

Dual Redundant Internal Power Supply: System Management

This document describes the system management and troubleshooting commands for the Cisco AS5300 Dual Redundant Internal Power Supply feature. In general, this document also applies to the redundant power supply feature available for the Cisco 3600 series and certain other Cisco products. For more information, see the “Platforms” section on page 2. The following topics are included:

- Feature Summary on page 1
- Platforms on page 2
- Prerequisites on page 3
- Supported MIBs and RFCs on page 3
- Functional Description on page 3
- Configuration Tasks on page 4
- Command Reference on page 6
- What to Do Next on page 17

Note This product and document are still in development. Some portions of this document might not be complete and are subject to change.

Feature Summary

The dual redundant internal power supply feature for the Cisco AS5300 provides optional DC or AC dual internally-redundant power supplies for the Cisco AS5300 chassis. Two versions are available:

- Dual AC input, 300-watt—The dual redundant AC power supply for the Cisco AS5300 has separate power cords.
- Dual DC input, 300-watt

Cisco IOS software commands manage the power supply, providing the following capability:

- Designate SNMP trap (message) address
- Enable/disable sending SNMP traps
- Send SNMP traps and alarms when a failure or recovery from the unit is detected
- Display of the SNMP environment monitor statistics

There are no configuration commands to enable the dual redundant internal power supply event monitoring; it is ON by default. However, SNMP traps can be enabled for environment events so that Cisco IOS software sends traps based on power supply failure or recovery events. The only configuration required is to turn on the sending of SNMP traps for environment monitoring and to specify an SNMP server to which the traps are sent. Events and status are displayed through console messages and the **show environment** command.

Cisco AS5300 software is implemented as two subsystems:

- The “env” subsystem monitors for failure events, displays console messages, and invokes functions to send SNMP traps.
- The “envmib” adds SNMP support for maintaining MIB tables and routines to send traps.

Benefits

This feature provides higher reliability, power-load balancing, and SNMP status messages.

Despite any changes in environmental status, the Cisco IOS software will always attempt to continue running normally and passing packets, while at the same time providing as much information as possible through the user interfaces.

Restrictions

This feature works in conjunction with an optional hardware module. Make sure your access server has the module installed.

Cisco AS5300 software maintains only the current status of the redundant power supply unit. It does not keep track of the history of Redundant Power Supply (RPS) unit failure events.

CISCO-ENVMON-MIB and CISCO-ACCESS-ENVMON-MIB are generally supported, however, the complete status MIB tables defined in CISCO-ENVMON-MIB are not supported due to a limitation in the power supply units. For example, the power supply units do not send current/threshold values, such as current voltage and current temperature, to the motherboard for failure events.

Platforms

This document describes the dual redundant power supply feature as supported by the Cisco AS5300.

This feature is also supported on these platforms:

- Cisco 3600 routers (3620 and 3640)
- Cisco 7200 series
- Cisco 12000 series

The information provided by the **show environment** command in this feature is a subset of the command already implemented on the Cisco 7200 series and the Cisco 12000 series. The software support for the Cisco 3620 and the Cisco 3640 routers that have a RPS installed is similar but is limited by the router series registers. Although the Cisco 3600 series routers RPS can be installed in other Access platforms, such as the Cisco 4000 series and the Cisco 2500 series, the latter platforms do not provide all the features described in this document.

Prerequisites

The following Cisco IOS releases fully support the redundant power supply:

- 11.3(6)T and later
- 11.3(6)AA and later
- 12.0(1) and later

If you use a Cisco AS5300 motherboard with an older Cisco IOS version, you can use the redundant power supply with older releases for power-load balancing purposes only.

Supported MIBs and RFCs

Whenever Cisco IOS software detects a failure or recovery event from the DRPS unit, it sends an SNMP trap to the configured SNMP server. Unlike console messages, only one SNMP trap is sent when the failure event is first detected. Another trap is sent when the recovery is detected.

Cisco AS5300 DRPS software reuses the MIB attributes and traps defined in CISCO-ENVMON-MIB and CISCO-ACCESS-ENVMON-MIB. CISCO-ENVMON-MIB is supported by all Cisco routers with RPS units, and CISCO-ACCESS-ENVMON-MIB is supported by the Cisco 3600 series routers.

- A power supply trap defined in CISCO-ENVMON-MIB is sent when a failure is detected and when a failure recovery occurs for the following events: input voltage fail, DC output voltage fail, thermal fail, and multiple failure events.
- A fan failure trap defined in CISCO-ENVMON-MIB is sent when a fan failure or recovery event is detected by Cisco IOS software.
- A temperature trap defined in CISCO-ACCESS-ENVMON-MIB is sent when a board overtemperature condition is detected by Cisco IOS software.
- CISCO-ACCESS-ENVMON-MIB is extended to define an overvoltage trap. A similar trap is defined in CISCO-ENVMON-MIB, but it requires the `ciscoEnvMonVoltageStatusValue` in `varbinds`. This value indicates the current value of the voltage in the redundant power supply. With Cisco AS5300 redundant power supply units, the current voltage value is not sent to the motherboard. The CISCO-ACCESS-ENVMON-MIB is extended to support overvoltage trap with new `varbinds`.
- CISCO-ENVMON-MIB is extended to add a new enumerated value, `internalRedundant(5)`, for MIB attribute `ciscoEnvMonSupplySource`. This is used to identify a Cisco AS5300 redundant power supply unit.

For descriptions of supported MIBs and how to use MIBs, see Cisco's MIB Web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Functional Description

The dual redundant power supply operates automatically. There are three ways to check the status of the power supply unit:

- Watch the console for messages
- Use the **show environment** command
- Configure SNMP to send trap messages to an SNMP management console

Messages are displayed on the console for each failure event when it is detected and are repeated each minute until the problem is corrected. When the Cisco AS5300 detects a recovered failure, another message is displayed on the console indicating the recovery. Table 1 shows the RPS failure events and the console messages they produce.

Table 1 Dual Redundant Power Supply Messages

Event	Failure and Recovery Messages
Input Voltage Fail/Recovery	System detected Redundant Power System Input Voltage Failure condition. Redundant Power System Input Voltage condition is now normal
DC Output Voltage Fail/Recovery	System detected Redundant Power System DC Output Voltage Failure condition. Redundant Power System DC Output Voltage condition is now normal.
Thermal Fail/Recovery	System detected Redundant Power System THERMAL FAIL condition. Redundant Power System THERMAL condition is now normal.
Fan Fail/Recovery	System detected Redundant Power System FAN FAIL condition. Redundant Power System FAN condition is now normal.
Overvoltage Condition/Recovery	System detected Redundant Power System OVERVOLTAGE condition. Redundant Power System VOLTAGE condition is now normal.
Multiple Failure Condition/Recovery	There is more than one failure with the Redundant Power System; please resolve problems immediately. The Redundant Power System is operating normally.
Board Overtemperature/Recovery	System detected OVERTEMPERATURE condition. Please resolve cooling problem immediately! System temperature is now normal.

Note One of the events tracked in the ENVMON MIB is the Cisco AS5300 motherboard overtemperature. Motherboard overtemperature was monitored in earlier Cisco IOS releases. This release enables the Cisco AS5300 to send SNMP traps for this event.

The quickest way to display a summary report of the RPS status is to enter the **show environment** command at the console. This command is described in “show environment” on page 7.

To report RPS events to an SNMP management console, you need to configure SNMP as described in the next section. When SNMP is configured and the Cisco IOS software detects a failure or recovery from the redundant power supply unit, it sends an SNMP message to the configured SNMP server. Unlike messages that are sent to the console every minute, only one SNMP message is sent when the failure is first detected; and another one is sent when the recovery is detected.

Configuration Tasks

This section describes how to configure the Cisco AS5300 to send SNMP traps to an SNMP management console. It includes the following tasks:

- Configuring SNMP
- Verifying the SNMP configuration
- Troubleshooting tips

Use this section to manage your Cisco AS5300 universal access server to use SNMP traps (messages). If you do not want to implement SNMP traps, skip this section.

Configure

The following table shows how to use the redundant power supply feature commands to configure the feature.

Step	Command	Purpose
1	5300> enable Password: <password> 5300#	Enter enable mode (also called privileged EXEC mode). Enter the password. You have entered enable mode when the prompt changes to 5300#.
2	5300# configure term 5300(config)#	Enter the configuration mode. (Note the prompt change.)
3	5300(config)# snmp-server enable traps envmon 5300(config)#	Begin sending traps that monitor the environment.
4	5300(config)# snmp-server host IP address community string 5300(config)#	Configure the Cisco AS5300 to send SNMP traps to the configured IP address and the defined the community string in the SNMP trap.
5	5300(config)# exit 5300#	Exit configuration mode.
6	5300# write memory	Save the configuration to NVRAM.

Verify

To verify you have enabled sending SNMP traps for redundant power supply events:

- Enter the **show running-config** command and note that **envmon** is enabled:

```
5300# show running-config
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname as5300
!
ip subnet-zero
!
!
interface Ethernet0
 ip address 1.16.44.23 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0
 no ip address
 no ip directed-broadcast
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0
```

```
ip route 223.255.254.0 255.255.255.0 Ethernet0
!
snmp-server community public RO
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps frame-relay
snmp-server enable traps syslog
snmp-server host 172.22.19.7 traps public
!
line con 0
  transport input none
line aux 0
line vty 0 4
  login
!
end
```

Tips

If you are having trouble:

- Verify that you installed the redundant power supply unit properly.
- Verify that you entered the **snmp-server** commands (mentioned in the “Configure” section) properly.

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 11.3 and 12.0 command references.

This section describes the following commands:

- **show environment**
- **snmp-server enable traps**
- **snmp-server host**

show environment

To display the SNMP environment statistics for the Cisco AS5300 Dual Redundant Internal Power Supply, use the **show environment** privileged EXEC command.

show environment

Syntax Description

When used on the Cisco AS5300, this command has no keywords or arguments.

Default

This command always displays the redundant internal power supply statistics in the same format.

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. It has been modified for the Cisco AS5300 for Cisco IOS Release 11.3(6)AA.

The information is displayed on the console only; it is not logged to a file.

For information on how this command is used with Cisco IOS 12.0 software on the Cisco 7000 series, Cisco 7200 series, Cisco 7500 series, and Cisco 12000 series Gigabit Switch Router, go to Cisco Connection Online (CCO) at <http://www.cisco.com>, or the Cisco Documentation CD-ROM.

The CCO path is:

Cisco Connection Online: Products and Ordering: Cisco Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References: Configuration Fundamentals Command Reference: System Management Commands: Troubleshooting Commands

To access platform documents on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References: Configuration Fundamentals Command Reference: System Management Commands: Troubleshooting Commands

For information on how this command is used with Cisco IOS 11.3 software on the Cisco 7000 series, Cisco 7200 series, Cisco 7500 series, and Cisco 12000 series Gigabit Switch Router, go to Cisco Connection Online (CCO) at <http://www.cisco.com>, or the Cisco Documentation CD-ROM.

The CCO path is:

Cisco Connection Online: Products and Ordering: Cisco Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 Configuration Guides, Command References: System Management: Troubleshooting Commands

To access platform documents on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 Configuration Guides, Command References: System Management: Troubleshooting Commands

Example

The following is sample output from the **show environment** command:

```
AS5300# show environment
Power Supply:
Redundant Power System is present.
RPS Input Voltage status: normal
RPS Output Voltage status: normal
RPS Fan status: normal
RPS Thermal status: normal
RPS OverVoltage status: normal
Board Temperature: normal.
AS5300#
```

Note All the above status reports will show either normal or failure. Thermal status refers to the power supply. Board Temperature refers to the motherboard. If more than one parameter displays failure, a separate multiple failure message is reported. For more information, see the “Functional Description” section.

Related Commands

- show environment**
- snmp-server host**
- snmp-server enable traps**

snmp-server enable traps

To enable the router to send SNMP traps and informs, use the `snmp-server enable traps` global configuration command. Use the `no` form of this command to disable SNMP notifications.

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

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

Syntax Description

notification-type

(Optional) Type of notification to enable. If no type is specified, all notifications are sent (including the `envmon` and repeater notifications). The notification type can be one of the following keywords:

- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **config**—Sends configuration notifications.
- **entity**—Sends Entity MIB modification notifications.
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. When the `envmon` keyword is used, you can specify a notification-option value.
- **frame-relay**—Sends Frame Relay notifications.
- **isdn**—Sends Integrated Services Digital Network (ISDN) notifications. When the `isdn` keyword is used on Cisco 1600 series routers, you can specify a notification-option value.
- **repeater**—Sends Ethernet hub repeater notifications. When the `repeater` keyword is selected, you can specify a notification-option value.
- **rtr**—Sends response time reporter (RTR) notifications.
- **snmp**—Sends Simple Network Management Protocol (SNMP) notifications. When the `snmp` keyword is used, you can specify a notification-option value.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the `logging history level` command.

notification-option

(Optional) When the **envmon** keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: **voltage**, **shutdown**, **supply**, **fan**, and **temperature**.

When the **isdn** keyword is used, you can specify the **call-information** keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the **isdnu-interface** keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem.

When the **repeater** keyword is used, you can specify the **repeater** option. If no option is specified, all repeater notifications are enabled. The option can be one or more of the following keywords:

- **health**—Enables IETF Repeater Hub MIB (RFC 1516) health notification.
- **reset**—Enables IETF Repeater Hub MIB (RFC 1516) reset notification.

When the **snmp** keyword is used, you can specify the **authentication** option to enable SNMP Authentication Failure notifications. (The **snmp-server enable traps snmp authentication** command replaces the **snmp-server trap-authentication** command.) If no option is specified, all SNMP notifications are enabled.

Defaults

This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command.

If you enter this command with no notification-type keywords, the default is to enable all notification types controlled by this command.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command is useful for disabling notifications that are generating a large amount of uninteresting or useless noise.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order 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. In order to enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

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. In order to send notifications, you must configure at least one **snmp-server host** command.

For a host to receive a notification controlled by this command, both the **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. If the notification type is not controlled by this command, just the appropriate **snmp-server host** command must be enabled.

The notification types used in this command all have an associated MIB object that allows them to be globally enabled or disabled. Not all of the notification types available in the **snmp-server host** command have notificationEnable MIB objects, so some of these cannot be controlled using the **snmp-server enable** command.

Examples

The following example enables the router to send all traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

The following example enables the router to send Frame Relay and environmental monitor traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps frame-relay
snmp-server enable traps envmon temperature
snmp-server host myhost.cisco.com public
```

snmp-server enable traps

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps.

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

The following example enables the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

show environment

snmp-server host

snmp-server informs

snmp-server trap-source

snmp trap illegal-address

snmp-server host

Use the **snmp-server host** command in global configuration mode to specify the SNMP server host to which you want to send traps. Use to **no** form of the command to remove the specified host.

```
snmp-server host ip-address [traps | informs] [version { 1 | 2c}] community-string [udp-port port]  
[notification-type]
```

```
no snmp-server host ip-address [traps | informs]
```

Syntax Description

<i>IP-address</i>	The IP address of the server that you want to receive the SNMP messages.
traps	(Optional) Send SNMP traps to this host. This is the default.
informs	(Optional) Send SNMP informs to this host.
version	(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps. <ul style="list-style-type: none">• 1—SNMPv1. This option is not available with informs.• 2c—SNMPv2C.
<i>community-string</i>	Identifies the management community to which the sending device belongs.
udp-port <i>port</i>	UDP port of the host to use. The default is 162.

notification-type

(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords:

- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **config**—Sends configuration notifications.
- **dspu**—Sends downstream physical unit (DSPU) notifications.
- **entity**—Sends Entity MIB modification notifications.
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **frame-relay**—Sends Frame Relay notifications.
- **isdn**—Sends Integrated Services Digital Network (ISDN) notifications.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
- **rptr**—Sends standard repeater (hub) notifications.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rtr**—Sends response time reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLLC notifications.
- **snmp**—Sends Simple Network Management Protocol (SNMP) notifications defined in RFC 1157.
- **stun**—Sends serial tunnel (STUN) notifications.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command.
- **tty**—Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes.
- **x25**—Sends X.25 event notifications.

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no version keyword is present, the default is version 1. If no traps or informs keyword is present, traps are enabled.

The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. In order to disable informs, use the **no snmp-server host informs** command.

Command Mode

Global configuration mode

Usage Guidelines

This command first appears in Cisco IOS Release 10.0.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

A notification-type option's availability depends on the router type and Cisco IOS software features supported on the router. For example, the envmon notification-type is available only if the environmental monitor is part of the system.

Examples

The following example sends the SNMP traps defined in RFC 1157 to the host specified by the name myhost.cisco.com. The community string is defined as comaccess.

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

The following example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
snmp-server enable traps
snmp-server host 172.30.2.160 public snmp envmon
```

The following example enables the router to send all traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host.

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

The following example enables the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

show environment

snmp-server enable traps

snmp-server informs

snmp-server trap-source

snmp-server trap-timeout

snmp trap link-status

What to Do Next

For more information on the Cisco AS5300, go to Cisco Connection Online (CCO) at <http://www.cisco.com>, or the Cisco Documentation CD-ROM.

The CCO path is:

Cisco Connection Online: Products and Ordering: Cisco Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300

To access platform documents on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300

