

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Comando snmp-server host](#)

[Descripción de la Sintaxis](#)

[Valores predeterminados](#)

[Modos de comando](#)

[Pautas para el uso](#)

[Configuración de notificaciones de información](#)

[Ejemplos](#)

[Comando snmp-server enable traps](#)

[Descripción de la Sintaxis](#)

[Valores predeterminados](#)

[Modos de comando](#)

[Pautas para el uso](#)

[Información Relacionada](#)

[Introducción](#)

Nota: Cisco IOS Software Release® 12.1(3)T fue utilizado para elaborar este documento. Cuando usa una versión del software IOS de Cisco anterior, no todas las opciones están soportadas. Cuando utiliza una versión de Cisco IOS Software posterior a la 12.1(3)T, se pueden soportar opciones [notification-type] adicionales. En este documento, puede encontrar una lista actual de todos los Identificadores de objetos (OID) de trampa del Protocolo de administración de red simple (SNMP) del software del IOS de Cisco soportados.

Los dispositivos de Cisco que funcionan con el software IOS estándar (Routers, Switches del Asynchronous Transfer Mode (ATM) y los servidores del Acceso Remoto) de Cisco pueden generar mucho SNMP traps.

[prerrequisitos](#)

[Requisitos](#)

Los Quien lea este documento deben entender esta información:

Usted no quisiera que un dispositivo de Cisco enviara todo el SNMP traps que el dispositivo sepa enviar. Por ejemplo, si usted habilita todos los desvíos en un Remote Access Server con 64 líneas dial in, usted consigue un desvío siempre que un usuario marque adentro y siempre que un usuario termina la conexión. Esto crea demasiadas trampas. El Cisco IOS Software define los grupos de desvíos que usted pueda habilitar o inhabilitar. Hay dos comandos global configuration

que usted utiliza para configurar el SNMP traps en un dispositivo del Cisco IOS Software:

- **host-addr del host del SNMP-servidor [desvíos | informa] [la versión {1 | 2c | 3 [auth | noauth | cadena de comunidad del priv]] [udp-port port] [notification-type]** Publique el comando **snmp-server host global configuration** de especificar al beneficiario de una operación de la notificación SNMP. No publique la **ninguna** forma de este comando de quitar el host especificado.
- **el permiso del SNMP-servidor atrapa [notification-type] [notification-option]** Publique el comando **snmp-server enable traps global configuration** de permitir al router para enviar el SNMP traps. No publique la **ninguna** forma de este comando para inhabilitar las notificaciones SNMP.

Los tipos de trampas se pueden especificar en ambos comandos. Usted debe publicar el comando **snmp-server host** para definir los sistemas de administración de red donde están ser enviado los desvíos. Usted debe especificar los tipos de trampa si usted no quisiera que todos los desvíos fueran enviados. Publique multiple **snmp-server** los **comandos enable traps**, uno para cada uno de los tipos de trampa que usted utilizó en el **comando snmp host**.

Nota: No todas las opciones del [notification-type] se soportan en ambos comandos. Por ejemplo, [notification-type] el X.25 y el teletipo (equipo teleescritor) no se utilizan para el **snmp-server enable trap**. los desvíos X.25, y equipo teleescritor se habilitan por abandono.

Por ejemplo, publique estos comandos de hacer que un dispositivo del Cisco IOS Software señala solamente la configuración, el Border Gateway Protocol (BGP), y los desvíos equipo teleescritor al sistema de administración de red 10.10.10.10:

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

[Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

[Comando snmp-server host](#)

Publique el comando **snmp-server host global configuration** de especificar al beneficiario de una operación de la notificación SNMP. No publique la **ninguna** forma de este comando de quitar el host especificado.

```
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]
```

[Descripción de la Sintaxis](#)

| | |
|-----------|---|
| host-addr | El nombre o la dirección de Internet del host (el beneficiario apuntado). |
|-----------|---|

| | |
|------------------------------------|---|
| desvíos | (Opcional) Envíe trampas SNMP a este host. Este es el valor predeterminado. |
| informa | (Opcional) envíe el SNMP informa a este host. |
| versión | <p>(Opcional) la versión del SNMP usado para enviar los desvíos. La versión 3 es el modelo más seguro, pues este modelo permite la encriptación de paquetes con la palabra clave priv. Si usted utiliza la palabra clave de la versión, usted debe especificar una de estas opciones:</p> <ul style="list-style-type: none"> • 1?SNMPv1. Esta opción no se encuentra disponible con informes. • 2c?SNMPv2C • 3?SNMPv3. Estas tres palabras claves optativas pueden seguir la palabra clave de la versión 3: el auth (opcional) habilita la autenticación de paquete de la publicación de mensaje 5 (MD5) y del Secure Hash Algorithm (SHA). noauth (valor por defecto) el nivel de seguridad del noAuthNoPriv. Éste es el valor por defecto si [auth noauth priv] no se especifica la elección de la palabra clave. el priv (opcional) habilita la encriptación de paquetes del Data Encryption Standard (DES) (también llamada "aislamiento"). |
| <i>identificación de comunidad</i> | <p>Contraseña-como la cadena de comunidad enviada con la operación de notificación. Aunque usted puede fijar esta cadena con el comando snmp-server host en sí mismo, Cisco recomienda que usted define esta cadena con el comando snmp-server community antes de que usted publique el comando snmp-server host.</p> |
| udp-port port | El puerto del Protocolo de datagrama de usuario (UDP) del host a ser utilizado. El valor predeterminado es 162. |
| tipo de notificación | <p>(Opcional) el Tipo de notificación que se enviará al host. Si no se especifica ningún tipo, se envían todas las notificaciones. El tipo de notificación puede ser uno o más de estas palabras claves:</p> <ul style="list-style-type: none"> • ¿AAA-servidor? Envía notificaciones de AAA. • ¿BGP? Envía notificaciones de cambio del estado del protocolo de la puerta de enlace de frontera (BGP). |

- ¿**bstun**? Envía las notificaciones de la tunelización en serie de bloques (BSTUN).
- ¿**calltracker**? Envía las notificaciones de CallTracker.
- ¿**config**? Envía notificaciones de configuración.
- ¿**dls**? Envía notificaciones de Conmutación de link de datos (DLSw).
- notificaciones **ds0-busyout**? Sends ds0-busyout.
- notificaciones **ds1-loopback**? Sends ds1-loopback.
- ¿**dspu**? Envía notificaciones de downstream physical unit (DSPU) (unidad física indirecta).
- ¿**dsp**? Envía las notificaciones del procesamiento de señal digital (DSP).
- ¿**entidad**? Envía notificaciones de modificación de la base de información para administración (MIB) de entidades.
- ¿**envmon**? Envía notificaciones de monitoreo de entorno de la empresa Cisco cuando se excede un umbral de entorno.
- ¿**Frame Relay**? Envía notificaciones de retransmisión de tramas.
- ¿**hsrp**? Envía las notificaciones del Hot Standby Router Protocol (HSRP).
- ¿**isdn**? Envía notificaciones de Red digital con servicio integrado (ISDN).
- ¿**msdp**? Envía notificaciones de protocolo de detección del origen de multidifusión (Multicast Source Discovery Protocol o MSDP).
- Logical Link Control **llc2**? Sends, notificaciones del tipo-2 (LLC2).
- ¿**repetidor**? Notificaciones de la manda repetidor standard (concentrador).
- ¿**rsrb**? Envía notificaciones de bridging remoto con ruteo de origen (RSRB).
- ¿**rsvp**? Envía notificaciones del Protocolo de reserva del recurso (RSVP).
- ¿**rtr**? Notificaciones del Sends SA Agent (RTR).

| | |
|--|---|
| | <ul style="list-style-type: none"> • ¿SDLC? Envía notificaciones de Control de link de datos síncronos (SDLC). • ¿SNMP? Envía las notificaciones del Simple Network Management Protocol (SNMP) (según lo definido en el RFC 1157). • ¿aturda? Envía notificaciones de Túnel en serie (STUN). • ¿Syslog? Envía notificaciones de mensaje de error (Cisco Syslog MIB). Especifique el nivel de mensajes que se enviarán con el comando logging history level. • ¿equipo teleescritor? Envía notificaciones específicas de empresa de Cisco cuando se cierra una conexión de Protocolo de control de transmisión (TCP). • ¿Voz? Envía las notificaciones de la Voz. • notificaciones de evento x25?Sends X.25. • ¿xgcp? Envía las notificaciones del protocolo external media gateway control (XGCP). |
|--|---|

Valores predeterminados

El comando `snmp-server host` se inhabilita de manera predeterminada. No se envían notificaciones.

Si ingresa este comando sin palabras clave, todos los tipos de trampas se envían al host de forma predeterminada.

Ningún informa se envían a este host. Si no hay **palabra clave de la versión** presente, el valor por defecto es versión 1. **El comando no `snmp-server host` sin las palabras claves inhabilita los desvíos, pero no informa, al host. Publique el comando no `snmp-server host informs` de inhabilitar informa.**

Nota: Si la *cadena de comunidad* no se define con el **comando `snmp-server community`** antes de que usted utilice este comando, la forma predeterminada del **comando `snmp-server community`** se inserta automáticamente en la configuración. La contraseña (*community-string*, identificación de la comunidad) empleada para esta configuración automática del comando `snmp-server community` es la misma que la especificada en el comando `snmp-server host`. Este es el comportamiento predeterminado de la versión 12.0(3) del software Cisco IOS y posterior.

Modos de comando

Configuración global – Historial de comandos

| Versión de software del IOS de Cisco | Modificación |
|--------------------------------------|---|
| 10.0 | Comando introducido |
| '12.0(3)T' | Se han agregado estas palabras claves: <ul style="list-style-type: none"> • versión 3 [auth noauth priv] • hsrp |

Pautas para el uso

Las notificaciones de SNMP pueden ser enviadas como solicitudes de trampa o de información. Los desvíos son no fiables porque el receptor no envía los acuses de recibo cuando este dispositivo recibe los desvíos. El remitente no puede determinar si las trampas fueron recibidas. Sin embargo, una entidad SNMP que recibe una petición de la información reconoce el mensaje con un unidad de datos del protocolo (PDU) de la respuesta SNMP. Si el remitente nunca recibe la respuesta, la petición de la información se puede enviar otra vez. Por lo tanto, informa son más probable alcanzar su destino deseado.

Sin embargo, las notificaciones de información consumen más recursos en el agente y en la red. A diferencia de una trampa, la cual se descarta tan pronto como se envía, un pedido de informe se debe mantener en la memoria hasta que se reciba una respuesta o se agote el tiempo de espera del pedido. Los desvíos se envían solamente una vez, mientras que una información se puede revisar varias veces. Los reintentos incrementan el tráfico y contribuyen a una sobrecarga mayor en la red.

Si usted no ingresa un **comando snmp-server host**, no se envía ningunas notificaciones. A fin de configurar el router para que envíe estas notificaciones SNMP debe ingresar, por lo menos, un comando snmp-server host. Si usted ingresa el comando sin las palabras claves, habilitan a todos los tipos de trampa para el host.

Para habilitar los host múltiples, usted debe publicar un **comando host del** servidor SNMP separado para cada host. Puede especificar varios tipos de notificación en el comando para cada host.

Cuando multiple snmp-server dan los **comandos host** para el mismo host y tipo de notificación (el desvío o informa), cada comando sobregaba el comando anterior. Sólo se considera el comando snmp-server host. Por ejemplo, si ingresa un comando snmp-server host inform para un host y luego ingresa otro comando snmp-server host inform para el mismo host, el segundo comando reemplazará al primero.

El comando snmp-server host se utiliza junto con el comando snmp-server enable. Publique el **comando snmp-server enable** para especificar qué notificaciones SNMP se envían global. Para que un host reciba la mayoría de las notificaciones, por lo menos un **comando snmp-server enable** y el **comando snmp-server host** para ese host deben ser habilitados.

Sin embargo, algunos tipos de notificación no pueden ser controlados con el **comando snmp-server enable**. Por ejemplo, algunas tipos de notificación están siempre habilitadas. Un diverso comando habilitan a otros tipos de notificación. Por ejemplo, las notificaciones linkUpDown son controladas por el comando snmp trap link-status. Estos tipos de notificación no requieren un

comando `snmp-server enable`.

La Disponibilidad de una opción del tipo de notificación depende del tipo del router y de las Características del Software Cisco IOS soportados en el router. Por ejemplo, el tipo de notificación del `envmon` está disponible solamente si el monitor de entorno es parte del sistema.

Configuración de notificaciones de información

Complete estos pasos para poder enviar una información:

1. Configure una ID de motor remoto.
2. Configure un usuario remoto.
3. Configure a un grupo en un dispositivo remoto.
4. Habilite trampas en el dispositivo remoto.
5. Habilite el administrador SNMP.

Ejemplos

Si usted quiere configurar una cadena de comunidad SNMP única para los desvíos, pero usted quiere prevenir el acceso de la Consulta SNMP con esta cadena, la configuración debe incluir una lista de acceso. En este ejemplo, la cadena de comunidad se nombra los "comaccess," y la lista de acceso se numera 10:

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

Este ejemplo envía el SNMP traps al host especificado por el nombre myhost.cisco.com. La identificación de comunidad se define como comaccess:

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

Este ejemplo envía el SNMP y el Cisco environmental monitor los desvíos específicos de la empresa para dirigir 172.30.2.160:

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

Este ejemplo permite al router para enviar todos los desvíos al host myhost.cisco.com con la cadena de comunidad pública:

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

Este ejemplo no envía los desvíos a ningún host. Las trampas BGP son activadas para todos los hosts pero sólo las trampas ISDN son activadas para ser enviadas a un host.

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

Este ejemplo permite al router para enviar todo informa a las peticiones al host myhost.cisco.com usando la cadena de comunidad pública:

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

Este ejemplo envía los desvíos del HSRP SNMPv2C al host especificado por el nombre myhost.cisco.com. La identificación de comunidad se define como pública.

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

Comando snmp-server enable traps

Utilice el comando **snmp-server enable traps global configuration** de permitir al router para enviar el SNMP traps. Use la opción no de este comando para deshabilitar las notificaciones SNMP.

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

Descripción de la Sintaxis

| | |
|-----------------------------|--|
| <i>tipo de notificación</i> | <p>(Opcional) el Tipo de notificación a habilitar. Si no se especifica a ningún tipo, se envían todas las notificaciones (envmon incluyendo y las notificaciones del repetidor). El tipo de notificación puede ser una de estas palabras claves:</p> <ul style="list-style-type: none">• ¿AAA-servidor? Envía las notificaciones del servidor de AAA. Esta palabra clave se incorpora a partir de la versión del software IOS de Cisco 12.1(3)T para las plataformas Cisco AS5300 y AS5800 únicamente. Esto es del CISCO-AAA-SERVER-MIB, y las notificaciones son: empresa 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange• ¿BGP? Envía notificaciones de cambio del estado del protocolo de la puerta de enlace de frontera (BGP). Esto es del BGP4-MIB, y las notificaciones son: la empresa 1.3.6.1.2.1.15.7 1 bgpEstablished el bgpBackwardTransition 2• ¿calltracker? Envía una notificación siempre que una nueva entrada de llamada activa se cree en el cctActiveTable o una nueva entrada de llamada del historial se crea en el cctHistoryTable esto es del CISCO-CALL-TRACKER-MIB, y las notificaciones son: empresa 1.3.6.1.4.1.9.9.163.2 1 cctCallTerminateNotification del cctCallSetupNotification 2• ¿config? Envía notificaciones de configuración. Esto es del CISCO-CONFIG-MAN-MIB, y las notificaciones son: empresa 1.3.6.1.4.1.9.9.43.2 1 ciscoConfigManEvent• ¿dial? Envía una notificación siempre que una llamada satisfactoria borre, un intento fallido de llamada se determina |
|-----------------------------|--|

para haber fallado en última instancia, o siempre que se reciba o se envíe un mensaje de configuración de llamada.

Esto es del [DIAL-CONTROL-MIB](#), y las notificaciones son: empresa

1.3.6.1.2.1.10.21.2 1

dialCtlPeerCallSetup del

dialCtlPeerCallInformation 2

- **¿dlsw?** Envía notificaciones desde los agentes DLSw Cuando la palabra clave dlsw es usada, puede especificar un valor de la opción de notificación. Esto es

del [CISCO-DLSW-MIB](#), y las

notificaciones son: empresa

1.3.6.1.4.1.9.10.9.1.7 1

ciscoDlswTrapCircuitDown del

ciscoDlswTrapCircuitUp 6 del

ciscoDlswTrapTConnDown 5 del

ciscoDlswTrapTConnUp 4 del

ciscoDlswTrapTConnProtViolation 3 del

ciscoDlswTrapTConnPartnerReject 2

- **ds0-busyout?** **Sends una** notificación siempre que el busyout de un estado de los cambios de la interfaz del DS0. Esta palabra clave se incorpora a partir de la versión del software de Cisco IOS

12.1(3)T para la plataforma Cisco

AS5300 únicamente. Esto es del [CISCO-](#)

[POP-MGMT-MIB](#), y la notificación es:

empresa 1.3.6.1.4.1.9.10.19.2 1

cpmDS0BusyoutNotification

- **ds1-loopback?** **Sends una** notificación siempre que la interfaz DS1 entre el Loopback Mode. Esta palabra clave se incorpora a partir de la versión del software de Cisco IOS 12.1(3)T para la plataforma Cisco AS5300 únicamente.

Esto es del [CISCO-POP-MGMT-MIB](#), y

la notificación es: empresa

1.3.6.1.4.1.9.10.19.2 2

cpmDS1LoopbackNotification

- **¿dspu?** Envía una notificación siempre que el estado operacional del physical unit (PU) o del logical unit (LU) cambie o detectan al error de activación. Esto es

del [CISCO-DSPU-MIB](#), y las

notificaciones son: empresa

1.3.6.1.4.1.9.9.24.1.5.3 del newdspuPuActivationFailureTrap
1newdspuPuStateChangeTrap 2 de la empresa 1.3.6.1.4.1.9.9.24.1.4.4 1 dspuLuActivationFailureTrap del newdspuLuStateChangeTrap 2

- ¿**dsp**? Envía una notificación siempre que vaya el indicador luminoso LED amarillo de la placa muestra gravedad menor del DSP hacia arriba o hacia abajo. Esto es del [CISCO-DSP-MGMT-MIB](#), y la notificación es: empresa 1.3.6.1.4.1.9.9.86.2 1 cdspMIBCardStateNotification
- ¿**entidad**? Envía notificaciones de modificaciones de Entity MIB. Esto es del [ENTITY-MIB](#), y las notificaciones son: empresa 1.3.6.1.2.1.47.2 1 entConfigChange
- ¿**envmon**? Envía las notificaciones del monitoreo de entorno del específico de empresa de Cisco cuando se excede un umbral de entorno. Cuando se utiliza la palabra clave envmon, se puede especificar un valor de la opción de notificación. Esto es del [CISCO-ENVMON-MIB](#), y las notificaciones son: empresa 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonRedundantSupplyNotification del ciscoEnvMonFanNotification 5 del ciscoEnvMonTemperatureNotification 4 del ciscoEnvMonVoltageNotification 3 del ciscoEnvMonShutdownNotification 2
- ¿**Frame Relay**? Envía notificaciones de retransmisión de tramas. Esto es del [RFC1315-MIB](#), y las notificaciones son: empresa 1.3.6.1.2.1.10.32 1 frDLCIStatusChange
- ¿**hsrp**? Envía las notificaciones del Hot Standby Router Protocol (HSRP). Esta característica se soporta desde el Cisco IOS Software Release 12.0(3)T. Esto es del [CISCO-HSRP-MIB](#), y las notificaciones son: empresa 1.3.6.1.4.1.9.9.106.2 1 cHsrpStateChange
- ¿**isdn**? Envía las notificaciones ISDN.

Cuando se utiliza la palabra clave isdn, puede especificar un valor de opción de notificación. Esto es del [CISCO-ISDN-MIB](#), y las notificaciones son: la empresa 1.3.6.1.4.1.9.9.26.2 1 [supported since Cisco IOS Software Release 12.1(5)T] del demandNbrCNANotification del [supported since Cisco IOS Software Release 12.1(1)T] 4 de los demandNbrCallDetails 3 demandNbrLayer2Change del demandNbrCallInformation 2 esto es del [CISCO-ISDNU-IF-MIB](#), y las notificaciones son: empresa 1.3.6.1.4.1.9.9.18.2 1 ciulfLoopStatusNotification

- ¿**msdp**? Envía notificaciones de protocolo de detección del origen de multidifusión (Multicast Source Discovery Protocol o MSDP). Esto es del [MSDP-MIB](#), y las notificaciones son: la empresa 1.3.6.1.3.92.1.1.7 1 msdpEstablished el msdpBackwardTransition 2
- ¿**repetidor**? Envía las **notificaciones del repetidor del** hub ethernet. Cuando se selecciona la palabra clave repeater, puede especificar un valor de opción de la notificación. Esto es del [CISCO-REPEATER-MIB](#), y las notificaciones son: empresa 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap
- ¿**rsvp**? Envía notificaciones del Protocolo de reserva del recurso (RSVP). Esta característica se soporta desde el Cisco IOS Software Release 12.0(2)T. Esto es del [RSVP-MIB](#), y las notificaciones son: empresa 1.3.6.1.3.71.2 1 lostFlow del newFlow 2
- ¿**rtr**? Envía notificaciones de Agente de servicio seguro (RTR) Esto es del [CISCO-RTTMON-MIB](#), y las notificaciones son: empresa 1.3.6.1.4.1.9.9.42.2 1 rttMonVerifyErrorNotification del rttMonThresholdNotification 4 del rttMonTimeoutNotification 3 del rttMonConnectionChangeNotification 2

| | |
|--------------------------------------|---|
| | <ul style="list-style-type: none"> • ¿SNMP? Envía las notificaciones del Simple Network Management Protocol (SNMP). Cuando se utiliza la palabra clave snmp, se puede especificar un valor de la opción de notificación. Esto es del CISCO-GENERAL-TRAPS, y las notificaciones son: empresa 1.3.6.1.2.1.11 0 empresas 1.3.6.1.4.1.9 del egpNeighborLoss del authenticationFailure 5 de la conexión 4 del linkdown 3 del coldstart 2 0 recargas Nota: Este desvío es controlado por el tipo de notificación “equipo teleescritor”:Nota: 1 tcpConnectionClose • ¿Syslog? Envía notificaciones de mensaje de error (Cisco Syslog MIB). Especifique el nivel de mensajes que se enviarán con el comando logging history level. Esto es del CISCO-SYSLOG-MIB, y las notificaciones son: empresa 1.3.6.1.4.1.9.9.41.2 1 clogMessageGenerated • ¿Voz? Envía las notificaciones de baja calidad de voz. Esto es del CISCO-VOICE-DIAL-CONTROL-MIBSMI, y las notificaciones son: empresa 1.3.6.1.4.1.9.9.63.2 1 cvdcPoorQoVNotification • ¿xgcp? Envía las notificaciones del protocolo external media gateway control (XGCP). Esto es del XGCP-MIB, y las notificaciones son: empresa 1.3.6.1.3.90.2 1 xgcpUpDownNotification |
| <p><i>opción de notificación</i></p> | <p>(Opcional)</p> <ul style="list-style-type: none"> • dlsw [circuito ¿tconn]? Cuando se utiliza la palabra clave del dlsw, usted puede especificar el tipo de notificación específico que usted desea habilitar o inhabilitar. Si no se utilizan palabras clave, se activan todos los tipos de notificaciones DLSw. La opción puede ser uno o más de estas palabras claves: <ul style="list-style-type: none"> ¿circuito? Habilita las trampas del circuito DLSw. ¿tconn? Habilita las trampas de conexión de transporte del par DLSw. • envmon [voltaje apagado fuente fan |

¿temperatura]? Cuando se utiliza la **palabra clave envmon**, usted puede habilitar un tipo de notificación de entorno específico, o valide todos los tipos de notificación del sistema de monitor de entorno. Si no se especifica ninguna opción, se habilitan todas las notificaciones de entorno. La opción puede ser uno o más de estas palabras claves: voltaje, apagado, suministro, ventilador y temperatura.

- **isdn [información de la llamada | isdn u-interface | chan-not-avail | se utiliza layer2]?When la palabra clave ISDN**, usted puede especificar la palabra clave de la **información de la llamada** para habilitar una notificación de información de la llamada ISDN SNMP para el subsistema ISDN MIB, o usted puede especificar la palabra clave del **isdn u-interface** para habilitar una notificación de la interfaz U SNMP ISDN para el subsistema MIB de la interfaz U ISDN.

- **repetidor [salud | ¿restauración]? Cuando se utiliza la palabra clave repeater**, usted puede especificar la opción de repetidor. Si no se especifica una opción, se activan todas las notificaciones de repetidor. La opción puede ser uno o más de estas palabras claves: integridad--Habilita la notificación de integridad MIB del eje de conexiones repetidor (RFC 1516) de Engineering Task Force (IETF) reiniciar--Activa la notificación de reinicio del MIB de eje de conexiones repetidor (RFC 1516) de IETF. ¿salud? Habilita la notificación sin problemas del MIB de eje de conexiones repetidor de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF) (RFC 1516). ¿restauración? Habilita la notificación de reinicio del MIB de eje de conexiones repetidor IETF (RFC 1516).

- **SNMP [autenticación | linkup | linkdown | link de palabras clave del coldstart] | linkdown | coldstart** agregado desde el Cisco IOS Software Release 12.1(3)T.

| | |
|--|--|
| | <p>¿? Cuando palabra clave snmp se utiliza, usted puede especificar el tipo de notificación específico que usted desea habilitar o inhabilitar. Si no se utiliza una palabra clave, todos los tipos de notificación SNMP están habilitados (o deshabilitados, si se utiliza la forma no). Los tipos de notificación disponibles son:</p> <p>¿autenticación? Controla la distribución de las notificaciones de fallas de la autenticación de SNMP. Una trampa por error de autenticación (4) significa que la entidad de protocolo de envío es la destinataria de un mensaje de protocolo que no está autenticado correctamente. ¿conexión? Controla el envío de las notificaciones del SNMP linkup. LinkUp(3) un desvío significa que la entidad de protocolo de envío reconoce que ha subido uno de los links de comunicación representados en la configuración del agente. ¿linkdown? Controla cómo se envían las notificaciones de interrupción del link SNMP. LinkDown(2) un desvío significa que la entidad de protocolo de envío reconoce un error en uno de los links de comunicación representados en la configuración del agente. ¿coldstart? Controla el envío de las notificaciones de arranque en frío SNMP. ColdStart(0) un desvío significa que la entidad de protocolo de envío se está reiniciando tales que la configuración del agente o de la implementación de la entidad de protocolo pudo ser alterada.</p> |
|--|--|

Valores predeterminados

Las notificaciones SNMP están desactivadas.

Si ingresa este comando sin palabras clave de notificación, la acción predeterminada será activar todos los tipos de notificación que este comando controla.

Modos de comando

Configuración global – Historial de comandos

| Versión de software del IOS de Cisco | Modificación |
|--------------------------------------|---|
| 11.1 | Este comando fue ingresado. |
| 12.0(2)T | La palabra clave del rsvp fue agregada. |
| '12.0(3)T' | Se agregó la palabra clave hrsp . |
| '12.1(3)T' | <p>Estas palabras claves se han agregado a la forma SNMP de los desvíos del permiso del SNMP-servidor de este comando:</p> <ul style="list-style-type: none">• linkup• linkdown• coldstart <p>Estas palabras claves del tipo de notificación se han agregado para la plataforma del Cisco AS5300 solamente:</p> <ul style="list-style-type: none">• ds0-busyout• isdn chan-not-avail• módem-salud• ds1-loopback <p>Esta palabra clave del tipo de notificación se ha agregado para el Cisco AS5300 and AS5800 platforms solamente:</p> <ul style="list-style-type: none">• aaa-server |

[Pautas para el uso](#)

La forma `snmp-server enable traps snmp` [enlace ascendente] [enlace descendente] de este comando reemplaza al comando `snmp trap link-status interface configuration mode`.

No hay la forma del comando `snmp-server enable traps` útil para inhabilitar las notificaciones que generan una gran cantidad de ruido innecesario en su red.

Las notificaciones de SNMP pueden ser enviadas como solicitudes de trampa o de información. Este comando habilita solicitudes de trampa y de información para tipos de notificación específicos.

Si usted no ingresa un **comando `snmp-server enable traps`**, no se envía ningunas notificaciones controladas por este comando. A fin de configurar el router para que envíe estas notificaciones SNMP debe ingresar, por lo menos, un comando `snmp-server enable traps`. Si ingresa el comando sin palabras clave, todos los tipos de notificación serán habilitados. Si introduce el comando con una palabra clave, sólo se habilita el tipo de notificación relacionado con esa palabra clave. A fin de habilitar varios tipos de notificaciones, debe ejecutar un comando `snmp-server enable traps` independiente para cada tipo de notificación y opción de notificación.

El comando `snmp-server enable traps` se utiliza junto con el comando `snmp-server host`. Publique el **comando `snmp-server host`** de especificar cuál recibe el host o los host las notificaciones SNMP. Para enviar notificaciones, debe configurar al menos un comando `snmp-server host`.

Para que un host reciba una notificación controlada por este comando, el **comando snmp-server enable traps** y el **comando snmp-server host** para ese host deben ser habilitados. Si este comando no controla al tipo de notificación, sólo el **comando snmp-server host** apropiado debe ser habilitado.

Los tipos de notificación usados en este comando all tienen un objeto de MIB asociado que permita que los habiliten o que sean inhabilitados (por ejemplo, los desvíos del HSRP se definen con el HSRP MIB, las trampas del repetidor se definen con el MIB de eje de conexiones repetidor, y así sucesivamente). No todos los tipos de notificación disponibles en el **comando snmp-server host** tienen objetos de MIB notificationEnable, así que algunos de éstos no se pueden controlar con el **comando snmp-server enable**.

[Información Relacionada](#)

- [Notificaciones de ATM SNMP y mejoras de OAM](#)
- [Soporte Técnico - Cisco Systems](#)