CHAPTER 60

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。

この章で説明する内容は、次のとおりです。

（注） この章で使用するスイッチ 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 で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』と関連資料を参照してください。

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

SNMP について

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 システムは、SNMP マネージャ、SNMP エージェント、および MIB（管理情報ベース）で構成されます。SNMP マネージャは、CiscoWorks などの Network Management System（NMS; ネットワーク管理システム）に統合できます。エージェントおよび 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します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイス パラメータやネットワーク データの保存場所である MIB から値を収集します。また、エージェントはマネージャからのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を 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、伝送制御プロトコル（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、次の情報について説明します。

SNMP 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：RFC1157 に規定された SNMP（完全インターネット標準）。
- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティ ベースの管理およびセキュリティ フレームワークをコミュニティ ストリング ベースの管理フレームワークに置き換えたものです。次の機能があります。
  - SNMPv2：RFC 1902 ～ 1907 に規定された SNMP バージョン 2（ドラフト版インターネット標準）。
  - SNMPv2C：RFC 1901 に規定された SNMPv2 のコミュニティ ストリング ベースの管理フレームワーク（試験版インターネット プロトコル）。
- SNMPv3：SNMP のバージョン 3 は、RFC 2273 ～ 2275 に規定されている相互運用可能な標準ベース プロトコルです。SNMPv3 は、ネットワーク上のパケットを認証、暗号化することでデバイスへのアクセスに対するセキュリティを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
  - メッセージの完全性：パケットが伝送中に改ざんされないようにします。
  - 認証：メッセージが有効な送信元からのものかどうかを判別します。
  - 暗号化：パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを防止します。

（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、ともにコミュニティベース形式のセキュリティを使用します。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が、IP アドレス アクセス コントロール リストおよび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が組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。バルク検索メカニズムは、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラー コードが使用されています。これらのエラーは、SNMPv1 では単一のエラー コードで報告されます。SNMPv2 では、エラー リターン コードでエラー タイプが報告されるようになりました。

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、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティ レベルは、セキュリティ モデル内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 パケットを扱うときに使用するセキュリティ メカニズムが決まります。使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	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv	ユーザ名	No	ユーザ名の照合を使用して認証します。
SNMPv3	authNoPriv	MD5 または SHA	No	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。
SNMPv3	authPriv 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いて認証します。 CBC-DES（DES-56）標準に基づいて認証する以外に、DES 56 ビット暗号化を行います。

管理ステーションでサポートされている 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 マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 60-1 に示す動作を実行します。

表 60-1　SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。[1]
get-bulk-request[2]	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要がある巨大なデータ ブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

1. この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。
2. **get-bulk** コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

SNMP エージェントは、次のようにして 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 からの要求に応答して、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、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、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 から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップ 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状態になった場合、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。

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 オブジェクトに対するアクセスを認証し、組み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するには、NMS のコミュニティ ストリング定義が、スイッチ上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致していなければなりません。

コミュニティ ストリングの属性は、次の 3 つのいずれかです。

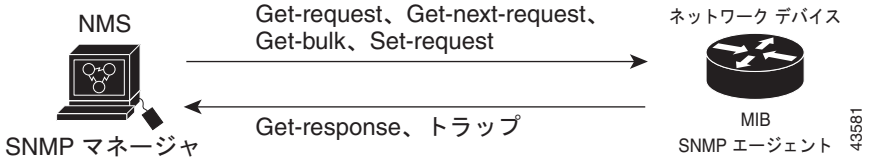
- Read-Only（RO）：許可された管理ステーションに、コミュニティ ストリングを除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- Read-Write（RW）：許可された管理ステーションに、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ ストリングに対するアクセスは許可しません。
- Read-write-all：認可された管理ステーションに、コミュニティ ストリングを含む MIB の全オブジェクトに対する読み取りおよび書き込みアクセス権を与えます。

SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフトウェアは、スイッチの 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をポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 60-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップ（特定イベントの通知）を送信でき、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、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス トラッキングなどの状況を SNMP マネージャに通知します。SNMP エージェントはさらに、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 関連のクエリーに応答します。

図 60-1　SNMP ネットワーク



SNMP 通知

SNMP を使用すると、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、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード *traps* はトラップ、情報、またはその両方を表します。**snmp-server host** コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

（注）　SNMPv1 は情報をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても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が送信側にわからないからです。情報要求の場合、受信した SNMP マネージャは SNMP 応答 Protocol Data Unit（PDU; プロトコル データ ユニット）でメッセージを確認します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、スイッチおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は 1 回限りですが、情報は数回にわたって再送信つまり再試行が可能です。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る原因になります。トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信することが重要な場合は、情報要求を使用してください。ネットワークまたはスイッチ メモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

SNMP の設定

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

SNMP のデフォルト設定

表 60-2 に、SNMP のデフォルト設定を示します。

表 60-2　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 レシーバ	未設定
SNMP トラップ	TCP 接続のトラップ（**tty**）以外は、イネーブルになりません。
SNMP 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	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで **noauth**（noAuthNoPriv）になります。
SNMP 通知タイプ	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 *グループ*は、SNMP ユーザを SNMP ビューに対応付けるテーブルです。SNMP *ユーザ*は、SNMP グループのメンバです。SNMP *ホスト*は、SNMP トラップ動作の受信側です。SNMP *エンジン 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ときは、通知ビューを指定しません。**snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザを対応す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、そのグループに対応付けられた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 ユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する 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のリモート 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 コマンドを **remote** オプションとともに使用して、SNMP エンジン ID を設定してください。リモート エージェントの SNMP エンジン ID およびユーザ パスワードを使用して認証およびプライバシー ダイジェストが算出されます。先にリモート エンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモート エージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- 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）の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、重大な影響が生じます。（コマンド ラインで入力された）ユーザのパスワードは、パスワードおよびローカル 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。コマンド ラインのパスワードは、RFC 2274 の規定に従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は SNMPv3 ユーザのセキュリティ ダイジェストが無効となり、**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 ユーザを再設定する必要がでてきます。エンジン ID を変更した場合は、同様の制限によってコミュニティ ストリングも再設定する必要があります。

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特定の Cisco IOS コマンドは存在しません。最初に入力する **snmp-server** グローバル コンフィギュレーション コマンドによって、SNMP のすべての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、スイッチ上のエージェントへのアクセスを許可するパスワードと同様に機能します。ストリングに対応する次の特性を 1 つまたは複数指定することもできます。

- コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

スイッチにコミュニティ ストリングを設定するには、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、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。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で MIB オブジェクトを取得する場合は読み取り専用（**ro**）、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き（**rw**）を指定します。デフォルトでは、コミュニティ ストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 • （任意）*access-list-number* には、1 ～ 99 および 1300 ～ 1999 の標準 IP アクセス リスト番号を入力します。 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、コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
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ないでください）。

（注）　**snmp-server enable informs** コマンドは使用できません。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、ストリング *comaccess* を SNMP に割り当てて読み取り専用アクセスを許可し、IP アクセス リスト 4 がこのコミュニティ ストリングを使用してスイッチの SNMP エージェントにアクセスできるように指定する例を示します。

```
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 エンジンを表す識別名（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、新規ユーザを SNMP グループに追加できます。

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 のコピー名を指定する 24 文字の ID ストリングです。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。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、グループを指定します。 • セキュリティ モデルを指定します。 – **v1** は、最も安全性の低いセキュリティ モデルです。 – **v2c** は、2 番めに安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を伝送できます。 – 最も安全な **v3** の場合、認証レベルを選択する必要があります。 **auth**：MD5 および SHA によるパケット認証が可能です。 **noauth**：noAuthNoPriv セキュリティ レベル。キーワードを指定しなかった場合、これがデフォルトです。 **priv**：DES によるパケット暗号化をイネーブルにします（*privacy* とも呼ばれます）。 （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* とともに、エージェントの内容を表示できるビューの名前を表すストリング（64 文字以下）を入力します。 • （任意）**write** *writeview* とともに、データを入力し、エージェントの内容を表示できるビューの名前を表すストリング（64 文字以下）を入力します。 • （任意）**notify** *notifyview* とともに、通知、情報、またはトラップを指定するビューの名前を表すストリング（64 文字以下）を入力します。 • （任意）**access** *access-list* とともに、アクセス リスト名のストリング（64 文字以下）を入力します。

	コマンド	目的
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でのユーザの名前です。 • *groupname* は、ユーザが対応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** を入力する場合は、次のオプションを追加します。 – **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** は、パスワードを暗号化形式で表示するように指定します。 • （任意）**access** *access-list* とともに、アクセス リスト名のストリング（64 文字以下）を入力します。
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、特定のイベントが発生したときにスイッチが生成するシステム アラートです。デフォルトでは、トラップ マネージャは定義されず、トラップは送信されません。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* というワード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かぎり、*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-server host** コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

表 60-3 に、サポートされているスイッチ トラップ（通知タイプ）を示します。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。

表 60-3　スイッチの通知タイプ

通知タイプのキーワード	説明
bgp	BGP ステート変更トラップを生成します。 （注）　このオプションは、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だけ使用できます。
bridge	スパニングツリー プロトコル（STP）ブリッジ MIB トラップを生成します。
config	SNMP 設定が変更された場合に、トラップを生成します。
config-copy	SNMP コピー設定が変更された場合に、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）　このオプションは、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だけ使用できます。
entity	SNMP エンティティが変更された場合に、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	ホットスタンバイ ルータ プロトコル（HSRP）が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャスト ルーティングが変更された場合に、トラップを生成します。
isis	IS-IS トラップをネーブルにします。 （注）　このオプションは、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だけ使用できます。
mac-notification	MAC アドレス通知のトラップを生成します。
msdp	Multicast Source Discovery Protocol（MSDP）が変更された場合に、トラップを生成します。 （注）　このオプションは、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だけ使用できます。
ospf	Open Shortest Path First（OSPF）が変更された場合に、トラップを生成します。シスコ固有、エラー、リンクステート アドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブルにできます。 （注）　このオプションは、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だけ使用できます。
pim	Protocol-Independent Multicast（PIM）が変更された場合に、トラップを生成します。無効な PIM メッセージ、ネイバー変更、およびランデブー ポイント（RP）マッピングの変更に関するトラップを任意に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。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。
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。

表 60-3　スイッチの通知タイプ （続き）

通知タイプのキーワード	説明
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 ダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 です。デフォルトは 0 に設定されています（制限なしの状態では、発生ごとにトラップが送信されます）。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP の Syslog トラップを生成します。
tty	TCP 接続の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 メンバーシップが変更された場合に、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）が変更された場合に、トラップを生成します。

表 60-3 に示す通知タイプを受信するには、特定のホストに対して **snmp-server host** グローバル コンフィギュレーション コマンドを実行します。

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）** アドレスに対応するリモート ユーザを設定するには、先にリモート ホストのエンジン ID を設定しておく必要があります。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。

	コマンド	目的
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（対象となる受信側）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）SNMP トラップをホストに送信するには、**traps**（デフォルト）を指定します。 • （任意）SNMP 情報をホストに送信するには、**informs** を指定します。 • （任意）SNMP **version**（**1**、**2c**、または **3**）を指定します。SNMPv1 は情報をサポートしていません。 • （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 60-3（P.60-12）に記載されているキーワードを使用します。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 60-3（P.60-12）を参照するか、または **snmp-server enable traps ?** と入力します。 複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **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。情報の送信元 IP アドレスも、このコマンドで設定します。
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。デフォルトは 10 です。
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 コマンドでは、通知を受信するホストを指定します。**snmp-server enable trap** コマンドによって、指定された通知（トラップおよび情報）のメカニズムがグローバルでイネーブルになります。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** 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。

指定したホストがトラップを受信しないようにするには、**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。情報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 コマンドを使用してください。特定のトラップ タイ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 コンタクトおよびロケーションの設定

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 ファイルを使用し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*	システムの場所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 を通して使用する TFTP サーバの制限

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 の標準 IP アクセス リスト番号を入力します。

	コマンド	目的
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 アドレスを入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 **（注）** アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
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。この設定では、任意の SNMP マネージャがコミュニティ ストリング public を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、スイッチはトラップを送信しません。

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

次に、任意の SNMP マネージャがコミュニティ ストリング public を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。スイッチは、ホスト 192.180.1.111 および 192.180.1.33（SNMPv1 を使用）や、ホスト 192.180.1.27（SNMPv2C を使用）へ 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、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の 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 認証障害トラップは、SNMPv2C がコミュニティ ストリング public を使用してホスト cisco.com に送信します。

```
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、エンティティ 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 ストリングは制限されます。先頭行は、すでにイネーブルに設定されているトラップに加えて、エンティティ MIB トラップを送信するようにスイッチをイネーブルにします。2 行目はこれらのトラップの宛先を指定し、ホスト **cisco.com** に対する以前の snmp-server host コマンドを無効にします。

```
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、すべてのトラップをホスト myhost.cisco.com に送信するようにスイッチをイネーブル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、ユーザとリモート ホストを関連付けて、グローバル コンフィギュレーション モードのときに **auth**（authNoPriv）認証レベルで情報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 60-4 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 60-4　SNMP 情報を表示するためのコマンド

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ているローカル SNMP エンジンおよびすべてのリモート エンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。

（注）　**snmp-server enable informs** コマンドは使用できません。SNMP インフォーム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。