



# EIGRP MIB

---

**First Published: February 28, 2005**

**Last Updated: February 19, 2007**

The EIGRP MIB feature introduces an Enhanced Interior Gateway Routing Protocol (EIGRP) MIB in Cisco IOS software. This MIB is accessed through remote Simple Network Management Support (SNMP) software clients. This MIB provides full EIGRP support for GET requests and limited notification (TRAP) support for stuck-in-active (SIA) and neighbor authentication failure events.

## 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 EIGRP MIB” section on page 21](#).

## 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 accountEIGRP MIB on Cisco.com is not required.

## Contents

- [Prerequisites for EIGRP MIB, page 2](#)
- [Restrictions for EIGRP MIB, page 2](#)
- [Information About EIGRP MIB, page 2](#)
- [How to Enable EIGRP MIB, page 8](#)
- [Configuration Examples for Enabling EIGRP MIB, page 9](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)
- [Feature Information for EIGRP MIB, page 21](#)



## Prerequisites for EIGRP MIB

- EIGRP MIB table objects are not visible via SNMP until an EIGRP routing process is enabled and an SNMP community string is configured on at least one router.
- Support for EIGRP notifications (TRAP) is not activated until a trap destination is configured.

## Restrictions for EIGRP MIB

- EIGRP MIB support has not been implemented for the EIGRP Prefix Limit Support feature.
- EIGRP MIB support is currently available for IPv4 only.

## Information About EIGRP MIB

The following concepts relate to EIGRP MIB:

- [EIGRP MIB Overview, page 2](#)
- [EIGRP VPN Table, page 3](#)
- [EIGRP Traffic Statistics Table, page 3](#)
- [EIGRP Topology Table, page 4](#)
- [EIGRP Neighbor Table, page 5](#)
- [EIGRP Interface Table, page 6](#)
- [EIGRP Notifications, page 7](#)

## EIGRP MIB Overview

This feature introduces EIGRP MIB support in Cisco IOS software. EIGRP routing processes that run over IPv4 are supported. The EIGRP MIB is accessed through remote SNMP software clients. MIB table objects are accessed as read-only through GET, GETINFO, GETMANY, GETNEXT, GETBULK, and SET requests. Counters for MIB table objects are cleared when the EIGRP routing process is reset or when the routing table is refreshed by entering the **clear ip route** or **clear ip eigrp** commands. Managed objects for all EIGRP routing processes are implemented as five table objects on a per-autonomous-system or per-Virtual-Private-Network (VPN) basis.

## EIGRP VPN Table

The EIGRP VPN Table contains information regarding which VPNs are configured to run an EIGRP routing process. VPN routes are indexed by the VPN name and the EIGRP autonomous system number. The EIGRP VPN table object and the value populated for that object are described in [Table 1](#).

**Table 1** VPN Table Object Description

EIGRP VPN Table	Description
<i>cEigrpVpnName</i>	The VPN routing and forwarding (VRF) name. Only VRFs that are configured to run an EIGRP routing process are populated.

## EIGRP Traffic Statistics Table

The EIGRP Traffic Statistics Table contains counters and statistics for the specific types of EIGRP packets that are sent and the related collective information that is generated. The objects in this table are populated on a per-autonomous-system basis. Objects in this table are populated for adjacencies formed on all interfaces with an IP address that is configured under an EIGRP network statement. Traffic statistics table objects and the values populated for each object are described in [Table 2](#).

**Table 2** Traffic Statistics Table Object Descriptions

EIGRP Traffic Statistics Table	Description
<i>cEigrpNbrCount</i>	Total number of live neighbors. This table object is incremented or decremented as peering sessions are established or expired.
<i>cEigrpHellosSent</i>	Total number of transmitted hello packets. This table object is incremented as packets are transmitted.
<i>cEigrpHellosRcvd</i>	Total number of received hello packets. This table object is incremented as packets are received.
<i>cEigrpUpdatesSent</i>	Total number of transmitted routing update packets. This table object is incremented as packets are transmitted.
<i>cEigrpUpdatesRcvd</i>	Total number of received routing update packets. This table object is incremented as packets are received.
<i>cEigrpQueriesSent</i>	Total number of alternate route query packets transmitted. This table object is incremented as packets are transmitted.
<i>cEigrpQueriesRcvd</i>	Total number of alternate route query packets received. This table object is incremented as packets are received.
<i>cEigrpRepliesSent</i>	Total number of reply packets that are transmitted in response to received query packets. This table object is incremented as packets are transmitted.
<i>cEigrpRepliesRcvd</i>	Total number of reply packets that are received in response to transmitted query packets. This table object is incremented as packets are transmitted.
<i>cEigrpAcksSent</i>	Total number of acknowledgement packets that are transmitted in response to received update packets. This table object is incremented as packets are transmitted.

**Table 2** Traffic Statistics Table Object Descriptions (continued)

<i>cEigrpAcksRcvd</i>	Total number of acknowledgement packets that are received in response to transmitted update packets. This table object is incremented as packets are received.
<i>cEigrpInputQHighMark</i>	The highest number of packets that have been in the input queue. This table object is incremented only when the previous highest number is exceeded.
<i>cEigrpInputQDrops</i>	Total number of packets dropped from the input queue because the input queue was full. This table object is incremented each time a packet is dropped.
<i>cEigrpSiaQueriesSent</i>	Total number of query packets sent in response to a destination that is in a SIA state for a down peer. This table object is incremented each time an SIA query packet is sent.
<i>cEigrpSiaQueriesRcvd</i>	Total number of SIA query packets received from neighbors searching for an alternate path to a destination. This table object is incremented each time an SIA query packet is received.
<i>cEigrpAsRouterIdType</i>	The type of IP address that is used as the router ID. The value for this table object can be an IPv4 address.
<i>cEigrpAsRouterId</i>	The configured or automatically selected router ID in IP address format. This table object is updated if the router ID is manually reconfigured or if the IP address that was automatically selected is removed.
<i>cEigrpTopoRoutes</i>	Total number of EIGRP-derived routes in the topology table. This table object is incremented if a route is added or removed.
<i>cEigrpHeadSerial</i>	Internal sequencing number (serial) applied to EIGRP topology table routes. Routes are sequenced starting with 1. A value of 0 is displayed when there are no routes in the topology table. The “Head” serial number is applied to the first route in the sequence.
<i>cEigrpNextSerial</i>	The serial number applied to the next route in the sequence.
<i>cEigrpXmitPendReplies</i>	Total number of replies expected in response to locally transmitted query packets. This table object contains a value of 0 until a route is placed in an active state.
<i>cEigrpXmitDummies</i>	Total number of temporary entries in the topology table. Dummies are internal entries and not transmitted in routing updates.

## EIGRP Topology Table

The EIGRP Topology Table contains information regarding EIGRP routes received in updates and routes that are locally originated. EIGRP sends routing updates to and receives routing updates from adjacent routers to which peering relationships (adjacencies) have been formed. The objects in this table are populated on a per-topology-table-entry (route) basis. Topology table objects and the values populated for each object are described in [Table 3](#).

**Table 3** Topology Table Object Descriptions

EIGRP Topology Table	Description
<i>cEigrpActive</i>	Displays the active status for routes in the topology table. The value for this table object is displayed on a per-route basis. A value of 1 is displayed when a route has gone into an active state. A value of 2 is displayed when a route is in a passive state (normal).
<i>cEigrpStuckInActive</i>	Displays the SIA status of a route. The value for this table object is displayed on a per-route basis. A value of 1 is displayed when a route is in an SIA state (no reply has been received for queries for alternate paths). SIA queries are transmitted when a route is placed in this state.
<i>cEigrpDestSuccessors</i>	Total number successors (a route that is the next hop to a destination network) for a topology table entry. The topology table will contain a successor for each path to a given destination. This table object is incremented each time a successor is added or removed.
<i>cEigrpFdistance</i>	The feasible (best) distance to a destination network. This value is used to calculate the feasible successor for a topology table entry.
<i>cEigrpRouteOriginAddr</i>	The protocol type of an IP address defined the origin of the topology table entry.
<i>cEigrpRouteOriginType</i>	Displays the IP address of the router that originated the route in the topology table entry. This table is populated only if the topology table entry was not locally originated.
<i>cEigrpNextHopAddressType</i>	Displays the protocol type for the next-hop IP address for the route in a topology table entry.
<i>cEigrpNextHopAddress</i>	The next-hop IP address for a route in a topology table entry.
<i>cEigrpNextHopInterface</i>	The interface through which the next-hop IP address is reached to send traffic to the destination.
<i>cEigrpDistance</i>	The computed distance to the destination network entry from the local router.
<i>cEigrpReportDistance</i>	The computed distance to the destination network in the topology entry as reported by the originator of the route.

## EIGRP Neighbor Table

The EIGRP Neighbor Table contains information about EIGRP neighbors to which adjacencies have been established. EIGRP uses a “Hello” protocol to form neighbor relationships with directly connected EIGRP neighbors. The objects in this table are populated on a per-neighbor basis. Neighbor table objects and the values populated for each object are described in [Table 4](#).

**Table 4** Neighbor Table Object Descriptions

EIGRP Neighbor Table	Description
<i>cEigrpPeerAddrType</i>	The protocol type of the remote source IP address used by the neighbor to establish the EIGRP adjacency with the local router.
<i>cEigrpPeerAddr</i>	The source IP address of the neighbor that was used to establish EIGRP adjacency with the local router.

**Table 4 Neighbor Table Object Descriptions (continued)**

<i>cEigrpPeerInterface</i>	The name of the local interface, through which the neighbor can be reached. This table object is populated on a per-neighbor basis.
<i>cEigrpPeerIfIndex</i>	The index of the local interface, through which this neighbor can be reached.
<i>cEigrpHoldTime</i>	The hold timer value for the adjacency with the neighbor. If this timer expires, the neighbor is declared down and removed from the neighbor table.
<i>cEigrpUpTime</i>	The length of time for which the EIGRP adjacency to the neighbor has been in an up state. The time period is displayed in hours:minutes:seconds.
<i>cEigrpSrtt</i>	The computed smooth round trip time (SRTT) for packets transmitted to and received from the neighbor.
<i>cEigrpRto</i>	The computed retransmission timeout (RTO) for the neighbor. The value for this table object is computed as an aggregate average of the time required for packet delivery. This table object is populated on a per-neighbor basis.
<i>cEigrpPktsEnqueued</i>	Total number of EIGRP packets (all types) currently queued for transmission to a neighbor. This table object is populated on a per-neighbor basis.
<i>cEigrpLastSeq</i>	The number of the last sequence number of a packet transmitted to a neighbor. This table object is incremented as the sequence number increases.
<i>cEigrpVersion</i>	The EIGRP version information reported by the remote neighbor. This table object is populated on a per-neighbor basis.
<i>cEigrpRetrans</i>	Cumulative number of packets retransmitted to the neighbor, while the neighbor is in an up state. This table object is populated on a per-neighbor basis.
<i>cEigrpRetries</i>	Total number of times an unacknowledged packet has been sent to a neighbor. This table object is populated on a per-neighbor basis.

## EIGRP Interface Table

The EIGRP Interface Table contains information and statistics for each interface that EIGRP has been configured to run over. The objects in this table are populated on a per-interface basis. Interface table objects and the values populated for each object are described in [Table 5](#).

**Table 5 EIGRP Interface Table Object Descriptions**

EIGRP Interface Table	Description
<i>cEigrpPeerCount</i>	Total number of neighbor adjacencies formed through this interface.
<i>cEigrpXmitReliableQ</i>	Total number of packets waiting in the reliable transport transmission queue (acknowledgement is required) to be sent to a neighbor.
<i>cEigrpXmitUnreliableQ</i>	Total number of packets waiting in the unreliable transmission queue (no acknowledgement required).
<i>cEigrpMeanSrtt</i>	The computed smooth round trip time (SRTT) for packets transmitted to and received from all neighbors on the interface.

**Table 5** EIGRP Interface Table Object Descriptions (continued)

<i>cEigrpPacingReliable</i>	The configured time interval (in milliseconds) between EIGRP packet transmissions on this interface when the reliable transport used.
<i>cEigrpPacingUnreliable</i>	The configured time interval (in milliseconds) between EIGRP packet transmissions on this interface when the unreliable transport used.
<i>cEigrpMFlowTimer</i>	The configured multicast flow control timer value (in milliseconds) for this interface.
<i>cEigrpPendingRoutes</i>	Total number of routing updates queued for transmission on this interface.
<i>cEigrpHelloInterval</i>	The configured time interval (in seconds) between Hello packet transmissions for this interface.
<i>cEigrpXmitNextSerial</i>	The serial number of the next packet that is queued for transmission on this interface.
<i>cEigrpUMcasts</i>	Total number of unreliable (no acknowledgement required) multicast packets transmitted on this interface.
<i>cEigrpRMcasts</i>	Total number of reliable (acknowledgement required) multicast packets transmitted on this interface.
<i>cEigrpUUcasts</i>	Total number of unreliable (no acknowledgement required) unicast packets transmitted on this interface.
<i>cEigrpRUcasts</i>	Total number of reliable (acknowledgement required) unicast packets transmitted on this interface.
<i>cEigrpMcastExcept</i>	The total number of EIGRP multicast exception transmissions that have occurred on this interface.
<i>cEigrpCRpkts</i>	Total number conditional-receive packets sent on this interface.
<i>cEigrpAcksSuppressed</i>	Total number of individual acknowledgement packets that have been suppressed and combined in an already enqueued outbound reliable packet on this interface.
<i>cEigrpRetranSent</i>	Total number of packet retransmissions sent on this interface.
<i>cEigrpOOSrvcd</i>	Total number of out-of-sequence packets received on this interface.
<i>cEigrpAuthMode</i>	The authentication mode configured for traffic that uses this interface. The value of 0 is displayed when no authentication is enabled. The value of 1 is displayed when MD5 authentication is enabled.
<i>cEigrpAuthKeyChain</i>	The name of the authentication key-chain configured on this interface. The key-chain is a reference to which set of secret keys are to be accessed to determine which key string to use. The key-chain name is not the key string (password).

## EIGRP Notifications

The EIGRP MIB provides limited notification (TRAP) support for stuck-in-active (SIA) and neighbor authentication failure events. The **snmp-server enable traps eigrp** command is used to enable EIGRP notifications on a Cisco router. Support for TRAP events is not activated until a trap destination is configured with the **snmp-server host** command and a community string is defined with the **snmp-server community** command. EIGRP notifications are described in [Table 6](#).

**Table 6** EIGRP Notifications

EIGRP Traps (Notifications)	Description
<i>cEigrpAuthFailureEvent</i>	When EIGRP MD5 authentication is enabled on any interface and neighbor adjacencies are formed, a notification is sent if any adjacency goes down as a result of an authentication failure. This notification will be sent once per down event. This notification includes the source IP address of the neighbor from which the authentication failure occurred.
<i>cEigrpRouteStuckInActive</i>	During the query phase for a new route to a destination network, the route is placed in the active state (an alternate path is actively being sought) and a query packet is broadcast to the network. If no replies are received to the query, an SIA query packets are broadcast. If a reply is not received for the SIA queries, the neighbor adjacency is dropped, the route is declared SIA, and this notification is sent.

## How to Enable EIGRP MIB

This section contains the following tasks:

- [Enabling EIGRP MIB, page 8](#)

## Enabling EIGRP MIB

Perform this task to specify an SNMP server host, configure an SNMP community string, and enable EIGRP notifications.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **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*] [**vrrp**]
4. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*]
5. **snmp-server enable traps eigrp**
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	<p>Enters global configuration mode.</p>
Step 3	<pre>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] [vrrp]</pre> <p><b>Example:</b> Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp </p>	<p>Specifies the destination host or address for SNMP notifications.</p>
Step 4	<pre>snmp-server community string [view view-name] [ro   rw] [ipv6 nacl] [access-list-number]</pre> <p><b>Example:</b> Router(config)# snmp-server community EIGRP1NET1A </p>	<p>Configures a community access string to permit SNMP access to the local router by the remote SNMP software client.</p> <ul style="list-style-type: none"> <li>Only IPv4 is supported in Cisco IOS Releases 12.3(14)T and 12.2(33)SRB.</li> </ul>
Step 5	<pre>snmp-server enable traps eigrp</pre> <p><b>Example:</b> Router(config)# snmp-server enable traps eigrp </p>	<p>Enables SNMP support for EIGRP notifications.</p> <ul style="list-style-type: none"> <li>Notifications can be configured for only SIA and neighbor authentication failure events.</li> </ul>
Step 6	<pre>end</pre> <p><b>Example:</b> Router(config)# end </p>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

## Configuration Examples for Enabling EIGRP MIB

The following examples show how to configure and verify this feature:

- [EIGRP MIB Configuration: Example, page 10](#)
- [EIGRP MIB Verification: Example, page 10](#)

## EIGRP MIB Configuration: Example

In the following example, an SNMP server host is specified, a community string is configured, and support for EIGRP notifications is enabled.

```
Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp
Router(config)# snmp-server community EIGRP1NET1A
Router(config)# snmp-server enable traps eigrp
```

## EIGRP MIB Verification: Example

In the following example, the local SNMP configuration is verified by entering the [show running-config](#) command:

```
Router# show running-config | include snmp
snmp-server community EIGRP1NET1A
snmp-server enable traps eigrp
snmp-server host 10.0.0.1 version 2c NETMANAGER
```

## Additional References

The following sections provide references related to the EIGRP MIB feature.

## Related Documents

Related Topic	Document Title
EIGRP commands	<a href="#">Cisco IOS IP Routing Protocols Command Reference, Release 12.4</a>
EIGRP configuration tasks	<a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a>
EIGRP overview	<a href="#">Introduction to EIGRP</a>
Troubleshooting SIA events	<a href="#">What Does the EIGRP DUAL-3-SIA Error Message Mean?</a>
SNMP commands	<a href="#">Cisco IOS Network Management Command Reference, Release 12.4</a>
SNMP configuration tasks	<a href="#">Configuring SNMP Support</a>

## 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
CISCO-EIGRP-MIB.my	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC-1213	<i>Management Information Base for Network Management of TCP/IP-based Internets: MIB-II</i>

## 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.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This section documents only commands that are new or modified:

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

## snmp-server enable traps eigrp

To enable support for Enhanced Interior Gateway Routing Protocol (EIGRP) notifications on a Cisco router, use the **snmp-server enable traps eigrp** command in global configuration mode. To disable EIGRP notification support, use the **no** form of this command.

**snmp-server enable traps eigrp**

**no snmp-server enable traps eigrp**

**Syntax Description** This command has no keywords or arguments.

**Command Default** EIGRP notification support is not enabled.

**Command Modes** Global configuration

### Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

### Usage Guidelines

The **snmp-server enable traps eigrp** command is used to enable notifications (traps) for stuck-in-active (SIA) and neighbor authentication failure events. Support for trap events is not activated until a trap destination is configured with the **snmp-server host** command and until a community string is defined with the **snmp-server community** command.

### Examples

In the following example, an SNMP server host is specified, a community string is configured, and support for EIGRP notifications is enabled:

```
Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp
Router(config)# snmp-server community EIGRP1NET1A
Router(config)# snmp-server enable traps eigrp
```

### Related Commands

Command	Description
<b>snmp-server community</b>	Configures a community access string to permit SNMP access to the local router by the remote SNMP software client.
<b>snmp-server host</b>	Specifies the destination host or address for SNMP 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</i>   <i>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.
<b>vrf</b>	(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.
<b>traps</b>	(Optional) Specifies that notifications should be sent as traps. This is the default.
<b>informs</b>	(Optional) Specifies that notifications should be sent as informs.
<b>version</b>	(Optional) Version of the SNMP used to send the traps. The default is 1.  If you use the <b>version</b> keyword, one of the following keywords must be specified: <ul style="list-style-type: none"> <li>• <b>1</b>—SNMPv1. This option is not available with informs.</li> <li>• <b>2c</b>—SNMPv2C.</li> <li>• <b>3</b>—SNMPv3. The most secure model because it allows packet encryption with the <b>priv</b> keyword. The default is <b>noauth</b>.</li> </ul> One of the following three optional security level keywords can follow the <b>3</b> keyword: <ul style="list-style-type: none"> <li>– <b>auth</b>—(Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.</li> <li>– <b>noauth</b>—(Optional) Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.</li> <li>– <b>priv</b>—(Optional) Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).</li> </ul>
<i>community-string</i>	Password-like community string is sent with the notification operation.  <b>Note</b> You can set this string using the <b>snmp-server host</b> command by itself, but Cisco recommends that you define the string using the <b>snmp-server community</b> command prior to using the <b>snmp-server host</b> command.  <b>Note</b> The sign (@) is used for delimiting the context information.

<b>udp-port</b>	(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"> <li>• <b>bgp</b>—Sends Border Gateway Protocol (BGP) state change notifications.</li> <li>• <b>calltracker</b>—Sends Call Tracker call-start/call-end notifications.</li> <li>• <b>cef</b> — Sends Cisco Express Forwarding-related notifications.</li> <li>• <b>config</b>—Sends configuration change notifications.</li> <li>• <b>cpu</b>—Sends CPU-related notifications.</li> <li>• <b>director</b>—Sends DistributedDirector-related notifications.</li> <li>• <b>dspu</b>—Sends downstream physical unit (DSPU) notifications.</li> <li>• <b>eigrp</b>—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.</li> <li>• <b>entity</b>—Sends Entity MIB modification notifications.</li> <li>• <b>envmon</b>—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.</li> <li>• <b>flash</b>—Sends flash media insertion and removal notifications.</li> <li>• <b>frame-relay</b>—Sends Frame Relay notifications.</li> <li>• <b>hsrp</b>—Sends Hot Standby Routing Protocol (HSRP) notifications.</li> <li>• <b>iplocalpool</b>—Sends IP local pool notifications.</li> <li>• <b>ipmobile</b>—Sends Mobile IP notifications.</li> <li>• <b>ipsec</b>—Sends IP Security (IPsec) notifications.</li> <li>• <b>isdn</b>—Sends ISDN notifications.</li> <li>• <b>l2tun-pseudowire-status</b>—Sends pseudowire state change notifications.</li> <li>• <b>l2tun-session</b>—Sends Layer 2 tunneling session notifications.</li> <li>• <b>llc2</b>—Sends Logical Link Control, type 2 (LLC2) notifications.</li> <li>• <b>memory</b>—Sends memory pool and memory buffer pool notifications.</li> <li>• <b>mpls-ldp</b>—Sends Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.</li> <li>• <b>mpls-traffic-eng</b>—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.</li> <li>• <b>mpls-vpn</b>—Sends MPLS VPN notifications.</li> <li>• <b>ospf</b>—Sends Open Shortest Path First (OSPF) sham-link notifications.</li> <li>• <b>pim</b>—Sends Protocol Independent Multicast (PIM) notifications.</li> <li>• <b>repeater</b>—Sends standard repeater (hub) notifications.</li> </ul>

- **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. No notifications are sent.

#### Command Modes

Global configuration

#### Command History

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

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

### 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 7](#) maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

**Table 7** Notification Keywords and Corresponding SNMP Enable Traps Commands

SNMP Enable Traps Command	SNMP Host Command Keyword
<b>snmp-server enable traps l2tun session</b>	<b>l2tun-session</b>
<b>snmp-server enable traps mpls ldp</b>	<b>mpls-ldp</b>
<b>snmp-server enable traps mpls traffic-eng<sup>1</sup></b>	<b>mpls-traffic-eng</b>
<b>snmp-server enable traps mpls vpn</b>	<b>mpls-vpn</b>

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
<b>snmp-server enable peer-trap poor qov</b>	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
<b>snmp-server enable traps</b>	Enables SNMP notifications (traps and informs).
<b>snmp-server informs</b>	Specifies inform request options.
<b>snmp-server link trap</b>	Enables linkUp/linkDown SNMP traps, which are compliant with RFC 2233.

Command	Description
<b>snmp-server trap-source</b>	Specifies the interface (and hence the corresponding IP address) from which a SNMP trap should originate.
<b>snmp-server trap-timeout</b>	Defines how often to try resending trap messages on the retransmission queue.

# Feature Information for EIGRP MIB

Table 8 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 8 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 8** Feature Information for EIGRP MIB

Feature Name	Releases	Feature Information
EIGRP MIB	12.3(14)T, 12.2(33)SRB	The EIGRP MIB feature introduces an EIGRP MIB in Cisco IOS software. This MIB is accessed through remote Simple Network Management Support (SNMP) software clients. This MIB provides full EIGRP support for GET requests and limited notification (TRAP) support for stuck-in-active (SIA) and neighbor authentication failure events.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo 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, BPX, 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, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, 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.

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.

