



Alarm Filtering Support in the Cisco Entity Alarm MIB

First Published: August 22, 2005

Last Updated: February 27, 2007

The Alarm Filtering Support in the Cisco Entity Alarm MIB feature implements the alarm filter profile capability defined in CISCO-ENTITY-ALARM-MIB. Also implemented are configuration commands to control the severity of syslog messages and SNMP notifications triggered by the alarms.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Alarm Filtering Support in the Cisco Entity Alarm MIB](#)” section on page 20.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Alarm Filtering Support in the Cisco Entity Alarm MIB, page 2](#)
- [Restrictions for Alarm Filtering Support in the Cisco Entity Alarm MIB, page 2](#)
- [Information About Alarm Filtering Support in the Cisco Entity Alarm MIB, page 2](#)
- [How to Configure Alarm Filtering for Syslog Messages and SNMP Notifications, page 3](#)
- [Configuration Examples for Alarm Filtering Support in the Cisco Entity Alarm MIB, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Feature Information for Alarm Filtering Support in the Cisco Entity Alarm MIB, page 20](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005, 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Alarm Filtering Support in the Cisco Entity Alarm MIB

- SNMP is configured on your routing devices.
- Familiarity with the ENTITY-MIB and the CISCO-ENTITY-ALARM-MIB.

Restrictions for Alarm Filtering Support in the Cisco Entity Alarm MIB

- The CISCO-ENTITY-ALARM-MIB supports reporting of alarms for physical entities only. For line cards, alarms are reported at the physical interface or port level.

Information About Alarm Filtering Support in the Cisco Entity Alarm MIB

To configure alarm filtering in the Cisco Entity Alarm MIB, you should understand the following concepts:

- [CISCO-ENTITY-ALARM-MIB, page 2](#)
- [ceAlarmGroup, page 2](#)
- [ceAlarmFilterProfileTable, page 3](#)
- [ceAlarmFilterProfile, page 3](#)

CISCO-ENTITY-ALARM-MIB

The CISCO-ENTITY-ALARM-MIB provides a management client with the capability to monitor alarms generated by physical entities in a network that are identified in the entPhysicalTable of the Entity-MIB (RFC 2737). Examples of these physical entities are chassis, fans, modules, ports, slots, and power supplies. The management client interfaces with an SNMP agent to request access to objects defined in the CISCO-ENTITY-ALARM-MIB.

ceAlarmGroup

The ceAlarmGroup is a group in the CISCO-ENTITY-ALARM-MIB that defines objects that provide current statuses of alarms and the capability to instruct an agent to stop (cut off) signaling for any or all external audible alarms.

Following are the objects in ceAlarmGroup:

- ceAlarmCriticalCount
- ceAlarmMajorCount
- ceAlarmMinorCount
- ceAlarmCutoff

- `ceAlarmFilterProfile`
- `ceAlarmSeverity`
- `ceAlarmList`

ceAlarmFilterProfileTable

The `ceAlarmFilterProfileTable` filters alarms according to configured alarm lists. The filtered alarms are then sent out as SNMP notifications or syslog messages, based on the alarm list enabled for each alarm type. This table is defined in the CISCO-ENTITY-ALARM-MIB and implemented in the group `ceAlarmGroup`.

ceAlarmFilterProfile

An alarm filter profile controls the alarm types that an agent monitors and signals for a corresponding physical entity. The `ceAlarmFilterProfile` object holds an integer value that uniquely identifies an alarm filter profile associated with a corresponding physical entity. When the value is zero, the agent monitors and signals all alarms associated with the corresponding physical entity.

How to Configure Alarm Filtering for Syslog Messages and SNMP Notifications

This section contains the following tasks:

- [Configuring Alarm Filtering for Syslog Messages, page 3](#) (optional)
- [Configuring Alarm Filtering for SNMP Notifications, page 4](#) (optional)

Configuring Alarm Filtering for Syslog Messages

This task describes how to configure the alarm severity threshold for generating syslog messages. When you use this command, the alarm severity threshold is included in the running configuration and automatically applied when the configuration is reloaded.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `logging alarm [severity]`
4. `show facility-alarm status`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	logging alarm [severity] Example: Router(config)# logging alarm 2	Configures the alarm severity threshold for generating syslog messages. All alarms at and above this threshold are sent as syslog messages.
Step 4	show facility-alarm status Example: Router(config)# show facility-alarm status	Generates output that shows information about each alarm depending on the severity level that is set.

Configuring Alarm Filtering for SNMP Notifications

This task describes how to configure the alarm severity threshold for generating SNMP notifications. When you use this command, the alarm severity threshold is included in the running configuration and automatically applied when the configuration is reloaded.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps alarms** [severity]
4. **show facility-alarm status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	snmp-server enable traps alarms [severity] Example: Router(config)# snmp-server enable traps alarms 2	Configures the alarm severity threshold for generating SNMP notifications. All alarms at and above this threshold are sent as SNMP notifications.
Step 4	show facility-alarm status Example: Router(config)# show facility-alarm status	Generates output that shows information about each alarm depending on the severity level that is set.

Configuration Examples for Alarm Filtering Support in the Cisco Entity Alarm MIB

This section provides the following configuration examples:

- [Configuring Alarm Filtering for Syslog Messages: Example, page 5](#)
- [Configuring Alarm Filtering for SNMP Notifications: Example, page 6](#)

Configuring Alarm Filtering for Syslog Messages: Example

The following example shows how to configure an alarm filter for syslog messages:

```
Router# enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# logging alarm 2
Router(config)# exit
Router#
Router# show facility-alarm status

System Totals Critical: 1 Major: 0 Minor: 0
Source Severity Description [Index]
-----
Fa0/0 CRITICAL Physical Port Link Down [0]
Fa0/1 INFO Physical Port Administrative State Down [1]
AT6/0 INFO Physical Port Administrative State Down [8]
```

Configuring Alarm Filtering for SNMP Notifications: Example

The following example shows how to configure an alarm filter for SNMP notifications:

```
Router#
Router# enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# snmp-server enable traps alarms 2
Router(config)#
Router(config)# exit
Router#
Router# show facility-alarm status

System Totals Critical: 1 Major: 0 Minor: 0
Source Severity Description [Index]
-----
Fa0/0 CRITICAL Physical Port Link Down [0]
Fa0/1 INFO Physical Port Administrative State Down [1]
AT6/0 INFO Physical Port Administrative State Down [8]
```

Additional References

The following sections provide references related to the Alarm Filtering Support in the Cisco Entity Alarm MIB feature.

Related Documents

Related Topic	Document Title
Network management configuration tasks	Cisco IOS Network Management Configuration Guide , Release 12.4
Network management commands	Cisco IOS Network Management Command Reference , Release 12.4T

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
- ENTITY-MIB - CISCO-ENTITY-ALARM-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2737	Entity MIB (Version 2)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

-
- [show facility-alarm](#)
- [snmp-server enable traps](#)

show facility-alarm

To display the status of a generated alarm, use the `show facility-alarm` command in global configuration mode.

show facility-alarm {**status** [*severity*] | **relay**}

Syntax Description

status	Shows facility alarms by status and displays the settings of all user-configurable alarm thresholds.
<i>severity</i>	(Optional) String that identifies the severity of an alarm. The default severity level is informational, which shows all alarms. Severity levels are defined as the following: • 1—Critical. The condition affects service. • 2—Major. Immediate action is needed. • 3—Minor. Minor warning conditions. • 4—Informational. No action is required. This is the default.
relay	Shows facility alarms by relay.

Command Default

All alarms are shown.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.4(4)T	The <i>severity</i> argument was added in Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the PRE3 for the Cisco 10000 series router.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

When a severity level is configured, statuses of alarms at that level and higher are shown. For example, when you set a severity of major, all major and critical alarms are shown.

Examples

The following example shows output of the **show facility-alarm status** command:

```
Router# show facility-alarm status

System Totals  Critical:1  Major:0  Minor:0
```

```

Source          Severity      Description [Index]
-----
Fa0/0           CRITICAL      Physical Port Link Down [0]
Fa1/0           INFO          Physical Port Administrative State Down [1]

```

The following example shows output of a **show facility-alarm status** command with a severity level set at major:

```

Router# show facility-alarm status major

System Totals  Critical:1  Major:0  Minor:0

Source          Severity      Description [Index]
-----
Fa0/0           CRITICAL      Physical Port Link Down [0]

```

Table 1 describes the significant fields shown in the output.

Table 1 *show facility-alarm status Field Descriptions*

Field	Description
System Totals	Total number of alarms generated, identified by severity.
Source	Interface from which the alarm was generated.
Severity	Severity level of the alarm generated.
Description [Index]	Type of the alarm and the index of the alarm type. The index can be any number based on the number of alarm types that the device supports.

Related Commands

Command	Description
clear facility-alarm	Clears alarm conditions and resets the alarm contacts.
facility-alarm	Configures threshold temperatures for minor, major, and critical alarms.

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notification types that are available on your system, use the **snmp-server enable traps** command in global configuration mode. To disable all available SNMP notifications, use the **no** form of this command.

snmp-server enable traps [*notification-type*] [**vrrp**]

no snmp-server enable traps [*notification-type*] [**vrrp**]

Syntax Description

<i>notification-type</i>	(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled (if the no form is used). The notification type can be one of the following keywords: alarms—Enables alarm filtering to limit the number of syslog messages generated. Alarms are generated for the severity configured as well as for the higher severity values. - The <i>severity</i> argument is an integer or string value that identifies the severity of an alarm. Integer values are from 1 to 4. String values are critical, major, minor, and informational. The default is 4, or informational. Severity levels are defined as follows: 1—Critical. The condition affects service. 2—Major. Immediate action is needed. 3—Minor. Minor warning conditions. 4—Informational. No action is required. This is the default. config—Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is (1) ciscoConfigManEvent. dot1x—Enables IEEE 802.1x traps. This notification type is defined in the CISCO PAE MIB. ds0-busyout—Sends notification when the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This notification is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2), and the notification type is (1) cpmDS0BusyoutNotification. ds1-loopback—Sends notification when the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as (2) cpmDS1LoopbackNotification. dsp—Enables SNMP digital signal processing (DSP) traps. This notification type is defined in the CISCO-DSP-MGMT-MIB. dsp oper-state—Sends a DSP notification made up of both a DSP ID that indicates which DSP is affected and an operational state that indicates whether the DSP has failed or recovered. entity—Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as (1) entConfigChange.
--------------------------	---

- **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is (1) cHsrpStateChange.
- **ipmulticast**—Controls IP multicast notifications.
- **modem-health**—Controls modem-health notifications.
- **rsvp**—Controls Resource Reservation Protocol (RSVP) flow change notifications.
- **tty**—Controls TCP connection notifications.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my, and the notification is enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification.

Note For additional notification types, see the Related Commands table.

vrp	(Optional) Specifies the Virtual Router Redundancy Protocol (VRRP).
------------	---

Command Default

No notifications controlled by this command are sent.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(2)T	The rsvp notification type was added in Cisco IOS Release 12.0(2)T.
12.0(3)T	The hsrp notification type was added in Cisco IOS Release 12.0(3)T.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.3(11)T	The vrp notification type was added in Cisco IOS Release 12.3(11)T.
12.4(4)T	Support for the alarms notification type and <i>severity</i> argument was added in Cisco IOS Release 12.4(4)T. Support for the dsp and dsp oper-state notification types was added in Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The dot1x notification type was added in Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

For additional notification types, see the Related Commands table for this command.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [traps | informs] command.

To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

Most notification types are disabled by default but some cannot be controlled with the **snmp-server enable traps** command.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example shows how to configure an alarm severity threshold of 3:

```
Router# snmp-server enable traps alarms 3
```

The following example shows how to enable the generation of a DSP operational state notification from the command-line interface (CLI):

```
Router(config)# snmp-server enable traps dsp oper-state
```

The following example shows how to enable the generation of a DSP operational state notification from a network management device:

```
setany -v2c 1.4.198.75 test cdspEnableOperStateNotification.0 -i 1
cdspEnableOperStateNotification.0=true(1)
```

The following example shows how to send no traps to any host. The Border Gateway Protocol (BGP) traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host user1 public isdn
```

The following example shows how to enable the router to send all inform requests to the host at the address myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

The following example shows that VRRP will be used as the protocol to enable the traps:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c vrrp
```

The following example shows how to send IEEE 802.1x MIB traps to the host “myhost.domain.com” using the community string defined as public:

```
Router(config)# snmp-server enable traps dot1x
Router(config)# snmp-server host myhost.domain.com traps public
```

Related Commands

Command	Description
snmp-server enable traps atm pvc	Enables ATM PVC SNMP notifications.
snmp-server enable traps atm pvc extension	Enables extended ATM PVC SNMP notifications.
snmp-server enable traps bgp	Enables BGP server state change SNMP notifications.
snmp-server enable traps calltracker	Enables Call Tracker callSetup and callTerminate SNMP notifications.
snmp-server enable traps envmon	Enables environmental monitor SNMP notifications.
snmp-server enable traps frame-relay	Enables Frame Relay DLCI link status change SNMP notifications.
snmp-server enable traps ipsec	Enables IPsec SNMP notifications.
snmp-server enable traps isakmp	Enables IPsec ISAKMP SNMP notifications.
snmp-server enable traps isdn	Enables ISDN SNMP notifications.
snmp-server enable traps memory	Enables memory pool and buffer pool SNMP notifications.
snmp-server enable traps mpls ldp	Enables MPLS LDP SNMP notifications.
snmp-server enable traps mpls traffic-eng	Enables MPLS TE tunnel state-change SNMP notifications.
snmp-server enable traps mpls vpn	Enables MPLS VPN specific SNMP notifications.
snmp-server enable traps repeater	Enables RFC 1516 hub notifications.
snmp-server enable traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server enable traps syslog	Enables the sending of system logging messages via SNMP.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp trap illegal-address	Issues an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router.
vrrp shutdown	Disables a VRRP group.

Feature Information for Alarm Filtering Support in the Cisco Entity Alarm MIB

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for Alarm Filtering Support in the Cisco Entity Alarm MIB

Feature Name	Releases	Feature Information
Alarm Filtering Support in the Cisco Entity Alarm MIB	12.4(4)T 12.2(33)SRB	The Alarm Filtering Support in the Cisco Entity Alarm MIB feature implements the alarm filter profile capability defined in CISCO-ENTITY-ALARM-MIB. Also implemented are configuration commands to control the severity of syslog messages and SNMP notifications triggered by the alarms. This feature was introduced in Cisco IOS Release 12.4(4)T. This feature was integrated into Cisco IOS Release 12.2(33)SRB.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005, 2007 Cisco Systems, Inc. All rights reserved.