53-1001770-01
30 March 2010

Fabric Watch

Administrator's Guide

Supporting Fabric OS v6.4.0

BROCADE

Brocade Communications Systems, Incorporated

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

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication Number	Summary of Changes	Date
Fabric Watch User's Guide	53-0001559-02	New document	May 2000
Fabric Watch User's Guide	53-0000198-02	n/a	January 2002
Fabric Watch User's Guide	53-0000186-02	n/a	March 2002
Fabric Watch User's Guide	53-0000504-02	n/a	April 2003
Fabric Watch User's Guide	53-0000524-02	n/a	April 2003
Fabric Watch User's Guide	53-0000524-03	Updated default values and restructured the document.	December 2003
Fabric Watch User's Guide	53-0000524-04	Rewrote the document completely and added new features. Reorganized procedures into steps, rewrote many sections to improve clarity. Added technical and editorial changes.	April 2004
Fabric Watch User's Guide	53-0000524-05	Updates to support Fabric OS v4.4.0 features and Brocade 3016 and 4100 switches. Rewrote Chapter 4, "Configuring Fabric Watch."	September 2004
Fabric Watch Administrator's Guide	53-0000524-06	Renamed book. Combined the Introduction and Concepts chapters into a single chapter. Added support for Brocade 200E, Brocade 3014, and Brocade 48000.	March 2005
Fabric Watch Administrator's Guide	53-1000047-01	Updates to support Fabric OS v5.1.0 features and Brocade 4900 and 7500 switches.	November 2005
Fabric Watch Administrator's Guide	53-1000243-01	Updates to support Fabric OS v5.2.0 features and the FC4-16IP and FC4-48 port blades. Removed references to Brocade 3014 and 3016, as embedded switches are not supported in Fabric OS v5.2.0.	September 2006
Fabric Watch Administrator's Guide	53-1000438-01	Updates to support Fabric OS v5.3.0, implementation of IPV6.	June 2007
Fabric Watch Administrator's Guide	53-1000601-01	Updates to support Fabric OS v6.0.0.	September 2007

Title	Publication Number	Summary of Changes	Date
Fabric Watch Administrator's Guide	53-1000601-02	Updates to support Fabric OS v6.1.0.	March 2008
Fabric Watch Administrator's Guide	53-1000601-03	Reorganized many sections to improve clarity. Updates to support Fabric OS v6.2.0: Virtual Fabric, port movement, fan monitoring behavior, link reset, DCX-4S.	November 2008
Fabric Watch Administrator's Guide	53-1001342-01	Updates to support Fabric OS v6.3.0: portThConfig, portFencing, and sysMonitor commands and Brocade 8000 support.	July 2009
Fabric Watch Administrator's Guide	53-1001770-01	Updates to support Fabric OS v6.4.0: portThConfig, sysMonitor, thConfig, and portFencing commands (recommended for use in configuring class areas instead of the fwConfigure command); recommended class settings added.	March 2010

Contents

Figures

Tables

About This Document

In this chapter

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible.

This document contains the following components:

- Chapter 1, "Fabric Watch," provides an introduction to Fabric Watch and the benefits of its use. It also defines concepts that are useful in Fabric Watch configuration.
- Chapter 2, "Fabric Watch Thresholds," explains the concept of high and low thresholds and buffer values and provides examples of various threshold settings.
- Chapter 3, "Fabric Watch Threshold Components," describes the components (class, area, and element) associated with every monitored behavior.
- Chapter 4, "Fabric Watch Activation," describes the Fabric Watch requirements, provides an overview of the interfaces, and explains the methods of accessing Fabric Watch through each interface.
- Chapter 5, "Fabric Watch Configuration," provides a comprehensive table that lists the commands you can use to create custom threshold configurations. This chapter discusses configuration files, setting the port persistence time, custom and default values, and e-mail notifications.
- Chapter 6, "Fabric, Security, SFP, and Performance Monitoring," describes how to configure high and low thresholds for Fabric Watch event monitoring for SFP, fabric, and security classes using the **ThConfig** command.
- Chapter 7, "Port Monitoring," describes how to configure high and low thresholds, buffers, triggers, and actions on specified ports using the **portThConfig** command.

- Chapter 8, "System Monitoring," describes how to configure system memory and CPU values using the **sysMonitor** command. This chapter also lists the switch status policy factors that affect the health of the switch, describes how to set and view switch status policies, and details how to configure FRUs.
- Chapter 9, "Fabric Watch Reports," describes the reports available through Fabric Watch and the methods of accessing each.
- Appendix A, "Fabric Watch Configuration Using Legacy Commands," describes how to configure port thresholds and perform advanced configuration tasks using the **fwConfigure** command.

Supported hardware and software

This document is specific to Brocade Fabric OS version 6.4.0 and all switches running Fabric OS version 6.4.0. Refer to the *Fabric OS Command Reference Manual* for a complete list of supported hardware and software products.

What's new in this document

This document contains information that was available at the time the product was released. Any information that becomes available after the release of this document is captured in the release notes.

New information

- A shift away from the interactive mode using **fwConfigure** and **fwShow** commands toward command-driven configuration using the new commands listed below.
  - **thConfig** command, used to configure Fabric class, Security class, SFP class, and Performance class areas and actions.
  - **portThConfig** command, used to configure the physical port and its subclasses, the E_Port, FOP_Port, and FCU_Port areas and actions.
  - **sysMonitor** command, used to configure the Resource class and Environment class areas and actions.
- Port fencing recommendations
- FCU_Port (copper) information

Changed information

The following information was changed:

- High, low, and buffer threshold settings for the following classes and areas:
  - Environment class, temperature area.
  - Port class, Class 3 Discard area, Invalid Transmission Word (ITW) area, Link Failure Count area, Loss of Synchronization Count area, and State Change area.
  - FOP_Port class, Class 3 Discard area, Loss of Synchronization Count area, State Changes area, Invalid Transmission Word (ITW) area, Link Failure Count area, Trunk Utilization area.
  - Resource class, Flash area.
- "F_Port" is now referred to as "FOP_Port."

Removed information

The following information was removed:

- Environment class, fan area (no longer supported).
- Performance Monitor, AL_PA area (this area still displays using the **fwConfigure** command, but it is no longer supported).
- The following security areas from the fwConfigure menu: API violations, RSNMP violations, WSNMP violations, SES violations, MS violations, serial violations, front panel violations, invalid timestamps, invalid signatures, invalid certificates, SLAP bad packets.

Document conventions

This section describes text formatting conventions and important notices formats.

Text formatting

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

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

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

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in 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 potential damage to hardware or data.

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.

Key terms

For definitions specific to Brocade and Fibre Channel, see the *Brocade Glossary*.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at *http://www.snia.org/education/dictionary*.

Additional information

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

To get up-to-the-minute information, go to *http://my.brocade.com* to register at no cost for a user ID and password.

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

http://www.brocade.com/products-solutions/products/index.page

For additional Brocade documentation, visit the Brocade website:

http://www.brocade.com

Release notes are available on the MyBrocade website and are also bundled with the Fabric OS firmware.

Other industry resources

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

http://www.t11.org

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

http://www.fibrechannel.org

Getting technical help

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

1. General Information
   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - syslog message logs
2. Switch Serial Number

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

   

   The serial number label is located as follows:

   - Brocade 300, 4100, 4900, 5100, 5300, 7500, 7500E, 7800, 8000, VA-40FC, and Brocade Encryption Switch—On the switch ID pull-out tab located inside the chassis on the port side on the left
   - Brocade 5000—On the switch ID pull-out tab located on the bottom of the port side of the switch
   - Brocade 7600—On the bottom of the chassis
   - Brocade 48000—Inside the chassis next to the power supply bays
   - Brocade DCX—On the bottom right on the port side of the chassis

- Brocade DCX-4S—On the bottom right on the port side of the chassis, directly above the cable management comb

3. World Wide Name (WWN)

   Use the **licenseIdShow** command to display the WWN of the chassis.

   If you cannot use the **licenseIdShow** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

Document feedback

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. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1 Fabric Watch

In this chapter

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 Action 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. Each switch within a fabric needs its own license, and that license is valid only for a particular version of the feature. If you want a newer version of the feature, you must purchase a new license.

Fabric OS includes basic switch and fabric support software, and support for optionally-licensed software that is enabled using license keys. Refer to the *Fabric OS Administrator’s Guide* for more information about licensing and how to obtain the Fabric Watch license key.

Fabric Watch threshold components

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.

An example of a very simple Class --> Area --> Element hierarchy follows.

Environment

--> Temperature

--> Fan

--> Power supply

--> Slot

For specific information about classes, areas, and elements, refer to Chapter 3, "Fabric Watch Threshold Components".

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 41.

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. See the *Fabric OS Command Reference Manual* 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. Since 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 49

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 44.

SFP monitoring

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

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 47.

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 Manual* for more information and for details about the **portThConfig** command.

If frame discard errors or any other configured areas exceed the currently effective threshold settings, the Fabric Watch daemon can take one or more of the following actions:

- Send an SNMP trap.
- Log a RASlog message.
- Send an E-mail alert.
- Log a port log message.
- Enable port fencing. Refer to "Port fencing" for more information.

For complete information about port monitoring, including configuration examples, port setting guidelines, and default settings, refer to "Port Monitoring" on page 57.

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 74.

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 using the portFencing command" on page 75 for instructions.

When a port that has exceeded its user-defined thresholds is fenced by software, the port is placed into the disabled state and held offline, thereby removing the ability of the port to transmit or receive frames. After a port is disabled, user intervention is necessary for frame traffic to resume on the port.

System resource monitoring

System resource monitoring enables you to monitor your system's RAM, flash, memory, 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.
- 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.

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.

See "Switch status policy planning" on page 89 for information on configuring switch policies.

See Chapter 9, "Fabric Watch Reports," for information on viewing the current switch policies using the switch policy report.

Virtual Fabric 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 the port was moved from, and created for the logical switch to where the port is moved.

A logical interswitch link (LISL) is the logical portion of the physical connection that joins base switches. You can enable or disable port thresholds and create thresholds for state changes on LISLs, but Fabric Watch does not support other threshold areas such as link loss or signal loss for LISLs as it does for normal E_Ports. See "Port class areas" on page 57, for a complete list of state changes that are allowed on an LISL.

NOTE
Only state changes are supported on LISL ports.

For complete information about system resource monitoring, including setting guidelines and default settings, refer to "System monitoring using the sysMonitor command" on page 85.

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 (MIBs) 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.

In Fabric OS v6.4.0 and later, SNMP traps are identified by their bit mask and can be read directly from the switch configuration. Refer to the *Fabric OS Command Reference* for information about how to enable or disable the sending of traps from the various MIBs, and to understand SNMP trap bit mask values.

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 MIB Reference Guide* 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.
- For some Fabric Watch parameters, you can create custom configurations to suit your unique environment.

The **fwSetToCustom** command allows you to switch from default to custom settings. The command assumes that a set of user-defined thresholds have been configured prior to executing the **fwSetToCustom** command. If no user-defined settings exist, this command reapplies the default values.

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.

NOTE
Event settings are non-persistent.

Types of event behaviors

Based on the number of notifications delivered for events, there are two categories of automatic notifications:

- Continuous event behavior
- Triggered event behavior

Continuous event behavior

A *continuous alarm* provides a warning message whenever a threshold is breached; it continues to send alerts until the condition is corrected. For example, if a switch exceeds its temperature threshold, Fabric Watch activates an alarm at every measurement interval until the temperature returns to an acceptable level.

You can set behavior type events to continuously trigger during a given sample period, until the fabric no longer meets the criteria defined for the event.

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

Triggered event behavior

A *triggered alarm* generates the first warning when a threshold condition is reached and a second alarm when the threshold condition is cleared.

If you do not want notification during each sample period from the port hardware failure to the time of its repair, you can define the event behavior as *triggered*. Triggered is the default behavior type signal for all class areas.

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

Whereas a *triggered* behavior type sends only one event notification when the fabric meets the criteria for the event, a *continuous* behavior type signals you continuously after a threshold has been crossed.

For specific configuration procedures, refer to the following chapters in this guide:

- "Setting Fabric Watch custom and default values" on page 35
- "Customizing thConfig command settings" on page 52
- "portThConfig command procedures" on page 69
- "System monitoring using the sysMonitor command" on page 85

For detailed information about all Fabric Watch commands, refer to the *Fabric OS Command Reference Manual*.

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 alert

An e-mail alert sends information about a switch event to a specified e-mail address. 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 e-mail alerts using one of the following methods:

- 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-mails 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

NOTE
The SNMP trap stores event information but does not actively send alerts.

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, see the *Fabric OS Command Reference.*

RASlog (switch event)

Following an event, Fabric Watch adds an entry to the internal event log for an individual switch. 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, see 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—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, see the *Fabric OS Message Reference*. For information on configuring an Audit Log, see the Audit Log Configuration section of the *Fabric OS Administrator's Guide* for more information.

Data values

A data value represents a measured value or a state value:

- *Measured value* is the current, measurable value of a fabric or fabric element, such as environmental temperature.
- *State value*, which is the only qualitative data value, provides 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.

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

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

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), or second (samples are compared every second). This configurable field affects the comparison of sensor-based data with user-defined threshold values.

See "Time bases" on page 17 for more information.

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

Before you begin an implementation, make some decisions surrounding the following major configuration tasks.

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:

- Step 1. Monitor Fabric class areas using the **thConfig** command.
  Refer to Chapter 6, "Fabric, Security, SFP, and Performance Monitoring," for details.
- Step 2: Monitor Port class areas using the **portThConfig** command.
  Refer to Chapter 7, "Port Monitoring," for details.
- Step 3: Monitor FRU class areas using the **fwFruCfg** command.
  Refer to Chapter 8, "System Monitoring," 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.

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).

Event behavior configuration

If you change the event type of an alert from *triggered* to *continuous*, 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.

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. Use the advanced configuration option provided with the **portThconfig**, **thConfig**, and **sysMonitor** commands

Valid intervals are day, hour, minute, or second.

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 which 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.
- If the event setting is continuous, consider switching to triggered. A continuous event setting will cause error messages to be sent repeatedly as long as the event conditions are met. While each message may be meaningful, a high volume of these messages could cause other important messages to be missed.
- Examine the notification settings. If you are not interested in receiving messages under certain conditions, ensure that the notification setting for that event is set to zero. For example, you may not be interested in knowing when the sensed temperature is between your high and low temperature settings, so setting the InBetween notification setting to zero for this area will eliminate messages generated in this situation.

We recommend using either SNMP trap alerting to your system management console or event log entry in conjunction with Syslog forwarding configured on your switches.

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 action.

1 Reasons to customize Fabric Watch settings

Chapter

Fabric Watch Thresholds

2

In this chapter

Threshold values

Threshold values are of the following types:

- High and low thresholds
- Buffer values

High and low thresholds

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

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

Buffer values

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

You can use buffer values to reduce the occurrence of events resulting from data fluctuation. When you assign a buffer value, it is used to create a zone below the high threshold and above the low threshold. When values cross above the high threshold or below the low threshold, an event occurs.

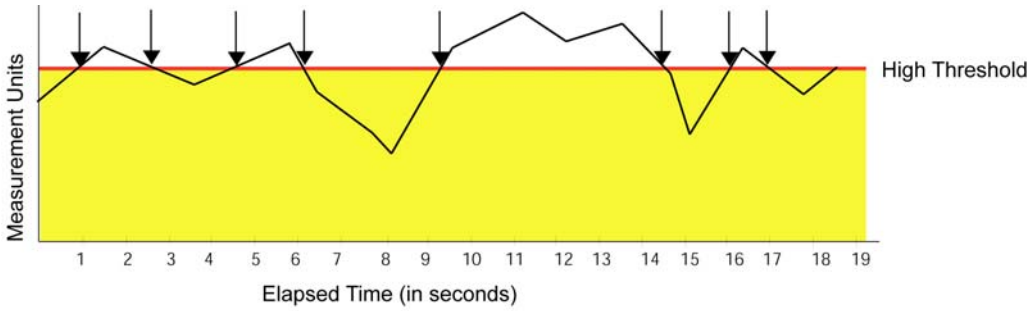

FIGURE 1 **Threshold monitoring**

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

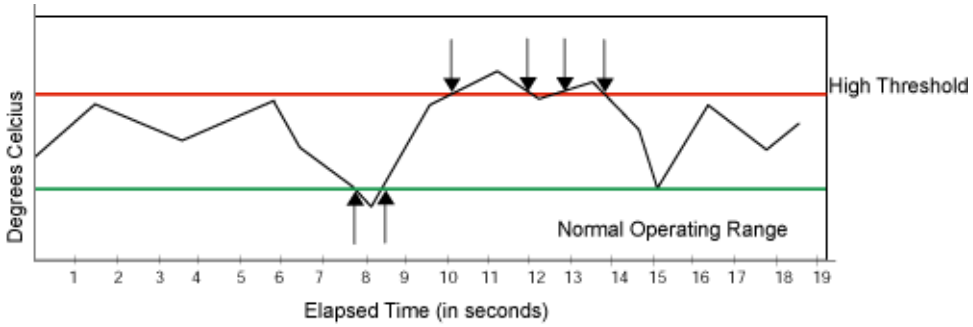

FIGURE 2 **A buffered data region**

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), or second (samples are compared every second). 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.

Figure 3 shows a high limit of 65 degrees 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.

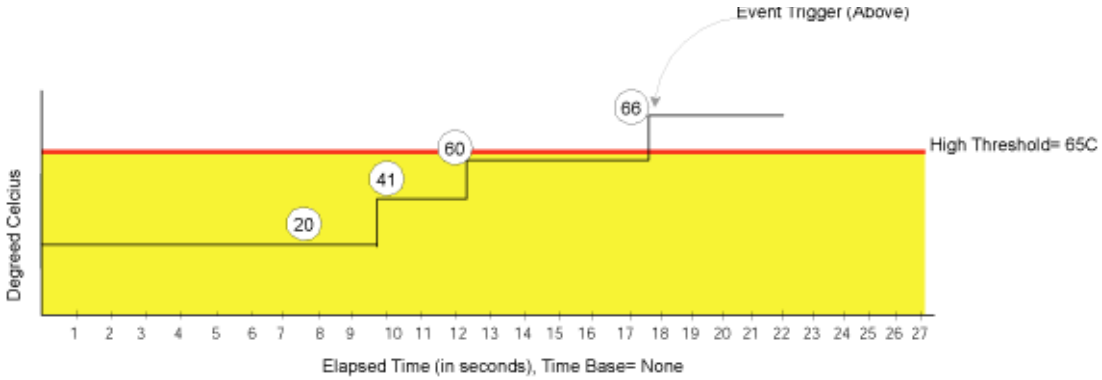

FIGURE 3 Time base set to none

Time base set to other than none

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

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

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

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

The following examples illustrate each point.

Example 1: Triggering an event

Figure 4 shows a sample graph of data obtained by Fabric Watch (the type of data is irrelevant to the example). A high threshold of 2 is specified to trigger an event. A time base of *minute* is defined. An event occurs only if the rate of change in the specific interval (one minute in this example) is across the threshold boundary. It should be either higher than the high threshold limit or lower than the low threshold limit.

As illustrated on the tenth sample, the counter value changes from 0 to 1; hence calculated rate of change is 1 per minute. At the thirteenth sample, the rate of change is 2 per minute. The rate of change must be at least 3 per minute to exceed the event-triggering requirement of 2, which is met on the eighteenth sample.

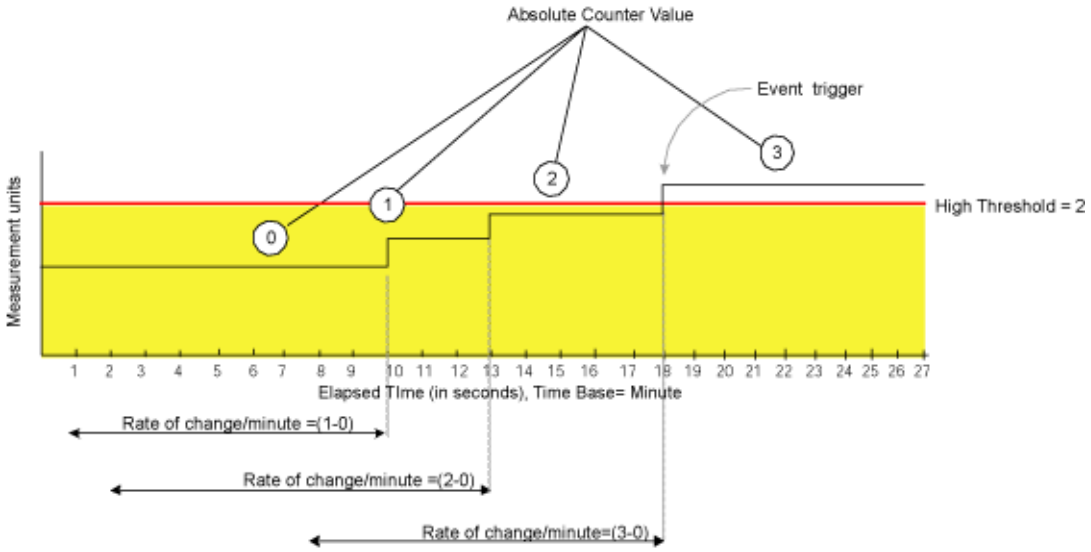

FIGURE 4 Event trigger

Example 2: Not triggering an event

Figure 5 uses the same data to illustrate a case in which a threshold is exceeded without triggering an event. In this case, the calculated rate of change in the data value is always less than or equal to the high threshold of 2.

At the tenth sample, the rate of change is one per minute. At the fourteenth, twenty-first, and twenty-fifth sample, the rate of change remains equal to the high threshold of 2. In this case, Fabric Watch does not trigger an event even though the absolute value of the counter reaches 4, which is well above the high threshold.

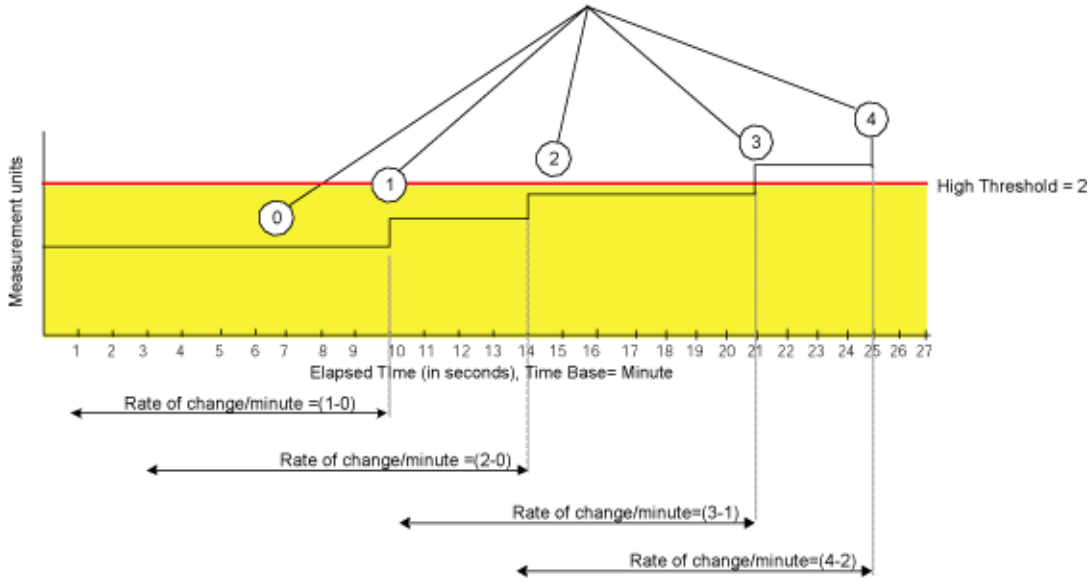

FIGURE 5 **Example without an event**

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. Figure 6 shows an *Above* event trigger with a buffer zone. The Above event trigger occurs when the counter crosses the high threshold (event 1 in Figure 6). 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.

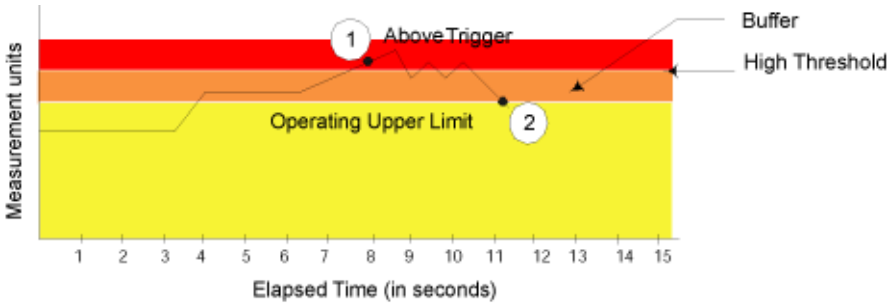

FIGURE 6 **Above event trigger with buffer zone**

Below event trigger

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

When a buffer is defined, the 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.

Changed event trigger

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

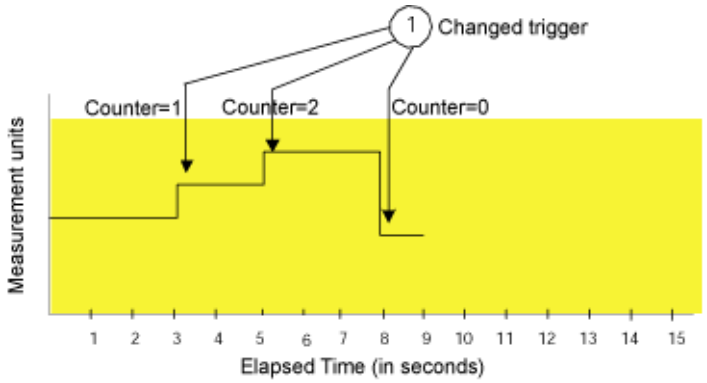

FIGURE 7 **Changed threshold**

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

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).

Chapter

Fabric Watch Threshold Components

3

In this chapter

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. Table 1 on page 24 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 Table 1, refer to one of the following chapters:

- Chapter 6, “Fabric, Security, SFP, and Performance Monitoring”

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

- Chapter 7, “Port Monitoring”

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

- Chapter 8, “System Monitoring”

  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.

Table 1 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.
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.

TABLE 1 Fabric Watch classes (Continued)

Class	Description
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. **Note:** If you are using a Brocade 48000 or a Brocade 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 (includes EX_Ports) — FCIP (includes VE_Ports and VEX_Ports) — State changes (applicable for all ports) — Utilization and packet loss (applicable to VE_Ports only) • 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.

3 Fabric Watch classes, areas, and elements

Chapter

Fabric Watch Activation

4

In this chapter

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. See "Activating Fabric Watch using a Telnet session" for instructions on how to activate Fabric Watch using a Telnet session.
- *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. See "Activating Fabric Watch using Web Tools" on page 28 for instructions on how to activate Fabric Watch using Web Tools.
- *SNMP* - Provides a receiver dedicated to monitoring the data center infracture; 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 Toos to set up SNMP on the Fabric OS switch. See "Activating Fabric Watch using SNMP" on page 29 for instructions on how to set up SNMP.

Activating Fabric Watch using a Telnet session

1. Connect to the switch and log in as admin.
2. Enter the following command, where *switch* represents the name or IP address of the switch:

   `telnet switch`

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

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 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:

```
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 username and password.
4. Select a switch from the Fabric Tree and log in if necessary.
5. Select **Tasks > Manage > Fabric Watch**.

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. First load the Brocade common MIB file, (SW.mib). If this is successful, the system displays a screen similar to Figure 8.

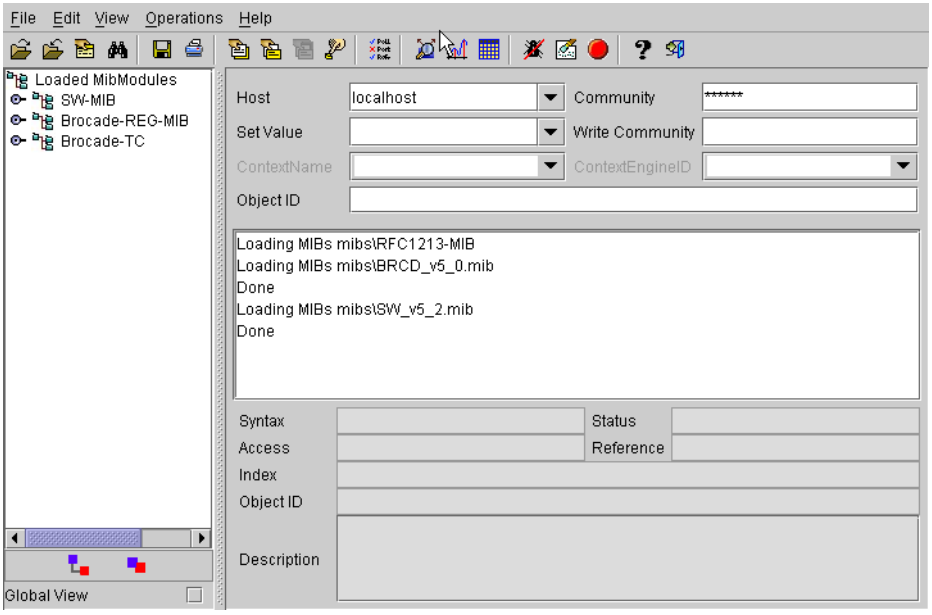

FIGURE 8 Configuring Fabric Watch using SNMP

In Figure 8, the MIB browser populated the left side of the screen with a MIB tree that you can navigate.

3. Open Web Tools and select **Tasks > Manage > Switch Admin**.
4. Click **Show Advanced Mode**.
5. 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.

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

NOTE
Currently, setting the SNMP MIB capability can only be done from the CLI.

```
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]
switch:admin>
```

7. Enter the **snmpConfig** command to configure the SNMP management host IP address.

```
switch:admin> snmpConfig

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

8. 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 into the **Write Community** field.
9. 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.

10. 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 screen similiar to the one shown in Figure 9.

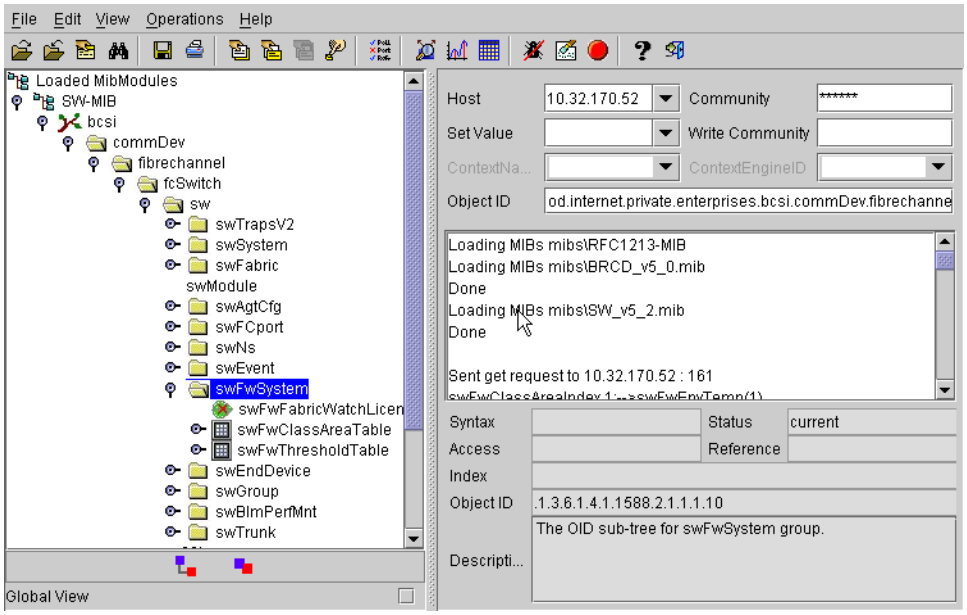

FIGURE 9 Example OID tree

11. 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, see the *Fabric OS MIB Reference.*

Chapter

Fabric Watch Configuration

5

In this chapter

Fabric Watch configuration tasks

Table 2 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 Manual*.

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 27.
Set the boundary and alarm level to custom or default. **Note:** These command resets all thresholds for all classes and cannot be configured on individual ports.	fwSetToCustom fwSetToDefault	"Setting Fabric Watch custom and default values" on page 35.
Configures Fabric Watch e-mail alerts for all classes.	fwMailCfg	"E-mail notification configuration" on page 35.
Configures and shows alarms filtering for Fabric Watch for all classes.	fwAlarmsFilterSet fwAlarmsFilterShow	"Configuring alarm notifications" on page 39.
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	Chapter 6, "Fabric, Security, SFP, and Performance Monitoring".

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 persistence • Port fencing	portThConfig portFencing	Chapter 7, "Port Monitoring"
Set the port persistence time	fwSet –port -persistence	"Setting the port persistence time" on page 74
Configure port fencing	portFencing	"Port fencing" on page 74
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 85.
Set and display the switch status policy parameters.	switchStatusPolicySet switchStatusPolicyShow	Chapter 8, "System Monitoring"
Show the overall switch status.	switchStatusShow	Chapter 8, "System Monitoring"
Configure FRU state and notifications.	fwFruCfg	*Chapter 8, "System Monitoring"*.
Display fan status	fanShow	*Chapter 8, "System Monitoring"*
Show sensor readings	sensorShow	*Chapter 8, "System Monitoring"*
Show switch temperature readings	tempShow	*Chapter 8, "System Monitoring"*
Create a detailed port report.	fwPortDetailShow	"Generating a Port Detail report" on page 99.
Show the availability of monitor information.	fwSamShow	"Switch Availability Monitor report" on page 96.

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. Enter the **fwMailCfg** command at the prompt.

   The fwMailcfg menu displays.

```
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]
```

2. Enter the number corresponding to the task you wish to perform.

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.

   The Config Show menu displays.

2. Select a class for which Fabric Watch should disable e-mail alerts.

   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.

   The Config Show menu displays.

2. Select a class for which Fabric Watch should enable e-mail alerts.

   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, see the *Fabric OS Command Reference Manual*.

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 recipient e-mail address for 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
   ```

Chapter

Fabric, Security, SFP, and Performance Monitoring 6

In this chapter

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

Table 3 lists Product Name areas in the Fabric class and describes each area. Configure the Fabric class using the **thConfig** command.

TABLE 3 Fabric class areas

Area	Description
Domain ID changes	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 has to assign another domain ID to a switch.
Fabric logins	Activates when ports and devices initialize with the fabric.
Fabric reconfigure	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	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	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	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.

- State changes

  SFP class areas and Port class (including E_Port and FOP_Port) areas are used to gather SFP state changes; therefore, don't change the default settings for the Fabric class.

- 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. Since fabric reconfigurations are monitored elsewhere, don't 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

Table 4 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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Loss of E_Port	Monitors E_Port and VE_Port status	Unit: Downs Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Fabric Logins	Monitors host device fabric logins	Unit: Logins Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Fabric Reconfiguration	Monitors configuration changes	Unit: Reconfigs Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Segmentation Changes	Monitors segmentation changes	Unit: Segmentations Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Zoning Changes	Monitors changes to currently enabled zoning configurations	Unit: Zone changes Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative 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

Table 5 lists Product Name areas in the security class and describes what each area indicates. Configure the Security class using the **thConfig** command.

TABLE 5 Security class areas

Area	Indicates
DCC violations	An unauthorized device attempts to log in to a secure fabric.
HTTP violations	A browser access request reaches a secure switch from an unauthorized IP address.
Illegal command	Commands permitted only to the primary Fibre Channel Switch (FCS) are executed on another switch.
Incompatible security DB	Secure switches with different version stamps have been detected.
Invalid certificates	Monitors invalid certificates.
Login violations	Login violations which occur when a secure fabric detects a login failure.
No-FCS	The switch has lost contact with the primary FCS.
SCC violations	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 (FCAP failures)	SLAP failures which occur when packets try to pass from a nonsecure switch to a secure fabric.
Telnet violations	Telnet violations which occur when a Telnet connection request reaches a secure switch from an unauthorized IP address.
TS Out of Sync	Time Server (TS) which occur when an out-of-synchronization error has been detected.

Security monitoring setting guidelines

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

Security class default settings

Table 6 provides default settings for areas in the Security class.

TABLE 6 Security class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
DCC Violations	Monitors DCC violations	Unit: Violations Time Base: minute Low: 1 High: 4 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
HTTP Violations	Monitors HTTP violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Illegal Commands	Monitors illegal commands	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Incompatible Security DB	Monitors incompatible security databases	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Invalid Certificates	Monitors invalid certificates	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Login Violations	Monitors login violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
No FCS Violations	Monitors No FCS violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
SCC Violations	Monitors SCC violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
SLAP Failures	Monitors SLAP failures	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range

TABLE 6 Security class default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Telnet Violations	Monitors Telnet violations	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
TS Out of Sync	Monitors instances in which the timestamp is out of sync	Unit: Violations Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range

SFP 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 or VEX_Ports.

NOTE
SFPs connected to GbE ports are not monitored.

SFP class areas

Table 7 lists Product Name areas in the SFP class and describes each area. 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. 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.
State Changes	Indicates whether the state of the SFP is normal or faulty, on or off. A faulty or off state means that you must reinsert, turn on, or replace the SFP. Fabric Watch monitors only the digital diagnostic SFP. **Note:** SFPs connected to GbE ports are not monitored.

SFP monitoring setting guidelines

Use the SFP default settings. 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.

SFP class default settings

Table 8 provides default settings for areas in the SFP class.

TABLE 8 SFP class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Current	Monitors SFP current	Unit: mA Time Base: none Low: 0 High: 50 Buffer: 1	Changed: 0 Below: 1 Above: 1 In-Between: 0	Informative Out_of_range Out_of_range Informative
Receive Power	Monitors receive power in µWatts	Unit: µWatts Time Base: none Low: 0 High: 5000 Buffer: 25	Changed: 0 Below: 1 Above: 1 In-Between: 0	Informative Out_of_range Out_of_range Informative
Supply Voltage	Monitors SFP electrical force in volts	Unit: mV Time Base: none Low: 2970 High: 3630 Buffer: 10	Changed: 0 Below: 1 Above: 1 In-Between: 0	Informative Out_of_range Out_of_range Informative
Temperature	Monitors SFP Temperature	Unit: Degrees C Time Base: none Low: -10 High: 85 Buffer: 3	Changed: 0 Below: 1 Above: 1 In-Between: 1	Informative Out_of_range Out_of_range Normal
Transmit Power	Monitors transmit power in µWatts	Unit: µWatts Time Base: none Low: 0 High: 5000 Buffer: 25	Changed: 0 Below: 1 Above: 1 In-Between: 0	Informative Out_of_range Out_of_range Normal
SFP State Changes	Monitors the insertion and removal of SFPs	Unit: Changes Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative 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

Table 9 lists Product Name areas in the Performance Monitor class and describes each area. Configure the Performance class using the **thConfig** command.

TABLE 9 Performance Monitor class areas

Area	Indicates
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

Table 10 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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

Table 11 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	Monitors the receiving traffic between a SID_DID pair in a port	Unit: KBps Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
End-to-End Transmit Performance	Monitors the transmit traffic between a SID_DID pair in a port	Unit: KBps Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

Configuration options for thConfig command

Use the **thConfig** command to configure thresholds for Fabric Watch event monitoring for the SFP, Fabric, Security, and Performance classes or to display the configuration. If configured areas exceed the currently-effective threshold settings, the Fabric Watch daemon can take one of the following actions:

- Send an SNMP message.
- Log a RASlog message.
- Send an e-mail alert.
- Log a port log message.

Setting guidelines and default settings for the Fabric, Security, SFP, and Performance classes are detailed later in this chapter.

For additional information about the **ThConfig** command, refer to the *Fabric OS Command Reference Manual*.

TABLE 12 Configuration options for **thConfig** command

Class name	Valid area types	Threshold	Threshold action	Configuration recommendation
SFP	TXP - Transmit areas RXP - Receive areas Current Voltage Temperature ST - SFP state changes	Default or Custom[1]	Default or Custom[2]	Use the SFP default settings. The traits are SFP-specific and there is no reason to alter them. See "SFP monitoring setting guidelines" on page 47 for more information.
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[1]	Default or Custom[2]	It is recommended that you leave the entire Fabric class in its default state (no alerts). See "Fabric monitoring setting guidelines" on page 42 for more information.
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[1]	Default or Custom[2]	Use the Security class default settings for areas and alarm configuration. There is no reason to alter the default settings.
Filter	CUSTDEF	Default or Custom[1]	Default or Custom[2]	Use the Filter default settings.

TABLE 12 Configuration options for **thConfig** command (Continued)

Class name	Valid area types	Threshold	Threshold action	Configuration recommendation
EE (End-to-end Performance)	RXF - Receive areas TXP - Transmit areas	Default or Custom[1]	Default or Custom[2]	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).

[1]To change the default, provide an integer value.
[2]Valid custom action setting values include snmp, raslog, portlog, email, or none.

Customizing thConfig command settings

Perform the following steps to customize **thConfig** settings. Refer to the *Fabric OS Command Reference Manual* for more information.

1. Connect to the switch and log in as admin.
2. Enter the **thconfig** command to display the list of operands.

```
switch:admin > thconfig

thconfig –show [<class_name>] [-area <area_type>]
[-current]|[-thresh_level|-action_level <thresh_action>]

thconfig –set <class_name> -area <area>
[-timebase <day:hour:minute:second:none>]
[-highth -value <val> -trigger above|below
-action [snmp],[raslog],[portlog],[email]|none]
[-lowth -value <val> -trigger above|below
-action [snmp],[raslog],[portlog],[email]|none]
[-buffer <val>]
[-nosave]

thconfig –apply [<class_name> -area <area_type> -thresh_level <thresh_level>
-action_level <action_level>

thconfig –cancel [<class_name> -area <area_type> -thresh_level <thresh_level>
-action_level <action_level>

thconfig –show [<class_name>][-area_only]
Applying the configuration changes
```

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.

thConfig command restriction

The Fabric and Security classes are not supported in Access Gateway mode.

CAUTION

When you use –set with the –nosave option and the switch reboots, your changes will be lost.

Example of thConfig command

The following example shows how to display the default threshold and alarms configuration for the DC area of the Fabric class.

```
Switch:admin> thconfig --show Fabric –area DC –thresh def

Class: Fabric
        Area    : DC
        ThLevel : Cust
        ActLevel: Cust
        High    :
                Default:
                        Value   : 1000
                        Trigger : Above Action: None
                        Trigger : Below Action: None
        Low:
                Default:
                        Value   : 0
                        Trigger : Below Action: None
        Buffer:
                Default:
                        Value   : 100
```

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

Table 13 lists the recommended settings for the Fabric, SFP, Security, and Performance classes discussed in this chapter. For all of these classes, it is recommended that you use the default settings.

TABLE 13 Recommended settings for Fabric, SFP, Performance, and Security monitoring

											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**	**Changed**	**Below**	**Above**	**In-between**	**Notes**
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	E	
	RX power	X		uWatts	None	0	5000	25	X			E	E	E	
	TX power	X		uWatts	None	0	5000	25	X			E	E	E	
	Current	X		mA	None	0	50	1	X			E	E	E	
	Voltage	X		uV	None	3150	3600	10	X			E	E	E	
	SFP state changes	X		Changes	None	0	0	0	X						
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						

TABLE 13 Recommended settings for Fabric, SFP, Performance, and Security monitoring (Continued)

																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**	**Changed**	**Below**	**Above**	**In-between**	**Notes**	
Security	Telnet violations	X		Violations	Minute	1	2	0	X				E,S			
	HTTP violations	X		Violations	Minute	1	2	0	X				E,S			
	RSNMP violations	X		Violations	Minute	1	2	0	X				E,S			
	WSNMP 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	4	0	X				E,S			
	Login violations	X		Violations	Minute	1	2	0	X				E,S			
	Invalid certificates	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			

Chapter

7

Port Monitoring

In this chapter

Port class areas

Table 14 lists and describes the Fabric OS v6.4.0 areas in the Port class. Configure the Port class using the **portThConfig** command. You can find port setting guidelines and specific examples of **portThConfig** configuration later in this chapter.

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 14 Port class areas

Area	Indicates
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.
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.
C3TX_TO	The number of Class 3 discards frames because of timeouts.
Link loss	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.
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. Note: Loss of signal count still displays using the fwConfigure command, but it is no longer supported.

TABLE 14 Port class areas (Continued)

Area	Indicates
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.
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 gliches. Persistent errors occur due to hardware problems.
RXP	The percentage of maximum bandwidth consumed in packet receipts.
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.
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 State Changes, Packet Loss, 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. Please refer to the following sections and plan carefully before you begin configuring the port.

- "Physical port setting guidelines"
- "E_Port subclass setting guidelines"
- "FOP_Port and FCU_Port subclass setting guidelines"

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

Physical port setting guidelines

For the physical port, use the default settings listed in Table 15 for all areas and alarms except for Invalid Transmission Words and Invalid CRC Count. For Invalid Transmission Words and Invalid CRC Count, the alarms should be set at two points: a low boundary and a high boundary, with the goal to alarm as the number of invalid words per minute rises above the low boundary and again as it rises above the high boundary. it is recommended that you set the high boundary at 25 and set the alarms to alert the error log any time this high boundary is exceeded.

Port class default settings

Table 15 provides default settings for areas in the Port class.

TABLE 15 Port class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Class 3 Discards	Class 3 discards frames due to timeout or destination unreachable.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Invalid CRC Count	Monitors the number of CRC errors	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Invalid Transmission Words	Monitors the number of invalid words transmitted	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Link Failure Count	Monitors the number of link failures	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

TABLE 15 Port class default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Loss of Signal Count	Monitors the number of signal loss errors	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Loss of Synchronization Count	Monitors the number of loss of synchronization errors	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Primitive Sequence Protocol Error	Monitors the number of primitive sequence errors	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Receive (Rx) Performance	Monitors receive rate, by percentage	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
State Changes	Monitors state changes	Unit: Changes Time Base: minute Low:0 High: 50 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Transmit (Tx) Performance	Monitors transmission rate, by percentage	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

E_Port subclass setting guidelines

E_Port guidelines for the areas listed below 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.

NOTE
The E_Port class represents ports connected to another switch. If you are using a Brocade 48000 or a Brocade 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 (includes EX_Ports), FCIP (includes VE_Ports and VEX_Ports), State changes (applicable for all ports).

- Area: Link Failure Count

  You want to be immediately notified if an E_Port loses a link, so set the alarm configuration to **Changed** for this area.

- 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 configuration" on page 68 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. See "Port configuration" on page 68 for instructions.

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

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

- Area: Link Reset

  Set the alarm to fence the port. This prevents a "flapping" E_Port, which could lead to congestion or frame loss. See "Port configuration" on page 68 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% and the alarms to Above and In-Between conditions. These settings indicate if the 75% threshold is exceeded and for how long.

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

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

E_Port class default settings

Table 16 provides default settings for areas in the E_Port class.

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 16 E_Port class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Class 3 Discards	Class 3 discards frames due to timeout or destination unreachable.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Invalid CRC Count	Monitors the number of CRC errors	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Invalid Transmission Words (ITW)	Monitors the number of invalid words transmitted	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Link Failure Count	Monitors the number of link failures	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Loss of Signal Count	Monitors the number of signal loss errors	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Link 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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

TABLE 16 E_Port class default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Loss of Synchronization Count	Monitors the number of loss of synchronization errors	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Primitive Sequence Protocol Error	Monitors the number of primitive sequence errors	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Receive (Rx) Performance	Monitors the receive rate, by percentage	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
State Changes	Monitors state changes	Unit: Changes Time Base: minute Low: 0 High: 50 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Transmit (Tx) Performance	Monitors the transmit rate, by percentage	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Packet Loss	The number of packets routed through a port exceeds the port bandwidth.	Unit: Errors Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

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. See "Port configuration" on page 68 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% 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

The following table provides default settings for areas in the FOP_Port and FCU_Port subclasses.

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

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

TABLE 17 FOP_Port subclass default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Class 3 Discards	Class 3 discards frames due to timeout or destination unreachable.	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Loss of Synchronization Count	Monitors the number of loss of synchronization errors	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Receive (Rx) Performance	Monitors the receive rate, by percentage	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative Informative
State Changes	Monitors state changes	Unit: Changes Time Base: minute Low: 0 High: 50 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

TABLE 17 FOP_Port subclass default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Transmit (Tx) Performance	Monitors the transmit rate, by percentage	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative Informative
Invalid CRC Count	Monitors the number of CRC errors	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Invalid Transmission Words	Monitors the number of invalid words transmitted	Unit: Errors Time Base: minute Low: 0 High: 1000 Buffer: 100	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Link Failure Count	Monitors the number of link failures	Unit: Errors Time Base: minute Low: 0 High: 500 Buffer: 50	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Loss of Signal Count	Monitors the number of signal loss errors	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Link 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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Primitive Sequence Protocol Error	Monitors the number of primitive sequence errors	Unit: Errors Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

VE_Port class default settings

Table 18 provides default settings (per minute) for areas in the VE_Port class.

TABLE 18 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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
State Changes	Monitors state changes	Unit: Changes Time Base: minute Low: 0 High: 50 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_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	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_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 Guide*.

Before you configure thresholds, you must first identify and select the appropriate class and areas, which are described in "Port class areas" on page 57.

Custom port settings

If you want to customize threshold and action settings (alarms), start with "Port class guidelines and default settings" on page 59. 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 higher, 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 Fabric or Admin Domain restrictions that may be in place. Refer to the *Fabric OS Command Reference Manual* 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. See "Port class guidelines and default settings" on page 59 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

In general, use the generic Port class to provide supplemental data for the specific E_Port, FOP_Port, or FCU_Port classes.

See "Physical port setting guidelines" on page 59 for more information.

Configuring a port with an Invalid CRC Count area

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

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

   ```
   portthconfig --set port -area crc -highth -value 25 -trigger above -action
   raslog
   ```

   - The alarms should be set at two points: a low threshold of 0 (the default) and a high threshold of 25 (the default is 1000). The goal 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 in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

   ```
   portthconfig --apply port -area crc -action_level cust -thresh_level cust
   ```

Configuring a port with an Invalid Transmission Words area

Invalid Transmission Words occur when a word does not transmit successfully, resulting in encoding errors. Invalid word messages usually indicate a hardware problem.

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

   ```
   portthconfig --set port -area itw -highth -value 25 -trigger above -action
   raslog,snmp,email,portlog
   ```

   - The alarms should be set at two points: a low threshold of 0 (the default) and a high threshold of 25 (the default is 1000). The goal 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 in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

```
portthconfig –apply port -area itw -action_level cust -thresh_level cust
```

Port type: E_Port

E_Port, FOP_Port, and FCU_Port guidelines represent a more aggressive approach in most areas than physical port guidelines, because failing or failed E_Ports, FOP_Ports, and FCU_Ports in a large fabric can cause serious fabric-wide issues if not detected early.

The following examples represent a sample configuration for an E_Port. See "E_Port subclass setting guidelines" on page 61 for detailed setting recommendations for each area.

Configuring an E_Port with an Invalid CRC Count area

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:

```
portthconfig –set e-port -area crc -highth -value 20 -trigger above -action
raslog,snmp,email,portlog
```

   - Excessive CRCs on E_Ports lead to fabric congestion and possible frame drops; therefore, change the high threshold value from 1000 (the default) to 20 (per minute).
   - Triggers specify actions for in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

```
portthconfig –apply e-port -area crc -action_level cust -thresh_level cust
```

Configuring an E_Port with an Invalid Transmission Words area

Invalid Transmission Words occur when a word does not transmit successfully, resulting in encoding errors. Invalid word messages usually indicate a hardware problem.

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

```
portthconfig –set e-port -area itw -highth -value 40 -trigger above -action
raslog,snmp,email,portlog
```

   - Excessive CRCs on E_Ports lead to fabric congestion and possible frame drops; therefore, change the high threshold value from 1000 (the default) to 40 (per minute).
   - Triggers specify actions for in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

```
portthconfig –apply e-port -area itw -action_level cust -thresh_level cust
```

Configuring an E_Port with a Class 3 Discards area

Class 3 (C3) discards frames because of timeouts (on 8 Gbps platforms only).

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

   ```
   portthconfig --set e-port -area c3tx_to -highth -value 5 -trigger above -action raslog,snmp,email,portlog
   ```

   - Unlike other areas, take a conservative approach for the C3 Discards area. Use the default setting of 5.
   - Triggers specify actions for in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

   ```
   portthconfig --apply e-port -area crc -action_level cust -thresh_level cust
   ```

Configuring an E_Port with a Link Reset area

Link reset errors occur on ports in which the number of link resets exceed the specified threshold value.

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

   ```
   portthconfig --set e-port -area lr -highth -value 5 -trigger above -action raslog,snmp,email,portlog
   ```

   - Change the high threshold value from 500 (the default) to 5 (per minute).
   - Triggers specify actions for in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).
   - Set the alarm to fence the port. This prevents a “flapping” E_Port, which could lead to congestion or frame loss. See “Port fencing configuration using the portFencing command” on page 75 for instructions.

2. Apply the changes.

   ```
   portthconfig --apply port -area lr -action_level cust -thresh_level cust
   ```

Configuring an E_Port with a Loss of Synchronization Count area

Loss of synchronization occurs when two devices fail to communicate at the same speed. Synchronization errors are always accompanied by a link failure, and frequently occur due to a faulty SFP or cable.

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

   ```
   portthconfig --set e-port -area los -highth -value 45 -trigger above -action
   raslog,snmp,email,portlog
   ```

   - Change the high threshold value from 500 (the default) to 45 (per minute).
   - Triggers specify actions for in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

   ```
   portthconfig --apply e-port -area los -action_level cust -thresh_level cust
   ```

Configuring an E_Port with a Link Failure Count area

Link failures frequently occur due to a loss of synchronization or a loss of a signal.

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

   ```
   portthconfig --set e-port -area lf -highth -value 5 -trigger changed -action
   raslog,snmp,email,portlog
   ```

   - Change the high threshold value from 500 (the default) to 5 (per minute).
   - Because you want to be immediately notified if an E_Port loses a link, set the trigger to **changed**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

   ```
   portthconfig --apply e-port -area lf -action_level cust -thresh_level cust
   ```

Configuring an E_Port with a Receive Performance area

The Receive (Rx) Performance area is used to monitor the bandwidth utilization of the interswitch (ISLs) in the fabric.

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

   ```
   portthconfig --set e-port -area rx -highth -value 75 -trigger above -action
   raslog,snmp,email,portlog
   ```

   - Set the high threshold value to 75 percent (the default is 100). These settings indicate if the 75% threshold is exceeded and for how long.
   - Triggers specify actions for in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

   ```
   portthconfig --apply port -area rx -action_level cust -thresh_level cust
   ```

Configuring an E_Port with a Transmit Performance area

The Transmit (Tx) Performance area is used to monitor the bandwidth utilization of the interswitch (ISLs) in the fabric.

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

   ```
   portthconfig --set e-port -area tx -highth -value 75 -trigger above -action
   raslog,snmp,email,portlog
   ```

   - Set the high threshold value to 75 percent (the default is 100).
   - Triggers specify actions for in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

   ```
   portthconfig --apply port -area tx -action_level cust -thresh_level cust
   ```

Configuring an E_Port with a Trunk Utilization area

Trunk utilization is the percentage of utilization at the time of the last poll.

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

   ```
   portthconfig --set e-port -area trunk-util -highth -value 75 -trigger above
   -action raslog,snmp,email,portlog
   ```

   - Set the high threshold value to 75 percent (the default is 100). These settings indicate if the 75 percent threshold is exceeded and for how long.
   - Triggers specify actions for in-range port behavior. Set the trigger to **above**.
   - Set the action to collect all notifications (raslog, snmp, email, and portlog).

2. Apply the changes.

   ```
   portthconfig --apply port -area trunk-util -action_level cust -thresh_level
   cust
   ```

Primitive Sequence Protocol Error area

The Primitive Sequence Protocol Error area is not used for monitoring; therefore, leave the default alarm settings at 0.

State Change area

The State Change area is not used for monitoring; therefore, leave the default alarm settings at 0.

Utilization area

The Utilization area is not used for monitoring; therefore, leave the default alarm settings at 0.

Packet Loss area

The Packet Loss area is not used for monitoring; therefore, leave the default alarm settings at 0.

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 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. Supported port types include physical ports, E_Ports, FOP_Ports, FCU_Ports, and Virtual E_Ports (VE_Ports).

Active or online ports with errors that exceed the threshold are fenced after a six-second delay. In cases where two types of errors occur within the six-second interval, the port is disabled and indicates the reason code for the first error type that exceeded the threshold. The following error types are supported on port fencing:

- Invalid Transmission Words (ITW)
- Invalid Cyclic Redundancy Checks (CRC)
- Link Reset (LR)
- State Change (ST)
- Protocol Error (PE)
- Class 3 discard frames (C3TXO)

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

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.

Recommended high port fencing thresholds

It is recommend you use conservative thresholds to prevent false triggers. Examples for the Invalid Transmitted Words and Invalid CRCs are shown in Table 19.

TABLE 19 High port fencing threshold recommendations

Area	High threshold (per minute) E_Ports	High threshold (per minute) Storage FOP_Ports	High threshold (per minute) Host FOP_Ports	Default
Invalid transmitted words (ITW)	40	80	1000	1000
Invalid cyclic redundancy check error (CRC)	20	40	1000	1000

Recommended low port fencing thresholds

Set in-between thresholds to much lower values with an alerting action (RASlog, SNMP trap, or e-mail). Examples for the Invalid Transmitted Words and Invalid CRCs are shown in Table 20. These alerts will trigger when the count exceeds the low threshold.

TABLE 20 Low port fencing threshold recommendations

Area	Low threshold (per minute) E_Ports	Low threshold (per minute) Storage FOP_Ports	Low threshold (per minute) Host FOP_Ports	Default
Invalid transmitted words (ITW)	25	25	25	1000
Invalid cyclic redundancy check error (CRC)	5	5	5	1000

Port fencing configuration using the portFencing command

The **portFencing** command enables and configures the port fencing feature; it does not set the thresholds for port fencing. You must configure port thresholds with the **portThconfig** command before you can enable port fencing.

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

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.

NOTE
Port fencing configuration on the VE_Port is supported on the FR4-18i router blade and the Brocade 7500 extension switch only. It is not supported on the Brocade 7800 extension switch or the DCX extension blade.

See "Port class guidelines and default settings" on page 59 for more information about the Port class areas and under what circumstances port fencing is recommended.

1. Connect to the switch and log in as admin.
2. Enter the **portFencing** command to display the list of operands.

   The **portFencing** menu displays.

```
switch:admin > portfencing

portfencing --show

portfencing --enable port_type_list|all
-area area_list|-area all

portfencing --disable port_type_list|all
-area area_list|-area all

portfencing --help
```

Enabling port fencing

1. Connect to the switch and log in as admin.
2. Configure port thresholds. Information about how to configure port thresholds is detailed in Chapter 7, "Port Monitoring".
3. Enter the **portFencing** –**enable** command:

```
portFencing –enable port_type_list|all -area area_list|-area all
```

Disabling port fencing

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

```
portFencing –disable port_type_list|all -area area_list|-area all
```

Port fencing configuration using DCFM

The Data Center Fabric Manager (DCFM) 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 DCFM 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 DCFM

You can add, edit, view, or remove thresholds on the following area types using DCFM. You can then assign the thresholds to available objects in the DCFM 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 (M-EOS only)
- Link Reset (Fabric OS only)
- Protocol Errors (M-EOS and Fabric OS)
- Security (M-EOS)
- State Changes (Fabric OS only)

Refer to Chapter 5, “Device Configuration,” of the *Data Center Fabric Manager User Manual* for detailed instructions on how to add, edit, view, and remove thresholds.

Recommended port configuration settings

Table 21 lists the recommended settings for physical port, E_Port, FOP_Port, and FCU_Port for both the host device and the storage device.

TABLE 21 Recommended configuration for the Port class

											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**	**Changed**	**Below**	**Above**	**In-between**	**Notes**
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						
	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	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	40	0		X		E,S,F			pf
	Invalid CRCs		X	Errors	Minute	0	20	0		X		E,S,F			pf
	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		Changes	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						

TABLE 21 Recommended configuration for the Port class (Continued)

													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**	**Changed**	**Below**	**Above**	**In-between**	**Notes**
E_Port continued	C3 Discard	X		Errors	Minute	0	5	0		X			E		
	Trunk Util	X		Percentage	Minute	0	75	0		X			E	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		pf
	Invalid CRCs	X		Errors	Minute	0	1000	100		X			E,S,F		pf
	RX Performance		X	Percentage	Minute	0	85	0		X			E	E	
	TX Performance		X	Percentage	Minute	0	85	0		X			E	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		pf
	Invalid CRCs		X	Errors	Minute	0	40	0		X			E,S,F		pf
	RX Performance		X	Percentage	Minute	0	85	0		X			E	E	
	TX Performance		X	Percentage	Minute	0	85	0		X			E	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						

7 Recommended port configuration settings

Chapter

System Monitoring 8

In this chapter

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 22 lists and describes the areas in the *Environment* class.

TABLE 22 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

Table 23 provides default Environment class settings for all switches. Check the appropriate hardware reference manual for differences in actual environmental requirements.

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 23 Environment class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Temperature	Monitors switch temperature in Celsius	Unit: degrees C Time Base: none *Brocade 200E* Low: 0 High: 60 Buffer: 10	Changed: 0 Below: 3 Above: 3 In-Between: 3 (Same setting for all devices)	Informative Out-of-range Out-of-range In_range (Same setting for all devices except Brocade DCX-4S)
		Brocade 300 Low: 0 High: 50 Buffer: 10		
		Brocade 4100 Low:0 High: 60 Buffer: 10		
		Brocade 4900 Low: 0 High: 47 Buffer: 10		
		Brocade 5000 Low:0 High: 60 Buffer: 10		
		Brocade 5100 Low: 0 High: 63 Buffer: 10		
		Brocade 5300 Low: 0 High: 48 Buffer: 10		

TABLE 23 Environment class default settings (Continued)

Area	Description	Default threshold settings	Default alarm settings	Threshold state
		Brocade 7500 Low: 0 High: 63 Buffer: 10		
		Brocade 7600 Low: 0 High: 63 Buffer: 10		
		Brocade 7800 Low: 0 High: 58 Buffer: 10		
		Brocade 8000 Low: 0 High: 73 Buffer: 10		
		Brocade 48000 Low: 0 High: 60 Buffer: 10		
		Brocade DCX Low: 0 High: 70 Buffer: 10		
		Brocade DCX-4S Low: 0 High: 75 Buffer: 10		Informative Out-of-range In-range Informative

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

Table 24 describes the Product Name Resource class area. Configure the Resource class using the **sysMonitor** command.

TABLE 24 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 setting guidelines

Use the Resource Class default settings listed in Table 25.

Resource class default settings

Table 25 provides default settings for areas in the Resource class.

TABLE 25 Resource class default settings

Area	Description	Default threshold settings	Default alarm settings	Threshold state
Flash	Monitors the percentage of compact flash used	Unit: Percentage (%) Time base: none Low: 0 High: 90 Buffer: 0	Changed: 0 Below: 3 Above: 3 In-Between: 1	Informative Informative Out_of_range In_range

System monitoring using the sysMonitor command

Use the **sysMonitor** command to configure thresholds for Fabric Watch event monitoring for temperature and system resources on the switch. For detailed information about the **sysMonitor** command, refer to the *Fabric OS Command Reference Manual*.

The following operations are supported by this 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 this command, you must have chassis-level permission in a virtual fabric (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.

Canceling sysMonitor command configurations

To cancel unsaved threshold or alarms configurations, enter the **cancel** command.

```
sysmonitor –cancel class -area area [-thresh_level def | custom] [-action_level
def | cust]
```

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. See "Environment monitoring setting guidelines" on page 82 for more information.

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
Class: ENV
CPU Usage:
  Area: TEMP
  ThLevel: Def
  ActLevel: Def
  High:
    Custom:
      TimeBase: None
      Value: 65
      Trigger: Above Action: Raslog, SNMP
      Trigger: Below Action: Raslog, SNMP
    Default:
      TimeBase: None
      Value: 65
      Trigger: Above Action: Raslog, SNMP
      Trigger: Below Action: Raslog, SNMP
      Low:
    Custom:
      TimeBase: None
      Value: 0
      Trigger: Above Action: None
      Trigger: Below Action: Raslog, SNMP
    Default:
      TimeBase: None
      Value: 0
      Trigger: AboveAction: None
      Trigger: Below Action: Raslog, SNMP
  Buffer:
    Custom:
      Value: 10
    Default:
      Value: 10
```

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
```

CPU and memory

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

When used to configure CPU monitoring, specify a value in the 1-100 range. When CPU usage exceeds the limit a Fabric Watch alert is triggered. The default CPU limit is 50% for the Brocade 48000 and 75% for all other platforms.

When used to configure memory monitoring the limit value must be greater than the low limit and smaller than the high 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 in the range between the low limit and 90%. The default is 70% on the Brocade 48000 and 60% on all other platforms.

The following operands are valid only with --config mem. They provide two additional limits above and below the middle usage limit.

- 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%. When memory usage exceeds this limit, Fabric Watch generates a CRITICAL RASlog message. The default is 90% for the Brocade 48000 and 80% for all other platforms.
- 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 an INFO RASlog message. The default for all platforms is 50%.

Configuring the system memory usage monitoring threshold

1. 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
```

2. Apply the changes:

```
switch:admin > sysmonitor --apply mem -action_level cust
```

Displaying the current CPU usage threshold

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

```
switch:admin > sysmonitor --show cpu
    CPU Usage : 5%
    CPU Usage Limit :75%
    Number of Retries :3
    Polling Interval :120 seconds
```

Configuring the system CPU usage monitoring threshold

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

```
switch:admin > sysmonitor --config cpu -poll 20 -retry 4 -limit 70 -action snmp
```

2. Apply the changes:

```
switch:admin > sysmonitor --apply cpu -action_level cust
```

Recommended environment and resource monitoring settings

Table 26 lists the recommended settings for Environment and Resource classes.

TABLE 26 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**	**Changed**	**Below**	**Above**	**In-between**	**Notes**
Environment	Temperature	X		C	None	0	Depends on switch type	10	X			E,S	E,S	E,S	
Resource	Flash	X		Percentage	None	0	90	0	X			E,S	E,S	E	

Switch monitoring

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

Switch status policy planning

Table 27 lists the monitors in a switch and identifies the factors that affect their health. Note that not all switches use the listed monitors.

TABLE 27 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. When intelligent blades like the FR4-18i are in the 48000 chassis, the 48000 operates in high power mode, which means that four power supplies are required for redundancy. In high power mode, Fabric Watch assumes a policy setting of 2,1, meaning that the switch goes to a Down state if two power supplies fail, and goes to a Marginal state when one power supply fails. Fabric Watch automatically changes the policy setting to 2,1 when an FR-18i, FC4-16IP, or FA4-18 blade is detected. If the blade is removed, the policy remains set to 2,1. 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, as with the blades listed above. Use the **switchstatuspolicyset** command if you need to manually change the policy setting.
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).
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.

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.

   The following example shows a switch status policy for Temperature:

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

   The following example shows a switch status policy for Fans:

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

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

Viewing your switch status policy

After you have defined and configured your switch status policy, view it with the **switchStatusPolicyShow** command.

The policy you defined here determines the output in the Switch Status Policy Report.

See Chapter 9, “Fabric Watch Reports,” 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, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 5100, and 5300 switches
- 7500, 7500E, 7600, and 7600E extension switches
- Brocade DCX and DXC-4S Data Center Backbone
- Brocade Encryption Switch

FRU class areas

Table 28 lists Product Name areas in the FRU class and describes each area. Possible states for all FRU-class areas are *absent*, *faulty*, *inserted*, *on*, *off*, *ready*, and *up*. Configure the FRU class using the **fwFruCfg** command

TABLE 28 FRU class areas

Area	Indicates
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.

Configuring FRUs

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

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

   The **fwFruCfg** command displays your current FRU configuration. 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.

```
swd123:admin> fwfrucfg

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

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

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

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 29 lists the recommended settings for field-replaceable units (FRUs).

TABLE 29 Recommended FRU settings

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

Chapter

9

Fabric Watch Reports

In this chapter

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 in this chapter use the command line interface.

Table 30 lists the Fabric OS commands to view reports.

TABLE 30 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 fwPortDetailShow --s h fwPortDetailShow --s m fwPortDetailShow --s f fwPortDetailShow --s o	Port detail report To view only health ports To view only marginal ports To view only faulty ports 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 in this chapter 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
2/8                  U       0           0           0          100
2/9                  U       0           0           0          100
2/10                 T     100           0           0            0
2/11                 T     100           0           0            0
```

```
2/12                LB     100          0          0          0
2/13                LB     100          0          0          0
2/14                 U       0          0          0        100
2/15                LB     100          0          0          0
3/0                  T     100          0          0          0
3/1                  U       0          0          0        100
3/2                  U       0          0          0        100
3/3                  U       0          0          0        100
3/4                  U       0          0          0        100
3/5                  U       0          0          0        100
3/6                  U       0          0          0        100
3/7                  U       0          0          0        100
3/8                  U       0          0          0        100
3/9                  U       0          0          0        100
3/10                VE     100          0          0          0
.
.
.
```

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. The following is an example of a switch health 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

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

```
cp0 login: admin
Password:
Sat 240        :admin> switchstatusshow
Switch Health Report                        Report time: 08/21/2006 05:23:22 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
WWN servers monitor     HEALTHY
Standby CP monitor      HEALTHY
```

```
Standby CP monitor      HEALTHY
Core blade monitor      HEALTHY
Blades monitor          HEALTHY
Flash monitor           HEALTHY
Marginal ports monitor  HEALTHY
Faulty ports monitor    HEALTHY
Missing SFPs monitor    HEALTHY


All ports are healthy
```

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

Switch Status Policy report

The Switch Status Policy report displays the current policy parameter.

The following example of the **switchStatusPolicyShow** command output is for enterprise-class platforms such as the Brocade 48000 director or the DCX Backbone. For modular switches, the switch status policy report also contains information on the WWN, Blade, and CP.

For standalone switches such as the Brocade 4100 and 5000, the WWN, Blade, CP, and core blade information is not displayed.

Generating a Switch Status Policy report

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

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

Port Detail report

If the Switch Health report shows marginal throughput or decreased performance, use the Port Detail report to see statistics on each port. The Port Detail report is a Fabric Watch licensed product. 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.

   See Table 30 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   -  -   -  -   -  -   -  -   -  -   -  -   -
218     VE  HEALTHY   061:19   -  -   -  -   -  -   -  -   -  -   -  -   -
219     VE  HEALTHY   003:37   -  -   -  -   -  -   -  -   -  -   -  -   -
220     VE  HEALTHY   002:48   -  -   -  -   -  -   -  -   -  -   -  -   -
221     VE  HEALTHY   061:19   -  -   -  -   -  -   -  -   -  -   -  -   -
222     VE  HEALTHY   061:19   -  -   -  -   -  -   -  -   -  -   -  -   -
223     VE  HEALTHY   061:19   -  -   -  -   -  -   -  -   -  -   -  -   -
```

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.

Example:

```
“000  ----------------Not a member of current Admin Domain------------------”
```

Table 31 lists and describes each item in the Port Detail report.

TABLE 31 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.

Appendix

Fabric Watch Configuration Using Legacy Commands A

In this appendix

Port threshold configuration using the fwConfigure command

The **fwConfigure** command is being deprecated in Fabric OS v6.4.0. The **thConfig**, **portThConfig**, **sysMonitor**, and **fwFruCfg** commands provide functional equivalents for configuring Fabric Watch thresholds. You can configure classes and areas using the commands that were detailed in earlier chapters:

- Chapter 6, "Fabric, Security, SFP, and Performance Monitoring"

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

- Chapter 7, "Port Monitoring"

  The physical port and its subclass areas and actions are configured using the **portThConfig** command (recommended) or the **fwConfigure** command (which is being phased out).

- Chapter 8, "System Monitoring"

  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.

The Fabric Watch classes and areas are provided in Chapter 3, "Fabric Watch Threshold Components". The following restrictions apply:

- The Port class does not support VE _Ports and VEX_Ports, except for State Changes.
- The E_Port class has the same port limitations as the Port class except under the following condition: On a Brocade 48000 with a FR4-18i blade, or on the Brocade 7500, the E_Port class monitors the following additional ports and creates monitors for each of the logical ports:
  - FCR (includes EX_Ports)
  - FCIP (includes VE_Ports, VEX_Ports)
- SFP class: The SFP class does not monitor SFPs.

Setting port thresholds using the fwConfigure command

Use the **fwConfigure** command to display and modify threshold information for the Fabric Watch configuration. Switch elements monitored by Fabric Watch are divided into classes, which are further divided into areas. Each area can include multiple thresholds. In addition, the command can be used to disable or enable all thresholds associated with a given port. When executed without operands, this command runs interactively.

On switches running Fabric OS v6.1.0 or later, you can use this command to enable port fencing. This feature allows the operating system to disable a port that is operating outside the bounds of normal operation. When an erratically behaving port is fenced, the port is placed into the disabled state and is kept offline, thereby preventing the port from transmitting or receiving frames. Refer to the "Configuring port fencing using the fwConfigure command" on page 109 for information on how to enable port fencing.

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

1. Connect to the switch and log in as admin.
2. Enter the **fwConfigure** command to display the list of classes.

   The fwConfigure menu displays. The **Quit** menu item, which is the default, exits the **fwConfigure** menu.

   NOTE
   For switches with embedded ports or copper ports, the **fwConfigure** menu has an additional menu item for the FOP_Port and FCU_Port classes.

3. Enter the number from the list that corresponds to the class that you want to configure. For example, if you enter **5**, the menu corresponding to the E_Port class displays.

```
switch:admin> fwconfigure

1  : Environment class
2  : SFP class
3  : Port class
4  : Fabric class
5  : E-Port class
6  : F/FL Port (Optical) class
7  : Alpa Performance Monitor class (not supported)
8  : EE Performance Monitor class
9  : Filter Performance Monitor class
10 : Security class
11 : Resource class
12 : Quit
Select a class => : (1..12) [12] 5
```

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

4. Enter the number corresponding to the area that you want to configure, such as **7** for **RXPerformance**.

```
1  : Link loss
2  : Sync loss
3  : Signal loss (not supported)
4  : Protocol error
5  : Invalid words
6  : Invalid CRCS
7  : RXPerformance
8  : TXPerformance
9  : State Changes
10 : Link reset
11 : return to previous page
Select an area => : (1..10) [10] 7
```

Fabric Watch displays a list of monitored elements in this area. The following sample output shows the monitored elements in the RXPerformance area menu.

```
Index ThresholdName   Port      CurVal   Status
  LastEvent  LasteventTime     LastVal   LastState
==========================================================================
  216 eportRXPerf216    8/24  0 Percentage(%)/min  enabled
  inBetween    Tue Jun 2 14:21:01 2009 0 Percentage(%)/min Informative
  217 eportRXPerf217    8/25  0 Percentage(%)/min  enabled
  inBetween    Tue Jun 2 14:21:07 2009 0 Percentage(%)/min Informative
  218 eportRXPerf218    8/26  0 Percentage(%)/min  enabled
  inBetween    Tue Jun 2 14:21:07 2009 0 Percentage(%)/min Informative
  219 eportRXPerf219    8/27  0 Percentage(%)/min  enabled
  inBetween    Tue Jun 2 14:21:07 2009 0 Percentage(%)/min Informative
  220 eportRXPerf220    8/28  0 Percentage(%)/min  enabled
  inBetween    Tue Jun 2 14:21:07 2009 0 Percentage(%)/min Informative
  221 eportRXPerf221    8/29  0 Percentage(%)/min  enabled
  inBetween    Tue Jun 2 14:21:07 2009 0 Percentage(%)/min Informative
  222 eportRXPerf222    8/30  0 Percentage(%)/min  enabled
  inBetween    Tue Jun 2 14:21:07 2009 0 Percentage(%)/min Informative
  223 eportRXPerf223    8/31  0 Percentage(%)/min  enabled
  inBetween    Tue Jun 2 14:21:07 2009 0 Percentage(%)/min Informative
```

where:

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

See Chapter 3, “Fabric Watch Threshold Components,” for details about classes and areas.

Refreshing a threshold configuration

The area menu displays five options, which are described in the following sections.

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

Enter **1** at the Select choice => prompt.

The screen refreshes with the most recently updated monitoring information.

After the screen refreshes, the same five options appear.

Disabling a threshold configuration

To stop monitoring a selected option, use the **disable a threshold** option.

1. Enter **2** at the Select choice => prompt.

   The system generates output, which varies based on the class and area you selected.

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

   Fabric Watch redraws the element table with the selected element disabled. The second row of information about the selected element does not appear anymore, and the status of the element is set to **disabled** (see the system output).

```
Select threshold index => : (216..223) [216] 218
Index ThresholdName   Port      CurVal   Status
  LastEvent  LasteventTime     LastVal   LastState
=========================================================================
  216 eportRXPerf216    8/24  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:01 2005 0 Percentage(%)/min Informative
  217 eportRXPerf217    8/25  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  218 eportRXPerf218    8/26  0 Percentage(%)/min  disabled
  219 eportRXPerf219    8/27  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  220 eportRXPerf220    8/28  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  221 eportRXPerf221    8/29  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  222 eportRXPerf222    8/30  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  223 eportRXPerf223    8/31  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
```

Enabling a threshold

1. Enter **3** at the Select choice => prompt.

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

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

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

```
Select threshold index => : (216..223) [216] 218

Index ThresholdName   Port      CurVal   Status
  LastEvent  LasteventTime     LastVal   LastState
==========================================================================
  216 eportRXPerf216    8/24  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:01 2005 0 Percentage(%)/min Informative
  217 eportRXPerf217    8/25  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  218 eportRXPerf218    8/26  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  219 eportRXPerf219    8/27  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  220 eportRXPerf220    8/28  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  221 eportRXPerf221    8/29  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  222 eportRXPerf222    8/30  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
  223 eportRXPerf223    8/31  0 Percentage(%)/min  enabled
  inBetween    Fri Oct 21 14:21:07 2005 0 Percentage(%)/min Informative
```

Enabling and disabling all port thresholds

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

1. Use the following command to disable the port threshold.

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

2. To enable all the thresholds for a port, enter the following command at the prompt.

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

Changing the threshold boundary level

NOTE
The allowed advanced settings are displayed on a per-class basis. Although port fencing is displayed for other areas, such as RX Performance, for which port fencing is not supported, you will not be able to set or apply the changes on such areas.

1. Enter **4** at the Select choice => prompt.

   The system generates output, which varies based on the class and area you select. In the example shown here, the output is based on the E_Port class and RXPerformance area.

```
Index ThresholdName    BehaviorType    BehaviorInt
  216 eportRXPerf216   Triggered  1
  217 eportRXPerf217   Triggered  1
  218 eportRXPerf218   Triggered  1
  219 eportRXPerf219   Triggered  1
  220 eportRXPerf220   Triggered  1
  221 eportRXPerf221   Triggered  1
  222 eportRXPerf222   Triggered  1
  223 eportRXPerf223   Triggered  1

Threshold boundary level is setat : Default

     DefaultCustom
      Unit    Percentage(%)    Percentage(%)
 Time base  minuteminute
       Low       0     0
      High     100   100
   BufSize       0     0

Threshold alarmlevel is set at: Default

Errlog-1, SnmpTrap-2, PortLogLock-4
RapiTrap-8, EmailAlert-16, PortFencing-32

Valid alarm matrix is 63

     DefaultCustom
   Changed       0     0
     Below       0     0
     Above       0     0
 InBetween       0     0

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

where:

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

2. Refer to the following system output to customize the high threshold boundary for RXPerformance.

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

   NOTE
   Default threshold boundary settings are Fabric OS default settings; custom settings are user-defined.

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

   In the following system output, a value of 80% is chosen as the custom high value for RXPerformance. The default value is 100%.

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

Index ThresholdName    BehaviorType    BehaviorInt
  216 eportRXPerf216   Triggered  1
  217 eportRXPerf217   Triggered  1
  218 eportRXPerf218   Triggered  1
  219 eportRXPerf219   Triggered  1
  220 eportRXPerf220   Triggered  1
  221 eportRXPerf221   Triggered  1
  222 eportRXPerf222   Triggered  1
  223 eportRXPerf223   Triggered  1

Threshold boundary level is setat : Default

    DefaultCustom
      Unit    Percentage(%)    Percentage(%)
 Time base  minuteminute
       Low       0     0
      High     100    80
   BufSize       0     0.
```

3. Enter **3** at the Select choice => prompt to change the threshold boundary level, and then enter **2** at the **Enter boundary level type = >** prompt to specify that this is a custom value, as shown in the following system output.

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

Index ThresholdName    BehaviorType    BehaviorInt
  216 eportRXPerf216   Triggered  1
  217 eportRXPerf217   Triggered  1
  218 eportRXPerf218   Triggered  1
  219 eportRXPerf219   Triggered  1
  220 eportRXPerf220   Triggered  1
  221 eportRXPerf221   Triggered  1
  222 eportRXPerf222   Triggered  1
  223 eportRXPerf223   Triggered  1

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

4. Enter **9** at the Select choice => prompt to apply the threshold boundary changes.

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

5. Enter **16** at the Select choice => prompt to apply the changes.

Configuring port fencing using the fwConfigure command

The following is an example of selecting the Port class with Invalid CRCs. With the exception of step 1, the same steps are required to enable the E_Port or FOP_Port class, as well as each available area for the selected class (described in step 4).

1. Enter **fwalarmsfilterset 1** to enable Fabric Watch alarms.
2. Navigate to a specific class and area with the **fwConfigure** command.

```
switch:admin> fwconfigure

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

3. Enter the number from the list that corresponds to the class that you want to configure. Select **3** for Port class, **5** for E_Port class, or **6** for F/FL Port (Optical) class.

   For each class that you select, Fabric Watch provides a list of the areas of the class available for configuration.

4. Select an area (areas **1 - 2** and **4 - 6** are available for port fencing).

```
1  : Link loss (E-port)
2  : Sync loss (E-port)
3  : Signal loss (E-port)
4  : Protocol error (E-port)
5  : Invalid words (E-port)
6  : Invalid CRCS (E-port)
7  : RXPerformance(E-port)
8  : TXPerformance (E-port)
9  : State Changes (E/VE-port)
10 : Link reset (E-port)
11 : Utilization (VE-port)
12 : Packet loss (VE-port)
13 : C3TX_TO
14 : return to previous page
Select an area => : (1..2) (4..6) [10] 1
```

   In this example, if you enter **1**, the menu corresponding to the **Link loss** displays.

   See Chapter 3, “Fabric Watch Threshold Components,” for more details about classes and areas.

5. Select **advanced configuration** by entering **4** at the **Select an area = >** prompt.

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

6. Select **change above alarm** by entering **14** at the **Select choice** prompt.

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

7. Set the **alarm for Port Fencing** (32) by entering **32** at the **Enter above alarm matrix = >** prompt.

```
Errlog-1, SnmpTrap-2, PortLogLock-4
RapiTrap-8, EmailAlert-16, PortFencing-32

Valid alarm matrix is 63
Enter above alarm matrix => : (0..63) [0] 32
```

8. Verify that the alarm matrix displays the **Above Custom** as 32, and then change the Threshold alarm level to custom by entering **11**.

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

9. Select **custom** by entering **2** at the **Enter alarm level type = >** prompt.

10. Select **apply threshold alarm changes** by entering **16** at the **Select choice = >** prompt.

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

11. Change the number of errors per minute using the following substeps:

    a. From the advanced configuration section, select **change custom high** by entering **7** at the **Select choice = >** prompt.

    b. Type the number of errors per minute at the **Enter high threshold = >** prompt.

```
1  : change behavior type             11 : change threshold alarm level
2  : change behavior interval         12 : change changed alarm
3  : change threshold boundary level  13 : change below alarm
4  : change custom unit               14 : change above alarm
5  : change custom time base          15 : change inBetween alarm
6  : change custom low                16 : apply threshold alarm changes
7  : change custom high               17 : cancel threshold alarm changes
8  : change custom buffer             18 : return to previous page
9  : apply threshold boundary changes
10 : cancel threshold boundary changes
Select choice => : (1..18) [18] 7
Enter high threshold => : (0..999999999) [500] 100
```

12. Change the Threshold boundary level to **custom** by entering **3**, and then select **custom** by entering **2** at the **Enter boundary level type = >** prompt.

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

13. Select **apply threshold boundary changes** by entering **9** at the **Select choice = >** prompt.

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

14. **Enter** until you reach the switch command prompt.

Advanced options using the fwConfigure command

During your planning activities, you should determine which elements or monitors you want to configure, and in which class they reside.

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

The area menu displays five options.

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

Enter **4** at the Select choice => prompt, for a list of advanced configuration options.

Table 32 describes the customization options displayed at the end of the Advanced Configuration menu. With the exception of the last option, which exits advanced configuration mode, each option has a similar behavior. For each option, one or two lines will appear, prompting you to accept the new setting information, and, after the information has been provided, the entire screen will refresh to display the updated information.

TABLE 32 Advanced configuration options using the fwConfigure command

Option	Effect	Input information
change behavior type	Changes the behavior type of a single element to either Triggered or Continuous. The change is volatile because this option is not saved to flash memory. Every time the switch is rebooted, this option is reset.	The element index and the required behavior type
change behavior interval	Changes the behavior interval for a single element. The change is volatile because this option is not saved to flash memory. Every time the switch is rebooted, this option is reset. This value is effective *only* when the behavior type is set to Continuous.	The element index and the required behavior interval, in seconds
change threshold boundary level	Changes between the factory default and custom threshold information.	The required threshold column
change custom unit	Obsolete	Obsolete
change custom time base	Changes the time base for the area, but only affects the custom column.	The required time base
change custom low	Changes the low setting for the threshold, but only affects the custom column.	The required low threshold, in the units defined by the area
change custom high	Changes the high setting for the threshold, but only affects the custom column.	The required high threshold, in the units defined by the area
change custom buffer	Changes the buffer size for the threshold, but only affects the custom column.	The required buffer size, in the units defined by the area
apply threshold boundary changes	Confirms the changes made to the threshold information. This must be done to retain the changes made.	None
cancel threshold boundary changes	Returns the boundary information to the last confirmed state.	None
change threshold alarm level	Changes between the factory default and custom event settings for the area.	The required event setting column
change changed alarm	Changes the notification method for changed event occurrences for this method, but only affects the custom column.	The required notification methods
change above alarm	Changes the notification method for above event occurrences for this method, but only affects the custom column.	The required notification methods
change below alarm	Changes the notification method for below event occurrences for this method, but only affects the custom column.	The required notification methods

TABLE 32 Advanced configuration options using the fwConfigure command (Continued)

Option	Effect	Input information
change inBetween alarm	Changes the notification method for inBetween event occurrences for this method, but only affects the custom column.	The required notification methods
apply threshold alarm changes	Confirms the changes made to the event setting information. This must be done to retain the changes made.	None
cancel threshold alarm changes	Returns the event setting information to the last confirmed state.	None

Changing the numerical values of notification methods

The numerical value of the notification method is the sum of the alarm matrix values; for example, PortFencing-32, SnmpTrap-2, and Errlog-1 (32+2+1=35).

Table 33 shows the assigned numerical values for each notification method.

TABLE 33 Numerical values of notification methods

Notification method	Assigned value
Error log entry	1
SNMP trap	2
Rapi trap	4
Port log lock	8
E-mail notification	16
Port fencing	32

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

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

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

To assign the notification method a value, follow these steps:

1. From the area menu, select **4 (advanced configuration)** from the area menu.
2. Add the numbers beside each state that you want to include using the values in Table 33. Enter the total at the prompt.

```
1 : change behavior type           11 : change threshold alarm level
2 : change behavior interval       12 : change changed alarm
3 : change threshold boundary level13 : change belowalarm
4 : change custom unit             14 : change abovealarm
5 : change custom timebase         15 : change inBetween alarm
6 : change custom low              16 : apply threshold alarm changes
7 : change custom high             17 : cancel threshold alarm changes
8 : change custom buffer           18 : return to previous page
9 : apply threshold boundary changes
10: cancel threshold boundary changes
Select choice => : (1..18) [18]14

Errlog-1, SnmpTrap-2, PortLogLock-4
RapiTrap-8, EmailAlert-16 PortFencing - 31

Valid alarm matrix is 63
Enter above alarm matrix => : (0..63) [0] 35

Index ThresholdName    BehaviorType    BehaviorInt
  216 eportRXPerf216   Triggered  1
  217 eportRXPerf217   Triggered  1
  218 eportRXPerf218   Triggered  1
  219 eportRXPerf219   Triggered  1
  220 eportRXPerf220   Triggered  1
  221 eportRXPerf221   Triggered  1
  222 eportRXPerf222   Triggered  1
  223 eportRXPerf223   Triggered  1

Threshold boundary level is setat : Custom

     DefaultCustom
       Unit    Percentage(%)    Percentage(%)
 Time base  minuteminute
       Low       0     0
      High     100    80
   BufSize       0     0

Threshold alarmlevel is set at: Default

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

```
Valid alarm matrix is 31

     DefaultCustom
   Changed       0     0
     Below       0     0
     Above       0    19
 InBetween       0     0
```

3. Enter **1** at the Select choice => prompt to change the alarm behavior type.

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

Index ThresholdName    BehaviorType    BehaviorInt
  216 eportRXPerf216   Triggered  1
  217 eportRXPerf217   Triggered  1
  218 eportRXPerf218   Triggered  1
  219 eportRXPerf219   Triggered  1
  220 eportRXPerf220   Triggered  1
  221 eportRXPerf221   Triggered  1
  222 eportRXPerf222   Triggered  1
  223 eportRXPerf223   Triggered  1

Threshold boundary level is setat : Custom

     DefaultCustom
      Unit    Percentage(%)    Percentage(%)
 Time base  minuteminute
       Low       0     0
      High     100    80
   BufSize       0     0

Threshold alarmlevel is set at: Custom
.
.
.
```

4. Enter **16** at the Select choice => prompt to apply the threshold alarm level changes. Unless you apply the value, it does not take effect.

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

A Advanced options using the fwConfigure command

Index

A

B

C

D

E

F

I

L

M

N

P

R

S

T

V

W