

サポートされるIOS SNMPトラップの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[コマンド](#)

[snmp-server hostコマンド](#)

[シンタックスの説明](#)

[デフォルト](#)

[コマンドモード](#)

[グローバル設定：コマンド履歴](#)

[使用ガイドライン](#)

[インフォームの設定](#)

[例](#)

[snmp-server enable trapsコマンド](#)

[シンタックスの説明](#)

[デフォルト](#)

[コマンドモード](#)

[グローバル設定：コマンド履歴](#)

[使用ガイドライン](#)

[関連情報](#)

概要

このドキュメントでは、サポートされているCisco SNMPトラップの設定方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

シスコのデバイスで送信方法が認識されているすべてのSNMPトラップを送信する必要はありません。たとえば、64本のダイヤルイン回線が接続されたりリモートアクセスサーバですべてのトラップを使用可能にすると、ユーザのダイヤルインや接続終了のたびにトラップが発生します。この結果、大量のトラップが作成されます。Cisco IOS®ソフトウェアは、有効または無効にできるトラップのグループを定義します。Cisco IOSソフトウェアが稼働するデバイスにSNMPトラップを設定するのに使用されるグローバル設定コマンドには、次の2つがあります。

- `snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type]`
`snmp-server host global configuration` コマンドを使用して、SNMP通知操作の受信者を指定します。
`no` 指定したホストを削除します。

- `snmp-server enable traps [notification-type] [notification-option]`
`snmp-server enable traps global configuration` コマンドを発行して、ルータがSNMPトラップを送信できるようにします。 `no` SNMP通知を無効にするには、このコマンドの形式を使用します。
トラップのタイプは、両方のコマンドで指定できます。このコマンドを実行するには、`snmp-server host` コマンドを発行して、トラップの送信先となるネットワーク管理システム (NMS) を定義します。すべてのトラップを送信するわけではない場合は、トラップのタイプも指定する必要があります。複数の問題 `snmp-server enable traps` コマンドを使用します。各トラップタイプは、`snmp host` コマンドが表示されない場合もあります。

注：すべてではない `[notification-type]` オプションは、これらのコマンドの両方でサポートされています。たとえば、`[notification-type] x25` および `tty` は次の目的では使用されません。 `snmp-server enable trap x25` および `tty` トラップはデフォルトで有効になっています。

たとえば、次のコマンドを発行して、Cisco IOSソフトウェアデバイスが設定、Border Gateway Protocol (BGP ; ボーダーゲートウェイプロトコル)、および `tty` トラップのみを Network Management System (NMS ; ネットワーク管理システム) 10.10.10.10 に報告するようにします。

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

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

注：このドキュメントの作成には、Cisco IOSソフトウェアリリース12.1(3)Tが使用されています。これより前のCisco IOSソフトウェアリリースを使用している場合は、すべてのオプションがサポートされていないことがあります。Cisco IOSソフトウェア 12.1(3)Tよ

りも後のバージョンを使用する場合は、追加の [notification-type] オプションがサポートされる場合があります。このドキュメントには、Cisco IOS ソフトウェアで現在サポートされている Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) トラップの Object Identifiers (OID; オブジェクト識別子) のリストが記載されています。

標準のCisco IOSソフトウェア(ルータ、Asynchronous Transfer Mode (ATM ; 非同期転送モード) スイッチ、およびリモートアクセスサーバ)を実行するシスコデバイスは、多くのSNMPトラップを生成できます。

コマンド

「 snmp-server host コマンド

snmp-server host global configuration コマンドを使用して、SNMP通知操作の受信者を指定します。 no 指定したホストを削除します。

```
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]
```

シンタックスの説明

host-addr	ホスト (ターゲットの受信者) の名前またはインターネット アドレス。
traps	(オプション) このホストに SNMP トラップを送信します。これはデフォルトです。
informs	(オプション) このホストに SNMP インフォームを送信します。
version	(オプション) トラップの送信に使用する SNMP バージョン。バージョン3は最も安全なキーワード。バージョンのキーワードを使用する場合は、次のいずれか 1 つのオプションを <ul style="list-style-type: none">• 1 : SNMPv1このオプションは、inform とともに使用できません。• 2c : SNMPv2C• 3 : SNMPv3次の3つのオプションキーワードは、バージョン3のキーワードの後に使 びSecure Hash Algorithm(SHA)パケット認証を有効にします。noauth noAuthNoPrivデ フォルトとなります : [auth noauth priv] キーワードの選択が指定されていません。 号化 (「プライバシー」とも呼ばれる) を有効にします。
community-string	通知処理で送られる、パスワードに似たコミュニティストリング。この文字列は、 snmp community コマンドを発行してから、 snmp-server host コマンドが表示されない場合もあり
udp-portport	使用するホストの User Datagram Protocol (UDP) ポート。デフォルトは 162 です。 (オプション) ホストに送信される通知のタイプ。タイプを指定しない場合、すべての 1 つ以上指定できます。 <ul style="list-style-type: none">• aaa-server —AAA 通知を送信します。• bgp —BGP 状態変更通知を送信します。• bstun – ブロックシリアルトンネリング(BSTUN)通知を送信します。• calltracker—CallTracker通知を送信します。
notification-type	<ul style="list-style-type: none">• config—設定通知を送信します。• dlsw—Data-Link Switching (DLSw; データリンク スイッチング) 通知を送信します。• ds0-busyout— ds0-busyout通知を送信します。• ds1-loopback— ds1-loopback通知を送信します。• dspu—Downstream Physical Unit (DSPU; 下流物理ユニット) 通知を送信します。• dsp – デジタル信号処理(DSP)通知を送信します。

- **entity**—エンティティ Management Information Base (MIB; 管理情報ベース) 変更通知
- **envmon**—環境のしきい値が設定値を超えたときに、Cisco Enterprise に固有の環境モニタリング
- **frame-relay**—フレームリレー通知を送信します。
- **hsrp**:Hot Standby Router Protocol(HSRP)通知を送信します。
- **isdn**—Integrated Services Digital Network (ISDN; サービス総合デジタルネットワーク)
- **msdp**—マルチキャスト ソース ディスカバリ プロトコル (MSDP) 通知を送信します。
- **llc2** – 論理リンク制御タイプ2(LLC2)通知を送信します。
- **repeater**—標準リピータ (ハブ) 通知を送信します。
- **rsrb**—Remote Source-Route Bridging (RSRB; リモート ソースルート ブリッジング)
- **rsvp**—Resource Reservation Protocol (RSVP; リソース予約プロトコル) 通知を送信します。
- **rtr**—SA エージェント (RTR) 通知を送信します。
- **sdhc**—Synchronous Data Link Control (SDLC; 同期データリンク制御) 通知を送信します。
- **snmp**—SNMP 通知を RFC 1157 の定義に従って送信します。
- **stun**—Serial Tunneling (STUN; シリアル トンネリング) 通知を送信します。
- **syslog**—エラー メッセージ通知を送信します (Cisco Syslog MIB)。メッセージのしきい値も場合があります。
- **tty**—Transmission Control Protocol (TCP; 伝送制御プロトコル) 接続を閉じたときに
- **voice** – 音声通知を送信します。
- **x25**- X.25イベント通知を送信します。
- **xgcp** – 外部メディアゲートウェイコントロールプロトコル(XGCP)通知を送信します。

デフォルト

「 **snmp-server host** コマンドはデフォルトで無効になっています。通知は送信されません。

キーワードを付けずにこのコマンドを入力すると、デフォルトでは全トラップ タイプがホストに送信されます。

このホストには、インフォームは送信されません。ない場合 **version** キーワードが存在する場合、デフォルトはバージョン1です。「 **no snmp-server host** コマンドにキーワードを指定しないと、ホストに対するトラップは無効になりますが、インフォームは無効になりません。 **no snmp-server host informs** インフォームを無効にするコマンド。

注: *community-string* はIPv6アドレスを使用して **snmp-server community** このコマンドを使用する前に実行する必要があります。 **snmp-server community** コマンドが自動的に設定に挿入されます。パスワード (*community-string*) この自動設定に使用される **snmp-server community** は、CLIコマンドの **snmp-server host** コマンドが表示されない場合もあります。これは、Cisco IOS ソフトウェア リリース 12.0(3) 以降のデフォルト動作です。

コマンド モード

グローバル設定 : コマンド履歴

Cisco IOS ソフトウェア リリース 変更箇所

10.0

コマンドが導入されました。

12.0(3)T

次のキーワードが追加されました。

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

使用ガイドライン

SNMP 通知は、トラップまたはインフォーム要求として送信できます。このデバイスでトラップが受信されても受信側は確認応答を送信しないので、トラップの信頼性は高くありません。送信側は、トラップが受信されたかどうかを判断できません。しかし、SNMP エンティティはインフォーム要求を受信すると、SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット) によって要求に応答します。送信側が応答をまったく受け取っていないければ、インフォーム要求を再送信できます。このため、インフォームは、目的の宛先に到達できる可能性が高くなります。

ただし、インフォームは、エージェントやネットワークでより多くのリソースを消費します。トラップは、送信されると同時に破棄されますが、インフォーム要求の場合は、応答が受信されるか、要求時間がタイムアウトになるまでメモリ内に残る必要があります。トラップの送信回数は1回だけですが、インフォームは数回、繰り返し送信される場合があります。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因になります。

を入力しない場合、 `snmp-server host` コマンドを使用すると、通知は送信されません。SNMP通知を送信するようにルータを設定するには、少なくとも1つを入力する必要があります `snmp-server host` コマンドが表示されない場合もあります。キーワードを付けずにコマンドを入力すると、すべてのトラップタイプがホストで有効になります。

複数のホストを有効にするには、 `snmp-server host` コマンドを発行します。ホストごとに、コマンドで、複数の通知タイプを指定することができます。

複数の `snmp-server host` コマンドは同じホストと通知の種類 (`trap` または `inform`) に対して与えられ、各コマンドは前のコマンドを上書きします。最後の `snmp-server host` コマンドが考慮されます。たとえば、 `snmp-server host inform` コマンドをホストに対して発行し、別のホストを入力する `snmp-server host inform` コマンドを発行します。2番目のコマンドは最初のコマンドを置き換えます。

「 `snmp-server host` コマンドは、 `snmp-server enable` コマンドが表示されない場合もあります。 `snmp-server enable` コマンドを発行して、グローバルに送信するSNMP通知を指定します。ほとんどの通知をホストが受け取るには、少なくとも1つの `snmp-server enable` コマンドおよび `snmp-server host` コマンドを有効にする必要があります。

ただし、一部の通知タイプは、 `snmp-server enable` コマンドが表示されない場合もあります。たとえば、一部の通知タイプは常に有効です。また、 `snmp-server enable` 以外のコマンドで使用可能になる通知タイプもあります。たとえば、 `linkUpDown` 通知は、 `snmp trap link-status` コマンドが表示されない場合もあります。これらの通知タイプでは、 `snmp-server enable` コマンドが表示されない場合もあります。

使用可能な通知タイプのオプションは、ルータのタイプおよびルータ上でサポートされる Cisco IOS ソフトウェア機能により異なります。たとえば、 `envmon` 通知タイプは、環境モニタがシステムの一部である場合にのみ使用できます。

インフォームの設定

インフォームの送信を可能にするには、次の手順を実行します。

1. リモート エンジンの ID を設定する。
2. リモート ユーザを設定する。
3. リモート装置でグループを設定する。
4. リモート装置でトラップを使用可能にする。

5. SNMP マネージャを使用可能にする。

例

トラップに一意の SNMP コミュニティ スtring を設定する場合に、この String による SNMP ポーリング アクセスを防止するには、設定に access-list を含める必要があります。次の例では、コミュニティ String 名に「comaccess」を、アクセスリストには 10 をそれぞれ指定しています。

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

次の例では、名前 myhost.cisco.com で指定されたホストに SNMP トラップを送信します。コミュニティ String を comaccess と定義しています。

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

次の例では、SNMP および Cisco Enterprise に固有の環境モニタリングのトラップをアドレス 172.30.2.160 に送信しています。

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

次の例では、ルータが、コミュニティ String の public を使用して、ホストの myhost.cisco.com にすべてのトラップを送信できるようにします。

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

次の例では、どのホストにもトラップがまったく送信されません。BGP トラップはすべてのホストで送信可能にできますが、ISDN トラップだけは 1 つのホストにだけ送信できます。

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

次の例では、ルータがコミュニティ String public を使用してすべてのインフォーム要求をホスト myhost.cisco.com に送信できるようにします。

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

次の例では、名前 myhost.cisco.com で指定されたホストに HSRP SNMPv2c トラップを送信します。コミュニティ String を、public と定義しています。

```
snmp-server enable traps
```

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

「 snmp-server enable traps コマンド

snmp-server enable traps ルータがSNMPトラップを送信できるようにするためのグローバル設定コマンド。 no SNMP通知を無効にする形式です。

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

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

シンタックスの説明

(オプション) 使用可能な通知タイプ。タイプが指定されていない場合は、すべてのタイプが有効になります。

- aaa-server—AAA サーバ通知を送信します。このキーワードは、Cisco IOS ソフトウェアのバージョンによって異なります。
 - enterprise 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange
- bgp—BGP 状態変更通知を送信します。これはBGP4-MIBによるものであり、通知は次のとおりです。enterprise 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange
- calltracker – 新しいアクティブコールエントリがcctActiveTableに作成されるか、新しいエントリが削除されるか、または古いエントリが削除されるかを通知します。これはRFC2865-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification 2 cctCallTerminateNotification 3 cctCallClearNotification のとおりです。
- config—設定通知を送信します。これはCISCO-CONFIG-MAN-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.10.1.1 1 configChangeNotification のとおりです。
- dial – 成功したコールがクリアされるか、失敗したコール試行が最終的に失敗したかを通知します。これはRFC2865-MIBによるものであり、通知はenterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation 2 dialCtlPeerCallSetupNotification のとおりです。
- dlsw — DLSwエージェントから通知を送信します。 dlsw キーワードを使用する場合、通知はenterprise 1.3.6.1.4.1.9.10.1.1.1 1 ciscoDlswTrapTConnPartnerReject 2 ciscoDlswTrapTConnProtViolation 3 ciscoDlswTrapTConnPartnerJoin のとおりです。
- ds0-busyout— DS0インターフェイスのbusyoutの状態が変わるたびに通知を送信します。これはMGMT-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.10.19.2 1 cpmDS0Busyout のとおりです。
- ds1-loopback— DS1インターフェイスがループバックモードになるたびに通知を送信します。これはMGMT-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.10.19.2 2 cpmDS1Loopback のとおりです。
- dspu – 物理ユニット(PU)または論理ユニット(LU)の動作状態の変更やアクティブ化を通知します。これはRFC2865-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.10.19.2 3 cpmDSPU のとおりです。
- dsp- DSPカードがアップまたはダウンするたびに通知を送信します。これはCISCO-DSM-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.10.19.2 4 cpmDSP のとおりです。
- entity—エンティティ MIB の変更通知を送信します。これはENTITY-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.10.19.2 5 cpmEntity のとおりです。
- envmon – 環境のしきい値が設定値を超えたときに、Cisco Enterpriseに固有の環境監視通知を送信します。通知は次のとおりです。enterprise 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonShutdownNotification のとおりです。
- frame-relay—フレームリレー通知を送信します。これはRFC1315-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.10.19.2 6 cpmFrameRelay のとおりです。
- hsrp:Hot Standby Router Protocol(HSRP)通知を送信します。この機能は Cisco IOS Softwareのバージョンによって異なります。通知はenterprise 1.3.6.1.4.1.9.10.19.2 7 cpmHsrpStateChange のとおりです。
- isdn- ISDN通知を送信します。ユーザがisdnキーワードを使用する場合は、anotification-typeはenterprise 1.3.6.1.4.1.9.9.18.2 1 ciulflLoopStatusNotification のとおりです。そうでない場合は、anotification-typeはenterprise 1.3.6.1.4.1.9.9.18.2 2 ciulflLoopStatusNotification のとおりです。
- msdp—マルチキャスト ソース ディスカバリ プロトコル (MSDP) 通知を送信します。これはRFC2865-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.10.19.2 8 cpmMsdp のとおりです。
- repeater – イーサネットハブを送信しますrepeater通知。repeaterキーワードを選択する場合は、anotification-typeはenterprise 1.3.6.1.4.1.9.10.19.2 9 cpmRepeater のとおりです。そうでない場合は、anotification-typeはenterprise 1.3.6.1.4.1.9.10.19.2 10 cpmRepeater のとおりです。
- rsvp—Resource Reservation Protocol (RSVP; リソース予約プロトコル) 通知を送信します。これはRFC2865-MIBによるものであり、通知はenterprise 1.3.6.1.3.71.2 1 newFlow 2 lostFlow のとおりです。
- rtr—サービス保証エージェント RTR (RTR) 通知を送信します。これはCISCO-RTR-MIBによるものであり、通知はenterprise 1.3.6.1.4.1.9.10.19.2 11 rttMonThresholdNotification 4 rttMonVerifyErrorNotification のとおりです。
- snmp – 簡易ネットワーク管理プロトコル(SNMP)通知を送信します。ユーザがsnmp

notification-type

- 1.3.6.1.2.1.11 0 coldStart 2 linkDown 3 linkUp 4 authenticationFailure 5 egpNeighbor
- **syslog**—エラー メッセージ通知を送信します (Cisco Syslog MIB)。メッセージの
1.3.6.1.4.1.9.9.41.2 1 clogMessageGenerated
- **voice** – 低品質の音声通知を送信します。これはCISCO-VOICE-DIAL-CONTROL-MIB
- **xgcp** – 外部メディアゲートウェイコントロールプロトコル(XGCP)通知を送信します
(オプション)
 - **dls** [circuit | tconn]—ユーザが dls キーワードを使用すると、特定の通知タイプを有効に
使用できます。 circuit—DLSw 回線トラップを使用可能にします。 tconn—DLSw ピア
 - **envmon** [voltage | shutdown | supply | fan | temperature]—ユーザが envmon キーワードを使用すると、
通知が使用可能になります。 オプションとして、次のキーワードを 1 つ以上使用
 - **isdn** [call-information | isdn u-interface | chan-not-avail | layer2]—ユーザが isdn キーワードが使用
スMIBサブシステムのSNMP ISDN Uインターフェイス通知を有効にするキーワー
 - **repeater** [health | reset]—ユーザが repeater キーワードを使用すると、リピータオプション
Engineering Task Force(IETF)リピータハブMIB(RFC 1516)の状態通知を有効にし
ピータハブMIB(RFC 1516)の状態通知を有効にします。 reset- IETFリピータハブM
 - **snmp** [authentication | linkup | linkdown | coldstart] キーワード linkup | linkdown | coldstart Cisco I
い場合、すべての SNMP 通知タイプが使用可能になります (または no 形式を使用
プロトコル エンティティが、正式に認証されていないプロトコル メッセージの受
プしたことが、送信側のプロトコル エンティティで認識されたことを示します。 r
送信側のプロトコル エンティティで認識されたことを示します。 coldstart- SNMP col
ティが自身を再初期化することを示します。

notification-option

デフォルト

SNMP 通知は使用禁止です。

notification-type キーワードを指定せずにこのコマンドを入力すると、デフォルト設定により、このコマンドで制御できる全通知タイプが使用可能になります。

コマンド モード

グローバル設定 : コマンド履歴

Cisco IOS ソフトウェア
リリース

変更箇所

11.1

このコマンドが導入されました。

12.0(2)T

「rsvp キーワードが追加されました。

12.0(3)T

「hsrp キーワードが追加されました。

これらのキーワードは、 snmp-server enable traps snmp このコマンドの形式は次のとおりです。

- linkup
- linkdown
- coldstart

12.1(3)T

次の通知タイプのキーワードは、Cisco AS5300 プラットフォームに限定して追加されています。

- ds0-busyout
- isdn chan-not-avail
- modem-health

- ds1-loopback

次の通知タイプのキーワードは、Cisco AS5300 および AS5800 プラットフォームに限定して追加されています。

- aaa-server

使用ガイドライン

「 snmp-server enable traps snmp [linkup] [linkdown] このコマンドの形式は、 snmp trap link-status interface コンフィギュレーション モードのコマンドです。

「 no の形式 snmp-server enable traps コマンドは、ネットワーク上で不要な大量のノイズを生成する通知を無効にする場合に便利です。

SNMP 通知は、トラップまたはインフォーム要求として送信できます。このコマンドは、特定の通知タイプのトラップおよびインフォーム要求の両方を使用可能にします。

を入力しない場合、 snmp-server enable traps コマンドを使用すると、このコマンドによって制御される通知は送信されません。これらのSNMP通知を送信するようにルータを設定するには、少なくとも1つを入力する必要があります snmp-server enable traps コマンドが表示されない場合もあります。キーワードを指定せずにコマンドを入力すると、すべてのトラップ タイプが使用可能になります。キーワードを指定してコマンドを入力した場合は、そのキーワードに関連した通知タイプだけが使用可能になります。複数のタイプの通知を有効にするには、 snmp-server enable traps コマンドを発行します。

「 snmp-server enable traps コマンドは、 snmp-server host コマンドが表示されない場合もあります。 snmp-server host コマンドを使用して、SNMP通知を受信するホストを指定します。通知を送信するには、少なくとも1つを設定する必要があります snmp-server host コマンドが表示されない場合もあります。

このコマンドで制御される通知をホストが受信するには、 snmp-server enable traps コマンドおよび snmp-server host コマンドを有効にする必要があります。通知タイプがこのコマンドで制御されない場合は、該当するAPの snmp-server host コマンドを有効にする必要があります。

snmp-server enable traps コマンドで使用する通知タイプにはすべて、対応する MIB オブジェクトが設定されており、そのオブジェクトによって通知タイプは使用可能または使用禁止となります (たとえば、HSRPトラップは、HSRP MIB によって、リピータトラップの場合は、Repeater Hub MIB によってそれぞれ定義されます)。一部の通知タイプは snmp-server host コマンドには notificationEnable MIBオブジェクトが含まれているため、 snmp-server enable コマンドが表示されない場合もあります。

関連情報

- [シスコテクニカルサポートおよびダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。