



Memory Pool—SNMP Notification Support

First Published: November 3, 2003

Last Updated: July 26, 2007

This feature adds command-line interface (CLI) commands to enable SNMP notifications for the Cisco Enhanced Memory Pool MIB (CISCO-ENHANCED-MEMPOOL-MIB).

History for the Memory Pool—SNMP Notification Support Feature

Release	Modification
12.3(4)T	This feature was introduced.
12.2(22)S	This feature was integrated into Cisco IOS 12.2(22)S.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.

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

- [Prerequisites for Memory Pool—SNMP Notification Support, page 2](#)
- [Restrictions for Memory Pool—SNMP Notification Support, page 2](#)
- [Information About Memory Pool—SNMP Notification Support, page 2](#)
- [How to Enable Memory Pool—SNMP Notification Support, page 2](#)
- [Configuration Examples for Memory Pool—SNMP Notification Support, page 3](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)



Corporate Headquarters:

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

© 2003–2004, 2006–2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Memory Pool—SNMP Notification Support

Before you can compile CISCO-ENHANCED-MEMPOOL-MIB, you need to compile the following MIBs in the order listed:

1. SNMPv2-SM (SNMP configuration MIB)
2. SNMPv2-TC (SNMP configuration MIB)
3. SNMPv2-CONF (SNMP configuration MIB)
4. SNMP-FRAMEWORK-MIB (SNMP configuration MIB)
5. CISCO-SMI (SNMP configuration MIB)
6. ENTITY-MIB (core MIB)
7. CISCO-ENHANCED-MEMPOOL-MIB (infrastructure MIB)

All MIBs used on Cisco devices are available through Cisco.com at <http://www.cisco.com/go/mibs>.

Restrictions for Memory Pool—SNMP Notification Support

Access to the MIB is restricted to a read-only level.

Information About Memory Pool—SNMP Notification Support

The CISCO-ENHANCED-MEMPOOL-MIB module describes SNMP objects that enable users to remotely monitor the memory pool statistics of all physical entities, such as line cards and route processors, in a managed device. This is particularly useful for high-end routers that may have a large number of line cards. Beginning in Cisco IOS Release 12.3(4)T, the MIB has been enhanced to provide buffer pool and buffer cache statistics.

In addition to the statistics provided by the MIB, SNMP notifications (traps or informs) can be configured to be sent when the maximum number of memory buffers changes (in other words, when a new buffer peak is reached).

How to Enable Memory Pool—SNMP Notification Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps memory [bufferpeak]**
4. **snmp-server host**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	snmp-server enable traps memory [bufferpeak] Example: Router(config)# snmp-server enable traps memory bufferpeak	Enables only buffer peak notifications (traps or informs) in the CISCO-ENHANCED-MEMPOOL-MIB.
Step 4	snmp-server host {hostname ip-address} [traps informs] [version {1 2c 3 [auth noauth priv]]] community-string [udp-port port] [notification-type] [vrf vrf-name] Example: Router(config)# snmp-server host NMS-host1.example.com community1 memory	Enables buffer peak notifications to be sent to the specified host.

Configuration Examples for Memory Pool—SNMP Notification Support

This section provides the following configuration example:

- [Enabling Memory Pool—SNMP Notification Support: Example](#)

Enabling Memory Pool—SNMP Notification Support: Example

In the following example, all available memory-related SNMP notifications are enabled and configured to be sent as informs to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps memory bufferpeak
Router(config)# snmp-server host myhost.cisco.com informs version 3 public memory
```

Note that as of this release, only the buffer peak memory notification type is available. Additional memory notification type keywords may be added in future releases.

Additional References

The following sections provide references related to the Memory Pool—SNMP Notification Support feature.

Related Documents

Related Topic	Document Title
Memory buffers	<i>Buffer Tuning</i> (Cisco Tech Note 15091) http://www.cisco.com/warp/public/63/buffertuning.html
SNMP Configuration	<i>Configuring SNMP Support</i> http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcprt3/fcf014.htm

Standards

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

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> CISCO-ENHANCED-MEMPOOL-MIB.my (Rev 2.3) 	<p>The Cisco Enhanced Memory Pool MIB module was updated with new objects in Release 12.3(4)T to provide information on Buffer Pools and Buffer Cache Pools.</p> <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

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

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 modified commands only.

- [snmp-server enable traps memory](#)
- [snmp-server host](#)

snmp-server enable traps memory

To enable a device to send Simple Network Management Protocol (SNMP) notifications when memory pool buffer usage reaches a new peak, use the **snmp-server enable traps memory** command in global configuration mode. To stop notifications from being generated, use the **no** form of this command.

snmp-server enable traps memory [**bufferpeak**]

no snmp-server enable traps memory [**bufferpeak**]

Syntax Description

bufferpeak (Optional) Specifies memory buffer peak notifications.

Command Default

SNMP notifications in the MEMPOOL-MIB are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables memory buffer peak (cempMemBufferNotify) notifications. When they are enabled, these notifications are sent when the value of the maximum number of buffer objects changes.

In current releases of Cisco IOS software, this command has the same behavior whether you use or omit the **bufferpeak** keyword.

The cempMemBufferNotify notification type is defined as {cempMIBNotifications 1} in the CISCO-ENHANCED-MEMPOOL-MIB. For a complete description of this notification and additional MIB functions, see the CISCO-ENHANCED-MEMPOOL-MIB.my file, available on Cisco.com at <http://www.cisco.com/go/mibs/>.

Examples

In the following example all available memory related SNMP notifications are enabled and configured to be sent as informs to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps memory
Router(config)# snmp-server host myhost.cisco.com informs version 3 public memory
```

Related Commands	Command	Description
	show buffers	Displays memory buffer pool related information.
	show memory	Displays memory pool related information.
	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 recipient (host) of the notifications.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

```
snmp-server host {hostname | ip-address} [vrf vrf-name] [traps | informs] [version {1 | 2c | 3
[auth | noauth | priv]}] community-string [udp-port port] [notification-type]
```

```
no snmp-server host {hostname | ip-address} [vrf vrf-name] [traps | informs] [version {1 | 2c | 3
[auth | noauth | priv]}] community-string [udp-port port] [notification-type]
```

Syntax Description

<i>hostname ip-address</i>	Name, IP address, or IPv6 address of the SNMP notification host. The <i>ip-address</i> can be an IP or IPv6 address. The SNMP notification host is typically a network management station (NMS or SNMP manager). This host is the recipient of the SNMP traps or informs.
vrf	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications.
<i>vrf-name</i>	(Optional) VPN VRF instance used to send SNMP notifications.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
informs	(Optional) Specifies that notifications should be sent as informs.
version	(Optional) Version of the SNMP used to send the traps. The default is 1. If you use the version keyword, one of the following keywords must be specified: <ul style="list-style-type: none"> • 1—SNMPv1. This option is not available with informs. • 2c—SNMPv2C. • 3—SNMPv3. The most secure model because it allows packet encryption with the priv keyword. The default is noauth. One of the following three optional security level keywords can follow the 3 keyword: <ul style="list-style-type: none"> – auth—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. – noauth—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. – priv—Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
<i>community-string</i>	Password-like community string is sent with the notification operation. Note You can set this string using the snmp-server host command by itself, but Cisco recommends that you define the string using the snmp-server community command prior to using the snmp-server host command. Note The sign (@) is used for delimiting the context information.

udp-port	(Optional) Specifies that SNMP notifications or informs are to be sent to an NMS host.
<i>port</i>	(Optional) UDP port number of the NMS host. The default is 162.
<i>notification-type</i>	<p>(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. The notification type can be one or more of the following keywords:</p> <ul style="list-style-type: none"> • bgp—Sends Border Gateway Protocol (BGP) state change notifications. • calltracker—Sends Call Tracker call-start/call-end notifications. • cef — Sends Cisco Express Forwarding-related notifications. • config—Sends configuration change notifications. • cpu—Sends CPU-related notifications. • director—Sends DistributedDirector-related notifications. • dspu—Sends downstream physical unit (DSPU) notifications. • eigrp—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications. • entity—Sends Entity MIB modification notifications. • envmon—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • flash—Sends flash media insertion and removal notifications. • frame-relay—Sends Frame Relay notifications. • hsrp—Sends Hot Standby Routing Protocol (HSRP) notifications. • iplocalpool—Sends IP local pool notifications. • ipmobile—Sends Mobile IP notifications. • ipsec—Sends IP Security (IPsec) notifications. • isdn—Sends ISDN notifications. • l2tun-pseudowire-status—Sends pseudowire state change notifications. • l2tun-session—Sends Layer 2 tunneling session notifications. • llc2—Sends Logical Link Control, type 2 (LLC2) notifications. • memory—Sends memory pool and memory buffer pool notifications. • mpls-ldp—Sends Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions. • mpls-traffic-eng—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels. • mpls-vpn—Sends MPLS VPN notifications. • ospf—Sends Open Shortest Path First (OSPF) sham-link notifications. • pim—Sends Protocol Independent Multicast (PIM) notifications. • repeater—Sends standard repeater (hub) notifications.

- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

Note To enable RFC 2233 compliant link up/down notifications, you should use the **snmp server link trap** command.

- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **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 TCP connection closes.
- **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command.
- **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
- **x25**—Sends X.25 event notifications.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 Mainline/T Train	
12.0(3)T	<ul style="list-style-type: none"> • The version 3 [auth noauth priv] syntax was added as part of the SNMPv3 Support feature. • The hsrp notification-type keyword was added. • The voice notification-type keyword was added.
12.1(3)T	The calltracker notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.

Release	Modification
12.2(2)T	<ul style="list-style-type: none"> The vrf <i>vrf-name</i> keyword/argument combination was added. The ipmobile notification-type keyword was added. Support for the vsimaster notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	<ul style="list-style-type: none"> The pim notification-type keyword was added. The ipsec notification-type keyword was added.
12.2(8)T	<ul style="list-style-type: none"> The mpls-traffic-eng notification-type keyword was added. The director notification-type keyword was added.
12.2(13)T	<ul style="list-style-type: none"> The srp notification-type keyword was added. The mpls-ldp notification-type keyword was added.
12.3(2)T	<ul style="list-style-type: none"> The flash notification-type keyword was added. The l2tun-session notification-type keyword was added.
12.3(4)T	<ul style="list-style-type: none"> The cpu notification-type keyword was added. The memory notification-type keyword was added. The ospf notification-type keyword was added.
12.3(8)T	The iplocalpool notification-type keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	The vrp keyword was added.
12.3(14)T	<ul style="list-style-type: none"> Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument. The eigrp notification-type keyword was added.
Cisco IOS Release 12.0S	
12.0(17)ST	The mpls-traffic-eng notification-type keyword was integrated into Cisco IOS Release 12.0(17)ST.
12.0(21)ST	The mpls-ldp notification-type keyword was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	<ul style="list-style-type: none"> All features in the Cisco IOS Release 12.0ST train were integrated into Cisco IOS Release 12.0(22)S. The mpls-vpn notification-type keyword was added.
12.0(23)S	The l2tun-session notification-type keyword was added.
12.0(26)S	The memory notification-type keyword was added.
12.0(27)S	<ul style="list-style-type: none"> Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument. The vrf <i>vrf-name</i> keyword argument pair was integrated into Cisco IOS Release 12.0(27)S to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	The l2tun-pseudowire-status notification-type keyword was added.
Release 12.2S	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

Release	Modification
12.2(25)S	<ul style="list-style-type: none"> The cpu notification-type keyword was added. The memory notification-type keyword was added.
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.
12.2(31)SB2	The cef notification-type keyword was added.
12.2(31)SB3	This command was implemented on the Cisco 10000 series.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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 the host.

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



Note

If the community-string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community-string) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

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, a SNMP entity that receives an inform request acknowledges the message with a SNMP response protocol data unit (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.

Compared to traps, 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; 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 a **snmp-server host** command, no notifications are sent. 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.

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.

Some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled and others 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. To see what notification types are available on your system, use the command **help ?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific VRF. The VRF defines a VPN membership of a customer so data is stored using the VPN.

Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no intervening spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls-traffic-eng** (containing an intervening space and a hyphen).

This syntax difference is necessary to ensure that the command-line interface (CLI) interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. [Table 1](#) maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 1 Notification Keywords and Corresponding SNMP Enable Traps Commands

SNMP Enable Traps Command	SNMP Host Command Keyword
snmp-server enable traps l2tun session	l2tun-session
snmp-server enable traps mpls ldp	mpls-ldp
snmp-server enable traps mpls traffic-eng¹	mpls-traffic-eng
snmp-server enable traps mpls vpn	mpls-vpn

1. See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string **comaccess** and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 172.20.2.160 comaccess
Router(config)# access-list 10 deny any
```



Note

The sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using **community@VLAN_ID** (for example, **public@100**) where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a host specified named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

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

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 172.30.2.160 public snmp envmon
```

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

```
Router(config)# snmp-server enable traps
Router(config)# 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. The community string is defined as public.

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

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string 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 informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

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

The following example shows how to send all SNMP notifications to company.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host company.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

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

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 10.56.125.47 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 10.56.125.47 informs version 2c public cef
```

Related Commands	Command	Description
	snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
	snmp-server enable traps	Enables SNMP notifications (traps and informs).
	snmp-server informs	Specifies inform request options.
	snmp-server link trap	Enables linkUp/linkDown SNMP traps, which are compliant with RFC 2233.
	snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which a SNMP trap should originate.
	snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

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.

© 2003–2004, 2006–2007 Cisco Systems, Inc. All rights reserved.