

SNMP Inform Requests

Description

The SNMP Inform Requests feature allows routers to send inform requests to SNMP managers.

Routers can send notifications to SNMP managers when particular events occur. For example, an agent router might send a message to a manager when the agent router experiences an error condition.

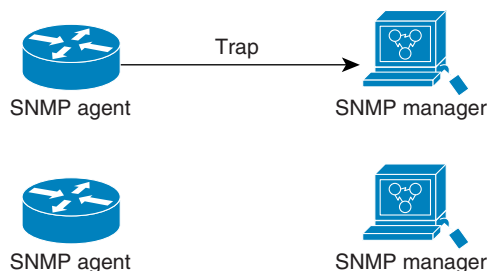
SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with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

Because they are more reliable, informs consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources. If it is important that the SNMP manager receives every notification, use inform requests. On the other hand, if you are concerned about traffic on your network or memory in the router and you do not need to receive every notification, use traps.

Figure 1 through Figure 4 illustrate the differences between traps and inform requests.

In Figure 1, the agent router successfully sends a trap to the SNMP manager. Although the manager receives the trap, it does not send any acknowledgment to the agent. The agent has no way of knowing that the trap reached its destination.

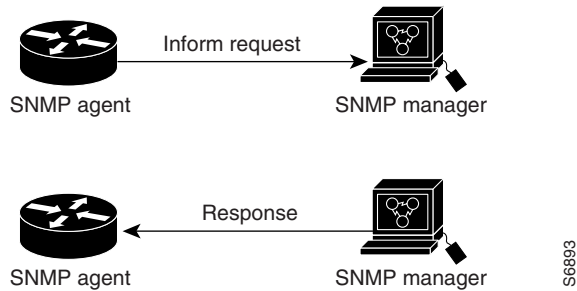
Figure 1 Trap Sent to SNMP Manager Successfully



S6892

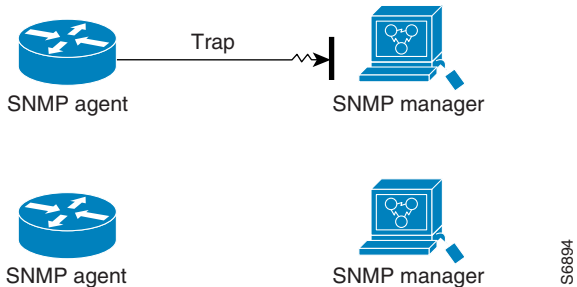
In Figure 2, the agent router successfully sends an inform request to the manager. When the manager receives the inform request, it sends a response back to the agent. Thus, the agent knows that the inform request successfully reached its destination. Notice that, in this example, twice as much traffic is generated as in Figure 1; however, the agent is sure that the manager received the notification.

Figure 2 Inform Request Sent to SNMP Manager Successfully



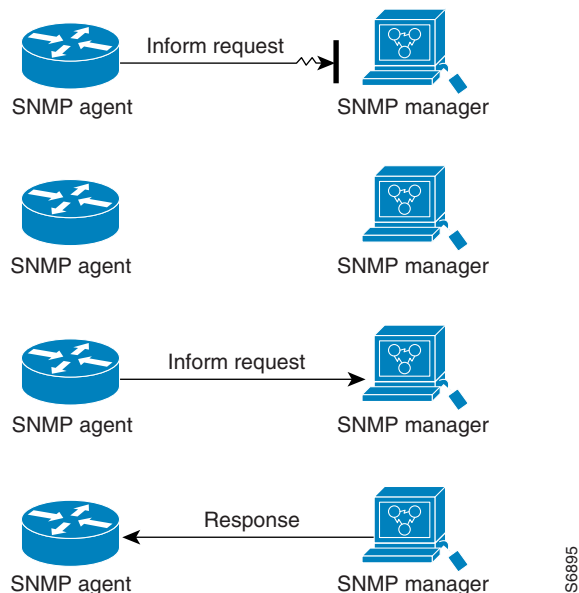
In Figure 3, the agent sends a trap to the manager, but the trap does not reach the manager. Since the agent has no way of knowing that the trap did not reach its destination, the trap is not sent again. The manager never receives the trap.

Figure 3 Trap Unsuccessfully Sent to SNMP Manager



In Figure 4, the agent sends an inform request to the manager, but the inform request does not reach the manager. Since the manager did not receive the inform request, it does not send a response. After a period of time, the agent will resend the inform request. The second time, the manager receives the inform request and replies with a response. In this example, there is more traffic than in Figure 3; however, the notification reaches the SNMP manager.

Figure 4 Inform Request Unsuccessfully Sent to SNMP Manager



S6895

Configuration Tasks

To configure the router to send SNMP traps, perform the following tasks. The second task is optional.

- Configure the Router to Send Traps
- Change Trap Operation Values

To configure the router to send SNMP informs, perform the following tasks. The second task is optional.

- Configure the Router to Send Informs
- Change Inform Operation Values

Configure the Router to Send Traps

To configure the router to send traps to a host, perform the following tasks in global configuration mode:

Task	Command
Specify the recipient of the trap message.	snmp-server host <i>host</i> [version {1 2c}] <i>community-string</i> [udp-port <i>port</i>] [<i>notification-type</i>]
Specify the types of traps sent. This command also specifies which types of informs are enabled.	snmp-server enable traps [<i>notification-type</i>] [<i>notification-option</i>]

The **snmp-server host** command specifies which hosts will receive traps. The **snmp-server enable traps** command globally enables the trap production mechanism for the specified traps.

Some traps are not controlled by the **snmp-server enable traps** command. These traps are either enabled by default or controlled through other commands. For example, by default, SNMP link traps are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by these traps may not be useful. Use the **no snmp trap link-status** interface configuration command to disable these traps.

In order for a host to receive a trap, an **snmp-server host** command must be configured for that host, and the trap must be enabled globally through the **snmp-server enable traps** command, through a different command, such as **snmp trap link-status**, or by default.

Change Trap Operation Values

Optionally, you can specify a value other than the default for the source interface, message (packet) queue length for each host, or retransmission interval.

To change trap operation values, perform any of the following optional tasks in global configuration mode:

Task	Command
Specify the source interface (and hence IP address) of the trap message. This command also sets the source IP address for informs.	snmp-server trap-source <i>interface</i>
Establish the message queue length for each trap host.	snmp-server queue-length <i>length</i>
Define how often to resend trap messages on the retransmission queue.	snmp-server trap-timeout <i>seconds</i>

Configure the Router to Send Informs

To configure the router to send informs to a host, perform the following tasks in global configuration mode:

Task	Command
Specify the recipient of the inform message.	snmp-server host <i>host informs</i> [version 2c] <i>community-string</i> [udp-port <i>port</i>] [<i>notification-type</i>]
Specify the types of inform requests sent. This command also specifies which types of traps are enabled.	snmp-server enable traps [<i>notification-type</i>] [<i>notification-option</i>]

The **snmp-server host** command specifies which hosts will receive informs. The **snmp-server enable traps** command globally enables the production mechanism for the specified notifications (traps and informs).

Some informs are not controlled by the **snmp-server enable traps** command. These informs are either enabled by default or controlled through other commands. For example, by default, SNMP link notifications are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by these notifications may not be useful. Use the **no snmp trap link-status** interface configuration command to disable these notifications.

In order for a host to receive an inform, an **snmp-server host informs** command must be configured for that host, and the inform must be enabled globally through the **snmp-server enable traps** command, through a different command, such as **snmp trap link-status**, or by default.

Change Inform Operation Values

Optionally, you can specify a value other than the default for number of retries, the retransmission interval, the maximum number of pending requests, or the source IP address.

To change inform operation values, perform the following optional task in global configuration mode:

Task	Command
Set options related to resending unacknowledged inform requests.	snmp-server informs [retries <i>retries</i>] [timeout <i>seconds</i>] [pending <i>pending</i>]
Specify the source interface (and hence IP address) of the inform request. This command also changes the source interface for traps.	snmp-server trap-source <i>interface</i>

Configuration Examples

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

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

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

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

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

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

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

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

Command Reference

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

show snmp

To check the status of SNMP communications, use the **show snmp** EXEC command.

show snmp

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

This command provides counter information for SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** command.

Sample Display

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

```
Router# show snmp

Chassis: 01506199
37 SNMP packets input
  0 Bad SNMP version errors
  4 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  24 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  28 Get-next PDUs
  0 Set-request PDUs
78 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  24 Response PDUs
  13 Trap PDUs

SNMP logging: enabled
  Logging to 171.69.58.33.162, 0/10, 13 sent, 0 dropped.

SNMP Manager-role output packets
  4 Get-request PDUs
  4 Get-next PDUs
  6 Get-bulk PDUs
  4 Set-request PDUs
  23 Inform-request PDUs
  30 Timeouts
  0 Drops
SNMP Manager-role input packets
  0 Inform response PDUs
  2 Trap PDUs
  7 Response PDUs
```

1 Responses with errors

```

SNMP informs: enabled
Informs in flight 0/25 (current/max)
Logging to 171.69.217.141.162
    4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
Logging to 171.69.58.33.162
    0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped

```

Table 1 describes the fields shown in the display.

Table 1 Show SNMP Field Descriptions

Field	Description
Chassis	Chassis ID string.
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of get requests received.
Get-next PDUs	Number of get-next requests received.
Set-request PDUs	Number of set requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object which does not exist.
Bad values errors	Number of SNMP set requests that specified an invalid value for a MIB object.
General errors	Number of SNMP set requests that failed due to some other error. (It was not a noSuchName error, badValue error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.
SNMP logging	Indicates whether logging is enabled or disabled.
sent	Number of traps sent.
dropped	Number of traps dropped. Traps are dropped when the trap queue for a destination exceeds the maximum length of the queue, as set by the snmp-server queue-length command.
SNMP Manager-role output packets	Information related to packets sent by the router as an SNMP manager.
Get-request PDUs	Number of get requests sent.

Table 1 Show SNMP Field Descriptions (Continued)

Field	Description
Get-next PDUs	Number of get-next requests sent.
Get-bulk PDUs	Number of get-bulk requests sent.
Set-request PDUs	Number of set requests sent.
Inform-request PDUs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of requests dropped. Reasons for drops include no memory, a bad destination address, or an unreasonable destination address.
SNMP Manager-role input packets	Information related to packets received by the router as an SNMP manager.
Inform response PDUs	Number of inform request responses received.
Trap PDUs	Number of SNMP traps received.
Response PDUs	Number of responses received.
Responses with errors	Number of responses containing errors.
SNMP informs	Indicates whether SNMP informs are enabled.
Informs in flight	Current and maximum possible number of informs waiting to be acknowledged.
Logging to	Destination of the following informs.
sent	Number of informs sent to this host.
in-flight	Number of informs currently waiting to be acknowledged.
retries	Number of inform retries sent.
failed	Number of informs that were never acknowledged.
dropped	Number of unacknowledged informs that were discarded to make room for new informs.

Related Commands

- snmp-server chassis-id**
- snmp-server queue-length**

snmp-server enable traps

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

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

Syntax Description

<i>notification-type</i>	<p>(Optional) Type of notification to enable. If no type is specified, all notifications are sent (including the envmon and repeater notifications). The notification type can be one of the following keywords:</p> <ul style="list-style-type: none"> • bgp—Sends Border Gateway Protocol (BGP) state change notifications. • config—Sends configuration notifications. • entity—Sends Entity MIB modification notifications. • envmon—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. When the envmon keyword is used, you can specify a <i>notification-option</i> value. • frame-relay—Sends Frame Relay notifications. • isdn—Sends Integrated Services Digital Network (ISDN) notifications. When the isdn keyword is used on Cisco 1600 series routers, you can specify a <i>notification-option</i> value. • repeater—Sends Ethernet hub repeater notifications. When the repeater keyword is selected, you can specify a <i>notification-option</i> value. • rtr—Sends response time reporter (RTR) notifications. • snmp—Sends Simple Network Management Protocol (SNMP) notifications. When the snmp keyword is used, you can specify a <i>notification-option</i> value. • syslog—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command.
<i>notification-option</i>	<p>(Optional) When the envmon keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: voltage, shutdown, supply, fan, and temperature.</p> <p>When the isdn keyword is used on Cisco 1600 series routers, you can specify the call-information keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the isdnu-interface keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem.</p>

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

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

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

Defaults

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

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

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

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

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

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

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

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

Examples

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

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

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

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

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

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

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

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

Related Commands

snmp-server host

snmp-server informs

snmp-server trap-source

snmp trap illegal-address

snmp-server host

To specify the recipient of an SNMP notification operation, use the **snmp-server host** global configuration command. Use the **no** form of this command to remove the specified host.

```
snmp-server host host [traps | informs] [version {1 | 2c}] community-string [udp-port port]
[notification-type]
no snmp-server host host [traps | informs]
```

Syntax Description

<i>host</i>	Name or Internet address of the host.
traps	(Optional) Send SNMP traps to this host. This is the default.
informs	(Optional) Send SNMP informs to this host.
version	(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps. <ul style="list-style-type: none"> • 1—SNMPv1. This option is not available with informs. • 2c—SNMPv2C.
<i>community-string</i>	Password-like community string sent with the notification operation.
udp-port <i>port</i>	UDP port of the host to use. The default is 162.
<i>notification-type</i>	(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords: <ul style="list-style-type: none"> • bgp—Sends Border Gateway Protocol (BGP) state change notifications. • config—Sends configuration notifications. • dspu—Sends downstream physical unit (DSPU) notifications. • entity—Sends Entity MIB modification notifications. • envmon—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • frame-relay—Sends Frame Relay notifications. • isdn—Sends Integrated Services Digital Network (ISDN) notifications. • llc2—Sends Logical Link Control, type 2 (LLC2) notifications. • rpnr—Sends standard repeater (hub) notifications. • rsrb—Sends remote source-route bridging (RSRB) notifications. • rtr—Sends response time reporter (RTR) notifications. • sdlc—Sends Synchronous Data Link Control (SDLC) notifications. • sdllc—Sends SDLLC notifications. • snmp—Sends Simple Network Management Protocol (SNMP) notifications defined in RFC 1157. • stun—Sends serial tunnel (STUN) notifications.

- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
- **tty**—Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes.
- **x25**—Sends X.25 event notifications.

Defaults

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

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

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

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

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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

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

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

- snmp-server enable traps**
- snmp-server informs**
- snmp-server trap-source**
- snmp-server trap-timeout**

snmp-server informs

To specify inform request options, use the **snmp-server informs** global configuration command. The **no** form of this command returns the settings to the defaults.

```
snmp-server informs [retries retries] [timeout seconds] [pending pending]  
no snmp-server informs [retries retries] [timeout seconds] [pending pending]
```

Syntax Description

retries <i>retries</i>	Maximum number of times to resend an inform request. The default is 3.
timeout <i>seconds</i>	Number of seconds to wait for an acknowledgment before resending. The default is 30 seconds.
pending <i>pending</i>	Maximum number of informs waiting for acknowledgments at any one time. When the maximum is reached, older pending informs are discarded. The default is 25.

Default

Inform requests are resent 3 times. Informs are resent after 30 seconds if no response is received. The maximum number of informs waiting for acknowledgments at any one time is 25.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

Examples

If you are seeing a large number of inform drops, you may want to increase the pending queue size.

```
snmp-server informs pending 50
```

If you are sending informs over slow network links, you may want to increase the default timeout. Since informs will be sitting in the queue for a longer period of time, you may also need to increase the pending queue size.

```
snmp-server informs timeout 60 pending 40
```

If you are sending informs over very fast links, you may want to decrease the default timeout.

```
snmp-server informs timeout 5
```

If you are sending informs over unreliable links, it may be desirable to increase the retry count. Since informs will be sitting in the queue for a longer period of time, you may need to increase the pending queue size.

```
snmp-server informs retries 10 pending 45
```

Related Commands

snmp-server enable traps