ADMINISTRATION GUIDE

Extreme Network OS MAPS Administration Guide

Supporting Network OS 7.3.0

9035243
15 June 2018

Contents

Preface

Document conventions

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

Notes, cautions, and warnings

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

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

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

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

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

Text formatting conventions

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

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.
`Courier font`	Identifies CLI output.

Format	Description
	Identifies command syntax examples.

Command syntax conventions

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

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Extreme resources

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

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at www.extremenetworks.com. Product documentation for all supported releases is available to registered users at www.extremenetworks.com/support/documentation.

Document feedback

Quality is our first concern at Extreme, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you.

You can provide feedback in two ways:

- Use our short online feedback form at http://www.extremenetworks.com/documentation-feedback-pdf/
- Email us at internalinfodev@extremenetworks.com

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

Contacting Extreme Technical Support

As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for immediate support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact.
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge - Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub - A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal - Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

About This Document

Supported hardware and software

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

Although many different software and hardware configurations are tested and supported by Extreme Networks, Inc. for Network OS, documenting all possible configurations and scenarios is beyond the scope of this document.

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

- ExtremeSwitching VDX 2746
- ExtremeSwitching VDX 6740
  - ExtremeSwitching VDX 6740-48
  - ExtremeSwitching VDX 6740-64
- ExtremeSwitching VDX 6740T
  - ExtremeSwitching VDX 6740T-48
  - ExtremeSwitching VDX 6740T-64
  - ExtremeSwitching VDX 6740T-1G
- ExtremeSwitching VDX 6940-36Q
- ExtremeSwitching VDX 6940-144S
- ExtremeSwitching VDX 8770
  - ExtremeSwitching VDX 8770-4
  - ExtremeSwitching VDX 8770-8

To obtain information about a Network OS version other than this release, refer to the documentation specific to that version.

Using the Network OS CLI

For complete instructions and support for using the Extreme Network OS command line interface (CLI), refer to the *Extreme Network OS Command Reference*.

What's new in this document

This document describes the concepts and configuration of the Extreme Monitoring and Alerting Policy Suite (MAPS) for Network OS.

On October 30, 2017, Extreme Networks, Inc. acquired the data center networking business from Brocade Communications Systems, Inc. This document has been updated to remove or replace references to Brocade Communications, Inc. with Extreme Networks., Inc., as appropriate.

The content has been updated with the following changes for Network OS v7.3.0 :

- No significant changes for this release.

The content has been updated with the following changes for Network OS v7.2.0 :

- BPQ Drop Threshold Monitoring -- Provides monitoring and Logging when traffic drops more packets on a BPQ port than the configured Per-Second Drop Threshold.

The content has been updated with the following changes for Network OS v7.1.0 :

- No significant changes for this release.

The content has been updated with the following changes for Network OS v7.0.1 :

- No significant changes for this release.

The content has been updated with the following changes for Network OS v7.0.0 :

- User configurable groups, policies, and rules for MAPS
- Updates for MAPS actions
- Updates for threshold values

Monitoring and Alerting Policy Suite Overview

MAPS overview

The Monitoring and Alerting Policy Suite (MAPS) is an optional network health monitor supported on all devices running Network OS v6.0.1 or later that enables each device to constantly monitor for potential faults and automatically alert you to problems.

MAPS has a dashboard that provides you with the ability to view in a quick glance what is happening on the device, and helps administrators dig deeper to see details of exactly what is happening on the device (for example, the kinds of errors, the error count, and so on.)

MAPS is disabled by default, but no license is required to enable it.

In addition to user-configurable custom monitoring policies, MAPS provides a set of predefined monitoring policies that allow you to immediately use MAPS on activation.

MAPS interoperability with other features

MAPS interacts in different ways with different Network OS features, including Fabric Watch and High Availability.

MAPS and Fabric Watch

MAPS cannot coexist with Fabric Watch. Once MAPS is enabled, Fabric Watch is automatically disabled.

MAPS and High Availability

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

MAPS upgrade and downgrade considerations

When upgrading or downgrading Network OS, the following MAPS-related behaviors should be expected:

- MAPS is not available in versions prior to Network OS v6.0.1.
- On a firmware upgrade from previous versions, MAPS will be disabled by default and all default policies will be present on the system.
- Downgrading from Network OS v6.0.1 to previous versions is blocked if MAPS is enabled and active. You must disable MAPS to perform a firmware downgrade.
- All user-defined rules need to be removed before downloading from Network OS v7.x.x to Network OS v6.0.1.

MAPS Groups, Policies, Rules, and Actions

MAPS groups overview

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

Predefined MAPS groups

MAPS provides several predefined groups that are used in the default polices for monitoring. These groups cannot be edited or deleted. For the groups that need dynamic membership update (such as ALL_ETH_PORTS or ALL_SFP), the updates are automatically handled by MAPS in the background. The following table lists these predefined groups organized by object type.

TABLE 1 Predefined MAPS groups

Group name	Element type	Description
ALL_ETH_PORTS	1G, 10G, 40G, 100 Gbps Interfaces	All ports physically present for interface error monitoring.
ALL_NAS_PORTS	Ethernet Ports	All Ethernet ports configured as Network-Attached Storage (NAS) ports.
ALL_DAS_PORTS	Ethernet Ports	All Ethernet ports configured as Direct Attached Storage (DAS) ports and hyperconverged appliences.
ALL_ISCSI_PORTS	iSCSI ports	All Ethernet ports configured to be connected to iSCSI targets using the interface CLI.
ALL_QSFP_SR	QSFP	All 40 Gbps Short Reach quad small form-factor pluggable (QSFP) transceivers (works up to 100 m)
ALL_QSFP_LR	QSFP	All 40 Gbps Long Reach QSFP transceivers (works up to 10 km)
ALL_1GSR_SFP	SFP	All 1 Gbps Short range GBIC/SFP transceivers
ALL_1GLR_SFP	SFP	All 1 Gbps Long range GBIC/SFP transceivers
ALL_10GSR_SFP	SFP	All 10 Gbps Short range GBIC/SFP transceivers
ALL_10GLR_SFP	SFP	All 10 Gbps Long range GBIC/SFP transceivers
ALL_10G_USR	SFP	All 10 Gbps UltraShort reach GBIC/SFP transceivers
ALL_100GSR_SFP	SFP	All 100 Gbps Short range GBIC/SFP transceivers
ALL_100GLR_SFP	SFP	All 100 Gbps Long range GBIC/SFPtransceivers
ALL_PS	Power supply	All power supplies present in the chassis. This group is used to monitor field-replaceable unit (FRU) events such as plug-in, plug-out, or faulty events.
ALL_LC	Line card	All line cards present in the system. This group is used to monitor FRU events such as plug-in, plug-out, or faulty events.

TABLE 1 Predefined MAPS groups (continued)

Group name	Element type	Description
ALL_SLOTS	Slots	All slots present in the system. This group is used to monitor FRU events such as plug-in, plug-out, or faulty events.
ALL_SFM	SFM – Core Blade	All Switch Fabric Modules (SFMs) present in the system. This group is used to monitor FRU events such as plug-in, plug-out, or faulty events.
CHASSIS	Chassis	Default group used of defining rules on parameters that are global for the whole chassis, such as CPU or Flash.
ALL_FANS	Fan	All fans present in the system. This group is used to monitor FRU events such as plug-in, plug-out, or faulty events.
ALL_TS	Temperature sensor	All temperature sensors present in the system.
ALL_WWN	WWN card	All World Wide Name (WWN) cards present in the system.
ALL_FLASH	Compact flash	Group for monitoring compact flash usage.

MAPS policies

A MAPS policy is a set of rules that defines 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 device can have multiple policies. For example, you can have a policy for everyday use and you can have another policy for when you are performing device 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 device. You can have an active policy with no actions, but you must have an active policy. You can only change the active policy by enabling a different policy.

Predefined MAPS policies

MAPS provides three predefined policies that you cannot modify or delete:

- dflt_aggressive_policy - Contains rules with very strict thresholds. Use this policy if you need a pristine fabric.
- dflt_moderate_policy - Contains rules with thresholds values between the aggressive and conservative policies.
- 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.

Viewing policy information

MAPS allows you to view all the policies on a device by using the **show maps policy** command. You can use this command to show all policies on a device or in an RBridge ID.

For complete information on viewing policy information, refer to the **show maps policy** command in the *Extreme Network OS Command Reference*.

To view a summary of all the policies for an RBridge ID, enter the following command in privileged EXEC mode.

```
device# show maps policy summary rbridge-id 1
       Policy Name                    Number of Rules
-----------------------------------------------------------
dflt_aggressive_policy           :              196
dflt_conservative_policy         :              198
```

```
dflt_moderate_policy              :              198
Active Policy is 'dflt_conservative_policy'.
```

To view detailed information on the policies for an RBridge ID, enter the following command in privileged EXEC mode.

```
device# show maps policy detail rbridge-id 1
------------------------------------------------------------------
                        Policies and Rules for RbridgeId 1
------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
                         dflt_aggressive_policy   Rules (ENABLED)
-------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
               Rules List
Action                                                  Condition
-------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------

        defALL_ETH_PORTS_CRCALN_6                   RASLOG,SNMP,EMAIL
CRCALNALL_ETH_PORTS(MIN>6)
        defALL_ETH_PORTS_CRCALN_150               RASLOG,SNMP,EMAIL
CRCALNALL_ETH_PORTS(MIN>150)
        defALL_ETH_PORTS_RX_SYM_ERR_0         RASLOG,SNMP,EMAIL               RX_SYM_ERRALL_ETH_PORTS(MIN>0)

-------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
               dflt_conservative_policy Rules  (NOT ENABLELD)
-------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
               Rules List
Action                                                   Condition
-------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
        defALL_ETH_PORTS_RX_SYM_ERR_0       RASLOG,SNMP,EMAIL               RX_SYM_ERRALL_ETH_PORTS(MIN>0)
        defALL_iSCSI_PORTS_RX_SYM_ERR_0     RASLOG,SNMP,EMAIL               RX_SYM_ERRALL_iSCSI_PORTS(MIN>0)
        defALL_NAS_PORTS_RX_SYM_ERR_0       RASLOG,SNMP,EMAIL               RX_SYM_ERRALL_NAS_PORTS(MIN>0)
-------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
               dflt_moderate_policy Rules (ENABLED)
-------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
               Rules List
Action                                                   Condition
-------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------

        defALL_ETH_PORTS_RX_SYM_ERR_0        RASLOG,SNMP,EMAIL               ALL_ETH_PORTS(RX_SYM_ERRMIN>0)
        defALL_iSCSI_PORTS_RX_SYM_ERR_0      RASLOG,SNMP,EMAIL
ALL_iSCSI_PORTS(RX_SYM_ERRMIN>0)
        defALL_NAS_PORTS_RX_SYM_ERR_0        RASLOG,SNMP,EMAIL               ALL_NAS_PORTS(RX_SYM_ERRMIN>0)
```

MAPS actions overview

A MAPS action defines the activity that occurs if the condition defined in a rule evaluates to true.

Each rule can have one or more actions associated with it.

MAPS provides the following predefined actions:

- RASLOG messages
- SNMP traps
- E-mail alerts
- Port Fencing
- SFP_MARGINAL (SFP marginal)

- USE-POLICY

For complete information on all threshold and fencing options, refer to the **threshold-monitor interface** command in the *Extreme Network OS Command Reference*.

Quick setup for MAPS

MAPS provides the capability to define what actions are allowable on the device, regardless of the actions that are specified in individual rules.

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 device. 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.

1. Enter RBridge configuration mode.

```
device(config)# rbridge-id 5
```

2. Enter MAPS configuration mode.

```
device(config-rbridge-id-5)# maps
```

3. Enter the **enable policy** command for each of the actions that you want to allow on the device, up to the complete set of actions. Action names must be separated by commas.

```
device(config-rbridge-id-5-maps)# enable policy dflt_aggressive_policy actions RASLOG,SW_CRITICAL
```

RASLog messages

Following an event, MAPS adds an entry to the internal event log for an individual device. The RASLog stores event information but does not actively send alerts. Use the **show logging raslog** command to view the RASLog. For details, refer to the *Extreme Network OS Command Reference*.

The RASLog message contains the following data:

- The notification level (all RASLog messages generated by MAPS are designated as "WARNING").
- The name of the device generating the message.
- The physical port on the device generating the message.
- The condition that was exceeded in order to generate the message.
- The current value of the condition violation.
- The name of the rule controlling the condition.
- The name of the category that displays this information when you use the MAPS dashboard.

The following example shows a RASLog log entry generated by MAPS:

```
 2015/04/16-01:06:05 , [MAPS-1003], 5973, SW/0 | Active, WARNING, sw0, Eth Port 1/0/4 , Condition=
ALL_ETH_PORTS(RX_SYM_ERR/min>5) , Current Value:[ RX_SYM_ERR,52 Errors ], RuleName
=defALL_ETH_PORTS_RX_SYM_ERR_5, Dashboard Category=Port Health.
```

SNMP traps

In environments where you have a high number of messages coming from a variety of devices, 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 device individually as you would have to do for error log notifications.

When specific events occur on a device, 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:

- The rule name that triggered the SNMP trap)
- The element type that triggered the rule (such as Ethernet port, SFP, and so on)
- The data type to be used to interpret the data sent for the "key" OID)
- The key OID (the unique ID for the element that triggered the rule)
- The condition that triggered the rule
- The number of MS/measures present in the condition
- The value for each of the MS/measures that triggered the rule
- The severity level of the MAPS event
- The action configured in the rule (this provides information on other actions triggered along with SNMP trap)
- The dashboard Category to which this rule belongs

To receive 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 device to send the trap to the management station. For additional information on configuring the SNMP agent, refer to the *Extreme Network OS Command Reference* and the *Extreme Network OS Management Configuration Guide*.

The following example shows a typical SNMP trap generated by MAPS.

```
Specific: 1
  Message reception date: 4/7/2015
  Message reception time: 5:41:52.861 PM
  Time stamp: 0 days 22h:43m:43s.00th
  Message type: Trap (v1)
  Protocol version: SNMPv1
  Transport: IP/UDP
Agent
    Address: 10.17.37.171
    Port: 8000
Manager
    Address: 172.26.3.166
    Port: 4425
  Community: public
  SNMPv1 agent address: 10.17.37.171
Enterprise: maps
  Specific Trap MIB Lookup Results
  Bindings (10)
    Binding #1: mapsConfigRuleName.0 *** (OCTET STRING) defSWITCHSEC_LV_4
    Binding #2: mapsConfigObjectGroupType.0 *** (INTEGER) switch(11)
    Binding #3: mapsConfigObjectKeyType.0 *** (INTEGER) int32(1)
    Binding #4: mapsConfigObjectKeyValue.0 *** (OCTET STRING) 0
    Binding #5: mapsConfigNumOfMS.0 *** (Integer32) 1
    Binding #6: mapsConfigMsList.0 *** (OCTET STRING) SEC_LV,1,5
    Binding #7: mapsConfigSeverityLevel.0 *** (INTEGER) warning(3)
    Binding #8: mapsConfigCondition.0 *** (OCTET STRING) SWITCH(SEC_LV/min>4)
    Binding #9: mapsConfigAction.0 *** (Integer32) 19
    Binding #10: mapsDbCategory.0 *** (OCTET STRING) Security Violations
```

SNMP MIB support

MAPS requires SNMP management information base (MIB) support on the device for management information collection.

For additional information on SNMP MIB support, refer to the *Extreme Network OS Management Configuration Guide*.

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 the **email** command. You must include the complete e-mail address. For example, abc@12.com is a valid e-mail address; abc@12 is not. Refer to Configuring MAPS alert targets on page 28 for more information.

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 Policy Status-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 Policy Status-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.

User-defined policies, groups, and rules

MAPS monitoring is based on the current rules in the active policy. If MAPS monitoring is to be customized then the MAPS policies must be modified with custom rules, then activated.

MAPS has three pre-defined policies (conservative, aggressive and moderate) that contain thresholds for various counters in accordance to the names of the policies. MAPS supports a pre-defined set of actions that can be taken when certain monitoring conditions are met. However, you can create custom policies, groups, and rules that cover specific issues or problems on your particular configuration.

These custom groups, policies, and rules function identically to the default policies, groups, and rules included with Extreme Network OS.

To create custom MAPS behavior, perform the following:

1. Create new custom logical groups of ports, if needed. [Creating user-defined groups on page 19]
2. Create custom rules that modify the existing behavior. [Creating user-defined rules on page 20]
3. Create a new custom policy and add or modify these rules to the policy. [Creating user-defined policies on page 19]

4. Add any predefined groups or rules to the policy you require to the policy.[Predefined MAPS policies on page 14]
5. Enable the policy so that all the rules in the policy are activated and monitored by MAPS. [Enabling MAPS on page 27]

Creating user-defined policies

Create a custom policy for MAPS to cover your specific situation and needs.

A MAPS policy is a set of rules that defines 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.

1. Enter global configuration mode.

```
device#configure terminal
```

2. Enter Rbridge ID configuration mode.

```
device(config)# rbridge-id 1
```

3. Enter MAPS configuration mode.

```
device(config-rbridge-id-1)# maps
```

4. Use the policy command to create an empty policy.

```
device(config-rbridge-id-1-maps)# policy TempMonitor
```

5. Specify the rules to be added using the **rule** parameter. Designate the rule followed by actions. Multiple actions can be specified by separating them with commas. These actions should not include USE-POLICY. This is allowed only with the **enable policy** command.

```
device(config-policy-TempMonitor)# rule HighTempAlert actions RASLOG,SW_CRITICAL
```

6. Exit policy configuration mode with the **exit** command.

```
device(config-policy-TempMonitor)# exit
device(config-rbridge-id-1-maps)#
```

7. Enable MAPS with a policy and action.

```
device(config-rbridge-id-1-maps)# enable policy TempMonitor actions RASLOG,EMAIL
```

Creating user-defined groups

As explained in earlier sections, MAPS currently supports pre-defined rules, polices and groups that are present out-of-box. These thresholds function well in most situations. But, in some cases you may want to apply your own thresholds, either because of the network quality requirements or because of known issues, you will need to customize thresholds applicable to the specific elements.

To help solve this situation, MAPS provides a capability to create groups containing one or more groups of ports or SFPs. The user-defined groups can in turn be used in custom rules and custom polices to create custom MAPS monitoring behavior as needed.

User-defined group's elements should be homogenous, for example all the elements in a groups should be of the same kind, such as either Ethernet ports or SFPs. Groups cannot contain different kinds of elements.

1. Enter global configuration mode.

```
device#configure terminal
```

2. Enter Rbridge ID configuration mode.

```
device(config)# rbridge-id 1
```

3. Enter MAPS configuration mode.

```
device(config-rbridge-id-1)# maps
```

4. Create a group with the **group** command, specifying the name of the group and the interface members.

```
device(config-rbridge-id-1-maps)# group CritEthPortGrp01 type interface members 1/0/1,1/0/2,1/0/3
```

5. Optionally, create any additional custom groups needed for the policy.

```
device(config-rbridge-id-1-maps)# group CritEthPortGrp02 type interface members
1/0/121,1/0/122,1/0/133
```

The following example displays the entire task.

```
device#configure terminal
device(config)# rbridge-id 1
device(config-rbridge-id-1)# maps
device(config-rbridge-id-1-maps)# group CritEthPortGrp01 type interface members 1/0/1,1/0/2,1/0/3
device(config-rbridge-id-1-maps)# group CritEthPortGrp02 type interface members 1/0/121,1/0/122,1/0/133
```

Creating user-defined rules

User-defined rules allow you to create rules based on the predefined or natively supported counters or statistics to cover your specific situation and needs.

The administrator can configure the following rules:

- Simple rules that monitor a single counter in each rule.
- Multiple rules with respective conditions defined across multiple time intervals (hour, minute, or day) for the same counter (the rules can be active simultaneously).
- Different rules for the same counter and time interval but with different thresholds (the rules can be active simultaneously).

The valid monitor names are:

- CRCALN
- RX_SYM_ERR
- RX_ABN_FRAME
- ASIC_PKTDROP
- SEC_TELNET
- SEC_LV
- TEMP
- CURRENT
- VOLTAGE
- RXP
- TXP
- FLASH_USAGE
- MEMORY_USAGE
- CPU

- BAD_TEMP
- BAD_PWR
- BAD_FAN
- SFP_STATE
- PS_STATE
- FAN_STATE
- ETH_MGMT_PORT_STATE
- SFP_TEMP
- WWN_DOWN
- DOWN_SFM
- FAULTY_BLADE
- HA_SYNC
- BLADE_STATE
- WWN

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter Rbridge ID configuration mode.

```
device(config)# rbridge-id 1
```

3. Enter MAPS configuration mode.

```
device(config-rbridge-id-1)# maps
```

4. Create a custom rule with the **rule** command, specifying the name of the group and the interface members.

```
device(config-rbridge-id-1-maps)# rule RuleOne group EthUser monitor BAD_TEMP interval min op eq
value 2
```

5. (Optional) Create any additional custom rules needed for the policy.

```
device(config-rbridge-id-1-maps)# rule RuleTwo group EthUser monitor BAD_TEMP interval day op eq
value 100
```

The following example creates user-defined rules..

```
device# configure terminal
device(config)# rbridge-id 1
device(config-rbridge-id-1)# maps
device(config-rbridge-id-1-maps)# rule RuleOne group EthUser monitor BAD_TEMP interval min op eq value 150
device(config-rbridge-id-1-maps)# rule RuleTwo group EthUser monitor BAD_TEMP interval day op eq value 125
```

Multiple threshold monitoring overview

Multiple threshold monitoring allows for early notification of issues before they potentially get worse. In addition, this allows administrator to prioritize the issues and efficiently resolve them, if needed, according to their severities.

Multiple threshold monitoring allows you to monitor for varying severity levels of an issue and trigger different actions at different levels. For example, you can configure MAPS to monitor for any change in CRC counters of a port against multiple threshold values at the same time:

- If a change in the CRC counters occurred in the one minute > 2 times, then trigger a RASLOG alert.
- If a change in the CRC counters occurred in the one minute > 5 times, then trigger an email alert and an SNMP trap.
- If a change in the CRC counters occurred in the one minute > 10 times, then fence the port.

MAPS takes different actions depending on the severity of the condition. This allows prioritizing more critical events, that are delivered through e-mail , trap, or fencing, over non-critical events that are delivered through RASLOG.

Monitoring across multiple time windows

You may need to monitor for spikes (which are the normal irregular behavior), as well as monitor for the non-critical but persistent issues. Taking the CRC counter as an example, you can have MAPS monitor for the following at same time:

- If a change in the CRC counters occurred in the last one minute > 5 times, then trigger an email alert and an SNMP trap.
- If a change in the CRC counters occurred in the last one day > 20 times, then trigger an email alert and a RASLOG alert.

This allows you to monitor for both severe and non-critical but persistent conditions, and provides better visibility into the behavior of the device, warning you of non-obvious issues that can degrade the performance of the fabric.

The example below demonstrates a typical multiple threshold example with fencing. For complete information on all threshold and fencing options, refer to the **threshold-monitor interface** command in the *Extreme Network OS Command Reference*.

```
device(config-rbridge-id-154)# threshold-monitor interface policy mypolicy type Ethernet area IFG alert
above highthresh-action fence raslog lowthresh-action email raslog
```

MAPS Elements and Categories

MAPS structural elements

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

TABLE 2 MAPS structural elements

Element	Description
Action	The activity performed by MAPS if a condition defined in a rule evaluates to true.
Category	A grouping of similar elements that can be monitored (for example, "Security Violations").
Condition	A true or false trigger created by the combination of a timebase and a threshold value.
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 *Extreme Network OS Management Configuration 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.
Rule	A direction associating a condition with one or more actions that must occur when the specified condition is evaluated to be true.
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.

MAPS monitoring categories

When you activate 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
- Switch Resource

NOTE

The MAPS dashboard also displays the status of these categories.

Switch Policy Status

The Switch Policy Status category enables you to monitor the health of the device by defining the number of types of errors that transitions the overall device state into a state that is not healthy. For example, you can specify a switch policy so that if a device has one fan failure, it is considered to be in a marginal state; if it has two failures, it is in a critical (down) state. The following table lists the monitored parameters in this category and identifies the factors that affect their health.

NOTE
Not all devices support the listed monitors.

TABLE 3 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.
Faulty blades (FAULTY_BLADE)	Faulty blades (applies to modular devices).
High Availability (HA_SYNC)	Switch does not have a redundant CP (applies to modular devices only).

Port Health

The Port Health category monitors port statistics and takes action based on the configured thresholds and actions. Only physical ports are configurable.

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. The following table lists the monitored parameters in this category and provides a brief description for each one.

TABLE 4 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.
Symbol Errors (RX_SYM_ERR)	The number of symbol errors received.
RX Abnormal Frames (RX_ABN_FRAME)	The number of abnormal frames received.
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.

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. The following table 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.

TABLE 5 FRU Health category parameters

Monitored parameter	Description
Power Supplies (PS_STATE)	State of a power supply has changed.

TABLE 5 FRU Health category parameters (continued)

Monitored parameter	Description
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.

Security Violations

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

TABLE 6 Security Violations category parameters

Monitored parameter	Description
Login violations (SEC_LV)	Login violations which occur when a secure fabric detects a login failure.
Telnet violations (SEC_TELNET)	Telnet violations which occur when a Telnet connection request reaches a secure switch from an unauthorized IP address.

Switch resource monitoring

Switch 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 elements. Environment thresholds enable temperature monitoring, and resource thresholds enable monitoring of flash memory.
- Configure memory or CPU usage parameters on the device 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.

The following table lists the monitored parameters in this category and provides a brief description for each one.

TABLE 7 Switch Resource category parameters

Monitored parameter	Description
Temperature (TEMP)	Refers to the ambient temperature inside the device, in degrees Celsius. Temperature sensors monitor the device in case the temperature rises to levels at which damage to the device might occur.
ETH_MGMT_PORT_STATE	Refers to the current state of the Ethernet ports.
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 RAM by calculating the percentage of memory consumed and comparing it with the configured threshold value.

Enabling and Configuring MAPS

Enabling MAPS

MAPS can be enabled at any time.

Once MAPS is enabled, all Fabric Watch system monitoring commands, such as **system-monitor** or **threshold-monitor**, will return an error.

When you enable MAPS, you must be logged in to the primary node.

1. Enter global configuration mode on the device.

```
device# configure terminal
```

2. Enter RBridge ID configuration mode on the device.

```
device(config)# rbridge-id 1
```

3. Enter MAPS configuration mode on the device.

```
device(config-rbridge-id-1)# maps
```

4. Enable MAPS with a policy and action.

```
device(config-rbridge-id-1-maps)#  enable policy dflt_aggressive_policy actions RASLOG
```

5. Confirm the MAPS configuration is active.

```
device(config-rbridge-id-1-maps)# do show running-config rbridge-id 1 maps
rbridge-id 1
 maps
  enable policy dflt_conservative_policy
  enable actions RASLOG
```

For complete information on the options for the **enable policy** command, refer to the *Extreme Network OS Command Reference*.

Configuring MAPS

The following table lists the MAPS configuration tasks and the commands you use for these tasks.

Note: Actions should be configured globally in order for the actions in a custom policy to be effective.

TABLE 8 MAPS configuration tasks

Configuration task	Command
Enabling MAPS	**maps**
Enabling a policy	**enable policy**
Enabling or disabling actions at a global level	**enable action**
Sending alerts using e-mail	**email**

TABLE 8 MAPS configuration tasks (continued)

Configuration task	Command
Sending alerts using a relay IP address and a domain name	**relay**

Configuring MAPS alert targets

Configure the MAPS alerts destination targets for all email and relay messages.

You must separate multiple targets with a comma and include the complete e-mail address, IP address, or domain name. For example, admin@abc123.com is a valid e-mail address; admin@12 is not.

Use the no form of the **email** or **relay** command to remove the target information. For example, **no email webmaster@abc123.com** removes the given e-mail address from the MAPS configuration.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter RBridge ID configuration mode.

```
device(config)# rbridge-id 5
```

3. Enter MAPS configuration mode.

```
device(config-rbridge-id-5)# maps
```

4. Configure the destination e-mail addresses for MAPS alerts.

```
device(config-rbridge-id-5-maps)# email admin@abc123.com
evice(config-rbridge-id-5-maps)# email webmaster@abc123.com
```

5. Configure the destination relay IP address for MAPS alerts.

```
device(config-rbridge-id-5-maps)# relay 10.25.248.25  domainname abc123.com
```

Multiple threshold monitoring overview

Multiple threshold monitoring allows for early notification of issues before they potentially get worse. In addition, this allows administrator to prioritize the issues and efficiently resolve them, if needed, according to their severities.

Multiple threshold monitoring allows you to monitor for varying severity levels of an issue and trigger different actions at different levels. For example, you can configure MAPS to monitor for any change in CRC counters of a port against multiple threshold values at the same time:

- If a change in the CRC counters occurred in the one minute > 2 times, then trigger a RASLOG alert.
- If a change in the CRC counters occurred in the one minute > 5 times, then trigger an email alert and an SNMP trap.
- If a change in the CRC counters occurred in the one minute > 10 times, then fence the port.

MAPS takes different actions depending on the severity of the condition. This allows prioritizing more critical events, that are delivered through e-mail , trap, or fencing, over non-critical events that are delivered through RASLOG.

Monitoring across multiple time windows

You may need to monitor for spikes (which are the normal irregular behavior), as well as monitor for the non-critical but persistent issues. Taking the CRC counter as an example, you can have MAPS monitor for the following at same time:

- If a change in the CRC counters occurred in the last one minute > 5 times, then trigger an email alert and an SNMP trap.
- If a change in the CRC counters occurred in the last one day > 20 times, then trigger an email alert and a RASLOG alert.

This allows you to monitor for both severe and non-critical but persistent conditions, and provides better visibility into the behavior of the device, warning you of non-obvious issues that can degrade the performance of the fabric.

The example below demonstrates a typical multiple threshold example with fencing. For complete information on all threshold and fencing options, refer to the **threshold-monitor interface** command in the *Extreme Network OS Command Reference*.

```
device(config-rbridge-id-154)# threshold-monitor interface policy mypolicy type Ethernet area IFG alert
above highthresh-action fence raslog lowthresh-action email raslog
```

Monitoring IP storage

If an IP or iSCSI storage element is added to the fabric through an interface port, you can monitor the element using existing rules for similar elements by using the **device connectivity** command to add that interface to the ALL_IP_TARGETS or ALL_ISCSI_TARGETS group monitoring.

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 designates a tengigabit Ethernet port as being connected to iSCSI storage for MAPS.

```
device(config)# interface tengigabitethernet 1/2/5
device(conf-if-te-1/2/5)# device-connectivity iSCSI
```

NOTE

MAPS does not monitor Flexports configured as fibre channel ports.

MAPS Dashboard

MAPS dashboard overview

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

MAPS dashboard viewing

After a policy is activated, you can monitor the device status by using the **show maps dashboard** command. There are three primary views: a summary view, a detailed view (which includes historical data), and a history-only view.

Viewing the MAPS dashboard

The dashboard is a central feature of MAPS, providing at-a-glance views of device health status, and allowing you to manage devices and easily know if the device is functioning within the limits that does not degrade the performance.

Use the **show maps dashboard** command to view the dashboard. The view displays the rules and the conditions in the rules that contributed to the information shown in other categories. Refer to the *Extreme Network OS Command Reference* for details on the **show maps dashboard** command.

The output of the command is divided into five basic sections:

- Basic information about the dashboard
- A status report on the current health of the device
- A summary of the focus areas of the device
- A list of the rules currently affecting the health of the device
- A historical summary of the events on the device over the last 24 hours

```
device# show maps dashboard rbridge-id 10
--------------------------------------------------------------------------------
                        Dashboard for RbridgeId 10
--------------------------------------------------------------------------------

1 Dashboard Information:
========================

DB start time :                 Thu May 21 17:27:28 2015

2 Switch Health Report:
=======================

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


3.1 Summary Report:
===================
```

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


3.2 Rules Affecting Health:
===========================

Category(Rule Count)|RepeatCount|Rule Name                  |Execution Time   |Object           |Triggered
Value(Units)|
_____________________________________________________________________________________________________________
_____________
Security Violations(|2          |defSWITCHSEC_LV_0          |05/21/15 19:26:54|Switch           |1
Violations          |
3)                  |           |                           |                 |
|                     |
                    |           |                           |                 |Switch           |1
Violations          |
                    |1          |defSWITCHSEC_TELNET_0      |05/21/15 19:26:54|Switch           |1
Violations          |


3.3 History Data:
===============

Stats(Units)        Current             --/--/--            --/--/--            --/--/--
--/--/--
                    Port(val)           Port(val)           Port(val)           Port(val)
Port(val)
-------------------------------------------------------------------------------------------------------------
--
CRCALN(CRCs)        -                   -                   -                   -
-
RX_ABN_FRAME(Errors)-                   -                   -                   -                   -
RX_SYM_ERR(Errors)  -                   -                   -                   -                   -
RX_IFG(IFGs)        -                   -                   -                   -                   -

<output truncated for clarity>
```

MAPS Threshold Values

Thresholds overview

The following tables describe the default monitoring thresholds used by the Monitoring and Alerting Policy Suite (MAPS) for RASLog, SNMP, and e-mail alert messages.

FRU state thresholds

The following table lists the default Field Replaceable Unit (FRU) monitoring thresholds. All threshold values are absolute.

TABLE 9 FRU state thresholds

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
PS	In, Out, Off, Faulty	Same as Aggressive policy	Same as Aggressive policy	RASLOG, SNMP, EMAIL
Fan	In, Out, Off, Faulty	Same as Aggressive policy	Same as Aggressive policy	RASLOG, SNMP, EMAIL
SFP	In, Out, Off, Faulty	Same as Aggressive policy	Same as Aggressive policy	RASLOG, SNMP, EMAIL
Blade	In, Out, Off, Faulty	Same as Aggressive policy	Same as Aggressive policy	RASLOG, SNMP, EMAIL
WWN	On, Out, Off, Faulty	Same as Aggressive policy	Same as Aggressive policy	RASLOG, SNMP, EMAIL

Switch Policy Status thresholds

The following table lists the default Switch Policy Status monitoring thresholds. All threshold actions are triggered when they exceed the listed value. For thresholds with both an upper value and a lower value, the threshold action is triggered when it exceeds the upper value or drops below the lower value. These values apply to both marginal and critical thresholds.

TABLE 10 Switch Policy Status thresholds

Statistic	Aggressive policy	Actions	Moderate policy	Actions	Conservative policy	Actions
Bad Power	1 of 2	SW_CRITICAL, SNMP, EMAIL	1 of 2	Same as Aggressive policy	1 of 2	Same as Moderate policy
Bad Temp	1 of 2 2 of 4 6 of 8	Low threshold: SW_MARGINAL, SNMP, EMAIL	1 of 2	Same as Aggressive policy	1 of 2	Same as Moderate policy

TABLE 10 Switch Policy Status thresholds (continued)

Statistic	Aggressive policy	Actions	Moderate policy	Actions	Conservative policy	Actions
	(depending on device model)	High threshold: SW_CRITICAL, SNMP, EMAIL				
Bad Fan	1 of 2	Low threshold: SW_MARGINAL, SNMP, EMAIL High threshold: SW_CRITICAL, SNMP, EMAIL	1 of 2	Same as Aggressive policy	1 of 2	Same as Moderate policy
Flash Usage	90	RASLOG, SNMP, EMAIL	90	Same as Aggressive policy	90	Same as Moderate policy
Faulty Blade	1/-	Low threshold: SW_MARGINAL, SNMP, EMAIL High threshold: N/A	1/-	Same as Aggressive policy	1/-	Same as Moderate policy
Faulty WWN	-/1	Low threshold: N/A High threshold: SW_MARGINAL, SNMP, EMAIL	-/1	Same as Aggressive policy	-/1	Same as Moderate policy
Faulty SFM	1 of 2	Low threshold: SW_MARGINAL, SNMP, EMAIL High threshold: SW_CRITICAL, SNMP, EMAIL	1 of 2	Same as Aggressive policy	1 of 2	Same as Moderate policy
HA Sync	sync = 0	SW_MARGINAL, SNMP, EMAIL	sync = 0	Same as Aggressive policy	sync = 0	Same as Moderate policy

Security monitoring thresholds

The following table lists the default monitoring thresholds for security criteria. Unless noted otherwise, all thresholds are measured per minute and the actions are triggered when the thresholds are greater than the shown value.

The following table applies to RASLog, SNMP, and e-mail thresholds.

TABLE 11 Security monitoring thresholds

Statistics	Aggressive policy	Moderate policy	Conservative policy	Actions
Login Violations	0	2	4	RASLOG, SNMP, EMAIL
Telnet Violations	0	2	4	RASLOG, SNMP, EMAIL

System monitoring thresholds

The following table lists the names of the default system monitoring thresholds.

TABLE 12 System monitoring threshold names

Category	Threshold name
Port Health	CRCALN, RX_SYM_ERR, RX_ABN_FRAME,CURRENT, RXP, TXP, VOLTAGE, SFP_TEMP
Security Health	SEC_LV, SEC_TELNET
Switch Resource	TEMP, FLASH_USAGE, CPU, MEMORY_USAGE, ETH_MGMT_PORT_STATE
Switch Status Policy	BAD_PWR, BAD_TEMP, BAD_FAN, FLASH_USAGE, WWN_DOWN, DOWN_SFM, FAULTY_BLADE, HA_SYNC
FRU Health	PS_STATE, FAN_STATE, SFP_STATE, BLADE_STATE
Timebase	DAY, HOUR, MIN, NONE
Op	L, LE, G, GE, EQ
FRU states	ON, OFF, IN, OUT, FAULTY
Action	RASLOG, EMAIL, SNMP, SFP_MARGINAL, NONE
Temp	IN_RANGE, OUT_OF_RANGE
Ethernet Port State	UP, DOWN

Resource monitoring thresholds

The following table lists the default monitoring thresholds for resource criteria. All thresholds are measured per minute and the actions are triggered when the value is greater than the shown value.

The following table applies to both RASLog , SNMP, and e-mail thresholds.

TABLE 13 Resource monitoring thresholds

Statistics	Aggressive policy	Moderate policy	Conservative policy	Actions
Flash (percent used)	90	90	90	RASLOG, SNMP, EMAIL
CPU (percent used)	80	80	80	RASLOG, SNMP, EMAIL
Memory (percent used)	75	75	75	RASLOG, SNMP, EMAIL

Monitoring thresholds for SFP transceivers

The following tables list the default monitoring thresholds for SFP transceivers. All threshold actions are triggered when they exceed the listed value. For thresholds with both an upper value and a lower value, the threshold action is triggered when the value exceeds the upper value or drops below the lower value.

The following tables apply to RASLog, SNMP, and e-mail thresholds.

TABLE 14 SFP monitoring thresholds for ALL_1GSR_SFP

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
Current (amps)	12	12	12	RASLOG, SNMP, EMAIL
RXP (µw)	1122	1122	1122	RASLOG, SNMP, EMAIL
TXP (µw)	1000	1000	1000	RASLOG, SNMP, EMAIL

TABLE 14 SFP monitoring thresholds for ALL_1GSR_SFP (continued)

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
VOLTAGE (volts)	3000 through 3600	3000 through 3600	3000 through 3600	RASLOG, SNMP, EMAIL
TEMP (°C)	-5 through 90	-5 through 90	-5 through 90	RASLOG, SNMP, EMAIL

TABLE 15 SFP monitoring thresholds for ALL_1GLR_SFP

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
Current (amps)	85	85	85	RASLOG, SNMP, EMAIL
RXP (µw)	1995	1995	1995	RASLOG, SNMP, EMAIL
TXP (µw)	1585	1585	1585	RASLOG, SNMP, EMAIL
VOLTAGE (volts)	2970 through 3630	2970 through 3630	2970 through 3630	RASLOG, SNMP, EMAIL
TEMP (°C)	-5 through 90	-5 through 90	-5 through 90	RASLOG, SNMP, EMAIL

TABLE 16 SFP monitoring thresholds for ALL_10GLR_SFP

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
Current (amps)	85	85	85	RASLOG, SNMP, EMAIL
RXP (µw)	1995	1995	1995	RASLOG, SNMP, EMAIL
TXP (µw)	1585	1585	1585	RASLOG, SNMP, EMAIL
VOLTAGE (volts)	2970 through 3630	2970 through 3630	2970 through 3630	RASLOG, SNMP, EMAIL
TEMP (°C)	-5 through 90	-5 through 90	-5 through 90	RASLOG, SNMP, EMAIL

TABLE 17 SFP monitoring thresholds for ALL_10GUSR_SFP

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
Current (amps)	13	13	13	RASLOG, SNMP, EMAIL
RXP (µw)	2000	1995	1995	RASLOG, SNMP, EMAIL
TXP (µw)	2000	1585	1585	RASLOG, SNMP, EMAIL
VOLTAGE (volts)	2900 through 3700	2970 through 3630	2970 through 3630	RASLOG, SNMP, EMAIL
TEMP (°C)	-13 through 100	-5 through 90	-5 through 90	RASLOG, SNMP, EMAIL

TABLE 18 SFP monitoring thresholds for ALL_100GSR_SFP

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
Current (amps)	10	10	10	RASLOG, SNMP, EMAIL
RXP (µw)	2187	2187	2187	RASLOG, SNMP, EMAIL
TXP (µw)	2187	2187	2187	RASLOG, SNMP, EMAIL
VOLTAGE (volts)	2970 through 3600	2970 through 3600	2970 through 3600	RASLOG, SNMP, EMAIL
TEMP (°C)	-5 through 75	-5 through 75	-5 through 75	RASLOG, SNMP, EMAIL

TABLE 19 SFP monitoring thresholds for ALL_100GLR_SFP

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
Current (amps)	110	110	110	RASLOG, SNMP, EMAIL
RXP (µw)	4500	4500	4500	RASLOG, SNMP, EMAIL
TXP (µw)	4500	4500	4500	RASLOG, SNMP, EMAIL
VOLTAGE (volts)	3100 through 3500	3100 through 3500	3100 through 3500	RASLOG, SNMP, EMAIL

TABLE 19 SFP monitoring thresholds for ALL_100GLR_SFP (continued)

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
TEMP (°C)	-5 through 73	-5 through 73	-5 through 73	RASLOG, SNMP, EMAIL

Monitoring thresholds for QSFP transceivers and all other SFP transceivers

The following tables list the default monitoring thresholds for QSFP transceivers and all other SFP transceivers. All thresholds are triggered when a value exceeds the listed value. For thresholds with both an upper value and a lower value, the action is triggered when the reported value exceeds the upper threshold value or drops below the lower threshold value.

The following table applies to RASLog, SNMP, e-mail thresholds.

TABLE 20 ALL_QSFP_SR

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
Current (amps)	10	10	10	RASLOG, SNMP, EMAIL
RXP (µw)	2188	2188	2188	RASLOG, SNMP, EMAIL
TXP (µw)	N/A	N/A	N/A	RASLOG, SNMP, EMAIL
VOLTAGE (volts)	2970 to 3600	2970 to 3600	2970 to 3600	RASLOG, SNMP, EMAIL
TEMP (°C)	-5 to 75	-5 to 75	-5 to 75	RASLOG, SNMP, EMAIL

TABLE 21 ALL_QSFP_LR

Statistic	Aggressive policy	Moderate policy	Conservative policy	Actions
Current (amps)	80	80	80	RASLOG, SNMP, EMAIL
RXP (µw)	3380	3380	3380	RASLOG, SNMP, EMAIL
TXP (µw)	N/A	N/A	N/A	RASLOG, SNMP, EMAIL
VOLTAGE (volts)	2970 to 3630	2970 to 3630	2970 to 3630	RASLOG, SNMP, EMAIL
TEMP (°C)	-8 to 78	-8 to 78	-8 to 78	RASLOG, SNMP, EMAIL