Unterstützte IOS SNMP-Traps konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie unterstützte Cisco SNMP-Traps konfiguriert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

Sie möchten nicht, dass ein Cisco Gerät alle SNMP-Traps sendet, die das Gerät senden kann. Wenn Sie z. B. alle Traps in einem RAS-Server mit 64 Einwahlleitungen aktivieren, erhalten Sie ein Trap, wenn sich ein Benutzer einwählt und ein Benutzer die Verbindung beendet. Dadurch entstehen zu viele Fallen. Die Cisco IOS® Software definiert Trap-Gruppen, die Sie aktivieren oder deaktivieren können. Es gibt zwei globale Konfigurationsbefehle, mit denen Sie SNMP-Traps auf einem Cisco IOS Software-Gerät konfigurieren:

-

snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type]
Stellen Sie die snmp-server host global configuration -Befehl, um den Empfänger einer SNMP-Benachrichtigung anzugeben. Stellen Sie die **no** um den angegebenen Host zu entfernen.

- **snmp-server enable traps [notification-type] [notification-option]**
Stellen Sie die**snmp-server enable traps global configuration**, damit der Router SNMP-Traps senden kann. Stellen Sie die **no** um SNMP-Benachrichtigungen zu deaktivieren.

Die Trap-Typen können in beiden Befehlen angegeben werden. Sie müssen die **snmp-server host< /strong>** , um die Netzwerkmanagementsysteme festzulegen, an die Traps gesendet werden sollen. Sie müssen die Trap-Typen angeben, wenn nicht alle Traps gesendet werden sollen. Mehrfachausgabe **snmp-server enable traps** -Befehlen einen für jeden der Trap-Typen, die Sie in der **snmp host** aus.

> **Hinweis**: Nicht alle [*notification-type*] -Optionen werden von beiden Befehlen unterstützt. Beispiele, [*notification-type*] x25 und Teletype (tty) werden nicht für **snmp-server enable trap** x25 und tty Traps sind standardmäßig aktiviert.

Geben Sie beispielsweise die folgenden Befehle ein, damit ein Cisco IOS-Software-Gerät nur die Konfiguration, das Border Gateway Protocol (BGP) und tty Traps an das Network Management System 10.10.10.10 meldet:

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

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

> **Hinweis**: Dieses Dokument wurde mit Version 12.1(3)T der Cisco IOS-Software erstellt. Wenn Sie eine frühere Cisco IOS-Softwareversion verwenden, werden nicht alle Optionen unterstützt. Wenn Sie eine Cisco IOS-Softwareversion nach 12.1(3)T verwenden, können zusätzliche Optionen vom Typ [notification-type] unterstützt werden. Eine aktuelle Liste aller unterstützten Cisco IOS Software Simple Network Management Protocol (SNMP) Trap Object Identifiers (OIDs) finden Sie in diesem Dokument.

Cisco Geräte, auf denen die Cisco IOS-Standardsoftware ausgeführt wird (Router, ATM-Switches (Asynchronous Transfer Mode) und Remote Access Server), können eine Vielzahl von SNMP-Traps generieren.

Befehle

Die Fehlermeldung snmp-server host Command

Stellen Sie die **snmp-server host global configuration** -Befehl, um den Empfänger einer SNMP-Benachrichtigung anzugeben. Stellen Sie die **no** um den angegebenen Host zu entfernen.

```
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]
```

Syntaxbeschreibung

host-addr	Der Name oder die Internetadresse des Hosts (der Zielempfänger).
traps	(Optional) Senden Sie SNMP-Traps an diesen Host. Dies ist die Standardeinstellur
informs	(Optional) Senden Sie SNMP-Informationen an diesen Host.
version	(Optional) Die Version des SNMP, die zum Senden der Traps verwendet wird. Vers ist das sicherste Modell, da dieses Modell die Paketverschlüsselung mit dem **priv** Schlüsselwort. Wenn Sie das version-Schlüsselwort verwenden, müssen Sie eine d folgenden Optionen angeben: • **1** - SNMPv1. Diese Option ist bei Informs nicht verfügbar. • **2c** - SNMPv2C • **3:** SNMPv3. Die folgenden drei optionalen Schlüsselwörter können nach dem Schlüsselwort der Version 3 eingefügt werden: **auth**(Optional) Aktiviert Message Digest 5 (MD5)- und Secure Hash Algorithm (SHA)-Paketauthentifizierung.**noau** (Standard) Die Sicherheitsstufe noAuthNoPriv. Dies ist der Standardwert, wenn [auth | noauth | priv] Schlüsselwortwahl ist nicht angegeben.**priv** (Optional) Aktiv die DES-Paketverschlüsselung (Data Encryption Standard) (auch "Privacy" genannt).
community-string	Der passwortähnliche Community String, der mit der Benachrichtigung gesendet w Sie können diesen String jedoch mit dem **snmp-server host** für sich genommen, empfie Cisco, diese Zeichenfolge mit dem **snmp-server community** vor der Ausgabe des **snmp-s host** aus.
udp-port*port*	User Datagram Protocol (UDP)-Port des zu verwendenden Hosts Der Standardwer 162.
Benachrichtigungstyp	(Optional) Die Art der Benachrichtigung, die an den Host gesendet werden soll. We kein Typ angegeben ist, werden alle Benachrichtigungen gesendet. Beim Benachrichtigungstyp kann es sich um eines oder mehrere der folgenden Schlüsselwörter handeln: • **aaa-server** - Sendet AAA-Benachrichtigungen. • **bgp** - Sendet Border Gateway Protocol (BGP)-Statusänderungsbenachrichtigun • **bstun**- Sendet BSTUN-Benachrichtigungen (Block Serial Tunneling). • **calltracker**- Sendet CallTracker-Benachrichtigungen. • **config**- Sendet Konfigurationsbenachrichtigungen. • **dlsw**- Sendet DLSw-Benachrichtigungen (Data-Link Switching). • **ds0-busyout**- Sendet ds0-busyout-Benachrichtigungen.

- **ds1-loopback**- Sendet ds1-Loopback-Benachrichtigungen.
- **dspu**- Sendet DSPU-Benachrichtigungen (Downstream Physical Unit).
- **dsp**- Sendet DSP-Benachrichtigungen (Digital Signal Processing).
- **entity**- Sendet MIB-Änderungsbenachrichtigungen (Entity Management Informat Base).
- **envmon**- Sendet Cisco unternehmensspezifische Umgebungsüberwachungsbenachrichtigungen, wenn ein umgebungsspezifisch Schwellenwert überschritten wird.
- **frame-relay**- Sendet Frame-Relay-Benachrichtigungen.
- **hsrp**- Sendet HSRP-Benachrichtigungen (Hot Standby Router Protocol).
- **isdn**- Sendet ISDN-Benachrichtigungen (Integrated Services Digital Network).
- **msdp**- Sendet MSDP-Benachrichtigungen (Multicast Source Discovery Protocol
- **llc2**- Sendet Benachrichtigungen über logische Verknüpfungssteuerung vom Ty (LLC2).
- **repeater**- Sendet Standard-Repeater-Benachrichtigungen (Hub).
- **rsrb**- Sendet Remote-RSRB-Benachrichtigungen (Source-Route Bridging).
- **rsvp**- Sendet RSVP-Benachrichtigungen (Resource Reservation Protocol).
- **rtr**- Sendet Benachrichtigungen des SA Agents (RTR).
- **sdlc**- Sendet SDLC-Benachrichtigungen (Synchronous Data Link Control).
- **snmp**- Sendet SNMP-Benachrichtigungen (Simple Network Management Protoc (wie in RFC 1157 definiert).
- **stun**- Sendet Benachrichtigungen über serielle Tunnel (STUN).
- **syslog**- Sendet Fehlermeldungen (Cisco Syslog MIB). Geben Sie die Nachrichtenebene an, die mit dem**logging history level**aus.
- **tty**- Sendet unternehmensspezifische Benachrichtigungen von Cisco, wenn ein TCP-Verbindung (Transmission Control Protocol) geschlossen wird.
- **voice**- Sendet Sprachbenachrichtigungen.
- **x25**- Sendet X.25-Ereignisbenachrichtigungen.
- **xgcp**- Sendet XGCP-Benachrichtigungen (External Media Gateway Control Pro

Standardwerte

Die Fehlermeldung **snmp-server host** ist standardmäßig deaktiviert. Es werden keine Benachrichtigungen gesendet.

Wenn Sie diesen Befehl ohne Schlüsselwörter eingeben, werden standardmäßig alle Trap-Typen an den Host gesendet.

Es werden keine Informationen an diesen Host gesendet. Wenn nein **version** -Schlüsselwort vorhanden ist, lautet der Standardwert Version 1. Die Fehlermeldung **no snmp-server host** -Befehl ohne Schlüsselwörter werden Traps für den Host deaktiviert, jedoch keine Informationen. Stellen Sie die **no snmp-server host informs** um Informationen zu deaktivieren.

> **Hinweis**: Wenn der *community-string* ist nicht definiert mit **snmp-server community** -Befehl, bevor Sie diesen Befehl verwenden, die Standardform des **snmp-server community** wird automatisch in die Konfiguration eingefügt. Das Passwort (*community-string*) für diese automatische Konfiguration der **snmp-server community** entspricht den Angaben im **snmp-server host** aus. Dies ist das Standardverhalten für Cisco IOS Software, Version 12.0(3) und höher.

Befehlsmodi

Globale Konfiguration - Befehlsverlauf

Cisco IOS-Softwareversion	Änderung
10.0	Befehl eingeführt.
12,0(3)T	Folgende Schlüsselwörter wurden hinzugefügt: • **version 3 [auth | noauth | priv]** • **hsrp**

Richtlinien verwenden

SNMP-Benachrichtigungen können als Traps oder Inform-Anfragen gesendet werden. Traps sind unzuverlässig, da der Empfänger keine Bestätigungen sendet, wenn dieses Gerät Traps empfängt. Der Absender kann nicht feststellen, ob die Traps empfangen wurden. Eine SNMP-Einheit, die eine Inform-Anfrage empfängt, bestätigt die Nachricht jedoch mit einer SNMP-Response Protocol Data Unit (PDU). Wenn der Absender die Antwort nie erhält, kann die Inform-Anfrage erneut gesendet werden. Informationen erreichen daher eher ihr beabsichtigtes Ziel.

Informationen belegen jedoch mehr Ressourcen im Agent und im Netzwerk. Im Gegensatz zu einem Trap, der verworfen wird, sobald er gesendet wird, muss eine Informationsanfrage im Speicher gehalten werden, bis eine Antwort empfangen wird oder die Anfrage eine Zeitüberschreitung aufweist. Traps werden nur einmal gesendet, während eine Benachrichtigung mehrmals wiederholt werden kann. Die Wiederholungsversuche erhöhen den Datenverkehr und tragen zu einem höheren Overhead im Netzwerk bei.

Wenn Sie keine **snmp-server host** -Befehl, werden keine Benachrichtigungen gesendet. Damit der Router SNMP-Benachrichtigungen senden kann, müssen Sie mindestens einen **snmp-server host** aus. Wenn Sie den Befehl ohne Schlüsselwörter eingeben, sind alle Trap-Typen für den Host aktiviert.

Um mehrere Hosts zu aktivieren, müssen Sie einen separaten **snmp-server host** -Befehls für jeden Host. Sie können im Befehl für jeden Host mehrere Benachrichtigungstypen angeben.

Wenn mehrere **snmp-server host** -Befehle für denselben Host und dieselbe Art von Benachrichtigung (Trap oder Inform) angegeben werden, überschreibt jeder Befehl den vorherigen Befehl. Nur die letzte **snmp-server host** berücksichtigt. Wenn Sie z. B. eine snmp-server host inform -Befehl für einen Host ein, und geben Sie dann einen anderen **snmp-server host inform** -Befehls für denselben Host, ersetzt der zweite Befehl den ersten.

Die Fehlermeldung **snmp-server host** wird zusammen mit dem Befehl **snmp-server enable** aus. Stellen Sie die **snmp-server enable** um festzulegen, welche SNMP-Benachrichtigungen global gesendet werden. Damit ein Host die meisten Benachrichtigungen erhalten kann, muss mindestens eine **snmp-server enable** und die **snmp-server host** -Befehls für diesen Host aktiviert werden.

Einige Benachrichtigungstypen können jedoch nicht mit dem **snmp-server enable** aus. Beispielsweise sind einige Benachrichtigungstypen immer aktiviert. Andere Benachrichtigungstypen werden durch einen anderen Befehl aktiviert. Zum Beispiel `linkUpDown` Meldungen werden von der **snmp trap link-status** aus. Für diese Benachrichtigungstypen ist keine **snmp-server enable** aus.

Die Verfügbarkeit einer Benachrichtigungsoption hängt vom Routertyp und den Cisco IOS-

Softwarefunktionen ab, die vom Router unterstützt werden. Zum Beispiel **envmon** Notification-Type ist nur verfügbar, wenn der Umgebungsmonitor Teil des Systems ist.

Informs konfigurieren

Gehen Sie wie folgt vor, um Informationen senden zu können:

1. Konfigurieren einer Remote-Engine-ID
2. Konfigurieren eines Remote-Benutzers
3. Konfigurieren einer Gruppe auf einem Remote-Gerät
4. Aktivieren Sie Traps auf dem Remote-Gerät.
5. Aktivieren Sie den SNMP-Manager.

Beispiele

Wenn Sie einen eindeutigen SNMP-Community-String für Traps konfigurieren, aber den SNMP-Polling-Zugriff mit diesem String verhindern möchten, muss die Konfiguration eine Zugriffsliste enthalten. In diesem Beispiel hat der Community-String den Namen "comaccess", und die Zugriffsliste hat die Nummer 10:

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

In diesem Beispiel werden die SNMP-Traps an den Host gesendet, der mit dem Namen myhost.cisco.com angegeben ist. Der Community-String wird als comaccess definiert:

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

In diesem Beispiel werden die unternehmensspezifischen Traps der SNMP- und Cisco Umgebungsüberwachung an die Adresse 172.30.2.160 gesendet:

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

In diesem Beispiel kann der Router alle Traps mit dem Community-String public an den Host myhost.cisco.com senden:

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

In diesem Beispiel werden keine Traps an einen Host gesendet. Die BGP-Traps sind für alle Hosts aktiviert, aber nur die ISDN-Traps können an einen Host gesendet werden.

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

In diesem Beispiel kann der Router alle Inform-Anfragen mit dem Community-String public an den Host myhost.cisco.com senden:

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

In diesem Beispiel werden HSRP-SNMPv2c-Traps an den Host gesendet, der mit dem Namen myhost.cisco.com angegeben ist. Der Community-String ist als public definiert.

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

Die Fehlermeldung snmp-server enable traps Command

Verwenden Sie **snmp-server enable traps** globaler Konfigurationsbefehl, um den Router zum Senden von SNMP-Traps zu aktivieren. Verwenden Sie **no** um SNMP-Benachrichtigungen zu deaktivieren.

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

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

Syntaxbeschreibung

Benachrichtigungstyp	(Optional) Der Typ der zu aktivierenden Benachrichtigung. Wenn kein Typ angegeben ist, werden alle Benachrichtigungen gesendet (einschließlich der **env** und **repeater** Benachrichtigungen). Beim Benachrichtigungstyp kann es sich um e der folgenden Schlüsselwörter handeln: • **aaa-server**- Sendet AAA-Serverbenachrichtigungen. Dieses Schlüsselwort wu seit Version 12.1(3)T der Cisco IOS-Software nur für die Plattformen Cisco AS5300 und AS5800 hinzugefügt. Dies stammt aus der CISCO-AAA-SERV MIB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange • **bgp** - Sendet Border Gateway Protocol (BGP)-Statusänderungsbenachrichtigungen. Dieser stammt aus BGP4-MIB, und d Benachrichtigungen lauten: enterprise 1.3.6.1.2.1.15.7 1 bgpEstablished 2 bgpBackwardTransition • **calltracker** - Sendet eine Benachrichtigung, wenn in der cctActiveTable ein ne aktiver Anrufeintrag oder in der cctHistoryTable ein neuer historischer Anrufeintrag erstellt wird. Dieser stammt aus der CISCO-CALL-TRACKER-M und die Benachrichtigungen lauten: enterprise 1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification 2 cctCallTermination DatumBenachrichtigung • **config** - Sendet Konfigurationsbenachrichtigungen. Dies stammt aus der CIS CONFIG-MAN-MIB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.4.1.9.9.43.2 1 ciscoConfigManEvent • **dial** - Sendet eine Benachrichtigung, wenn ein erfolgreicher Anruf beendet w festgestellt wird, dass ein fehlgeschlagener Anrufversuch letztendlich fehlgeschlagen ist, oder wenn eine Anrufeinrichtungsnachricht empfangen c

gesendet wird. Dies ist aus der DIAL-CONTROL-MIB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation 2 dialCtlPeerCallSetup

- **dlsw** - Sendet Benachrichtigungen von DLSw-Agenten, wenn der **dlsw** - Schlüsselwort verwendet wird, können Sie *anotification*-optionvalue angebe Dies ist aus der CISCO-DLSW-MIB, und die Benachrichtigungen sind: Ente 1.3.6.1.4.1.9.10.9.1.7 1 ciscoDlswTrapTConnPartnerReject 2 ciscoDlswTrapTConnProtViolation 3 ciscoDlswTrapTConon Bis 4 ciscoDlswTrapTConnDown 5 ciscoDlswTrapCircuitUp 6 ciscoDlswTrapCircuitDown
- **ds0-busyout**- Sendet eine Benachrichtigung, wenn sich der Status des Busyou einer DS0-Schnittstelle ändert. Dieses Schlüsselwort wurde seit Version 12 der Cisco IOS-Software nur für die Cisco AS5300-Plattform hinzugefügt. Die aus der CISCO-POP-MGMT-MIB, und die Benachrichtigung lautet: enterpris 1.3.6.1.4.1.9.10.19.2 1 cpmDS0BusyoutNotification
- **ds1-loopback**- Sendet eine Benachrichtigung, wenn die DS1-Schnittstelle in de Loopback-Modus wechselt. Dieses Schlüsselwort wurde seit Version 12.1(3 der Cisco IOS-Software nur für die Cisco AS5300-Plattform hinzugefügt. Die stammt aus der CISCO-POP-MGMT-MIB, und die Benachrichtigung lautet: Enterprise 1.3.6.1.4.1.9.10.19.2 2 cpmDS1LoopbackNotification
- **dspu**- Sendet eine Benachrichtigung, wenn der Betriebszustand der physisch Einheit (PU) oder der logischen Einheit (LU) sich ändert oder ein Aktivierungsfehler erkannt wird. Dies ist aus der CISCO-DSPU-MIB, und die Benachrichtigungen sind: enterprise 1.3.6.1.4.1.9.9.24.1.4.4 1newdspuPuStateChangeTrap 2 newdspuPuActivationFailureTrap enterpris 1.3.6.1.4.1.9.9.24.1 2.5.3 1 newdspuLuStateChangeTrap 2 dspuLuActivationFailureTrap
- **dsp**- Sendet eine Benachrichtigung, wenn die DSP-Karte hoch- oder herunterfährt. Dieser stammt aus der CISCO-DSP-MGMT-MIB, und die Benachrichtigung lautet: enterprise 1.3.6.1.4.1.9.9.86.2 1 cdspMIBCardStateNotification
- **entity**- Sendet Benachrichtigungen über Änderungen an Entity MIB. Diese st aus ENTITY-MIB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.2.1 1 entConfigChange
- **envmon**- Sendet unternehmensspezifische Umgebungsüberwachungsbenachrichtigungen von Cisco, wenn ein Umgeb Schwellenwert überschritten wird. Wenn die**envmon**-Schlüsselwort verwende wird, können Sie *anotification*-optionvalue angeben. Dies ist aus der CISCO ENVMON-MIB, und die Benachrichtigungen sind: Enterprise 1.3.6.1.4.1.9.9 1 ciscoEnvMonShutdownNotification 2 ciscoEnvMonVoltageNotification 3 ciscoEnvMonTemperatureNotification 4 ciscoEnvMonFanNotification 5 ciscoUmvMonRedundanteLieferankündigung
- **frame-relay**- Sendet Frame-Relay-Benachrichtigungen. Dies stammt aus RFC MIB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.2.1.10.32.1 frDLCIStatusChange
- **hsrp**- Sendet HSRP-Benachrichtigungen (Hot Standby Router Protocol). Die Funktion wird seit Version 12.0(3)T der Cisco IOS-Software unterstützt. Die

stammt aus der CISCO-HSRP-MIB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.4.1.9.9.106.2 1 cHsrpStateChange

- **isdn**- Sendet ISDN-Benachrichtigungen. Wenn die**isdn**-Schlüsselwort verwen wird, können Sie *anotification*-optionvalue angeben. Dies ist aus der CISCO ISDN-MIB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.4.1.9.9.26 demandNbrCallInformation 2 demandNbrCallDetails 3 demandNbrLayer2Cl [unterstützt seit Cisco IOS Software Release 12.1(1)T] 4 demandNbrCNAN Benachrichtigung [wird seit Version 12.1(5)T der Cisco IOS-Software unters Dies stammt aus der CISCO-ISDNU-IF-MIB, und die Benachrichtigungen la Enterprise 1.3.6.1.4.1.9.9.18.2.1 ciuIfLoopStatusNotification
- **msdp**- Sendet MSDP-Benachrichtigungen (Multicast Source Discovery Proto Diese stammt aus der MSDP-MIB, und die Benachrichtigungen lauten: ente 1.3.6.1.3.92.1.1.7 1 msdpEstablished 2 msdpBackwardTransition
- **repeater**—Sendet Ethernet-Hub**repeater**Benachrichtigungen. Wenn das Repea Schlüsselwort ausgewählt ist, können Sie eine *notification-option* wert. Dies ist a der CISCO-REPEATER-MIB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap
- **rsvp**- Sendet RSVP-Benachrichtigungen (Resource Reservation Protocol). D Funktion wird seit Version 12.0(2)T der Cisco IOS-Software unterstützt. Die stammt aus der RSVP-MIB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.3.71.2 1 newFlow 2 lostFlow
- **rtr**- Sendet RTR-Benachrichtigungen (RTR) des Service Assurance Agent. D stammt aus der CISCO-RTTMON-MIB. Die Benachrichtigungen lauten wie enterprise 1.3.6.1.4.1.9.9.42.2 1 rttMonConnectionChangeNotification 2 rttMonTimeoutNotification 3 rttMonThresholdNotification 4 rttMonVerifyErrorNotification
- **snmp**- Sendet SNMP-Benachrichtigungen (Simple Network Management Protocol). Wenn die**snmp**-Schlüsselworts verwendet wird, können Sie einen für die Benachrichtigungsoption angeben. Dies ist aus CISCO-GENERAL-TRAPS, und die Benachrichtigungen sind: enterprise 1.3.6.1.2.1.11 0 coldS linkDown 3 linkUp 4 authenticationFailure 5 egpNeighborLoss enterprise 1.3.6.1.4.1.9 0 reload **Hinweis**: Dieses Trap wird vom Benachrichtigungstyp gesteuert: 1 tcpConnectionClose
- **syslog**- Sendet Fehlermeldungen (Cisco Syslog MIB). Geben Sie die Nachrichtenebene an, die mit dem**logging history level**aus. Dies ist aus CISCO SYSLOG-MIB, und die Benachrichtigungen sind: enterprise 1.3.6.1.4.1.9.9.4 1 clogMessageGenerated
- **voice**- Sendet qualitativ minderwertige Sprachbenachrichtigungen. Dies stam aus der CISCO-VOICE-DIAL-CONTROL-MIBSMI, und die Benachrichtigung lauten: Enterprise 1.3.6.1.4.1.9.9.63.2 1 cvdcPoorQoVNotification
- **xgcp**- Sendet XGCP-Benachrichtigungen (External Media Gateway Control Protocol). Dies stammt aus dem XGCP-MOB, und die Benachrichtigungen lauten: enterprise 1.3.6.1.3.90.2 1 xgcpUpDownNotification

Benachrichtigungsoption (Optional)

- **dlsw [circuit | tconn]**- Wenn die**dlsw**-Schlüsselworts verwendet wird, können Sie Benachrichtigungstyp angeben, den Sie aktivieren oder deaktivieren möchte Wenn kein Schlüsselwort verwendet wird, sind alle DLSw-Benachrichtigungstypen aktiviert. Bei der Option kann es sich um eines ode

mehrere der folgenden Schlüsselwörter handeln: **circuit**- Aktiviert DLSw-Schaltkreis-Traps.**tconn**- Aktiviert DLSw-Peer-Transport-Verbindungs-Traps.

- **envmon [voltage | shutdown | supply | fan | temperature]**- Wenn die**envmon**-Schlüsselwo verwendet wird, können Sie einen bestimmten umgebungsbezogenen Benachrichtigungstyp aktivieren oder alle Benachrichtigungstypen vom Umgebungsüberwachungssystem akzeptieren. Wenn keine Option angegeb ist, werden alle Umgebungsbenachrichtigungen aktiviert. Bei der Option kan sich um eines oder mehrere der folgenden Schlüsselwörter handeln:**voltage**,**shutdown**,**supply**,**fan**und**temperature**.
- **isdn [call-information | isdn u-interface | chan-not-avail | layer2]**- Wenn die**isdn**verwende können Sie die**call-information**Schlüsselwort, um eine SNMP ISDN-Anrufinformationsbenachrichtigung für das ISDN MIB-Subsystem zu aktivier oder Sie können die**isdn u-interface**Schlüsselwort, um eine SNMP-ISDN U-Schnittstellenbenachrichtigung für das ISDN U-Schnittstellen-MIB-Subsyste aktivieren.
- **repeater [health | reset]**- Wenn die **repeater** verwendet wird, können Sie die Repea Option angeben. Wenn keine Option angegeben ist, werden alle Repeater-Benachrichtigungen aktiviert. Bei der Option kann es sich um eines oder me der folgenden Schlüsselwörter handeln: health—Enables Internet Engineeri Task Force (IETF) Repeater Hub MIB (RFC 1516) health notification. reset—Enables IETF Repeater Hub MIB (RFC 1516) reset notification. **healt** Aktiviert die Integritätsbenachrichtigung des IETF-Repeater-Hubs MIB (RFC 1516).**reset**- Aktiviert die Rücksetzbenachrichtigung für den IETF Repeater H MIB (RFC 1516).
- **snmp [authentication | linkup | linkdown | coldstart]**Schlüsselwörter **linkup | linkdown | col** seit Version 12.1(3)T der Cisco IOS-Software hinzugefügt. - Wenn die **snmp** Schlüsselworts verwendet wird, können Sie den Benachrichtigungstyp ange den Sie aktivieren oder deaktivieren möchten. Wenn kein Schlüsselwort verwendet wird, sind alle SNMP-Benachrichtigungstypen aktiviert (oder deaktiviert, wenn das Formular no verwendet wird). Folgende Benachrichtigungstypen sind verfügbar: **authentication**- Steuert die Verteilung SNMP-Authentifizierungsfehlerbenachrichtigungen. Ein authenticationFailur Trap bedeutet, dass die sendende Protokollentität der Empfänger einer Protokollnachricht ist, die nicht ordnungsgemäß authentifiziert wurde.**linkup**- Steuert das Senden von SNMP-Verbindungsbenachrichtigungen. Ein linkUp Trap bedeutet, dass die sendende Protokolleinheit erkennt, dass eine der Kommunikationsverbindungen, die in der Konfiguration des Agenten darges werden, aktiv ist.**linkdown**- Steuert, wie SNMP-Linkdown-Benachrichtigungen gesendet werden. Ein linkDown(2)-Trap bedeutet, dass die sendende Protokolleinheit einen Fehler in einer der Kommunikationsverbindungen erk die in der Konfiguration des Agenten dargestellt werden.**coldstart**- Steuert da Senden von SNMP-Coldstart-Benachrichtigungen. Ein coldStart(0)-Trap bedeutet, dass die sendende Protokolleinheit sich selbst neu initialisiert, soc die Konfiguration des Agenten oder die Implementierung der Protokolleinhe geändert werden kann.

Standardwerte

SNMP-Benachrichtigungen sind deaktiviert.

Wenn Sie diesen Befehl ohne Schlüsselwörter für Benachrichtigungstypen eingeben, werden standardmäßig alle Benachrichtigungstypen aktiviert, die von diesem Befehl gesteuert werden.

Befehlsmodi

Globale Konfiguration - Befehlsverlauf

Cisco IOS-Softwareversion	Änderung
11.1	Dieser Befehl wurde eingeführt.
12,0(2)T	Die Fehlermeldung**rsvp**Schlüsselwort wurde hinzugefügt.
12,0(3)T	Die Fehlermeldung **hsrp** Schlüsselwort wurde hinzugefügt.
12.1(3)T	Diese Schlüsselwörter wurden dem **snmp-server enable traps snmp** Form dieses Be • **linkup** • **linkdown** • **coldstart** Die folgenden Schlüsselwörter für Benachrichtigungstypen wurden nur für die Cisco AS5300-Plattform hinzugefügt: • **ds0-busyout** • **isdn chan-not-avail** • **modem-health** • **ds1-loopback** Dieses Schlüsselwort für den Benachrichtigungstyp wurde nur für die Cisco AS5300- und AS5800-Plattformen hinzugefügt: • **aaa-server**

Richtlinien verwenden

Die Fehlermeldung **snmp-server enable traps snmp [linkup] [linkdown]** Form dieses Befehls ersetzt die **snmp trap link-status interface** Konfigurationsmodusbefehl.

Die Fehlermeldung **no** Form der **snmp-server enable traps** ist nützlich, um Benachrichtigungen zu deaktivieren, die eine große Menge an nicht benötigten Geräuschen in Ihrem Netzwerk erzeugen.

SNMP-Benachrichtigungen können als Traps oder Inform-Anfragen gesendet werden. Mit diesem Befehl werden sowohl Traps als auch Inform-Anforderungen für die angegebenen Benachrichtigungstypen aktiviert.

Wenn Sie keine **snmp-server enable traps** -Befehls, werden keine Benachrichtigungen gesendet, die von diesem Befehl gesteuert werden. Um den Router zum Senden dieser SNMP-Benachrichtigungen zu konfigurieren, müssen Sie mindestens einen **snmp-server enable traps** aus. Wenn Sie den Befehl ohne Schlüsselwörter eingeben, sind alle Benachrichtigungstypen aktiviert. Wenn Sie den Befehl mit einem Schlüsselwort eingeben, wird nur der Benachrichtigungstyp für dieses Schlüsselwort aktiviert. Um mehrere Benachrichtigungstypen zu aktivieren, müssen Sie einen separaten **snmp-server enable traps** für jeden Benachrichtigungstyp und jede Benachrichtigungsoption.

Die Fehlermeldung **snmp-server enable traps** wird zusammen mit dem Befehl **snmp-server host** aus. Stellen Sie die **snmp-server host** -Befehl, um anzugeben, welcher Host oder welche Hosts SNMP-

Benachrichtigungen empfangen soll. Um Benachrichtigungen zu senden, müssen Sie mindestens eine **snmp-server host** aus.

Damit ein Host eine von diesem Befehl gesteuerte Benachrichtigung erhalten kann, müssen sowohl **snmp-server enable traps** und die **snmp-server host** -Befehls für diesen Host aktiviert werden. Wenn der Benachrichtigungstyp nicht durch diesen Befehl gesteuert wird, sollten Sie nur den entsprechenden **snmp-server host** muss aktiviert sein.

Die in diesem Befehl verwendeten Benachrichtigungstypen verfügen alle über ein zugehöriges MIB-Objekt, mit dem sie aktiviert oder deaktiviert werden können (z. B. werden HSRP-Traps mit der HSRP-MIB definiert, Repeater-Traps mit der Repeater-Hub-MIB definiert usw.). Nicht alle Benachrichtigungstypen im **snmp-server host** verfügen über eine **BenachrichtigungMIB-**Objekte **aktivieren**, sodass einige dieser Objekte nicht mit dem **snmp-server enable** aus.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.