



SNMP の設定

この章では、Catalyst 3550 スイッチに SNMP (簡易ネットワーク管理プロトコル) を設定する方法について説明します。



(注)

この章で使用されるコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチのコマンドリファレンス、および『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.2 を参照してください。

この章で説明する内容は、次のとおりです。

- [SNMP の概要 \(p.27-2\)](#)
- [SNMP の設定 \(p.27-7\)](#)
- [SNMP ステータスの表示 \(p.27-19\)](#)

SNMP の概要

SNMP はアプリケーション レイヤ プロトコルで、マネージャとエージェント間の通信用メッセージ形式を規定します。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) の一部に組み入れることができます。エージェントおよび MIB はスイッチで動作します。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間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保管したりもできます。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保管場所である MIB からデータを収集します。また、エージェントはマネージャから要求されるデータ取得または設定に対応します。

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します。トラップとは、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。トラップは、不正なユーザ認証、再起動、リンクのステータス (アップまたはダウン)、MAC (メディア アクセス制御) アドレス追跡、TCP 接続の切断、またはネイバとの接続の切断、その他の重要なイベントを表示します。

ここでは、次の内容について説明します。

- [SNMP のバージョン \(p.27-2\)](#)
- [SNMP マネージャの機能 \(p.27-4\)](#)
- [SNMP エージェントの機能 \(p.27-4\)](#)
- [SNMP コミュニティ スtring \(p.27-4\)](#)
- [SNMP による MIB 変数へのアクセス \(p.27-5\)](#)
- [SNMP 通知 \(p.27-5\)](#)
- [SNMP ifIndex MIB オブジェクト値 \(p.27-6\)](#)

SNMP のバージョン

このソフトウェア リリースでは、次の SNMP バージョンをサポートしています。

- SNMPv1 簡易ネットワーク管理プロトコル、完全インターネット標準 (RFC 1157 に定義)
- SNMPv2C は、SNMPv2Classic のパーティベース管理およびセキュリティ フレームワークを SNMPv2C のコミュニティ スtring ベース管理フレームワークに置き換えるもので、SNMPv2Classic の一括検索を保持しながら、エラー処理が改良されています。SNMPv2C の機能は次のとおりです。
 - SNMPv2 SNMP のバージョン 2、インターネット標準草案 (RFC1902 ~ 1907 に定義)
 - SNMPv2C SNMPv2 に対応するコミュニティ スtring ベース管理フレームワーク、実験的インターネット プロトコル (RFC 1901 に定義)
- SNMPv3 SNMP のバージョン 3 は、RFC 2273 ~ 2275 に定義された相互運用可能な標準ベース プロトコルです。SNMPv3 はネットワーク経由でパケットの認証および暗号化を行い、デバイスへの安全なアクセスを実現します。以下のセキュリティ機能が組み込まれています。
 - メッセージ整合性 パケットが送信中に不正に変更されないようにします。
 - 認証 メッセージの送信元が有効かどうかを判別します。
 - 暗号化 パッケージの内容をスクランブルし、不正送信元に読みとられないようにします。



(注) 暗号化を選択する場合は、**priv** キーワードを指定します。このキーワードは、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のみ使用できます。

SNMPv1 と SNMPv2C は、共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は、IP アドレスのアクセス制御リストとパスワードによって定義されています。

SNMPv2C には、一括検索メカニズムと管理ステーションへのより詳細なエラー メッセージ報告機能が組み込まれています。一括検索メカニズムは表や大量の情報を検索し、必要なラウンドトリップ数を最小限にします。SNMPv2C の改良されたエラー処理には、各種のエラー状況を区別する拡張エラー コードが組み込まれています。エラー状況は、SNMPv1 の単一のエラー コードを使用して報告されます。SNMPv2C のエラー リターン コードが、エラー タイプを報告します。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を備えています。セキュリティ モデルは、ユーザおよびそのユーザが所属するグループに対して設定する認証方法です。セキュリティ レベルは、1 つのセキュリティ モデルの中で許可されるセキュリティのレベルを表します。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットを処理するとき使用するセキュリティ メカニズムが決まります。使用可能なモデルは SNMPv1、SNMPv2C、および SNMPv3 です。

表 27-1 に、セキュリティ モデルおよびセキュリティ レベルをさまざまに組み合わせた場合の特性を示します。

表 27-1 SNMP セキュリティ モデルおよびレベル

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	なし	認証にコミュニティ ストリングの照合を使用します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	なし	認証にコミュニティ ストリングの照合を使用します。
SNMPv3	noAuthNoPriv	ユーザ名	なし	認証にユーザ名の照合を使用します。
SNMPv3	authNoPriv	MD5 または SHA	なし	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行います。
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いて認証を行います。 CBC-DES(DES-56)標準に基づく認証以外に DES 56 ビット暗号化を行います。

管理ステーションがサポートする SNMP の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、SNMPv1、SNMPv2C、または SNMPv3 を使用した通信をサポートするようにソフトウェアを設定できます。

SNMP マネージャの機能

SNMP マネージャは MIB 情報を使用し、表 27-2 に示す動作を実行します。

表 27-2 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	テーブルの複数行など、データの大きなブロックを取得します。データの小さなブロックを何回も送信する必要はありません。
get-response	NMS から送られる get-request、get-next-request、および set-request に応答します。
set-request	特定の変数に値を格納します。
trap	イベントの発生時に、SNMP エージェントから SNMP マネージャに送られる、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、必要な変数を検出します。
2. get-bulk コマンドが機能するのは SNMPv2 以降に限定されます。

SNMP エージェントの機能

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

- 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、その値で 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。

また、SNMP エージェントは非送信請求トラップメッセージを送信し、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起動または停止した場合、スパンニングツリートポロジの変更が発生した場合、認証障害が発生した場合などがあります。

SNMP コミュニティ スtring

SNMP コミュニティ スtring は MIB オブジェクトへのアクセスを認証し、内蔵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 上のコミュニティ スtring の定義が、スイッチの 3 つのコミュニティ スtring の定義と最低限 1 つ一致する必要があります。

コミュニティ スtring は、次のいずれかの属性を持ちます。

- read-only (RO) 許可した管理ステーションに、コミュニティ スtring を除く MIB 内のオブジェクトすべてに対する読み取りアクセス権を与えます。ただし、書き込みアクセスは許可しません。
- read-write (RW) 許可した管理ステーションに、MIB 内のオブジェクトすべて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。ただし、コミュニティ スtring へのアクセスは許可しません。



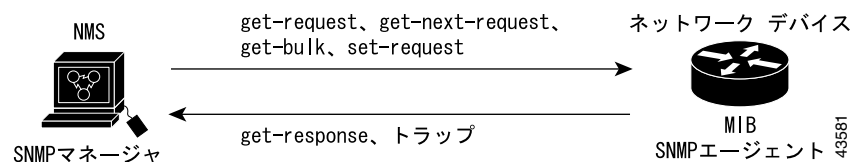
(注) クラスタを作成すると、コマンド スイッチがメンバー スイッチと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンド スイッチで最初に設定された RW および RO コミュニティ スtring にメンバー スイッチ番号 (@esN、N はスイッチ番号) を追加し、これらの String をメンバー スイッチに伝播します。詳細については、第 5 章「スイッチのクラスタ設定」および Cisco.com の『Getting Started with Cisco Network Assistant』を参照してください。

SNMP による MIB 変数へのアクセス

NMS の一例は、CiscoWorks ネットワーク管理ソフトウェアです。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の変数を設定し、ネットワーク上のデバイスに対するポーリングを実行して特定の情報を入手します。ポーリング結果は、グラフ形式で表示されます。この結果を分析して、インターネットワーキングに関する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、デバイスの設定の確認、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 27-1 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 マネージャに対してトラップ (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それを処理します。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 アドレス追跡などに関する条件を 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*、*set-request* 形式で送られる MIB 関連のクエリに応答します。

図 27-1 SNMP ネットワーク



サポートされている MIB とそのアクセス方法については、付録 A「サポートされている MIB」を参照してください。

SNMP 通知

SNMP を使用し、スイッチは特定のイベントが発生したときに SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたはインフォーム要求として送信されます。コマンド構文内に、トラップまたはインフォームを選択するオプションが指定されていない場合、キーワード *traps* はトラップまたはインフォーム、またはその両方を表します。SNMP 通知をトラップまたはインフォームのどちらで送信するかを指定するには、*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ていません。

レシーバーはトラップの受信時に確認応答を送信しないため、トラップは信頼性が低く、送信側はトラップが受信されたかどうかを判別できません。SNMP マネージャ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) を使用してメッセージを確認します。送信側が応答を受信しない場合は、インフォーム要求を再送信します。このため、インフォームの方がトラップよりも目的の宛先に到達する可能性が高くなります。

インフォームはトラップよりも信頼性が高いため、スイッチおよびネットワーク内のリソースの消費量も多くなります。送信後すぐに廃棄されるトラップと異なり、インフォーム要求は応答が受信されるか、または要求が時間切れ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、インフォームは何回も再送信されたり、再試行されることがあります。再試行が繰り返され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大きくなるため、トラップおよびインフォームには信頼性とリソースのバランスが必要となります。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インフォーム要求を使用し、ネットワークトラフィックまたはスイッチのメモリが重要で、通知が必要ない場合は、トラップを使用します。

SNMP ifIndex MIB オブジェクト値

NMS では、IF-MIB はインターフェイス インデックス (ifIndex) のオブジェクト値を生成および割り当てます。オブジェクト値は物理または論理インターフェイスを識別し、ゼロより大きい一意の識別番号です。スイッチが再起動する、またはスイッチのソフトウェアがアップグレードされるとき、スイッチはインターフェイスに同じ値を使用します。たとえば、ポート 2 に ifIndex 値 10003 を割り当てた場合、スイッチが再起動したあとでもこの値は同じです。

スイッチ上で ifindex の持続性をイネーブルにするには、`snmp-server ifindex persist` 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。

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。具体的な設定情報は次のとおりです。

- [SNMP のデフォルト設定 \(p.27-7\)](#)
- [SNMP 設定時の注意事項 \(p.27-7\)](#)
- [SNMP エージェントのディセーブル化 \(p.27-8\)](#)
- [コミュニティ スtring の設定 \(p.27-9\)](#)
- [SNMP グループおよびユーザの設定 \(p.27-10\)](#)
- [SNMP 通知の設定 \(p.27-12\)](#)
- [SNMP トラップ通知プライオリティの設定 \(p.27-15\)](#)
- [エージェント コンタクトおよびロケーション情報の設定 \(p.27-16\)](#)
- [SNMP 経由で使用する TFTP サーバの制限 \(p.27-17\)](#)
- [SNMP の例 \(p.27-18\)](#)

SNMP のデフォルト設定

表 27-3 に、SNMP のデフォルト設定を示します。

表 27-3 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	ディセーブル ¹
SNMP コミュニティ スtring	Read-Only : パブリック Read-Write : プライベート
SNMP トラップ レシーバー	設定なし
SNMP トラップ	TCP 接続のトラップ (tty) 以外はイネーブルなし
SNMP バージョン	version キーワードを指定しない場合、デフォルトはバージョン 1 です。
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 レベルです。
SNMP 通知トラップ	タイプを指定しない場合、すべての通知が送信されます。

1. スイッチ起動時およびスタートアップ コンフィギュレーションに `snmp-server` グローバル コンフィギュレーション コマンドがない場合、この設定がデフォルトになります。

SNMP 設定時の注意事項

スイッチの起動時、スタートアップ コンフィギュレーションに `snmp-server` グローバル コンフィギュレーション コマンドが最低 1 つでもあれば、SNMP エージェントはイネーブルになります。

SNMP グループは、SNMP ユーザを SNMP ビューにマッピングするテーブルです。SNMP ユーザは、SNMP グループのメンバーです。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 を設定する場合の注意事項は、次のとおりです。

- SNMP グループを設定する場合は、通知ビューを指定しないでください。snmp-server host グローバル コンフィギュレーション コマンドを使用すると、ユーザ用の通知ビューが自動生成され、そのユーザに関連付けられたグループに追加されます。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たすべてのユーザに影響を与えます。通知ビューを設定する時期については、『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、ユーザが属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 `remote` オプションを指定し、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。リモート エンジン ID を先に設定しないと、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は、SNMP データベース内のリモート エージェントの SNMP エンジン ID を設定してから、プロキシ要求またはインフォームを送信する必要があります。
- ローカル ユーザがリモート ホストと関連していない場合、スイッチはインフォームを `auth` (`authNoPriv`) および `priv` (`authPriv`) 認証レベル用に送信しません。
- SNMP エンジン ID の値を変更すると、重大な悪影響を及ぼします。ユーザのパスワード (コマンドラインに入力したパスワード) が、パスワードおよびローカル エンジン ID に基づいて Message Digest 5 (MD5) または Secure Hash Algorithm (SHA) セキュリティ ダイジェストに変換されます。そのあと、RFC 2274 の規定によりコマンドラインのパスワードは廃棄されます。この廃棄によってエンジン ID の値が変化した場合、SNMPv3 ユーザのセキュリティ ダイジェストは無効になるため、ユーザは `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あります。同様に、エンジン ID が変化した場合は、コミュニティ スtring を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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>no snmp-server</code>	SNMP エージェントの動作をディセーブルにします。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(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、デバイス上で実行されてい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 コマンドはありません。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tring の設定

SNMP マネージャとエージェント間の関係を定義するには、SNMP コミュニティ スtring を使用します。コミュニティ スtring はパスワードと同様に機能し、スイッチのエージェントへのアクセスを許可します。任意で、スString に関連付けられた次の特性を 1 つまたは複数指定できます。

- エージェントへアクセスするコミュニティ スString の使用が許可されている、SNMP マネージャの IP アドレスに関するアクセス リスト
- MIB ビュー。指定のコミュニティ がアクセス可能な全 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権限、または読み取り専用権限

スイッチでコミュニティ スString を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>snmp-server community string [view view-name] [ro rw] [access-list-number]</code>	<p>コミュニティ スString を設定します。</p> <ul style="list-style-type: none"> • <i>string</i> には、パスワードのように機能し、SNMP プロトコルへのアクセスを許可するスString を指定します。任意の文字数で、1 つまたは複数のコミュニティ スString を設定できます。 • (任意) <i>view</i> には、コミュニティ がアクセス可能なビュー レコードを指定します。 • (任意) 許可した管理ステーションに MIB オブジェクトを検索させる場合は読み取り専用 (<i>ro</i>)、MIB オブジェクトを検索して変更させる場合は読み取り / 書き込み (<i>rw</i>) を指定します。デフォルトでは、コミュニティ スString は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します。 • (任意) <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の範囲で標準の IP アクセス リスト番号を入力します。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>(任意) ステップ 2 で標準の IP アクセス リスト番号を指定した場合はリストを作成し、必要な回数だけこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> を指定する場合は、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。 • <i>deny</i> キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。<i>permit</i> キーワードを指定すると、条件が一致した場合にアクセスが許可されます。 • <i>source</i> には、エージェントへアクセスするコミュニティ スString の使用が許可されている SNMP マネージャの IP アドレスを入力します。 • (任意) <i>source-wildcard</i> を指定する場合は、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 進表記で入力します。無視するビット位置に 1 を入力します。 <p>アクセス リストの末尾には、すべてに適用される暗黙的な拒否ステートメントが常に存在する点に注意してください。</p>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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、そのコミュニティに対するコミュニティ スtring をヌル スtring に設定します (コミュニティ スtring の値は入力しません)。

特定のコミュニティ スtring 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。

次に、SNMP にス String `comaccess` を割り当て読み取り専用アクセスを許可し、IP アクセス リスト 4 がコミュニティ ス String を使用してスイッチの SNMP エージェントにアクセスするよう指定する方法を示します。


```
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、識別名 (`engineID`) 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 グループに新規ユーザを追加できます。

スイッチで SNMP を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>snmp-server engineID {local engineid-string remote ip-address [udp-port port-number] engineid-string}</code>	SNMP のローカル コピーまたはリモート コピーのいずれかの名前を設定します。 <ul style="list-style-type: none"> <code>engineid-string</code> は、SNMP のコピー名を含む 24 文字の ID スtring です。後続の値が 0 の場合、エンジン ID に 24 文字すべてを指定する必要はありません。後続値がすべて 0 となる位置まで、エンジン ID の一部を指定します。たとえば、123400000000000000000000 のエンジン ID を設定する場合は、<code>snmp-server engineID local 1234</code> と入力します。 <code>remote</code> を選択した場合は、SNMP のリモート コピーが格納されたデバイスの <code>ip-address</code>、およびリモート デバイス上のオプションの UDP ポートを指定します。デフォルト値は 162 です。

コマンド	説明
ステップ 3 <code>snmp-server group groupname {v1 v2c v3 {auth noauth priv}} [read readview] [write writeview] [notify notifyview] [access access-list]</code>	<p>リモート デバイスに新規の SNMP グループを設定します。</p> <ul style="list-style-type: none"> • <code>groupname</code> には、グループ名を指定します。 • セキュリティ モデルを指定します。 <ul style="list-style-type: none"> - <code>v1</code> は、使用可能なセキュリティ モデルのうち、安全性が最も低いモデルです。 - <code>v2c</code> は、2 番めに安全性が低いモデルです。このモデルを使用すると、インフォームおよび整数を標準の 2 倍の幅で伝送できます。 - <code>v3</code> は最も安全性が高いモデルで、認証レベルを選択する必要があります。 <p>auth MD5 および SHA パケット認証をイネーブルにします。</p> <p>noauth <code>noAuthNoPriv</code> セキュリティ レベルをイネーブルにします。キーワードを指定しない場合は、このレベルがデフォルトです。</p> <p>priv Data Encryption Standard (DES) パケット暗号化 (別名 <i>プライバシ</i>) をイネーブルにします。</p> <p> (注) priv キーワードは、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のみ使用できます。</p> <ul style="list-style-type: none"> • (任意) read <code>readview</code> には、エージェントの内容表示のみが可能なビューの名前を示すストリング (64 文字以下) を指定して、入力します。 • (任意) write <code>writeview</code> には、データを入力してエージェントの内容を設定するビューの名前を示すストリング (64 文字以下) を指定して、入力します。 • (任意) notify <code>notifyview</code> には、通知、インフォーム、またはトラップを指定するビューの名前を示すストリング (64 文字以下) を指定して、入力します。 • (任意) access <code>access-list</code> には、アクセス リストの名前を示すストリング (64 文字以下) を指定して、入力します。

	コマンド	説明
ステップ 4	<code>snmp-server user username groupname {remote host [udp-port port]} {v1 [access access-list] v2c [access access-list] v3 [encrypted] [access access-list] [auth {md5 sha} auth-password]}</code>	SNMP グループに新規ユーザを設定します。 <ul style="list-style-type: none"> <code>username</code> は、エージェントに接続されたホスト上のユーザ名です。 <code>groupname</code> は、ユーザが関連付けられているグループの名前です。 ユーザが属するリモート SNMP エンティティおよびホスト名を指定する場合は、<code>remote</code> を入力します。このエンティティの IP アドレスを指定する場合は、さらにオプションの UDP ポート番号を指定します。デフォルト値は 162 です。 SNMP バージョン番号 (<code>v1</code>、<code>v2c</code>、または <code>v3</code>) を入力します。<code>v3</code> を入力する場合は、次のオプションを使用します。 <ul style="list-style-type: none"> <code>encrypted</code> パスワードが暗号化形式で表示されるように指定します。このキーワードは、<code>v3</code> キーワードが指定されている場合のみ使用できます。 <code>auth</code> 認証レベル設定セッションです。HMAC-MD5-96(<code>md5</code>)または HMAC-SHA-96(<code>sha</code>) 認証レベルのいずれかを指定でき、パスワード ストリング (64 文字以下) が必要となります。 (任意) <code>access access-list</code> には、アクセス リストの名前を示すストリング (64 文字以下) を指定して、入力します。
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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場合に、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 マネージャが定義されていないため、トラップは送信されません。この Cisco IOS リリースが稼働するスイッチでは、無制限にトラップ マネージャを設定できます。



(注) 多くのコマンドは、コマンド構文内でワード `traps` を使用します。トラップまたはインフォームを選択するオプションがコマンド内に指定されていない場合、キーワード `traps` はトラップまたはインフォーム、あるいはその両方を表します。SNMP 通知をトラップまたはインフォームのどちらで送信するかを指定するには、`snmp-server host` グローバル コンフィギュレーション コマンドを使用します。



表 27-4 に、サポートされているスイッチのトラップ (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、トラップ マネージャがトラップを受信するように設定できます。

表 27-4 スイッチの通知タイプ

通知タイプのキーワード	説明
bgp	Border Gateway Protocol (BGP) ステート変更トラップ。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のみ使用できます。
bridge	SpanningTree Protocol (STP; スパニングツリー プロトコル) ブリッジ MIB トラップを生成します。
cluster	クラスタ設定の変更時にトラップを生成します。
config	SNMP 設定の変更時にトラップを生成します。
copy-config	SNMP コピー設定の変更時にトラップを生成します。
entity	SNMP エンティティの変更時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 (ファン、シャットダウン、供給、温度) の一部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。
hsrp	Hot Standby Router Protocol (HSRP) の変更時にトラップを生成します。
ipmulticast	IP マルチキャスト ルーティングの変更時にトラップを生成します。
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) の変更時にトラップを生成します。
ospf	Open Shortest Path First (OSPF) の変更時にトラップを生成します。シスコ固有、エラー、Link-State Advertisement (LSA; リンクステート アドバタイズ)、速度制限、再送信、ステートの変更のトラップの一部またはすべてをイネーブルにできます。
pim	Protocol-Independent Multicast (PIM) の変更時にトラップを生成します。無効な PIM メッセージ、ネイバの変更、ランデブー ポイント (RP) マッピングの変更のトラップの一部またはすべて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 レートも設定できます (秒)。指定できる範囲は 0 ~ 1000 です。デフォルト設定は 0 (レート制限なし) です。
rtr	SNMP Response Time Reporter (RTR) に対してトラップを生成します。
snmp	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。最大トラップ レートも設定できます (秒)。指定できる範囲は 0 ~ 1000 です。デフォルト値は 0 です (制限がなく、トラップはすべての発生時に送信されます)。
stpx	SNMP STP Extended 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 接続に対して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。
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。
vlan-membership	SNMP VLAN (仮想 LAN) メンバーシップの変更時に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) の変更時にトラップを生成します。

表 27-4 に示す通知タイプを受信する場合は、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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>snmp-server engineID remote ip-address engineid-string</code>	リモート ホストのエンジン ID を指定します。
ステップ 3	<code>snmp-server user username groupname {remote host [udp-port port]} {v1 [access access-list] v2c [access access-list] v3 [encrypted] [access access-list] [auth {md5 sha} auth-password]}</code>	<p>ステップ 2 で作成したりモート ホストに対応する SNMP ユーザを設定します。</p> <p> (注) アドレスに対してリモート ユーザを設定する場合は、最初にそのリモート ホストのエンジン ID を設定する必要があります。設定しないとエラー メッセージが表示され、コマンドは実行されません。</p>
ステップ 4	<code>snmp-server group [groupname {v1 v2c v3 {auth noauth priv}}] [read readview] [write writeview] [notify notifyview] [access access-list]</code>	SNMP グループを設定します。
ステップ 5	<code>snmp-server host host-addr [informs traps] [version {1 2c 3 {auth noauth priv}}] community-string [notification-type]</code>	<p>SNMP トラップ操作の受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、ホスト (対象となる受信デバイス) 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 インフォームをホストに送信する場合は、<code>informs</code> を入力します。 (任意) SNMP トラップをホストに送信する場合は、<code>traps</code> (デフォルト) を入力します。 (任意) SNMP <code>version</code> (1、2c、または 3) を指定します。SNMPv1 では、インフォームを使用できません。 (任意)バージョン 3 の場合は、認証レベル (<code>auth</code>、<code>noauth</code>、または <code>priv</code>) を選択します。 <p> (注) <code>priv</code> キーワードは、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のみ使用できます。</p> <ul style="list-style-type: none"> <code>community-string</code> には、<code>version 1</code> または <code>version 2c</code> が指定されたときに、通知操作によって送信されたパスワードと類似したコミュニティ スtring を入力します。<code>version 3</code> が指定されたときは、SNMPv3 のユーザ名を入力します。 (任意) <code>notification-type</code> には、表 27-4 (p.27-13) に示されているキーワードを使用します。タイプを指定しない場合、すべての通知が送信されます。

	コマンド	説明
ステップ 6	<code>snmp-server enable traps notification-types</code>	トラップまたはインフォームを送信するスイッチをイネーブルにし、送信する通知タイプを指定します。通知タイプの一覧については、表 27-4 (p.27-13) を参照するか、または <code>snmp-server enable traps ?</code> を入力してください。 複数のトラップタイプをイネーブルにする場合は、トラップタイプごとに <code>snmp-server enable traps</code> コマンドを入力します。
ステップ 7	<code>snmp-server trap-source interface-id</code>	(任意) 送信元インターフェイスを指定します。これにより、トラップメッセージ用の IP アドレスが設定されます。このコマンドを実行すると、インフォーム用の送信元 IP アドレスも設定されます。
ステップ 8	<code>snmp-server queue-length length</code>	(任意) 各トラップホストのメッセージキュー長を設定します。指定できる範囲は 1 ~ 1000 で、デフォルトは 10 です。
ステップ 9	<code>snmp-server trap-timeout seconds</code>	(任意) トラップメッセージの再送信間隔を定義します。指定できる範囲は 1 ~ 1000 秒で、デフォルトは 30 秒です。
ステップ 10	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 11	<code>show running-config</code>	設定を確認します。
ステップ 12	<code>copy running-config startup-config</code>	(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、指定された通知 (トラップまたはインフォーム用) のメカニズムをグローバルにイネーブルにします。インフォームを受信するホストをイネーブルにするには、ホストに対して `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。

トラップを受信するように指定されたホストを削除する場合は、`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。`no snmp-server host` コマンドにキーワードを指定しないで使用すると、ホストに対するトラップはディセーブルになりますが、インフォーム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。

SNMP トラップ通知プライオリティの設定

送信 SNMP トラップ通知に優先順位をつけることにより、輻輳が発生してもネットワーク間を効率的に移動させることができます。スイッチには、次の SNMP パケットに関するプライオリティ オプションがあります。

- IP precedence マーカー
- Differential Services Code Point (DSCP) マーカー

これらのマーカーは、SNMP パケットがネットワーク間を移動する際に受信する優先順位を指定します。最大 8 つの異なる IP precedence マーキングまたは最大 64 個の異なる IP DSCP マーキングを設定できます。デフォルトの IP precedence および DSCP マーカーは 0 で、SNMP パケットを通常のトラフィックとして転送します。マーカーの最大値 (IP precedence は 7、DSCP は 63) は、一般に

ネットワーク制御トラフィック用に予約されています。ネットワーク内の SNMP 通知の重要度に対応する値を選択してください。たとえば、発信 SNMP 通知により高いプライオリティを割り当てるには、IP precedence を 6 に設定します。

DSCP は、IP precedence と部分的に下位互換性があります。IP precedence 値のように機能する DSCP 値を選択するには、0、8、16、24、32、40、48、および 56 の値を使用します。DSCP には、64 個の値を使用することが可能ですが、ネットワークは最下位ビットを無視するか、または値のブロックを同じものとして扱います。

スイッチに発信 SNMP トラップ通知のプライオリティを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>snmp-server ip {precedence precedence-value dscp dscp-value}</code>	SNMP 通知の IP precedence または DSCP のマーカー値を指定します。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(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 トラップを受信するようにホストを指定する場合は、`snmp-server host` グローバル コンフィギュレーション コマンドを使用します。特定のトラップ タイプをイネーブルにするには、`snmp-server enable traps` 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情報の設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>snmp-server contact text</code>	システム コンタクト スtring を設定します。 次に例を示します。 <code>snmp-server contact Dial System Operator at beeper 21555.</code>
ステップ 3	<code>snmp-server location text</code>	システム ロケーション スtring を設定します。 次に例を示します。 <code>snmp-server location Building 3/Room 222</code>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 経由で使用する TFTP サーバの制限

SNMP を経由してコンフィギュレーション ファイルの保存およびロードに使用する TFTP (簡易ファイル転送プロトコル) サーバを、アクセス リストに指定されたサーバに限定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>snmp-server tftp-server-list access-list-number</code>	SNMP を経由して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 リスト内のサーバに限定します。 <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の範囲で標準の IP アクセス リスト番号を入力します。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none"> <i>access-list-number</i> を指定する場合は、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。 <code>deny</code> キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。<code>permit</code> キーワードを指定すると、条件が一致した場合にアクセスが許可されます。 <i>source</i> には、スイッチへのアクセスが許可された TFTP サーバの IP アドレスを入力します。 (任意) <i>source-wildcard</i> を指定する場合は、送信元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 1 を入力します。 アクセス リストの末尾には、すべてに適用される暗黙的な拒否ステートメントが常に存在する点に注意してください。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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

最初の例は、SNMP のすべてのバージョンをイネーブルにする方法を示します。この設定では、SNMP マネージャが読み取り専用権限でコミュニティ スtring *public* を使用し、すべてのオブジェクトにアクセスすることを許可します。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
```

次の例は、SNMP マネージャが読み取り専用権限でコミュニティ スtring *public* を使用し、すべてのオブジェクトへのアクセスを許可する方法を示します。このスイッチは、SNMPv1 を使用してホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に、それぞれ VTP トラップを送信します。コミュニティ スtring *public* が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
```

次の例は、コミュニティ スtring *comaccess* を使用するアクセス リスト 4 のメンバーに、すべてのオブジェクトの読み取り専用アクセスを許可する方法を示します。その他の SNMP マネージャは、オブジェクトにアクセスしません。コミュニティ スtring *public* を使用し、SNMPv2C に よって SNMP 認証失敗トラップがホスト *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、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tring は制限されています。スイッチは最初の行により、以前イネーブルにしたトラップ以外にエンティティ MIB トラップを送信することが可能となります。2 番目の行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、スイッチがコミュニティ スtring *public* を使用し、すべてのトラップをホスト *myhost.cisco.com* に送信できるように設定する例を示します。

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

次に、ユーザーをリモート ホストに関連付けて、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に *auth* (*authNoPriv*) 認証レベル 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

無効なコミュニティ ストリング エントリの数、エラー、要求された変数など、SNMP 入出力統計情報を表示する場合は、`show snmp` イネーブル EXEC コマンドを使用します。表 27-5 に示されたイネーブル EXEC コマンドを使用し、SNMP 情報を表示することもできます。この出力に表示されるフィールドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。

表 27-5 SNMP 情報表示用のコマンド

機能	デフォルト設定
<code>show snmp</code>	SNMP の統計情報を表示します。
<code>show snmp engineID [local remote]</code>	デバイス上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。
<code>show snmp group</code>	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。
<code>show snmp pending</code>	ペンディング中の SNMP 要求に関する情報を表示します。
<code>show snmp sessions</code>	現在の SNMP セッションに関する情報を表示します。
<code>show snmp user</code>	SNMP ユーザテーブル内の各 SNMP ユーザ名に関する情報を表示します。

