Configurar trampas SNMP de IOS admitidas

Contenido

Introducción

Este documento describe cómo configurar las trampas SNMP de Cisco admitidas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

No es conveniente que un dispositivo de Cisco envíe todas las capturas de SNMP que el dispositivo sabe cómo para enviar. Por ejemplo, si habilita todas las capturas en un servidor de acceso remoto con 64 líneas de acceso, recibirá una captura cada vez que un usuario acceda y cada vez que finalice la conexión. Esto crea demasiadas trampas. El software Cisco IOS® define grupos de trampas que puede habilitar o inhabilitar. Hay dos comandos de configuración global que puede utilizar para configurar las capturas de SNMP en un dispositivo con software Cisco IOS:

- **snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type]**
  Ejecute el comando snmp-server host global configuration para especificar el destinatario de una operación de notificación SNMP. Ejecute el comando **no** de este comando para quitar el host especificado.

- **snmp-server enable traps [notification-type] [notification-option]**
  Ejecute el comando**snmp-server enable traps global configuration**para permitir que el router envíe capturas SNMP. Ejecute el comando **no** de este comando para inhabilitar las notificaciones SNMP.

Los tipos de trampas se pueden especificar en ambos comandos. Debe emitir el comando **snmp-server host< /strong>** para definir los sistemas de administración de red donde se enviarán las trampas. Debe especificar los tipos de capturas si no desea que se envíen todas las capturas. Emitir varios **snmp-server enable traps** , uno para cada uno de los tipos de capturas que se utilizaron en el **snmp host** comando.

> **Nota**: no todas [*notification-type*] se admiten opciones en ambos comandos. Por ejemplo, [*notification-type*] x25 y teletipo (tty) no se utilizan para **snmp-server enable trap** Las capturas x25 y tty están habilitadas de manera predeterminada.

Por ejemplo, ejecute estos comandos para hacer que un dispositivo de Cisco IOS Software notifique solamente la configuración, el Protocolo de gateway fronterizo (BGP) y las trampas tty al Sistema de administración de redes 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.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

> **Nota**: Para preparar este documento se utilizó la versión 12.1(3)T del software del IOS de Cisco. 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 ejecutan el software Cisco IOS estándar (routers, switches de modo de transferencia asíncrono (ATM) y servidores de acceso remoto) pueden generar muchas trampas SNMP.

Comandos

snmp-server host Comando

Ejecute el comando **snmp-server host global configuration** para especificar el destinatario de una operación de notificación SNMP. Ejecute el comando **no** de este comando para 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 destinatario objetivo).
traps	(Opcional) Envíe trampas SNMP a este host. Este es el valor predeterminado.
informs	(Opcional) Enviar informes de SNMP a este host.
version	(Opcional) La versión de SNMP que se utiliza para enviar las capturas. La versión 3 es el modelo más seguro, ya que permite el cifrado de paquetes con el **priv** palabra clave. Si utiliz palabra clave “version”, debe especificar una de estas opciones: • 1: SNMPv1. Esta opción no se encuentra disponible con informes. • 2c: SNMPv2C • 3: SNMPv3. Estas tres palabras clave opcionales pueden ser posteriores a la palabra c version 3: **auth**(Opcional) Habilita la autenticación de paquetes Message Digest 5 (MD5) algoritmo hash seguro (SHA).**noauth** (Valor predeterminado) El nivel de seguridad noAuthNoPriv. Este es el valor predeterminado si [auth | noauth | priv] no se ha especificado la opción de palabra clave.**priv** (Opcional) Habilita el cifrado de paquetes d Estándar de cifrado de datos (DES) (también denominado "privacidad").
community-string	La cadena comunitaria similar a una contraseña que se envía con la operación de notificaci Aunque puede establecer esta cadena con el **snmp-server host** , Cisco recomienda que defina cadena con el comando **snmp-server community** antes de ejecutar el comando **snmp-server host** comando.
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	(Opcional) El tipo de notificación que se debe enviar al host. Si no se especifica ningún tipo envían todas las notificaciones. El tipo de notificación puede ser una o más de las siguiente palabras clave: • **aaa-server** —Envía notificaciones de AAA. • **bgp** —Envía notificaciones de cambio del estado del protocolo de la puerta de enlace de frontera (BGP).

- **bstun**: envía notificaciones de tunelación en serie por bloques (BSTUN).
- **calltracker**: envía notificaciones de CallTracker.
- **config**—Envía notificaciones de configuración.
- **dlsw**—Envía notificaciones de Conmutación de link de datos (DLSw).
- **ds0-busyout**: envía notificaciones ds0-busyout.
- **ds1-loopback**: envía notificaciones ds1-loopback.
- **dspu**—Envía notificaciones de downstream physical unit (DSPU) (unidad física indirecta
- **dsp**: envía notificaciones de procesamiento de señales digitales (DSP).
- **entity**—Envía notificaciones de modificación de la base de información para administrac (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 notificaciones del protocolo de router en espera en caliente (HSRP).
- **isdn**—Envía notificaciones de Red digital con servicio integrado (ISDN).
- **msdp**—Envía notificaciones de protocolo de detección del origen de multidifusión (Multic Source Discovery Protocol o MSDP).
- **llc2**: envía notificaciones de control de enlace lógico, tipo 2 (LLC2).
- **repeater**: envía notificaciones del repetidor estándar (hub).
- **rsrb**—Envía notificaciones de bridging remoto con ruteo de origen (RSRB).
- **rsvp**—Envía notificaciones del Protocolo de reserva del recurso (RSVP).
- **rtr**: envía notificaciones del agente SA (RTR).
- **sdlc**—Envía notificaciones de Control de link de datos síncronos (SDLC).
- **snmp**: envía notificaciones del protocolo simple de administración de red (SNMP) (como define en RFC 1157).
- **stun**—Envía notificaciones de Túnel en serie (STUN).
- **syslog**—Envía notificaciones de mensaje de error (Cisco Syslog MIB). Especifique el niv de mensajes que se enviarán con el**logging history level**comando.
- **tty**—Envía notificaciones específicas de empresa de Cisco cuando se cierra una conexi de Protocolo de control de transmisión (TCP).
- **voice**: envía notificaciones de voz.
- **x25**: envía notificaciones de eventos X.25.
- **xgcp**: envía notificaciones del protocolo de control de gateway de medios externos (XGC

Valores predeterminados

snmp-server host está desactivado de forma predeterminada. No se envían notificaciones.

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

No se envían informes a este host. Si no **version** está presente, el valor predeterminado es la versión 1. **no snmp-server host** comando sin palabras clave inhabilita las trampas, pero no informa, al host. Ejecute el comando **no snmp-server host informs** para desactivar los informes.

> Nota: si el *community-string* no se ha definido con el **snmp-server community** antes de utilizar este comando, la forma predeterminada del comando **snmp-server community** se inserta

automáticamente en la configuración. La contraseña (*community-string*) se utiliza para esta configuración automática del **snmp-server community** es el mismo que el especificado en el **snmp-server host** comando. 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 agregaron estas palabras clave: • **version 3 [auth | noauth | priv]** • **hsrp**

Pautas para el uso

Las notificaciones de SNMP pueden ser enviadas como solicitudes de trampa o de información. Las capturas son poco confiables, ya que el receptor no envía acuses de recibo cuando este dispositivo las recibe. El remitente no puede determinar si las trampas fueron recibidas. Sin embargo, una entidad de SNMP que recibe una solicitud de informe hace acuse de recibo del mensaje con una unidad de datos del protocolo (PDU) de respuesta SNMP. Si el emisor nunca recibe la respuesta, la solicitud de informe puede enviarse de nuevo. Por lo tanto, los informes tienen más probabilidad de llegar al 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. Las capturas se envían una sola vez, mientras que un informe puede intentar enviarse varias veces. Los reintentos incrementan el tráfico y contribuyen a una sobrecarga mayor en la red.

Si no introduce un **snmp-server host** , no se envían notificaciones. Para configurar el router para enviar notificaciones SNMP, debe ingresar al menos una **snmp-server host** comando. Si introduce el comando sin palabras clave, todos los tipos de capturas están habilitadas para el host.

Para habilitar varios hosts, debe emitir un comando independiente **snmp-server host** para cada host. Puede especificar varios tipos de notificación en el comando para cada host.

Cuando hay varios **snmp-server host** se dan comandos para el mismo host y tipo de notificación (trampa o informe), cada comando sobrescribe el comando anterior. Sólo el último **snmp-server host** se tiene en cuenta. Por ejemplo, si introduce un snmp-server host inform para un host y, a continuación, introduzca otro **snmp-server host inform** para el mismo host, el segundo comando reemplaza al primero.

snmp-server host se utiliza junto con el comando **snmp-server enable** comando. Ejecute el comando **snmp-server enable** para especificar qué notificaciones SNMP se envían globalmente. Para que un host reciba la mayoría de las notificaciones, al menos una **snmp-server enable** y el comando **snmp-server host** para ese host debe estar habilitado.

Sin embargo, algunos tipos de notificación no se pueden controlar con el **snmp-server enable**

comando. Por ejemplo, algunas tipos de notificación están siempre habilitadas. Otros tipos de notificación son habilitados por un comando diferente. Por ejemplo, el `linkUpDown` las notificaciones son controladas por el **snmp trap link-status** comando. Estos tipos de notificación no requieren un **snmp-server enable** comando.

La disponibilidad de una opción de tipo de notificación depende del tipo de router y de las funciones del software CISCO IOS admitidas en el router. Por ejemplo, el **envmon** notification-type está disponible sólo si el monitor de entorno forma parte del sistema.

Configurar informes

Siga los pasos detallados a continuación para poder enviar un informe:

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

Examples

Si desea configurar una única cadena comunitaria de SNMP para las capturas, pero desea evitar el acceso de sondeo de SNMP con esta cadena, la configuración debe incluir una lista de acceso. En este ejemplo, la cadena comunitaria se denomina “comaccess”, y la lista de acceso tiene el número 10:

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

En este ejemplo, las capturas de SNMP se envían al host especificado por el nombre myhost.cisco.com. La identificación de comunidad se define como comaccess:

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

En este ejemplo, se envían las capturas específicas de la empresa y de control ambiental de SNMP y Cisco a la dirección 172.30.2.160:

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

En este ejemplo, se habilita el router para que envíe todas las capturas al host myhost.cisco.com con la cadena comunitaria pública:

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

En este ejemplo, no se envían capturas 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 bgp
snmp-server host bob public isdn
```

Este ejemplo permite que el router envíe todas las solicitudes de informe al host myhost.cisco.com con la cadena de comunidad public:

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

En este ejemplo, las capturas de SNMPv2c HSRP se envían al host especificado por el nombre myhost.cisco.com. La identificación de comunidad se define como pública.

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

snmp-server enable traps Comando

Use el comando **snmp-server enable traps** comando de configuración global para permitir que el router envíe capturas SNMP. Use el comando **no** de este comando para desactivar las notificaciones SNMP.

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

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

Descripción de la Sintaxis

tipo de notificación

(Opcional) El tipo de notificación que desea habilitar. Si no se especifica ningún tipo, se envía todas las notificaciones (que incluyen **envmon** y **repeater** notificaciones). El tipo de notificación pu ser una de las siguientes palabras clave:

- **aaa-server**: envía notificaciones del servidor AAA. Esta palabra clave se incorpora a partir d versión del software IOS de Cisco 12.1(3)T para las plataformas Cisco AS5300 y AS580 únicamente. Proviene de CISCO-AAA-SERVER-MIB y las notificaciones son: enterprise 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). Proviene de BGP4-MIB, y las notificaciones son: enterprise 1.3.6.1.2.1.15 bgpEstablished 2 2 bgpBackwardTransition
- **calltracker** : envía una notificación cada vez que se crea una nueva entrada de llamada act en cctActiveTable o se crea una nueva entrada de llamada de historial en cctHistoryTabl Proviene de CISCO-CALL-TRACKER-MIB, y las notificaciones son: enterprise 1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification 2 cctCallTerminateNotification
- **config** —Envía notificaciones de configuración. Proviene de CISCO-CONFIG-MAN-MIB, y notificaciones son: enterprise 1.3.6.1.4.1.9.9.43.2 1 ciscoConfigManEvent
- **dial** : envía una notificación cada vez que se borra una llamada correcta, se determina qu

intento de llamada fallido ha fallado en última instancia o cuando se recibe o se envía un mensaje de configuración de llamada. Proviene de DIAL-CONTROL-MIB, y las notificacio son: enterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation 2 dialCtlPeerCallSetup

- **dlsw** : envía notificaciones de los agentes DLSw cuando el **dlsw** se utiliza, puede especifica *anotification*-optionvalue. Proviene de CISCO-DLSW-MIB, y las notificaciones son: enterp 1.3.6.1.4.1.9.10.9.1.7 1 ciscoDlswTrapTConnPartnerReject 2 ciscoDlswTrapTConnPortViolation 3 ciscoDlswTrapTConnUp 4 ciscoDlswTrapTConnDow ciscoDlswTrapCircuitUp 6 cisco DlswTrapCircuitDown
- **ds0-busyout**: envía una notificación cada vez que el busyout de una interfaz DS0 cambia d estado. 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. Proviene de CISCO-POP-MGMT MIB, y la notificación es: enterprise 1.3.6.1.4.1.9.10.19.2 1 cpmDS0BusyoutNotification
- **ds1-loopback**: envía una notificación cada vez que la interfaz DS1 entra en modo de loopba Esta palabra clave se incorpora a partir de la versión del software de Cisco IOS 12.1(3)T la plataforma Cisco AS5300 únicamente. Proviene de CISCO-POP-MGMT-MIB, y la notificación es: enterprise 1.3.6.1.4.1.9.10.19.2 2 cpmDS1LoopbackNotification
- **dspu**: envía una notificación siempre que cambia el estado de funcionamiento de la unida física (PU) o la unidad lógica (LU) o se detecta un fallo de activación. Proviene de CISC DSPU-MIB, y las notificaciones son: enterprise 1.3.6.1.4.1.9.9.24.1.4.4 1newdspuPuStateChangeTrap 2 newdspuPuActivationFailureTrap enterprise 1.3.6.1.4.1.9.9.24.1.5.3 1 newdspuLuStateChangeTrap 2 dspuLuActivationFailureTrap
- **dsp**: envía una notificación cada vez que la tarjeta DSP se activa o desactiva. Proviene d CISCO-DSP-MGMT-MIB, y la notificación es: enterprise 1.3.6.1.4.1.9.9.86.2 1 cdspMIBCardStateNotification
- **entity**—Envía notificaciones de modificaciones de Entity MIB. Proviene de ENTITY-MIB, y notificaciones son: enterprise 1.3.6.1.2.1.47.2.1 entConfigChange
- **envmon**: envía notificaciones de supervisión de entorno específicas de la empresa de Cisc cuando se supera un umbral de entorno. Cuando el**envmon**se utiliza, puede especificar *anotification*-optionvalue. Proviene de CISCO-ENVMON-MIB, y las notificaciones son: enterprise 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonShutdownNotification 2 ciscoEnvMonVoltageNotification 3 ciscoEnvMonTemperatureNotification 4 ciscoEnvMonFanNotification 5 ciscoEnvMonRedundantSupplyNotification
- **frame-relay**—Envía notificaciones de retransmisión de tramas. Proviene de RFC1315-MIB, notificaciones son: enterprise 1.3.6.1.2.1.10.32.1 frDLCIStatusChange
- **hsrp**: envía notificaciones del protocolo de router en espera en caliente (HSRP). Esta func se admite desde la versión del software Cisco IOS 12.0(3)T. Proviene de CISCO-HSRP- y las notificaciones son: enterprise 1.3.6.1.4.1.9.9.106.2.1 cHSRPStateChange
- **isdn**: envía notificaciones ISDN. Cuando el**isdn**se utiliza, puede especificar *anotification*-optionvalue. Proviene de CISCO-ISDN-MIB, y las notificaciones son: enterprise 1.3.6.1.4.1.9.9.26.2 1 demandNbrCallInformation 2 demandNbrCallDetails 3 demandNbrLayer2Change [compatible desde la versión 12.1(1)T del software Cisco IOS demandNbrCNANotification [compatible desde la versión 12.1(5)T del software Cisco IOS Proviene de CISCO-ISDNU-IF-MIB, y las notificaciones son: enterprise 1.1 3.6.1.4.1.9.9. 1 ciuIfLoopStatusNotification
- **msdp**—Envía notificaciones de protocolo de detección del origen de multidifusión (Multica Source Discovery Protocol o MSDP). Proviene de MSDP-MIB, y las notificaciones son: enterprise 1.3.6.1.3.92.1.1.7 1 msdpEstablished 2 msdpBackwardTransition

- **repeater**: envía un concentrador Ethernet**repeater**notificaciones. Cuando se selecciona la pa clave repeater, puede especificar una *notification-option* valor. Proviene de CISCO-REPEATE MIB, y las notificaciones son: enterprise 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTra
- **rsvp**—Envía notificaciones del Protocolo de reserva del recurso (RSVP). Esta función se admite desde la versión del software Cisco IOS 12.0(2)T. Proviene de RSVP-MIB, y las notificaciones son: enterprise 1.3.6.1.3.71.2 1 newFlow 2 lostFlow
- **rtr**—Envía notificaciones de Agente de servicio seguro (RTR) Proviene de CISCO-RTTM MIB, y las notificaciones son: enterprise 1.3.6.1.4.1.9.9.42.2 1 rttMonConnectionChangeNotification 2 rttMonTimeoutNotification 3 rttMonThresholdNotification 4 rttMonVerifyErrorNotification
- **snmp**: envía notificaciones del protocolo simple de administración de red (SNMP). Cuando el**snmp**, puede especificar un valor de opción de notificación. Proviene de CISCO-GENER TRAPS, y las notificaciones son: enterprise 1.3.6.1.2.1.11 0 coldStart 2 linkDown 3 linkU authenticationFailure 5 egpNeighborLoss enterprise 1.3.6.1.4.1.9 0 reload Nota: Esta tra es controlada por el tipo de notificación "tty": 1 tcpConnectionClose
- **syslog**—Envía notificaciones de mensaje de error (Cisco Syslog MIB). Especifique el nivel mensajes que se enviarán con el**logging history level**comando. Proviene de CISCO-SYSLO MIB, y las notificaciones son: enterprise 1.3.6.1.4.1.9.9.41.2.1 clogMessageGenerated
- **voice**: envía notificaciones de baja calidad de voz. Proviene de CISCO-VOICE-DIAL-CONTROL-MIBSMI, y las notificaciones son: enterprise 1.3.6.1.4.1.9.9.63.2 1 cvdcPoorQoVNotification
- **xgcp**: envía notificaciones del protocolo de control de gateway de medios externos (XGCP Proviene de XGCP-MOB, y las notificaciones son: enterprise 1.3.6.1.3.90.2 1 xgcpUpDownNotification

(Opcional)

- **dlsw [circuit | tconn]**: cuando el**dlsw**, puede especificar el tipo de notificación específico que d activar o desactivar. Si no se utilizan palabras clave, se activan todos los tipos de notificaciones DLSw. La opción puede ser una o más de las siguientes palabras clave: **circuit**—Habilita las trampas del circuito DLSw.**tconn**—Habilita las trampas de conexión de transporte del par DLSw.
- **envmon [voltage | shutdown | supply | fan | temperature]**: cuando el**envmon**, puede habilitar un tipo de notificación de entorno específico o aceptar todos los tipos de notificación del sistema de supervisión de entorno. Si no se especifica ninguna opción, se habilitan todas las notificaciones ambientales. La opción puede ser una o más de las siguientes palabras clave:**voltage**,**shutdown**,**supply**,**fan**,y**temperature**.

opción de notificación

- **isdn [call-information | isdn u-interface | chan-not-avail | layer2]**: cuando el**isdn**se utiliza, puede especi el**call-information**para habilitar una notificación de información de llamada ISDN SNMP para subsistema MIB ISDN, o puede especificar la palabra clave**isdn u-interface**para habilitar una notificación de interfaz SNMP ISDN U para el subsistema MIB de interfaz ISDN U.
- **repeater [health | reset]**: cuando el **repeater** se utiliza, puede especificar la opción repetidor. Si se especifica una opción, se activan todas las notificaciones de repetidor. La opción pued ser una o más de las siguientes palabras clave: health—Habilita la notificación de estado MIB de concentrador repetidor (RFC 1516) del Grupo de trabajo de ingeniería de Interne (IETF). reset—Habilita la notificación de restablecimiento de MIB de concentrador repetid (RFC 1516) de IETF. **health**: habilita la notificación de estado de MIB (RFC 1516) del hub repetidor del Grupo de trabajo de ingeniería de Internet (IETF).**reset**: habilita la notificació restablecimiento de MIB de concentrador repetidor IETF (RFC 1516).
- **snmp [authentication | linkup | linkdown | coldstart]**palabras clave **linkup | linkdown | coldstart** agregado

desde Cisco IOS Software Release 12.1(3)T. —Cuando el **snmp** , puede especificar el tipo notificación específico que desea activar o desactivar. Si no se utiliza una palabra clave, todos los tipos de notificación SNMP están habilitados (o deshabilitados, si se utiliza la fo no). Los tipos de notificación disponibles son los siguientes: **authentication**: controla la distribución de las notificaciones de fallos de autenticación SNMP. Una trampa por error autenticación (4) significa que la entidad de protocolo de envío es la destinataria de un mensaje de protocolo que no está autenticado correctamente.**linkup**: permite controlar el e de notificaciones de conexión SNMP. Una captura linkUp(3) significa que la entidad de protocolo emisora advierte que uno de los enlaces de comunicación que se representa e configuración del agente se ha conectado.**linkdown**: controla el modo en que se envían las notificaciones de enlace SNMP. Una captura linkUp(2) significa que la entidad de protoco emisora advierte que uno de los enlaces de comunicación que se representa en la configuración del agente falla.**coldstart**: permite controlar el envío de notificaciones de arranque en frío SNMP. Una trampa coldStart(0) significa que la entidad de protocolo de envío se reinicializa de tal manera que se puede alterar la configuración del agente o la implementación de la entidad de protocolo.

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	**rsvp**se agregó la palabra clave.
‘12.0(3)T’	**hsrp** se agregó la palabra clave.
‘12.1(3)T’	Estas palabras clave se han agregado al **snmp-server enable traps snmp** forma de e comando: • **linkup** • **linkdown** • **coldstart** Se agregaron estas palabras clave de tipo de notificación para la plataforma c Cisco AS5300 solamente: • **ds0-busyout** • **isdn chan-not-avail** • **modem-health** • **ds1-loopback** Esta palabra clave de tipo de notificación se ha agregado para las plataforma Cisco AS5300 y AS5800 solamente: • **aaa-server**

Pautas para el uso

snmp-server enable traps snmp [linkup] [linkdown] forma de este comando reemplaza el **snmp trap link-status interface** comando configuration mode.

no forma de la **snmp-server enable traps** es 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 no introduce un **snmp-server enable traps** , no se envían notificaciones controladas por este comando. Para configurar el router para enviar estas notificaciones SNMP, debe ingresar al menos una **snmp-server enable traps** comando. 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. Para habilitar varios tipos de notificaciones, debe emitir una notificación independiente **snmp-server enable traps** para cada tipo de notificación y opción de notificación.

snmp-server enable traps se utiliza junto con el comando **snmp-server host** comando. Ejecute el comando **snmp-server host** para especificar qué host o hosts reciben notificaciones SNMP. Para enviar notificaciones, debe configurar al menos una **snmp-server host** comando.

Para que un host reciba una notificación controlada por este comando, ambos **snmp-server enable traps** y el comando **snmp-server host** para ese host debe estar habilitado. Si el tipo de notificación no está controlado por este comando, sólo el **snmp-server host** debe estar habilitado.

Todos los tipos de notificación que se utilizan en este comando tienen un objeto MIB asociado que les permite ser habilitados o deshabilitados (por ejemplo, las capturas HSRP se definen con HSRP MIB, las capturas de repetidor se definen con MIB de concentrador repetidor y así sucesivamente). No todos los tipos de notificación disponibles en el **snmp-server host** tienen objetos **notificationEnable MIB**, por lo que algunos de estos no se pueden controlar con el comando **snmp-server enable** comando.

Información Relacionada

- Asistencia técnica y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).