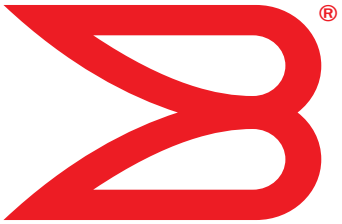
53-1002933-02
9 September 2013



Monitoring and Alerting Policy Suite

Administrator's Guide

Supporting Fabric OS v7.2.0a

BROCADE

Copyright © 2010-2013 Brocade Communications Systems, Inc. All Rights Reserved.

ADX, AnyIO, Brocade, Brocade Assurance, the B-wing symbol, DCX, Fabric OS, ICX, MLX, MyBrocade, OpenScript, VCS, VDX, and Vyatta are registered trademarks, and HyperEdge, The Effortless Network, and The On-Demand Data Center are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of their respective owners.

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

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
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
Monitoring and Alerting Policy Suite Administrator’s Guide	53-1002933-01	First release	July 2013
Monitoring and Alerting Policy Suite Administrator’s Guide	53-1002933-02	Updated to match FOS 7.2.0a	September 2013

Contents

Index

About This Document

In this chapter

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Fabric OS v7.2.0a, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Fabric OS:

- Fixed-port switches:
  - Brocade 300 switch
  - Brocade 5100 switch
  - Brocade 5300 switch
  - Brocade 5410 embedded switch
  - Brocade 5424 embedded switch
  - Brocade 5430 embedded switch
  - Brocade 5431 embedded switch
  - Brocade 5450 embedded switch
  - Brocade 5460 embedded switch
  - Brocade 5470 embedded switch
  - Brocade 5480 embedded switch
  - Brocade M6505 embedded switch
  - Brocade 6505 switch
  - Brocade 6510 switch
  - Brocade 6520 switch

- Brocade 6547 embedded switch
- Brocade 7800 extension switch
- Brocade VA-40FC
- Brocade Encryption Switch

- Brocade DCX Backbone family:
  - Brocade DCX
  - Brocade DCX-4S
- Brocade DCX 8510 Backbone family:
  - Brocade DCX 8510-4
  - Brocade DCX 8510-8

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used 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 command 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.

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are in bold.
--option, option	Command options are in bold.
-**argument, arg**	Arguments are in bold.
[ ]	Optional element.

variable	Variables are in italics.
...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are in plain font. For example, **--show** WWN
|	Boolean. Elements are exclusive. Example: **--show -mode** egress | ingress

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, refer to the *Brocade Glossary*.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Windows, Windows NT, Internet Explorer
Mozilla Corporation	Mozilla, Firefox
Netscape Communications Corporation	Netscape
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover
Oracle, Inc.	Sun, Solaris, Oracle, Java

Additional information

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

Brocade resources

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

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

http://www.brocade.com

Release notes are available on the My Brocade 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:

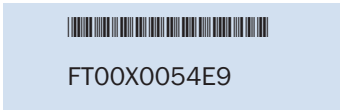
http://www.fibrechannel.org

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, 5100, 5300, 6505, M6505, 6510, 6520, 6547, 7800, 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 5410, 5424, 5430, 5431, 5450, 5460, 5470, 5480*—Serial number label attached to the module
- *Brocade 6510*—On the pull-out tab on the front of the switch
- *Brocade DCX* and *DCX 8510-8*—On the bottom right on the port side of the chassis
- *Brocade DCX-4S* and *DCX 8510-4*—On the bottom right on the port side of the chassis, directly above the cable management comb

3. World Wide Name (WWN)

    Use the **wwn** command to display the switch WWN.

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

    For the Brocade 5424 embedded switch: Provide the license ID. Use the **licenseIdShow** command to display the WWN.

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

Monitoring and Alerting Policy Suite Overview 1

In this chapter

MAPS overview

The Monitoring and Alerting Policy Suite (MAPS) is an optional storage area network (SAN) health monitor supported on all switches running Fabric OS 7.2.0 or later that allows you to enable each switch to constantly monitor itself for potential faults and automatically alerts you to problems before they become costly failures.

MAPS tracks a variety of SAN fabric metrics and events. Monitoring fabric-wide events, ports, and environmental parameters enables early fault detection and isolation as well as performance measurements.

MAPS provides a set of pre-defined monitoring policies that allow you to immediately use MAPS on activation. Refer to "Predefined policies" for more information on using these policies.

In addition, MAPS provides customizable monitoring thresholds. These allow you to configure specific groups of ports or other elements so that they share a common threshold value. You can configure MAPS to provide notifications before problems arise, for example, when network traffic through a port is approaching the bandwidth limit. MAPS lets you define how often to check each switch and fabric measure and specify notification thresholds. Whenever fabric measures exceed these thresholds, MAPS automatically provides notification using several methods, including e-mail messages, SNMP traps, and log entries. Refer to "MAPS Groups, Policies, Rules, and Actions" for more information on using these features.

The MAPS dashboard provides you with the ability to view in a quick glance what is happening on the switch, and helps administrators dig deeper to see details of exactly what is happening on the switch (for example, the kinds of errors, the error count, and so on.) Refer to "MAPS dashboard overview" for more information.

MAPS provides a seamless migration of all customized Fabric Watch thresholds to MAPS, thus allowing you to take advantage of the advanced capabilities of MAPS. MAPS provides additional advanced monitoring, such as monitoring for the same error counters across different time periods, or having more than two thresholds for any error counters. MAPS also provides support for you to monitor the statistics provided by the Flow Monitor feature of Flow Vision.
Refer to "Differences between Fabric Watch and MAPS configurations" and "Migrating from Fabric Watch to MAPS" for details.

MAPS license requirements

MAPS is an optionally licensed feature of Fabric OS. MAPS requires an active and valid Fabric Vision license. If you already have a license for Fabric Watch plus a license for Advanced Performance Monitoring, you will automatically get MAPS functionality without having to obtain an additional license.

MAPS interoperability with other features

MAPS interacts in different ways with different Fabric OS features, including Virtual Fabrics, Fabric Watch, High Availability, and Admin Domains.

MAPS and Virtual Fabrics

When using virtual fabrics, different logical switches in a chassis can have different MAPS configurations.

MAPS and Fabric Watch

MAPS cannot coexist with Fabric Watch. For information about migrating from Fabric Watch to MAPS, refer to "Migrating from Fabric Watch to MAPS" on page 3.

MAPS configuration files

The MAPS configuration is stored in two separate configuration files, one for the default MAPS configuration and one for the user-created MAPS configuration. Only one user configuration file can exist for each logical switch. A configuration upload or download affects only the user-created configuration files. You cannot upload or download the default MAPS configuration file. To remove the user-created MAPS configuration run **mapsConfig --purge**. For more information on this command, refer to the *Fabric OS Command Reference*.

MAPS and High Availability

MAPS configuration settings are maintained across a HA failover or HA reboot; however, MAPS will restart monitoring after a HA failover or reboot and the MAPS cached statistics are not retained.

MAPS and Admin Domains

MAPS is supported on switches that have Admin Domains. There can only be one MAPS configuration that is common to all the Admin Domains on the chassis. Users with Administrator privileges can modify the MAPS configuration from any Admin Domain.

ATTENTION
If MAPS is enabled, do not download configuration files that have Admin Domains defined.

MAPS upgrade and downgrade considerations

When downgrading from Fabric OS 7.2 to any previous version of the OS, the following MAPS-related behaviors should be expected:

- When an active CP is running Fabric OS 7.2 with MAPS disabled, and the standby device has an earlier version of the Fabric OS, High Availability will be synchronized, but MAPS will not be allowed to be enabled until the firmware on the standby device is upgraded. The **mapsConfig --enablemaps** command fails and an error message is displayed.
- When an active CP is running Fabric OS 7.2 and MAPS is enabled, but the standby device is running Fabric OS 7.1 or earlier, then High Availability will not be synchronized until the standby CP is upgraded to Fabric OS 7.2.
- On devices with a single CP, there is no change in behavior when downgrading to an earlier version of the Fabric OS.
- When a configuration download occurs, the MAPS configuration is downloaded onto a switch only if MAPS is enabled on that local switch.

Migrating from Fabric Watch to MAPS

To use MAPS, you must migrate from Fabric Watch to MAPS. On a switch running Fabric OS 7.2.0 or later, or when you upgrade your existing switch to Fabric OS 7.2.0, Fabric Watch is enabled by default. On an upgraded switch, Fabric Watch continues to monitor as in Fabric OS 7.1.0 until MAPS is activated.

When you migrate from Fabric Watch to MAPS, the Fabric Watch configuration can be converted to a MAPS-compatible configuration so you do not need to reconfigure all of the thresholds and rules. If you do not make the conversion as part of the migration, you will need to configure the rules manually.

Activating MAPS is a chassis-specific process, and you can activate only one chassis at a time. On a given chassis there can be multiple logical switches. Activating MAPS will enable it for all logical switches in the chassis. Each logical switch can have its own MAPS configuration.

To migrate from Fabric Watch and activate MAPS, run the following commands:

mapsconfig --enablemaps

followed by

mapsconfig --fwconvert -enablepolicy *policyname*

Upon successful completion of this command, the following happens:

- Fabric Watch configurations are converted to MAPS policies. Refer to "Fabric Watch legacy policies" on page 23 for additional information.
  To not convert the Fabric Watch configurations when you activate MAPS, do not include **--fwconvert** in the command.
- Fabric Watch monitoring and commands are disabled.
- MAPS commands are enabled.
- The MAPS policy that is specified in the **-enablepolicy** *policy* parameter is enabled.

CAUTION

MAPS activation is a non-reversible process. Downgrading to Fabric OS 7.1 will enable Fabric Watch with its last configured settings. When you upgrade back to Fabric OS 7.2, Fabric Watch will continue to be enabled.

Differences between Fabric Watch and MAPS configurations

The MAPS monitoring and alerting configurations are not as complex as those available in Fabric Watch; consequently MAPS does not have some functionality that was available in Fabric Watch.

Table 1 shows differences between Fabric Watch and MAPS configurations.

TABLE 1 Differences between Fabric Watch and MAPS configurations

Configuration	Fabric Watch behavior	MAPS behavior
End-to-End monitoring (Performance Monitor class)	Supported.	Supported through flows. Refer to "Monitoring end-to-end performance" on page 37 for details.
Frame monitoring (Performance Monitor class)	Supported.	Supported through flows. Refer to "Monitoring frames for a specified set of criteria" on page 37 for details.
RX, TX monitoring	Occurs at the individual physical port level.	Occurs at the trunk or port level as applicable.
Pause/Continue behavior	Occurs at the element or counter level. For example, monitoring can be paused for CRC on one port and for ITW on another port.	Occurs at the element level. Monitoring can be paused on a specific port, but not for a specific counter on that port.
CPU/Memory polling interval	Can configure the polling interval as well as the repeat count.	This configuration can be migrated from Fabric Watch, but cannot be changed.
E-mail notification configuration	Different e-mail addresses can be configured for different classes.	E-mail configuration supported globally.
Temperature sensor monitoring	Can monitor temperature values.	Can monitor only the states of the sensors (In_Range or Out_of_range).

MAPS and Flow Vision

MAPS can work with information generated by the Brocade Flow Vision application. For more information, refer to "Flow Vision integration with the MAPS dashboard" on page 48, and the *Fabric OS Flow Vision Administrator's Guide*.

MAPS supports only the following statistics generated by Flow Vision flow monitors.

- Frame statistics:
  - Number of frames transmitted from the flow source
  - Number of frames received by the flow destination
  - Number of megabytes (MB) transmitted per second by the flow source
  - Number of megabytes (MB) received per second by the flow destination
- SCSI statistics:
  - Number of SCSI I/O read command frames recorded for the flow
  - Number of SCSI I/O write command frames recorded for the flow
  - Number of SCSI I/O bytes read as recorded for the flow
  - Number of SCSI I/O bytes written as recorded for the flow

Chapter

2

Enabling and Configuring MAPS

In this chapter

Enabling MAPS

MAPS is not enabled by default. To enable MAPS, enter the following command:

mapsConfig --enableMaps -policy *policyname*

You must supply a named policy to enable MAPS.

Once you have converted the Fabric Watch rules for use in MAPS (this must be done first), you can enable and configure MAPS. Refer to "MAPS configuration quick start" on page 7 and "Migrating from Fabric Watch to MAPS" on page 3 for more information on making the migration and getting started with MAPS.

MAPS configuration quick start

You can quickly start monitoring your switch using one of the predefined policies. Alternatively, if you are already using Fabric Watch and would like MAPS to use the same thresholds, convert the Fabric Watch policies into MAPS policies and then enable MAPS using the policy named "fw_active_policy". This provides the same monitoring functionality as Fabric Watch. Refer to "Fabric Watch legacy policies" on page 23 for more information about Fabric Watch converted policies.

You can monitor your switch for a while using the default policy, then fine-tune the policy as necessary to fit your environment. When you are satisfied with the configuration settings, you activate the actions you want to happen when thresholds are crossed.

To monitor a switch in this manner, complete the following steps.

1. Enable MAPS using **mapsConfig --enablemaps**.
2. Migrate from Fabric Watch using the default policy **mapsConfig --fwconvert -enablepolicy**. Refer to "MAPS and Fabric Watch" on page 2 for more details.

   Unless you specify otherwise, as part of the migration, Fabric Watch configurations are not converted to MAPS policies, Fabric Watch commands are disabled, and MAPS commands are enabled. The default active policy is named dflt_conservative_policy.

3. Set global actions on the switch to none using use **mapsConfig --actions none**.

   Setting the global actions to "none" allows you to test the configured thresholds before enabling the actions. Refer to "MAPS actions" on page 27 for more details.

4. Monitor the switch using **mapsDb --show** or **mapsDb --show all**.

   Refer to "Viewing the MAPS dashboard" on page 41 more details.

5. Fine-tune the rules used by the policy as necessary.

   Refer to "Modifying a policy" on page 25 more details.

6. Set global actions on the switch to the allowed actions by using **mapsConfig --actions** and specifying all of the actions that you want to allow on the switch.

   Refer to "Enabling or disabling actions at a global level" on page 28 more details.

The following example enables MAPS, loads the policy named "dflt_aggressive_policy", sets the actions to none, and then sets approved actions.

```
switch:admin> mapsconfig --enablemaps
switch:admin> mapsconfig --fwconvert -policy dflt_aggressive_policy

WARNING:
This command enables MAPS and replaces all Fabric Watch configurations and
monitoring. Once MAPS is enabled, the Fabric Watch configuration can't be
converted to MAPS.
If you wish to convert your Fabric Watch configuration into MAPS policies, select
NO to this prompt and first issue the "mapsconfig --fwconvert" command. Once the
Fabric Watch configuration is concerted into MAPS policies, you may reissue the
"mapsconfig --enablemaps" command to continue this process.  If you do not use
Fabric Watch or need the configuration, then select YES to enable MAPS now.
Do you want to continue? (yes, y, no, n): [no] yes
...
MAPS is enabled.
switch:admin> mapsconfig --actions none
switch:admin> mapsconfig --actions raslog,fence,snmp,email,sw_marginal
```

MAPS configuration tasks

Table 2 lists the MAPS configuration tasks and the commands you use for these tasks.

TABLE 2 MAPS configuration tasks

Configuration task	Command
Enabling MAPS	mapsconfig --enablemaps
Migrating from Fabric Watch to MAPS (Converting Fabric Watch policies to MAPS policies)	mapsconfig --fwconvert
Viewing group information	logicalgroup --show
Modifying a policy	mapspolicy
Creating a policy	mapspolicy --create
Enabling a policy	mapspolicy --enable
Modifying a default policy	mapspolicy --clone
Adding a rule to a policy	mapspolicy --addrule

TABLE 2 MAPS configuration tasks (Continued)

Configuration task	Command
Deleting a rule from a policy	**mapspolicy --delrule**
Creating a rule	**mapsrule --create**
Modifying a rule	**mapsrule --config**
Enabling or disabling actions at a global level	**mapsconfig --actions**
Sending alerts using e-mail	**mapsconfig --emailcfg**
Viewing the MAPS dashboard	**mapsdb --show**
Viewing historical data	**mapsdb --show history**

Refer to the *Fabric OS Command Reference* for additional information on the MAPS-related commands **logicalGroup**, **mapsConfig**, **mapsPolicy**, **mapsRule**, **mapsDb**, and **mapsSam**.

Monitoring a new port using existing rules

If a new element, such as a host, target, or small form-factor pluggable (SFP) transceiver is added to the fabric, you can monitor the element using existing rules for similar elements by using **logicalGroup --addmember** *group* **-member** *member1,member2, ...*. The element you want to add must be the same type as those already in the group (port, circuit, or SFP transceiver).

The added element is automatically monitored using the existing rules that have been set up for the group as long as the rules are in the active policy. You do not need to re-enable the active policy.

The following example adds the element members 31 and 41 to the existing group “critical_ports”:

```
switch:admin> logicalgroup --addmember critical_ports -members "31,41"
```

Monitoring across different time windows

You can create rules across multiple time bases if, for example, you want to monitor for both severe conditions and non-critical but persistent conditions.

In the following example, two rules are created:

- If the change in the CRC counter in the last minute is greater than 5, trigger an e-mail alert and SNMP trap.
- If the change in the CRC counter in the last day is greater than 20, trigger a RASLog message and e-mail alert.

The first rule monitors for the severe condition. It monitors sudden spikes in the CRC error counter over a period of one minute.

The second rule monitors for slow occurrences of CRC errors that could accumulate to a bigger number over the period of a day.

Both of these cases could indicate potential issues in the fabric. Configuring rules to monitor these conditions allows you to correct issues before they become critical.

```
switch:admin> mapsrule --create crc_critical -monitor crc -group ALL_PORTS
-timebase min -op g -value 5 -action email,snmp
switch:admin> mapsrule --show crc_critical
```

```
Rule Data:
----------
RuleName: crc_critical
Condition: ALL_PORTS(crc/min>5)
Actions: email,snmp
Policies Associated: none

switch:admin> mapsrule --create crc_persistent -monitor crc -group ALL_PORTS
-timebase day -op g -value 20 -action raslog,email
switch:admin> mapsrule --show crc_persistent
Rule Data:
----------
RuleName: crc_persistent
Condition: ALL_PORTS(crc/day>20)
Actions: raslog,email
Policies Associated: none
```

Resetting MAPS configuration upload and download to Brocade defaults

To reset MAPS to the Brocade defaults, use **mapsPolicy --enable** *default policy*. Default policies are dflt_conservative_policy, dflt_aggressive_policy, and dflt_moderate_policy. For more information, refer to "Predefined policies" on page 22.

Chapter

3

MAPS Elements and Categories

In this chapter

MAPS structural elements

MAPS has the following structural elements: categories, groups, rules, and policies. Table 3 provides a brief description of each structural element.

TABLE 3 MAPS structural elements

Element	Description
Action	The activity performed by MAPS if a condition defined in a rule evaluates to true. For more information, refer to "MAPS actions" on page 27.
Category	A grouping of similar elements that can be monitored (for example, "Security Violations". For more information, refer to "MAPS monitoring categories" on page 11.
Condition	A true or false trigger created by the combination of a time base and a threshold value. For more information, refer to "MAPS conditions" on page 26.
Element	A value (measure or statistic) that can be monitored. This includes switch conditions, data traffic levels, error messages, and other values. For a complete list of elements, refer to the *Fabric OS Administrator's Guide*.
Group	A collection of similar objects that you can monitor as a single entity. For example, a collection of ports can be assembled as a group. For more information, refer to "MAPS groups overview" on page 19.
Rule	A direction associating a condition with one or more actions that must occur when the specified condition is evaluated to be true. For more information, refer to "MAPS rules overview" on page 26.
Policy	A set of rules defining thresholds for triggering actions MAPS is to take when that threshold is triggered. When a policy is enabled, all of the rules in the policy are in effect. For more information, refer to "MAPS policies overview" on page 22.

MAPS monitoring categories

When you create rules, you specify an element to be monitored. MAPS provides the following categories you can monitor:

- Switch Policy Status
- Port Health
- FRU Health

- Security Violations
- Fabric State Changes
- Switch Resource
- Traffic Performance
- FCIP Health

The MAPS dashboard also displays the status of these categories. Refer to "MAPS dashboard overview" on page 39 for information on using the MAPS dashboard.

Switch Policy Status

The Switch Policy Status category enables you monitor the health of the switch by defining 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 critical (down) state. Table 4 lists the monitored parameters in this category and identifies the factors that affect their health. You should be aware that not all switches support the listed monitors.

TABLE 4 Switch Policy Status category parameters

Monitored parameter	Description
Power Supplies (BAD_PWR)	Power supply thresholds detect absent or failed power supplies, and power supplies that are not in the correct slot for redundancy.
Temperatures (BAD_TEMP)	Temperature thresholds, faulty temperature sensors.
Fans (BAD_FAN)	Fan thresholds, faulty fans.
Flash (FLASH_USAGE)	Flash thresholds.
Marginal Ports[1] (MARG_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[1] (FAULTY_PORTS)	Hardware-related port faults.
Missing SFPs[1] (MISSING_SFP)	Ports that are missing SFP media.
Error Ports[1] (ERR_PORTS)	Ports with errors.
WWN (WWN_DOWN)	Faulty WWN card (applies to modular switches).
Core Blade (DOWN_CORE)	Faulty core blades (applies to modular switches).
Faulty blades (FAULTY_BLADE)	Faulty blades (applies to modular switches).
High Availability (HA_SYNC)	Switch does not have a redundant CP (Applies to modular switches only.)

1. Marginal ports, faulty ports, error ports, and missing SFP transceivers are calculated as a percentage of the physical ports (excluding FCoE and VE_Ports).

Port Health

The Port Health category 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. Configurable ports include physical ports, E_Ports, optical F_Ports (FOP_Ports), copper F_Ports (FCU_Ports), and Virtual E_Ports (VE_Ports).

The Port Health category also monitors the physical aspects of a small form-factor pluggable (SFP) transceiver, such as voltage, current, receive power (RXP), transmit power (TXP), and state changes in physical ports, E_Ports, FOP_Ports, and FCU_Ports. Table 5 lists the monitored parameters in this category and provides a brief description for each one. In the Monitored parameter column, the value in parentheses is the value you can specify for the **mapsRule -monitor** parameter.

TABLE 5 Port Health category parameters

Monitored parameter	Description
Cyclic redundancy check (CRC)	The number of times an invalid cyclic redundancy check error occurs on a port or a frame that computes to an invalid CRC. Invalid CRCs can represent noise on the network. Such frames are recoverable by retransmission. Invalid CRCs can indicate a potential hardware problem.
Invalid transmission words (ITW)	The number of times an invalid transmission word error occurs on a port. A word did not transmit successfully, resulting in encoding errors. Invalid word messages usually indicate a hardware problem.
Sync loss (LOSS_SYNC)	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 transceiver or cable.
Link failure (LF)	The number of times a link failure occurs on a port or sends or receives the Not Operational Primitive Sequence (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 (LOSS_SIGNAL)	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.
Protocol errors (PE)	The number of times a protocol error occurs on a port. Occasionally, protocol errors occur due to software glitches. Persistent errors occur due to hardware problems.
Link reset (LR)	The ports on which the number of link resets exceed the specified threshold value.
Class 3 time outs (C3TXTO)	The number of Class 3 discards frames because of time outs.
State changes (STATE_CHG)	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
SFP current (CURRENT)	The amperage supplied to the SFP transceiver. Current area events indicate hardware failures.
SFP receive power (RXP)	The power of the incoming laser in microwatts (µw). This is used to help determine if the SFP transceiver is in good working condition. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.
SFP transmit power (TXP)	The power of the outgoing laser in microwatts (µw). This is used to help determine if the SFP transceiver is in good working condition. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.
SFP voltage (VOLTAGE)	The voltage supplied to the SFP transceiver. If this value exceeds the threshold, the SFP transceiver is deteriorating.
SFP temperature (SFP_TEMP)	The temperature of the SFP transceiver in degrees Celsius. A high temperature indicates that the SFP transceiver may be in danger of damage.
SFP power on hours (PWR_HRS)	The number of hours the SFP transceiver is powered on.

FRU Health

The FRU Health category enables you to define rules for field-replaceable units (FRUs), including small form-factor pluggable (SFP) transceivers, power supplies, and flash memory. Table 6 lists the monitored parameters in this category and provides a brief description for each one. Possible states for all FRU measures are faulty, inserted, on, off, ready, and up.

MAPS monitors FRUs (except for SFP FRUs) in only in the default switch so you will not get FRU-related alerts for other switches, nor will the FRU category in the MAPS dashboard be updated for FRU alerts on non-default switches.

TABLE 6 FRU Health category parameters

Monitored parameter	Description
Power Supplies (PS_STATE)	State of a power supply has changed.
Fans (FAN_STATE)	State of a fan has changed.
Blades (BLADE_STATE)	State of a slot has changed.
SFPs (SFP_STATE)	State of the SFP transceiver has changed.
WWN (WWN_STATE)	State of a WWN card has changed.

Security Violations

The Security Violations category monitors different security violations on the switch and takes action based on the configured thresholds and their actions. Table 7 lists the monitored parameters in this category and provides a brief description for each one.

TABLE 7 Security Violations category parameters

Monitored parameter	Description
DCC violations (SEC_DCC)	An unauthorized device attempts to log in to a secure fabric.
HTTP violations (SEC_HTTP)	A browser access request reaches a secure switch from an unauthorized IP address.
Illegal command (SEC_CMD)	Commands permitted only to the primary Fibre Channel Switch (FCS) are executed on another switch.
Incompatible security DB (SEC_IDB)	Secure switches with different version stamps have been detected.
Login violations (SEC_LV)	Login violations which occur when a secure fabric detects a login failure.
Invalid Certifications (SEC_CERT)	Certificates are not valid.
No-FCS (SEC_FCS)	The switch has lost contact with the primary FCS.
SCC violations (SEC_SCC)	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 (SEC_AUTH_FAIL)	SLAP failures which occur when packets try to pass from a non-secure switch to a secure fabric.
Telnet violations (SEC_TELNET)	Telnet violations which occur when a Telnet connection request reaches a secure switch from an unauthorized IP address.
TS out of sync (SEC_TS)	Time Server (TS) violations, which occur when an out-of-synchronization error has been detected.

Fabric State Changes

The Fabric State Changes category 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. Table 8 lists the monitored parameters in this category and provides a brief description for each one.

TABLE 8 Fabric State Changes category parameters

Monitored parameter	Description
Domain ID changes (DID_CHG)	Monitors forced domain ID changes. Forced domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch must assign another domain ID to a switch.
Fabric logins (FLOGI)	Activates when ports and devices initialize with the fabric.
Fabric reconfigurations (FAB_CFG)	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 (EPORT_DOWN)	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 transceiver (where there are SFP transceiver failures or transient errors).
Segmentation changes (FAB_SEG)	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 (ZONE_CHG)	Tracks the number of zone changes. Because zoning is a security provision, frequent zone changes may indicate a security breach or weakness. Zone change messages occur whenever there is a change in zone configurations.

Switch Resource

System resource monitoring enables you to monitor your system's temperature, flash usage, memory usage, and CPU usage.

You can use Switch Resource monitors to perform the following tasks:

- Configure thresholds for MAPS 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 MAPS alerts. You can set up the system monitor to poll at certain intervals and specify the number of retries required before MAPS takes action.

Table 9 lists the monitored parameters in this category and provides a brief description for each one.

TABLE 9 Switch Resource category parameters

Monitored parameter	Description
Temperature (TEMP)	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.
Flash (FLASH_USAGE)	Monitors the compact flash space available by calculating the percentage of flash space consumed and comparing it with the configured high threshold value.
CPU usage (CPU)	Monitors the percentage of CPU available by calculating the percentage of CPU consumed and comparing it with the configured threshold value.
Memory (MEMORY_USAGE)	Monitors the available memory by calculating the percentage of memory consumed and comparing it with the configured threshold value.

Traffic Performance

The Traffic Performance category groups areas that track the source and destination of traffic. You can use traffic thresholds and alarms to determine traffic load and flow and to reallocate resources appropriately. Table 10 lists the monitored parameters in this category and provides a brief description for each one.

TABLE 10 Traffic Performance category parameters

Monitored parameter	Description
Receive bandwidth usage percentage (RX)	The percentage of port bandwidth being used by RX traffic. For example, if the port speed is 10 Gbps and the port receives 5 Gb of data in one second, then the %RX utilization is 50 percent (5 Gb*100/(10 Gb*1 second)). For a master trunk port this indicates the RX percentage for the entire trunk.
Transmit bandwidth usage percentage (TX)	The percentage of port bandwidth being used by TX traffic. For example, if the port speed is 10 Gbps and the port sends 5 Gb of data in one second, then the %TX utilization is 50 percent (5 Gb*100/(10 Gb*1 second)). For a master trunk port, this indicates the TX percentage for the entire trunk.
Utilization (UTIL)	The percentage of individual port (or trunk) bandwidth being used at the time of the most recent poll.
Transmitted frame count (TX_FCNT)	The number of frames transmitted from the flow source.
Received frame count (RX_FCNT)	The number of frames received by the flow destination.
Transmitted throughput (TX_THPUT)	The number of megabytes (MB) transmitted per second by the flow source.
Received throughput (RX_THPUT)	The number of megabytes (MB) received per second by the flow destination.
SCSI frames read (IO_RD)	The number of SCSI I/O read command frames recorded for the flow.
SCSI frames written (IO_WR)	The number of SCSI I/O write command frames recorded for the flow.
SCSI frames read (IO_RD_BYTES)	The number of SCSI I/O bytes read as recorded for the flow.
SCSI frames written (IO_WR_BYTES)	The number of SCSI I/O bytes written as recorded for the flow.

FCIP Health

The FCIP Health category enables you to define rules for FCIP health, including circuit state changes, circuit state utilization, and packet loss. Table 11 lists the monitored parameters in this category and provides a brief description for each one.

TABLE 11 FCIP Health category parameters

Monitored parameter	Description
FCIP circuit state changes (CIR_STATE)	The state of the circuit has changed for one of the following reasons: • The circuit has gone offline • The circuit has come online • The circuit is faulty
FCIP circuit utilization (CIR_UTIL)	The percentage of circuit utilization in the configured time period (this can be minute, hour, or day).
FCIP circuit packet loss (CIR_PKTLOSS)	The percentage of the total number of packets that have had to be retransmitted.

Chapter

4

MAPS Groups, Policies, Rules, and Actions

In this chapter

MAPS groups overview

A MAPS group is a collection of similar objects that you can monitor using a common threshold.

You can create a group of objects and then use that group in rules, thus simplifying rule configuration and management. For example, you can create a group of UNIX ports, and then create specific rules for monitoring this group.

Predefined groups

MAPS provides several predefined groups that you cannot edit or delete.Table 12 lists these predefined groups, organized by object type.

TABLE 12 Predefined MAPS groups

Predefined group name	Object type	Description
ALL_PORTS	FC Port	All ports in the logical switch.
ALL_E_PORTS	FC Port	All E_Ports and EX_Ports in the logical switch. This includes all the ports in E_Port and EX_Port trunks as well.
ALL_F_PORTS	FC Port	All F_Ports in the logical switch. This includes all the ports in F_Port trunks as well.
ALL_HOST_PORTS	FC Port	All ports in the logical switch connected to hosts. MAPS automatically detects if a device connected on this port is a server device and adds it to this set.
ALL_TARGET_PORTS	FC Port	All logical switch ports connected to targets. MAPS automatically detects if a device connected on this port is a target device and adds it to this set. If the device connected to the port is identified as both a Host and a Target device, MAPS treats the port as Target port.
ALL_OTHER_F_PORTS	FC Port	All F_Ports in the logical switch which are neither Host ports nor Target ports.

TABLE 12 Predefined MAPS groups (Continued)

Predefined group name	Object type	Description
NON_E_F_PORTS	FC Port	All ports in the logical switch which are neither E_Ports nor F_Ports.
ALL_10GSWL_SFP	SFP	All 10-Gbps SWL SFP transceivers on FC Ports in the logical switch.
ALL_10GLWL_SFP	SFP	All 10-Gbps LWL SFP transceivers on FC Ports in the logical switch.
ALL_16GSWL_SFP	SFP	All 16-Gbps Short Wavelength (SWL) SFP transceivers in the logical switch.
ALL_16GLWL_SFP	SFP	All 16-Gbps Long Wavelength (LWL) SFP transceivers in the logical switch.
ALL_OTHER_SFP	SFP	All small form-factor pluggable (SFP) transceivers which do not belong to one of the following groups: • ALL_10GSWL_SFP • ALL_10GLWL_SFP • ALL_16GSWL_SFP • ALL_16GLWL_SFP • ALL_QSFP
ALL_QSFP	SFP	All quad small form-factor pluggable (QSFP) transceivers in the logical switch.
ALL_SLOTS	Slot	All slots present in the chassis.
ALL_SW_BLADES	Blade	All port and application blades in the chassis.
ALL_CORE_BLADES	Blade	All core blades in the chassis.
ALL_CIRCUITS	Circuit	All Fibre Channel over Internet Protocol (FCIP) circuits in the logical switch.
ALL_FAN	Fan	All fans in the chassis.
ALL_FLASH	Flash	The flash memory card in the chassis.
ALL_PS	Power Supply	All power supplies in the chassis.
ALL_TS	Temperature Sensor	All temperature sensors in the chassis.
ALL_WWN	WWN	All WWN cards in the chassis.
SWITCH	Switch	Default group used for defining rules on parameters that are global for the whole switch level, for example, security violations or fabric health.
CHASSIS	Chassis	Default group used for defining rules on parameters that are global for the whole chassis, for example, CPU or flash.

User-defined groups

In many cases, you need groups of elements that are more suited for your environment than the predefined groups. For example, small form-factor pluggable (SFP) transceivers from a specific vendor can have different specifications than SFP transceivers from another vendor. For example, when monitoring SFP transceivers, you might want to create a seperate group of SFP transceivers for each separate vendor. In another scenario, some ports may be more critical than others, and so would be monitored using different thresholds than other ports. A maximum of 64 user-defined groups and imported flows combined is permitted per logical switch.

Viewing group information

MAPS allows you to view the information for all groups or a specific group.

To view a summary of all the logical groups on a switch, enter **logicalGroup --show**. This command returns the group name, and whether the group is predefined.

The following example shows the output of **logicalGroup --show**.

```
switch:admin> logicalgroup --show
--------------------------------------------------------------------------------
Group Name        |Predefined |Type              |Member Count |Members
ALL_PORTS          Yes         Port               48            6/0-15,7/0-31
ALL_SFP            Yes         SFP                11            7/8-14,7/24-27
ALL_PS             Yes         PowerSupply        2             0-1
  :                :           :                  :             :
Group1             No          Port               10            1/1-5,3/7-9,3/12
Group2             No          SFP                10            1/1-5,3/7-9,3/12
```

To view details of a specific logical group on a switch, enter the following command:

logicalGroup --show *groupname*

This command returns the group name, whether the group is predefined, the group's type (port, SFP, and so on), the number of members, and the group members.

The following example shows the output of **logicalGroup --show ALL_TS**.

```
switch:admin> logicalgroup --show ALL_TS
--------------------------------------------------------------------------------
Group Name        |Predefined |Type              |Member Count |Members
--------------------------------------------------------------------------------
ALL_TS             Yes         Temperature Sensor 4             0-3
```

You can also use this command to display the state of flows from a MAPS perspective. The state of a flow is shown in the output in the "Members" column.The following example shows the output of **logicalGroup --show** for a flow imported into MAPS that is active in Flow Vision, and being monitored through MAPS.

```
switch:admin> logicalgroup -show fpm1
--------------------------------------------------------------------------------
Group Name        |Predefined |Type              |Member Count |Members
--------------------------------------------------------------------------------
fpm1               No          Flow               1             Monitored Flow
```

The following example shows the output of **logicalGroup --show** for a flow imported into MAPS that has either been deleted in Flow Vision or has been changed in Flow Vision to be a learning flow, or has been changed in Flow Vision in such a way that statistics are not being generated. MAPS is not monitoring this flow, but it is maintained as a zero member group. If you want to start monitoring this flow, you must reimport the flow using **mapsConfig --import -force**. Refer to the *Fabric OS Command Reference* for more information on using **mapsConfig** or **logicalGroup**.

```
switch:admin> logicalgroup --show fpm2
--------------------------------------------------------------------------------
Group Name        |Predefined |Type              |Member Count |Members
--------------------------------------------------------------------------------
fpm2               No          Flow               0             Not Monitored
(Stale Flow)
```

Monitoring similar ports using the same rules

You can create groups of ports that behave in a similar manner and monitor these ports using the same rules and thresholds.

Often on a switch there are sets of ports that behave in a similar manner and have a different behavior from other sets of ports. For example, the behavior of ports connected to UNIX hosts and servers is different from the behavior of ports connected to Windows hosts and servers.

To easily monitor these similar sets of ports using the same rules, you can create a group and apply rules to the group.

To create a group and apply rules to the group, complete the following steps.

1. Create a logical group of similar ports.

   ```
   switch:admin> logicalgroup --create unix_ports -type port -members "1,3,17,21"
   ```

2. Create rules using this logical group and add them to the active policy.

   ```
   switch:admin> mapsrule --create unix_hi_crc -monitor crc -group unix_ports
   -timebase min  -op g -value 50 -action raslog -policy my_policy
   ```

3. Enable the policy.

   ```
   switch:admin> mapspolicy --enable my_policy
   ```

   You must enable the policy even if it is the active policy. Adding a rule to the active policy does not take effect until you re-enable the policy.

MAPS policies overview

A MAPS policy is a set of rules that define thresholds for measures and action to take when a threshold is triggered. When you enable a policy, all of the rules in the policy are in effect.

A switch can have multiple policies. For example, you can have a policy for everyday use and you can have another policy for when you are running backups or performing switch maintenance.

Only one policy can be active at a time. When you enable a policy, it becomes the active policy and the rules in the active policy take effect.

One policy must always be active on the switch. You can have an active policy with no rules, but you must have an active policy. You cannot disable the active policy. You can only change the active policy by enabling a different policy.

Predefined policies

MAPS provides three predefined policies that you can neither modify or delete:

- dflt_moderate_policy

  Contains rules with thresholds values between the aggressive and conservative policies.

  This is the default policy.

- dflt_aggressive_policy

  Contains rules with very strict thresholds. Use this policy if you need a pristine fabric (for example, FICON fabrics).

- dflt_conservative_policy

  Contains rules with more lenient thresholds that allow a buffer and do not immediately trigger actions. Use this policy in environments where the elements are resilient and can accommodate errors.

Although you cannot modify the preconfigured policies, you can create a policy based on these policies. For more information, refer to "Modifying a default policy" on page 25.

User-defined policies

MAPS allows you to define your own policies. You can create a policy and add rules to it, or you can clone one of the default policies and modify the cloned policy. Refer to "Working with MAPS policies" on page 24 for information on working with user-defined policies.

Fabric Watch legacy policies

When you migrate from Fabric Watch to MAPS, three policies are automatically created if you have run **mapsConfig --fwconvert**. If you do not run this command, then these policies are not created. The three policies are:

- fw_custom_policy

  This policy contains all of the monitoring rules based on the custom thresholds configured in Fabric Watch.

- fw_default_policy

  This policy contains all of the monitoring rules based on the default thresholds configured in Fabric Watch.

- fw_active_policy

  This policy contains all of the monitoring rules based on the active thresholds in Fabric Watch at the time of the conversion.

These policies are treated as user-defined policies. You can modify them by adding and deleting rules, and you can delete them.

The following factors also apply to Fabric Watch conversions:

- Converted active Fabric Watch policies reference either custom or default Fabric Watch rules.
- No custom rules are created if the "custom" thresholds are the same as the default thresholds. Instead, the default Fabric Watch rule will be referenced in the fw_custom policy.
- Converted rules are prefixed with fw_def_*name* or fw_cust_*name*. The value for *name* is a string based on the Fabric Watch class, the area, threshold criteria (above high/below low), and the threshold number. This is the same pattern that MAPS rules use.

Working with MAPS policies

The following sections discuss working with MAPS policies.

Viewing policy information

MAPS allows you to view all the policies on a switch by using **mapsPolicy --show**. You can use this command to show all policies, only a particular policy, or a summary.

To view a summary of all the policies on a switch, enter the following command:

```
switch:admin> mapspolicy --show -summary
```

This command displays the policy names and the number of rules in each policy.

To view the features of all the policies on a switch, enter the following command:

```
switch:admin> mapspolicy --show -all
```

This command displays for all policies, the policy names, rule names, actions, and condition for each policy.

To view the features of a specific policy, enter the following command:

```
switch:admin> mapspolicy --show policyname
```

This command displays for the named policy, the policy names, rule names, actions, and condition.

Creating a policy

In some cases you need multiple policies, for example, to apply a different set of rules when maintenance operations are in progress. You can create multiple policies beforehand and then easily switch between policies when necessary.

To create policies and then add rules to them, complete the following steps.

1. Create a new policy or clone a policy from one of your existing policies.

   Use **mapsPolicy** with **--create** to create a policy, or **--clone** to clone an existing policy.

2. Create rules or modify rules to configure the required thresholds in the new policy.

   Use **mapsRule** with **--add** to create rules, or **--config** to modify existing rules.

The policy is automatically saved, but not enabled. It is not enabled unless you explicitly enable it.

The following example creates a policy by cloning another policy, and adds a rule to the new policy.

```
switch:admin> mapspolicy --clone defpol -name backup_pol
switch:admin> mapsrule --create chassiscpu -monitor CPU -group chassis -op ge
-value 70 -action raslog -policy backup_pol
```

Enabling a policy

A policy must be enabled before it takes effect. If the active policy is changed, or if the rules in the active policy are changed, the active policy must be re-enabled for the changes to take effect. Only one policy can be enabled at a time. To enable a policy, enter **mapsPolicy --enable** *policyname.* When you do this, the previously enabled policy is automatically disabled and the specified policy is then enabled.

Modifying a policy

In some cases you might need to modify a policy, for example, if elements in the fabric change or if threshold configurations need to be modified to catch certain error conditions.

To modify a policy and its associated rules, complete the following steps.

1. Modify the rules in the policy based on your requirements.

   You cannot modify the default rules, but you can add rules to and delete rules from the policy, and you can create rules and add them to the policy.

   Use **mapsPolicy** to add rules to and delete rules from the policy. Use **mapsRule** to modify rules or to create rules and add them to the policy.

2. If the policy is the active policy, you must enable the policy for the changes to take effect.

   ```
   switch:admin> mapspolicy --enable my_policy
   ```

   Changing the rules of the active policy does not take effect until you re-enable the policy.

The following example adds a rule to the policy named daily_policy, displays the policy, and then re-enables the policy so the change can become active.

```
switch:admin> mapspolicy --addrule daily_policy -rulename check_crc
switch:admin> mapspolicy --show daily_policy
Policy Name: daily_policy
Rule List  :
               check_crc
               defALL_E_PORTSITW_21
               defALL_E_PORTSITW_40
               myCHASSISFLASH_USAGE_90

Active Policy is 'daily_policy'
switch:admin> mapspolicy --enable daily_policy
```

Modifying a default policy

For a new switch or when you upgrade an existing switch to Fabric OS 7.1.0 or later, the default MAPS policy is dflt_moderate_policy. You cannot modify this predefined policy, but you can clone it to create a new policy.

To modify the default policy, complete the following steps.

1. Create a copy of the default policy.

   ```
   switch:admin> mapspolicy --clone dflt_moderate_policy -name my_policy
   ```

2. Modify the rules in the policy based on your requirements.

   You cannot modify the default rules, but you can add rules to and delete rules from the policy, and you can create or clone rules and add them to the policy.

   Use **mapsPolicy** to add and delete rules to and from the policy. Use **mapsRule** to create rules and add them to the policy.

3. Enable the policy.

   ```
   switch:admin> mapspolicy --enable my_policy
   ```

The previously-enabled policy is disabled, and the specified policy is enabled.

The following example clones the default policy, deletes two rules, and modifies a rule to send an e-mail message in addition to a RASLog entry.

```
switch:admin> mapspolicy --clone dflt_moderate_policy -name rule_policy
switch:admin> mapspolicy --delrule rule_policy -rulename defCHASSISFLASH_USAGE_90
switch:admin> mapspolicy --delrule rule_policy
-rulename defCHASSISMEMORY_USAGE_75
switch:admin> mapsrule --clone myCHASSISFLASH_USAGE_90 -monitor flash_usage
-group chassis -timebase none -op ge -value 90 -action raslog,email
-policy rule_policy
switch:admin> mapspolicy --enable rule_policy
```

MAPS rules overview

A MAPS rule associates a condition with actions that need to be triggered when the specified condition is evaluated to be true.

Each rule specifies the following items:

- A group of objects to be evaluated.
  Refer to "MAPS groups overview" on page 19 for additional information.
- The element to be monitored.
  Refer to "MAPS conditions" on page 26 for additional information.
- The condition being monitored.
  Each rule specifies a single condition. A condition includes a time base and a threshold.
  Refer to "MAPS conditions" on page 26 for additional information.
- The actions to take if the condition is evaluated to be true.
  Refer to "MAPS actions" on page 27 for additional information.

The combination of actions, conditions, and elements allow you to create a rule for almost any scenario required for your environment.

MAPS conditions

A MAPS condition includes a time base and a threshold. If the condition is evaluated as true, the rule is triggered. The condition depends on the element that is to be monitored.

Consider the following rule:

> For all F_Ports, if the change in the CRC counter in the last minute is greater than 10, then fence the port and issue a RASLog message.

In this rule, the condition is whether the change in the CRC counter in the last minute is greater than 10. For more details on RASLog messages in MAPS, refer to the *Fabric OS Message Reference*.

Thresholds

Thresholds are the values at which potential problems may occur. For example, in configuring a port threshold, you can select a specific value at which an action is triggered because of too many threshold violations.

Consider the following condition:

The change in the CRC counter in the last minute is greater than 10.

For this condition, the threshold is “greater than 10”.

NOTE
MAPS conditions are applied on a per-port basis, not switch- or fabric-wide. For example, 20 ports that each get 1 CRC counter would not trigger a “greater than 10” rule.

Time base

Time bases specify the time interval between two samples to be compared. You can set the time base to day (samples are compared once a day), hour (samples are compared once an hour), or minute (samples are compared every minute).

The time base affects the comparison of sensor-based data with user-defined threshold values.For measures where the time base is not applicable, set the time base to “none”.

MAPS actions

When you create a rule, you associate an action for MAPS to take if the condition defined in the rule evaluates to true.

Each rule can have one or more actions associated with it. For example, you can configure a rule to issue a RASLog message and fence the port if the number of CRC errors on any E_Port is greater than 20 per minute.

The global action settings on the switch take precedence over the actions defined in the rules. For example, if the global action settings allow RASLog alerts, but do not allow port fencing, then in the previous example, if the CRC threshold is reached, a RASLog message would be issued but the port would not be fenced. To enable global actions, use **mapsConfig --actions**. For more details, refer to “Enabling or disabling actions at a global level” on page 28. Refer to the *Fabric OS Command Reference* for further details on using this command.

MAPS provides the following actions:

- RASLog messages
- SNMP traps
- E-mail alert
- Port fencing
- Switch critical
- Switch marginal
- SFP marginal

Enabling or disabling actions at a global level

You can define what actions are allowable on the switch, regardless of the actions that are specified in individual rules.

Enabling and disabling actions at a global level allows you to configure rules with stricter actions, such as port fencing, but disable the action globally until you can test the configured thresholds. After validating the thresholds, you can enable port fencing globally without having to change all of the rules.

To enable or disable actions at a global level, complete the following steps.

1. Enter **mapsConfig --show** to display the actions that are currently allowed on the switch.
2. Enter **mapsConfig --actions** and specify all of the actions that you want to allow on the switch, for example, **mapsConfig --actions** *action1*,*action2*,*action3* ... (up to the complete set of actions.)

   You only need to specify the parameter values you are changing. The list of actions you specify replaces the existing list of actions on the switch. If you want to add an action, you must specify all of the existing actions as well as the new action. If you want to delete an action, you must specify the existing list minus the action you want to delete.

NOTE
To disable all actions, enter **mapsConfig --actions none**. The **none** keyword cannot be combined with any other action.

The following example shows that port fencing (**fence**) is not an allowed action on the switch, and then adds it to the list of allowed actions.

```
switch:admin> mapsconfig --show
Configured Notifications:       RASLOG,EMAIL
Mail Recipient:                 admin@mycompany.com
Relay Host:                     Relay Host IP is: 1.1.1.1
Paused members :
PORT :
CIRCUIT :
SFP :
switch:admin> mapsconfig --actions raslog,email,fence
switch:admin> mapsconfig --show
Configured Notifications:       RASLOG,EMAIL,FENCE
Mail Recipient:                 admin@mycompany.com
Relay Host:                     Relay Host IP is: 1.1.1.1
Paused members :
PORT :
CIRCUIT :
SFP :
```

RASLog messages

Following an event, MAPS adds an entry to the internal event log for an individual switch. The RASLog stores event information but does not actively send alerts. You can use **errShow** to view the RASLog. Refer to the *Fabric OS Message Reference* for a complete listing and explanation of MAPS-related RASLog messages.

SNMP traps

In environments where you have a high number of messages coming from a variety of switches, you may want to receive them in a single location and view them using a graphical user interface (GUI). In this type of scenario, Simple Network Management Protocol (SNMP) notifications may 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.

When specific events occur on a switch, SNMP generates a message (called a "trap") that notifies a management station using SNMP. 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

The SNMP trap only stores event information. In order to get the event notifications, you must configure the SNMP software to receive the trap information from the network device, and configure the SNMP agent on the switch to send the trap to the management station. You can configure SNMP notifications using **snmpConfig** or Brocade Network Advisor (refer to Event notification in the *Brocade Network Advisor User's Manual* or online help). For additional information on configuring the SNMP agent using **snmpConfig**, refer to the *Fabric OS Command Reference*.

SNMP MIB support

MAPS requires SNMP management information base (MIB) support on the device for management information collection. Refer to the *Fabric OS MIB Reference* for more detailed information on SNMP MIB support.

E-mail alert

An e-mail alert sends information about the event to one or more specified e-mail addresses. The e-mail alert specifies the threshold and describes the event, much like an error message.

You configure the e-mail recipients using **mapsConfig --emailcfg**. You must separate multiple e-mail addresses with a comma and include the complete e-mail address. For example, abc@12.com is a valid e-mail address; abc@12 is not. Refer to "Sending alerts using e-mail" on page 33 for more information.

Port fencing

The port fencing action fences the port if port fencing is enabled. Port fencing 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).

If you configure port fencing as an action, make sure that port fencing is configured for the rule with the highest monitored threshold. For example, if you configure a rule for CRC values greater than 10 per minute and you configure a second rule for CRC values greater than 20 per minute, do not configure port fencing as the action for the rule with the threshold value of 10.

This action is valid only for conditions evaluated on ports.

Switch critical

The switch critical action sets the state of the affected switch in the MAPS dashboard display to SW_CRITICAL. This action does not bring the switch down, but only affects what is displayed in the dashboard.

This action is valid only in the context of Switch Status Policy-related rules.

Switch marginal

The switch marginal action sets the state of the affected switch in the MAPS dashboard to SW_MARGINAL. This action does not affect the actual state of the switch, but only affects what is displayed in the dashboard.

This action is valid only in the context of Switch Status Policy-related rules.

SFP marginal

The SFP marginal action sets the state of the affected small form-factor pluggable (SFP) transceiver in the MAPS dashboard to “down”. This action does not bring the SFP transceiver down, but only affects what is displayed in the dashboard.

This action is valid only in the context of Advanced SFP groups.

Working with MAPS rules and actions

The following sections cover how to work with MAPS rules and actions, including creating, modifying, and deleting rules, and enabling or disabling actions.

Creating a rule

Each rule monitors a single condition. When you create a rule, you can choose to add it to a policy.

To create a policy rule, complete the following steps.

1. Enter **mapsRule --create** to create the rule.

   ```
   mapsrule --create rule_name -monitor monitor -group group_name
   -timebase timebase -op comparison_operator -value threshold_value
   -action action -policy policy
   ```

2. Enter **mapsRule --show** to display the rule.

   ```
   mapsrule --show rule_name
   ```

3. If you added the rule to the active policy, you must re-enable the policy for the rule to take effect.

mapspolicy --enable *policy*

The following example creates a rule to generate a RASLog message if the CRC counter for a group of critical ports is greater than 10 in an hour. This rule is added to the daily_policy, and the daily_policy is re-enabled for the rule to take effect.

```
switch:admin> mapsrule --create check_crc -monitor crc -group critical_ports
-timebase hour -op g -value 10 -action raslog -policy daily_policy
switch:admin> mapsrule --show check_crc
Rule Data:
----------
RuleName: check_crc
Condition: critical_ports(crc/hour>10)
Actions: raslog
Policies Associated: daily_policy
switch:admin> mapspolicy --enable daily_policy
```

To accommodate creating a rule for a flow, **mapsrule** accepts a flow name as a value for the **-group** parameter. The following example illustrates the structure.

```
switch:admin> mapsrule --create check_crc2 -monitor crc -group MyFlow
-timebase min -op g -value 15 -action raslog -policy daily_policy2
```

Modifying a rule

You can modify only user-defined rules. You cannot modify the default rules.

To modify a user-defined policy rule, complete the following steps.

1. Enter **mapsRule --show** to display the rule you want to modify.

   mapsrule --show *rule_name*

2. Enter **mapsRule --config** followed by the parameters you are changing to modify the rule.

   mapsrule --config check_crc2 -timebase hour

   You only need to specify the parameters you are changing. Any parameters you do not specify are not changed. The configuration settings you specify replace the existing configuration settings for the rule.

3. Enter **mapsRule --show** to display the new rule.

   mapsrule --show *rule_name*

4. If the rule is included in the active policy, you must re-enable the policy for the modified rule to take effect.

   mapspolicy --enable *policy*

The following example modifies the check_crc rule to generate a RASLog message if the CRC counter for a group of critical ports is greater than 15 in an hour. This rule is part of the active policy, so the policy is re-enabled for the change to take effect.

```
switch:admin> mapsrule --show check_crc
Rule Data:
----------
RuleName: check_crc
Condition: critical_ports(crc/hour>10)
Actions: raslog
Policies Associated: daily_policy
switch:admin> mapsrule --config check_crc -monitor crc -group critical_ports
-timebase hour -op g -value 15 -action raslog -policy daily_policy
```

```
switch:admin> mapsrule --show check_crc
Rule Data:
----------
RuleName: check_crc
Condition: critical_ports(crc/hour>15)
Actions: raslog
Policies Associated: daily_policy
switch:admin> mapspolicy --enable daily_policy
```

Cloning a rule

You can clone both default and user-defined rules.

To clone a rule, complete the following steps.

1. Enter **mapsRule --show** to display the rule you want to clone.

   mapsrule --show *rule_name*

2. Enter **mapsRule --clone** *oldRuleName* **-rulename** *newRuleName* to duplicate the rule.

   mapsrule --clone *existing ruleName* **-rulename** *new ruleName*
   [**-group** *group name | flow name*] [**-monitor** *ms name*] [**-timebase** *day:hour:min*]
   [**-op** *l:le:g:ge:eq*] [**-value** *value*] [**-action** *action*]

   Optionally, you can specify the parameters you want to be different from the old rule in the new rule. If no parameters other than **-rulename** are specified, an exact copy of the original rule is created. You can later modify the rule by using **--config**.

   For example, the following command clones “myOldRule” as “myNewRule”, but changes the flow that is being monitored to “flow2” and assigns it the monitor “monitor2”.

   ```
   switch:admin> mapsrule --clone myOldRule -rulename myNewRule -group flow2
   -monitor monitor2
   ```

Cloned rule examples

The following example creates a cloned rule that is exactly the same as the source rule.

```
admin> mapsrule --clone Rule1 -rulename NewRule1
admin> mapsrule --show NewRule1
RuleName: NewRule1
Action: Raslog, Fence, SNMP
Condition: Switch(SEC_IDB/Min>0)
Policies Associated: none
```

The following example creates a cloned rule with a changed time base.

```
admin> mapsrule --clone Rule1 -rulename NewRule2 -timebase hour
admin> mapsrule --show NewRule2
RuleName: NewRule2
Action: Raslog, Fence, SNMP
Condition: Switch(SEC_IDB/Hour>0)
Policies Associated: none
```

The following example modifies the time base of an existing rule.

```
admin> mapsrule --config Rule2 -timebase hour
admin> mapsrule --show Rule2
RuleName: Rule2
Action: Raslog, Fence, SNMP
Condition: Switch(SEC_IDB/Hour>0)
```

```
Policies Associated: none
```

The following example shows all rules. Notice that the actions are not abbreviated in the output.

```
admin> mapsrule --show all
--------------------------------------------------------------------------
RuleName                  Action                      Condition
--------------------------------------------------------------------------
Rule1                     Raslog, Fence, SNMP         Switch(SEC_IDB/Min>0)
Rule2                     Raslog                      Switch(SEC_IDB/Hour>1)
NewRule1                  Raslog, Fence, SNMP         Switch(SEC_IDB/Min>0)
NewRule2                  Raslog, Fence, SNMP         Switch(SEC_IDB/Hour>1)
```

The following example shows the policy names associated with the rule. If the rule is not associated with a policy, nothing is shown. The actions are abbreviated in the output.

```
admin> mapsrule --show rule1
RuleName: Rule1
Action: Raslog, Fence, SNMP
Condition: Switch(SEC_IDB/Min>0)
Policies Associated: daily_policy, crc_policy
```

Sending alerts using e-mail

In environments where it is critical that you are notified about errors quickly, you can use e-mail alerts. With e-mail alerts, you can be notified of serious errors by e-mail or a pager, so you can react quickly. There is a limit of five e-mail addresses per alert, and the maximum length for each individual e-mail address is 128 characters.

To configure MAPS to send an alert using e-mail, complete the following steps.

1. Enter the **mapsConfig --emailcfg** command to set the e-mail parameters.

   ```
   mapsconfig --emailcfg -address email_address
   ```

   To send an alert to multiple email addresses, separate the addresses using a comma.

2. Enter the **mapsConfig --show** command to display the e-mail configuration settings. Refer to "Configuring e-mail server information" on page 34 for information on specifying the email server to be used.

   ```
   mapsconfig --show
   ```

The following example specifies the e-mail address for e-mail alerts on the switch.

```
switch:admin> mapsconfig --emailcfg -address admin@mycompany.com
switch:admin> mapsconfig --show
Configured Notifications:       RASLOG,EMAIL,FENCE
Mail Recipient:                 admin@mycompany.com
Relay Host:                     Relay Host IP is: 10.168.39.118
Relay Host Domain Name:         brocade.com
Paused members :
PORT :
CIRCUIT :
SFP :
```

The following example specifies multiple e-mail addresses for e-mail alerts on the switch.

```
switch:admin> mapsconfig --emailcfg -address admin@mycompany.com,
admin2@mycompany.com, admin3@mycompany.com
switch:admin> mapsconfig --show
Configured Notifications:       RASLOG,EMAIL,FENCE
Mail Recipient:                 admin@mycompany.com,
```

```
                                admin2@mycompany.com,
                                admin3@mycompany.com,
Relay Host:                     Relay Host IP is: 10.168.39.118
Relay Host Domain Name:         brocade.com
Paused members :
PORT :
CIRCUIT :
SFP :
```

Configuring e-mail server information

Fabric OS 7.2.0 and later allows you to specify the e-mail server used to send e-mail alerts using the **relayConfig** command. The e-mail configuration is global at the chassis level and is common for all logical switches in the chassis.

relayConfig --config -rla_ip *relay IP address* **-rla_dname** *"relay domain name"*

The following example configures the switch to use an e-mail server located at 10.70.212.168 named "mail.brocade.com".

```
switch:admin> relayconfig --config -rla_ip 10.70.212.168 -rla_dname
"mail.brocade.com"
```

Viewing configured e-mail server information

Running **relayConfig --show** displays the configured e-mail server host address and domain name. The following example illustrates this command:

```
switch:admin> relayconfig --show
Relay Host:                     10.70.212.168
    Relay Domain Name:           mail.brocade.com
```

Chapter

5

Monitoring flows using MAPS

In this chapter

Flows and MAPS

MAPS can monitor only static flows created using Flow Vision and generates alert messages based on user-defined rules. To monitor a flow, the flow must first be created in Flow Vision, and then imported into MAPS. For information on working with Flow Vision, refer to the *Fabric OS Flow Vision Administrator's Guide*.

NOTE
Only the statistics monitoring functionality is supported in MAPS. The Flow Generator and Flow Mirror features are not integrated with MAPS.

Importing flows

A flow can be imported any time after it has been defined in Flow Vision. Only static flows can be imported into MAPS. Learned flows (those created using an asterisk (*)) cannot be imported or monitored. When importing a flow, the flow name must be specified.

Only active flows can be monitored in MAPS. MAPS monitoring starts after a flow has both been activated in Flow Vision and imported into MAPS. Deactivating a flow causes monitoring to stop until it is reactivated. When the flow is reactivated, monitoring automatically restarts.

Once a flow is imported to MAPS, you can define MAPS rules to monitor the flow. Each rule has a threshold criterion and alerting mechanism defined. If the threshold criterion is met, then a configured alert is generated.

The following example imports an existing flow named "myflow22" into MAPS.

```
switch:admin> mapsconfig --import myflow22
```

Removing flows from MAPS

If you do not want to monitor a flow using MAPS, use **mapsConfig --deimport** *flow name* to remove the flow from MAPS.

The following example removes the flow named "myflow22" from MAPS.

```
switch:admin> mapsconfig --deimport myflow22
```

Notes on removing flows

- Deimporting will succeed only if there are no MAPS rules associated with the flow. Before removing a flow, you must delete all the rules associated with that flow.
- You can only remove one flow at a time.
- Removing a flow only removes it from MAPS. It does not affect the flow definition in Flow Vision.

Monitoring flows using MAPS

To monitor the network, you can define flows on a switch with different feature sets. Flows defined in Flow VIsion can be imported into MAPS as groups. MAPS supports thresholding on statistics monitored by the Flow Vision statistics-monitoring feature. For more details on flows and Flow Vision, refer to the *Fabric OS Flow Vision Administrator's Guide*.

To monitor flows using MAPS, complete the following steps.

1. Create the flow in Flow Vision using **flow --create**.
2. Import the flow into MAPS using **mapsConfig --import**.
3. Define a MAPS rule using **mapsRule --create**.

   Once a flow is imported to MAPS, you can define MAPS rules to monitor it. Refer to "MAPS rules overview" on page 26 for information on creating and using rules.

The following example illustrates these steps.

```
switch:admin> flow --create myflow22 -feature monitor -egrport 21
-srcdev 0x010200  -dstdev 0x040500
switch:admin> mapsconfig --import myflow22
switch:admin> mapsrule --create myRule22 -group myflow22 -monitor TX_FCNT
-timebase hr -op g -value 22 -action RASLOG –policy myPolicy
```

If an imported flow is deleted in Flow Vision

If you delete a flow that has not been imported into MAPS, there is no change in MAPS. If you delete a flow that has been imported into MAPS, the flow is marked as deleted, but the group corresponding to the flow will remain. Groups are only removed if the **flow --deimport** command is used. Creating the flow again will not cause it to be monitored automatically. If, after you have deleted a flow, you then try to import a flow with the same name as the deleted flow, the import will fail and a RASLog message is generated. If you are certain that you want to import that flow and monitor it using the existing rules for that flow, you must use the **-force** keyword as part of **mapsConfig --import**. For more details on RASLog messages in MAPS, refer to the *Fabric OS Message Reference*.

The following example demonstrates importing a flow using the **-force** keyword.

```
switch:admin> mapsconfig --import myExFlow -force
```

ATTENTION
Subflow monitoring is not supported at this time.

ATTENTION
Small form-factor pluggable (SFP) transceiver monitoring on simulated mode (SIM) ports is not supported for MAPS.

Examples of using MAPS to monitor traffic performance

The following examples illustrate using MAPS to monitor traffic performance.

Monitoring end-to-end performance

The following example monitors the percentage of frames exceeding the configured threshold of RX and TX values in a flow between two devices. To achieve this, it defines a flow using the **-feature monitor** parameter for a particular SID, DID, and port.

```
switch:admin> flow --create E2Eflow -feature monitor -ingrport 5 -scrdev 0x010200
-dstdev 0x020300
switch:admin> mapsconfig --import endtoendflow
switch:admin> mapsrule --create E2E -monitor TX_THPUT -group E2E_10 -timebase min
-op g -value 10 -action rasLog -policy flowPolicy
```

Monitoring frames for a specified set of criteria

The following example watches for frames in a flow going through a port that contain ABORT sequence markers.

```
switch:admin> flow --create abtsflow -feature mon -ingrport 128 -frametype abts
switch:admin> mapsconfig --import abtsflow
```

You can then define rules for this flow (group).

```
switch:admin> mapsrule --create abts cnt rl -monitor TxFcnt -group abtsFlow
-timebase min -ops ge -value 10 -action rasLog -policy flowPolicy
```

Chapter

MAPS Dashboard

6

In this chapter

MAPS dashboard overview

The MAPS dashboard provides a summary view of the switch health status that allows you to easily determine whether everything is working according to policy or whether you need to investigate further.

MAPS dashboard sections

The MAPS dashboard output is divided into three main sections: dashboard high-level information, switch health report information, and categorized health information, plus a history section that is displayed if you enter **mapsDb –show all**.

Dashboard high-level information

The Dashboard high-level information section displays the basic data for the dashboard: the time the dashboard was started, the name of the active policy, and any fenced ports.

Switch Health Report information

The Switch Health Report information section displays the current switch policy status and lists any factors contributing to that status as defined by the Switch Health Report rules in the active policy. Refer to "Switch Policy Status" on page 12 for more details.

Categorized health information

The Categorized health information section collects and summarizes the various switch statistics monitored by MAPS into seven categories, and displays the current status of each category since the previous midnight, and the status of each category for the past seven days. If a rule violation has caused a change in the status of a category, rule-related information is included for that category. The following categories are monitored by MAPS:

- Port Health: Refer to "Port Health" on page 12.
- FRU Health: Refer to "FRU Health" on page 14.
- Security Violations: Refer to "Security Violations" on page 14.

- Fabric State Changes: Refer to "Fabric State Changes" on page 15.
- Switch Resource: Refer to "Switch Resource" on page 15.
- Traffic Performance: Refer to "Traffic Performance" on page 16.
- FCIP Health: Refer to "FCIP Health" on page 17.

When a category contains an "out-of-range" error, the dashboard displays a table showing the rules triggered in that category since the previous midnight. This allows you to see more precisely where the problem is occurring. Each category in the table contains the following information:

- The number of times rules were triggered in each category
- The rules that were triggered
- The number of times that a rule was triggered in the hour that it was triggered
- The entities (ports, circuits, and so on) that triggered the rule
- The values set for these entities when the rule was triggered

For each category, the dashboard stores the five most recent distinct rule violations that occurred in each hour since the previous midnight. For each rule violation the dashboard stores the five most recent entities on which the rules were triggered. Consequently, while a rule might be triggered multiple times within a given hour, only the timestamp of the latest violation is stored, along with the last five entities on which the rule was triggered. However, each violation of a rule individually is reflected in the "Rule Count" for that category and the "Repeat Count" for that rule in that hour.

For example, if the same rule was triggered 12 times in one hour, the "Repeat Count" value for that rule will be 12, but only the timestamp for the last occurrence is displayed. In addition the last five distinct entities on which this rule was triggered are stored (and these can include different instances of the rule's violation). Alternatively, if a rule was triggered 12 times since midnight, but each violation happened in a different hour, then each violation is logged separately in the dashboard.

Historical data

The historical data section provides information on how the switch has been behaving regardless of whether rules were triggered. It contains only port-related statistics. The historical information is the raw counter information since the previous midnight. Using this information, you can get an idea of the errors seen on the switch even though none of the rules might have been violated. And if you see potential issues, you can reconfigure the appropriate rule thresholds to specifically fit the switch based on the information shown instead of using the default thresholds. The historical data log stores the last seven days on which errors were recorded (not the last seven calendar days but the last seven days, irrespective of any interval between these days). If a day does not have any errors, the dashboard does not include that day in the results.

Notes on dashboard data

- The dashboard displays data only for days that have errors. If a day does not have any errors, the dashboard does not include that day in the results.
- The “Rule Count” value is the absolute number of different violations in that category since the previous midnight. The “Repeat Count” is the number of times a rule has been violated in the hour, for example between 10:00:00 and 10:59:59.
- By default only the last five violations are displayed for each category. However, running **mapsDb --show all** causes the dashboard to display all the rule violations currently stored along with additional historical data.
- If there are no errors for the switch ports, security, fabric, or FCIP health, the dashboard displays “No-error”. If there are no errors for any of the other categories, the dashboard displays “In-range”. The following dashboard state conditions may be displayed:
  - No-error: Displayed if there is no error, for example, if no port has had an error since midnight.
  - In-range: Displayed if there are errors but no rule was triggered.
  - Out of range: Displayed if at least one error triggered a rule belonging to the category in which this state message appears.
- CIR_UTIL errors (CIR_UTIL, RX, TX, UTIL) are not displayed in the Historical data section unless other errors are recorded for that day.

MAPS dashboard display options

You can set the dashboard to display data gathered since midnight, for any 60-minute period since midnight, or for the last seven days on which errors were recorded. Refer to the *Fabric OS Command Reference* for detailed instructions on using the **mapsDb** command options to configure the dashboard.

Viewing the MAPS dashboard

After a policy is created and activated, you can monitor the switch status by running **mapsDb --show** with the appropriate parameter. There are three primary views: a summary view, a detailed view (which includes historical data), and a history-only view. Refer to “MAPS monitoring categories” for explanations of the categories listed in the dashboard output.

Viewing a summary switch status report

A summary view provides health status at a high level, and includes enough information for you to investigate further if necessary.

To view a summary switch status report, complete the following steps.

1. Connect to the switch and log in using an account with admin permissions.
2. Enter **mapsDb --show** with no other parameters to display the summary status.

The following example displays the general status of the switch (“CRITICAL”) and lists the overall status of the monitoring categories for the current day (measured since midnight) and for the last seven days. If any of the categories are shown as being “Out of operating range”, the last five conditions that caused this status are listed.

```
switch:admin> mapsdb --show
DB start time: Tue Jul  9 17:17:33 2013
Active policy: dflt_conservative_policy
Fenced Ports : none

1 Switch Health Report:
=======================

Current Switch Policy Status: CRITICAL
Contributing Factors:
---------------------
*BAD_PWR (MARGINAL).
*BAD_FAN (CRITICAL).


2.1 Summary Report:
===================

Category                |Today                    |Last 7 days               |
-------------------------------------------------------------------------------
Port Health             |Out of operating range   |No Errors                 |
Fru Health              |Out of operating range   |In operating range        |
Security Violations     |No Errors                |No Errors                 |
Fabric State Changes    |No Errors                |No Errors                 |
Switch Resource         |In operating range       |In operating range        |
Traffic Performance     |In operating range       |In operating range        |
FCIP Health             |Not applicable           |Not applicable            |


2.2 Rules Affecting Health:
===========================

Category(Rule Count)|RepeatCount|Rule Name                 |Execution Time   |Object            \
-------------------------------------------------------------------------------------------------\
Port Health(2)      |1          |defALL_OTHER_F_PORTSCRC_40 |07/09/13 17:18:18|Port 1            \
                    |1          |defALL_OTHER_F_PORTSCRC_21 |07/09/13 17:18:18|Port 1            \
Fru Health(2)       |2          |defALL_FANFAN_STATE_FAULTY |07/09/13 19:15:17|Fan 2             \
                    |           |                           |                 |Fan 1             \

                |Triggered Value(Units)|
                ------------------------
                |876 CRCs              |
                |876 CRCs              |
                |FAULTY                |
                |FAULTY                |
```

Viewing a detailed switch status report

The detailed switch status displays historical data for port performance errors in addition to the summary view.

To view a detailed switch status report, complete the following steps.

1. Connect to the switch and log in using an account with admin permissions.
2. Enter **mapsDb --show all** to display the detailed status.

The following example shows the detailed switch status. The status includes the summary switch status, plus port performance data for the current day (measured since midnight).

```
switch:admin> mapsdb --show all
DB start time: Tue Jul  9 17:17:33 2013
Active policy: dflt_conservative_policy
Fenced Ports : none

1 Switch Health Report:
=======================

Current Switch Policy Status: CRITICAL
Contributing Factors:
---------------------
*BAD_PWR (MARGINAL).
*BAD_FAN (CRITICAL).


2.1 Summary Report:
===================

Category                |Today                     |Last 7 days               |
-------------------------------------------------------------------------------
Port Health             |Out of operating range    |No Errors                 |
Fru Health              |Out of operating range    |In operating range        |
Security Violations     |No Errors                 |No Errors                 |
Fabric State Changes    |No Errors                 |No Errors                 |
Switch Resource         |In operating range        |In operating range        |
Traffic Performance     |In operating range        |In operating range        |
FCIP Health             |Not applicable            |Not applicable            |


2.2 Rules Affecting Health:
===========================

Category(Rule Count)|RepeatCount|Rule Name                  |Execution Time   |Object            \
-------------------------------------------------------------------------------------------------\
Port Health(2)      |1          |defALL_OTHER_F_PORTSCRC_40 |07/09/13 17:18:18|Port 1            \
                    |1          |defALL_OTHER_F_PORTSCRC_21 |07/09/13 17:18:18|Port 1            \
Fru Health(2)       |2          |defALL_FANFAN_STATE_FAULTY |07/09/13 19:15:17|Fan 2             \
                    |           |                           |                 |Fan 1             \

                  |Triggered Value(Units)|
                  ------------------------
                  |876 CRCs              |
                  |876 CRCs              |
                  |FAULTY                |
                  |FAULTY                |


3 History Data:
===============

Stats(Units)        Current   --/--/--   --/--/--   --/--/--   --/--/--   --/--/--   --/--/--
                    Port(val)
-------------------------------------------------------------------------------------------
CRC(CRCs)           0(>999)    -          -          -          -          -          -
                    1(876)     -          -          -          -          -          -
ITW(ITWs)           -          -          -          -          -          -          -
LOSS_SYNC(SyncLoss) -          -          -          -          -          -          -
```

```
LF                  -          -          -          -          -          -          -
LOSS_SIGNAL(LOS)    -          -          -          -          -          -          -
PE(Errors)          -          -          -          -          -          -          -
STATE_CHG           -          -          -          -          -          -          -
LR                  -          -          -          -          -          -          -
C3TXTO(Timeouts)    -          -          -          -          -          -          -
RX(%)               -          -          -          -          -          -          -
TX(%)               -          -          -          -          -          -          -
UTIL(%)             -          -          -          -          -          -          -
BN_SECS(Seconds)    -          -          -          -          -          -          -
```

Viewing historical data

Entering **mapsDb --show history** displays a summarized history of the switch status since the previous midnight. This is useful if you want a quick view of what has been happening on the switch in that period. The output of this command differs depending on the platform you run it on. On fixed-port switches, ports are shown in port index format; on chassis-based platforms, ports are shown in slot/port format.

To view a summarized history of the switch status, complete the following steps.

1. Connect to the switch and log in using an account with admin permissions.
2. Run **mapsDb --show history**.

The following example displays all stored historical port performance data for a fixed-port switch.

```
switch:admin> mapsdb --show history
History Data:
===============

Stats(Units)        Current   --/--/--   --/--/--   --/--/--   --/--/--   --/--/--   --/--/--
                    Port(val)
-------------------------------------------------------------------------------------------
CRC(CRCs)           0(>999)    -          -          -          -          -          -
                    1(876)     -          -          -          -          -          -
ITW(ITWs)           -          -          -          -          -          -          -
LOSS_SYNC(SyncLoss) -          -          -          -          -          -          -
LF                  -          -          -          -          -          -          -
LOSS_SIGNAL(LOS)    -          -          -          -          -          -          -
PE(Errors)          -          -          -          -          -          -          -
STATE_CHG           -          -          -          -          -          -          -
LR                  -          -          -          -          -          -          -
C3TXTO(Timeouts)    -          -          -          -          -          -          -
RX(%)               -          -          -          -          -          -          -
TX(%)               -          -          -          -          -          -          -
UTIL(%)             -          -          -          -          -          -          -
BN_SECS(Seconds)    -          -          -          -          -          -          -
```

The following example displays all stored historical port performance data for a chassis-based platform.

```
switch:admin> mapsdb --show history
History Data:
===============

Stats(Units)        Current   --/--/--   --/--/--   --/--/--   --/--/--   --/--/--   --/--/--
                    Port(val)
-------------------------------------------------------------------------------------------
CRC(CRCs)           1/4(>999)  -          -          -          -          -          -
                    1/16(876)  -          -          -          -          -          -
```

```
ITW(ITWs)           -          -          -          -          -          -
LOSS_SYNC(SyncLoss) -          -          -          -          -          -
LF                  -          -          -          -          -          -
LOSS_SIGNAL(LOS)    -          -          -          -          -          -
PE(Errors)          -          -          -          -          -          -
STATE_CHG           -          -          -          -          -          -
LR                  -          -          -          -          -          -
C3TXTO(Timeouts)    -          -          -          -          -          -
RX(%)               -          -          -          -          -          -
TX(%)               -          -          -          -          -          -
UTIL(%)             -          -          -          -          -          -
BN_SECS(Seconds)    -          -          -          -          -          -
```

Viewing data for a specific time window

Detailed historical data provides the status of the switch for a specific time window. This is useful if, for example, users are reporting problems on a specific day or time. The same port-display patterns apply to viewing detailed historical data as for ordinary historical data.

To view detailed historical data about a switch, complete the following steps.

1. Connect to the switch and log in using an account with admin permissions.
2. Run mapsDb --show details and specify either the day or the hour of the current day you want to view.

   mapsdb --show details -day *dd/mm/yyyy*

   or

   mapsdb --show details -hour *hh*

The following example displays historical port performance data for July 9, 2013 for a chassis-based platform. Because the health status of the current switch poliucy is “CRITICAL”, the sections “Contributing Factors” and “Rules affecting health” are displayed. If the current switch policy status was “HEALTHY”, neither of these sections would be displayed.

```
switch:admin> mapsdb --show details -day 7/09/2013
DB start time: Tue Jul  9 17:17:33 2013
Active policy: dflt_conservative_policy
Fenced Ports : none

1 Switch Health Report:
=======================

Current Switch Policy Status: CRITICAL
Contributing Factors:
---------------------
*BAD_PWR (MARGINAL).
*BAD_FAN (CRITICAL).


2.1 Summary Report:
===================

Category                |Today                     |Last 7 days               |
-------------------------------------------------------------------------------
Port Health             |Out of operating range    |No Errors                 |
Fru Health              |Out of operating range    |In operating range        |
Security Violations     |No Errors                 |No Errors                 |
Fabric State Changes    |No Errors                 |No Errors                 |
```

```
Switch Resource          |In operating range        |In operating range        |
Traffic Performance      |In operating range        |In operating range        |
FCIP Health              |Not applicable            |Not applicable            |


2.2 Rules Affecting Health:
===========================

Category(Rule Count)|RepeatCount|Rule Name                  |Execution Time   |Object            \
-------------------------------------------------------------------------------------------------\
Port Health(2)      |1          |defALL_OTHER_F_PORTSCRC_40 |07/09/13 17:18:18|Port 1            \
                    |1          |defALL_OTHER_F_PORTSCRC_21 |07/09/13 17:18:18|Port 1            \
Fru Health(2)       |2          |defALL_FANFAN_STATE_FAULTY |07/09/13 19:15:17|Fan 2             \
                    |           |                           |                 |Fan 1             \

                  |Triggered Value(Units)|
                  ------------------------
                  |876 CRCs              |
                  |876 CRCs              |
                  |FAULTY                |
                  |FAULTY                |


3 History Data:
===============

Stats(Units)        Current   07/09/13   --/--/--   --/--/--   --/--/--   --/--/--   --/--/--
                    Port(val)
-------------------------------------------------------------------------------------------
CRC(CRCs)           0(>999)    0(>999)    -          -          -          -          -
                    1(876)     1(876)     -          -          -          -          -
ITW(ITWs)           -          -          -          -          -          -          -
LOSS_SYNC(SyncLoss) -          -          -          -          -          -          -
LF                  -          -          -          -          -          -          -
LOSS_SIGNAL(LOS)    -          -          -          -          -          -          -
PE(Errors)          -          -          -          -          -          -          -
STATE_CHG           -          -          -          -          -          -          -
LR                  -          -          -          -          -          -          -
C3TXTO(Timeouts)    -          -          -          -          -          -          -
RX(%)               -          -          -          -          -          -          -
TX(%)               -          -          -          -          -          -          -
UTIL(%)             -          -          -          -          -          -          -
BN_SECS(Seconds)    -          -          -          -          -          -          -
```

Clearing data

The **mapsDb --clear** command deletes the stored data from the dashboard. This is useful if, for example, you want to see only the data logged after making a change on the switch (or to a rule).

To clear the stored dashboard data from a switch, complete the following steps.

1. Connect to the switch and log in using an account with admin permissions.
2. Enter **mapsDb --clear** and specify the level of data (all, history, or summary) you want to remove from the display.

   mapsdb --clear -[all | history | summary]

The following example clears only the dashboard summary data.

```
switch:admin> mapsdb --clear -summary
```

NOTE
When the dashboard is cleared, a RASLog message is generated. For more details on RASLog messages in MAPS, refer to the *Fabric OS Message Reference*.

Bottleneck detection integration with the MAPS dashboard

The Fabric OS bottleneck daemon is responsible for detecting persistent bottlenecks and providing notifications. Bottleneck monitoring is integrated with the MAPS dashboard enabling you to easily see which ports are impacted by both persistent and transient bottlenecks. In the MAPS dashboard, the Summary section includes bottleneck events detected by the bottleneck daemon, and the Historical section displays entries both for those ports that have bottleneck time detected by the daemon and for those ports that have "cred_zero" counters that are not zero.

NOTE
For the bottleneck daemon to produce notifications, the sub-second bottleneck monitoring parameters must be correctly configured and the bottlenecks must be seen persistently on the ports.

Bottleneck events detected by the bottleneck daemon are shown in the Rules section of the Summary view. However, even if the bottleneck daemon does not log a bottleneck event (due to lack of persistence) the data shown in the Historical section can be used in the following ways:

- MAPS identifies the ports on which bottlenecks are seen and sorts them based on the number of seconds that they exceeded the bottleneck threshold. This identifies the most strongly affected ports, whether they are affected by persistent or transient bottlenecks.
- The cred_zero counter can also be used to detect bottlenecks. If the cred_zero counter increases for a port but no bottleneck time is recorded, this indicates a potential transient bottleneck on the port.

Additional information about bottleneck detection

The following information may help you to use MAPS as an aid to bottleneck detection.

- No existing bottleneck daemon logic and behaviors have been changed for Fabric OS 7.2.
- All bottleneck configurations must be made using **bottleneckmon** commands. Refer to the "Bottleneck Detection" chapter in the *Fabric OS Administrator's Guide* for specific command details.
- The MAPS dashboard is used only for logging bottleneck latency events. Congestion bottleneck events are not logged on the MAPS dashboard. Latency events include:
  - Latency bottleneck on any port.
  - Timeouts occurring on any 16 Gbps-capable Fibre Channel platform port.
  - Stuck Virtual Channel on any port.
- The MAPS dashboard will continue to log events whether RASLogs are set to on or off in the bottleneck configuration.

Dashboard output for bottleneck data

The Summary portion of the MAPS dashboard includes bottleneck (BN) information when available. In the following example, the “Traffic Performance” line is where bottleneck information appears. Notice that the last line indicates a bottleneck caused by a timeout rather than a numeric value.

```
                (MAPS Dashboard output trimmed)
2.2 Rules affecting health:
===========================
Category(Rule Count)|RepeatCount|Rule Name                      |Execution Time   |Object         \
--------------------------------------------------------------------------------------------------\
Port Health(12)     |1          |defALL_OTHER_F_PORTSLR_10     |08/21/02 0:30:06 |Port 23        \
                     1          |defALL_OTHER_F_PORTSLR_5      |08/21/02 0:29:54 |Port 23        \
                     1          |defALL_OTHER_F_PORTSC3TXTO_3  |08/21/02 0:29:36 |Port 23        \
                     1          |defALL_OTHER_F_PORTSC3TXTO_10 |08/21/02 0:29:36 |Port 23        \
                     6          |Bottleneck_stuckvc            |08/21/02 0:30:24 |Port 23        \
                     1          |Bottleneck_latency            |08/21/02 0:30:20 |Port 23        \
                     1          |Bottleneck_timeout            |08/21/02 0:30:27 |Port 23        \

                    |Triggered Value(Units)|
                    ------------------------
                    |11                     |
                    |7                      |
                    |57                     |
                    |57                     |
                    |STUCKVC                |
                    |60                     |
                    |TIMEOUT                |
```

Flow Vision integration with the MAPS dashboard

In the MAPS dashboard summary view, flow-related statistics are shown as part of traffic performance, and are displayed under this category in the Switch Health Report section of the dashboard. This data is not included in the History Data section.

Chapter

7

Additional MAPS features

In this chapter

Overview

The following sections describe additional features in the Monitoring and Alerting Policy Suite (MAPS).

Pausing and resuming MAPS monitoring

If you want to temporarily stop monitoring a port or other element in MAPS, for example, during maintain an ce operations such as device or server upgrades, run **mapsConfig --config pause** and specify both the element type and the specific member(s) that you want monitoring paused for. This suspends MAPS monitoring for that element member. You must specify both the type and the member information in the command; you specify multiple members by separating them with a comma for individual members, or a hyphen for a range of members. You resume MAPS monitoring by entering **mapsConfig --config continue** and specify both the element type and the specific member(s) that you want monitoring resumed for.

The following example pauses MAPS monitoring for ports 5 and 7, and then resumes port 5.

```
switch: admin> mapsConfig --config pause -type port -members 5,7
switch: admin> mapsConfig --config continue -type port -members 5
```

MAPS Service Availability Module

The MAPS Service Availability Module (MAPSSAM) 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.

Although the **switchShow** command provides basic switch information, the MAPSSAM report provides detailed information, which enables you to track marginal or faulty ports that can affect throughput or switch performance.

The MAPSSAM report displays a summary record of the status of each port on the switch as a percentage of the total time since either the switch was rebooted, MAPS was activated or **mapsSam --clear** was run. This allows you to see if any port is failing more often than others. The report lists each for each port the port number, type, total up and down times, the number of times the port recorded a fault, and the total offline time for the port.

Notes on MAPSSAM

- The MAPSSAM report does not distinguish why a port is recorded as down, it only reports that how long the port has been down.
- The MAPSSAM report does not include the health status of GbE ports. MAPS only monitors and reports the status for physical and virtual FC ports.

The following example shows a typical output for mapsSam --show.

```
switch:admin> mapssam --show
                          Total        Total         Down          Total
Port      Type          Up Time      Down Time    Occurrence  Offline Time
                       (Percent)     (Percent)     (Times)       (Percent)
================================================================================
0           E             0.00        98.00           7             2.00
1           F            99.97         0.00           0             0.03
2           U             0.00         0.00           0           100.00
3           U             0.00         0.00           0           100.00
4           U             0.00         0.00           0           100.00
5           U             0.00         0.00           0           100.00
6           U             0.00         0.00           0           100.00
7           F            99.97         0.00           0             0.03
8           M            99.97         0.00           0             0.03
Number of Ports: 8
```

Appendix

MAPS Threshold values

A

In this chapter

MAPS threshold value tables

The following tables describe monitoring thresholds used by the Monitoring and Alerting Policy Suite (MAPS). In these tables, AG indicates the Aggressive policy, MO indicates the Moderate policy, and CO indicates the Conservative policy.

TABLE 13 Switch Status Policy thresholds

Monitoring Statistic	MAPS Thresholds (Marginal/Critical)[1]		
	AG	MO	CO
Bad Power	DCX/DCX+: -/3 DCX-4S/4s+: -/1 All Other Platforms: 1/2		
Bad Temp	1/2	1/2	1/2
Bad Fan	1/2	1/2	1/2
Flash Usage	90	90	90
Marginal Ports (%)	-/5	6/10	6/10
Error Ports (%)	-/5	6/10	6/10
Faulty ports (%)	-/5	6/10	6/10

1. All thresholds conditions are greater than or equal to the shown value.

TABLE 14 Port Monitoring thresholds

Monitoring Statistic	MAPS Thresholds (RASLOG Threshold/Port Fencing Threshold)[1]														
	E_Ports			F_Ports (Host)			F_Ports (Target)			F-Ports (Unknown)			NON-E_F_Ports		
	AG	MO	CO	AG	MO	CO	AG	MO	CO	AG	MO	CO	AG	MO	CO
C3TX_TO	5	10	20	2/4	3/10	11/20	0/2	3/5	6/10	2/4	3/10	11/20	N/A		
CRC	0/2	10/20	21/40	Same As E_Ports			0/2	5/10	11/20	Same As E_Ports			Same As E_Ports		
ITW	15/20	21/40	41/80				5/10	11/20	21/40						
Link Reset	2/4	5/10	11/20				0/2	3/5	6/10						
State Change	2/4	5/10	11/20				0/2	3/7	8/15						
Protocol Err	0/2	3/7	5/10				0/2	3/4	5/6						
Loss of signal	0	3	5				0	3	5						
Link Failure	0	3	5				0	3	5						
Sync Loss	0	3	5				0	3	5						
RXP (%)	60	75	90				60	75	90						
TXP (%)															
Trunk Util % (E_ and F_Ports)															

1. **Unless noted otherwise, all thresholds conditions are greater than the shown value.**

TABLE 15 FCIP Monitoring thresholds

Monitoring Statistic	MAPS Thresholds (RASLOG Threshold/Port Fencing Threshold)[1]		
	AG	MO	CO
State Change	0	3	5
Utilization %	60	75	90
Packet Loss	0.01	0.05	0.1

1. **Unless noted otherwise, all thresholds conditions are greater than the shown value.**

TABLE 16 Fabric Monitoring thresholds

Monitoring Statistic	MAPS Thresholds (RASLOG Threshold/Port Fencing Threshold)[1]		
	AG	MO	CO
Domain ID Change	1		
Fabric Logins	4	6	8
Fabric Reconfigurations	1	2	4
E_ports down	1	2	4
Segmentation changes	1	2	4
Zone changes	2	5	10

1. **Unless noted otherwise, all thresholds conditions are greater than the shown value.**

TABLE 17 Security Monitoring thresholds

Monitoring Statistic	MAPS Thresholds (RASLOG Threshold/Port Fencing Threshold)[1]		
	AG	MO	CO
DCC Violations	0	2	4
HTTP Violation	0	2	4
Illegal Command	0	2	4
Incompatible security DB	0	2	4
Login Violations	0	2	4
Invalid Certifications	0	2	4
No-FCS	0	2	4
SCC Violations	0	2	4
SLAP failures	0	2	4
Telnet Violations	0	2	4
TS out of sync	1/hr 2/day	2/hr 4/day	4/hr 10/day

1. **Unless noted otherwise, all thresholds conditions are greater than the shown value.**

TABLE 18 Resource Monitoring thresholds

Monitoring Statistic	MAPS Thresholds (RASLOG Threshold/Port Fencing Threshold) [1]		
	AG	MO	CO
Flash (%)	90	90	90
CPU (%)	80	80	80
Memory (%)	75	75	75

1. **Unless noted otherwise, all thresholds conditions are greater than the shown value.**

TABLE 19 SFP Monitoring thresholds

Monitoring Statistic	MAPS Thresholds (RASLOG Threshold/Port Fencing Threshold)[1]																	
	ALL_10GSWL_SFP			ALL_10GLWL_SFP			ALL_16GSWL_SFP			ALL_16GLWL_SFP			ALL_QSFP			ALL_OTHER_SFP		
	AG	MO	CO	AG	MO	CO	AG	MO	CO	AG	MO	CO	AG	MO	CO	AG	MO	CO
CURRENT	10			95			12			70			10			50		
RXP	1999			2230			1259			1995			2180			5000		
TXP	1999			2230			1259			1995			-			5000		
VOLTAGE	3000 to 3600			2970 to 3600			3000 to 3600			3000 to 3600			2940 to 3630			2960 to 3630		
TEMP	-5 to 90			-5 to 90			-5 to 85=			-5 to 90			-5 to 85			-13 to 85		

1. **Unless noted otherwise, all thresholds conditions are greater than the shown value.**

A MAPS threshold value tables

Index

E

F

G

H

I

L

M

P

Q

R

S

T

U

V

W