

Cómo dar soporte y configurar notificaciones del SNMP de Cisco Catalyst OS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[¿Cómo descubro qué traps están habilitadas en mi switch?](#)

[¿Cómo configuro el receptor de traps en el SNMP del switch?](#)

[¿Cómo habilito las traps en el switch y qué significa cada una?](#)

[Sintaxis](#)

[Descripción de la Sintaxis](#)

[¿Cómo habilito las traps en los puertos individuales, por ejemplo, linkUp/linkDown?](#)

[Sintaxis](#)

[Descripción de la Sintaxis](#)

[Ejemplo:](#)

[¿Qué otras traps puede enviar el switch Catalyst?](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe las trampas que soporta el OS Catalyst (CatOS) y cómo configurarlas en el switch.

Las operaciones de notificación (traps) permiten que los agentes del protocolo simple de administración de redes (SNMP) envíen notificaciones asíncronas de la ocurrencia de un evento. Las traps se envían de la mejor manera posible, sin ningún método que verifique su recepción.

Prerequisites

Requirements

Cisco recomienda que, antes de intentar esta configuración, se asegure de haber configurado correctamente las cadenas de comunidad del SNMP en el switch.

Nota: Consulte [Cómo configurar las cadenas de comunidad del SNMP para obtener más información.](#)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switches Catalyst de las series 4500/4000, 5500/5000 y 6500/6000
- CatOS versión 7.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

¿Cómo descubro qué traps están habilitadas en mi switch?

Emita el comando `show snmp` en el modo de habilitación. Éste es un ejemplo de salida:

```
6509 (enable) show snmp

RMON:                               Enabled
Extended RMON Netflow Enabled : None.
Traps Enabled:
Port, Module, Chassis, Bridge, Repeater, Vtp, Auth, ippermit, Vmps, config, entity, stpx, syslog
Port Traps Enabled: 2/1-2,3/1-48,4/1-8

Community-Access      Community-String
....
....
!--- Output suppressed.
```

¿Cómo configuro el receptor de traps en el SNMP del switch?

Emita el comando `set snmp trap host string` .

Nota: La sintaxis del comando incluye:

- host: dirección IP o alias IP del sistema para recibir traps del SNMP.
- string: cadena de comunidad que se usa para enviar traps de autenticación.

Aquí tiene un ejemplo:

```
6509 (enable) set snmp trap 1.1.1.1 public
SNMP trap receiver added.
```

Emita el comando `show snmp` para verificar la adición de la sentencia `set snmp trap`. Éste es un ejemplo de salida:

```
6509 (enable) show snmp
6509 (enable) show snmp
RMON:                               Enabled
Extended RMON Netflow Enabled : None.
!--- Output suppressed. .... !--- Output suppressed. Trap-Rec-Address  Trap-Rec-Community
-----
1.1.1.1                             public
```

¿Cómo habilito las traps en el switch y qué significa cada una?

Emita el comando **set snmp trap** para habilitar o deshabilitar las distintas traps del SNMP en el sistema. El comando también agrega una entrada en la tabla de receptores de traps de autenticación del SNMP.

Sintaxis

set snmp trap {enable | disable} [all | auth | bridge | chasis | config | entidad | entidad | envfan | envpower | envshutdown | ippermit | módulo | repeater | stpx | syslog | sistema | vmps | vtp]

Nota: Este comando debe estar en *una* línea.

Descripción de la Sintaxis

Palabra clave	Descripción	Trampa	MIB
enable	Palabra clave para habilitar las traps del SNMP.		
inhabilitar	Palabra clave para deshabilitar las traps del SNMP.		
all	(Opcional) Palabra clave para especificar todos los tipos de traps. Consulte la documentación del switch antes de usar esta opción.		
autenticación	(Opcional) Palabra clave para especificar la trap <code>authenticationFailure</code> de la RFC 1157 .	<code>authenticationFailure</code> (.1.3.6.1.2.1.11.0.4)	SNMPv2-MIB
bridge	(Opcional) Palabra clave para especificar las traps <code>newRoot</code> y <code>topologyChange</code> de la RFC 1493 . Consulte BRIDGE-MIB .	<code>newRoot</code> (.1.3.6.1.2.1.17.0.1) <code>topologyChange</code> (.1.3.6.1.2.1.17.0.2)	BRIDGE-MIB
chasis	(Opcional) Palabra clave para especificar las traps <code>chassisAlarmOn</code> (.1.3.6.1.4.1.9.5.0.5) y <code>chassisAlarmOff</code> (.1.3.6.1.4.1.9.5.0.6) de CISCO-STACK-MIB .	<code>chassisAlarmOn</code> (.1.3.6.1.4.1.9.5.0.5) <code>chassisAlarmOff</code> (.1.3.6.1.4.1.9.5.0.6)	CISCO-STACK-MIB
config	(Opcional) Palabra clave para especificar la trap <code>sysConfigChange</code> de CISCO-STACK-MIB .	<code>sysConfigChangeTrap</code> (.1.3.6.1.4.1.9.5.0.9)	CISCO-STACK-MIB
entidad	(Opcional) Palabra clave para especificar la trap <code>entityMIB</code> de ENTITY-MIB .	<code>entConfigChange</code> (.1.3.6.1.2.1.47.2.0.1)	ENTITY-MIB
entityfru	(Opcional) Palabra clave para especificar la entidad FRU1.	<code>cefcModuleStatusChange</code> (.1.3.6.1.4.1.9.9.117.2.0.1) <code>cefcPowerStatusChange</code> (.1.3.6.1.4.1.9.9.117.2.0.2) <code>cefcFRUInserted</code> (.1.3.6.1.4.1.9.9.117.2.0.3) <code>cefcFRURemoved</code>	CISCO-STACK-MIB

		(.1.3.6.1.4.1.9.9.117.2.0.4)	
envfan	(Opcional) Palabra clave para especificar el ventilador ambiental.	ciscoEnvMonFanNotification (.1.3.6.1.4.1.9.9.13.3.0.4)	CI
envpower	(Opcional) Palabra clave para especificar la potencia ambiental.	ciscoEnvMonRedundantSupplyNotification (.1.3.6.1.4.1.9.9.13.3.0.5)	CI
envshutdown	(Opcional) Palabra clave para especificar el apagado ambiental.	ciscoEnvMonShutdownNotification (.1.3.6.1.4.1.9.9.13.3.0.1)	CI
envtemp	(Opcional) Palabra clave para especificar la notificación de temperatura ambiental.	ciscoEnvMonTemperatureNotification (.1.3.6.1.4.1.9.9.13.3.0.3)	CI
ippermit	(Opcional) Palabra clave para especificar el acceso denegado al permiso IP de CISCO-STACK-MIB .	ipPermitDeniedTrap (.1.3.6.1.4.1.9.5.0.7)	CI
macnotification	(Opcional) Palabra clave para especificar la notificación de dirección MAC.	cmnMacChangedNotification (.1.3.6.1.4.1.9.9.215.2.0.1)	CI
módulo	(Opcional) Palabra clave para especificar las traps <code>moduleUp</code> y moduleDown de CISCO-STACK-MIB .	moduleUp (.1.3.6.1.4.1.9.5.0.3) moduleDown (.1.3.6.1.4.1.9.5.0.4)	CI
repetidor	(Opcional) Palabra clave para especificar las traps <code>rpPtrHealth</code> , rpPtrGroupChange y <code>rpPtrResetEvent</code> de la RFC 1516 . Consulte SNMP-REPEATER-MIB .	rpPtrHealth (.1.3.6.1.2.1.22.0.1) rpPtrGroupChange (.1.3.6.1.2.1.22.0.2) rpPtrResetEvent (.1.3.6.1.2.1.22.0.3)	SN
stpx	(Opcional) Palabra clave para especificar la trap STPX2 .	stpxInconsistencyUpdate (.1.3.6.1.4.1.9.9.82.2.0.1) stpxLoopInconsistencyUpdate (.1.3.6.1.4.1.9.9.82.2.0.3) stpxRootInconsistencyUpdate (.1.3.6.1.4.1.9.9.82.2.0.2)	CI
syslog	(Opcional) Palabra clave para especificar las traps de notificación de syslog.	clogMessageGenerated (.1.3.6.1.4.1.9.9.41.2.0.1)	CI
system	(Opcional) Palabra clave para especificar el sistema.	ciscoSystemClockChanged (.1.3.6.1.4.1.9.9.131.2.0.1)	CI
vmmps	(Opcional) Palabra clave para especificar la trap <code>vmVmmpsChange</code> de CISCO-VLAN-MEMBERSHIP-MIB .	vmVmmpsChange (.1.3.6.1.4.1.9.9.68.2.0.1)	CI
vtp	(Opcional) Palabra clave para especificar VTP3 de CISCO-VTP-MIB .	vtpConfigDigestError (.1.3.6.1.4.1.9.9.46.2.0.2) vtpConfigRevNumberError (.1.3.6.1.4.1.9.9.46.2.0.1) vlanTrunkPortDynamicStatusChange (.1.3.6.1.4.1.9.9.46.2.0.7) vtpVersionOneDeviceDetected (.1.3.6.1.4.1.9.9.46.2.0.6)	CI

2 STPX = Extensiones del protocolo de árbol de expansión

3 VTP = Protocolo de enlace troncal de la VLAN

¿Cómo habilito las traps en los puertos individuales, por ejemplo, linkUp/linkDown?

Emita el comando **set port trap** para habilitar o deshabilitar la operación de la trap de enlace del **SNMP estándar** para un puerto o rango de puertos. De manera predeterminada, todas las traps del puerto están deshabilitadas.

Nota: El módulo de análisis de red (NAM) no admite este comando.

Sintaxis

set port trap mod/port {enable | disable}

Descripción de la Sintaxis

- **mod/port:** número de módulo y puerto del módulo.
- **enable:** palabra clave para activar la trap de enlace del SNMP.
- **disable:** palabra clave para desactivar la trap de enlace del SNMP.

Si habilita las traps, las traps correspondientes que se generan son `linkUp` (.1.3.6.1.2.1.11.0.3) y `linkDown` (.1.3.6.1.2.1.11.0.2). Estas traps provienen de [IF-MIB](#).

Ejemplo:

En este ejemplo se muestra cómo habilitar la trap de enlace del SNMP para el módulo 1, puerto 2:

```
Console> (enable) set port trap 1/2 enable
Port 1/2 up/down trap enabled.
Console> (enable)
```

¿Qué otras traps puede enviar el switch Catalyst?

Consulte esta tabla:

Nombre del objeto de MIB	OID (ID del objeto)	MIB
ciscoFlashCopyCompletionTrap	.1.3.6.1.4.1.9.9.10.1.3.0.1	CISCO-FLASH-MIB
ciscoFlashDeviceChangeTrap	.1.3.6.1.4.1.9.9.10.1.3.0.4	CISCO-FLASH-MIB
ciscoFlashMiscOpCompletionTrap	.1.3.6.1.4.1.9.9.10.1.3.0.3	CISCO-FLASH-MIB
coldstart	.1.3.6.1.6.3.1.1.5.1	RFC 1157-SNMP (SNMPv2-MIB)
warmStart	.1.3.6.1.6.3.1.1.5.2	RFC 1157-SNMP (SNMPv2-MIB)
tokenRingSoftErrExceededTrap	.1.3.6.1.4.1.9.5.0.10	CISCO-STACK-MIB
lerAlarmOn	.1.3.6.1.4.1.9.5.0.1	CISCO-STACK-MIB
lerAlarmOff	.1.3.6.1.4.1.9.5.0.2	CISCO-STACK-MIB
entSensorThresholdNotification	.1.3.6.1.4.1.9.9.91.2.0.1	CISCO-ENTITY-SENSOR-MIB
fallingAlarm	.1.3.6.1.2.1.16.0.2	RMON-MIB

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Productos y servicios de Cisco: switches](#)
- [Trampas de SNMP \(Protocolo simple de gestión de redes\) compatibles con IOS de Cisco y cómo configurarlas](#)
- [Ejemplos de configuración de los servicios de aplicación IP y notas técnicas](#)
- [Descargas de software de administración de redes: MIB \(solo clientes registrados\)](#)
- [Página de Soporte de LAN Switching](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)