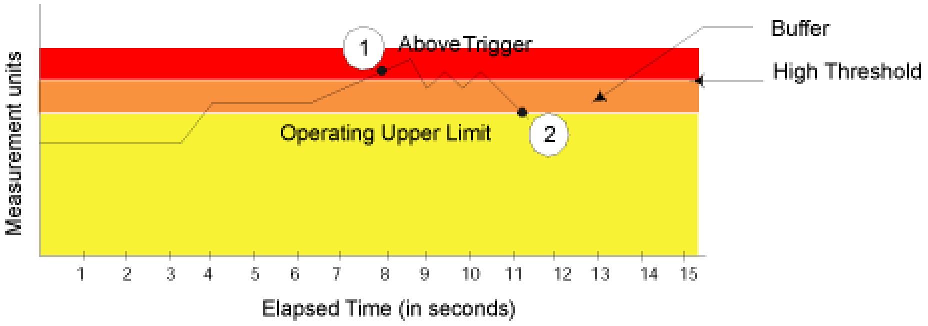
For Fabric Watch to monitor data values for one of the following conditions, the alarm setting must be set to a nonzero value.

Above event trigger

Set 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 goes above the high threshold and fluctuates around it. The next event will not occur until the counter value falls below the buffer zone created by the high threshold. The figure below shows an Above event trigger with a buffer zone. The Above event trigger occurs when the counter crosses the high threshold (event 1 in the figure below). When the data value becomes less than the high threshold and buffer value, Fabric Watch triggers a second event (event 2) to indicate that it has returned to normal operation. The second event will not be triggered until the counter value falls below the high threshold and buffer values.

FIGURE 2 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 event will be triggered only when the value goes below the lower threshold. A second event will not be generated until the value crosses the buffer region set above the lower threshold.

Audit and RASLog messages

Fabric Watch generates an Audit message along with a RASLog message when the current threshold exceeds the high threshold limit configured for the following thresholds:

- SCSI reservation
- Class 3 discards (C3TXT0)
- Switch memory usage
- Switch flash usage
- Switch CPU usage

Time bases

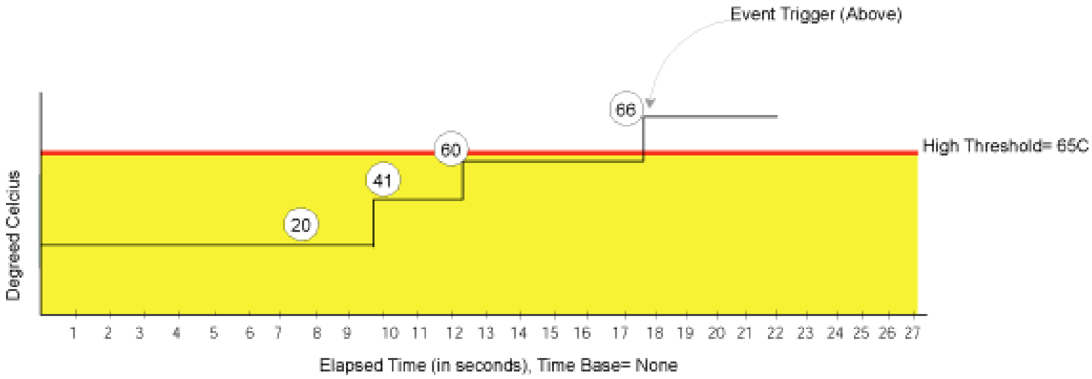
Time bases specify the time interval between two samples to be compared. You can set the time base to day (samples are compared once a day), hour (samples are compared once an hour), minute (samples are compared every minute). This configurable field affects the comparison of sensor-based data with user-defined threshold values.

Time base set 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.

The figure below shows a high limit of 65° Celsius placed on a counter measuring temperature. During each sample period, Fabric Watch measures the temperature and compares it to the high threshold. If the measured temperature exceeds the high threshold, it triggers an event.

FIGURE 3 Time base set to none



Time base set to other than none

If you specify a time base value other than **none** (**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.

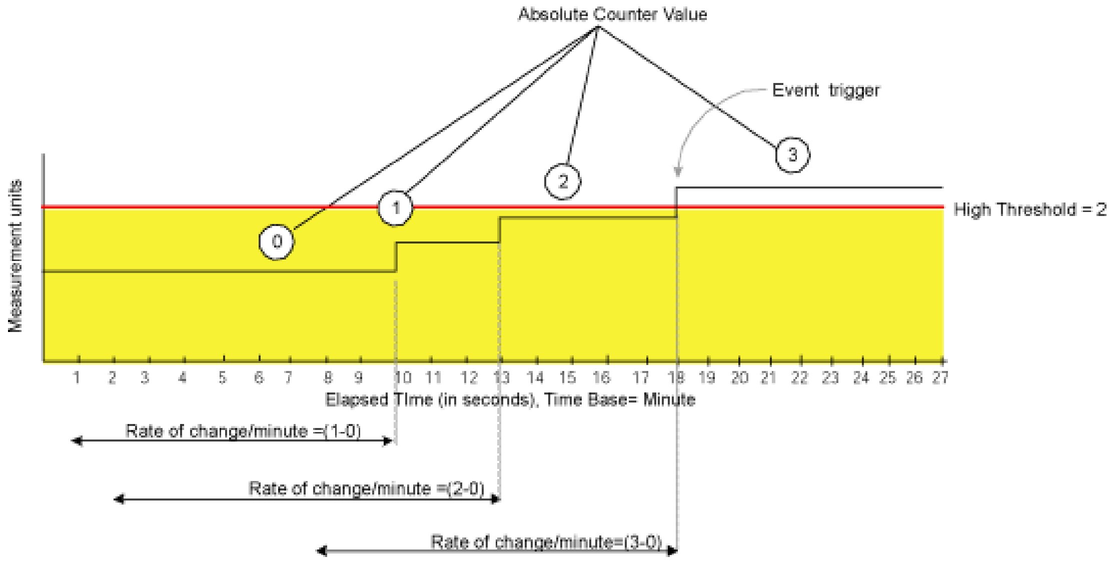
When you set a time base to a value other than **none**, there are two main points to remember when configuring events:

- 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 figure below 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; thus the 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 4 Event trigger



Fabric Watch alarm behavior

Fabric Watch alarm behavior depends on the threshold states associated with the Above, Below and Changed thresholds. Threshold states can be INFORMATIVE, IN_RANGE, and OUT_OF_RANGE. Notifications are generated only for the following transitions:

- IN_RANGE to OUT_OF_RANGE
- OUT_OF_RANGE to IN_RANGE

No alarm is generated for INFORMATIVE to IN_RANGE (or IN_RANGE to INFORMATIVE).

Fabric Watch Threshold Components

Fabric Watch classes, areas, and elements

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 wide groupings of similar fabric devices or fabric data. Elements on page 32 describes the classes into which Fabric Watch groups all switch and fabric elements.

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.

Class 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”.

For detailed information about how to configure areas, including recommended threshold and action settings for the classes listed in Elements on page 32, refer to one of the following chapters:

- Fabric, Security, SFP, and Performance Monitoring on page 47.

  Fabric class, Security class, SFP class, and Performance class areas and actions are configured using the **thConfig** command.

- Port Monitoring on page 65.

  The physical port and its subclass areas and actions are configured using the **portThConfig** command.

- System Monitoring on page 87.

The Resource class and Environment class areas and actions are configured using the **sysMonitor** command. The FRU class actions are configured using the **fwFruCfg** command

Elements

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

Each element contains information pertaining to the description suggested by the area. To continue the Ports example, each element in the Invalid Transmission Words area of the Ports class 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 1 can be viewed by accessing the first temperature sensor within the temperature area of the environment class.

Subclasses are a minor exception to the preceding mapping 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.

The table below describes the classes into which Fabric Watch groups all switch and fabric elements.

TABLE 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. Configure the Environment class using the **sysMonitor** command.
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. Configure the Fabric class using the **thConfig** command.
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. Configure the FRU class using the **fwFruCfg** command.

TABLE 1 Fabric Watch classes (Continued)

Class	Description
Performance Monitor	Serves as a tuning tool. The Performance Monitor class groups areas that track the source and destination of traffic. Use the Performance Monitor class thresholds and notifications to determine traffic load and flow and to reallocate resources appropriately. The Performance Monitor class is divided into the following areas: EE (end-to-end) Performance Monitor, and Filter Performance Monitor. **NOTE** Performance Monitoring is not supported on VE_Ports, EX_Ports, and VEX _Ports. Configure the Performance class using the **thConfig** command.
Port	Enables you to set additional thresholds specific to different types of ports. The Port class is made up of the following sub-classes: • E_Port class — Represents ports connected to another switch. • FOP_Port class — Represents fabric or fabric loop ports that are made of optical fiber. • FCU_Port class — Represents fabric or fabric loop ports that are made of copper. • VE_Port — Represents a port that is similar to the E_Port but terminates at the switch and does not propagate fabric services from one edge fabric to another. Configure the Port class using the **portThConfig** command.
Resource	Manages your system’s memory or CPU usage. Monitors flash memory. It calculates the amount of flash space consumed and compares it to a defined threshold. Configure the Resource class using the **sysMonitor** command.
Security	Monitors all attempts to breach your SAN security, helping you fine-tune your security measures. Configure the Security class using the **thConfig** command.
SFP	Groups areas that monitor the physical aspects of SFPs. An SFP class alarm alerts you to an SFP malfunction fault. SFP performance monitoring is not supported on VE_Ports. **NOTE** SFPs connected to any GbE ports are not monitored. Configure the SFP class using the **thConfig** command.

Fabric Watch Activation

Interfaces for activating Fabric Watch

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

- Telnet session — Provides a command prompt where you can run Fabric OS commands to configure your switch monitoring settings. Refer to Activating Fabric Watch using a Telnet session on page 35 for instructions on how to activate Fabric Watch using a Telnet session.
- SNMP — Provides a receiver dedicated to monitoring the data center infrastructure; Brocade switches and directors enable monitoring of specific incidents and trigger an SNMP alert based on a user-defined threshold sending the alert to the dedicated SNMP trap receiver.

  Configuring SNMP threshold alerts for Fabric OS switches requires using Web Tools to set up SNMP on the Fabric OS switch. Refer to Activating Fabric Watch using SNMP on page 36 for instructions on how to set up SNMP.
- Web Tools — Provides a graphical user interface that can be launched from an Internet browser, which allows you to launch a Fabric Watch window to configure switch monitoring settings. Using Web Tools, you can configure thresholds, alarms, and e-mail notifications. Refer to Fabric Watch Activation on page 35 for instructions on how to configure Fabric Watch using the Web Tools GUI.

Activating Fabric Watch using a Telnet session

1. Connect to the switch and log in as admin.
2. Enter the **telnet** *switch* command, where *switch* is either the name or IP address of the switch.

   ```
   switch:admin> telnet
   ```

   After you enter this command, respond to the prompts for a user name and password.

   NOTE
   You can also use PuTTY or a similar application to log in.
3. Enter the **licenseShow** command to determine if the Fabric Watch license is installed.

   ```
   switch:admin> licenseshow
   edzbzQStu4ecS:
       Fabric Watch license
       Performance Monitor license
   Trunking license
   Full Ports on Demand license - additional 16 port upgrade license
   ```

   If the Fabric Watch license is not listed, continue to step 4; otherwise, you are ready to use Fabric Watch.

4. Enter the license key with the **licenseAdd** *key* command, 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"
```

5. Enter the **licenseShow** command to verify successful activation. If the license is not listed, verify that you typed the key correctly; if you did not, then repeat step 4.

   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 4.

6. Enter the **fwClassinit** command to initialize the Fabric Watch classes.

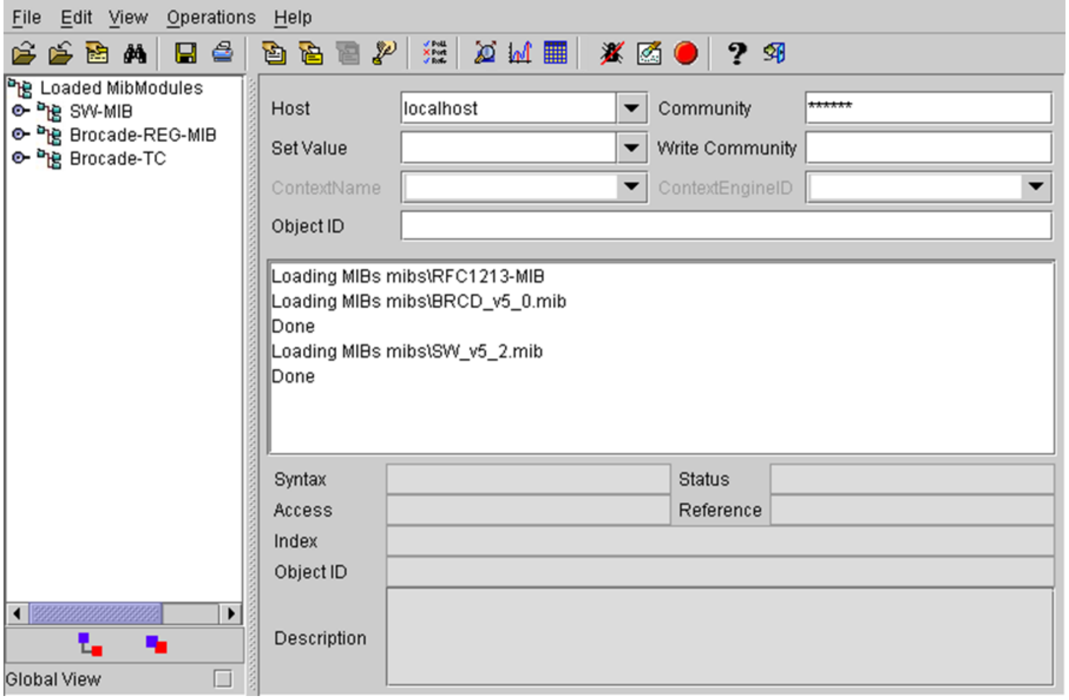
Activating Fabric Watch using SNMP

You can integrate Fabric Watch with existing enterprise systems management tools, such as SNMP. The Fabric Watch Management Information Base (MIB) lets system administrators configure fabric elements, receive SNMP traps generated by fabric events, and obtain the status of fabric elements through SNMP-based enterprise managers.

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

1. Open a MIB browser.
2. Load the appropriate MIB files if you have not already done so.
3. Load the Brocade common MIB file, SW.mib first. If this is successful, the system displays a window similar to that displayed in the figure below.

FIGURE 5 Configuring Fabric Watch using SNMP



Host localhost

Community ******

```
Loading MIBs mibs\RFC1213-MIB
Loading MIBs mibs\BRCD_v5_0.mib
Done
Loading MIBs mibs\SW_v5_2.mib
Done
```

In the above figure, the MIB browser populated the left side of the window with a MIB tree that you can navigate.

4. Open Web Tools and select **Tasks** > **Manage** > **Switch Admin**.
5. Click **Show Advanced Mode**.
6. On the **SNMP** tab, enter the IP address of the trap receiver and the severity level, and click **Apply**.

NOTE
The severity level must be Informational (4) in order to forward threshold alerts.

7. Start a Telnet session, and enter the **snmpConfig --set mibcapability** command at the prompt to set the SNMP MIB capability.

```
switch:admin> snmpConfig --set mibcapability
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]
```

8. Enter the **snmpConfig --set snmpv1** or **--set snmpv3** (depending on your configuration) command to configure the SNMP management host IP address.

```
switch:admin> snmpConfig --set snmpv1
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] 1080::8:800:200C:417A
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]
…
Committing configuration...done.
```

9. Enter the IP address for the switch in the **Host** field in the MIB browser. Enter the community string in the **Community** field. To perform set operations, enter the write community in the **Write Community** field.
10. View and listen for trap details from a MIB browser menu.

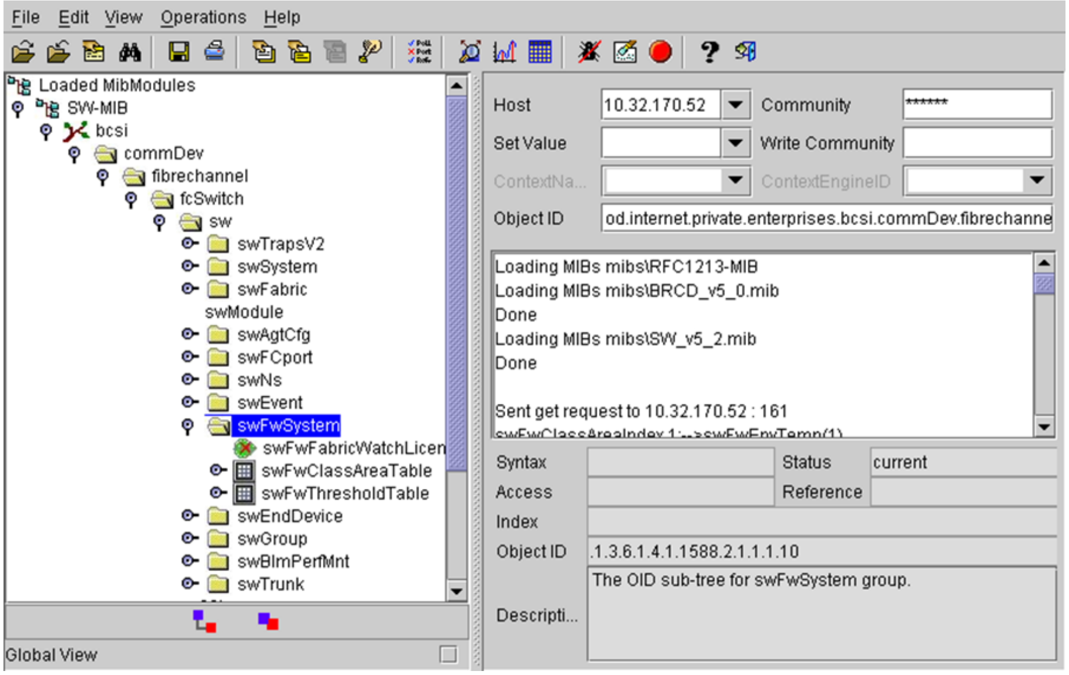
NOTE
Any changes related to Fabric Watch, such as changing the status of the temperature sensor, will generate traps.

---

11. Expand the tree on the left to find the Fabric Watch OID information.

    To find the OID, navigate the following hierarchy: **SW-MIB** > **bcsi** > **commDev** > **fibrechannel** > **fcSwitch** > **sw** > **swFWSystem**. Fabric Watch displays a window similar to the one shown in the figure below.

FIGURE 6 Example OID tree



Host: 10.32.170.52
Community: ******
Set Value:
Write Community:
ContextNa...:
ContextEngineID:
Object ID: od.internet.private.enterprises.bcsi.commDev.fibrechanne

```
Loading MIBs mibs\RFC1213-MIB
Loading MIBs mibs\BRCD_v5_0.mib
Done
Loading MIBs mibs\SW_v5_2.mib
Done

Sent get request to 10.32.170.52 : 161
swFwClassAreaIndex.1:-->swFwEnvTemp(1)
```

Syntax:
Status: current
Access:
Reference:
Index:
Object ID: .1.3.6.1.4.1.1588.2.1.1.1.10
Descripti...: The OID sub-tree for swFwSystem group.

12. 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.

    For detailed descriptions of the SNMP fields in both Telnet and Web Tools, refer to the Fabric OS release notes, the *Fabric OS Administrator's Guide*, and the MIB files themselves.

Activating Fabric Watch using Web Tools

You can open Web Tools on any workstation with a compatible Web browser installed.

1. Open the Web browser and type the IP address of the device in the Address field. For example, http://10.77.77.77 or https://10.77.77.77
2. Press **Enter**.

   A browser window opens to open Web Tools. A login dialog box opens.
3. Enter your user name and password.
4. Select a switch from the Fabric Tree and log in if necessary.
5. Select **Tasks** > **Manage** > **Fabric Watch**.

   For information about how to configure Fabric Watch using Web Tools, refer to Fabric Watch Configuration Using Web Tools on page 99.

Fabric Watch Configuration

Fabric Watch configuration tasks

The table below lists the Fabric Watch commands you can use to create custom threshold configurations. For complete information about any of these commands, refer to the *Fabric OS Command Reference*.

TABLE 2 Fabric Watch configuration tasks

Configuration task	Command	Location of procedure
Initialize all Fabric Watch classes.	**fwClassInit**	Activating Fabric Watch using a Telnet session on page 35
Set the boundary and alarm level to custom or default.	**fwSetToCustom** **fwSetToDefault**	Setting Fabric Watch custom and default values on page 43
NOTE These commands reset all thresholds for all classes and cannot be configured on individual ports.		
Configure Fabric Watch e-mail alerts for all classes.	**fwMailCfg**	E-mail notification configuration on page 43
Configure and show alarms filtering for Fabric Watch for all classes.	**fwAlarmsFilterSet** **fwAlarmsFilterShow**	Configuring alarm notifications on page 46
Set the following parameters for SFP, Fabric, Security, and Performance monitoring: • Class • Area type • Time base • Threshold level • Trigger (boundary level) • Action (notification type) • Buffer	**thConfig**	Fabric monitoring guidelines and default settings on page 47 Security monitoring guidelines and default settings on page 50 Performance monitoring guidelines and default settings on page 54
Enable or disable monitoring for the 10 Gbps and 16 Gbps SFPs and QSFPs.	**thMonitor**	SFP monitoring guidelines and default settings on page 52

TABLE 2 Fabric Watch configuration tasks (Continued)

Configuration task	Command	Location of procedure
Set the following parameters for port monitoring: • Port type • Area type • Time base • Threshold level • Trigger (boundary level) • Action (notification type) • Buffer • Port fencing	**portThConfig** **portFencing**	Port Monitoring on page 65
Set the port persistence time.	**fwSet --port -persistence**	Setting the port persistence time on page 79
Configure port fencing.	**portFencing**	Port fencing on page 79
Set the following parameters for system monitoring: • Class • Area type • Threshold level • Trigger (boundary level) • Action (notification type) • Buffer	**sysMonitor**	System monitoring using the sysMonitor command on page 89
Set and display the switch status policy parameters.	**switchStatusPolicySet** **switchStatusPolicyShow**	System Monitoring on page 87
Show the overall switch status.	**switchStatusShow**	System Monitoring on page 87
Configure FRU state and notifications, and monitor power supply, fan, and SFP FRUs.	**fwFruCfg**	System Monitoring on page 87
Display fan status.	**fanShow**	System Monitoring on page 87
Show sensor readings.	**sensorShow**	System Monitoring on page 87
Show switch temperature readings.	**tempShow**	System Monitoring on page 87
Create a detailed port report.	**fwPortDetailShow**	Generating a Port Detail report on page 110
Show the availability of monitor information.	**fwSamShow**	Switch Availability Monitor report on page 108

Setting Fabric Watch custom and default values

Use the following commands to switch between custom and default values. These commands reset all thresholds for all classes:

- **fwSetToCustom** — Sets the boundary and alarm level to custom.
- **fwSetToDefault** — Restores the boundary and alarm level to the default.

E-mail notification configuration

In environments where it is critical that you are notified about errors quickly, you can use e-mail notifications. With e-mail notifications, you can be notified of serious errors by e-mail or a pager, so you can react quickly.

To configure e-mail notifications in a Telnet session, perform the following steps:

1. Log in using Telnet or PuTTY.
2. Enter the **fwMailCfg** command at the prompt.
3. Enter the number from the mail configuration menu corresponding to the task you wish to perform.

The following shows the default response to the **fwMailCfg** command:

```
switch# fwMailCfg
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  : Relay Host IP Configuration
7  : Quit
Select an item  => : (1..7) [7]
```

Showing e-mail configuration information

1. Enter `1` in the **fwMailCfg** menu to view the current e-mail configuration classes.

   The Config Show menu displays:

   ```
   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 e-mail address.

2. Enter the number corresponding to the class for which the e-mail configuration should be displayed.

Fabric Watch displays e-mail alert information such as:

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

The system returns to the main **fwMailCfg** menu.

Disabling an e-mail alert

1. Enter `2` in the **fwMailCfg** menu to disable e-mail alerts for a specific class.
2. Select a class for which Fabric Watch should disable e-mail alerts from the Config Show menu.

   The following confirmation message displays:

   ```
   Email Alert is disabled!
   ```

   The system returns to the **fwMailCfg** menu.

Enabling an e-mail alert

1. Enter **3** in the **fwMailCfg** menu to enable e-mail alert for a specific class.
2. Select a class for which Fabric Watch should enable e-mail alerts from the Config Show menu.

   The following confirmation message displays:

   ```
   Email Alert is enabled!
   ```

   If the class does not have an e-mail configuration (there is no e-mail address assigned to the class), the following error message displays:

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

   The system returns to the **fwMailCfg** menu.

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

Sending a test e-mail message

1. Enter **4** in the **fwMailCfg** menu to test the e-mail configuration for a specific class.

   The Config Show menu displays.
2. Select a class to test.

   If the e-mail configuration for the class is complete, the following confirmation message displays:

   ```
   Email has been sent
   ```

   If the e-mail configuration for the class is not complete, the following error message displays:

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

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

   The system returns to the **fwMailCfg** menu.

Setting the recipient e-mail address for an e-mail alert

1. Enter **5** in the **fwMailCfg** menu to specify the recipient to whom Fabric Watch should send the e-mail alert for a class.

   The Config Show menu displays.
2. Select a class.

   The following prompt displays:

   Mail To: [NONE]
3. Enter the e-mail 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 e-mail address for the class. A value of NONE indicates that no e-mail address has been provided.

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

Setting the relay host IP address

1. Enter **6** in the **fwMailCfg** menu to configure a relay host IP address.

   The relay host configuration menu is displayed.

   ```
   1 Display Relay Host configuration
   2 Set Relay Host IP
   3 Remove Relay Host configuration
   4 Quit
   ```
2. Select **2** to set the relay host IP address.

   The following message displays:

   ```
   enter the Relay Host IP:
   ```
3. Enter the relay host IP address (example: 192.168.39.118).

   The following message displays:

   ```
   Setting 192.168.39.118 as Relay Host...
   ```
4. Enter the Domain Name (example: Brocade.com).

Displaying the relay host configuration

1. Enter **6** in the **fwMailCfg** menu to display the relay host configuration menu.
   ```
   1 Display Relay Host configuration
   2 Set Relay Host IP
   3 Remove Relay Host configuration
   4 Quit
   ```
2. Enter **1** to display the configuration.

Removing the relay host configuration

1. Enter **6** in the **fwMailCfg** menu to display the relay host configuration menu.
   ```
   1 Display Relay Host configuration
   2 Set Relay Host IP
   3 Remove Relay Host configuration
   4 Quit
   ```
2. Enter **3** to remove the configuration.

Notification configuration

Notifications act as a signal or alert that notifies you when a threshold has been crossed.

When you use alarm notifications, error messages are sent to designated locations such as an error log, SNMP trap view, or e-mail. 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.

Configuring alarm notifications

1. Ensure that notifications appear in the error log by using the following command.

   ```
   switch:admin> fwAlarmsFilterSet 1
   ```

   The **1** option turns on the alarm notification.
2. Enter the following command if you decide not to have notifications sent.

   ```
   switch:admin> fwAlarmsFilterSet 0
   ```

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

   All notifications are suppressed when alarm notifications are turned off, except for the Environment class and Resource class.
3. Verify or view your current alarm notifications by using the **fwAlarmsFilterShow** command.

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

Fabric, Security, SFP, and Performance Monitoring

Fabric monitoring guidelines and default settings

The Fabric class 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.

Fabric class areas

The table below lists Fabric Watch areas in the Fabric class and describes each area. Although it is recommended that you leave the entire Fabric class in its default state (no alerts), you can configure the Fabric class using the **thConfig** command.

TABLE 3 Fabric class areas

Area	Description
Domain ID changes (DC)	Monitors forced domain ID changes. Forced domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch must assign another domain ID to a switch.
Fabric logins (FLOGI)	Activates when ports and devices initialize with the fabric.
Fabric reconfigurations (FC)	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 or VE_Port goes offline. • A principal link segments from the fabric.
E_Port downs (ED)	Tracks the number of times that an E_Port or VE_Port goes down. E_Ports and VE_Ports go down each time you remove a cable or an SFP (where there are SFP failures or transient errors).

TABLE 3 Fabric class areas (Continued)

Area	Description
Segmentation changes (SC)	Tracks the cumulative number of segmentation changes. Segmentation changes occur because of one of the following: • Zone conflicts. • Incompatible link parameters. During E_Port and VE_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.
Zone changes (ZC)	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.

Fabric monitoring setting guidelines

It is recommended that you leave the entire Fabric class in its default state (no alerts) for the following reasons:

- Domain ID changes

  Plan and use strict change control practices to avoid Domain ID changes.
- Loss of E_Port

  Detect if an E_Port is down using the E_Port class areas.
- Fabric logins

  In a large environment of numerous devices, this area is of no interest.
- Fabric reconfiguration

  Fabric reconfigurations typically occur when new switches are added to a fabric, which is a planned activity, or when an upstream or downstream ISL fails, which is detected through the E_Port class areas. Because fabric reconfigurations are monitored elsewhere, do not change the default settings for the Fabric class.
- Segmentation changes

  Segmentations only occur in the event of an entire switch failure. In this rare case, you can gather multiple reports from all the attached E_Ports of the link failures.
- Zoning changes

  Zone changes are captured through the Audit facility in Fabric OS. All zone changes can be configured to be recorded in the RASLog, which is the recommended practice.

Fabric class default settings

The table below provides default settings for areas in the Fabric class.

TABLE 4 Fabric class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Domain ID changes	Monitors forcible DOMAIN ID changes	Unit: D_ID Changes Time Base: none Low: 0 High: 0 Buffer: 0	Below: 0 Above: 0	Informative Informative
Loss of E_Port	Monitors E_Port and VE_Port status	Unit: Downs Time Base: none Low: 0 High: 0 Buffer: 0	Below: 0 Above: 0	Informative Informative
Fabric logins (FLOGI)	Monitors host device fabric logins	Unit: Logins Time Base: none Low: 0 High: 0 Buffer: 0	Below: 0 Above: 0	Informative Informative
Fabric reconfiguration	Monitors configuration changes	Unit: Reconfigs Time Base: none Low: 0 High: 0 Buffer: 0	Below: 0 Above: 0	Informative Informative
Segmentation changes	Monitors segmentation changes	Unit: Segmentations Time Base: none Low: 0 High: 0 Buffer: 0	Below: 0 Above: 0	Informative Informative
Zoning changes	Monitors changes to currently-enabled zoning configurations	Unit: Zone changes Time Base: none Low:0 High:0 Buffer: 0	Below: 0 Above: 0	Informative Informative

Security monitoring guidelines and default settings

The Security class monitors all attempts to breach your SAN security, helping you fine-tune your security measures.

Security class areas

The table below lists Fabric Watch areas in the Security class and describes what each area indicates. Although it is recommended that you leave the entire Security class in its default state (no alerts), you can configure the Security class using the **thConfig** command.

TABLE 5 Security class areas

Area	Description
DCC violations (DV)	An unauthorized device attempts to log in to a secure fabric.
HTTP violations (HV)	A browser access request reaches a secure switch from an unauthorized IP address.
Illegal commands (IV)	Commands permitted only to the primary Fibre Channel Switch (FCS) are executed on another switch.
Incompatible security DB (ISB)	Secure switches with different version stamps have been detected.
Login violations (LV)	Login violations which occur when a secure fabric detects a login failure.
Invalid certifications (IC)	Invalid security certificates have been detected.
No-FCS (NF)	The switch has lost contact with the primary FCS.
SCC violations (SV)	SCC violations which occur when an unauthorized switch tries to join a secure fabric. The WWN of the unauthorized switch appears in the ERRLOG.
SLAP failures (FSLAP)	SLAP failures which occur when packets try to pass from a nonsecure switch to a secure fabric.
Telnet violations (TV)	Telnet violations which occur when a Telnet connection request reaches a secure switch from an unauthorized IP address.
TS out of sync (TS)	Time Server (TS) errors which occur when an out-of-synchronization error has been detected.

Security monitoring default settings

Use the Security class default settings shown in the table below for area and notification configuration. There is no reason to alter the default settings.

TABLE 6 Security class area default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
DCC violations (DV)	Monitors DCC violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range
HTTP violations (HV)	Monitors HTTP violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range
Illegal commands (IV)	Monitors illegal commands	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range
Incompatible security DB (ISB)	Monitors incompatible security databases	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range
Login violations (LV)	Monitors login violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range
Invalid certifications (IC)	Monitors invalid certifications	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range

TABLE 6 Security class area default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
No-FCS (NF)	Monitors No FCS violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range
SCC violations (SV)	Monitors SCC violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range
SLAP failures (FSLAP)	Monitors SLAP failures	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range
Telnet violations (TV)	Monitors Telnet violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range
TS out of sync (TS)	Monitors instances in which the timestamp is out of sync	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Below: 0 Above: 3	Informative Out_of_range

SFP monitoring guidelines and default settings

The SFP class groups areas that monitor the physical aspects of SFPs. An SFP class alarm alerts you to an SFP malfunction fault. SFP performance monitoring is not supported on VE_Ports.

When a port goes offline, the RXP and TXP area values of the SFP become zero. Brocade recommends non-zero low thresholds for RXP and TXP; therefore, Fabric Watch stops monitoring RXP and TXP parameters of the SFP once the port goes offline.

SFP class areas

The table below lists Fabric Watch areas in the SFP class and describes each area. Although it is recommended that you leave the entire SFP class in its default state (no alerts), you can configure the SFP class using the **thConfig** command.

NOTE
SFPs connected to GbE ports are not monitored.

TABLE 7 SFP class areas

Area	Description
Temperature	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 (RXP)	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 (TXP)	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	Measures the amount of supplied current to the SFP transceiver in Amps. Current area events indicate hardware failures.
Voltage	Measures the amount of voltage supplied to the SFP. If this value exceeds the threshold, the SFP is deteriorating.

SFP monitoring default settings

The SFP default settings are shown in the below table. The default alarm configuration (log all alarms only to the error log) is sufficient. It is recommended that you do not allow alerts to go out as SNMP traps. If other Port class issues are reported, review the error log for any supporting data for SFP issues.

TABLE 8 SFP class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Temperature	Monitors SFP temperature	Unit: Degrees C Time Base: none Low: -10 High: 85 Buffer: 3	Below: 1 Above: 1	Out_of_range Out_of_range

TABLE 8 SFP class default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Receive power (RXP)	Monitors receive power	Unit: µWatts Time Base: none Low: 0 High: 5000 Buffer: 25	Below: 1 Above: 1	Out_of_range Out_of_range
Transmit power (TXP)	Monitors transmit power	Unit: µW Time Base: none Low: 0 High: 5000 Buffer: 25	Below: 1 Above: 1	Out_of_range Out_of_range
Current	Monitors SFP current	Unit: mAmps Time Base: none Low: 0 High: 50 Buffer: 1	Below: 1 Above: 1	Out_of_range Out_of_range
Voltage	Monitors SFP electrical force	Unit: mVolts Time Base: none Low: 2970 High: 3630 Buffer: 10	Below: 1 Above: 1	Out_of_range Out_of_range
Power on hours	Monitors the number of hours the SFP is powered on.	Unit: Changes Time Base: none Low: 0 High: 0 Buffer: 0	Below: 0 Above: 0	Informative Informative

Performance monitoring guidelines and default settings

Performance monitoring serves as a tuning tool. The Performance Monitor class groups 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.

NOTE
Performance Monitoring is not supported on VE_Ports.

Performance Monitor class areas

The table below lists Fabric Watch areas in the Performance Monitor class and describes each area. Although it is recommended that you leave the entire Performance Monitor class in its default state (no alerts), you can configure the Performance class using the **thConfig** command.

TABLE 9 Performance Monitor class areas

Area	Description
RXP (EE performance monitor)	The percentage of word frames traveling from the configured S_ID to the D_ID exceeds the configured thresholds.
TXP (EE performance monitor)	The percentage of word frames traveling from the configured D_ID to the S_ID; user configuration triggers these messages, so you can use the Transmit Performance area to tune your network.

Performance monitoring setting guidelines

It is recommended that you leave the entire Performance Monitor Class and End-to-End Performance Monitor Class area settings in their default state (no alerts).

Performance Monitor class default settings

The table below provides default settings for areas in the Customer-Defined Performance Monitor class.

TABLE 10 Performance Monitor class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Customer-defined filter	Monitors the number of frames per second that are filtered out by the port	Unit: Frames Time Base: none Low: 0 High: 0 Buffer: 0	Below: 0 Above: 0	Informative Informative

The table below provides default settings for areas in the End-to-End Performance Monitor class.

TABLE 11 End-to-End Performance Monitor class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
End-to-end receive performance (RX performance)	Monitors the receiving traffic between a SID_DID pair in a port	Unit: KBps Time Base: none Low: 0 High: 0 Buffer: 0	Below: 0 Above: 0	Informative Informative
End-to-end transmit performance (TX performance)	Monitors the transmit traffic between a SID_DID pair in a port	Unit: KBps Time Base: none Low: 0 High: 0 Buffer: 0	Below: 0 Above: 0	Informative Informative

thConfig command

You can use the **thConfig** command to customize event monitoring thresholds for the Fabric, Security, SFP, and Performance classes, or to display the configuration. It is recommended, however, that you use the default settings for these classes.

If configured areas exceed the currently-effective threshold settings, the Fabric Watch daemon can take one of the following actions:

- Send an SNMP alarm.
- Log a RASLog message.
- Send an e-mail alert.

The table below lists the configuration options for **thConfig** command. For complete information about using the **thConfig** command, refer to the *Fabric OS Command Reference*.

TABLE 12 Configuration options for thConfig command

Class name	Valid area types	Threshold	Threshold action	Configuration recommendation
Fabric	ED - Number of E_Ports down FC - Fabric reconfiguration DC - Domain ID changes SC - Segmentation changes ZC - Zone changes FL - Fabric logins	Default or Custom	Default or Custom	It is recommended that you leave the entire Fabric class in its default state (no alerts). Refer to Fabric monitoring setting guidelines on page 48 for more information.

[1] To change the default, provide an integer value.
[2] Valid custom action setting values include SNMP, RASLog, portlog, e-mail, or none.

TABLE 12 Configuration options for thConfig command (Continued)

Class name	Valid area types	Threshold	Threshold action	Configuration recommendation
Security	TV - Telnet violations HV - HTTP violations SV - Serial violations DV - DCC violations IC - Invalid certifications LV - Login violations TS - TS out-of-sync FF - SLAP failures NF - No FCS ISB - Incompatible security IV - Illegal command	Default or Custom	Default or Custom	Use the Security class default settings for areas and alarm configuration. There is no reason to alter the default settings.
SFP	TXP - Transmit areas RXP - Receive areas Current Voltage Temperature PWROnHours	Default or Custom	Default or Custom	Use the SFP default settings. The traits are SFP-specific and there is no reason to alter them. Refer to SFP monitoring default settings on page 53 for more information.
Filter	CUSTDEF	Default or Custom	Default or Custom	It is recommended that you use the Filter default settings.
EE (End-to-end performance)	RXF - Receive areas TXP - Transmit areas	Default or Custom	Default or Custom	It is recommended that you leave the entire Performance Monitor Class and End-to-End Performance Monitor Class area settings in their default state (no alerts).

thConfig command examples

With the exception of setting thresholds for the RX area of an end-to-end (EE) performance monitor, which requires special licensing in Access Gateway mode, it is recommended that you use the default settings for these classes.

Setting the high threshold of the RX area of an EE monitor

The **thConfig** command provides the ability to monitor thresholds for frame monitoring and end-to-end (EE) performance on both Access Gateway (AG) switches and non-AG switches.

NOTE
Both the APM license and the Fabric Watch license must be installed on the platform configured in AG mode to use the frame monitoring and EE monitoring capabilities. The APM license provides the counters and the Fabric Watch license provides the monitoring and alert mechanisms for these counters.

To set the high threshold of the RX area, enter the **thConfig** command using the following parameters.

```
switch:admin> thconfig --set ee -area RX -timebase minute -high -val 12
```

Pausing and continuing monitoring

To pause the monitoring of a class, area, and port or index, enter the **thConfig** command using the following parameters.

NOTE
You cannot specify **all** for all classes but you can specify **all** for all areas.

```
switch:admin> thconfig --pause | --continue class -area area_type -port[/slot] port
switch:admin> thconfig --pause | --continue class -area area_type -index index
```

NOTE
The Security and Fabric classes do not have a port or index value. For those classes, a value of 0 is assumed.

Monitoring the filter performance class

You can monitor the Filter Performance Monitor class and specify a filter monitor to be tracked by Fabric Watch. The PERFPT area provides threshold values to the user-defined frame type. When a new user-defined frame type is created using the **fmMonitor** command, the threshold value is automatically based on the PERFPT configuration at the time the frame type is created.

To specify and track a filter monitor, use the **thConfig** command.

In the following example the high threshold value is 10. Therefore, all frame monitors configured hereafter will have a high threshold value of 10.

```
switch:admin> thconfig --set filter -area PERFPT -high -val 10
```

16 Gbps SFP and QSFP monitoring

Fabric Watch can monitor Brocade 16 Gbps SFPs. By default, if the SFP crosses a configured threshold, Fabric Watch generates an SNMP alarm, a RASLog message, and an e-mail alert for the following SFP areas:

- Current
- Voltage
- Temperature
- RXP
- TXP
- Power on Hours (Power on Hours is not supported on the 10 Gbps SFP or the QSFP.)

Fabric Watch also monitors the Brocade Quad SFP (QSFP) and, as for 16 Gbps SFPs, if configured thresholds are crossed, Fabric Watch generates an SNMP alarm, a RASLog message, and an e-mail alert for the following SFP areas:

- Current
- Voltage
- Temperature
- RXP

NOTE
On core blades, only 16 Gbps QSFPs can be installed.

Voltage and temperature monitoring using the QSFP

A QSFP connects four ports of one core blade of a chassis to another core blade of a different chassis. Typically, voltage and temperature values for all ports, on a single chassis, that are connected using one QSFP unit will have the same values, resulting in redundant information. To avoid this, Fabric Watch monitors the voltage and temperature areas on the first available port of the QSFP unit only, which reduces the display of redundant information. If the port crosses the voltage or temperature thresholds, Fabric Watch takes the SNMP, RASlog, or e-mail action on the first port and sends a warning to the user that the other ports are affected.

Logical switch considerations with QSFP

Fabric Watch monitors QSFPs in each logical switch. Temperature and voltage are monitored on the first available port of the QSFP unit to minimize the display of redundant information. However, if individual ports of a QSFP belong to different logical switches, then there will be separate action notifications for each logical switch.

NOTE
This applies only to QSFP voltage and temperature monitoring.

Monitoring the SFP and QSFP

You can use the **thMonitor** command to enable the Brocade 10 Gbps and 16 Gbps SFPs and 16 Gbps QSFPs. By default, the 16 Gbps SFP and QSFP are disabled.

To enable or start the monitoring of the SFP and QSFP, enter the **thMonitor** command using the following parameter:

```
switch:admin> thmonitor --enable brcdSfp
```

To disable or stop the monitoring of the SFP and QSFP, enter the **thMonitor** command using the following parameter:

```
switch:admin> thmonitor --disable brcdSfp
```

To show the monitoring status of the SFP and QSFP, enter the **thMonitor** command using the following parameter:

```
switch:admin> thmonitor --show brcdSfp
```

Specifying the 16 Gbps SFP type

You can use the **--sfpType** operand as part of the **thconfig** command to manage the actions and thresholds for the Current, Voltage, RXP, TXP, and Temperature areas of the 16 Gbps SFPs as shown in the following example.

```
switch:admin> thconfig --apply sfp --sfptype sfptype1 -area TXP 1270 temperature 82
current 10
```

If you do not provide the SFP type parameters (as shown in the example below) the existing thresholds and actions of the SFP class are changed to their default values.

```
switch:admin> thconfig --set sfp -area TXP --sfptype
```

SFP types for the 10 Gbps SFPs and 16 Gbps SFPs and QSFPs are listed in the table below.

TABLE 13 16 Gbps and QSFP configurable SFP types

SFP Type	Serial Number	Area	Default High	Default Low
16GSWL	HA	Temperature (°Centigrade)	85	-5
		Voltage (mVolts)	3600	3000
		RXP (µWatts)	1259	32
		TXP (µW)	1259	126
		Current (mAmp)	12	3
		Power on Hours (hours)	0	0
16GLWL	HB	Temperature (°C)	90	-5
		Voltage (mV)	3600	3000
		RXP (µW)	1995	10
		TXP (µW)	1995	126
		Current (mA)	70	1
QSFP	HT	Temperature (°C)	85	-5
		Voltage (mV)	3600	2970
		RXP (µW)	2180	44
		TXP (µW)	0	0
		Current (mA)	10	1
10GSWL	KA	Temperature (°C)	90	-5
		Voltage (mV)	3600	3000
		RXP (µW)	1999	30

TABLE 13 16 Gbps and QSFP configurable SFP types (Continued)

SFP Type	Serial Number	Area	Default High	Default Low
		TXP (µW)	1999	125
		Current (mA)	10	3
10GLWL	KD	Temperature (°C)	90	-5
		Voltage (mV)	3600	2970
		RXP (µW)	2230	14
		TXP (µW)	2230	60
		Current (mA)	95	10
Others	N/A	Temperature (°C)	85	-10
		Voltage (mV)	3630	2970
		RXP (µW)	5000	0
		TXP (µW)	5000	0
		Current (mA)	50	0

Refer to the *Fabric OS Command Reference* for details on using the **--sfpType** operand as part of the **thconfig** command.

Displaying the number of 16 Gbps SFP operational hours

To show the number of hours that the 16 Gbps SFP is operational, enter the **thConfig** command using the following parameters. The only supported time base for this area is **none**.

```
switch:admin> thconfig --show sfp -area PWRONHRS -sfptype 16GSWL
```

Displaying the SFP health information

To display the health of 10 and 16 Gbps SFPs and QSFPs, enter the **sfpshow --health** command.

Fabric Watch monitors the current, voltage, receiver (RXP) of the SFP, and transmitter (TXP) and if any of these parameters crosses the low or high thresholds, the state of the SFP is yellow; otherwise, the state is green. The SFP can also be in one of the following states:

- Paused — Health monitoring is not enabled.
- No license — The switch does not have the Fabric Watch license.
- Unknown — Fabric Watch cannot determine the state of the SFP.

Recommended settings for Fabric, SFP, Performance, and Security classes

The table below lists the recommended settings for the Fabric, SFP, Security, and Performance classes discussed in this document. For all of these classes, it is recommended that you use the default settings.

TABLE 14 Recommended Environment and Resource class settings

								E=Error_Log, S=SNMP_Trap, P=Port_LOG_LOCK, M=EMAIL_ALERT, PF=Port Fence		
				Trait Configuration						
Class	Area	Default	Unit	Time Base	Low Thresh	High Thresh	Buffer	Default	Below	Above
Fabric	E_Port downs	X	Downs	None	0	0	0	X		
	Fabric reconfig	X	Reconfigs	None	0	0	0	X		
	Domain ID changes	X	DID changes	None	0	0	0	X		
	Segmentation	X	Segmentations	None	0	0	0	X		
	Zone changes	X	Zone changes	None	0	0	0	X		
	Fabric logins	X	Logins	None	0	0	0	X		
SFP	Temperature	X	C	None	-10	85	3	X	E	E
	RX power (RXP)	X	µWatts	None	0	5000	25	X	E	E
	TX power (TXP)	X	µWatts	None	0	5000	25	X	E	E
	Current	X	mA	None	0	50	1	X	E	E
	Voltage	X	µV	None	2970	3630	10	X	E	E
	PWR on Hours	X	Changes	None	0	0	0	X	E	E
End-to-End Performance	RX performance	X	KB/s	None	0	0	0	X		
	TX performance	X	KB/s	None	0	0	0	X		
Filter-based Performance	Custom filter counter	X	Frames	None	0	0	0	X		
Security	Telnet violations	X	Violations	Minute	1	2	0	X		E,S

TABLE 14 Recommended Environment and Resource class settings (Continued)

								E=Error_Log, S=SNMP_Trap, P=Port_LOG_LOCK, M=EMAIL_ALERT, PF=Port Fence	
	HTTP violations	X	Violations	Minute	1	2	0	X	E,S
	SCC violations	X	Violations	Minute	1	2	0	X	E,S
	DCC violations	X	Violations	Minute	1	2	0	X	E,S
	Login violations	X	Violations	Minute	1	2	0	X	E,S
	SLAP failures	X	Violations	Minute	1	2	0	X	E,S
	TS out-of-sync	X	Violations	Minute	1	2	0	X	E,S
	No FCS	X	Violations	Minute	1	2	0	X	E,S
	Incompatible security DB	X	Violations	Minute	1	2	0	X	E,S
	Illegal commands	X	Violations	Minute	1	2	0	X	E,S

Port Monitoring

Port class areas

You can use the **portThConfig** command to configure the Port class. Port setting guidelines and specific examples of **portThConfig** configurations are presented in subsequent sections.

NOTE
Fabric Watch monitors and reports the status of physical and virtual FC ports. Physical GbE ports and iSCSI ports are not monitored and are not included in the Port Class area.

TABLE 15 Port class areas

Area	Description
Cyclic redundancy check (CRC)	The number of times an invalid cyclic redundancy check error occurs on a port or a frame that computes to an invalid CRC. Invalid CRCs can represent noise on the network. Such frames are recoverable by retransmission. Invalid CRCs can indicate a potential hardware problem.
Invalid transmission words (ITW)	The number of times an invalid transmission word error occurs on a port. A word did not transmit successfully, resulting in encoding errors. Invalid word messages usually indicate a hardware problem. **NOTE** For Fabric OS 7.1.0 and later, the ITW counter includes a physical coding sublayer (PCS) violation. ITW violations can occur due to an ITW violation, a PCS violation, or both.
Class 3 discards (C3TX_TO)	The number of Class 3 discards frames because of time-outs.
Link loss (LOS)	The number of times a link failure occurs on a port or sends or receives NOS. Both physical and hardware problems can cause link failures. Link failures also frequently occur due to a loss of synchronization or a loss of signal.

TABLE 15 Port class areas (Continued)

Area	Description
Signal loss	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.
Sync loss	The number of times a synchronization error occurs on the port. Two devices failed to communicate at the same speed. Synchronization errors are always accompanied by a link failure. Loss of synchronization errors frequently occur due to a faulty SFP or cable.
Packet loss (VE_Port only)	The number of packets routed through a port exceeds the port bandwidth.
Protocol errors (PE)	The number of times a protocol error occurs on a port. Invalid state due to LRR on an online link. Occasionally these errors occur due to software glitches. Persistent errors occur due to hardware problems.
Received packets (RXP)	The percentage of maximum bandwidth consumed in packet receipts.
State changes (ST) (Port and VE_Port)	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 faulty.
Transmitted packets (TXP)	The percentage of maximum bandwidth consumed in packet transmissions.
Trunk utilization (E_Port, FCU_Port, and FOP_Port)	The percent of utilization for the trunk at the time of the last poll.
Utilization (VE_Port only)	The percent of utilization for the trunk at the time of the last poll.
Link reset	The ports on which the number of link resets exceed the specified threshold value.

NOTE
Only the Packet loss, State changes, and Utilization areas are supported on the VE_Port.

Port class guidelines and default settings

There are different recommendations and default settings for the physical port, the E_Port, and the FOP_Port and FCU_Port. Refer to the following sections and plan carefully before you begin configuring the port:

- Physical port setting guidelines on page 67
- E_Port subclass setting guidelines on page 71
- FOP_Port and FCU_Port subclass setting guidelines on page 74
- VE_Port class default settings on page 78

NOTE
E_Ports and VE_Ports are not supported in Access Gateway mode.

Physical port setting guidelines

It is recommended that you use the default settings listed in Port class default settings on page 67 for most Port class areas. Consider the Port class to be a superset containing the E_Port, FOP_Port, and FCU_Port subclasses. If you make a change to a default setting for an area in the Port class, it applies to all of the subclasses. This is convenient if you have determined that changes you plan to make to the default settings for the subclasses are the same for certain areas. In this case, you only need to make the changes to the Port class. Note, however, that if you make a change to one of the subclasses, that change overrides the Port class setting.

Port class default settings

TABLE 16 Port class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Cyclic redundancy check (CRC with good EOF (crc g_eof) markers)	Monitors the number of CRC errors.	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Below: 0 Above: 0	Informative Out_of_range
Invalid transmission words (ITW)	Monitors the number of invalid words transmitted.	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Below: 0 Above: 0	Informative Out_of_range
Class 3 discards (C3TX_T0)	Class 3 discards frames due to time-out or destination unreachable.	Unit: Errors Time Base: minute Low: 0 High: 2 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Link loss	Monitors the number of link failures.	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Below: 0 Above: 0	Informative Out_of_range
Signal loss	Monitors the number of signal loss errors.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range

TABLE 16 Port class default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
State changes (ST)	Monitors state changes.	Unit: Changes Time Base: minute Low: 0 High: 50 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Sync loss	Monitors the number of loss of synchronization errors.	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Below: 0 Above: 0	Informative Out_of_range
Protocol errors (PE)	Monitors the number of primitive sequence errors.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Received packets (RXP)	Monitors receive rate, by percentage.	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Below: 0 Above: 0	Informative Informative
Transmitted packets (TXP)	Monitors transmission rate, by percentage.	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Below: 0 Above: 0	Informative Informative
Link reset	Monitors the number of link resets sent by a given port (LR-Out) and received on a given port (LR-In).	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Below: 0 Above: 0	Informative Out_of_range

Port configuration

Use the **portThConfig** command to configure thresholds for Fabric Watch event monitoring for all ports of a specified type and to display the configuration and current port status in real time. The command syntax is detailed in the *Fabric OS Command Reference*.

Before you configure thresholds, you must first identify and select the appropriate class and areas, which are described in Port class areas on page 65.

Custom port settings

If you want to customize threshold and action settings (alarms), start with Port class guidelines and default settings on page 66. Setting guidelines and default settings for the physical port, E_Port, FOP_Port, FCU_Port, and VE_Port are different.

NOTE
The FCU_Port, supported on Fabric Watch version 6.4.0 and later, is applicable to copper ports.

The **portThConfig** command follows a transaction model. When you configure thresholds and actions with the **--set** option, the changes are saved persistently to non-volatile storage, but the changes do not become effective until you execute **portThConfig --apply**. The **--apply** option allows you to toggle between default settings and your own saved custom configuration and to apply actions and thresholds separately. You may choose to use default thresholds together with a customized subset of available actions, or you may modify some of the thresholds and use the default actions. Use the **-nosave** option to save the configuration non-persistently, and use **--cancel** to remove a non-persistent configuration.

NOTE
The execution of this command is subject to Virtual Fabrics or Admin Domain restrictions that may be in place. Refer to the *Fabric OS Command Reference* for more information and for details about the **portThConfig** command.

Using the nosave command

The **nosave** command prevents the configuration changes from being saved persistently. This option allows you to make and view changes without overwriting the saved configuration.

CAUTION

When you use --set with the --nosave option and the switch reboots, your changes are lost.

portThConfig command procedures

The following sections provides specific examples for the Port class. Refer to Port class guidelines and default settings on page 66 for recommendations on how to set areas for the physical port, the E_Port, the FOP_Port, and the FCU_Port.

Port type: physical port

The Port class is a superset containing the E_Port, FOP_Port, and FCU_Port subclasses. In general, use the default settings listed in Port class default settings on page 67, or use the generic Port class to configure an area whose settings are common to one or more of the port subclasses; for example, configuring all physical ports to monitor invalid CRC counts. In most cases, the default settings are adequate for the physical port.

Configuring all physical ports to monitor invalid CRC counts

Invalid Cyclic Redundancy Check (CRC) count errors on a port can represent noise on the network or a potential hardware problem.

1. Enter the **portThConfig** command using the following parameters.
   ```
   switch:admin> portthconfig --set port -area crc -highthreshold -value 100 -
   trigger above -action raslog,email,snmp -buffer 0

   switch:admin> portthconfig --set port -area crc -lowthreshold -value 1 -trigger
   above -action raslog -buffer 0
   ```
   - In this example, the alarms are set at two points: a low threshold of 1 and a high threshold of 100 (the default is 1000). The goal is to be notified as the number of invalid CRCs per minute rises above the low boundary and again when it rises above the high boundary.
   - Triggers specify actions for below the high threshold. Here, the trigger for both is **above**.
   - Set the action to take when a trigger occurs. Here, for the high threshold, log the event in the RASlog, send an e-mail message, and issue an SNMP trap. For the low threshold, only log the event in the RASLog.
   - Set the buffer setting to 0 (the default is 100). Note that if you do not specify the buffer value, Fabric Watch automatically recalculates the buffer.
   - Apply the new custom settings so they become effective.
2. Apply the new custom settings so they become effective.
   ```
   switch:admin> portthconfig --apply port -area crc -action cust -thresh_level
   custom
   ```
3. To display the port threshold configuration for the Port class and all areas, use the following command.
   ```
   switch:admin> portthconfig --show port
   ```

Configuring all physical ports to monitor for invalid transmission words

Invalid transmission words (ITW) occur when a word does not transmit successfully, resulting in encoding errors. Invalid word messages usually indicate a hardware problem.

NOTE
For Fabric OS versions 7.1.0 and later, the ITW counter includes a physical coding sublayer (PCS) violation. ITW violations can occur due to an ITW violation, a PCS violation, or both.

1. Enter the **portThConfig** command using the following parameters.
   ```
   switch:admin> portthconfig --set port -area itw -highthreshold -value 40 -trigger
   above -action raslog,snmp, --buffer 0

   switch:admin> portthconfig --set port -area itw -lowthreshold -value 25 -trigger
   above -action raslog --buffer 0
   ```
   - In this example, the alarms are set at two points: a high threshold of 40 and a low threshold of 25. The goal is to be notified as the number of invalid transmission words per minute rises above the low boundary and again when it rises above the high boundary.
   - Triggers specify actions for in-range port behavior. Here, the trigger for both is **above**.

- Set the action to take when a trigger occurs. Here, for the low threshold, only log the event in the RASLog. For the high threshold, log the event in the RASLog and issue an SNMP trap.
- Set the buffer to 0 (the default is 100).

2. Apply the new custom settings so they become effective.

```
switch:admin> portthconfig --apply port -area itw -action cust -thresh_level custom
```

3. To display the port threshold configuration for the Port class and all areas, use the following command.

```
switch:admin> portthconfig --show port
```

Pausing and continuing monitoring

You must first enable the Brocade 10 Gbps SFP and 16 Gbps QSFP with the **thMonitor** command before the **portThConfig** pause and continue commands can take effect. Refer to Monitoring the SFP and QSFP on page 59 for instructions.

To pause the monitoring of a class, area, and port or index, enter the **portThConfig** command using the following parameters.

```
switch:admin> portthconfig --pause class -area area_type -port [-slot]/port
```

To resume the monitoring of a class, area, and port or index, enter the **portThConfig** command using the following parameters.

```
switch:admin> portthconfig --continue class -area area_type -port [-slot]/port
```

NOTE
You cannot specify **all** for all classes, but you can specify **all** for all areas.

E_Port subclass setting guidelines

E_Port guidelines for the following areas represent a more aggressive approach in most areas, because failing or failed E_Ports in a large fabric can cause serious fabric-wide issues if not detected early. The E_Port class represents ports connected to another switch.

NOTE
If you are using a Brocade 48000 or DCX Backbone with an FR4-18i blade or the Brocade 7500, the E_Port class monitors the following additional ports and creates monitors for each of the logical ports: FCR ports (includes EX_Ports); FCIP (includes VE_Ports and VEX_Ports). In these configurations, state changes are applicable for all ports and utilization and packet loss are applicable to VE_Ports only.

- Area: Loss of Synchronization

  Change the default high boundary from 500 to 45 (per minute) and make sure the Buffer setting is set to 0 (the default).
- Area: Invalid Transmission Words

  Change the default high boundary from 1000 to 40 (per minute) and make sure the Buffer setting is set to 0 (the default). Excessive invalid transmission words on E_Ports leads to fabric congestion and possible frame drops if left unchecked; therefore, set the alarm to fence the port. Refer to Port type: E_Port, FOP_Port, or FCU_Port on page 79 for instructions.
- Area: Invalid Cyclic Redundancy Check (CRC) Count

  Change the default high boundary from 1000 to 20 (per minute) and make sure the Buffer setting is set to 0 (the default is 100). Excessive CRCs on E_Ports lead to fabric congestion and possible frame drops if left unchecked; therefore, set the alarm to fence the port. Refer to Port type: E_Port, FOP_Port, or FCU_Port on page 79 for instructions.

- Areas: Receive (Rx) and Transmit (Tx) Performance

  Rx and Tx Performance areas are used to monitor the bandwidth utilization of the interswitch links (ISLs) in the fabric. Set the high boundary to 75 percent and the alarms to Above and In-Between conditions. These settings indicate if the 75 percent threshold is exceeded and for how long. With this information, you can determine if additional ISL bandwidth is required in the fabric.

  NOTE
  This only applies if trunking is not enabled. If trunking is enabled, use trunk utilization to monitor this bandwidth utilization.

- Area: Link Reset

  Set the alarm to fence the port. This prevents a "flapping" E_Port, which could lead to congestion or frame loss. Refer to Port type: E_Port, FOP_Port, or FCU_Port on page 79 for instructions.

- Area: Class 3 (C3) Discards

  Unlike the other areas, take a conservative approach for the C3 Discards area. Use the default settings and configure the alarms for Above. The goal is to determine the high boundary at which the port would be fenced, so monitor the high boundary and change the settings accordingly.

- Area: Trunk Utilization

  Set the high boundary to 75 percent and the alarms to Above and In-Between conditions. These settings indicate if the 75 percent threshold is exceeded and for how long.

  NOTE
  This can only be configured if the trunking license is present.

- Areas: Primitive Sequence Protocol Error, State Changes, Utilization, Packet Loss

  Use the default settings.

E_Port class default settings

Port fencing can be enabled or disabled for the following areas for the E_Port class:

- Link Failure Count
- Loss of Synchronization Count
- Primitive Sequence Protocol Error
- Invalid Transmission Word
- Invalid CRC Count

TABLE 17 E_Port class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Cyclic redundancy check (CRC with good EOF (crc g_eof) markers)	Monitors the number of CRC errors.	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Below: 0 Above: 0	Informative Out_of_range

TABLE 17 E_Port class default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Invalid transmission words (ITW)	Monitors the number of invalid words transmitted.	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Below: 0 Above: 0	Informative Out_of_range
Class 3 discards (C3TX_TO)	Class 3 discards frames due to time-out or destination unreachable.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Link loss	Monitors the number of link failures.	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Below: 0 Above: 0	Informative Out_of_range
Signal loss	Monitors the number of signal loss errors.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Sync loss	Monitors the number of loss of synchronization errors.	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Below: 0 Above: 0	Informative Out_of_range
Protocol errors (PE)	Monitors the number of primitive sequence errors.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range

TABLE 17 E_Port class default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Received packets (RXP)	Monitors the receive rate, by percentage.	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Below: 0 Above: 0	Informative Informative
State changes (ST)	Monitors state changes.	Unit: Changes Time Base: minute Low: 0 High: 50 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Transmitted packets (TXP)	Monitors the transmit rate, by percentage.	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Below: 0 Above: 0	Informative Informative
Trunk utilization	The percent of utilization for the trunk at the time of the last poll.	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Below: 0 Above: 0	Informative Informative
Link reset	Monitors the number of link resets sent by a given port (LR-Out) and received on a given port (LR-In).	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Below: 0 Above: 0	Informative Out_of_range

NOTE
Port fencing can be enabled on 7500/FR18i VE ports under the E_Port class. Port fencing is not supported on FX8-24/7800 VE ports, but is supported on FR4-18i/7500 VE ports.

FOP_Port and FCU_Port subclass setting guidelines

FOP_Port and FCU_Port guidelines for the areas listed below represent a more aggressive approach in most areas.

NOTE
The settings in these subclasses include settings for the host bus adapter (HBA) ports as well as the storage ports.

- Areas: Link Failure Count, Loss of Synchronization Count

  Change the default high boundary from 500 to 15 (per minute) for Link Failure Count and from 500 to 45 (per minute) for Loss of Synchronization Count. Leave the Buffer setting to 0 (the default). Set the alarm configurations to send alerts to both the error log and SNMP. These settings are the same for an HBA port or a storage port.
- Area: Loss of Signal Count

  Unlike the other areas, take a conservative approach for the Loss of Signal Count area. Change the default high boundary from 5 to 45 (per minute) and set the alarm configuration to send alerts to both the error log and SNMP.
- Areas: Invalid Transmission Words, Invalid CRC Count

  For these two classes, the high boundary settings are split. For Host devices, keep the defaults of 1000 (per minute) and buffer of 100. For storage devices, tighten the boundaries substantially: change the default high boundary for Invalid Transmission Words to 80, and change the high boundary for Invalid CRC Count to 40 (per minute).

  Hosts and HBAs reboot so do not set alerts for these devices. Storage devices, however, should not be rebooting, so you should set the alarm to alert more frequently.

  Excessive invalid words or CRCs on F/FL_ports lead to fabric congestion and possible frame drops if left unchecked; therefore, set the alarm to fence the port. Refer to Port type: E_Port, FOP_Port, or FCU_Port on page 79 for instructions. In addition, set the alarm configurations to send alerts to both the error log and SNMP.
- Areas: Receive (Rx) Performance, Transmit (Tx) Performance

  Rx and Tx Performance areas are used to monitor the bandwidth utilization of the device ports in the fabric. Set the high boundary to 85 percent and the alarms to Above and In-Between conditions. The same levels should be set on both Host and storage device ports.

  NOTE
  With the increased use of virtual environments, alerts from device ports are increasing more than ever in the past. This provides a good gauge as to the overall bandwidth requirement changes and utilization and could indicate that additional ISL trunks are required.
- Area: Link Reset

  The goal of the Link Reset area is to avoid excessive link resets which can cause back pressure in the fabric. The Link Reset area is new; therefore, recommended settings are not available. Keep the default settings, monitor the results, and adjust your settings accordingly.
- Area: Class 3 (C3) Discards

  Unlike the other areas, take a conservative approach for the C3 Discards area. Use the default settings and configure the alarms for Above. The goal is to locate issues with the device or its infrastructure, so monitor the data to help isolate issues. Port fencing is one of the recommended solutions for isolating issues.
- Area: Trunk Utilization

  The Trunk Utilization area is new; therefore, recommended settings are not yet available. Use the default settings, monitor the results, and adjust your settings accordingly.
- Areas: Primitive Sequence Protocol Error, State Changes

  These areas are not used for monitoring; therefore, leave the default alarm settings at 0.

FOP_Port and FCU_Port subclass default settings

Port fencing can only be enabled or disabled for the following areas for the FOP_Port and FCU_Port subclasses:

- Link Failure Count
- Loss of Synchronization Count
- Primitive Sequence Protocol Error
- Invalid Transmission Word
- Invalid CRC Count
- Class 3 Discards

The only ports which fall into the FCU_Port subclass are internal copper-based ports on embedded switches. Copper-based ICL ports are not part of the FCU_Port subclass, and optical ICL ports are not part of the FOP_Port subclass.

TABLE 18 FOP_Port and FCU_Port subclass default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Cyclic redundancy check (CRC with good EOF (crc g_eof) markers)	Monitors the number of CRC errors.	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Below: 0 Above: 0	Informative Out_of_range
Invalid transmission words (ITW)	Monitors the number of invalid words transmitted. For Fabric OS 7.1.0 and later, the ITW counter includes a physical coding sublayer (PCS) violation. ITW violations can occur due to an ITW violation, a PCS violation, or both.	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Below: 0 Above: 0	Informative Out_of_range
Class 3 discards (C3TX_TO)	Class 3 discards frames due to time-out or destination unreachable.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Link loss	Monitors the number of link failures.	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Below: 0 Above: 0	Informative Out_of_range
Signal loss	Monitors the number of signal loss errors.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range

TABLE 18 FOP_Port and FCU_Port subclass default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Sync loss	Monitors the number of loss of synchronization errors.	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Below: 0 Above: 0	Informative Out_of_range
Protocol errors (PE)	Monitors the number of primitive sequence errors.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Received packets (RXP)	Monitors the receive rate, by percentage.	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Below: 0 Above: 0	Informative Informative
State changes (ST)	Monitors state changes.	Unit: Changes Time Base: minute Low: 0 High: 50 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Transmitted packets (TXP)	Monitors the transmit rate, by percentage.	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Below: 0 Above: 0	Informative Informative
Trunk utilization (E_Port, FCU_Port, and FOP_Port)	The percent of utilization for the trunk at the time of the last poll.	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Below: 0 Above: 0	Informative Informative

TABLE 18 FOP_Port and FCU_Port subclass default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Link reset	Monitors the number of link resets sent by a given port (LR-Out) and received on a given port (LR-In).	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Below: 0 Above: 0	Informative Out_of_range

VE_Port class default settings

NOTE
Only a subset of areas can be configured for the VE_Port class. When setting VE_Port thresholds for the Packet Loss area, the threshold value accepts up to two decimal points; for example: **-value 0.60**, as shown in Packet loss monitoring enhancements on the VE_Port on page 78.

TABLE 19 VE_Port class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Packet loss	The number of packets routed through a port exceeds the port bandwidth.	Unit: Errors Time Base: minute Low: 0 High: 10 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
State changes (ST)	Monitors state changes.	Unit: Changes Time Base: minute Low: 0 High: 50 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range
Utilization	The percent of utilization for the port at the time of the last poll.	Unit: Errors Time Base: minute Low: 0 High: 100 Buffer: 0	Below: 0 Above: 0	Informative Out_of_range

Packet loss monitoring enhancements on the VE_Port

Fabric Watch provides monitoring for packet loss percentage for the VE_Port. Previously, configuring the packet loss percentage for the VE_Port was allowed as a whole number; however, packet loss is usually found at less than one percent. Now there is support for configuring packet loss percentages in decimals.

To set the high threshold for packet loss for a VE port, enter the **portThConfig** command using the following parameters:

```
switch:admin> portthconfig --set ve-port -area PKTLOSS -highthreshold -value 0.60 -
trigger above -action snmp
```

Port type: E_Port, FOP_Port, or FCU_Port

E_Port, FOP_Port, and FCU_Port guidelines represent a more aggressive approach in most areas than physical port guidelines. Refer to E_Port subclass setting guidelines on page 71 and FOP_Port and FCU_Port subclass setting guidelines on page 74 for configuration recommendations.

Setting the port persistence time

Port persistence is used to transition a port into a marginal status. Fabric Watch does not record the 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 the event.

The port persistent time is measured in seconds and can be configured. Configuring the port persistence time to 0 (zero) disables this feature. The default value for port persistence is 18 seconds.

1. Use the **fwSet --port -persistence** command to set the port persistence time.
   ```
   switch:admin> portthconfig --show [port_type]
   ```
2. Set the port persistence time.
   ```
   switch:admin> fwSet --port -persistence seconds
   ```

Port fencing

Port fencing monitors ports for erratic behavior and disables a port if specified error conditions are met. You can customize the thresholds and configure the ports to report errors for one or more areas using the **portThConfig** command. After the ports are configured, you can enable port fencing for specific areas of the physical ports, E_Ports, FOP_Ports, and FCU_Ports using the **portFencing** command. Port fencing can be enabled on 7500/FR18i VE ports under the E_Port class. Port fencing is not supported on FX8-24/7800 VE ports, but is supported on FR4-18i/7500 VE ports.

The table below shows the areas that support port fencing for the different physical port class and E_Port, FOP_Port, and FCU subclasses.

NOTE
Port fencing is not supported for the Loss of Sync (LOS) and Link Failure (LF) areas.

TABLE 20 Port fencing class and subclass areas

Port type	Areas supported for port fencing
Physical ports	Cyclic Redundancy Checks (CRC) Invalid Transmission Words (ITW) Link Reset (LR) Protocol Error (PE) State Change (ST) Class 3 Discard Frames (C3TXO)
FOP_Ports	Cyclic Redundancy Checks (CRC) Invalid Transmission Words (ITW) Link Reset (LR) Protocol Error (PE) State Change (ST) Class 3 Discard Frames (C3TXO)
E_Ports EX_Ports	Cyclic Redundancy Checks (CRC) Invalid Transmission Words (ITW) Link Reset (LR) Protocol Error (PE) State Change (ST)

NOTE
The execution of the **portFencing** command is subject to Virtual Fabrics (VF) or Admin Domain restrictions that may be in place. For example, in non-VF chassis environments, the state change counter of a trunked slave port gets incremented by more than 1 when the master EX_Port changes its state. Therefore, it is advisable to set the port fencing high threshold for the State Change area to a value greater than 4 in this environment.

The allowed threshold configuration settings are displayed on a per-class basis. FOP_Port class thresholds apply to the entire switch. You can set different thresholds for Storage and Host FOP_Ports if they are on different switches, based on the fabric configuration.

Port fencing configuration

You must configure port thresholds with the **portThConfig** command before you can enable port fencing using the **portFencing** command. Refer to portThConfig command procedures on page 69 for example port configurations, or the *Fabric OS Command Reference* for complete threshold recommendations for CRC errors and Invalid Words.

You can configure a specified port type or a list of port types to enable port fencing for one or more areas. Use the **all** option to indicate all port types or all areas.

Port fencing recommended area settings

Cyclic redundancy check (CRC) errors and invalid transmission words (ITW) can occur on normal links. They have also been known to occur during certain transitions such as server reboots. When these errors occur more frequently, they can cause a severe impact. While most systems can tolerate infrequent CRC errors or invalid words, other environments can be sensitive to even infrequent instances. The overall quality of the fabric interconnects is also a factor.

NOTE
For Fabric OS versions 7.1.0 and later, the ITW counter includes a physical coding sublayer (PCS) violation. ITW violations can occur due to an ITW violation, a PCS violation, or both.

When establishing thresholds for CRC errors and Invalid Words, consider the following:

- In general, "cleaner" interconnects can have lower thresholds as they should be less likely to introduce errors on the links.
- Moderate (recommended), conservative and aggressive threshold recommendations are provided in the table below. After selecting the type of thresholds for an environment:
  - Set the low threshold with an action of ALERT (RASlog, e-mail, SNMP trap). The alert will be triggered whenever the low threshold is exceeded.
  - Set the high threshold with an action of Fence. The port will be fenced (disabled) whenever the high threshold is detected.
- Aggressive threshold suggestions do not include settings for low, and instead only have the high values to trigger fencing formation on the **portThConfig** command.

TABLE 21 Recommended port fencing thresholds

Area	Moderate/recommended threshold	Aggressive threshold	Conservative threshold
Cyclic redundancy check (CRC)	Low 5 High 20	Low 0 High 2	Low 5 High 40
Invalid transmission word (ITW)	Low 25 High 40	Low 0 High 25	Low 25 High 80
Link reset (LR)	Low 0 High 5	Defaults	Defaults
State change (ST)	Low 0 High 7	Defaults	Defaults
Class 3 frame discard due to timeout (C3TX_TO)	Low 0 High 5	N/A	N/A

Enabling port fencing

1. Connect to the switch and log in as admin.
2. Configure port thresholds.
3. Enter the **portFencing --enable** command.

The following example configures port fencing on an FOP_Port for the Class 3 discard frame area.

```
portFencing --enable fop-port --area C3TX_TO
```

Disabling port fencing

Use the **portFencing --disable** command to disable port fencing for the specified areas on all ports of the specified port types. You can use the **portFencing --show** command to display the configuration. The output of this command includes the configured port types, error types, and port fencing status (disabled or enabled). Port fencing is disabled by default.

1. Connect to the switch and log in as admin.
2. Enter the **portFencing --disable** command.

The following example disables port fencing on an FOP_Port for the Link Reset area.

```
portFencing --disable fop_port --area LR
```

Port fencing configuration using BNA

The Brocade Network Advisor (BNA) management application supports port fencing. Port fencing objects include the SAN, Fabrics, Directors, Switches (physical), Virtual Switches, Ports, as well as Port Types (E_Port, F_Port, and FX_Port). Use port fencing to directly assign a threshold to these objects. When a switch does not support port fencing, a "No Fencing Changes" message displays in the Threshold field in the Ports table.

If the port detects more events during the specified time period, the device firmware blocks the port, disabling transmit and receive traffic until you investigate, solve the problem, and manually unblock the port. Physical fabrics, directors, switches, port types, and ports display when you have the privileges to manage that object and are indicated by the standard product icons.

Port fencing requirements

To configure port fencing using the BNA management application, all Fabric OS devices must have Fabric Watch and must be running firmware Fabric OS 6.2 or later.

Port fencing threshold areas supported on BNA

You can add, edit, view, or remove thresholds on the following area types using Brocade Network Advisor (BNA). You can then assign the thresholds to available objects in the BNA tree.

Port fencing threshold areas include the following:

- C3 Discard Frames (Fabric OS only)
- Invalid CRCs (Fabric OS only)
- Invalid Transmission Words (Fabric OS only)
- Link Reset (Fabric OS only)
- Protocol Errors (M-EOS and Fabric OS)
- Security (M-EOS)
- State Changes (Fabric OS only)

Refer to the *Brocade Network Advisor User Manual* for detailed instructions on how to add, edit, view, and remove thresholds.

Port health and CRC monitoring

There are two types of CRC errors that can be logged on a switch; taken together they can assist in determining which link introduced the error into the fabric. The two types are plain CRCs, which have bad end-of-frame (EOF) markers and CRCs with good EOF (crc g_eof) markers. When a crc g_eof error is detected on a port, it indicates that the transmitter or path from the sending side may be a possible source. When a complete frame containing a CRC error is first detected, the error is logged, and the good EOF (EOFn) is replaced with a bad EOF marker (EOFni). Because Brocade switches forward all packets to their endpoints, changing the EOF marker allows the packet to continue but not be counted.

For thresholding and fencing purposes, only frames with CRC errors and good end-of-frame markers are counted. This enables you to know exactly how many errors were originated in a specific link.

Recommended port configuration settings

The following table lists the recommended settings for physical port, E_Port, FOP_Port, and FCU_Port for both the host device and the storage device.

TABLE 22 Recommended configuration for the port class

									E=Error_Log, S=SNMP_Trap, P=Port_LOG_LOCK, M=EMAIL_ALERT, F=Port Fence			
					Trait Configuration							
Class	Area	Default	Custom	Unit	Time Base	Low Thresh	High Thresh	Buffer	Default	Custom	Below	Above
Port	Link Loss	X		Errors	Minute	0	500	50	X			
	Sync Loss	X		Errors	Minute	0	500	50	X			
	Signal Loss	X		Errors	Minute	0	5	0	X			
	Protocol Error	X		Errors	Minute	0	5	0	X			
	Invalid Words		X	Errors	Minute	0	25	0		X		E
	Invalid CRCs		X	Errors	Minute	0	5	0		X		E
	RX Performance	X		Percentage	Minute	0	100	0	X			
	TX Performance	X		Percentage	Minute	0	100	0	X			

TABLE 22 Recommended configuration for the port class (Continued)

									E=Error_Log, S=SNMP_Trap, P=Port_LOG_LOCK, M=EMAIL_ALERT, F=Port Fence			
	State Changes	X		Changes	Minute	0	50	0	X			
	Link Reset	X		Errors	Minute	0	500	50	X			
	C3 Discard	X		Errors	Minute	0	5	0	X			
E_Port	Link Loss		X	Errors	Minute	0	0	0		X		
	Sync Loss		X	Errors	Minute	0	45	0		X	E,S	
	Signal Loss		X	Errors	Minute	0	45	0		X	E,S	
	Protocol Error	X		Errors	Minute	0	5	0	X			
	Invalid Words		X	Errors	Minute	0	40	0		X	E,S	
	Invalid CRCs		X	Errors	Minute	0	20	0		X	E,S	
	RX Performance		X	Percentage	Minute	0	75	0		X	E	E
	TX Performance		X	Percentage	Minute	0	75	0		X	E	E
	State Changes E/VE_Port	X		Errors	Minute	0	50	0	X			
	Link Reset	X		Errors	Minute	0	500	50	X			
	Utilization (VE_Port)	X		Percentage	Minute	0	100	0	X			
	Packet Loss (VE_Port)	X		Errors	Minute	0	10	0	X			
	C3 Discard	X		Errors	Minute	0	5	0		X		E
	Trunk Util	X		Percentage	Minute	0	75	0		X		E
FOP_Port and FCU_Port HOST	Link Loss		X	Errors	Minute	0	15	0		X		E,S
	Sync Loss		X	Errors	Minute	0	45	0		X		E,S
	Signal Loss		X	Errors	Minute	0	45	0		X		E,S
	Protocol Error	X		Errors	Minute	0	5	0	X			
	Invalid Words	X		Errors	Minute	0	1000	100		X		E,S,F
	Invalid CRCs	X		Errors	Minute	0	1000	100		X		E,S,F

TABLE 22 Recommended configuration for the port class (Continued)

									E=Error_Log, S=SNMP_Trap, P=Port_LOG_LOCK, M=EMAIL_ALERT, F=Port Fence		
	RX Performance		X	Percentage	Minute	0	85	0		X	E
	TX Performance		X	Percentage	Minute	0	85	0		X	E
	State Changes	X		Changes	Minute	0	5	0	X		
	Link Reset	X		Errors	Minute	0	500	50		X	E
	C3 Discard	X		Errors	Minute	0	5	0		X	E
	Trunk Util	X		Percentage	Minute	0	100	0	X		
FOP_Port and FCU_Port STORAGE	Link Loss		X	Errors	Minute	0	15	0		X	E,S
	Sync Loss		X	Errors	Minute	0	45	0		X	E,S
	Signal Loss		X	Errors	Minute	0	45	0		X	E,S
	Protocol Error	X		Errors	Minute	0	5	0	X		
	Invalid Words		X	Errors	Minute	0	80	0		X	E,S,F
	Invalid CRCs		X	Errors	Minute	0	40	0		X	E,S,F
	RX Performance		X	Percentage	Minute	0	85	0		X	E
	TX Performance		X	Percentage	Minute	0	85	0		X	E
	State Changes	X		Changes	Minute	0	5	0	X		
	Link Reset	X		Errors	Minute	0	500	50		X	E
	C3 Discard	X		Errors	Minute	0	5	0		X	E
	Trunk Util	X		Percentage	Minute	0	100	0	X		

System Monitoring

Environment monitoring

The Environment class provides information about the internal temperature of the switch. You can configure the Environment class using the **sysMonitor** command.

Environment class area

TABLE 23 Environment class area

Area	Description
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
Event Manager (EM) now manages fan monitoring; the switch status is calculated based on fan status reported by EM. You can use the **fanShow** command to view the fan status.

Environment monitoring setting guidelines

Use Environment Class default settings. Temperature settings are switch-dependent and there is no need to alter them. The default alarm configuration, sending alerts to the error log and SNMP, is sufficient.

Environment class default settings

Check the appropriate hardware reference manual for differences in actual environmental requirements. The temperature sensors monitor the switch temperature in Celsius.

NOTE
Fabric Watch no longer supports fan monitoring. Event Manager (EM) now manages fan monitoring and the switch status is calculated based on the fan status reported by EM.

TABLE 24 Environment class default settings for temperature

Switch	Default threshold settings Unit: Degrees Celsius			Default alarm settings	Threshold state
	Low	High	Buffer		
Brocade 300	0	50	10	Below: 3 Above: 3 (Same setting for all devices)	Out-of-range Out-of-range (Same setting for all devices except Brocade DCX-4S)
Brocade 5100	0	63	10		
Brocade 5300	0	48	10		
Brocade 6505	0	58	10		
Brocade 6510	0	65	10		
Brocade 6520	0	61	10		
Brocade 7800	0	58	10		
Brocade Encryption Switch	0	63	10		
Brocade VA-40FC	0	63	10		
Brocade DCX	0	70	10		
Brocade DCX-4S	0	75	10		Informative Out-of-range

Resource class settings

The Resource class monitors flash memory. It calculates the amount of flash space consumed and compares it to a defined threshold.

Resource class area

Configure the Resource class using the **sysMonitor** command.

TABLE 25 Resource class area

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

Resource class default settings

TABLE 26 Resource class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Flash	Monitors the percentage of compact flash used	Unit: Percentage (%)	Below: 3	Informative
		Time base: none	Above: 3	Out_of_range
		Low: 0		
		High: 90		
		Buffer: 0		

System monitoring using the sysMonitor command

Use the **sysMonitor** command to configure temperature and system resource settings at the chassis level. For detailed information about the **sysMonitor** command, refer to the *Fabric OS Command Reference* .

The following operations are supported by the **sysMonitor** command:

- Configure thresholds for Fabric Watch event monitoring and reporting for the environment and resource classes. Environment thresholds enable temperature monitoring, and resource thresholds enable monitoring of flash memory.

Configuration changes are saved persistently to non-volatile storage, but the changes do not take effect until you execute --**apply** . The --**apply** option allows you to toggle between default settings and your own saved custom configuration and to apply actions and thresholds separately.

- Configure memory or CPU usage parameters on the switch or display memory or CPU usage. Configuration options include setting usage thresholds which, if exceeded, trigger a set of specified Fabric Watch alerts. You can set up the system monitor to poll at certain intervals and specify the number of retries required before Fabric Watch takes action. Configuring thresholds for CPU and memory does not follow the transaction model of the typical Fabric Watch command. The --**apply** and --**cancel** options are not valid in this context.

When the system crosses any of the limits, SNMP, RASlog, e-mail (or all) messages are generated. Flash and temperature configuration are at the chassis level. To execute the **sysMonitor** command, you must have chassis-level permission in a Virtual Fabrics (VF) environment.

NOTE
Spikes in memory and CPU utilization are normal during the firmware download process and you may see threshold warning messages while the process is running. After the firmware download process has completed, memory and CPU utilization should return to normal.

System monitoring is disabled by default. You must run both the **--config -mem** and the **--config -cpu** commands to enable both memory and CPU system monitoring.

Using the nosave command

The **nosave** command prevents the configuration changes from being saved persistently. This option allows you to make and view changes without overwriting the saved configuration.

CAUTION

When you use --config with the --nosave option and the switch reboots, your changes are lost.

Examples of the sysMonitor command

The following sections provide specific examples for the Environment class, CPU, and memory.

Environment class settings

Temperature settings are switch-dependent and there is no need to alter them. The default alarm configuration, sending alerts to the error log and SNMP, is sufficient. Refer to Environment monitoring setting guidelines on page 87 for more information.

Pausing and continuing monitoring

To pause the monitoring of a class, area, and port or index, enter the **sysMonitor** command using the following parameters.

```
switch:admin> sysmonitor --pause env -area temp
```

To resume the monitoring of a class, area, and port or index, enter the **sysMonitor** command using the following parameters.

```
switch:admin> sysmonitor --continue env -area temp
```

NOTE
You cannot use the **all** parameter for all classes, but you can specify the **all** parameter for all areas.

Displaying the threshold of the system areas

The temperature area 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.

Enter the **sysMonitor** command using the following parameters:

```
switch:admin> sysmonitor --show env -area temp index
```

Example of configuring the temperature threshold

1. Enter the **sysMonitor** command using the following parameters:

   ```
   switch:admin> sysmonitor
   ```

```
  --config env -area temp -highth -value 99
  -trigger above -action raslog
```

2. Apply the changes:

```
  switch:admin> sysmonitor
  --apply env -area temp -action_level cust -thresh_level cust
```

Resource class settings

The flash area of the Resource class monitors the percentage of compact flash memory used on the system.

Displaying the system flash parameters

Enter the **sysMonitor** command using the following parameters:

```
switch:admin> sysmonitor --show resource -area flash
```

CPU and memory

When configuring CPU monitoring, you must specify a value in the range from 1 through 100. When the CPU usage exceeds the limit, a Fabric Watch alert is triggered. The default CPU limit is 75 percent.

When configuring memory, the limit specifies a usage limit as a percentage of available resources.

When used to configure memory monitoring, the **-limit** value must be greater than the low limit and smaller than the high limit.

The following operands are valid only with the **--config mem** operand. Three thresholds are supported for memory monitoring:

- *high_limit* — Specifies an upper usage limit for memory as percentage of available memory. This value must be greater than the value set by the **-limit** parameter. The maximum is 90 percent. When memory usage exceeds this limit, Fabric Watch generates a RASLog CRITICAL message. The default is 80 percent.
- *limit* — Specifies the default CPU limit. When the limit is exceeded, Fabric Watch sends out a RASLog WARNING message. When usage returns below the limit, Fabric Watch sends a RASLog INFO message. Valid values are range from 0 through 80 percent and the default value is different for different systems.
- *low_limit* — Specifies a lower usage limit for memory as percentage of available memory. This value must be smaller than the value set by the **-limit** parameter. When memory usage exceeds or falls below this limit, Fabric Watch generates a RASLog INFO message. The default for all platforms is 50 percent.

Examples of the CPU and memory commands

The following sections provides specific examples for CPU and memory.

Displaying the current CPU usage threshold

Enter the **sysMonitor** command using the following parameters:

```
switch:admin> sysmonitor --show cpu
CPU Usage : 2%
CPU Usage Limit : 75%
Number of Retries :3
Polling Interval : 120 seconds
Actions: snmp
```

Displaying the current memory usage threshold

To display the current memory usage threshold, enter the **sysMonitor --show mem** command.

```
switch:admin> sysmonitor --show mem
Used Memory: 171476k 34%
Total Memory: 504344k
Free Memory: 332868k
Used Memory Limit: 60%
Low Used Memory Limit: 40%
High Used Memory Limit: 70%
Polling Interval: 10 seconds
No Of Retries: 1
Actions: snmp,raslog
```

Configuring the system memory usage monitoring threshold

Enter the **sysMonitor** command using the following parameters:

```
switch:admin> sysmonitor --config mem -poll 10 -retry 1 -limit 20 -action snmp,
raslog -high_limit 80
```

Recommended environment and resource monitoring settings

TABLE 27 Recommended Environment and Resource class settings

									E=Error_Log, S=SNMP_Trap, P=Port_LOG_LOCK, M=EMAIL_ALERT, PF=Port Fence			
					Trait Configuration							
Class	Area	Default	Custom	Unit	Time Base	Low Thresh	High Thresh	Buffer	Default	Custom	Below	Above
Environment	Temperature	X		C	None	0	Depends on switch type	10	X		E, S	E, S
Resource	Flash	X	Percentage		None	0	90	0	X		E, S	E, S

Switch monitoring

Before entering the **switchStatusPolicySet** command, plan your switch status policy. Determine your system requirements and the factors that affect its monitors.

NOTE
Based on the configuration of the core blade component of the switch status policy, Fabric Watch generates two RASlogs when a core blade is removed either on the Brocade DCX or the Brocade DCX-4S. For example, if the Down and Marginal configuration is 0 and 1 on the DCX, upon removal of the first core blade, Fabric Watch generates one RASLog for the switch status policy and the other RASLog for the error itself.

Switch status policy planning

Fabric Watch monitors the health of the switch under various classes. The table below lists the current overall switch status policy parameters in a switch and identifies the factors that affect their health. Note that not all switches use the listed monitors.

Use the **switchStatusPolicySet** command to manually change the policy setting. Refer to the *Fabric OS Command Reference* for more information.

NOTE
The default setting for a MARGINAL state is 0, which prevents Fabric Watch from generating notifications due to missing power supplies. For configurations with a 2+2 power supply (PS) combination, it is recommended that you change the default Fabric Watch default setting of 0 to 2 power supplies, which forces the overall switch status to a MARGINAL state.

TABLE 28 Switch status policy factors

Monitor	Health factors
Power Supplies	Power supply thresholds detect absent or failed power supplies, and power supplies that 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).
Blades	Faulty blades (applies to modular switches).
Core Blade	Faulty core blades.
Flash	Flash thresholds.
Marginal Ports	Port, E_Port, FOP_Port (optical), and FCU_Port (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.
Error Ports	Ports with errors.

Brocade DCX 8510-8 default policy

The default Fabric Watch policy for the Brocade DCX 8510-8 with total power consumption of more than 2,000 watts does not properly reflect the switch status on the power supply. Fabric Watch users must manually update the default configuration for the minimum number of power supplies to three if they have installed more than 256 ports in a DCX 8510-8 chassis.

[3] Marginal ports, faulty ports, error ports, and missing SFPs are calculated as a percentage of the physical ports (excluding FCoE and VE_Ports).

NOTE
The presence of four or more FS8-18 encryption blades in the DCX Data Center Backbone causes the Fabric Watch switch status policy for power supplies to assume a policy setting of 2,1.

Brocade 6505 default policy

The default Fabric Watch policy for the Brocade 6505 is one power supply in the left bay with an optional configuration of two power supplies in both the left and right bays. The default configuration for the Brocade 6505 is a 2 (DOWN) and 0 (MARGINAL), corresponding to a one power supply configuration. If converting to a two power supply configuration, use the **switchStatusPolicySet** command to manually change the configuration to 2,1 for the power supply and fan FRU units. If converting back to a one power supply configuration, use the **switchStatusPolicySet** command to manually change the power supply and fan FRU units to 1,0.

Implementing your switch status policy

After you plan and define your switch status policy, implement it using the following procedure.

1. Enter the **switchStatusPolicySet** command to configure each policy.

   Each policy has two parameters that can be configured: Marginal and Down.
2. Set the number of units Marginal or Down based on your system requirements for each policy or parameter.

NOTE
Switch status policies are saved in a nonvolatile memory, and therefore are persistent until changed.

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
```

Viewing your switch status policy

After you have defined and configured your switch status policy, view it with the **switchStatusPolicyShow** command. The **switchStatusPolicyShow** command displays the following policy parameters that determine the overall switch status:

NOTE
FCoE and VE_Ports are not considered in marginal port or faulty port calculations.

- Power Supplies — The power supply thresholds detect absent or failed power supplies.
- Temperature — Temperature thresholds detect faulty temperature sensors.
- Fan — Fan thresholds detect faulty fans.

- Flash — Flash thresholds monitor flash memory.
- Marginal Ports — Ports that move into the marginal state for reasons such as insufficient buffer credits.
- Port Persistence Time — Fabric Watch waits for the port persistence time duration before it declares the port to be in the MARGINAL state when it crosses the high threshold.
- Faulty Ports — Ports that are faulty because of hardware faults, such as invalid SFPs.
- Missing SFPs — Monitors the number of ports without SFPs.
- Error Ports — Ports that are disabled because of segmentation, an authentication failure, port fencing, or bottleneck detection.

The policy you defined determines the output in the Switch Status Policy Report. Refer to Fabric Watch Reports on page 107 for more details about the Switch Status Policy Report.

FRU monitoring

Supported FRU areas depend on the type of Brocade switch. For the following switches, the slot and WWN areas are not supported:

- Brocade 300, 5100, and 5300 switches
- Brocade DCX and DCX-4S Data Center Backbone
- Brocade Encryption Switch

FRU class areas

The table below lists Fabric Watch areas in the FRU class and describes each area. Possible states for all FRU-class areas are: absent or removed, faulty, inserted, on, off, ready, or up. You configure the FRU class using the **fwFruCfg** command.

TABLE 29 FRU class areas

Area	Description
Fan	State of a fan has changed.
Power supply	State of a power supply has changed.
Slot	State of a slot has changed.
WWN	State of a WWN card has changed.
SFP	State of the SFP has changed.

Configuring FRUs

The configuration of field-replaceable units (FRUs) is an exception to the procedures described elsewhere in this document. 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.

NOTE
The Off state is applicable only to fans on some platforms, such as the Brocade DCX and Brocade DCX-4S. The Off state is not applicable to the power supply, slot, or WWN FRUs.

1. Establish a Telnet or PuTTY connection to the switch.
2. Log in using administrative privileges.
3. Enter the **fwFruCfg** command at the command prompt.

   The **fwFruCfg** command displays your current FRU configuration. The types of FRUs are different for the various platforms.
4. 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, 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.

```
switch123:admin> fwfrucfg

The current FRU configuration:

                Alarm State  Alarm Action
Slot                 1            1
Power Supply         1            1
Fan                  1            1
SFP                  1            1

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) [1]
Slot Alarm Action: (0..17) [1]
Power Supply Alarm State: (0..31) [1]
Power Supply Alarm Action: (0..17) [1]
Fan Alarm State: (0..31) [1]
Fan Alarm Action:(0..17) [1]
WWN Alarm State: (0..31) [1]
WWN Alarm Action: (0..31) [1]
SFP Alarm State: (0..31) [1]
SFP Alarm Action:(0..17) [1]
Fru configuration left unchanged
```

Specifying triggers for FRU alarms

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.

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.

Recommended FRU settings

TABLE 30 Recommended FRU settings

							E=ERROR_LOG, M=EMAIL_ALERT	
Class	Area	Absent	Inserted	On	Off	Faulty	Below	Above
FRU	Slot	X				X		
	Power Supply	X				X		
	Fan	X				X		
	WWN	X				X		

Fabric Watch Configuration Using Web Tools

Using Web Tools to configure Fabric Watch

Enter a short description of your concept here (optional).

You can use Web Tools to define the following Fabric Watch configurations:

- Configure custom threshold values on particular elements.
- Place limits on the acceptable values of those elements and enable the custom limits (configure threshold boundaries).
- Configure Fabric Watch to alert you to errant values.
- Configure Fabric Watch to identify unacceptable values (threshold traits).

NOTE
You do not need the Enhanced Group Management (EGM) license to perform Fabric Watch operations using Web Tools.

Opening the Fabric Watch window

To open the **Fabric Watch** window, perform the following steps:

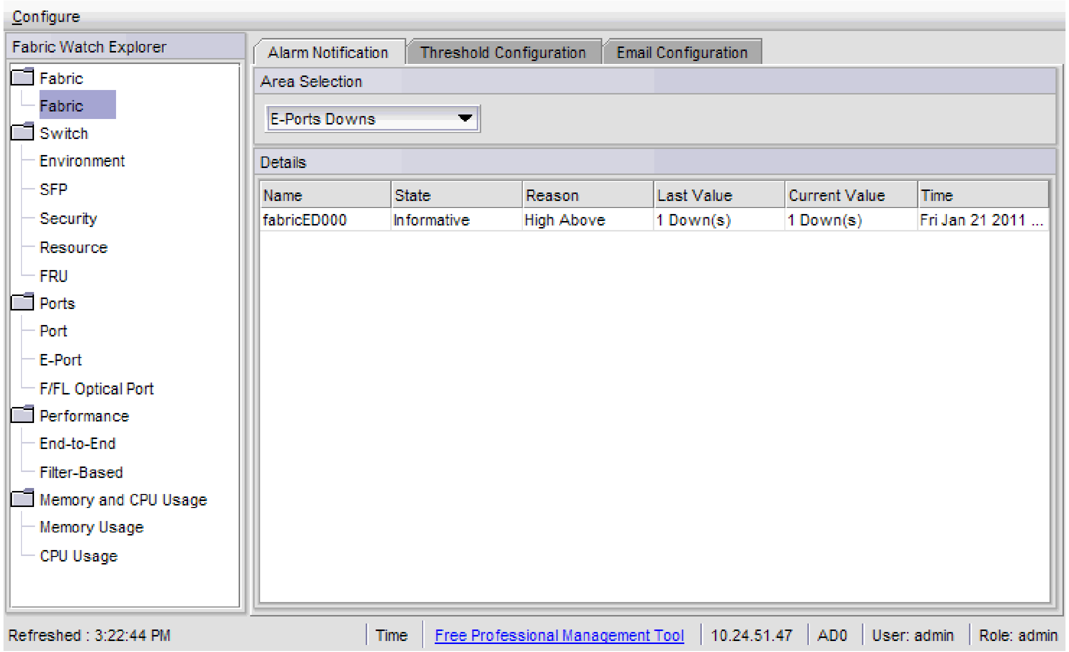
1. Select a switch from the Fabric Tree and log in if necessary.
2. Select **Tasks** > **Manage** > **Fabric Watch**.

   The **Fabric Watch** window displays.

   The figure below shows the **Fabric Watch** window.

   NOTE
   Unless the switch is a member of the current Admin Domain context, Fabric Watch is view-only.

FIGURE 7 Fabric Watch Window



Area Selection

E-Ports Downs

Details

Name	State	Reason	Last Value	Current Value	Time
fabricED000	Informative	High Above	1 Down(s)	1 Down(s)	Fri Jan 21 2011 ...

Refreshed : 3:22:44 PM | Time | Free Professional Management Tool | 10.24.51.47 | AD0 | User: admin | Role: admin

The **Fabric Watch Explorer** pane on the left side of the window displays the available classes. Not all classes are available for all switches. The status bar at the bottom of the window provides you with a summary of recent actions, and the date and time the module was last updated.

System monitoring using Web Tools

The Fabric Watch license must be installed to view and modify the System Monitor details. Select **Monitor** > **System Monitor** to display the System Monitor.

When the switch exceeds the configured usage limit, an alarm triggers. You can configure the alarm with the **Alarm Configuration** tab. The alarm can be configured for SNMP trap, RAS log, or both.

There are three trait and alarm configuration values for System Monitor:

- Polling Interval
- Usage Limit
- No. of Retries

To configure the usage limits for System Monitor, perform the following steps.

1. Open the **Fabric Watch** window.
2. Select either **Memory Usage** or **CPU usage**.
3. Modify the values in the **Trait Configuration** tab.

   When these values are exceeded, the alarm triggers.
4. Click the **Alarm Configuration** tab.
5. Select **SNMP Trap**, **RAS log**, or both options.
6. Click **Apply**.

Fabric Watch threshold configuration using Web Tools

The **Threshold Configuration** tab enables you to configure event conditions. From this tab, you configure threshold traits, alarms, and e-mail configurations.

NOTE
Use the procedures in this section to configure threshold traits for all classes except for the FRU class. Use the procedure described in Configuring alarms for FRUs using Web Tools on page 103 for the FRU class.

Configuring threshold traits

Configure threshold traits to define a threshold for a particular class and area. You can configure the following traits for a threshold:

- Time Base — The time base (minute, hour, day) for the area
- Low Boundary — The low threshold for the event-setting comparisons
- High Boundary — The high threshold for the event-setting comparisons
- Buffer Size — The size of the buffer zone used in event-setting comparisons

NOTE
When you are configuring the **VE-Port** > **Packet Loss** area thresholds, the packet loss threshold values are a percentage. You can configure from 0.01 percent (low boundary) to 100.00 percent (high boundary).

To configure threshold traits, perform the following steps:

1. Click **Fabric Watch** in the Manage section of the **Tasks** menu.
2. Select the **Threshold Configuration** tab.
3. Select the **Trait Configuration** subtab.
4. In the **Fabric Watch Explorer** pane, select a class.
5. Under Area Selection, select an area from the list.

   This sets the units in the **Units** field.

   The module displays two columns of trait information, labeled “System Default” and “Custom Defined”. You cannot modify the information in the System Default column.
6. In the Activate Level area, choose one of the following:
   - Use the system default settings.
   - Click **Custom Defined** to specify new settings and proceed to the next step.
7. If necessary, select a time to record the event in the **Time Base** field.
8. Enter the lowest boundary of the normal zone in the **Low Boundary** field.
9. Enter the highest boundary of the normal zone in the **High Boundary** field.
10. Enter the size of the buffer zone in the **Buffer Size** field.
11. Click **Apply**.

Configuring threshold alarms

After you update the threshold information, use the **Alarm Configuration** subtab to customize the notification settings for each event setting.

The alarm-naming convention is modified for Port, E_Port, F_Port, FL_Port, and VE_Port class types:

- “Above” is called “High Above”
- “Below” is called “Low Below”
- “In Between” is called “High Below”

The “Low Above” action alarm supports all port class types for these options:

- CRC errors
- Invalid words
- Protocol errors
- State change
- Trunk utilization
- C3 discards
- RX performance
- TX performance
- Loss of signal
- Link failures
- Link resets
- Packet loss (not for E_Port)
- Utilization (not for E_Port)

To configure threshold alarms, perform the following steps.

1. From the **Fabric Watch** window, select the **Threshold Configuration** tab.
2. Select the **Alarm Configuration** subtab.
3. In the **Fabric Watch Explorer** pane, select a class.
4. Under **Area Selection**, select an area from the list.

NOTE
The module displays two tables of alarm configuration information, labeled “System Default” and “Custom Defined”. You cannot modify the information in the System Default table.

5. In the Activate Level area, choose one of the following:
   - Click **System Default** to use the system default settings.
   - Click **Custom Defined** to specify new settings and proceed to the next step.
6. Select the check box for the type of notification method you want to use for each event type.

   The following alarm actions are available:

   - ERROR_LOG
   - SNMP_TRAP
   - PORT_LOG_LOCK
   - EMAIL_ALERT
7. Click **Apply**.

Enabling or disabling threshold alarms for individual elements

To configure element-specific alarm settings, perform the following steps:

1. Open the **Fabric Watch** window.
2. In the **Fabric Watch Explorer** pane, select a class.

   You can set alarms for information on a switch only if that information is monitored by Fabric Watch for that switch; not all alarm options are available for all switches.
3. Select the **Threshold Configuration** tab.
4. Under Area Selection, select the area with the alarms that you want to enable or disable.
5. Select the **Element Configuration** subtab.
6. Select an element from the **Element Selection** menu.
7. In the Status area, choose one of the following:
   - To disable threshold alarms, click **Disabled** and click **Apply**. The threshold alarms are disabled and you do not need to continue with this procedure.
   - To enable threshold alarms, click **Enabled** and continue with the next step.
8. Select the **Triggered** behavior type to receive threshold alarms only when they are triggered by events that you defined.
9. Select a time interval in which to receive the threshold alarms from the **Time Interval** menu.
10. Click **Apply**.
11. You can apply the selections on this panel to multiple elements simultaneously by performing the following steps.
    a) Click **Apply More**. The **Multiple Selection** dialog box displays.
    b) Select the check boxes next to the indices of all applicable elements and click **OK**.

Configuring alarms for FRUs using Web Tools

Configuration for the FRU class is different from configuration for the other classes. Because FRUs are not monitored through a threshold-based system, they have a simpler interface for configuration.

For FRUs, you configure the states for which an event occurs, using the following procedure.

1. Open the **Fabric Watch** window.
2. Select the **Threshold Configuration** tab.
3. In the **Fabric Watch Explorer** pane, select a FRU class.
4. Under **Area Selection**, select a FRU type from the list.
5. Select the alarm states for which you want an event to register.

   If a FRU of the selected type is determined that it is one of the selected states, an event will occur.
6. Select the methods by which you want to be notified about the FRU alarms.

   For FRUs, the only options are error log and e-mail alert.
7. Click **Apply** to apply the changes to the switch.

   A confirmation dialog box displays, asking if you want to apply the changes to the switch.
8. Click **OK** to save the changes to the switch.

Configuring alarm filters using Web Tools

The **Fabric Watch** window provides GUI support for the CLI command **fwalarmsfilterset**. This option is used to configure the alarm filtering for Fabric Watch. By disabling the alarms, all non-environment and non-resource class alarms are suppressed. By enabling the alarms, all class alarms are generated.

To configure the alarm filter, perform the following steps:

1. Open the **Fabric Watch** window.
2. Select **Configure** > **Alarm Filter** > **Enable**.
3. Click **Yes** in the confirmation message.

Fabric Watch alarm information

In Fabric Watch you can view two types of reports:

- Alarm notifications — Displays the alarms that occurred for a selected class or area.
- Alarm configuration — Displays threshold and alarm configurations for a selected class or area.

Viewing an alarm configuration report

Use the **Threshold Configuration** tab, **Configuration Report** subtab to display a report of the configuration for a selected class or area with the following information:

- Threshold settings (labeled Threshold Configuration)
- Notification settings (labeled Action Configuration)
- Element settings (not labeled). You can scroll through this information, but cannot make changes.

To view an alarm configuration report, perform the following steps.

1. Open the **Fabric Watch** window.
2. Select the **Threshold Configuration** tab.
3. Select a previously configured element from the **Fabric Watch Explorer** pane (for instructions, refer to Enabling or disabling threshold alarms for individual elements on page 102).
4. Under Area Selection, select the alarm area report to be viewed.
5. Select the **Configuration Report** subtab.

   This tab displays a report of the configuration for the selected area.

Displaying alarms

Using the **Alarm Notification** tab, you can view a list of all alarms that occurred for a selected class or area (Opening the Fabric Watch window on page 99). The table below describes the columns in this report. You can click the header of each column to change the way the information is sorted in your view. You can also right-click the column header and select sort options from a menu.

NOTE
For the FRU class, only the Name, State, and Time columns are displayed. In addition, if the FRU area is Fan, the Name column refers to either a fan or a fan FRU, depending on the switch model.

TABLE 31 Alarm notification tab fields

Field	Description
Name	The string assigned to the element that had an event
State	The current state of the element
Reason	The event type that was triggered
Last Value	The data value of the element when the event was triggered
Current Value	The current data value of the element
Time	Time when the event occurred

To display the alarms page, perform the following steps.

1. Open the **Fabric Watch** window.
2. In the **Fabric Watch Explorer** pane, select the class that you want to check for alarms.
3. Select the **Alarm Notification** tab.
4. Under Area Selection, select the area that you want to check for alarms from the list. All alarms for that area display.

E-mail notification using Web Tools

You can be notified of an alarm condition through an e-mail alert. If you have configured alarms to send an e-mail notification, you must also configure the e-mail server and the e-mail recipient, as described in the following sections.

Configuring the e-mail server on a switch

You must set up the e-mail notification recipient's DNS server and domain name on each switch for which e-mail notification is enabled.

To configure the alert e-mail address on the switch, perform the following steps:

1. Open the **Switch Administration** window.
2. Select the **Switch** tab.
3. In the DNS Configuration area, enter the primary Domain Name Server IP address in the **DNS Server 1** field. You can enter the IP address in IPv4 or IPv6 format.
4. Enter the secondary Domain Name Server IP address in the **DNS Server 2** field. You can enter the IP address in IPv4 or IPv6 format.

5. In the **Domain Name** field, enter the domain name (between 4 and 32 characters).
6. Click **Apply**.

Enabling the e-mail alert

You can set a different e-mail alert configuration for each FRU class. For example, you can set one e-mail notification for SFPs and another for E_Ports. Before configuring e-mail alert recipients, you must set up the e-mail notification recipient's DNS server and domain name. Refer to Configuring the e-mail server on a switch on page 105.

Fabric OS 7.3.0 supports up to five e-mail addresses. E-mail addresses must not exceed 128 characters.

NOTE
You must execute the **fwalfilterset 1** command to enable e-mail notification. Refer to the *Fabric OS Command Reference* for information on this command.

To enable an e-mail alerts recipient, perform the following steps:

1. Open the **Fabric Watch** window.
2. Select the **Email Configuration** tab.
3. Select a FRU class in the **Fabric Watch Explorer** pane.
4. Click **Enable**.
5. Enter the e-mail addresses of the recipients in the **Recipient Email Address** field.

   Separate multiple e-mail addresses with commas.
6. Click **Apply**.
7. Repeat steps 3 through 6 for any additional FRU classes.
8. Click **Send Test Email** to receive a test e-mail so you can verify the e-mail notification is working correctly. You can send a test e-mail only after you have applied your settings.

Disabling the e-mail alert

When you disable e-mail alerts, Fabric Watch does not send e-mail notification, even if the e-mail notification method is assigned to monitored areas.

To disable an e-mail alerts recipient, perform the following steps:

1. Open the **Fabric Watch** window.
2. Select the **Email Configuration** tab.
3. Select a FRU class in the **Fabric Watch Explorer** pane.
4. Click **Disable**.
5. Enter the word "NONE" in the **Recipient Email Address** field.

   You can disable the e-mail notification without removing the e-mail addresses.
6. Click **Apply**.

   Repeat steps 3 through 6 for any additional FRU classes.

Fabric Watch Reports

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, which enables you to track marginal or faulty ports that can affect throughput or switch performance.

You can generate reports from the command line using a Telnet session or by using Web Tools. The examples given here use the command line interface.

TABLE 32 Fabric OS commands to view Fabric Watch reports

Command	Displays
fwSamShow	Port failure rate report
switchStatusShow	Switch health report
switchStatusPolicyShow	Switch status policy report
fwPortDetailShow	Port detail report
fwPortDetailShow --s h	To view only health ports
fwPortDetailShow --s m	To view only marginal ports
fwPortDetailShow --s f	To view only faulty ports
fwPortDetailShow --s o	To view only offline ports

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

- Switch Availability Monitor report
- Switch Health report
- Switch Status Policy report
- Port Detail report

Switch Availability Monitor 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.

NOTE
SAM report details do not display the health status of GbE ports. Fabric Watch only monitors and reports the status for physical and virtual FC ports.

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, which enables you to track marginal or faulty ports that can affect throughput or switch performance.

You can generate reports from the command line using a Telnet session or by using Web Tools. The examples provided here use the command line interface.

Generating a Switch Availability Monitor report

1. Connect to the switch and log in as admin.
2. Enter the **fwSamShow** command to generate a SAM report.

   The following is an example of a SAM report.

```
                             Total       Total       Down        Total
Port               Type      Up Time     Down Time   Occurrence  Offline Time
                             (Percent)   (Percent)   (Times)     (Percent)
=============================================================================
1/0                    U       0           0           0         100
1/1                    U       0           0           0         100
1/2                    U       0           0           0         100
1/3                    U       0           0           0         100
1/4                    U       0           0           0         100
1/5                    U       0           0           0         100
1/6                    U       0           0           0         100
1/7                    U       0           0           0         100
1/8                    U       0           0           0         100
1/9                    U       0           0           0         100
1/10                   U       0           0           0         100
1/11                   U       0           0           0         100
1/12                  EX     100           0           0           0
1/13                  EX     100           0           0           0
1/14                  EX     100           0           0           0
1/15                  EX     100           0           0           0
2/0                    U       0           0           0         100
2/1                    U       0           0           0         100
2/2                    U       0           0           0         100
2/3                   LB     100           0           0           0
2/4                    U       0           0           0         100
2/5                   LB     100           0           0           0
2/6                    U       0           0           0         100
2/7                    U       0           0           0         100
      (output truncated)
```

Switch Health report

The Switch Health report lists the following information:

- Current health of each port, based on the currently configured policy settings.
- High-level state of the switch, the power supplies, and temperature monitor.
- All ports that are in an abnormal state and 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.

NOTE
Switch Health report details do not display the health status of GbE ports. Fabric Watch only monitors and reports the status for physical and virtual FC ports.

Generating a Switch Health report

The following is an example of a Switch Health report.

1. Connect to the switch and log in as admin.
2. Enter the **switchStatusShow** command to generate a Switch Health report.

```
switch: admin
Password:******

admin> switchstatusshow
Switch Health Report        Report time: 03/09/2011 04:54:45 PM
Switch Name:    Sat 240
IP address: 1080::8:800:200C:417A
SwitchState:    HEALTHY
Duration:       01:10

Power supplies monitor    HEALTHY
Temperatures monitor      HEALTHY
Fans monitor              HEALTHY
Marginal ports monitor    HEALTHY
Faulty ports monitor      HEALTHY
Missing SFPs monitor      HEALTHY
Error ports monitor       HEALTHY
All ports are healthy
```

NOTE
The final portion of the report detailing port health (below the “Duration” line) , is not available without a Fabric Watch license.

Switch Status Policy report

The Switch Status Policy report displays the current policy parameter.

The following example of the **switchStatusPolicyShow** command output is for enterprise-class platforms such as the DCX Backbone. For modular switches, the switch status policy report also contains information on the WWN, blade, and CP.

Generating a Switch Status Policy report

1. Connect to the switch and log in as admin.
2. Enter **switchStatusPolicyShow**. This generates a Switch Status Policy report.

```
switch:admin> switchStatusPolicyShow
The current overall switch status policy parameters:
```

```
                          Down        Marginal
PowerSupplies       2           1
Temperatures        2           1
Fans                2           1
Flash               0           1
MarginalPorts       6.15%       2.25%
FaultyPorts         16.50%      12.19%
MissingSFPs         20.00%      10.89%
ErrorPorts          20.10%      20.96%
Number of Ports: 512
```

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. You can also see port details by health. For example, you can see only healthy ports, only marginal ports, only faulty ports, or only offline ports.

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

NOTE
Port Detail reports do not display the health status of GbE ports. Fabric Watch only monitors and reports the status for physical and virtual FC ports.

Generating a Port Detail report

1. Connect to the switch and log in as admin.
2. Enter the **fwPortDetailShow** command to generate a Port Detail report.

   Refer to Fabric Watch reports on page 107 for additional commands to view more port detail information.

```
Port Detail Report                Report time: 04/24/2007 03:40:10 AM
Switch Name:    geo_hi
IP address:    1080::8:800:200C:417A
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 SVO
--------------------------------------------------------------------------------
080    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
081    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
082    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
083    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
084    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
085    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
086    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
087    F   HEALTHY   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
088    F   HEALTHY   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
089    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
090    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
091    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
092    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
093    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
094    U   OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
095    DP  OFFLINE   062:17   -      -   -      -   -      -   -      -   -      -   -      -   -
208    G   HEALTHY   000:00   -      -   -      -   -      -   -      -   -      -   -      -   -
209    G   HEALTHY   000:00   -      -   -      -   -      -   -      -   -      -   -      -   -
210    G   HEALTHY   000:00   -      -   -      -   -      -   -      -   -      -   -      -   -
211    G   HEALTHY   000:00   -      -   -      -   -      -   -      -   -      -   -      -   -
212    G   HEALTHY   000:00   -      -   -      -   -      -   -      -   -      -   -      -   -
213    G   HEALTHY   000:00   -      -   -      -   -      -   -      -   -      -   -      -   -
214    G   HEALTHY   000:00   -      -   -      -   -      -   -      -   -      -   -      -   -
```

```
215    G   HEALTHY   000:00   -       -   -      -   -      -   -      -   -      -   -      -   -
216    VE  HEALTHY   061:19   -       -   -      -   -      -   -      -   -      -   -      -   -
217    VE  HEALTHY   061:19   -       -   -      -   -      -   -      -   -      -   -      -   -
      (output truncated)
```

NOTE
Output of the Port Detail report depends on the ports that belong to the current Admin Domain context. If a port does not belong to the current Admin Domain, nothing other than the port number is displayed for that port; for example: `000 ----------------Not a member of current Admin Domain-------------------`.

The table below lists and describes each item in the Port Detail report.

TABLE 33 Port Detail report columns

Report item	Description
LFA	Link Loss: The number of link loss occurrences out of range for a specified time period.
LSY	Sync Loss: The number of sync loss occurrences out of range for a specified time period.
LSI	Signal Loss: The number of signal loss occurrences out of range for a specified time period.
PER	Protocol Error: The number of protocol errors out of range for a specified time period.
INW	Invalid Word: The number of invalid words out of range for a specified time period.
CRC	Invalid CRC: The number of CRC errors out of range for a specified time period.
PSC	Port hardware state changed too often because of 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.
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.

Index