CHAPTER 52

SNMP の設定

この章では、Catalyst 4500 シリーズ スイッチに Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を設定する方法を説明します。

この章の内容は、次のとおりです。

（注） ここで使用するコマンドの構文および使用方法の詳細については、次の URL にある『*Cisco IOS Configuration Fundamentals Command Reference*』

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html

および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

SNMP の概要

SNMP は、マネージャとエージェント間の通信にメッセージ形式を提供するアプリケーションレイヤ プロトコルです。SNMP は、SNMP マネージャ、SNMP エージェント、および Management Information Base（MIB; 管理情報ベース）で構成されています。SNMP マネージャは、Cisco Works などの NMS（Network Management System; ネットワーク管理システム）の一部になることができます。エージェントと MIB はスイッチに常駐します。スイッチに SNMP を設定するには、マネージャとエージェントの関係を定義する必要があります。

SNMP エージェントには、SNMP マネージャが値を要求または変更できる MIB 変数が含まれています。マネージャはエージェントから値を取得することも、エージェントに値を保存することもできます。エージェントは、デバイス パラメータおよびネットワーク データに関する情報のリポジトリである MIB からデータを収集します。エージェントは、マネージャの要求に応じてデータを取得または設定できます。

エージェントはマネージャに非送信請求トラップを送信できます。トラップとは、そのネットワークの状態を SNMP マネージャに通知するメッセージです。トラップには、間違ったユーザ認証、再起動、リンク状態（アップまたはダウン）、MAC アドレスの追跡、Transmission Control Protocol（TCP）接続の終了、ネイバーへの接続の消失、その他の重要なイベントがあります。

ここでは、次の内容について説明します。

SNMP のバージョン

Catalyst 4500 シリーズ スイッチは、次の SNMP バージョンをサポートします。

- SNMPv1 - 完全インターネット標準の SNMP で、RFC 1157 で定義されています。
- SNMPv2C - SNMPv2Classic のパーティベース管理およびセキュリティ フレームワークが SNMPv2C のコミュニティストリングベース管理フレームワークに置き換えられていますが、SNMPv2Classic のバルク検索は引き継がれ、エラー処理は改良されています。SNMPv2C には次の機能があります。
  - SNMPv2 - SNMP のバージョン 2 で、RFC 1902 ～ 1907 で定義されているドラフト インターネット標準です。
  - SNMPv2C - SNMPv2 のコミュニティストリングベース管理フレームワークで、RFC 1901 で定義されている実験的インターネット プロトコルです。
- SNMPv3 - SNMP のバージョン 3 で、RFC 2273 ～ 2275 で定義されている相互運用可能な標準ベースのプロトコルです。NMPv3 はネットワーク上のパケットを認証して暗号化することによってデバイスへのセキュアなアクセスを提供するプロトコルで、次のセキュリティ機能を持ちます。
  - メッセージ完全性 - 送信中にパケットが改ざんされないようにします。
  - 認証 - 有効な送信元からのメッセージであることを判断します。
  - 暗号化 - パッケージの内容を混ぜ合わせ、不正なソースによって読み取られることを防ぎます。

（注）　暗号化を選択するには、**priv** キーワードを入力します。このキーワードは、暗号（暗号化）ソフトウェア イメージがインストールされている場合にだけ指定できます。

SNMPv1 と SNMPv2C はどちらもコミュニティスベースのセキュリティ形式を使用します。エージェントの MIB にアクセスできるマネージャのコミュニティは、IP アドレス Access Control List（ACL; アクセス コントロール リスト）とパスワードによって定義されます。

SNMPv2C には、バルク検索メカニズムと、詳細なエラー メッセージを管理ステーションに報告する機能が備わっています。バルク検索メカニズムはテーブルおよび大量の情報を検索し、必要な往復回数を最小限に抑えます。SNMPv2C の改良されたエラー処理には多様なエラー状態を区別する拡張型エラー コードがあります。これらの状態は、SNMPv1 では 1 つのエラー コードで報告されます。SNMPv2C ではエラー戻りコードがエラーの種類を報告します。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザおよびユーザが存在するグループに設定された認証方法です。セキュリティ レベルは、セキュリティ モデルで許可されたセキュリティのレベルです。セキュリティ レベルとセキュリティ モデルの組み合わせにより、SNMP パケットを処理する場合に使用するセキュリティ メカニズムが決まります。利用可能なセキュリティ モデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

次の表に、セキュリティ モデルとセキュリティ レベルの各組み合わせの特性を示します。

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	不可	コミュニティ ストリングの照合を認証に使用
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	不可	コミュニティ ストリングの照合を認証に使用
SNMPv3	noAuthNoPriv	ユーザ名	不可	ユーザ名の照合を認証に使用
SNMPv3	authNoPriv	MD5 または SHA	不可	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を行う
SNMPv3	authPriv（暗号化ソフトウェア イメージが必要）	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を行う CBC-DES（DES-56）標準に基づく認証のほか、DES 56 ビット暗号化を行う

管理ステーションがサポートする SNMP バージョンを使用するには SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、ソフトウェアを設定して SNMPv1、SNMPv2C、および SNMPv3 プロトコルを使用する通信をサポートすることができます。

SNMP マネージャの機能

SNMP マネージャは MIB の情報を使用して、表 52-1 に示す動作を行います。

表 52-1　SNMP の動作

動作	説明
get-request	指定した変数の値を取得します。
get-next-request	テーブル内の変数の値を取得します。[1]
get-bulk-request[2]	テーブル内の複数行のような大きなデータ ブロックを取得します。多数の小さなデータ ブロックの送信が必要になります。
get-response	NMS が送信した get-request、get-next-request、および set-request に応答します。
set-request	指定した変数に値を保存します。
trap	イベント発生時に SNMP エージェントから SNMP マネージャに送信される割り込みメッセージ

1. この動作では、SNMP マネージャが正しい変数名を知る必要はありません。必要な変数が見つかるまでテーブル内でのシーケンシャルな検索が実行されます。
2. **get-bulk** コマンドは SNMPv2 以降でだけ動作します。

SNMP エージェントの機能

SNMP エージェントは、次のような SNMP マネージャ要求に応答します。

- MIB 変数の取得 - SNMP エージェントは、NMS の要求に応じてこの機能を開始します。エージェントは要求された MIB 変数の値を取得して NMS にその値を返します。
- MIB 変数の設定 - SNMP エージェントは、NMS のメッセージに応じてこの機能を開始します。SNMP エージェントは MIB 変数の値を NMS が要求する値に変更します。

SNMP エージェントは、重要なイベントがエージェントで発生したことを NMS に知らせる割り込みトラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウンになった場合、スパニングツリー トポロジが変更された場合、認証に失敗した場合などがありますが、これだけに限定されることはありません。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは MIB オブジェクトへのアクセスを認証し、埋め込みパスワードとして機能します。NMS がスイッチにアクセスできるためには、NMS のコミュニティ ストリング定義がスイッチに定義された 3 つのコミュニティ ストリングの少なくとも 1 つと一致する必要があります。

コミュニティ ストリングには次のいずれかのアトリビュートがあります。

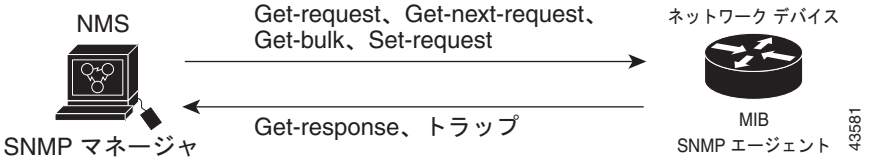
- Read-only（RO）- 認可された管理ステーションに、コミュニティ ストリングを除く MIB の全オブジェクトに対する読み取りアクセス権を与えますが、書き込みアクセス権は与えません。
- Read-write（RW）- 認可された管理ステーションに、MIB の全オブジェクトに対する読み取りおよび書き込みアクセス権を与えますが、コミュニティ ストリングへのアクセス権は与えません。
- Read-write-all - 認可された管理ステーションに、コミュニティ ストリングを含む MIB の全オブジェクトに対する読み取りおよび書き込みアクセス権を与えます。

SNMP を使用した MIB 変数へのアクセス

NMS の 1 つに CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 はスイッチ MIB 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスの特定の情報をポーリングします。ポーリングした結果をグラフなどで表示して分析し、インターネットワーキングのトラブルシューティング、ネットワーク パフォーマンスの向上、デバイスの設定確認、トラフィック負荷のモニタリングなどを行うことができます。

図 52-1 で示すように、SNMP エージェントは MIB のデータを収集します。エージェントは SNMP マネージャにトラップや特定イベントの通知を送信し、SNMP マネージャはトラップを受信して処理します。トラップは SNMP マネージャにネットワークの状態を通知します。不適切なユーザ認証、再起動、リンクの状態（アップまたはダウン）、MAC アドレスの追跡などが通知されます。SNMP エージェントは、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送信される MIB 関連のクエリーにも応答します。

図 52-1　SNMP ネットワーク



SNMP 通知

SNMP では、特定のイベントが発生した場合にスイッチから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、コマンドでトラップとインフォームのどちらかを任意で選択できない限り、*traps* キーワードは、トラップとインフォームのどちらか一方または両方を意味します。SNMP 通知をトラップまたはインフォームとして送信するには、**snmp-server host** コマンドを使用します。

（注）　SNMPv1 はインフォームをサポートしません。

受信側はトラップを受信しても acknowledgment（ACK; 確認応答）を送信しないのでトラップが受信されたかどうかを送信側で判断することができないため、トラップには信頼性があるとは言えません。SNMP マネージャが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）を使用してメッセージに確認応答します。送信側が応答を受信しなかった場合、インフォーム要求が再送信されます。このため、インフォームは、指定した宛先に到着する可能性がトラップよりも高くなります。

インフォームにはトラップよりも信頼性が高いという特性がありますが、より多くのスイッチおよびネットワークのリソースを消費します。送信後すぐに廃棄されるトラップとは異なり、インフォーム要求は、応答を受信するか要求期限が過ぎるまでメモリに保存されます。トラップは 1 回しか送信されませんが、インフォームは何度か再送信されます。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなります。このため、トラップとインフォームには信頼性とリソースの間で妥協が必要になります。SNMP マネージャがすべての通知を受け取ることが重要であれば、インフォーム要求を使用します。ネットワークのトラフィックやスイッチのメモリが問題であり通知が不要であれば、トラップを使用します。

SNMP の設定

ここでは、スイッチに SNMP を設定する方法を説明します。内容は次のとおりです。

SNMP のデフォルト設定

表 52-2 に、SNMP のデフォルト設定を示します。

表 52-2　SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	イネーブル
SNMP トラップ受信者	設定なし
SNMP トラップ	TCP 接続へのトラップ（**tty**）以外はイネーブルになっていません。
SNMP のバージョン	**version** キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを指定しない場合、デフォルトは **noauth**（noAuthNoPriv）セキュリティ レベル
SNMP 通知の種類	タイプが指定されていない場合、すべての通知が送信されます。

SNMP 設定時の注意事項

SNMP *group* は、SNMP ユーザを SNMP ビューにマッピングするテーブルです。SNMP *user* は、SNMP グループのメンバです。SNMP *host* は、SNMP トラップ動作の受信者です。SNMP *engine ID* は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP を設定する場合は、以下の注意事項に従ってください。

- SNMP グループを設定する場合、通知ビューを設定しないようにします。**snmp-server host** グローバル コンフィギュレーション コマンドはユーザの通知ビューを自動的に生成し、そのユーザに関連付けられているグループに追加します。グループの通知ビューを変更すると、そのグループに関連付けられているすべてのユーザが影響を受けます。通知ビューを設定するタイミングについては、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。
- リモート ユーザを設定するには、ユーザが存在するデバイスのリモート SNMP エージェントの IP アドレスまたはポート番号を指定します。
- 特定のエージェントにリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドに **remote** オプションを使用して SNMP エンジン ID を設定します。リモート エージェントの SNMP エンジン ID とユーザ パスワードは、認証およびプライバシー ダイジェストを計算するために使用されます。最初にリモート エンジン ID を設定しなかった場合、コンフィギュレーション コマンドは失敗します。
- SNMP インフォームを設定する場合、まず SNMP データベースにリモート エージェントの SNMP エンジン ID を設定し、それからプロキシ要求やインフォームを送信します。
- ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると大きな影響が発生します。ユーザのパスワード（コマンドラインで入力）は、パスワードとローカル エンジン ID に基づいて MD5 または SHA セキュリティ ダイジェストに変換されます。その後、RFC 2274 に従ってコマンドライン パスワードは破棄されます。このため、エンジン ID の値を変更すると SNMPv3 ユーザのセキュリティ ダイジェストが無効になり、**snmp-server user** *username* グローバル コンフィギュレーション コマンドを使用して SNMP ユーザを再設定しなければならなくなります。エンジン ID を変更した場合にも、同様の制約によってコミュニティ ストリングの再設定が必要になります。

SNMP エージェントのディセーブル化

SNMP エージェントをディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# no snmp-server`	SNMP エージェント動作をディセーブルにします。
ステップ 3	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Switch# show running-config`	入力を確認します。
ステップ 5	`Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

no snmp-server グローバル コンフィギュレーション コマンドは、デバイスで実行するすべてのバージョン（バージョン 1、バージョン 2C、およびバージョン 3）をディセーブルにします。SNMP をイネーブルにするための特別な IOS コマンドはありません。最初に **snmp-server** グローバル コンフィギュレーション コマンドを入力すると、SNMP の全バージョンがイネーブルになります。

コミュニティ ストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングは、スイッチのエージェントへのアクセスを許可するパスワードのように機能します。オプションとして、コミュニティ ストリングに関連付けられた次の特性のうち 1 つまたは複数を指定できます。

- エージェントへのアクセスを取得するためにコミュニティ ストリングを使用することを許可された SNMP マネージャの IP アドレスのアクセス リスト
- MIB ビュー。指定したコミュニティがアクセス可能なすべての MIB オブジェクトのサブセットを定義します。
- コミュニティがアクセス可能な MIB オブジェクトの読み取りおよび書き込み、または読み取りアクセス権

スイッチにコミュニティ ストリング設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# [no] snmp-server community string [view view-name] [ro | rw] [access-list-number]`	コミュニティ ストリングを設定します。 • *string* には、パスワードのように機能する、SNMP プロトコルへのアクセスを許可する文字列を設定します。最大 117 文字までの 1 つまたは複数のコミュニティ ストリングを設定できます。 • （任意）**view** には、コミュニティがアクセスできるビュー レコードを指定します。 • （任意）許可された管理ステーションに MIB オブジェクトを取得させる場合は読み取り（**ro**）を、許可された管理ステーションに MIB オブジェクトの取得を変更させる場合は読み取りおよび書き込み（**rw**）を指定します。デフォルトでは、コミュニティ ストリングは全オブジェクトに対する読み取りアクセスを許可します。 • （任意）*access-list-number* には、番号が 1 ～ 99 および 1300 ～ 1999 の IP 標準アクセス リストを入力します。 特定のコミュニティ ストリングを削除するには、**no snmp-server community** *string* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	`Switch(config)# access-list access-list-number {deny | permit} source [source-wildcard]`	（任意）ステップ 2 の IP 標準アクセスリストの番号を指定した場合、必要な回数だけコマンドを実行してリストを作成します。 • *access-list-number* には、ステップ 2 で指定したアクセス リストの番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、エージェントへのアクセスを取得するためにコミュニティ ストリングを使用することを許可されている SNMP マネージャの IP アドレスを指定します。 • （任意）*source-wildcard* には、送信元に適用するワイルド カード ビットをドット付き 10 進表記で指定します。無視するビットの位置に 1 を入力します。 アクセス リストは、すべてに対する黙示的な拒否（deny）文によって常に終了します。
ステップ 4	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Switch# show running-config`	入力を確認します。
ステップ 6	`Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

（注）　SNMP コミュニティへのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します（コミュニティ ストリングに値を入力しません）。

（注）　**snmp-server enable informs** コマンドはサポートされません。SNMP 応答要求型通知の送信をイネーブルにするには、**snmp-server enable traps** コマンドを **snmp-server host** *host-addr* **informs** コマンドとともに使用します。

次に、SNMP に文字列 *comaccess* を割り当てて読み取りアクセス権を設定し、IP アクセス リスト 4 でコミュニティ ストリングを使用してスイッチ SNMP エージェントへのアクセスを取得する例を示します。

```
Switch(config)# snmp-server community comaccess ro 4
```

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバ エンジンに ID 名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする SNMP サーバ グループを設定し、SNMP グループに新しいユーザを追加することができます。

スイッチに SNMP を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# snmp-server engineID {local engineid-string | remote ip-address [udp-port port-number] engineid-string}`	SNMP のローカル コピーまたはリモート コピーに名前を設定します。 • *engineid-string* は SNMP のコピー名を持つ 24 文字の ID 文字列です。末尾にゼロが続いている場合は、エンジン ID を 24 文字全部指定する必要はありません。エンジン ID の値がゼロばかりになるところまでを指定すれば十分です。たとえば、エンジン ID 123400000000000000000000 を設定するには、次のように入力します。 **snmp-server engineID local 1234** • **remote** を選択する場合、SNMP のリモート コピーを含むデバイスの *ip-address* と、任意でリモート デバイスの UDP ポートを指定します。デフォルト値は 162 です。

	コマンド	目的
ステップ 3	`Switch(config)# snmp-server group` *groupname* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	リモート デバイス上で新しい SNMP グループを設定します。 • *groupname* には、グループ名を指定します。 • 次のセキュリティ モデルを指定します。 – **v1** は、セキュリティが最も低いセキュリティ モデルです。 – **v2c** は、2 番めに低いセキュリティ モデルです。通常の 2 倍の幅でインフォームと整数を送信します。 – **v3** は、最もセキュアなセキュリティ モデルです。次の認証レベルを選択する必要があります。 **auth** - MD5 および Secure Hash Algorithm（SHA）パケット認証をイネーブルにします。 **noauth** - noAuthNoPriv セキュリティ レベル。キーワードが指定されていない場合は、これがデフォルトです。 **priv** - Data Encryption Standard（DES; データ暗号規格）パケット暗号化（*プライバシー*ともいう）をイネーブルにします。 **（注）** **priv** キーワードは、暗号イメージがインストールされている場合にだけ指定できます。 • （任意）**read** *readview* は、エージェントの内容が表示されるだけのビューの名前（64 文字以内の文字列）とともに指定します。 • （任意）**write** *writeview* は、データを入力しエージェントの内容を設定できるビューの名前（64 文字以内の文字列）とともに指定します。 • （任意）**notify** *notifyview* は、通知、インフォーム、トラップを指定できるビューの名前（64 文字以内の文字列）とともに指定します。 • （任意）**access** *access-list* は、アクセス リストの名前（64 文字以内の文字列）とともに指定します。
ステップ 4	`Switch(config)# snmp-server user` *username groupname* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} *auth-password*]} [**encrypted**] [**access** *access-list*]	SNMP グループに新しいユーザを設定します。 • *username* は、エージェントに接続するホストのユーザ名です。 • *groupname* は、ユーザが関連付けられるグループの名前です。 • （任意）**remote** を入力して、ユーザが所属するリモート SNMP エンティティと、そのエンティティのホスト名または IP アドレスを UDP ポート番号（任意）とともに指定します。デフォルト値は 162 です。 • SNMP バージョン番号を指定します（**v1**、**v2c**、または **v3**）。**v3** を指定した場合は、次のオプションも設定できます。 – **auth**。認証レベル設定セッションです。HMAC-MD5-96 と HMAC-SHA-96 のどちらかを指定でき、64 文字以内のパスワード文字列が必要です。 – **encrypted**。パスワードが暗号形式で表示されます。 • （任意）**access** *access-list* は、アクセス リストの名前（64 文字以内の文字列）とともに指定します。

	コマンド	目的
ステップ 5	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	`Switch# show running-config`	入力を確認します。
ステップ 7	`Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP 通知の設定

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップはシステムの警報で、特定のイベントが発生した場合にスイッチが生成します。デフォルトでは、トラップ マネージャは定義されておらず、トラップは送信されません。IOS Cisco IOS Release 12.2(31)SG 以降のリリースを実行するスイッチで使用できるトラップ マネージャの数には制限がありません。

（注）　コマンド構文で *traps* という単語を使用するコマンドは多数あります。トラップとインフォームのどちらかを選択するオプションがコマンドにない限り、*traps* キーワードは、トラップとインフォームのどちらか一方または両方を意味します。SNMP 通知をトラップまたはインフォームとして送信するには、**snmp-server host** コマンドを使用します。

表 52-3 に、サポートされるスイッチ トラップを示します（通知の種類）。これらのトラップの一部または全部をイネーブルにし、受信するためのトラップ マネージャを設定できます。

表 52-3　スイッチの通知の種類

通知の種類のキーワード	説明
bgp	BGP ステート変更トラップを生成します。 **（注）**　拡張マルチレイヤ イメージがインストールされている場合にだけ指定できます。
bridge	STP ブリッジ MIB トラップを生成します。
config	SNMP 設定変更に対するトラップを生成します。
config-copy	SNMP コピー設定変更に対するトラップを生成します。
cpu	CPU 関連トラップを許可します。
eigrp	EIGRP トラップをイネーブルにします。 **（注）**　拡張マルチレイヤ イメージがインストールされている場合にだけ指定できます。
entity	SNMP エンティティ変更に対するトラップを生成します。
envmon	環境モニタ トラップを生成します。環境トラップのファン、シャットダウン、電源装置、温度のいずれかまたはすべてをイネーブルにできます。
flash	SNMP FLASH 通知を生成します。
fru-ctrl	SNMP エンティティ FRU 制御トラップをイネーブルにします。
hsrp	Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）変更に対するトラップを生成します。
ipmulticast	IP マルチキャスト ルーティング変更に対するトラップを生成します。

表 52-3　スイッチの通知の種類 （続き）

通知の種類のキーワード	説明
isis	IS-IS トラップをネーブルにします。 （注）　拡張マルチレイヤ イメージがインストールされている場合にだけ指定できます。
mac-notification	MAC アドレス通知に対するトラップを生成します。
msdp	Multicast Source Discovery Protocol（MSDP）変更に対するトラップを生成します。 （注）　拡張マルチレイヤ イメージがインストールされている場合にだけ指定できます。
ospf	OSPF 変更に対するトラップを生成します。Cisco 固有、エラー、リンクステート アドバタイズメント、レート制限、再送信、およびステート変更のトラップのいずれかまたはすべてをイネーブルにできます。 （注）　拡張マルチレイヤ イメージがインストールされている場合にだけ指定できます。
pim	PIM 変更に対するトラップを生成します。無効 PIM メッセージ、ネイバー変更、Rendezvous Point（RP; ランデブー ポイント）マッピング変更のいずれかまたはすべてのトラップをイネーブルにできます。
port-security	SNMP ポート セキュリティ トラップを生成します。最大トラップ レートを秒単位で設定することもできます。範囲は 0 ～ 1000 で、デフォルトは 0（レート制限なし）です。
rf	Cisco-RF-MIB で定義したすべての SNMP トラップをイネーブルにします。
snmp	認証、コールド スタート、ウォーム スタート、リンク アップまたはリンクダウンの SNMP タイプの通知に対するトラップを生成します。
storm-control	SNMP ストーム制御に対するトラップを生成します。最大トラップ レートを秒単位で設定することもできます。範囲は 0 ～ 1000 で、デフォルトは 0（制限なし、発生するたびにトラップが送信される）です。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP Syslog トラップを生成します。
tty	TCP 接続に対するトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバシップ変更に対するトラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）変更に対するトラップを生成します。

特定のホストに **snmp-server host** グローバル コンフィギュレーション コマンドを使用して、表 52-3 に示した通知の種類を受信することができます。

ホストにトラップまたはインフォームを送信するようにスイッチを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# snmp-server engineID remote ip-address engineid-string`	リモート ホストのエンジン ID を指定します。
ステップ 3	`Switch(config)# snmp-server user username groupname remote host [udp-port port] {v1 | v2c | v3 [auth {md5 | sha} auth-password]} [encrypted] [access access-list]`	SNMP ユーザを設定し、ステップ 2 で作成したリモート ホストに関連付けます。 **（注）** リモート ユーザのアドレスを設定するには、最初にリモート ホストにエンジン ID を設定する必要があります。リモート エンジン ID を設定する前にユーザを設定しようとするとエラー メッセージが表示され、コマンドは実行されません。
ステップ 4	`Switch(config)# snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type]`	SNMP トラップ動作の受信先を指定します。 • *host-addr* には、ホスト（受信対象）の名前またはインターネット アドレスを指定します。 • （任意）**traps** を入力すると、ホストに SNMP トラップが送信されます（デフォルト）。 • （任意）**informs** を入力すると、ホストに SNMP インフォームが送信されます。 • （任意）SNMP **バージョン**（**1**、**2c**、または **3**）を指定します。SNMPv1 はインフォームをサポートしません。 • （任意）バージョン 3 の場合、認証レベル **auth**、**noauth**、または **priv** を選択します。 **（注）** **priv** キーワードは、暗号イメージがインストールされている場合にだけ指定できます。 • *community-string* には、通知動作とともに送信される、パスワードに似たコミュニティ ストリングを指定します。 • （任意）**udp-port** *port* には、リモート デバイス UDP ポートを指定します。 • （任意）*notification-type* には、表 52-3（P.52-11）に示すキーワードを指定します。タイプが指定されていない場合、すべての通知が送信されます。
ステップ 5	`Switch(config)# snmp-server enable traps notification-types`	スイッチでのトラップまたはインフォームの送信をイネーブルにし、送信する通知の種類を指定します。通知の種類については、表 52-3（P.52-11）を参照するか、**snmp-server enable traps ?** と入力します。 複数の種類のトラップをイネーブルにするには、トラップの種類ごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。
ステップ 6	`Switch(config)# snmp-server trap-source interface-id`	（任意）送信元インターフェイスを指定します。このインターフェイスによってトラップ メッセージの IP アドレスが提供されます。このコマンドはインフォームの送信元 IP アドレスも設定します。
ステップ 7	`Switch(config)# snmp-server queue-length length`	（任意）各トラップ ホストのメッセージ キューの長さを指定します。指定できる範囲は 1 ～ 1000 です。デフォルト値は 10 です。

	コマンド	目的
ステップ 8	Switch(config)# **snmp-server trap-timeout** *seconds*	（任意）トラップ メッセージを再送信する頻度を指定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 30 秒です。
ステップ 9	Switch(config)# **end**	特権 EXEC モードに戻ります。
ステップ 10	Switch# **show running-config**	入力を確認します。
ステップ 11	Switch# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

snmp-server host コマンドは、通知を受信するホストを指定します。**snmp-server enable trap** コマンドは、指定した通知（トラップおよびインフォーム）のメカニズムをグローバルにイネーブルにします。ホストにインフォームを受信させるには、ホストに **snmp-server host informs** コマンドを設定し、**snmp-server enable traps** コマンドを使用してインフォームをグローバルにイネーブルにする必要があります。

受信トラップから指定したホストを削除するには、**no snmp-server host** *host* グローバル コンフィギュレーション コマンドを使用します。キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。インフォームをディセーブルにするには、**no snmp-server host informs** グローバル コンフィギュレーション コマンドを使用します。特定の種類のトラップをディセーブルにするには、**no snmp-server enable traps** *notification-types* グローバル コンフィギュレーション コマンドを使用します。

エージェントの連絡先および設置場所の設定

システムの連絡先および SNMP エージェントの設置場所を設定してコンフィギュレーション ファイルを通じてアクセスできるようにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# **snmp-server contact** *text*	システムの連絡先の文字列を設定します。 次に例を示します。 **snmp-server contact Dial System Operator at beeper 21555.**
ステップ 3	Switch(config)# **snmp-server location** *text*	システムの設置場所の文字列を設定します。 次に例を示します。 **snmp-server location Building 3/Room 222**
ステップ 4	Switch(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	Switch# **show running-config**	入力を確認します。
ステップ 6	Switch# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP で使用する TFTP サーバの限定

SNMP を介したコンフィギュレーション ファイルの保存とロードに使用する TFTP サーバを、アクセス リストで指定したサーバに限定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# snmp-server tftp-server-list` *access-list-number*	SNMP を介したコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リストのサーバに限定します。 *access-list-number* には、1 ～ 99 および 1300 ～ 1999 の番号の IP 標準アクセス リストを入力します。
ステップ 3	`Switch(config)# access-list` *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リストの番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、スイッチにアクセスできる TFTP サーバの IP アドレスを指定します。 • （任意）*source-wildcard* には、送信元に適用するワイルド カード ビットをドット付き 10 進表記で指定します。無視するビットの位置に 1 を入力します。 アクセス リストは、すべてに対する黙示的な拒否（deny）文によって常に終了します。
ステップ 4	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Switch# show running-config`	入力を確認します。
ステップ 6	`Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP の例

次に、SNMP の全バージョンをイネーブルにする例を示します。コミュニティ ストリング *public* を使用して、SNMP マネージャからすべてのオブジェクトへの読み取りアクセスを許可します。この設定によりスイッチがトラップを送信することはありません。

```
Switch(config)# snmp-server community public
```

次に、コミュニティ ストリング *public* を使用して、SNMP マネージャからすべてのオブジェクトへの読み取りアクセスを許可する例を示します。スイッチはまた、SNMPv1 を使用した場合はホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用した場合はホスト 192.180.1.27 に、VTP トラップを送信します。コミュニティ ストリング *public* はトラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバに対してすべてのオブジェクトへの読み取りアクセスを許可する例を示します。他の SNMP マネージャはどのオブジェクトにもアクセスできません。SNMP Authentication Failure トラップは、コミュニティ ストリング *public* を使用して SNMPv2C によってホスト *cisco.com* に送信されます。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

次に、Entity MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは restricted です。最初の行では、それまでにイネーブルになったトラップのほかに Entity MIB トラップをスイッチで送信できるようにします。2 番めの行ではこれらのトラップの宛先が指定され、ホスト **cisco.com** についての以前の *snmp-server host* コマンドを上書きします。

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティ ストリング *public* を使用して、スイッチですべてのトラップをホスト *myhost.cisco.com* に送信できるようにする例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザをリモート ホストに関連付け、ユーザがグローバル コンフィギュレーション モードを開始したとき **auth**（authNoPriv）認証レベルのインフォームを送信する例を示します。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

SNMP ステータスの表示

SNMP の出入力統計情報を、不正なコミュニティ ストリング エントリの数、エラー、および要求された変数を含めて表示するには、**show snmp** 特権 EXEC コマンドを使用します。表 52-4 の他の特権 EXEC コマンドを使用して SNMP 情報を表示することもできます。出力のフィールドについては、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.4 を参照してください。

表 52-4　SNMP 情報の表示コマンド

機能	デフォルト設定
show snmp	SNMP 統計情報を表示します。
show snmp engineID	デバイスに設定されたローカル SNMP エンジンおよびすべてのリモート エンジンの情報を表示します。
show snmp group	ネットワークの各 SNMP グループの情報を表示します。
show snmp pending	保留中の SNMP 要求に関する情報を表示します。
show snmp sessions	現在の SNMP セッションに関する情報を表示します。
show snmp user	SNMP ユーザ テーブル内の SNMP ユーザ名別の情報を表示します。

（注）　**snmp-server enable informs** コマンドはサポートされません。SNMP 応答要求型通知の送信をイネーブルにするには、**snmp-server enable traps** コマンドを **snmp-server host** *host-addr* **informs** コマンドとともに使用します。