

Ondersteunde IOS SNMP-traps configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Opdrachten](#)

[De opdracht SNMP-server host](#)

[Syntax Beschrijving](#)

[Standaard](#)

[Opdrachtmodi](#)

[Wereldwijde configuratie - Opdrachtgeschiedenis](#)

[Richtlijnen gebruiken](#)

[Configureren van informatie](#)

[Voorbeelden](#)

[De SNMP-server schakelt de opdracht Vallen in](#)

[Syntax Beschrijving](#)

[Standaard](#)

[Opdrachtmodi](#)

[Wereldwijde configuratie - Opdrachtgeschiedenis](#)

[Richtlijnen gebruiken](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de ondersteunde Cisco SNMP-traps kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

U wilt niet dat een Cisco-apparaat alle SNMP-traps verstuurt die het apparaat weet te versturen. Als u bijvoorbeeld alle traps in een Remote Access Server met 64 inbellijnen inschakelt, krijgt u een val wanneer een gebruiker inbelt en wanneer een gebruiker de verbinding beëindigt. Dit leidt tot te veel vallen. Cisco IOS®-software definieert groepen traps die u kunt in- of uitschakelen. Er zijn twee globale configuratieopdrachten die u gebruikt om SNMP-traps te configureren naar een Cisco IOS-softwareapparaat:

-

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

Geef het `snmp-server host` global configuration opdracht om de ontvanger van een SNMP-waarschuwing op te geven. Geef het `no` vorm van deze opdracht om de gespecificeerde host te verwijderen.

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

Geef het `snmp-server enable traps` global configuration opdracht om de router in staat te stellen SNMP-traps te verzenden. Geef het `no` vorm van deze opdracht om SNMP-meldingen uit te schakelen.

De typen vallen kunnen in beide opdrachten worden gespecificeerd. U moet de `snmp-server host` </strong> opdracht om de netwerkbeheersystemen te definiëren waarin vallen moeten worden verzonden. Als u niet wilt dat alle traps worden verzonden, moet u de traptypes specificeren. Problemen oplossen `snmp-server enable traps` voor elk type val dat u in het programma hebt gebruikt. `snmp host` uit.

**Opmerking:** niet alle *[notification-type]* De opties worden op beide opdrachten ondersteund. Voorbeeld, *[notification-type]* x25 en teletype (tty) worden niet gebruikt voor `snmp-server enable trap x25-`, en tty-traps zijn standaard ingeschakeld.

Geef deze opdrachten bijvoorbeeld uit om een Cisco IOS-softwareapparaat alleen te configureren, BGP-protocol (Border Gateway Protocol) te maken en te proberen overvulling op te nemen in 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
```

## Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

## Achtergrondinformatie

**Opmerking:** dit document is opgesteld met behulp van Cisco IOS-software release 12.1(3)T. Wanneer u een eerdere Cisco IOS-software release gebruikt, worden niet alle opties ondersteund. Wanneer u een Cisco IOS-software release lager dan 12.1(3)T gebruikt, kunnen extra *[meldingstype]* opties worden ondersteund. Dit document bevat een actuele

lijst van alle ondersteunde object-ID's (OID's) van SNMP-traps (Simple Network Management Protocol) van Cisco IOS-software.

Cisco-apparaten die de standaard Cisco IOS-software (routers, ATM-switches (Asynchronous Transfer Mode) en externe toegangsservers) uitvoeren, kunnen veel SNMP-traps genereren.

## Opdrachten

### Het `snmp-server host` Opdracht

Geef het `snmp-server host` global configuration opdracht om de ontvanger van een SNMP-waarschuwing op te geven. Geef het `no` vorm van deze opdracht om de gespecificeerde host te verwijderen.

```
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]
```

### Syntax Beschrijving

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>host-addr</code>          | De naam of het internetadres van de host (de beoogde ontvanger).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <code>traps</code>              | (Optioneel) Verzend SNMP-traps naar deze host. Dit is de standaardinstelling.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>informs</code>            | (Optioneel) Verzend SNMP-informatie naar deze host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>version</code>            | (Optioneel) De versie van de SNMP die wordt gebruikt om de traps te verzenden. Versie 3 is het veiligste model, aangezien dit model pakketencryptie met toestaat <code>priv</code> trefwoord. Als u het trefwoord voor de versie gebruikt, moet u een van de volgende opties instellen: <ul style="list-style-type: none"><li>• <b>1</b>—SNMPv1. Deze optie is niet beschikbaar bij <code>informs</code>.</li><li>• <b>2c</b>—SNMPv2C</li><li>• <b>3</b>—SNMPv3. Deze drie optionele trefwoorden kunnen worden toegevoegd na het trefwoord versie 3: <code>auth</code> (Optioneel) Schakelt Message Digest 5 (MD5) en Secure Hash Algorithm (SHA) in met pakketverificatie. <code>noauth</code> (Standaard) Het noAuthNoPriv-beveiligingsniveau. Dit is de standaardwaarde als de <code>[auth   noauth   priv]</code> sleutelwoordkeuze niet gespecificeerd. <code>priv</code> (Optioneel) Schakelt gegevenscodering standaard (DES) pakketcodering in (ook "privacy" genoemd).</li></ul> |
| <code>community-string</code>   | De wachtwoordachtige <code>community-string</code> die met de notificatiebewerking wordt verzonden. Alhoewel u deze string kunt instellen met de <code>snmp-server host</code> opdracht op zich, raadt Cisco u aan deze tekenreeks te definiëren met de <code>snmp-server community</code> opdracht voordat u de <code>snmp-server host</code> opdracht uitvoert.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <code>udp-port</code>           | <code>port</code> User Datagram Protocol (UDP) poort van de host die wordt gebruikt. De standaardwaarde is 162.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>soort kennisgeving</code> | (Facultatief) Het type van bericht dat naar de gastheer moet worden verzonden. Als er geen type is opgegeven, worden alle meldingen verzonden. Het soort melding kan een of meer van de volgende trefwoorden bevatten: <ul style="list-style-type: none"><li>• <code>aaa-server</code> —stuurt AAA-meldingen.</li><li>• <code>bgp</code> —Verzendt BGP-kennisgevingen van wijzigingen in de status.</li><li>• <code>bstun</code>—Verstuurt BSTUN-meldingen (Block Serial Tunnelling).</li><li>• <code>calltracker</code>—Verzendt CallTracker-meldingen.</li><li>• <code>config</code>—Verzendt configuratie meldingen.</li><li>• <code>dls</code>—Verzendt DLSw-meldingen (Data-Link Switching).</li><li>• <code>ds0-busyout</code>—Verzendt ds0-busyout meldingen.</li></ul>                                                                                                                                                                                                            |

- **ds1-loopback**—Verzendt ds1-loopback meldingen.
- **dspu**—Verzendt stroomafwaartse berichten van de fysieke eenheid (DSPU).
- **dsp**—Verzendt DSP-meldingen (Digital Signal Processing).
- **entity**—Verstuurt wijzigingsmeldingen in de Entity Management Information Base (MIB).
- **envmon**—Hiermee worden meldingen voor Cisco Enterprise-Specific Environment Monitoring verzonden wanneer een omgevingsdrempel wordt overschreden.
- **frame-relay**—Verzendt Frame Relay-meldingen.
- **hsrp**—Verzendt Hot Standby Router Protocol (HSRP)-meldingen.
- **isdn**—Hiermee worden meldingen verzonden via het digitale netwerk voor geïntegreerd services (ISDN).
- **msdp**—Hiermee worden meldingen verzonden via Multicast Source Discovery Protocol (MSDP).
- **llc2**—Verzendt Logical Link Control, type 2 (LLC2) meldingen.
- **repeater**—Verzendt standaard repeater (hub) meldingen.
- **rsrb**—Hiermee worden RSRB-meldingen (Remote Source-Route Bridging) verzonden.
- **rsvp**—Verzendt RSVP-meldingen (Resource Reservation Protocol).
- **rtr**—Verzendt SA Agent (RTR) meldingen.
- **sdlc**—Verstuurt meldingen via Synchronous Data Link Control (SDLC).
- **snmp**—Verzendt Simple Network Management Protocol (SNMP)-meldingen (zoals gedefinieerd in RFC 1157).
- **stun**—Verzendt seriële tunnelmeldingen (STUN).
- **syslog**—Verzendt foutmeldingen (Cisco Syslog MIB). Specificeer het niveau van de berichten die met `debugging history level` uit.
- **tty**—Verzendt Cisco-ondernemings specifieke meldingen wanneer een TCP-verbinding (Transmission Control Protocol) wordt gesloten.
- **voice**—Stuurt spraakmeldingen.
- **x25**—Verzendt X.25 gebeurtenismeldingen.
- **xgcp**—Verzendt externe media Gateway Control Protocol (XGCP)-meldingen.

## Standaard

Het `snmp-server host` Deze opdracht is standaard uitgeschakeld. Er worden geen meldingen verzonden.

Als u deze opdracht zonder trefwoorden invoert, is de standaardinstelling dat alle traotypes naar de host worden verzonden.

Er worden geen informatie naar deze host verzonden. Indien neen `version` het sleutelwoord is aanwezig, is het gebrek versie 1. Het `no snmp-server host` De opdracht zonder trefwoorden schakelt vallen uit, maar informeert niet, naar de host. Geef het `no snmp-server host informs` opdracht om `informs` uit te schakelen.

**Opmerking:** Indien de `community-string` wordt niet gedefinieerd met de `snmp-server community` opdracht voordat u deze opdracht gebruikt, de standaardvorm van de `snmp-server community` het bevel wordt automatisch opgenomen in de configuratie. Het wachtwoord (`community-string`) automatische configuratie van de `snmp-server community` is hetzelfde als gespecificeerd in de `snmp-server host` uit. Dit is het standaardgedrag voor Cisco IOS-software release 12.0(3) en hoger.

# Opdrachtmodi

## Wereldwijde configuratie - Opdrachtgeschiedenis

### Cisco IOS-software release Wijziging

10.0

Opdracht geïntroduceerd

12,0(3)T

Deze trefwoorden zijn toegevoegd:

- `version 3 [auth | noauth | priv]`
- `hsrp`

## Richtlijnen gebruiken

SNMP-meldingen kunnen als vallen worden verzonden of verzoeken informeren. Vallen zijn onbetrouwbaar omdat de ontvanger geen bevestigingen verstuurt wanneer dit apparaat vallen ontvangt. De afzender kan niet bepalen of de valstrikken zijn ontvangen. Een SNMP-entiteit die een verzoek om informatie ontvangt, erkent het bericht echter met een SNMP Response Protocol Data Unit (PDU). Indien de afzender nooit antwoord ontvangt, kan het informatieverzoek opnieuw worden verzonden. Daarom is het waarschijnlijker dat informanten hun bestemming bereiken.

Echter, informeert verbruiken meer middelen in de agent en in het netwerk. In tegenstelling tot een val, die wordt verwijderd zodra het wordt verzonden, moet een inlichtingenverzoek worden bewaard in het geheugen totdat een antwoord is ontvangen, of de verzoeken worden uitgesteld. Vallen worden slechts één keer verzonden, terwijl een informatie meerdere keren opnieuw kan worden geprobeerd. De herhalingen verhogen het verkeer en dragen bij aan een hogere overhead op het netwerk.

Als u geen `snmp-server host` het bevel, worden geen berichten verzonden. Om de router te configureren om SNMP-meldingen te verzenden, moet u ten minste één bericht invoeren `snmp-server host` uit. Als u de opdracht zonder trefwoorden invoert, zijn alle traptypes ingeschakeld voor de host.

Om meerdere hosts mogelijk te maken, moet u een afzonderlijke `snmp-server host` opdracht voor elke host. U kunt in de opdracht voor elke host meerdere soorten meldingen opgeven.

Wanneer meerdere `snmp-server host` de bevelen worden gegeven voor de zelfde gastheer en soort bericht (val of informeer), elk bevel beschrijft het vorige bevel. Alleen de laatste `snmp-server host` met het commando rekening wordt gehouden. Bijvoorbeeld, als u een `snmp-server host inform` opdracht voor een host en voer vervolgens een andere in `snmp-server host inform` De tweede opdracht vervangt de eerste.

Het `snmp-server host` opdracht wordt gebruikt in combinatie met de `snmp-server enable` uit. Geef het `snmp-server enable` opdracht om aan te geven welke SNMP-meldingen wereldwijd worden verzonden. Om een host de meeste meldingen te laten ontvangen, moet ten minste één `snmp-server enable` bevel en de `snmp-server host` het bevel voor die gastheer moet worden toegelaten.

Sommige soorten meldingen kunnen echter niet worden gecontroleerd met de `snmp-server enable` uit. Sommige soorten meldingen zijn bijvoorbeeld altijd ingeschakeld. Andere berichttypes worden toegelaten door een ander bevel. Bijvoorbeeld, `linkUpDown` kennisgevingen worden gecontroleerd door de `snmp trap link-status` uit. Voor deze soorten meldingen is geen `snmp-server enable` uit.

De beschikbaarheid van een melding-type optie hangt af van het routertype en Cisco IOS-

softwarefuncties die op de router worden ondersteund. Bijvoorbeeld, `envmon` het soort kennisgeving is alleen beschikbaar als de milieumoniteur deel uitmaakt van het systeem.

## Configureren van informatie

Voltooi deze stappen om te kunnen verzenden en informeren:

1. Configureer een externe engine-id.
2. Configureer een externe gebruiker.
3. Configureer een groep op een extern apparaat.
4. Schakel traps op het externe apparaat in.
5. Schakel SNMP-beheer in.

## Voorbeelden

Als u een unieke SNMP-community-string voor traps wilt configureren, maar u wilt voorkomen dat SNMP-polling toegang heeft tot deze string, moet de configuratie een toegangslijst bevatten. In dit voorbeeld wordt de community string "comaccess" genoemd en de toegangslijst heeft nummer 10:

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

Dit voorbeeld verstuurt de SNMP-traps naar de host die wordt opgegeven met de naam `myhost.cisco.com`. De community string is gedefinieerd als `comaccess`:

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

In dit voorbeeld worden de ondernemings specifieke vallen van SNMP en Cisco Environmental Monitor verstuurd naar adressen van `172.30.2.160`:

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

Dit voorbeeld laat de router toe om alle vallen naar de gastheer `myhost.cisco.com` met het communautaire koordpubliek te verzenden:

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

Dit voorbeeld stuurt geen vallen naar een host. De BGP-traps zijn ingeschakeld voor alle hosts, maar alleen de ISDN-traps kunnen naar een host worden verzonden.

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

Dit voorbeeld laat de router toe om alle informatieverzoeken naar de gastheer myhost.cisco.com met het communautaire koordpubliek te verzenden:

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

In dit voorbeeld worden HSRP SNMPv2c-traps naar de host verzonden die wordt gespecificeerd met de naam myhost.cisco.com. De community string is gedefinieerd als public.

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

## Het `snmp-server enable traps` Opdracht

Gebruik de `snmp-server enable traps` globale configuratieopdracht om de router in staat te stellen SNMP-traps te verzenden. Gebruik de `no` vorm van deze opdracht om SNMP-meldingen uit te schakelen.

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

## Syntax Beschrijving

(Optioneel) Het type melding dat moet worden ingeschakeld. Als er geen type is opgegeven worden alle meldingen verzonden (inclusief de `envmon` en `repeater` kennisgevingen). Het soort melding kan een van de volgende trefwoorden zijn:

- `aaa-server`—stuurt AAA-servermeldingen. Dit trefwoord wordt alleen toegevoegd sinds Cisco IOS-software release 12.1(3)T voor Cisco AS5300- en AS5800-platforms. Dit is van Cisco-AAA-SERVER-MIB en de meldingen zijn: enterprise 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange
- `bgp`—Verzendt BGP-kennisgevingen van wijzigingen in de status. Dit is van de BGP4-MIB en de meldingen zijn: onderneming 1.3.6.1.2.1.15.7 1 bgpOpgericht 2 bgpBackwardTransition
- `calltracker`—Verzendt een bericht wanneer een nieuwe actieve gespreksingang in cctActiveTable wordt gecreëerd of een nieuwe geschiedenisvraag ingang in cctHistoryTable wordt gemaakt Dit is van Cisco-CALL-TRACKER-MIB, en de berichten zijn: enterprise 1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification 2 ccctCallTerminateNotification
- `config`—Verzendt configuratie meldingen. Dit gebeurt via Cisco-CONFIG-MAN-MIB en de meldingen zijn: enterprise 1.3.6.1.4.1.9.9.43.2 1 ciscoConfigManEvent
- `dial`—Verzendt een bericht wanneer een succesvolle vraag ontruimt, wordt een ontbrok vraagpoging bepaald om uiteindelijk te hebben ontbroken, of wanneer een bericht van een vraagopstelling wordt ontvangen of verzonden. Dit is van de DIAL-CONTROL-MIB, en de meldingen zijn: enterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation 2 dialCtlPeerCallSetup
- `dls`—Verzendt meldingen van DLSw-agents Wanneer de `dls` het sleutelwoord wordt gebruikt, kunt u *notification-option* specificeren. Dit gebeurt via Cisco-DLSW-MIB

*soort  
kennisgeving*

- de meldingen zijn: enterprise 1.3.6.1.4.1.9.10.9.1.7 1 ciscoDLSWTrapTConnPartnerRe  
2 ciscoDLSWTrapTConnProtViolation 3 ciscoDLSWTrapTConnUp 4  
ciscoDLSwTrapTrapTConnDown 5 ciscoDlswCircuitUp 6 ciscoDlw Circuit Down
- **ds0-busyout**—Verzendt een bericht wanneer het busyout van een DS0 interface staat verandert. Dit trefwoord wordt toegevoegd sinds Cisco IOS-software release 12.1(3)T, alleen voor het Cisco AS5300-platform. Dit komt uit de Cisco-POP-MGMT-MIB en het bericht is: enterprise 1.3.6.1.4.1.9.10.19.2 1 cpmDS0BusyoutNotification
  - **ds1-loopback**—Verzendt een bericht wanneer de DS1 interface in loopbackwijze gaat. Dit trefwoord wordt toegevoegd sinds Cisco IOS-software release 12.1(3)T, alleen voor het Cisco AS5300-platform. Dit is van het Cisco-POP-MGMT-MIB en de melding is: Enterprise 1.3.6.1.4.1.9.10.19.2 2 cpmDS1LoopbackNotification
  - **dspu**—Verstuurt een melding wanneer de operationele status van de fysieke eenheid (FI) of de logische eenheid (LU) verandert of wanneer een activeringsfout wordt gedetecteerd. Dit is van Cisco-DSPU-MIB, en de meldingen zijn: enterprise 1.3.6.1.4.1.9.24.1.4.4 1 newdspuPuStateChangeTrap 2 newdspuActiveringFailureTrap enterprise 1.3.6.1.4.1.9.9.24.1.5.3 1 newdspuLuStateChangeTrap 2 dspuActiveringFailureTrap
  - **dsp**—Verstuurt een bericht wanneer de DSP-kaart omhoog of omlaag gaat. Dit is van Cisco DSP-MGMT-MIB en de melding is: Enterprise 1.3.6.1.4.1.9.9.86.2 1 cdspMIBCardStateNotification
  - **entity**—Hiermee worden wijzigingskennisgevingen van Entiteiten MIB verzonden. Dit is van de ENTITEIT-MIB, en de meldingen zijn: enterprise 1.3.6.1.2.1.47.2 1 entConfigChange
  - **envmon**—Hiermee worden kennisgevingen voor milieubewaking verzonden die specifiek zijn voor Cisco's bedrijf wanneer een milieudrempel wordt overschreden. Wanneer de *envmon* sleutelwoord wordt gebruikt, kunt u *notification-optionvalue* specificeren. Dit komt uit de Cisco-ENVMON-MIB, en de meldingen zijn: enterprise 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonShutdownNotification 2 ciscoEnvMonVoltageNotification 3 ciscoEnvMonTemperatureNotification 4 ciscoEnvMonNotification 5 ciscoEnvMonRedundantSupplyNotification
  - **frame-relay**—Verzendt Frame Relay-meldingen. Dit is van de RFC1315-MIB, en de meldingen zijn: enterprise 1.3.6.1.2.1.10.32 1 forDLCIStatusChange
  - **hsrp**—Verzendt Hot Standby Router Protocol (HSRP)-meldingen. Deze functie wordt ondersteund sinds Cisco IOS-software release 12.0(3)T. Dit komt uit Cisco-HSRP-MIB, en de meldingen zijn: enterprise 1.3.6.1.4.1.9.9.106.2 1 cHSRPstateChange
  - **isdn**—Hiermee worden ISDN-meldingen verzonden. Wanneer de *isdn* het sleutelwoord wordt gebruikt, kunt u *notification-optionvalue* specificeren. Dit komt uit Cisco-ISDN-MIB en de meldingen zijn: bedrijf 1.3.6.1.4.1.9.9.2 1 demandNbrCallInformation 2 demandNbrCallDetails 3 demandNbrLayer2Change [ondersteund sinds Cisco IOS-software release 12.1(1)T ] 4 demandNbrCNANotification [ondersteund sinds Cisco IOS-software release 12.1(5)T ] Dit komt uit Cisco-ISDNU-IF-MIB en de meldingen zijn: bedrijf 1.3.6.1.4.1 9.18.2.1 melding van CIU-status
  - **msdp**—Hiermee worden meldingen verzonden via Multicast Source Discovery Protocol (MSDP). Dit is van de MSDP-MIB, en de meldingen zijn: enterprise 1.3.6.1.3.92.1.1.7 1 msdpOpgericht 2 msdpBackwardTransition
  - **repeater**—Verzendt Ethernet-hubrepeaterkennisgevingen. Wanneer het trefwoord van de repeater is geselecteerd, kunt u een *notification-option* waarde. Dit komt uit de Cisco-REPEATER-MIB-module en de meldingen zijn: enterprise 1.3.6.1.4.1.9.9.2.3 1 ciscoRptrIllegalSrcAddrTrap



- **rsvp**—Verzendt RSVP-meldingen (Resource Reservation Protocol). Deze functie wordt ondersteund sinds Cisco IOS-software release 12.0(2)T. Dit is van de RSVP-MIB, en de meldingen zijn: enterprise 1.3.6.1.3.71.2 1 newFlow 2 verlorenFlow
- **rtr**—Hiermee worden RTR-meldingen (Service Assurance Agent) verzonden. Dit komt uit de Cisco-RTMON-MIB, en de meldingen zijn: enterprise 1.3.6.1.4.1.9.9.42.2 1 rttMonConnectionChangeNotification 2 rttMonTimeoutNotification 3 rtrmonThresholdNotification 4 rttMonverifyerrorNotification
- **snmp**—Verzendt Simple Network Management Protocol (SNMP)-meldingen. Wanneer de **desnmphet** sleutelwoord wordt gebruikt, kunt u een bericht-optie waarde specificeren. Dit is van Cisco-GENERAL-TRAPS, en de meldingen zijn: enterprise 1.3.6.1.2.1.11 0 ColdStart 1 linkDown 3 linkUp 4 authenticatieFailure 5 egpNeighborLoss enterprise 1.3.6.1.4.1.9.9.43.2 1 reload **Opmerking:** Deze val wordt gecontroleerd door het meldingstype "tty": 1 tcpConnectionClose
- **syslog**—Verzendt foutmeldingen (Cisco Syslog MIB). Specificeer het niveau van de berichten die met **debugging history level** uit. Dit is van Cisco-SYSLOG-MIB, en de meldingen zijn: enterprise 1.3.6.1.4.1.9.9.41.2 1 clogBericht gegenereerd
- **voice**—Verzendt slechte kwaliteit van stemberichten. Dit komt uit de Cisco-VOICE-DIAL-CONTROL-MIBSMI-module en de meldingen zijn: enterprise 1.3.6.1.4.1.9.9.63.2 1 cvdcPoorQoVPN-melding
- **xgcp**—Verzendt externe media Gateway Control Protocol (XGCP)-meldingen. Dit is van de XGCP-MOB, en de meldingen zijn: enterprise 1.3.6.1.3.90.2 1 xgcpUpNotification (Optioneel)
- **dls w [circuit | tconn]**—Wanneer de **dls w** het sleutelwoord wordt gebruikt, kunt u het specifieke berichtstype specificeren dat u wilt in- of uitschakelen. Als er geen trefwoord wordt gebruikt, zijn alle DLSw-berichttypes ingeschakeld. De optie kan één of meer van deze trefwoorden zijn: **circuit**—Schakelt DLSw-circuittraps in. **tconn**—Maakt DLSw-peer-transportverbindingen mogelijk.
- **envmon [voltage | shutdown | supply | fan | temperature]**—Wanneer de **envmon** het sleutelwoord wordt gebruikt, kunt u een specifiek type van milieubericht toelaten, of alle berichttypes van het milieumonitoringsysteem goedkeuren. Als er geen optie is opgegeven, worden alle omgevingsmeldingen ingeschakeld. De optie kan één of meer van deze trefwoorden zijn: **voltage, shutdown, supply, fan, temperature**.
- **isdn [call-information | isdn u-interface | chan-not-avail | layer2]**—Wanneer de **isdn** het sleutelwoord wordt gebruikt, kunt u specificeren **call-information** het sleutelwoord om een SNMP-ISDN-gespreksinformatiebericht voor het ISDN MIB-subsysteem in te schakelen, of u kunt het **u-interface** trefwoord om een SNMP ISDN U-interface waarschuwing voor het MIB-subsysteem voor ISDN U-interface in te schakelen.
- **repeater [health | reset]**—Wanneer de **repeater** het sleutelwoord wordt gebruikt, kunt u de **repeater** optie specificeren. Als er geen optie is opgegeven, worden alle herhaalmeldingen ingeschakeld. De optie kan één of meer van deze trefwoorden zijn: **gezondheid**—laat de gezondheidsbericht van de Groep van de Techniek van Internet (IETF) toe van de Repeater Hub MIB (RFC 1516). **reset**—laat IETF Repeater Hub MIB (RFC 1516) **reset** toe. **health**—Schakelt de Internet Engineering Task Force (IETF) Repeater Hub MIB (RFC 1516) gezondheidsmelding in. **reset**—Schakelt de IETF Repeater Hub MIB (RFC 1516) **reset**-melding in.
- **snmp [authentication | linkup | linkdown | coldstart]** trefwoorden **linkup | linkdown | coldstart** toegevoegd sinds Cisco IOS-software release 12.1(3)T. —Wanneer de **snmp** het sleutelwoord wordt gebruikt, kunt u het specifieke berichtstype specificeren dat u wilt in- of uitschakelen. Als

*meldingsoptie*

geen trefwoord wordt gebruikt, worden alle SNMP-berichttypen ingeschakeld (of uitgeschakeld als het formulier No wordt gebruikt). De beschikbare soorten meldingen

**authentication**—Controleert de distributie van SNMP-verificatiefouten. Een authenticatieFailure(4)-trap geeft aan dat de verzendende protocolentiteit de adressaan van een protocolbericht dat niet correct is geverifieerd.

**linkup**—Controleert het verzenden van SNMP-koppelingsmeldingen. Een linkUp(3)-trap betekent dat de verzendende protocolentiteit herkent dat een van de communicatieverbindingen die in de configuratie van de agent worden weergegeven, is opgekomen.

**linkdown**—Controleert de manier waarop SNMP-linkdown-meldingen worden verzonden. Een linkDown(2) val betekent dat de verzendende protocolentiteit een storing in een van de communicatieverbindingen herkent die worden weergegeven in de configuratie van de agent.

**coldstart**—Bestuurt het verzenden van SNMP coldstart meldingen. Een ColdStart(0)-val betekent dat de verzendende protocolentiteit zichzelf opnieuw initialiseert, zodat de configuratie van de agent of de implementatie van de protocolentiteit kan worden gewijzigd.

## Standaard

SNMP-meldingen zijn uitgeschakeld.

Als u dit commando invoert zonder aanmeldingstypen, staat het standaard om alle soorten meldingen die door dit commando worden beheerst, in te schakelen.

## Opdrachtmodi

### Wereldwijde configuratie - Opdrachtgeschiedenis

#### Cisco IOS- softwarerelease

#### Wijziging

11.1

Dit commando werd geïntroduceerd.

12,0(2)T

Het **svpt** trefwoord toegevoegd.

12,0(3)T

Het **hsrp** trefwoord toegevoegd.

Deze trefwoorden zijn toegevoegd aan de **snmp-server enable traps snmp** vorm van de opdracht:

- **linkup**
- **linkdown**
- **coldstart**

12.1(3)T

Deze soort trefwoorden zijn alleen toegevoegd voor het Cisco AS5300-platform:

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

Dit aanmeldtype trefwoord is alleen toegevoegd voor de Cisco AS5300- en AS5300-  
platforms:

- **aaa-server**

## Richtlijnen gebruiken

Het `snmp-server enable traps snmp [ linkup] [linkdown]` deze opdracht vervangt de `snmp trap link-status interface` opdracht voor configuratiemodus.

Het `no` vorm van de `snmp-server enable traps` De opdracht is handig om meldingen uit te schakelen die een grote hoeveelheid onnodige ruis op uw netwerk genereren.

SNMP-meldingen kunnen als vallen worden verzonden of verzoeken informeren. Met deze opdracht kunnen zowel vallen als verzoeken om de gespecificeerde soorten meldingen worden doorgegeven.

Als u geen `snmp-server enable traps` het bevel, worden geen berichten die door dit bevel worden gecontroleerd verzonden. Om de router te configureren om deze SNMP-meldingen te verzenden, moet u ten minste één bericht invoeren `snmp-server enable traps` uit. Als u de opdracht zonder trefwoorden invoert, zijn alle soorten meldingen ingeschakeld. Als u de opdracht met een trefwoord invoert, wordt alleen het berichttype met betrekking tot dat trefwoord ingeschakeld. Om meerdere soorten meldingen mogelijk te maken, moet u een afzonderlijke `snmp-server enable traps` bevel voor elk berichttype en berichtoptie.

Het `snmp-server enable traps` opdracht wordt gebruikt in combinatie met de `snmp-server host` uit. Geef het `snmp-server host` opdracht om te specificeren welke host of hosts SNMP-meldingen ontvangen. Om meldingen te verzenden, moet u ten minste één configuratie instellen `snmp-server host` uit.

Om een host een melding te laten ontvangen die door dit commando wordt gecontroleerd, `snmp-server enable traps` bevel en de `snmp-server host` het bevel voor die gastheer moet worden toegelaten. Indien het type melding niet door deze opdracht wordt beheerst, dient alleen de juiste `snmp-server host` De opdracht moet zijn ingeschakeld.

De notificatietypen die in deze opdracht worden gebruikt, hebben allemaal een gekoppeld MIB-object waarmee ze kunnen worden ingeschakeld of uitgeschakeld (HSRP-traps worden bijvoorbeeld gedefinieerd met de HSRP MIB, repeater-traps worden gedefinieerd met de Repeater Hub MIB, enzovoort). Niet alle soorten kennisgevingen zijn beschikbaar in de `snmp-server host` de opdracht heeft **een melding**MIB-objecten **inschakelen**, zodat sommige hiervan niet kunnen worden beheerd met de `snmp-server enable` uit.

## Gerelateerde informatie

- [Cisco technische ondersteuning en downloads](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.