

配置支持的IOS SNMP陷阱

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[命令](#)

[snmp-server host命令](#)

[语法说明](#)

[默认设置](#)

[命令模式](#)

[全局配置 - 命令历史](#)

[使用指南](#)

[配置通知](#)

[Examples](#)

[snmp-server enable traps命令](#)

[语法说明](#)

[默认设置](#)

[命令模式](#)

[全局配置 - 命令历史](#)

[使用指南](#)

[相关信息](#)

简介

本文档介绍如何配置支持的Cisco SNMP陷阱。

先决条件

要求

Cisco 建议您了解以下主题：

不要让思科设备发送它知道如何发送的所有 SNMP 陷阱。例如，如果您启用一台拥有 64 条拨入线路的远程接入服务器中的所有陷阱，那么每当有用户呼入或终止连接，您都将收到一个陷阱。这样会创建太多陷阱。Cisco IOS®软件定义可以启用或禁用的陷阱组。有两种全局配置命令可用于为 Cisco IOS 软件设备配置 SNMP 陷阱：

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

发出 `snmp-server host global configuration` 命令指定SNMP通知操作的收件人。发出 `no` 此命令的形式删除指定的主机。

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

发出 `snmp-server enable traps global configuration` 命令使路由器能够发送SNMP陷阱。发出 `no` 此命令的格式来禁用SNMP通知。

两种命令中都可以指定陷阱类型。您必须发出 `snmp-server host </strong>` 命令定义要发送陷阱的网络管理系统。如果不希望发送所有陷阱，必须指定陷阱类型。发出多个 `snmp-server enable traps` 命令，对于您在 `snmp host` 命令。

**注：**并非全部 `[notification-type]` 这两个命令均支持选项。例如，`[notification-type] x25`和电传(tty)不用于 `snmp-server enable trap` 默认情况下，`x25` 和 `tty` 陷阱处于启用状态。

例如，发出以下命令使Cisco IOS软件设备仅向网络管理系统10.10.10.10报告配置、边界网关协议(BGP)和tty陷阱：

```
snmp-server host 10.10.10.10 public config bgp tty
snmp-server enable traps config
snmp-server enable traps bgp
```

## 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

## 背景信息

**注：**本文档使用Cisco IOS软件版本12.1(3)T。较低的 Cisco IOS 软件版本不支持其中部分选项。高于 12.1(3)T 的 Cisco IOS 软件版本可支持更多 `[notification-type]` 选项。在本文中，您能找到系统支持的Cisco IOS软件简单网络管理协议（SNMP）陷阱对象标识符（OID）的最新列表。

运行标准Cisco IOS软件(路由器、异步传输模式(ATM)交换机和远程访问服务器)的Cisco设备可以生成许多SNMP陷阱。

## 命令

### 此 `snmp-server host` 命令

发出 `snmp-server host global configuration` 命令指定SNMP通知操作的收件人。发出 `no` 此命令的形式删除

指定的主机。

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

## 语法说明

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host-addr         | 主机 ( 目标接收方 ) 的名称或互联网地址。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| traps             | ( 可选 ) 向此主机发送 SNMP 陷阱。这是默认设置。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| informs           | ( 可选 ) 向此主机发送 SNMP 通知。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| version           | ( 可选 ) 用于发送陷阱的 SNMP 的版本。版本3是最安全的型号，因为此型号允许使用 priv 本关键字，必须指定以下选项之一： <ul style="list-style-type: none"><li>• 1 - SNMPv1。通知中不可使用此选项。</li><li>• 2c - SNMPv2C</li><li>• 3 - SNMPv3。以下三个可选关键字可以位于version 3关键字之后：auth ( 可选 ) 启用散列算法(SHA)数据包身份验证。noauth ( 默认 ) noAuthNoPriv安全级别。未指定 [auth   priv]关键字选择。priv ( 可选 ) 启用数据加密标准(DES)数据包加密 ( 也称为“隐私” )。与通知操作一起发送的类似密码的社区字符串。尽管您可以通过 snmp-server host 命令本身 server community 命令，然后发出 snmp-server host 命令。</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| community-string  | 要使用的主机上的用户数据报协议 (UDP) 端口。默认值为 162。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| udp-port          | 要发送给主机的通知的类型。如不指定类型，将发送所有通知。通知类型可以是： <ul style="list-style-type: none"><li>• aaa-server — 发送AAA通知。</li><li>• bgp — 发送边界网关协议(BGP)状态更改通知。</li><li>• bstun — 发送块串行隧道(BSTUN)通知。</li><li>• calltracker — 发送CallTracker通知。</li><li>• config — 发送配置通知。</li><li>• dlsw — 发送数据链路交换(DLSw)通知。</li><li>• ds0-busyout — 发送ds0-busyout通知。</li><li>• ds1-loopback — 发送ds1-loopback通知。</li><li>• dspu — 发送下游物理单元(DSPU)通知。</li><li>• dsp — 发送数字信号处理(DSP)通知。</li><li>• entity — 发送实体管理信息库(MIB)修改通知。</li><li>• envmon — 在超过环境阈值时发送思科企业特定的环境监控器通知。</li><li>• frame-relay — 发送帧中继通知。</li><li>• hsrp — 发送热备份路由器协议(HSRP)通知。</li><li>• isdn — 发送集成多业务数字网络(ISDN)通知。</li><li>• msdp — 发送组播源发现协议(MSDP)通知。</li><li>• llc2 — 发送逻辑链路控制，第2类(LLC2)通知。</li><li>• repeater — 发送标准转发器 ( 集线器 ) 通知。</li><li>• rsrb — 发送远程源路由桥接(RSRB)通知。</li><li>• rsvp — 发送资源预留协议(RSVP)通知。</li><li>• rtr — 发送SA代理(RTR)通知。</li><li>• sdlc — 发送同步数据链路控制(SDLC)通知。</li><li>• snmp — 发送简单网络管理协议(SNMP)通知 ( 如RFC 1157中所定义 )。</li><li>• stun — 发送串行隧道(STUN)通知。</li><li>• syslog — 发送错误消息通知(Cisco Syslog MIB)。指定要与一起发送的消息的级别loggi</li><li>• tty — 在传输控制协议(TCP)连接关闭时发送思科企业特定通知。</li><li>• voice — 发送语音通知。</li></ul> |
| notification-type |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

- x25 — 发送X.25事件通知。
- xgcp — 发送外部媒体网关控制协议(XGCP)通知。

## 默认设置

此 `snmp-server host` 命令默认处于禁用状态。不会发送任何通知。

如果输入没有关键字的命令，默认情况是向主机发送所有陷阱类型。

没有通知会发送到此主机。如果否 `version` 存在关键字，默认为版本1。此 `no snmp-server host` 不带关键字的命令会禁用陷阱，但不会向主机发出通知。发出 `no snmp-server host informs` 命令禁用通知。

**注：**如果 `community-string` 未使用 `snmp-server community` 命令后才能使用此命令，该命令的默认形式 `snmp-server community` 命令会自动插入到配置中。密码 (`community-string`) 用于此自动配置的 `snmp-server community` 与 `snmp-server host` 命令。这是 Cisco IOS 软件版本 12.0(3) 及更高版本的默认行为。

## 命令模式

### 全局配置 - 命令历史

#### Cisco IOS 软件版本 修改

|          |                                                                                                                             |
|----------|-----------------------------------------------------------------------------------------------------------------------------|
| 10.0     | 引入此命令。<br>添加了这些关键字：                                                                                                         |
| 12.0(3)T | <ul style="list-style-type: none"><li>• <code>version 3 [auth   noauth   priv]</code></li><li>• <code>hsrp</code></li></ul> |

### 使用指南

SNMP 通知可以陷阱或通知请求的方式发送。陷阱方式不可靠，因为接收方不会在设备收到陷阱时发送确认消息。发送方无法确认陷阱是否已收到。然而，收到通知请求的SNMP实体识别带SNMP响应协议数据单元(PDU)的消息。如果发送方一直没收到回应，可以再次发送通知请求。这样通知更有可能安全到达预定目标。

不过，在代理和网络中，通知会消耗更多资源。与陷阱一发送就被抛弃不同，信息请求必须保存在内存中，直到收到答复或请求暂停为止。陷阱只会发送一次，而通知可能会重试多次。重试会增加流量，并且造成网络上的开销更高。

如果不输入 `snmp-server host` 命令，不发送通知。要将路由器配置为发送SNMP通知，必须至少输入一个 `snmp-server host` 命令。如果您输入没有关键字的命令，可以为主机启用所有陷阱类型。

要启用多台主机，您必须发出单独的 `snmp-server host` 命令。您可以在给每台主机的命令中指定多种通知类型。

当多个 `snmp-server host` 为同一主机和通知类型（陷阱或通知）指定命令，每个命令会覆盖上一个命令。仅最后一个 `snmp-server host` 命令会考虑在内。例如，如果输入 `snmp-server host inform` 命令，然后输入另一个命令 `snmp-server host inform` 命令，第二个命令取代第一个命令。

此 `snmp-server host` 命令与 `snmp-server enable` 命令。发出 `snmp-server enable` 命令，以指定全局发送哪些 SNMP 通知。为了让主机接收大多数通知，至少需要一个 `snmp-server enable` 命令和 `snmp-server host` 必须启用该主机的命令。

但是，某些通知类型不能通过 `snmp-server enable` 命令。例如，有些通知类型是始终启用的。其他通知类型需由其他命令启用。例如，`linkUpDown` 通知由 `snmp trap link-status` 命令。这些通知类型不需要 `snmp-server enable` 命令。

通知类型选项的可用性取决于路由器的类型和路由器支持的 Cisco IOS 软件功能。例如，`envmon notification-type` 仅在环境监控器是系统的一部分时才可用。

## 配置通知

要发送通知，请完成以下步骤：

1. 配置一个远程引擎 ID。
2. 配置一个远程用户。
3. 在远程设备上配置一个组。
4. 在远程设备上启用陷阱。
5. 启用 SNMP 管理器。

## Examples

如果您希望为陷阱配置唯一的 SNMP 社区字符串，但是要防止此字符串的 SNMP 轮询访问，您的配置中必须包含一个访问列表。在本例中，社区字符串被命名为“comaccess”，访问列表的数量限制为 10：

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

本例会将 SNMP 陷阱发送到通过名称 `myhost.cisco.com` 指定的主机。社区字符串被定义为 `comaccess`：

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

本例会将 SNMP 陷阱和思科环境监控器企业特定陷阱发送到地址 `172.30.2.160`：

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

本例使用社区字符串 `public` 允许路由器将所有陷阱发送到主机 `myhost.cisco.com`：

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

本例不发送陷阱到任何主机。不是所有主机都启用 BGP 陷阱，但只有 ISDN 陷阱能够发送到主机。

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

此示例使路由器能够使用社区字符串public将所有通知请求发送到主机myhost.cisco.com:

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

本例会将 HSRP SNMPv2c 陷阱发送到通过名称 myhost.cisco.com 指定的主机。社区字符串被定义为 public。

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

## 此 `snmp-server enable traps` 命令

请使用 `snmp-server enable traps` 全局配置命令，使路由器能够发送SNMP陷阱。请使用 `no` 此命令的形式以禁用SNMP通知。

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

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

## 语法说明

(可选) 要启用的通知的类型。如果未指定类型，则发送所有通知(包括 `envmon` 和 `repeat`)

- `aaa-server` — 发送AAA服务器通知。此关键字从 Cisco IOS 软件版本 12.1(3)T 起添加。通知内容为：`enterprise 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange`
- `bgp` — 发送边界网关协议(BGP)状态更改通知。此关键字来自BGP4-MIB，通知内容为：`enterprise 1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification 2 cctCallTermination`
- `calltracker` — 每次在cctActiveTable中创建新的活动呼叫条目或在cctHistoryTable中创建新的条目。通知内容为：`enterprise 1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification 2 cctCallTermination`
- `config` — 发送配置通知。此关键字来自CISCO-CONFIG-MAN-MIB，通知内容为：`enterprise 1.3.6.1.4.1.9.10.101.1 1 configChangeNotification`
- `dial` — 每当成功的呼叫被清除、失败的呼叫尝试被确定为最终失败时，或者当收到或清除呼叫时。通知内容为：`enterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation 2 dialCtlPeerCallSetup`
- `dls` — 从DLsw代理发送通知 `dls` 关键字时，可以指定 `notification-option-value`。通知内容为：`enterprise 1.3.6.1.4.1.9.10.101.1 1 ciscoDlswTrapTConnPartnerReject 2 ciscoDlswTrapTConnProviolation 3 ciscoDlswTrapTConnPartnerReject`
- `ds0-busyout` — 每当DS0接口的忙出状态更改时发送通知。此关键字从 Cisco IOS 软件版本 12.1(3)T 起添加。通知内容为：`enterprise 1.3.6.1.4.1.9.10.19.2 1 cpmDS0BusyoutNotification`
- `ds1-loopback` — 每当DS1接口进入环回模式时发送通知。此关键字从 Cisco IOS 软件版本 12.1(3)T 起添加。通知内容为：`enterprise 1.3.6.1.4.1.9.10.19.2 2 cpmDS1LoopbackNotification`
- `dspu` — 只要检测到物理单元(PU)或逻辑单元(LU)的操作状态更改或激活失败，就会发送通知。通知内容为：`enterprise 1.3.6.1.4.1.9.9.24.1.4.4 1newdspuPuStateChangeTrap 2 newdspuPuActivationFailureTrap 3 dspuLuActivationFailureTrap`
- `dsp` — 每当DSP卡启动或关闭时发送通知。此关键字来自CISCO-DSP-MGMT-MIB
- `entity` — 发送实体MIB修改通知。此关键字来自ENTITY-MIB，通知内容为：`enterprise 1.3.6.1.4.1.9.10.101.1 1 entityChangeNotification`
- `envmon` — 在超过环境阈值时发送思科企业特定的环境监控通知。当 `envmon` 关键字时

*notification-type*

- `enterprise 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonShutdownNotification 2 ciscoEnvMonFanNotification 5 ciscoEnvMonRedundantSupplyNotification`
  - **frame-relay** — 发送帧中继通知。此关键字来自RFC1315-MIB，通知内容为：`enterprise 1.3.6.1.4.1.9.9.106.2 1 cHsrpStateChange`
  - **hsrp** — 发送热备份路由器协议(HSRP)通知。此功能从 Cisco IOS 软件版本 12.0(3)T 起支持。此关键字来自CISCO-SDNU -MIB，通知为：`enterprise 1.3.6.1.4.1.9.9.106.2 1 cHsrpStateChange`
  - **isdn** — 发送ISDN通知。当**isdn**关键字时，可以指定`notification-option`。此关键字来自CISCO-SDNU -MIB，通知为：`enterprise 1.3.6.1.4.1.9.9.106.2 1 cHsrpStateChange`
  - **msdp** — 发送组播源发现协议(MSDP)通知。此关键字来自MSDP-MIB，通知内容为：`enterprise 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap`
  - **repeater** — 发送以太网集线器repeater通知。选择repeater关键字时，可以指定 `notification-option`
  - **rsvp** — 发送资源预留协议(RSVP)通知。此功能从 Cisco IOS 软件版本 12.0(2)T 起支持。此关键字来自CISCO-RESERVATION-MIB，通知为：`enterprise 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap`
  - **rtr** — 发送Service Assurance Agent RTR(RTR)通知。此关键字来自CISCO-RTTMON-MIB，通知为：`enterprise 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap`
  - **snmp** — 发送简单网络管理协议(SNMP)通知。当**snmp**关键字时，可以指定`notification-option`
  - **syslog** — 发送错误消息通知(Cisco Syslog MIB)。指定要与一起发送的消息的级别log
  - **voice** — 发送质量较差的语音通知。此关键字来自CISCO-VOICE-DIAL-CONTROL-MIB，通知为：`enterprise 1.3.6.1.2.1.11 0 coldStart 2 linkDown 3 linkUp 4 authenticationFailure 5 egpNeighborDown 6 tcpConnectionClose`
  - **xgcp** — 发送外部媒体网关控制协议(XGCP)通知。此关键字来自XGCP-MOB，通知为：`enterprise 1.3.6.1.2.1.11 0 coldStart 2 linkDown 3 linkUp 4 authenticationFailure 5 egpNeighborDown 6 tcpConnectionClose`
- (可选)
- **dls** [`circuit` | `tconn`]—当**dls**关键字时，您可以指定要启用或禁用的特定通知类型。如：`circuit` — 启用DLSw电路陷阱。`tconn` — 启用DLSw对等传输连接陷阱。
  - **envmon** [`voltage` | `shutdown` | `supply` | `fan` | `temperature`]—当**envmon**关键字，则您可以启用特定环境通知。选项可以是以下一个或多个关键字：`voltage,shutdown,supply,fan,和temperature`
  - **isdn** [`call-information` | `isdn u-interface` | `chan-not-avail` | `layer2`]—当**isdn**关键字时，您可以指定**isdn u-interface**关键字，用于为ISDN U接口MIB子系统启用SNMP ISDN U接口通知。
  - **repeater** [`health` | `reset`]—当 **repeater** 关键字，您可以指定repeater选项。如不指定选项，则为IETF中继器集线器MIB(RFC 1516)运行状况通知。`reset` — 启用IETF中继器集线器MIB(RFC 1516)重置运行状况通知。`reset` — 启用IETF中继器集线器MIB(RFC 1516)重置运行状况通知。
  - **snmp** [`authentication` | `linkup` | `linkdown` | `coldstart`]关键字 `linkup` | `linkdown` | `coldstart` 自Cisco IOS 12.0(2)T 起支持。如果没有关键字可以使用，所有SNMP提示类型都被启用(或者失效，如果使用no形式的命令)。`authenticationFailure(4)`陷阱表示，发送的协议实体是没有正确验证协议消息的收信方。当**linkdown**关键字时，发送的协议实体是通信链路已恢复。`linkdown` — 控制SNMP链路关闭通知的发送方向。`coldstart` — 控制SNMP coldstart通知的发送。`coldStart(0)`陷阱表示发送协议实体重置。

### notification-option

## 默认设置

SNMP 通知处于禁用状态。

如果您不使用通知类型关键字输入此命令，默认值是启用所有此命令控制的提示类型。

## 命令模式

### 全局配置 - 命令历史

## Cisco IOS 软件版本 修改

- 11.1 引入此指令。
- 12.0(2)T 此 `rsvp` 添加了关键字。
- 12.0(3)T 此 `hsrp` 添加了关键字。

这些关键字已添加到 `snmp-server enable traps snmp` 此命令的形式：

- `linkup`
- `linkdown`
- `coldstart`

添加了以下通知类型关键字，仅适用于 Cisco AS5300 平台：

12.1(3)T

- `ds0-busyout`
- `isdn chan-not-avail`
- `modem-health`
- `ds1-loopback`

添加了以下通知类型关键字，仅适用于 Cisco AS5300 和 AS5800 平台：

- `aaa-server`

## 使用指南

此 `snmp-server enable traps snmp [ linkup] [linkdown]` 此命令的形式替换了 `snmp trap link-status interface` 配置模式命令。

此 `no` 的形式 `snmp-server enable traps` 命令可用于禁用在网络上生成大量不必要噪音的通知。

SNMP 通知可以陷阱或通知请求的方式发送。此命令同时支持在指定通知类型中使用陷阱和通知请求。

如果不输入 `snmp-server enable traps` 命令，不会发送此命令控制的通知。要将路由器配置为发送这些 SNMP 通知，必须至少输入一个 `snmp-server enable traps` 命令。如果您输入没有关键字的命令，所有通知类型都会启用。如果输入带有关键字的命令，只启用与该关键字有关的提示类型。要启用多种类型的通知，您必须发出单独的 `snmp-server enable traps` 命令来指定通知类型和通知选项。

此 `snmp-server enable traps` 命令与 `snmp-server host` 命令。发出 `snmp-server host` 命令指定接收 SNMP 通知的主机。要发送通知，必须至少配置一个 `snmp-server host` 命令。

为了让主机接收由此命令控制的通知，主机和 `snmp-server enable traps` 命令和 `snmp-server host` 必须启用该主机的命令。如果通知类型不受此命令控制，则仅适用的 `snmp-server host` 命令必须启用。

此命令中使用的所有通知类型都有一个关联的 MIB 对象，可用于启用或禁用这些类型（例如：`HSRP` 陷阱通过 `HSRP` MIB 定义，`中继器陷阱` 通过 `中继集线器` MIB 定义，等等）。并非所有可用的通知类型 `snmp-server host` 命令具有 `notificationEnable` MIB 对象，因此其中一些对象无法通过 `snmp-server enable` 命令。

## 相关信息

- [思科技术支持和下载](#)



## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。