DSP Operational State Notifications

The DSP Operational State Notifications feature enables notifications to be generated when digital signaling processor (DSP) failure and recovery events occur. These notifications help facilitate troubleshooting and lessen downtime.

This feature module describes updates to the Cisco DSP Management MIB (CISCO-DSP-MGMT-MIB) for enabling and generating DSP operational state notifications. Also described is how to enable the feature either using the command-line interface (CLI) or by modifying settings at the network management device.

History for the DSP Operational State Notifications Feature

Release	Modification
12.4(4)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

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

Prerequisites for DSP Operational State Notifications

- Familiarity with the CISCO-DSP-MGMT-MIB and Simple Network Management Protocol (SNMP).

Information About DSP Operational State Notifications

To enable DSP operational state notifications when a DSP fails and when it recovers, you should understand the following concepts:

CISCO-DSP-MGMT-MIB

The CISCO-DSP-MGMT-MIB monitors DSP resources and status.

DSP Operational State Notification

A DSP notification consists of a DSP ID that indicates which DSP is affected and an operational state that indicates whether the DSP has failed or recovered.

When this feature is configured using the **snmp-server enable traps dsp oper-state** command, a notification is generated when a single DSP fails instead of after all DSPs have failed. For example, a DSP fails, and you lose your voice calls. In a DSP failure notification, the problem is identified. If no DSP failure notification is generated, a network management station (NMS) has to poll the router for configuration and status information to diagnose the problem.

Benefits of DSP Operational State Notifications

The DSP Operational State Notifications feature enables the generation of notifications when DSP failure and recovery events occur. These notifications help facilitate troubleshooting and lessen downtime because an NMS does not have to poll the router for configuration and status information to diagnose the problem..

How to Enable DSP Operational State Notifications

DSP operational state notifications can be configured in two ways. To configure these notifications, perform one of the following tasks:

Enabling DSP Operational State Notifications from the CLI

Perform this task to enable DSP operational state notifications from the CLI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps** [*notification type*][**vrrp**]
4. **end**
5. **exit**

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** [*notification-type*] [**vrrp**] **Example:** `Router(config)# snmp-server enable traps dsp oper-state`	Enables the generation of DSP notifications made up of the DSP ID that indicates which DSP is affected and the operational state that indicates whether the DSP has failed or recovered.
Step 4	**end** **Example:** `Router(config)# end`	Returns the device to privileged EXEC mode.
Step 5	**exit** **Example:** `Router# exit`	Returns the device to user EXEC mode.

Enabling DSP Operational State Notifications Using an SNMP Application

Perform this task to enable DSP operational state notifications using your SNMP application.

SUMMARY STEPS

1. **setany -v2c 1.4.198.75 test cdspEnableOperStateNotification.0 -i 1**

DETAILED STEPS

Step 1 **setany -v2c 1.4.198.75 test cdspEnableOperStateNotification.0 -i 1**

This SNMP command sets the enable operation state notification object identifier (OID) to true.

After entering this command, the system returns the following response:
cdspEnableOperStateNotification.0 = true(1).

Configuration Examples for DSP Operational State Notifications

Enabling DSP Operational State Notifications Using the CLI: Example

The following sample configuration code shows how to enable DSP operational state notifications using the CLI:

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

The following example shows a typical DSP failure notification:

```
*Jun 1 02:37:05.720:SNMP:V1 Trap, ent cdspMIBNotificationPrefix, addr 1.4.198.75, gentrap
6, spectrap 2
cdspOperState.37 = 2
entPhysicalEntry.7.37 = DSP (C549) 1/2/0
```

The following example shows a typical DSP recover notification:

```
*Jun 1 02:37:10.820:SNMP:V1 Trap, ent cdspMIBNotificationPrefix, addr 1.4.198.75, gentrap
6, spectrap 2
cdspOperState.37 = 1
entPhysicalEntry.7.37 = DSP (C549) 1/2/0
```

Enabling DSP Operational State Notifications Using an SNMP Application: Example

The following sample configuration code shows how to enable DSP operational state notifications from your SNMP application:

In your SNMP application, you type the following command:

```
setany -v2c 1.4.198.75 test cdspEnableOperStateNotification.0 -i 1
```

The application shows the following response:

```
cdspEnableOperStateNotification.0 = true(1)
```

Additional References

The following sections provide references related to the DSP Operational State Notifications 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 12.4

MIBs

MIB	MIBs Link
• CISCO-DSP-MGMT-MIB • CISCO-DSP-MGMT-CAPABILITY-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

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents the following modified command only.

- **snmp-server enable traps**

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

notification-type	(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: • **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. • **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.
vrrp	(Optional) Specifies the Virtual Router Redundancy Protocol (VRRP).

Command Default

All notification types controlled by this command are enabled.

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.
12.3(11)T	The *vrrp* notification type was added in Cisco IOS Release 12.3(11)T.
12.4(4)T	Support for the *dsp* and *dsp oper-state* notification types was added in Cisco IOS Release 12.4(4)T.

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.

If you do not enter a **snmp-server enable traps** command, no notifications controlled by this command are sent. 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 enable the generation of a DSP operational state notification from 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 enable the router to send Frame Relay and environmental monitor traps to the host myhost.cisco.com using the community string public:

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

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
```

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.

Command	Description
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.