



IS-IS MIB

First Published: August 22, 2005

Last Updated: February 23, 2007

This feature introduces MIB support for the Intermediate System-to-Intermediate System (IS-IS) link-state routing protocol. IS-IS is used as the link-state routing protocol of choice by major service providers. The IS-IS MIB feature offers service providers an improved capability to continuously monitor the changing state of an IS-IS network by use of MIB objects to gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant protocol events such as an authentication failure or a mismatch in area addresses between Intermediate Systems (ISs). The protocol information collected by the IS-IS MIB objects and trap objects can be used by the network manager to derive statistics that can help monitor and improve overall network performance.

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 IS-IS MIB” section on page 33](#).

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

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

Contents

- [Prerequisites for IS-IS MIB, page 2](#)
- [Restrictions for IS-IS MIB, page 2](#)
- [Information About IS-IS MIB, page 2](#)
- [How to Enable IS-IS MIB, page 12](#)
- [Configuration Examples for IS-IS MIB, page 18](#)
- [Where to Go Next, page 19](#)
- [Additional References, page 19](#)



Americas Headquarters:

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

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

- [Command Reference, page 20](#)
- [Feature Information for IS-IS MIB, page 33](#)

Prerequisites for IS-IS MIB

- Simple Network Management Protocol (SNMP) must be enabled on the router before notifications (traps) can be configured or before SNMP GET operations can be performed.
- IS-IS must be configured on the router.

Restrictions for IS-IS MIB

- All enhancements that are introduced by this feature are provided only by the Cisco private MIB CISCO-IETF-ISIS-MIB.my.
- The SNMP SET capability will not be supported for any IS-IS MIB objects. Objects with read-create or read-write access are understood to operate only as read-only.
- This feature is not supported for multiple instances of IS-IS.

Information About IS-IS MIB

To enable the IS-IS MIB feature, you should understand the following concepts:

- [Cisco IS-IS MIB Table Object Definitions, page 2](#)
- [Cisco IS-IS MIB Trap Notifications, page 10](#)

Cisco IS-IS MIB Table Object Definitions

The IS-IS MIB feature introduces network management support for the IS-IS routing protocol through the use of IS-IS MIB table entries, MIB objects and MIB trap notification objects that comprise the Cisco private MIB CISCO-IETF-ISIS-MIB.my. New CLI has been added to enable SNMP notifications for IS-IS MIB objects. Notifications are provided for errors and other significant event information for the IS-IS network.

For more information on how to configure IS-IS MIB to receive the SNMP notifications, refer to the [“How to Enable IS-IS MIB” section on page 12](#).

The following MIB objects describe IS-IS MIB table entries:

The `ciiManAreaAddrEntry` table contains the set of area addresses manually configured for the IS. The `ciiManAreaAddrEntry` table defines the following MIB objects:

- `ciiManAreaAddr`
- `ciiManAreaAddrExistState`

The `ciiAreaAddrEntry` table groups sets of relevant area addresses reported in all Level 1 link-state packets (LSPs) that were generated or received by an IS from other ISs that are reachable through Level 1 routing.

Each entry contains one area address per LSP. The `ciiAreaAddrEntry` table defines the following MIB object:

- `ciiAreaAddr`

The `ciiSysProtSuppEntry` table contains a manually configured set of protocols supported by the IS. The supported protocol types are IPv4, IPv6 and ISO8473. The `ciiSysProtSuppEntry` table defines the following MIB objects:

- `ciiSysProtSuppProtocol`
- `ciiSysProtSuppExistState`

The `ciiSummAddrEntry` table contains a set of manually configured summary addresses used to form summarized IP TLVs originated by an ISS. This table is useful to combine and modify IP reachability announcements, and also controls leaking of L1 routes into L2. The `ciiSummAddrEntry` table defines the following MIB objects:

- `ciiSummAddressType`
- `ciiSummAddress`
- `ciiSummAddrPrefixLen`
- `ciiSummAddrExistState`
- `ciiSummAddrMetric`
- `ciiSummAddrFullMetric`

The `ciiRedistributeAddrEntry` table provides the criteria to decide if a route should be leaked from L2 to L1. When Domain Wide Prefix leaking is enabled (represented by `ciiSysL2toL1Leaking`), addresses that match the summary mask in the table are announced at L1 by routers. The Cisco MIB implementation also allows retrieval of routes for masked entries based on configured access lists or route maps. The `ciiRedistributeAddrEntry` table defines the following MIB objects:

- `ciiRedistributeAddrType`
- `ciiRedistributeAddrAddress`
- `ciiRedistributeAddrPrefixLen`
- `ciiRedistributeAddrExistState`

The `ciiRouterEntry` table has one entry for every peer and it tracks the hostnames and Router IDs associated with that peer. The `ciiRouterEntry` table defines the following MIB objects.

- `ciiRouterSysID`
- `ciiRouterLevel`
- `ciiRouterHostName`
- `ciiRouterID`

**Note**

The IS-IS MIB defines the `ciiRouterLevel` object to be the level of the IS. The Cisco implementation interprets the `ciiRouterLevel` object to be the level of the link-state packet (LSP) in which the hostname (`ciiRouterHostName`) and router ID (`ciiRouterID`) were received.

The `ciiSysLevelEntry` table captures level-specific information about the IS. This information includes parameters that control how LSPs are generated, metrics for SPF computation and the decision of whether to perform traffic engineering at this level.

The `ciiSysLevelEntry` table defines the following MIB objects:

- `ciiSysLevelIndex`
- `ciiSysLevelOrigLSPBuffSize`
- `ciiSysLevelMinLSPGenInt`
- `ciiSysLevelOverloadState`
- `ciiSysLevelSetOverload`
- `ciiSysLevelSetOverloadUntil`
- `ciiSysLevelMetricStyle`
- `ciiSysLevelSPFConsiders`
- `ciiSysLevelTEEnabled`



Note

For the `ciiSysLevelOverloadState` MIB object, the Cisco MIB follows the correct interpretation of IS state transition per the future IETF draft MIB revisions. The draft-ietf-isis-wg-16.txt did not follow the ISO 10589:2002 definition correctly. Per the ISO 10589:2002 definition, the waiting state is defined for low memory resource condition and the overloaded state is enabled by the administrator. Moreover, the Cisco implementation does not support a transition to a waiting state on low memory.

The `ciiCircEntry` table contains circuit-specific information about each broadcast or point-to-point interface used in this IS-IS. Each entry is associated with a corresponding interface, based on the circuit type (broadcast or point-to-point interfaces). In other words, only interfaces that are configured as broadcast or point-to-point can be polled. The Cisco implementation of the IS-IS MIB does not support the following circuit types: `staticIn`, `staticOut`, `dA` (dynamically assigned). The `ciiCircEntry` table defines the following MIB objects:

- `ciiCircIndex`
- `ciiCircIfIndex`
- `ciiCircIfSubIndex`
- `ciiCircAdminState`
- `ciiCircExistState`
- `ciiCircType`
- `ciiCircExtDomain`
- `ciiCircLevel`
- `ciiCircPassiveCircuit`
- `ciiCircMeshGroupEnabled`
- `ciiCircMeshGroup`
- `ciiCircSmallHellos`
- `ciiCircLastUpTime`
- `ciiCirc3WayEnabled`
- `ciiCircExtendedCircID`



Note

The `ciiCircExtDomain` MIB table object is not implemented because `externalDomain` linkage is not supported by Cisco IOS software.

The `ciiNextCircIndex` object, which is defined outside `ciiCircTable`, is used to assign a unique index value to the `ciiCircIndex` through a SET operation. The Cisco MIB implementation does not implement this object because the SET ability currently is not supported, and `ciiCircIndex` is determined uniquely through data from configured interfaces.

The `ciiCircLevelEntry` table contains level-specific information about IS-IS circuits. The `ciiCircLevelEntry` table contains the following MIB objects:

- `ciiCircLevelIndex`
- `ciiCircLevelMetric`
- `ciiCircLevelWideMetric`
- `ciiCircLevelISPriority`
- `ciiCircLevelIDOctet`
- `ciiCircLevelID`
- `ciiCircLevelDesIS`
- `ciiCircLevelHelloMultiplier`
- `ciiCircLevelHelloTimer`
- `ciiCircLevelDRHelloTimer`
- `ciiCircLevelLSPThrottle`
- `ciiCircLevelMinLSPRetransInt`
- `ciiCircLevelCSNPInterval`
- `ciiCircLevelPartSNPInterval`

The `ciiSystemCounterEntry` table has a sequence of entries used to track system-wide events using counters. The `ciiSystemCounterEntry` table defines the following MIB objects:

- `ciiSysStatLevel`
- `ciiSysStatCorrLSPs`
- `ciiSysStatAuthTypeFails`
- `ciiSysStatAuthFails`
- `ciiSysStatLSPDbaseOloads`
- `ciiSysStatManAddrDropFromAreas`
- `ciiSysStatAttmptToExMaxSeqNums`
- `ciiSysStatSeqNumSkips`
- `ciiSysStatOwnLSPPurges`
- `ciiSysStatIDFieldLenMismatches`
- `ciiSysStatPartChanges`
- `ciiSysStatSPFRuns`
- `ciiSysStatLSPErrors`

**Note**

The `ciiSysStatPartChanges` object is not implemented because the ability to detect partition changes currently is not supported by Cisco IOS software.

The `ciiCircuitCounterEntry` table is used to track system-wide events specific to a circuit and level. The `ciiCircuitCounterEntry` table defines the following MIB objects:

- `ciiCircuitType`
- `ciiCircAdjChanges`
- `ciiCircNumAdj`
- `ciiCircInitFails`
- `ciiCircRejAdjs`
- `ciiCircIDFieldLenMismatches`
- `ciiCircMaxAreaAddrMismatches`
- `ciiCircAuthTypeFails`
- `ciiCircAuthFails`
- `ciiCircLANDesISChanges`

**Note**

The `ciiCircInitFails` MIB object does not return any data because circuit initialization failures are not tracked by Cisco IOS software.

The `ciiPacketCounterEntry` table tracks the number of IS-IS packets sent and received over a circuit at one level. At any time, the traffic flow along one direction is recorded. All objects defined in this table are Counter objects. The `ciiPacketCounterEntry` table defines the following MIB objects:

- `ciiPacketCountLevel`
- `ciiPacketCountDirection`
- `ciiPacketCountIIHellos`
- `ciiPacketCountISHellos`
- `ciiPacketCountESHellos`
- `ciiPacketCountLSPs`
- `ciiPacketCountCSNPs`
- `ciiPacketCountPSNPs`
- `ciiPacketCountUnknowns`

**Note**

- The `ciiPacketCountISHellos` MIB object tracks the number of end system-Intermediate system (ES-IS) hellos only at system granularity and not at per-level or per-circuit.
- The `ciiPacketCountESHellos` MIB objects tracks the number of end-system (ES) hellos only at system granularity and not at per-level or per-circuit.
- The `ciiPacketCountUnknowns` MIB object can track only unknown packet types that are received, not those that are sent in any given level.

The `ciiISAdjEntry` table has one entry associated with every adjacency to an IS (in other words, a table of adjacencies).

However, this object cannot be used to track multiple adjacencies in a LAN, with each adjacency corresponding to a level. Thus the best priority level is selected among the configured objects.

The `ciiISAdjEntry` table defines the following MIB objects:

- `ciiISAdjChanges`
- `ciiISAdjIndex`
- `ciiISAdjState`
- `ciiISAdj3WayState`
- `ciiISAdjNeighSNPAAAddress`
- `ciiISAdjNeighSysType`
- `ciiISAdjNeighSysID`
- `ciiISAdjNbrExtendedCircID`
- `ciiISAdjUsage`
- `ciiISAdjHoldTimer`
- `ciiIsAdjNeighPriority`
- `ciiISAdjLastUpTime`

**Note**

- The `ciiISAdjChanges` MIB object gathers information based on the best priority level that is selected among the configured objects, per the restriction against the software support of multiple adjacencies in a LAN for the `ciiISAdjEntry` table.
- The `ciiISAdjNeighPriority` MIB object gathers information based on the best priority level that is selected among the configured objects, per the restriction against the software support of multiple adjacencies in a LAN for the `ciiISAdjEntry` table.

The `ciiISAdjAreaAddrEntry` table contains entries for the sets of area addresses of neighboring ISs as reported in received IS-IS Hello protocol data units (PDU)s. The `ciiISAdjAreaAddrEntry` table defines the following MIB objects:

- `ciiISAdjAreaAddrIndex`
- `ciiISAdjAreaAddress`

The `ciiISAdjIPAddrEntry` table contains entries that are formed by a set of IP addresses of neighboring ISs as reported in received Hello PDUs. The `ciiISAdjIPAddrEntry` table defines the following MIB objects:

- `ciiISAdjIPAddrIndex`
- `ciiISAdjIPAddrType`
- `ciiISAdjIPAddrAddress`

The `ciiISAdjProtSuppEntry` table contains information about the protocols supported by neighboring ISs as reported in received Hello PDUs. The `ciiISAdjProtSuppEntry` table defines the following MIB object:

- `ciiISAdjProtSuppProtocol`

The `ciiRAEntry` table records information about a reachable NSAP or address prefix that is manually configured or learned dynamically.

The `ciiRAEntry` table defines the following MIB objects:

- `ciiRAIndex`
- `ciiRAExistState`

- `ciiRAAdminState`
- `ciiRAAddrPrefix`
- `ciiRAMapType`
- `ciiRAMetric`
- `ciiRAMetricType`
- `ciiRASNPAddress`
- `ciiRASNPAMask`
- `ciiRASNPAPrefix`
- `ciiRAType`

**Note**

- The `ciiRAMapType` MIB Object supports only implicit (null) and explicit mapping types. The `extractIDI` and `extractDSP` types are not supported.
- Because the `ciiRAMapType` MIB Object does not support the `extractIDI` and `extractDSP` mapping types, the `ciiRASNPAPrefix` and `ciiRASNPAMask` MIB objects will hold no data, as they depend on the unsupported mapping types. The `ciiRAMapType` and `ciiRASNPAMask` MIB objects are not implemented.
- The `ciiRAType` MIB object does not support the manual creation of IP reachability addresses.

Each entry in the `ciiIPRAEntry` table records information about one IP reachable address manually configured on the IS or learned from another protocol. The `ciiIPRAEntry` table defines the following MIB objects:

- `ciiIPRADestType`
- `ciiIPRADest`
- `ciiIPRADestPrefixLen`
- `ciiIPRANextHopIndex`
- `ciiIPRANextHopType`
- `ciiIPRANextHop`
- `ciiIPRAType`
- `ciiIPRAExistState`
- `ciiIPRAAdminState`
- `ciiIPRAMetric`
- `ciiIPRAMetricType`
- `ciiIPRAFullMetric`
- `ciiIPRASNPAddress`
- `ciiIPRASourceType`

**Note**

The `ciiIPRAType` MIB object does not support manually created IP reachability addresses.

The `ciiLSPSummaryEntry` table (LSP Summary Table) provides LSP summary information.

The `ciiLSPSummaryEntry` table defines the following MIB objects:

- `ciiLSPLevel`
- `ciiLSPID`
- `ciiLSPSeq`
- `ciiLSPZeroLife`
- `ciiLSPChecksum`
- `ciiLSPLifetimeRemain`
- `ciiLSPPDULength`
- `ciiLSPAttributes`

The `ciiLSPTLVEntry` table provides a complete record of all LSPs as a sequence of {Type, Length, Value} tuples. The `ciiLSPTLVEntry` table defines the following MIB objects:

- `ciiLSPTLVIndex`
- `ciiLSPTLVSeq`
- `ciiLSPTLVChecksum`
- `ciiLSPTLVType`
- `ciiLSPTLVLen`
- `ciiLSPTLVValue`

Fields that are required for notifications are recorded in the `ciiNotificationEntry` table. The `ciiNotificationEntry` table is not meant for query since the MAX-ACCESS clause of the MIB objects is “accessible-for-notify.” The information for notifications will be directly provided at the time of event generation. The following MIB objects are used only in trap notifications where their value is determined and directly based on input parameters for the IS-IS trap generation process.

- `ciiPduLspId`
- `ciiPduFragment`
- `ciiPduFieldLen`
- `ciiPduMaxAreaAddress`
- `ciiPduProtocolVersion`
- `ciiPduLspSize`
- `ciiPduOriginatingBufferSize`
- `ciiPduProtocolsSupported`
- `ciiAdjState`
- `ciiErrorOffset`
- `ciiErrorTLVType`
- `ciiNotifManualAddress`
- `ciiNotifIsLevelIndex`

**Note**

The MIB objects `ciiNotifManualAddress` and `ciiNotifIsLevelIndex` were added separately and are not defined in draft-ietf-isis-wg-mib-16.txt. These have been provided as a replacement for `ciiManAreaAddr` and `ciiSysLevelIndex` respectively to be used only in trap notifications. They have a MAX-ACCESS clause of “accessible-for-notify.”

Cisco IS-IS MIB Trap Notifications

The following sections describe the traps that you can enable when you configure the IS-IS MIB feature:

- [IS-IS MIB for Generic, System-Wide Errors, page 10](#)
- [IS-IS MIB for LSP-Specific Errors, page 10](#)
- [MIB Support for IS-IS Hello PDU-Specific Errors, page 11](#)
- [MIB Support for IS-IS Transition State Changes, page 11](#)

IS-IS MIB for Generic, System-Wide Errors

The following MIB trap objects are for generic, system-wide errors that can occur in the IS-IS network:

- **ciiManualAddressDrops**—The **ciiManualAddressDrops** trap is generated when one of the manually configured area addresses assigned to the system is ignored while computing routes.
- **ciiAuthenticationFailure**—The **ciiAuthenticationFailure** trap is generated when the authenticating type information field in the PDU received from a circuit is incorrect. This is an edge-triggered notification.
- **ciiIDLenMismatch**—When an LSP with a different value of SystemID length is received, the **ciiIDLenMismatch** notification is generated specific to the circuit where the LSP was detected. This is an edge-triggered notification and hence will be generated only once for PDUs received on the same circuit.
- **ciiMaxAreaAddressesMismatch**—When the value of Maximum Area Addresses is changed in the LSP that is received from a circuit, the **ciiMaxAreaAddressesMismatch** trap notification is generated. The header of the packet is used to identify the cause of the mismatch in Maximum Area Address. This trap is an edge-triggered notification and hence will be generated only once for PDUs received on the same circuit.

IS-IS MIB for LSP-Specific Errors

The following MIB trap objects are for LSP-specific errors that can occur in the IS-IS network:

- **ciiCorruptedLSPDetected**—When an LSP stored in memory is corrupted, the **ciiCorruptedLSPDetected** trap is generated.
- **ciiAttemptToExceedMaxSequence**—The **ciiAttemptToExceedMaxSequence** trap is generated each time a sequence number on a generated LSP wraps around the 32-bit sequence counter, forcing it to be purged and hence waiting for its reannouncement.
- **ciiOwnLSPPurge**—The **ciiOwnLSPPurge** trap is generated when a LSP is received from a circuit with your systemID and zero age.
- **ciiSequenceNumberSkip**—When an LSP is received without a SystemID or differing contents, the **ciiSequenceNumberSkip** trap is generated in order to increment the sequence number by 1.
- **ciiAuthenticationTypeFailure**—When an LSP is received from a circuit filled with a wrong authentication type field, the **ciiAuthenticationTypeFailure** notification is generated. This is an edge-triggered notification.
- **ciiLSPTooLargeToPropagate**—When an attempt is made to send an LSP over the circuit with a size greater than **dataLinkBlockSize** (link-specific parameter for maximum size of a data packet), the **ciiLSPTooLargeToPropagate** trap is generated indicating that the LSP could not be propagated. This is an edge-triggered notification and will be generated only once for all PDUs received on the same circuit.

**Note**

Cisco IOS software does not support the condition that leads to this event. Therefore, this trap will not be generated.

- **ciiOrigLSPBuffSizeMismatch**—When an L1 or L2 LSP that has been received from a circuit has a size larger than the local value of `ciiOriginatingBufferSize`, or when an LSP has been received with the `ciiOriginatingBufferSize` option and there is a mismatch between local `ciiOriginatingBufferSize` and value of the PDU option field, this notification is generated. This is an edge-triggered notification and will be generated only once.

**Note**

The originating buffer size TLV that is used to advertise this condition is not currently supported in Cisco IOS software and sufficient information to determine which condition caused the trap is not available. Therefore, this trap will not be generated.

- **ciiProtocolsSupportedMismatch**—The `ciiProtocolsSupportedMismatch` trap is generated when a non-pseudonode segment 0 LSP is received that does not have any matching protocols supported. This is an edge-triggered notification.

**Note**

Cisco IOS software does not provide checks in the IS-IS implementation for detecting matching protocols in the case of received PDUs. The generation of the `ciiProtocolsSupportedMismatch` trap does not indicate a mismatch in protocols supported as specified in the protocol field of the received PDU.

- **ciiLSPErrorDetected**—The `ciiLSPErrorDetected` trap is generated to indicate that an LSP with a parse error has been received.

MIB Support for IS-IS Hello PDU-Specific Errors

The following MIB trap objects are for Hello PDU-specific errors that can occur in the IS-IS network:

- **ciiVersionSkew**—The `ciiVersionSkew` trap notification is generated when a Hello PDU is received from an IS running a different version of the IS-IS protocol. This is an edge-triggered notification and will be generated once for all PDUs received on the same circuit.
- **ciiAreaMismatch**—When a Hello PDU is received from an IS that does not share any area address, the `ciiAreaMismatch` notification is generated. This is an edge-triggered notification and will be generated only once for all PDUs received on the same circuit.
- **ciiRejectedAdjacency**—When a correct Hello PDU is received from an IS but adjacency is not established, the `ciiRejectedAdjacency` notification is generated to indicate that adjacency formation was not allowed. This is an edge-triggered notification.

MIB Support for IS-IS Transition State Changes

The following MIB trap objects are used to notify the network manager when a transition state change has occurred for an IS:

- **ciiDatabaseOverload**—The `ciiDatabaseOverload` trap object is used to notify the network manager when the system enters or leaves the Overload state.
- **ciiAdjacencyChange**—When an IS-IS adjacency changes its state to UP or moves out of this state, it causes the `ciiAdjacencyChange` trap notification to be generated.

How to Enable IS-IS MIB

This section describes the configuration tasks for the IS-IS MIB feature. Each task in the list is described as either required or optional.

- [Configuring the Router to Send SNMP Notifications for IS-IS to a Host, page 12](#) (required)
- [Enabling All IS-IS Traps, page 13](#) (optional)
- [Enabling IS-IS Error Traps, page 15](#) (optional)
- [Enabling IS-IS State-Change Traps, page 16](#) (optional)
- [Verifying IS-IS MIB Traps on the Router, page 17](#) (optional)

Configuring the Router to Send SNMP Notifications for IS-IS to a Host

Perform this task to enable the router to send SNMP notifications (traps) defined in the IS-IS MIB to a host.

Prerequisites

SNMP must be enabled on your network.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **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]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
	Example: Router> enable	
Step 2	show running-config	Displays the running configuration to determine if an SNMP agent is already running. <ul style="list-style-type: none"> • If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify the information or change it as needed.
	Example: Router# show running-config	

	Command or Action	Purpose
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	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] Example: Router(config)# snmp-server host 172.16.1.1 traps version 3 mycommunitystring isis	Specifies the recipient (target host) for IS-IS SNMP notification operations. <ul style="list-style-type: none"> If no <i>notification-type</i> is specified, all enabled notifications (traps or informs) will be sent to a specified host. If you want to send only IS-IS notifications to the specified host, you can use the optional isis keyword as the value for the <i>notification-type</i> argument. (See the example.)
Step 5	end Example: Router(config)# end	Ends your configuration sessions and exits global configuration mode.

Examples

The following example configures the router to send SNMP notifications for IS-IS to a host:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server host 172.31.1.1 traps version 3 mycommunity string isis
```

What to Do Next

If you want to globally enable all IS-IS traps, refer to the [“Enabling All IS-IS Traps” section on page 13](#). If you want to enable groups of IS-IS traps, refer to the [“Enabling IS-IS Error Traps” section on page 15](#) and the [“Enabling IS-IS State-Change Traps” section on page 16](#).



Enabling All IS-IS Traps

SNMP notifications can be configured on the router only after MIB support is enabled. This task shows how to configure IS-IS MIB and how to (optionally) enable all IS-IS traps. Once you have enabled all IS-IS traps, you can choose to selectively disable one or more specific traps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps isis**
4. **no snmp-server enable traps isis** [errors [error-type]] [state-change [state-change-type]]
5. **exit**
6. **show running-config** [options]

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 isis Example: Router(config)# snmp-server enable traps isis	Enables all SNMP notifications defined in the IS-IS MIB. <div>  Note This step is required only if you wish to enable all IS-IS traps. To enable specific groups of traps, see the “Enabling IS-IS Error Traps” section on page 15 or the “Enabling IS-IS State-Change Traps” section on page 16. </div> <div>When you enter the no snmp-server enable traps isis command, all IS-IS traps will be disabled.</div>
Step 4	no snmp-server enable traps isis [error-type] [state-change [state-change-type]] Example: Router(config)# no snmp-server enable traps isis state-change database-overload	Disables the sending of SNMP notifications for IS-IS state changes. <div>  Note This step is required only if you wish to disable a particular trap or set of traps. To enable specific groups of traps, see the “Enabling IS-IS Error Traps” section on page 15 or the “Enabling IS-IS State-Change Traps” section on page 16. </div>
Step 5	exit Example: Router(config)# exit	Returns to privileged EXEC mode.
Step 6	show running-config [options] Example: Router# show running-config include traps	Displays the running configuration to verify which traps have been enabled.

Examples

The following example shows how to globally enable all IS-IS traps:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps isis
```

What to Do Next

If you do not wish to enable all IS-IS traps, refer to the [“Enabling IS-IS Error Traps”](#) section on page 15 for enabling one or more IS-IS error traps, or refer to the [“Enabling IS-IS State-Change Traps”](#) section on page 16 for enabling one or more IS-IS state-change traps.

Enabling IS-IS Error Traps

You can enable SNMP notifications to be sent when IS-IS errors and mismatches related to invalid field values in PDUs are detected. Errors can be classified as generic (applied to all PDUs), LSP-related, and IS-IS Hello PDU-related. When you enter the **snmp-server enable traps isis errors** command without specifying any of the optional keywords and arguments, all IS-IS traps are enabled. You can enter specific keywords and arguments to enable certain traps. For more information on how to enable specific traps or groups of traps, refer to the **snmp-server enable traps isis** command page.

You can enable IS-IS traps for the following system-wide errors that apply to all PDUs:

- Authentication
- Authentication type
- System ID field length mismatch
- Manually-configured address drop
- Mismatch in maximum area address values

You can enable IS-IS traps for the following errors that apply specifically to IS-IS Hello PDUs:

- Adjacency creation failure
- Mismatch in the area addresses between ISs
- IS-IS protocol version mismatch

You can enable IS-IS traps for the following errors that apply specifically to LSPs:

- Mismatch in LSP and originating buffer size
- Attempt made to exceed a maximum sequence number
- LSP in-memory corruption with an invalid checksum
- Packet parse failure on a receiving circuit
- Protocol-supported mismatch for non-pseudonode LSP
- Invalid attempt to purge a the LSP of a local IS
- Propagation failure caused by an oversized LSP
- A system ID has been configured with a sequence number skip.

Complete the following task to enable one or more IS-IS error traps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps isis [errors [error-type]] [state-change [state-change-type]]**
4. **end**

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 isis [errors [error-type]] [state-change [state-change-type]] Example: Router(config)# snmp-server enable traps isis errors lsp	Enables SNMP notifications for IS-IS errors. <ul style="list-style-type: none"> When you enter the lsp keyword for the <i>error-type</i>, only the LSP error traps are enabled. (See the snmp-server enable traps command in the “Command Reference” section for a list of <i>error-type</i> keywords.)
Step 4	end Example: Router(config)# end	Ends your configuration sessions and exits global configuration mode.

Examples

The following example shows how to enable only the IS-IS traps related to authentication errors:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps isis errors authentication
```


Enabling IS-IS State-Change Traps

You can enable SNMP notifications to be sent when significant IS-IS state changes occur in the system. Perform this task to enable the IS-IS trap MIB objects `cliDatabaseOverload` and `cliAdjacencyChange`.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps isis** [state-change [state-change-type]]
4. **end**

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 isis [state-change [state-change-type]] Example: Router(config)# snmp-server enable traps isis state-change	Enables SNMP notifications for IS-IS state changes. <div>  Note When the snmp-server enable traps isis state-change command is entered without any of the optional keywords, both IS-IS state change traps are enabled. Entering the no snmp-server enable traps isis state-change command will disable both IS-IS state-change traps. </div>
Step 4	end Example: Router(config)# end	Ends your configuration sessions and exits global configuration mode.

Examples

The following example shows how to enable only the IS-IS traps related to adjacency transition state changes:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps isis state-change adjacency
```

Verifying IS-IS MIB Traps on the Router

This task verifies that you have enabled IS-IS MIB.

SUMMARY STEPS

1. enable
2. show running-config [options]

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	show running-config [<i>options</i>] Example: Router# show running-config include traps	Displays the contents of the currently running configuration file and includes information about enabled traps. <ul style="list-style-type: none"> Verifies if the traps have been enabled.

Configuration Examples for IS-IS MIB

This section provides the following configuration examples:

- [Enabling and Verifying IS-IS Error Traps: Example, page 18](#)
- [Enabling and Verifying IS-IS State Change Traps: Example, page 18](#)

Enabling and Verifying IS-IS Error Traps: Example

The following example enables all IS-IS error traps:

```
Router(config)# snmp-server enable traps isis
Router# end
```

The **show running-config** command is entered to verify that the traps are enabled:

```
Router# show running-config | include traps
snmp-server enable traps isis
```

Enabling and Verifying IS-IS State Change Traps: Example

The following example shows how to enable the `ciidatabaseOverload` and `ciimanualAddressDrops` traps:

```
Router(config)# snmp-server enable traps isis state-change database-overload
Router(config)# snmp-server enable traps isis errors manual-address-drop
Router(config)# end
```

The **show running-config** command is entered to verify that these traps are enabled:

```
Router# show running-config | include traps

snmp-server enable traps isis state-change database-overload
snmp-server enable traps isis errors manual-address-drop
```

Where to Go Next

For more information about SNMP and SNMP operations, refer to the “Configuring SNMP Support” section of the [Cisco IOS Network Management Configuration Guide](#).

Additional References

The following sections provide references related to the IS-IS MIB feature.

Related Documents

Related Topic	Document Title
Configuring IS-IS	“Configuring Integrated IS-IS” chapter of the Cisco IOS IP Routing Protocols Configuration Guide , Release 12.4
IS-IS commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<ul style="list-style-type: none">• Cisco IOS IP Routing Protocols Command Reference, Release 12.2SR• Cisco IOS IP Routing Protocols Command Reference, Release 12.2SB
SNMP configuration	Cisco IOS Network Management Configuration Guide , Release 12.4
SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<ul style="list-style-type: none">• Cisco IOS Network Management Command Reference• Cisco IOS Network Management Command Reference, Release 12.2SB

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-IETF-ISIS-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: http://www.cisco.com/go/mibs

RFCs

RFC	Title
IETF draft draft-ietf-isis-wg-mib-16.txt	<i>Management Information Base for IS-IS</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.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are modified.

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

snmp-server enable traps isis

To enable Simple Network Management Protocol (SNMP) notifications for Intermediate System-to-Intermediate System (IS-IS) errors and transition state changes, use the **snmp-server enable traps isis** command in global configuration mode. To disable all or some of the IS-IS SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps isis [errors [error-type]] [state-change [state-change-type]]
```

```
no snmp-server enable traps isis [errors [error-type]] [state-change [state-change-type]]
```

Syntax Description	errors	(Optional) Enables Simple Network Management Protocol (SNMP) notifications for errors and mismatches that occur as a result of invalid field values in PDUs that have been received on a circuit for an IS.
	<i>error-type</i>	<p>(Optional) One or more of the optional IS-IS error type keywords can follow the errors keyword:</p> <ul style="list-style-type: none"> • authentication—Enables SNMP notifications only for authentication failures in a PDU received by an IS. • authentication-type—Enables SNMP notifications only for invalid authentication type fields in a PDU received by an IS. • id-length-mismatch—Enables SNMP notifications only for mismatches in system ID field lengths. • iih—Enables SNMP notifications only for IS-IS Hello PDU errors. One or more of the following three optional IS-IS Hello PDU error keywords can follow the iih keyword: <ul style="list-style-type: none"> – adjacency-rejected—Enables SNMP notifications for link-state packet (LSP)-specific errors and mismatches. – area-mismatch—Enables SNMP notifications for mismatches in area addresses between ISs. – version-skew—Enables SNMP notifications for IS-IS protocol version mismatches. • lsp—Enables SNMP notifications only for LSP-specific errors and mismatches. One or more of the following eight optional IS-IS Hello PDU error keywords can follow the lsp keyword: <ul style="list-style-type: none"> – buffsize-mismatch—Enables SNMP notifications for buffer size mismatches for LSPs. – max-seq-overflow—Enables SNMP notifications for attempts to exceed the maximum sequence number. – packet-corrupt—Enables SNMP notifications for LSP in-memory corruptions with invalid checksums. – packet-parse—Enables SNMP notifications for packet parse failures on received circuit. – protocol-support—Enables SNMP notifications for supported protocol mismatches non-pseudonode LSPs. – purge-zero-age—Enables SNMP notifications for invalid attempts to purge the LSP of an IS. – size-exceeded—Enables SNMP notifications for oversized LSPs that cause propagation failures. – skip-sequence-number—Enables SNMP notifications for system ID duplications (the sequence number is greater than 1). • manual-address-drop—Enables SNMP notifications only for manually configured area addresses that have been dropped. • maxarea-mismatch—Enables SNMP notifications only for mismatches in maximum area address values.

state-change	(Optional) Enables SNMP notifications for all IS-IS transition state change traps.
<i>state-change-type</i>	<p>(Optional) One or both of the optional IS-IS transition state change keywords can follow the state-change keyword:</p> <ul style="list-style-type: none"> • adjacency—Enables SNMP notifications only for adjacency changes between IS-IS neighbors. • database-overload—Enables SNMP notifications only for authentication failures on IS-IS neighbors.

Command Default

This command is disabled by default. If you enter this command with no keywords, the default is to enable all SNMP notifications.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SG	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(31)SB3	This command was implemented on the Cisco 10000 series.

Usage Guidelines

To globally enable all IS-IS MIB traps, enter the **snmp-server enable traps isis** command in global configuration mode. If you want to disable one or more traps, you can enter the **no snmp-server enable traps isis errors** command or the **no snmp-server enable traps isis state-change** command followed by the keywords that represent the traps that you want to disable. Entering the **no snmp-server enable traps isis errors** command without any keywords will disable all IS-IS error traps. Entering the **no snmp-server enable traps isis state-change** command without any keywords will disable all IS-IS state-change traps.

Examples

The following example shows how to enable the router to send IS-IS SNMP notifications only for IS-IS errors involving authentication to the host at the address myhost.cisco.com using the community string defined as public:

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

The following example shows how to enable the router to send IS-IS SNMP notifications for state changes involving adjacencies between Intermediate Systems (ISs) to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.

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 vrrp 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.

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.

Feature Information for IS-IS MIB

Table 2 lists the release history for this feature.

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

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



Note

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

Table 2 Feature Information for IS-IS MIB

Feature Name	Releases	Feature Information
IS-IS MIB	12.2(25)SG 12.2(31)SB2 12.2(33)SRB 12.2(31)SB3	<p>This feature introduces MIB support for the Intermediate System-to-Intermediate System (IS-IS) link-state routing protocol. IS-IS is used as the link-state routing protocol of choice by major service providers. The IS-IS MIB feature offers service providers an improved capability to continuously monitor the changing state of an IS-IS network by use of MIB objects to gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant protocol events such as an authentication failure or a mismatch in area addresses between Intermediate Systems (ISs). The protocol information collected by the IS-IS MIB objects and trap objects can be used by the network manager to derive statistics that can help monitor and improve overall network performance.</p> <p>In 12.2(31)SB2, this feature was implemented on the Cisco 7000 series routers.</p> <p>In 12.2(31)SB3, this feature was implemented on the Cisco 10000 series routers.</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

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

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