Supporto delle trap SNMP Cisco IOS e modalità di configurazione

Sommario

Introduzione

Nota: Per preparare questo documento è stato usato il software Cisco IOS release® 12.1(3)T. Nelle versioni precedenti del Cisco IOS Software non sono supportate tutte le opzioni. Nelle versioni di Cisco IOS Software precedenti a 12.1(3)T possono essere supportate altre opzioni [notification-type]. In questo documento sono stati elencati tutti gli identificatori di oggetti (OID) delle trap del protocollo SNMP (Simple Network Management Protocol) su Cisco IOS Software.

I dispositivi Cisco con software IOS standard (router, switch ATM (Asynchronous Transfer Mode) e server di accesso remoto) possono generare molte trap SNMP.

Prerequisiti

Requisiti

I lettori di questo documento devono comprendere queste informazioni:

Si desidera che un dispositivo Cisco non invii tutte le trap SNMP che il dispositivo è in grado di

inviare. Ad esempio, se si attivano tutte le registrazioni in un server di accesso remoto con 64 linee di connessione remota, si otterrà una registrazione ogni volta che un utente effettua una chiamata e ogni volta che interrompe la connessione. In questo modo vengono create troppe registrazioni. Il software Cisco IOS definisce i gruppi di trap che è possibile abilitare o disabilitare. Per configurare le trap SNMP in un dispositivo software Cisco IOS, è possibile utilizzare due comandi di configurazione globale:

- **snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port** *port*] **[notification-type]**
  Utilizzare il **snmp-server host global configuration** per specificare il destinatario di un'operazione di notifica SNMP. Utilizzare il **no** per rimuovere l'host specificato.
- **snmp-server enable traps [***notification-type***] [***notification-option***]**
  Utilizzare il **snmp-server enable traps global configuration** per consentire al router di inviare i trap SNMP. Utilizzare il **no** per disabilitare le notifiche SNMP.

I tipi di registrazione dei colori possono essere specificati in entrambi i comandi. È necessario emettere il **snmp-server host** per definire i sistemi di gestione della rete a cui inviare le trap. Se non si desidera inviare tutti i trap, è necessario specificare i tipi di trap. Emissione multipla **snmp-server enable traps** uno per ogni tipo di registrazione utilizzato nel **snmp host**

Nota: Non tutti [*notification-type*] le opzioni sono supportate su entrambi i comandi. Ad esempio, [*notification-type*] x25 e teletype (tty) non sono utilizzati per **snmp-server enable trap.** le trap x25 e tty sono abilitate per impostazione predefinita.

Ad esempio, eseguire questi comandi per configurare un dispositivo software Cisco IOS in modo che restituisca solo la configurazione, il protocollo Border Gateway Protocol (BGP) e tty trap a Network Management System 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
```

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Comando host snmp-server

Utilizzare il **snmp-server host global configuration** per specificare il destinatario di un'operazione di notifica SNMP. Utilizzare il **no** per rimuovere l'host specificato.

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]**

Descrizione della sintassi

host-addr	Il nome o l'indirizzo Internet dell'host (il destinatario di destinazione).
traps	(Facoltativo) Inviare trap SNMP a questo host. Questa è l'impostazione predefinita.
informs	(Facoltativo) Inviare le informazioni SNMP a questo host.
version	(Facoltativo) Versione di SNMP utilizzata per inviare i trap. La versione 3 è il modello più sicuro, poiché consente la crittografia dei pacchetti con **priv** parola chiave. Se si utilizza la parola chiave version, è necessario specificare una delle opzioni seguenti: • **1**—SNMPv1. Questa opzione non è disponibile con informs. • **2c**: SNMPv2C • **3**—SNMPv3. Queste tre parole chiave opzionali possono seguire la parola chiave versione 3: **auth** (Facoltativo) Abilita l'autenticazione dei pacchetti MD5 (Message Digest 5) e SHA (Secure Hash Algorithm).**noauth** Impostazione predefinita. Livello di protezione noAuthNoPriv. Si tratta dell'impostazione predefinita se [auth | noauth | priv], la scelta della parola chiave non è specificata.**priv** (Facoltativo) Abilita la crittografia dei pacchetti DES (Data Encryption Standard), definita anche "privacy".
community-string	Stringa della community di tipo password inviata con l'operazione di notifica. Sebbene sia possibile impostare questa stringa con il **snmp-server host** , Cisco consiglia di definire questa stringa con il comando **snmp-server community** prima di usare il comando **snmp-server host**
udp-port *port*	Porta UDP (User Datagram Protocol) dell'host da utilizzare. Il valore predefinito è 162.
tipo di notifica	(Facoltativo) Il tipo di notifica da inviare all'host. Se non viene specificato alcun tipo, verranno inviate tutte le notifiche. Il tipo di notifica può essere rappresentato da una o più delle seguenti parole chiave: • **aaa-server**- Invia notifiche AAA. • **bgp**- Invia notifiche di modifica dello stato

	Border Gateway Protocol (BGP). • **bstun**- Invia notifiche BSTUN (Block Serial Tunneling). • **calltracker**- Invia notifiche CallTracker. • **config**- Invia notifiche di configurazione. • **dlsw**— Invia notifiche DLSw (Data-Link Switching). • **ds0-busyout**- Invia notifiche ds0-busyout. • **ds1-loopback**- Invia notifiche di loopback ds1. • **dspu**- Invia notifiche DSPU (downstream physical unit). • **dsp**- Invia notifiche DSP (Digital Signal Processing). • **entity**- Invia notifiche di modifica MIB (Entity Management Information Base). • **envmon**- Invia notifiche sul monitoraggio ambientale specifico per l'azienda Cisco quando viene superata una soglia ambientale. • **frame-relay**- Invia notifiche Frame Relay. • **hsrp**- Invia notifiche HSRP (Hot Standby Router Protocol). • **isdn**- Invia notifiche ISDN (Integrated Services Digital Network). • **msdp**- Invia notifiche MSDP (Multicast Source Discovery Protocol). • **llc2**- Invia notifiche LLC2 (Logical Link Control) di tipo 2. • **repeater**- Invia notifiche di ripetitore standard (hub). • **rsrb**- Invia notifiche RSRB (Source-Route Bridging) remote. • **rsvp**- Invia notifiche RSVP (Resource Reservation Protocol). • **rtr**- Invia notifiche di Agente SA (RTR). • **sdlc**- Invia notifiche SDLC (Synchronous Data Link Control). • **snmp**- Invia notifiche SNMP (Simple Network Management Protocol), come definito nella RFC 1157. • **stun**- Invia notifiche STUN (serial tunnel). • **syslog**- Invia notifiche di messaggi di errore (Cisco Syslog MIB). Specificare il livello di messaggi da inviare con **logging history level** • **tty**- Invia notifiche specifiche

	dell'organizzazione Cisco alla chiusura di una connessione TCP (Transmission Control Protocol). • **voice**- Invia notifiche vocali. • **x25**- Invia notifiche di eventi X.25. • **xgcp**- Invia notifiche XGCP (External Media Gateway Control Protocol).

Valori predefiniti

OSPF (Open Shortest Path First) **snmp-server host** è disattivato per impostazione predefinita. Nessuna notifica inviata.

Se si immette questo comando senza parole chiave, per impostazione predefinita tutti i tipi di trap vengono inviati all'host.

Nessuna informazione inviata a questo host. Se no **version** parola chiave è presente, il valore predefinito è versione 1. Il **no snmp-server host** senza parole chiave disattiva le registrazioni all'host, ma non ne informa. Utilizzare il **no snmp-server host informs** per disabilitare le informazioni.

Nota: Se il *community-string* non è definito con **snmp-server community** prima di utilizzare questo comando, la forma predefinita del **snmp-server community** viene inserito automaticamente nella configurazione. La password *(community-string)* utilizzato per questa configurazione automatica **snmp-server community** è uguale a quello specificato nella **snmp-server host** Questo è il comportamento predefinito del software Cisco IOS versione 12.0(3) e successive.

Modalità dei comandi

Configurazione globale - Cronologia comandi

Per preparare questo documento, è stato utilizzato Cisco IOS Software Release	Modifica
10.0	Comando introdotto.
12.0(3)T	Sono state aggiunte le seguenti parole chiave: • **version 3 [auth	noauth	priv]** • **hsrp**

Linee guida sull'utilizzo

Le notifiche SNMP possono essere inviate come trap o come richieste informative. I trap non sono affidabili perché il ricevitore non invia conferme quando il dispositivo riceve trap. Il mittente non può determinare se le trap sono state ricevute. Tuttavia, un'entità SNMP che riceve una richiesta inform riconosce il messaggio con una unità di risposta del protocollo (PDU) SNMP. Se il mittente non riceve mai la risposta, la richiesta di informazioni può essere inviata di nuovo. È quindi più

probabile che le informazioni raggiungano la destinazione prevista.

Tuttavia, le informazioni consumano più risorse nell'agente e nella rete. A differenza di una trap, che viene scartata non appena viene inviata, una richiesta informata deve essere mantenuta in memoria fino a quando non viene ricevuta una risposta o la richiesta scade. I trap vengono inviati una sola volta, mentre è possibile eseguire più tentativi di invio di un'informazione. I tentativi aumentano il traffico e contribuiscono a un maggiore sovraccarico sulla rete.

Se non si immette un **snmp-server host** non viene inviata alcuna notifica. Per configurare il router per l'invio di notifiche SNMP, è necessario immettere almeno una **snmp-server host** Se si immette il comando senza parole chiave, tutti i tipi di trap vengono abilitati per l'host.

Per abilitare più host, è necessario **snmp-server host** per ciascun host. È possibile specificare più tipi di notifica nel comando per ogni host.

Quando più **snmp-server host** vengono forniti comandi per lo stesso host e tipo di notifica (trap o inform), ogni comando sovrascrive il comando precedente. Solo l'ultimo **snmp-server host** è stato preso in considerazione. Ad esempio, se si immette un **snmp-server host inform** per un host, quindi immetterne un altro **snmp-server host inform** per lo stesso host, il secondo comando sostituisce il primo.

OSPF (Open Shortest Path First) **snmp-server host** viene utilizzato insieme al comando **snmp-server enable** Utilizzare il **snmp-server enable** per specificare quali notifiche SNMP devono essere inviate globalmente. Affinché un host riceva la maggior parte delle notifiche, almeno una **snmp-server enable** e **snmp-server host** per l'host.

Tuttavia, alcuni tipi di notifica non possono essere controllati con **snmp-server enable** Ad esempio, alcuni tipi di notifica sono sempre attivati. Altri tipi di notifica sono attivati da un comando diverso. Ad esempio, la `linkUpDown` le notifiche sono controllate dal **snmp trap link-status** Questi tipi di notifica non richiedono **snmp-server enable**

La disponibilità di un'opzione del tipo di notifica dipende dal tipo di router e dalle funzionalità software di Cisco IOS supportate sul router. Ad esempio, la **envmon** il tipo di notifica è disponibile solo se il monitoraggio ambientale fa parte del sistema.

Configurazione delle informazioni

Per inviare un'informazione, completare i seguenti passaggi:

1. Configurare un ID motore remoto.
2. Configurare un utente remoto.
3. Configurare un gruppo in un dispositivo remoto.
4. Abilitare i trap nel dispositivo remoto.
5. Abilitare SNMP Manager.

Esempi

Se si desidera configurare una stringa della community SNMP univoca per le trap, ma si desidera impedire l'accesso al polling SNMP con questa stringa, la configurazione deve includere un elenco degli accessi. Nell'esempio, la stringa della community è chiamata "comaccess" e l'elenco degli accessi è numerato 10:

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

In questo esempio vengono inviate le trap SNMP all'host specificato con il nome myhost.cisco.com. La stringa della community viene definita come comaccess:

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

In questo esempio vengono inviate trap specifiche dell'organizzazione per SNMP e Cisco Environmental Monitor all'indirizzo 172.30.2.160:

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

In questo esempio il router viene abilitato a inviare tutte le trap all'host myhost.cisco.com con la stringa della community public:

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

In questo esempio non vengono inviati trap ad alcun host. I trap BGP sono abilitati per tutti gli host, ma solo i trap ISDN possono essere inviati a un host.

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

In questo esempio il router viene abilitato a inviare tutte le richieste inform all'host myhost.cisco.com utilizzando la stringa della community public:

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

In questo esempio vengono inviati trap SNMPv2c HSRP all'host specificato dal nome myhost.cisco.com. La stringa della community è definita come pubblica.

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

snmp-server enable traps Command

Utilizzare il **snmp-server enable traps** comando di configurazione globale per consentire al router di inviare trap SNMP. Utilizzare il **no** per disabilitare le notifiche SNMP.

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

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

Descrizione della sintassi

tipo di notifica	(Facoltativo) Tipo di notifica da abilitare. Se non viene specificato alcun tipo, vengono inviate tutte le notifiche (inclusa la **envmon** e **repeater** notifiche). Il tipo di notifica può essere una delle seguenti parole chiave: • **aaa-server**- Invia notifiche al server AAA. Questa parola chiave viene aggiunta dal software Cisco IOS versione 12.1(3)T solo per piattaforme Cisco AS5300 e AS5800. Questo è tratto dal CISCO-AAA-SERVER-MIB, e le notifiche sono: enterprise 1.3.6.1.4.1.9.10.56.2.1 casServerStateChange • **bgp**- Invia notifiche di modifica dello stato Border Gateway Protocol (BGP). Questa è la versione del MIB BGP4, e le notifiche sono: enterprise 1.3.6.1.2.1.15.7 1 bgpTransizione all'indietro stabilita a 2 bgp • **calltracker**—Invia una notifica ogni volta che viene creata una nuova voce di chiamata attiva in cctActiveTable o una nuova voce di chiamata della cronologia in cctHistoryTable. Questa voce proviene da CISCO-CALL-TRACKER-MIB e le notifiche sono: enterprise 1.3.6.1.4.1.9.9.163.2.1 cctCallSetupNotification 2 cctCallTerminateNotification • **config**- Invia notifiche di configurazione. Questo è quello che si ottiene da CISCO-CONFIG-MAN-MIB, e le notifiche sono: enterprise 1.3.6.1.4.1.9.9.43.2.1 ciscoConfigManEvent • **dial**- Invia una notifica ogni volta che una chiamata viene cancellata, un tentativo di chiamata non riuscito viene considerato come effettivamente fallito oppure ogni volta che viene ricevuto o inviato un messaggio di impostazione della chiamata. Questo viene

	da DIAL-CONTROL-MIB e le notifiche sono: enterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation 2 dialCtlPeerCallSetup • **dlsw**- Invia notifiche dagli agenti DLSw quando **dlsw** parola chiave, è possibile specificare un valore *notification-option*. Questo è tratto dal CISCO-DLSW-MIB, e le notifiche sono: Enterprise 1.3.6.1.4.1.9.10.9.1.7 1 ciscoDlswTrapTConPartnerReject 2 ciscoDlswTrapTConPortViolation 3 ciscoDlswTrapTConUp 4 ciscoDlswTrapTConDown 5 ciscoDlswTrapCircuitUp 6 ciscoDlswTrapCircuitDown • **ds0-busyout**- Invia una notifica ogni volta che lo stato del ciclo di vita di un'interfaccia DS0 cambia. Questa parola chiave viene aggiunta dal software Cisco IOS versione 12.1(3)T solo per la piattaforma Cisco AS5300. A tal fine, si utilizza il comando CISCO-POP-MGMT-MIB e la notifica è la seguente: Enterprise 1.3.6.1.4.1.9.10.19.2 1 cpmDS0BusyoutNotification • **ds1-loopback**- Invia una notifica ogni volta che l'interfaccia DS1 entra in modalità loopback. Questa parola chiave viene aggiunta dal software Cisco IOS versione 12.1(3)T solo per la piattaforma Cisco AS5300. A tal fine, si utilizza il comando CISCO-POP-MGMT-MIB e la notifica è la seguente: enterprise 1.3.6.1.4.1.9.10.19.2 2 cpmDS1Notifica loopback • **dspu**- Invia una notifica ogni volta che viene rilevato lo stato operativo dell'unità fisica (PU) o la modifica dell'unità logica (LU) o un errore di attivazione. Questa è la procedura descritta di seguito nel documento CISCO-DSPU-MIB, e le notifiche sono: enterprise 1.3.6.1.4.1.9.9.24.1.4.4 1newdspuPuStateChangeTrap 2 newdspuPuActivationFailureTrap enterprise 1.3.6.1.4.1.9.24.1.5.3 1 newdspuLuStateChangeTrap 2 dspuLuActivationFailureTrap • **dsp**- Invia una notifica ogni volta che la

	scheda DSP diventa attiva o inattiva. Questa è una richiesta del CISCO-DSP-MGMT-MIB, e la notifica è: Enterprise 1.3.6.1.4.1.9.9.86.2.1 cdspMIBCardaStateNotification • **entity**- Invia notifiche di modifica MIB entità. Questo viene dal ENTITY-MIB e le notifiche sono: enterprise 1.3.6.1.2.1.47.2.1 1 entConfigChange • **envmon**- Invia notifiche di monitoraggio ambientale specifiche per le aziende Cisco quando viene superata una soglia ambientale. Quando **envmon** parola chiave, è possibile specificare un valore *notification-option*. Questa è la procedura descritta di seguito nel documento CISCO-ENVMON-MIB, e le notifiche sono: Enterprise 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonShutdownNotification 2 ciscoEnvMonVoltageNotification 3 ciscoEnvMonTemperatureNotification 4 ciscoEnvMonFanNotification 5 ciscoEnvMonRedundantSupplyNotification • **frame-relay**- Invia notifiche Frame Relay. Questa è la risposta della RFC1315-MIB e le notifiche sono: enterprise 1.3.6.1.2.1.10.32.1 frDLCIStatusChange • **hsrp**- Invia notifiche HSRP (Hot Standby Router Protocol). Questa funzione è supportata dal software Cisco IOS versione 12.0(3)T. Questa è una procedura del CISCO-HSRP-MIB, e le notifiche sono: enterprise 1.3.6.1.4.1.9.9.106.2.1 cHsrpStateChange • **isdn**- Invia notifiche ISDN. Quando **isdn** parola chiave, è possibile specificare un valore *notification-option*. Questa è la procedura descritta di seguito nel documento CISCO-ISDN-MIB, e le notifiche sono: enterprise 1.3.6.1.4.1.9.9.26.2 1 demandNbrCallInformation 2 demandNbrCallDetails 3 demandNbrLayer2Change [supportato dal software Cisco IOS versione 12.1(1)T] 4 demandNbrCNANotification [supportato dal software Cisco IOS versione 12.1(5)T] Questa è una notifica di CISCO-ISDN-IF-

	MIB, e le notifiche sono: Notifica ciuIfLoopStatus dell'organizzazione 1.3.6.1.4.1.9.9.18.2 • **msdp**- Invia notifiche MSDP (Multicast Source Discovery Protocol). A tal fine, viene generato l'MSDP-MIB e le notifiche sono: enterprise 1.3.6.1.3.92.1.1.7.1 msdpEstablished 2 msdpBackwardTransition • **repeater**- Invia hub Ethernet **repeater** notifiche. Quando si seleziona la parola chiave del ripetitore, è possibile specificare una *notification-option* valore. Questo è tratto da CISCO-REPEATER-MIB, e le notifiche sono: enterprise 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap • **rsvp**- Invia notifiche RSVP (Resource Reservation Protocol). Questa funzione è supportata dal software Cisco IOS versione 12.0(2)T. Questa è la RSVP-MIB, e le notifiche sono: enterprise 1.3.6.1.3.71.2.1 newFlow 2 lostFlow • **rtr**- Invia notifiche RTR (Service Assurance Agent). Questo è tratto da CISCO-RTTMON-MIB e le notifiche sono: Enterprise 1.3.6.1.4.1.9.9.42.2.1 rttMonConnectionChangeNotification 2 rttMonTimeoutNotification 3 rttMonThresholdNotification 4 rttMonVerifyErrorNotification • **snmp**- Invia notifiche SNMP (Simple Network Management Protocol). Quando **snmp** , è possibile specificare un valore per l'opzione di notifica. Questo viene generato dalla CISCO-GENERAL-TRAPS, e le notifiche sono: enterprise 1.3.6.1.2.1.11 0 coldStart 2 linkDown 3 linkUp 4 authenticationFailure 5 egpNeighborLoss enterprise 1.3.6.1.4.1.9 0 reload **Nota:** questa trap è controllata dal tipo di notifica "tty":**Nota:** 1 tcpConnectionClose • **syslog**- Invia notifiche di messaggi di errore (Cisco Syslog MIB). Specificare il livello di messaggi da inviare con **logging history level** Questa è una procedura del CISCO-SYSLOG-MIB, e le notifiche sono:

	enterprise 1.3.6.1.4.1.9.9.41.2.1 clogMessageGenerato • **voice**- Invia notifiche vocali di scarsa qualità. Questo è da CISCO-VOICE-DIAL-CONTROL-MIBSMI, e le notifiche sono: notifica QoV di classe enterprise 1.3.6.1.4.1.9.9.63.2.1 cvdcPoor • **xgcp**- Invia notifiche XGCP (External Media Gateway Control Protocol). Questa è la XGCP-MIB e le notifiche sono: 1.3.6.1.3.90.2.1 xgcpUpDownNotification
opzione-notifica	(Facoltativo) • **dlsw [circuit | tconn]**- Quando **dlsw** è possibile specificare il tipo di notifica specifico che si desidera attivare o disattivare. Se non viene utilizzata alcuna parola chiave, vengono attivati tutti i tipi di notifica DLSw. L'opzione può essere rappresentata da una o più delle seguenti parole chiave: **circuit**- Attiva le trap del circuito DLSw.**tconn**- Abilita le trap delle connessioni di trasporto peer DLSw. • **envmon [voltage | shutdown | supply | fan | temperature]**- Quando **envmon** è possibile abilitare un tipo specifico di notifica ambientale oppure accettare tutti i tipi di notifica dal sistema di monitoraggio ambientale. Se non viene specificata alcuna opzione, vengono abilitate tutte le notifiche ambientali. L'opzione può essere rappresentata da una o più delle seguenti parole chiave: **voltage**, **shutdown**, **supply**, **fan**,e **temperature**. • **isdn [call-information | isdn u-interface | chan-not-avail | layer2]**- Quando **isdn** parola chiave, è possibile specificare la **call-information** per abilitare una notifica delle informazioni sulle chiamate ISDN SNMP per il sottosistema MIB ISDN oppure è possibile specificare **isdn u-interface** parola chiave per abilitare una notifica dell'interfaccia ISDN U SNMP per il sottosistema MIB dell'interfaccia ISDN U. • **repeater [health | reset]**- Quando **repeater** , è possibile specificare l'opzione del ripetitore. Se non viene specificata alcuna opzione, verranno attivate tutte le notifiche ripetute. L'opzione può essere

	rappresentata da una o più delle seguenti parole chiave: integrità: abilita la notifica di integrità MIB (RFC 1516) dell'hub ripetitore IETF (Internet Engineering Task Force). reset - Abilita la notifica di ripristino MIB (RFC 1516) dell'hub ripetitori IETF. **health**- Attiva la notifica di integrità MIB (RFC 1516) dell'hub ripetitori IETF (Internet Engineering Task Force).**reset**- Attiva la notifica di ripristino MIB (RFC 1516) dell'hub ripetitori IETF. • **snmp [authentication** | **linkup** | **linkdown** | **coldstart]** parole chiave **linkup** | **linkdown** | **coldstart** aggiunto dal software Cisco IOS versione 12.1(3)T. - Quando il **snmp** è possibile specificare il tipo di notifica specifico che si desidera attivare o disattivare. Se non viene utilizzata alcuna parola chiave, tutti i tipi di notifica SNMP verranno attivati (o disattivati se viene utilizzato il modulo no). I tipi di notifica disponibili sono: **authentication**- Controlla la distribuzione delle notifiche di errore dell'autenticazione SNMP. Un trap authenticationFailure(4) indica che l'entità del protocollo di invio è il destinatario di un messaggio di protocollo non autenticato correttamente.**linkup**- Controlla l'invio delle notifiche di collegamento SNMP. Una trap linkUp(3) indica che l'entità del protocollo di invio riconosce che è stato rilevato uno dei collegamenti di comunicazione rappresentati nella configurazione dell'agente.**linkdown**- Controlla la modalità di invio delle notifiche di collegamento SNMP. Un trap linkDown(2) indica che l'entità del protocollo di invio riconosce un errore in uno dei collegamenti di comunicazione rappresentati nella configurazione dell'agente.**coldstart**- Controlla l'invio delle notifiche coldstart SNMP. Una trap coldStart(0) indica che l'entità del protocollo di invio viene reinizializzata in modo che la configurazione dell'agente o l'implementazione dell'entità del protocollo possa essere modificata.

Valori predefiniti

Le notifiche SNMP sono disabilitate.

Se si immette questo comando senza parole chiave per il tipo di notifica, per impostazione predefinita vengono abilitati tutti i tipi di notifica controllati da questo comando.

Modalità dei comandi

Configurazione globale - Cronologia comandi

Per preparare questo documento, è stato utilizzato Cisco IOS Software Release	Modifica
11.1	Questo comando è stato introdotto.
12.0(2)T	OSPF (Open Shortest Path First) **rsvp** parola chiave aggiunta.
12.0(3)T	OSPF (Open Shortest Path First) **hsrp** parola chiave aggiunta.
12.1(3)T	Queste parole chiave sono state aggiunte al **snmp-server enable traps snmp** forma del comando: • **linkup** • **linkdown** • **coldstart** Queste parole chiave del tipo di notifica sono state aggiunte solo per la piattaforma Cisco AS5300: • **ds0-busyout** • **isdn chan-not-avail** • **modem-health** • **ds1-loopback** Questa parola chiave per il tipo di notifica è stata aggiunta solo per le piattaforme Cisco AS5300 e AS5800: • **aaa-server**

Linee guida sull'utilizzo

OSPF (Open Shortest Path First) **snmp-server enable traps snmp [linkup] [linkdown]** questo comando sostituisce il **snmp trap link-status interface** modalità di configurazione.

OSPF (Open Shortest Path First) **no** forma **snmp-server enable traps** è utile per disattivare le notifiche che generano una grande quantità di rumore non necessario sulla rete.

Le notifiche SNMP possono essere inviate come trap o come richieste informative. Questo comando abilita sia le trap che le richieste di informazioni per i tipi di notifica specificati.

Se non si immette un **snmp-server enable traps** , non vengono inviate notifiche controllate da questo comando. Per configurare il router per l'invio di queste notifiche SNMP, è necessario immettere almeno una **snmp-server enable traps** Se si immette il comando senza parole chiave, vengono attivati tutti i tipi di notifica. Se si immette il comando con una parola chiave, viene abilitato solo il tipo di notifica relativo a tale parola chiave. Per abilitare più tipi di notifiche, è necessario emettere un **snmp-server enable traps** per ogni tipo di notifica e opzione di notifica.

OSPF (Open Shortest Path First) **snmp-server enable traps** viene utilizzato insieme al comando **snmp-server host** Utilizzare il **snmp-server host** per specificare l'host o gli host che ricevono le notifiche SNMP. Per inviare le notifiche, è necessario configurarne almeno una **snmp-server host**

Affinché un host riceva una notifica controllata da questo comando, è necessario che **snmp-server enable traps** e **snmp-server host** per l'host. Se il tipo di notifica non è controllato da questo comando, solo il **snmp-server host** deve essere abilitato.

I tipi di notifica utilizzati in questo comando dispongono tutti di un oggetto MIB associato che consente di abilitarli o disabilitarli (ad esempio, le trap HSRP vengono definite con MIB HSRP, le trap ripetitori vengono definite con MIB Hub ripetitori e così via). Non tutti i tipi di notifica disponibili nel **snmp-server host** dispongono di un oggetto notificationEnable MIB, pertanto alcuni di questi non possono essere controllati con **snmp-server enable**

Informazioni correlate

- Miglioramenti ATM SNMP Trap e OAM
- Supporto tecnico – Cisco Systems