CHAPTER 44

SNMP の設定

この章では、Catalyst 6500 シリーズ スイッチ上で 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。

この章で説明する内容は、次のとおりです。

（注） この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

SNMP の用語

表 44-1 に、SNMP で使用する用語を定義します。

表 44-1　SNMP の用語

用語	定義
認証	データ整合性、データ オリジン認証など、メッセージ整合性およびメッセージ再送に対する保護を行うプロセス
信頼できる SNMP エンジン	ネットワーク通信に使用される SNMP の 1 つが、メッセージの再送、遅延、転送に対して保護する許容 SNMP エンジンに指定されます。SNMPv3 パケットの認証および暗号化に使用されるセキュリティ キーは、信頼できる SNMP エンジンの ID およびユーザ パスワードと同等の機能を持ちます。応答を返す SNMP メッセージ（たとえば、get exact、get next、set request）の場合、このメッセージの*受信側*が信頼できる相手となります。応答を返さない SNMP メッセージの場合、*送信側*が信頼できる相手となります。
コミュニティ ストリング	管理ステーションと SNMPv1 または SNMPv2c エンジンとの間でメッセージの認証に使用する文字列
データ整合性	不正な方法でメッセージ パケットが変更または破壊されていないデータの状態（ステート）
データ オリジン認証	メッセージの送信先と思われるユーザの ID を確認する能力。この能力により、別の SNMP エンジンによるメッセージ取り込みと再送からユーザを保護します。また、誤ったパスワードまたはセキュリティ レベルを使用する特定のユーザとのパケット送受信からも保護します。
暗号化	SNMP パケットの内容をスクランブルして不正なユーザからデータを隠す方法
グループ	特定のセキュリティ モデルに属すユーザの集合。グループは、そこに属するすべてのユーザのアクセス権を定義します。アクセス権は、読み取り、書き込み、作成ができる SNMP オブジェクトを定義します。また、グループはユーザが受け取りを許可される通知も定義します。
通知ホスト	通知（トラップおよび通知）の送信先となる SNMP エンティティ
通知ビュー	各グループのビューの名前（最大 64 文字）。ビュー名は、グループ内の各ユーザに送信できる通知リストを定義します。
プライバシ	SNMP パケットの内容の暗号化されたステート。このステートでは、内容はネットワーク上で公開されないようになっています。暗号化は、CBC-DES（DES-56）と呼ばれるアルゴリズムで実行されます。
読み取りビュー	各グループのビューの名前（最大 64 文字）。ビュー名は、グループ内の各ユーザが読み取りできる Object Identifier（OID; オブジェクト識別子）リストを定義します。

表 44-1　SNMP の用語（続き）

用語	定義
セキュリティ レベル	各 SNMP パケット上で実行されるセキュリティ アルゴリズムのタイプ。noauth、auth、および priv の 3 つのレベルがあります。noauth レベルは、ユーザ名のストリング照合によってパケットを認証します。auth レベルは、HMAC MD5 または SHA アルゴリズムを使用してパケットを認証します。priv レベルは、HMAC MD5 または SHA アルゴリズムを使用してパケットを認証し、CBC-DES（DES-56）アルゴリズムでパケットを暗号化します。
セキュリティ モデル	SNMP エージェントが使用するセキュリティ戦略。現在、Cisco IOS ソフトウェアは SNMPv1、SNMPv2c、および SNMPv3 という 3 種類のセキュリティ モデルをサポートしています。
SNMP	ネットワーク装置をモニタおよび制御し、設定、統計情報収集、パフォーマンス、およびセキュリティを管理する手段を備えたネットワーク管理プロトコル
SNMPv2c	SNMP の 2 番めのバージョン。中央集中および分散型ネットワーク管理計画をサポートし、SMI、プロトコル動作、管理アーキテクチャ、およびセキュリティ機能が強化されています。
SNMP エンジン	ローカルまたはリモート装置に常駐できる SNMP
SNMP エンティティ	SNMPv1 や SNMPv2c と異なり、SNMPv3 では、SNMP エージェントや SNMP マネージャなどの用語は廃止されています。これらの概念を統合して SNMP エンティティと呼びます。SNMP エンティティは、SNMP エンジンと SNMP アプリケーションで構成されます。
SNMP グループ	アクセス ポリシーを定義する共通 SNMP リストに属する SNMP ユーザの集合で、ここでは OID 番号は読み取りアクセスも書き込みアクセスもともに可能です。特定の SNMP グループに属するユーザは、そのグループによって定義されたこれらの属性をすべて継承します。
SNMP ユーザ	SNMP 管理操作のサービス対象者。ユーザとは情報を受信するリモート SNMP エンジン上にいる人のことです。
SNMP ビュー	SNMP オブジェクトとそのオブジェクトが利用できるアクセス権との間のマッピング。オブジェクトは、それぞれのビューにさまざまなアクセス権を持っています。アクセス権は、コミュニティ ストリングまたはユーザがオブジェクトにアクセス可能かどうかを示します。
書き込みビュー	各グループのビューの名前（最大 64 文字）。ビュー名は、グループ内の各ユーザが作成または変更できる OID リストを定義します。

SNMP の機能

SNMP はアプリケーション レイヤ プロトコルで、ネットワーク装置間の管理情報の交換を容易にします。SNMP を使用することにより、ネットワーク管理者はネットワーク パフォーマンスの管理、ネットワーク障害の発見と解決、ネットワーク拡大の計画立案ができます。

SNMP には次の 3 つのバージョンがあります。

- バージョン 1（SNMPv1）— SNMP の初期の実装です。機能の詳細については、RFC 1157 を参照してください。SNMPv1 の詳細については、「SNMPv1 および SNMPv2c の機能」（p.44-6）を参照してください。
- バージョン 2（SNMPv2c）— SNMP の 2 番めのリリースで、RFC 1902 に規定されており、データ型、カウンタ サイズ、およびプロトコルの動作について、機能の追加および拡張が施されています。SNMPv2c の詳細については、「SNMPv1 および SNMPv2c の機能」（p.44-6）を参照してください。
- バージョン 3（SNMPv3）— SNMP の最新バージョンで、詳細は RFC 2571、RFC 2572、RFC 2573、RFC 2574、RFC 2575 に規定されています。SNMPv1 および SNMPv2c 対応の Catalyst エンタープライズ LAN スイッチでの SNMP 機能は変わりませんが、管理およびセキュリティについては大幅に機能が強化されています。SNMPv3 の詳細については、「SNMPv3 の機能」（p.44-8）を参照してください。

セキュリティ モデルおよびセキュリティ レベル

セキュリティ モデルは、ユーザと、ユーザが属するグループに対して設定された認証戦略です。セキュリティ レベルとは、セキュリティ モデル内のセキュリティの許可されたレベルです。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 パケットの処理の際に採用されるセキュリティ メカニズムが決まります。SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルがあります。表 44-2 に、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を示します。

表 44-2　SNMP セキュリティ レベル

モデル	レベル	認証	暗号化	処理
v1	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。
v2c	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。
v3	noAuthNoPriv	ユーザ名	なし	認証にユーザ名の照合を使用します。
v3	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。
v3	authPriv	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。認証の他に、CBC-DES（DES-56）に基づく DES 56 ビット暗号化を行います。

SNMPv3 オブジェクトについて次の事項に注意してください。

- 各ユーザは 1 つのグループに属します。
- グループは、ユーザの集合に対するアクセス ポリシーを定義します。

- SNMP オブジェクトは、読み取り、書き込み、および作成のアクセス ポリシーを参照します。
- グループによって、ユーザが受信できる通知リストが決まります。
- グループは、そのユーザのセキュリティ モデルおよびセキュリティ レベルも定義します。

SNMP ifindex 持続機能

SNMP ifIndex 持続機能は常にイネーブルです。ifIndex 持続機能により、次に示す処理が発生したあとも、ポートおよび VLAN の ifIndex 値は常に保持および使用されます。

- スイッチの再起動
- ハイアベイラビリティ スイッチオーバー
- ソフトウェア アップグレード
- モジュールのリセット
- モジュールの取り外し、および同じタイプのモジュールの取り付け

Fast EtherChannel および Gigabit EtherChannel インターフェイスの場合、ifIndex 値が保持および使用されるのは、ハイアベイラビリティ スイッチオーバーが発生したあとのみです。

SNMPv1 および SNMPv2c の機能

SNMPv1 および SNMPv2c ネットワーク管理で使用するコンポーネントは、次の 3 つのカテゴリに分類されます。

- 管理対象装置（スイッチなど）
- 管理対象装置で実行される SNMP エージェントおよび MIB（管理情報ベース）（Remote Monitoring [RMON] MIB など）
- エージェントと通信して管理対象装置から統計情報およびアラートを入手する、CiscoWorks2000 などの SNMP ネットワーク管理アプリケーション。CiscoWorks2000 の詳細については、「CiscoWorks2000 の使用方法」（p.44-7）を参照してください。

（注）　SNMP　管理アプリケーションおよび　SNMP　管理アプリケーションを実行するコンピュータを Network Management System（NMS; ネットワーク管理システム）といいます。

管理対象装置の使用方法

Catalyst 6500 シリーズ スイッチは、次の機能を使用した SNMP ネットワーク管理をサポートする管理対象装置です。

- SNMP トラップ（「CLI での SNMPv1 および SNMPv2c の設定」[p.44-12] を参照）
- スーパバイザ エンジン ソフトウェアの RMON（第 45 章「RMON の設定」を参照）
- 外部 SwitchProbe 装置の RMON および RMON2

SNMP エージェントおよび MIB の使用方法

SNMP ネットワーク管理では、次の SNMP エージェント機能を使用します。

- MIB 変数へのアクセス — この機能は、NMS からの要求への応答として、SNMP エージェントによって実行されます。SNMP エージェントは要求された MIB 変数の値を検索し、NMS にこれらの値を戻します。
- MIB 変数の設定 — この機能もまた、NMS からのメッセージへの応答として、SNMP エージェントにより実行されます。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。

（注）　MIB の詳細については、http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml を参照してください。

- SNMP トラップ — この機能は、エージェントで重大イベントが発生したことを NMS に通知するために使用されます。次のいずれかのトラップ イベントが発生すると、SNMP エージェントはトラップ レシーバーとして指定された NMS に対して、SNMP トラップ メッセージを送信します。
  - ポートまたはモジュールがアップまたはダウンした場合
  - 温度が制限値を超えた場合
  - スパニングツリー トポロジーが変更された場合
  - 認証に失敗した場合
  - 電源障害が発生した場合

- 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する組み込みパスワードです。
  - read-only — コミュニティ ストリング以外のすべての MIB 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 — すべての MIB 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 ストリングへのアクセスは許可しません。
  - read-write-all — コミュニティ ストリングを含むすべての MIB オブジェクトへの読み書きアクセスを許可します。

（注） NMS のコミュニティ ストリング定義は、スイッチの 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致している必要があります。

CiscoWorks2000 の使用方法

CiscoWorks2000 は、シスコのエンタープライズ系ネットワークおよび装置を管理する、管理プラットフォームに依存しない Web ベース製品ファミリーの 1 つです。CiscoWorks2000 には、スイッチド インターネットワークの配置、設定、モニタ、管理、およびトラブルシューティングを実行できる Resource Manager Essentials および CWSI Campus が統合されています。詳細については、次のマニュアルを参照してください。

- 『*Getting Started With Resource Manager Essentials*』
- 『*Getting Started With CWSI Campus*』

SNMPv3 の機能

SNMPv3 には SNMPv1 および SNMPv2c の機能がすべて搭載されているだけでなく、管理とセキュリティについて機能が大幅に強化されています。SNMPv3 は相互運用が可能な標準ベースのプロトコルであり、ネットワーク上でパケットを認証および暗号化して装置に安全にアクセスできるようにします。SNMPv3 に搭載されているセキュリティ機能には、次のものがあります。

- メッセージ整合性 — 不正変更または破壊することなくデータを安全に収集します。
- 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 — パケットの内容をスクランブルして許可されていない送信元から見えないようにします。

SNMP エンティティ

SNMPv1 や SNMPv2c と異なり、SNMPv3 では、*SNMP エージェント*や *SNMP マネージャ*などの概念は廃止されています。これらの概念は *SNMP エンティティ*として統合されています。SNMP エンティティは、SNMP エンジンと SNMP アプリケーションで構成されます。SNMP エンジンは、次の 4 つのコンポーネントで構成されます。

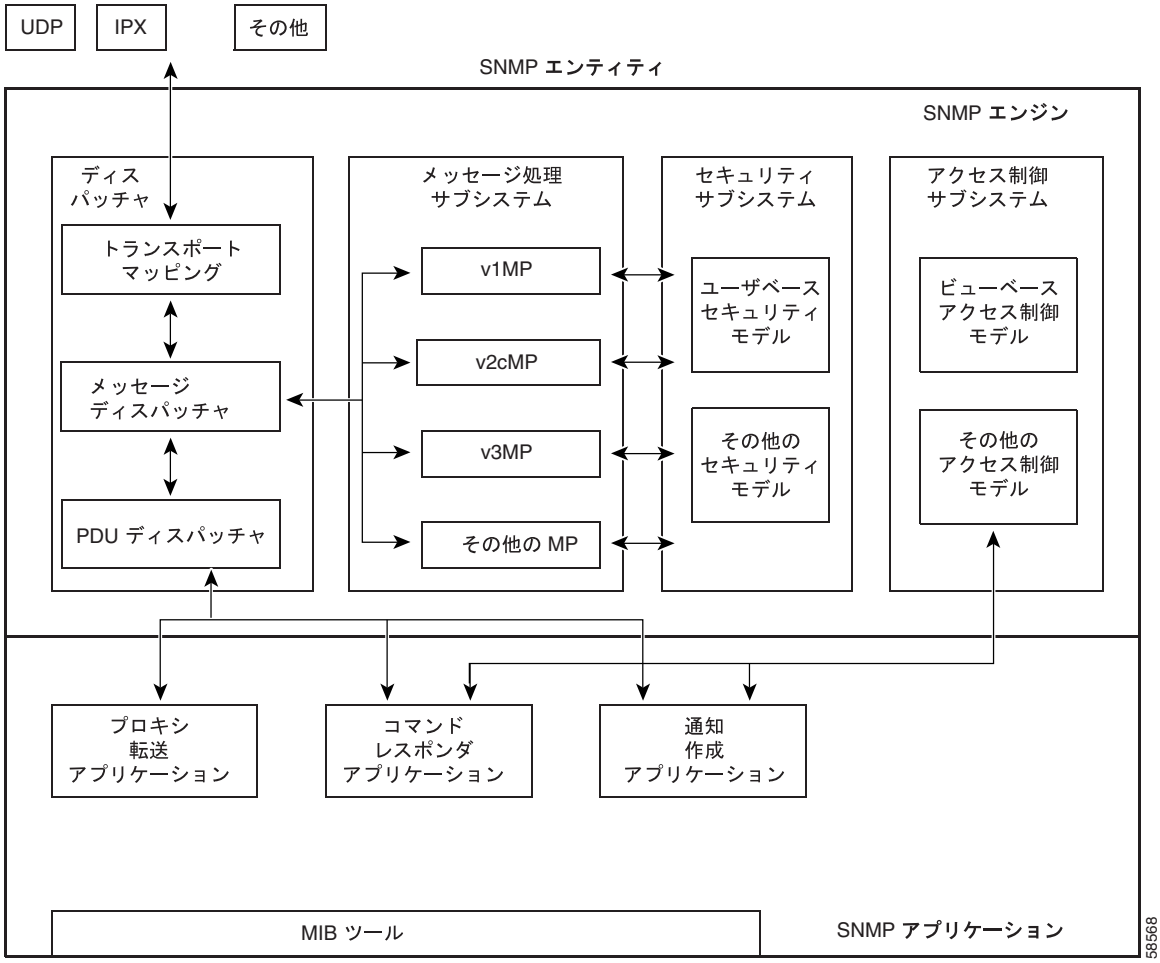
- ディスパッチャ
- メッセージ処理サブシステム
- セキュリティ サブシステム
- アクセス制御サブシステム

図 44-1 に、SNMP エンティティを示します。

ディスパッチャ

ディスパッチャは、メッセージを送受信するトラフィック マネージャです。メッセージの受信後、ディスパッチャは、メッセージのバージョン番号を調べてからそのメッセージを該当するメッセージ処理モデルに渡します。ディスパッチャには、アプリケーションに Protocol Data Unit（PDU; プロトコル データ ユニット）をディスパッチし、メッセージ送信用のトランスポートを選択する役割もあります。

図 44-1　従来の SNMP エージェントに対する SNMP エンティティ



メッセージ処理サブシステム

メッセージ処理サブシステムは、ディスパッチャからの発信 PDU を受け入れ、メッセージ ヘッダーでラップしてディスパッチャに戻すことで伝送の準備をします。また、ディスパッチャからの着信メッセージも受け入れ、各メッセージ ヘッダーを処理し、同封された PDU をディスパッチャに戻します。メッセージ処理サブシステムを実装すると、SNMP（SNMPv1、SNMPv2c、SNMPv3）の 1 つのバージョンに対応する 1 つのメッセージ形式をサポートするか、それぞれが異なるバージョンの SNMP をサポートしている多数のモジュールを装備することになります。

セキュリティ サブシステム

セキュリティ サブシステムは、メッセージを認証して暗号化します。各発信メッセージは、メッセージ処理サブシステムからセキュリティ サブシステムに渡されます。セキュリティ サブシステムは、必要なサービスに応じて同封された PDU とメッセージ ヘッダーの一部のフィールドを暗号化します。また、認証コードを生成してメッセージ ヘッダーに挿入します。メッセージは、暗号化のあと、メッセージ処理サブシステムに戻されます。

各着信メッセージは、メッセージ処理サブシステムからセキュリティ サブシステムに渡されます。セキュリティ サブシステムは、必要に応じて認証コードをチェックし、復号化を実行します。処理されたメッセージは、メッセージ処理サブシステムに戻されます。セキュリティ サブシステムを実装すると、1 つまたは複数の個別のセキュリティ モデルをサポートします。現在、唯一定義されているセキュリティ モデルは SNMPv3 対応の User-based Security Model（USM）で、RFC 2274 に規定されています。

USM は、以下のセキュリティ上の潜在的な脅威から SNMPv3 メッセージを保護します。

- 未許可の SNMP エンティティによって送信中に変更されたメッセージを送信する許可ユーザ
- 許可ユーザになりすます不正ユーザ
- メッセージ ストリームを変更するユーザ
- メッセージを傍受する不正ユーザ

USM は現在、認証プロトコルとして HMAC-MD5-96 および HMAC-SHA-96、プライバシ プロトコルとして CBC-DES を定義しています。

SNMPv1 および SNMPv2c セキュリティ モデルはコミュニティ名の認証しか備えておらず、プライバシは備えていません。

アクセス制御サブシステム

アクセス制御サブシステムは、管理対象オブジェクトへのアクセスを許可するかどうかを決定します。View-based Access Control Model（VACM）を使用することで、どのユーザのどの操作がどの管理対象オブジェクトにアクセスできるかを制御できます。

アプリケーション

SNMPv3 アプリケーションとは、SNMP エンティティ内の内部アプリケーションを指します。この内部アプリケーションでは、次の処理を行います。

- SNMP メッセージの生成
- 受信した SNMP メッセージへの応答
- 通知の生成および受信
- SNMP エンティティ間のメッセージの転送

現在、5 種類のアプリケーションがあります。

- コマンド ジェネレータ — SNMP コマンドを生成して管理データを収集または設定します。
- コマンド レスポンダ — 管理データにアクセスします。たとえば、コマンド レスポンダ アプリケーションでは、**processing get**、**get-next**、**get-bulk**、および **set pdus** が使用されます。
- 通知作成 — トラップまたは情報メッセージを起動します。
- 通知受信 — トラップまたは情報メッセージを受信し処理します。
- プロキシ転送 — SNMP エンティティでメッセージを転送します。

SNMP 処理のイネーブル化およびディセーブル化

ここでは、**set snmp enable** | **disable** コマンドを使用して、スイッチに対する SNMP 要求とスイッチからの SNMP トラップの処理をイネーブルまたはディセーブルに設定する手順を説明します。

SNMP をイネーブル モードに設定した場合、そのスイッチに対する他の SNMP 設定と競合しなければ、スイッチへの SNMP 要求が処理されて、SNMP トラップが送出されます。

SNMP をディセーブル モードに設定した場合、そのスイッチに対する他の SNMP 設定とは関係なく、SNMP 要求は無視され、SNMP トラップは送出されません。

いずれの SNMP モードでも（イネーブルまたはディセーブル）、他の SNMP 設定を変更できます。RMON 関連の処理は、いずれのモードにも影響しません。

CLI（コマンド ライン インターフェイス）を使用して SNMP 処理をイネーブルにするには、イネーブル モードで次の作業を行います（SNMP 処理はイネーブル モードがデフォルトです）。

	作業	コマンド
ステップ 1	SNMP 処理をイネーブルにします。	**set snmp enable** | **disable**
ステップ 2	SNMP 処理がイネーブルに設定されたことを確認します。	**show snmp**

次に、SNMP 処理をイネーブルにする例を示します。

```
Console> (enable) set snmp enable
SNMP enabled.
Console> (enable)
```

次に、SNMP 処理をディセーブルにする例を示します。

```
Console> (enable) set snmp disable
SNMP disabled.
Console> (enable)
```

次に、SNMP の設定を確認する例を示します。

```
Console> (enable) show snmp
SNMP:                       Disabled
RMON:                       Disabled
Extended RMON Netflow Enabled : None.
Memory usage limit for new RMON entries: 85 percent
Traps Enabled:
None
Port Traps Enabled: None

Community-Access     Community-String
----------------     --------------------
read-only            public
read-write           private
read-write-all       secret

Trap-Rec-Address Trap-Rec-Community Trap-Rec-Port Trap-Rec-Owner Trap-Rec-Index
---------------- ------------------ ------------- -------------- --------------
Console> (enable)
```

スイッチ上での SNMPv1 および SNMPv2c の設定

ここでは、SNMPv1 および SNMPv2c の基本設定について説明します。Catalyst 6500 シリーズ スイッチによってサポートされる SNMP コマンドの詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

SNMPv1 および SNMPv2c のデフォルト設定

ここに記載されている各コマンドの SNMP デフォルト設定については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

NMS での SNMPv1 および SNMPv2c の設定

NMS での SNMP の設定手順については、NMS のマニュアルを参照してください（「CiscoWorks2000 の使用方法」[p.44-7] を参照）。

スイッチは、RMON2 トラップ宛先テーブルに指定された 20 までのトラップ レシーバーをサポートしています。RMON2 トラップ宛先テーブルは、NMS を使用して設定します。

CLI での SNMPv1 および SNMPv2c の設定

（注） Release 7.5(1) の拡張 SNMP 機能については、「Release 7.5(1) の SNMPv1 および SNMPv2c 拡張機能」（p.44-14）を参照してください。

CLI を使用して SNMP を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	各アクセス タイプについて SNMP コミュニティ ストリングを定義します。	**set snmp community read-only** *community_string* **set snmp community read-write** *community_string* **set snmp community read-write-all** *community_string*
ステップ 2	トラップ レシーバーおよびコミュニティを指定します。最大 10 のトラップ レシーバーを指定できます。	**set snmp trap** *rcvr_address rcvr_community*
ステップ 3	トラップ レシーバーに送信する SNMP トラップを指定します。	**set snmp trap enable** [**all** | **auth** | **bridge** | **chassis** | **config** | **entity** | **entityfru** | **envfan** | **envpower** | **envshutdown** | **envtemp** | **flashinsert** | **flashremove** | **ippermit** | **module** | **stpx** | **syslog** | **system** | **vlancreate** | **vlandelete** | **vmps** | **vtp**]
ステップ 4	SNMP の設定を確認します。	**show snmp**

次に、コミュニティ ストリングを定義し、トラップ レシーバーを割り当て、トラップ レシーバーに送信するトラップを指定する例を示します。

```
Console> (enable) set snmp community read-only Everyone
SNMP read-only community string set to 'Everyone'.
Console> (enable) set snmp community read-write Administrators
SNMP read-write community string set to 'Administrators'.
Console> (enable) set snmp community read-write-all Root
SNMP read-write-all community string set to 'Root'.
Console> (enable) set snmp trap 172.16.10.10 read-write
SNMP trap receiver added.
Console> (enable) set snmp trap 172.16.10.20 read-write-all
SNMP trap receiver added.
Console> (enable) set snmp trap enable all
All SNMP traps enabled.
Console> (enable) show snmp
RMON:                         Disabled
Extended RMON:                Extended RMON module is not present
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,entity,stpx
Port Traps Enabled: 1/1-2,4/1-48,5/1
Community-Access     Community-String
----------------     --------------------
read-only            Everyone
read-write           Administrators
read-write-all       Root
Trap-Rec-Address                            Trap-Rec-Community
------------------------------------------  --------------------
172.16.10.10                                read-write
172.16.10.20                                read-write-all
Console> (enable)
```

（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 ストリングを空白にします（コミュニティ ストリングには値を入力しないでください）。

Release 7.5(1) の SNMPv1 および SNMPv2c 拡張機能

ここでは、Release 7.5(1) に追加された拡張機能について説明します。

複数の SNMP コミュニティ ストリングの設定

community-ext キーワードを使用すると、複数の SNMP コミュニティ ストリングを設定できます。**community-ext** キーワードを使用して定義したコミュニティ ストリングは、既存のコミュニティ ストリングの複製にはできません。**community-ext** キーワードを使用して新しいコミュニティ ストリングを追加すると、vacmAccessTable（ビューを指定した場合）、snmpCommunityTable、および vacmSecurityToGroup のテーブルに該当するエントリが作成されます。

CLI を使用して複数の SNMP コミュニティ ストリングを設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	複数の SNMP コミュニティ ストリングを設定します。	**set snmp community-ext** *community_string* {**read-only** | **read-write** | **read-write-all**} [**view** *view_oid*] [**access** *access_number*]
ステップ 2	SNMP の設定を確認します。	**show snmp**

次に、追加 SNMP コミュニティ ストリングを設定する例を示します。

```
Console> (enable) set snmp community-ext public1 read-only

Community string public1 is created with access type as read-only
Console> (enable)
```

次に、コミュニティ ストリングをアクセス番号に制限する例を示します。

```
Console> (enable) set snmp community-ext private1 read-write access 2

Community string private1 is created with access type as read-write access number 2
Console> (enable)
```

次に、コミュニティ ストリングのアクセス番号を変更する例を示します。

```
Console> (enable) set snmp community-ext private1 read-write access 3

Community string private1 is updated with access type as read-write access
number 3
Console> (enable)
```

次に、SNMP 設定を表示する例を示します。

```
Console> (enable) show snmp

SNMP:Enabled
RMON:Disabled
Extended RMON Netflow Enabled :None.
Memory usage limit for new RMON entries:85 percent
Traps Enabled:None
Port Traps Enabled:None

Community-Access Community-String
---------------- --------------------
read-only        public
read-write       private
read-write-all   secret

Additional-                          Access-
Community-String     Access-Type     Number  View
-------------------- --------------- ------- ----------------------------------
public1              read-only
public2              read-only       1
private1             read-write      2       1.3.6
secret1              read-write-all  500     1.3.6.1.4.1.9.9

Trap-Rec-Address Trap-Rec-Community Trap-Rec-Port Trap-Rec-Owner Trap-Rec-Index
---------------- ------------------ ------------- -------------- --------------
Console> (enable)
```

SNMP コミュニティ ストリングの消去

コミュニティ ストリングは、**clear snmp community-ext** *community-string* コマンドを使用すると消去できます。このコマンドを使用してコミュニティ ストリングを消去すると、vacmAccessTable および vacmSecurityToGroup テーブルの対応するエントリも削除されます。

CLI を使用して SNMP コミュニティ ストリングを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	SNMP コミュニティ ストリングを消去します。	**clear snmp community-ext** *community-string*
ステップ 2	SNMP の設定を確認します。	**show snmp**

次に、SNMP コミュニティ ストリングを消去する例を示します。

```
Console> (enable) clear snmp community-ext public1
Community string public1 has been removed
Console> (enable)
```

ホストのアクセス番号の指定

1 つまたは複数のホストに対応付けられたアクセス番号のリストを指定して、特定のコミュニティ ストリングを使用してシステムにアクセスできるホストを制限できます。各 IP アドレスをスペースで区切って、アクセス番号に対応付けられた複数の IP アドレスを指定できます。既存のアクセス番号が使用されている場合は、新しい IP アドレスはリストに追加されます。

CLI を使用してホストのアクセス番号を指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ホストのアクセス番号を指定します。	**set snmp access-list** *access_number IP_address* [**ipmask** *maskaddr*]
ステップ 2	SNMP の設定を確認します。	**show snmp access-list**

次に、ホストのアクセス番号を指定する例を示します。

```
Console> (enable) set snmp access-list 1 172.20.60.100
Access number 1 has been created with new IP Address 172.20.60.100

Console> (enable) set snmp access-list 2 172.20.60.100 mask 255.0.0.0
Access number 2 has been created with new IP Address 172.20.60.100 mask 255.0.0.0

Console> (enable) set snmp access-list 2 172.20.60.7
Access number 2 has been updated with new IP Address 172.20.60.7

Console> (enable) set snmp access-list 2 172.20.60.7 mask 255.255.255.0
Access number 2 has been updated with existing IP Address 172.20.60.7 mask
255.255.255.0
Console> (enable)
```

次に、SNMP 設定を表示する例を示します。

```
Console> (enable) show snmp access-list
Access-Number   IP-Addresses/IP-Mask
-------------   ------------------------
1               172.20.60.100/255.0.0.0
                1.1.1.1/-
2               172.20.60.7/-
                2.2.2.2/-
3               2.2.2.2/155.0.0.0
4               1.1.1.1/2.1.2.4
                2.2.2.2/-
                2.2.2.5/-
Console> (enable)
```

アクセス番号に対応付けられた IP アドレスの消去

CLI を使用してアクセス番号に対応付けられた IP アドレスを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	アクセス番号に対応付けられた IP アドレスを消去します。	**clear snmp access-list** *access_number IP_address* [[*IP_address*] ...]
ステップ 2	SNMP の設定を確認します。	**show snmp access-list**

次に、アクセス番号に対応付けられた IP アドレスを消去する例を示します。

```
Console> (enable) clear snmp access-list 101
All IP addresses associated with access-number 101 have been cleared.
Console> (enable)

Console> (enable) clear snmp access-list 2 172.20.60.8
Access number 2 no longer associated with 172.20.60.8
Console> (enable)
```

インターフェイス エイリアスの指定、表示、および消去

インターフェイス エイリアスの指定、表示、および消去ができます。エイリアスには最大 64 文字まで使用できます。

（注）　バイナリ コンフィギュレーション モードでは、**set snmp ifalias** コマンドを使用できません。このコマンドを入力する場合、または ifalias が NVRAM（不揮発性 RAM）に保存されてない場合は、テキスト ファイル コンフィギュレーション モードを使用する必要があります。

インターフェイス エイリアスの指定、表示、および消去を行うには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	インターフェイス エイリアスを指定します。	**set snmp ifalias** {*ifIndex*} [*ifAlias*]
ステップ 2	インターフェイス エイリアスを表示します。	**show snmp ifalias** [*ifIndex*]
ステップ 3	インターフェイス エイリアスを消去します。	**clear snmp ifalias** {*ifIndex*} **all**

次に、インターフェイス エイリアスを指定、表示、および消去する例を示します。

```
Console> (enable) set snmp ifalias 1 Inband port

ifIndex 1 alias set
Console> (enable)

Console> (enable) show snmp ifalias 1
ifIndex    ifName               ifAlias
---------- -------------------- ---------------------------------
1          sc0                  Inband port
Console> (enable)

Console> (enable) clear snmp ifalias all
Console> (enable)
```

スイッチ上での SNMPv3 の設定

ここでは、SNMPv3 の基本設定について説明します。Catalyst 6500 シリーズ スイッチによってサポートされる SNMP コマンドの詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

SNMPv3 のデフォルト設定

ここに記載されている各コマンドの SNMP デフォルト設定については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

NMS での SNMPv3 の設定

NMS での SNMP の設定手順については、NMS のマニュアルを参照してください（「CiscoWorks2000 の使用方法」[p.44-7] を参照）。

スイッチは、RMON2 トラップ宛先テーブルに指定された 20 までのトラップ レシーバーをサポートしています。RMON2 トラップ宛先テーブルは、NMS を使用して設定します。

CLI での SNMPv3 の設定

CLI を使用して SNMPv3 を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ローカル SNMP エンジンに対して SNMP サーバエンジン ID 名を設定します。	**set snmp engineid** *engineid*
ステップ 2	MIB ビューを設定します。	**set snmp view** [**-hex**] {*viewname*} {*subtree*} [*mask*] [***included*** | ***excluded***] [***volatile*** | ***nonvolatile***]
ステップ 3	各種のセキュリティ レベルで 1 つの特定のセキュリティ モデルを持つグループのアクセス権を設定します。	***set snmp access*** [***-hex***] {*groupname*} {***security-model v3***} {***noauthentication*** | ***authentication*** | ***privacy***} [**read** [***-hex***] {*readview*}] [***write*** [***-hex***] {*writeview*}] [***notify*** [***-hex***] {*notifyview*}] [***context*** [***-hex***] {*contextname*} [***exact*** | ***prefix***]] [***volatile*** | ***nonvolatile***]
ステップ 4	通知用のターゲット アドレスを指定します。	***set snmp notify*** [***-hex***] {**notifyname**} ***tag*** [***-hex***] {*notifytag*} [***trap*** | ***inform***] [***volatile*** | ***nonvolatile***]
ステップ 5	ターゲット アドレス テーブルに snmpTargetAddrEntry を設定します。	***set snmp targetaddr*** [***-hex***] {*addrname*} ***param*** [***-hex***] {*paramsname*} {*ipaddr*} [***udpport*** {*port*}] [***timeout*** {**value**}] [***retries*** {**value**}] [***volatile*** | ***nonvolatile***] [***taglist*** {[***-hex***] *tag*} [[***-hex***] *tag*]]
ステップ 6	ターゲットへのメッセージ生成に使用する SNMP パラメータを設定します。	***set snmp targetparams*** [***-hex***] {*paramsname*} ***user*** [***-hex***] {*username*} {***security-model v3***} {***message-processing v3***} {***noauthentication*** | ***authentication*** | ***privacy***} [***volatile*** | ***nonvolatile***]
ステップ 7	新しいユーザを設定します。	***set snmp user*** [***-hex***] {*username*} [***remote*** {*engineid*}] [{***authentication*** [***md5*** | *sha*] {*authpassword*}] [***privacy*** {*privpassword*}] [***volatile*** | ***nonvolatile***]
ステップ 8	指定されたセキュリティ モデルでユーザをグループに関連付けます。	***set snmp group*** [***-hex***] {*groupname*} ***user*** [***-hex***] {*username*} {***security-model v1*** | ***v2*** | ***v3***} [***volatile*** | ***nonvolatile***]

	作業	コマンド
ステップ 9	システムのデフォルト部分用のコミュニティ テーブルを設定します。これは、SNMP の旧バージョンのコミュニティ ストリングを SNMPv3 にマッピングします。	***set snmp community*** {***read-only*** | ***read-write*** | ***read-write-all***} [*community_string*]
ステップ 10	各種コミュニティ ストリングとフル アクセス権を備えたセキュリティ モデルとの間のマッピング用のコミュニティ テーブルを設定します。	***set snmp community index*** {*index_name*} ***name*** [*community_string*] ***security*** {*security_name*} ***context*** {*context_name*} ***transporttag*** {*tag_value*} [***volatile*** | ***nonvolatile***]
ステップ 11	SNMP の設定を確認します。	***show snmp***

次に、interfacesMibView に MIB ビューを設定する例を示します。

```
Console> (enable) set snmp view interfacesMibView 1.3.6.1.2.1.2 included
Snmp view name was set to interfacesMibView with subtree 1.3.6.1.2.1.2 included,
nonvolatile.
```

次に、guestgroup というグループに SNMPv3 認証読み取りモードに対するアクセス権を設定する例を示します。

```
Console> (enable) set snmp access guestgroup security-model v3 authentication read
interfacesMibView
Snmp access group was set to guestgroup version v3 level authentication,
readview interfacesMibView, context match:exact, nonvolatile.
```

次に、ターゲット アドレスを指定する例を示します。

```
Console> (enable) set snmp notify notifytable1 tag routers trap
Snmp notify name was set to notifytable1 with tag routers notifyType trap, and
storageType nonvolatile.
```

次に、ターゲット アドレス テーブルに snmpTargetAddrEntry を設定する例を示します。

```
Console> (enable) set snmp targetaddr router_1 param p1 172.20.21.1
Snmp targetaddr name was set to router_1 with param p1
ipAddr 172.20.21.1, udpport 162, timeout 1500, retries 3, storageType nonvolatile.

Console> (enable) set snmp targetaddr router_2 param p2 172.20.30.1
Snmp targetaddr name was set to router_2 with param p2
ipAddr 172.20.30.1, udpport 162, timeout 1500, retries 3, storageType nonvolatile.
```

次に、SNMP ターゲット パラメータの設定例を示します。

```
Console> (enable) set snmp targetparams p1 user guestuser1 security-model v3
message-processing v3 authentication
Snmp target params was set to p1 v3 authentication, message-processing v3,
user guestuser1 nonvolatile.

Console> (enable) set snmp targetparams p2 user guestuser2 security-model v3
message-processing v3 privacy
Snmp target params was set to p2 v3 privacy, message-processing v3,
user guestuser2 nonvolatile.
```

次に、ユーザとして guestuser1 および guestuser2 を設定する例を示します。

```
Console> (enable) set snmp user guestuser1 authentication md5 guestuser1password
privacy privacypasswd1
Snmp user was set to guestuser1 authProt md5 authPasswd guestuser1password privProt
des privPasswd
privacypasswd1 with engineid 00:00:00:09:00:10:7b:f2:82:00:00:00 nonvolatile.

Console> (enable) set snmp user guestuser2 authentication sha guestuser2password
Snmp user was set to guestuser2 authProt sha authPasswd guestuser2password privProt
no-priv with engineid
00:00:00:09:00:10:7b:f2:82:00:00:00 nonvolatile.
```

次に、グループ guestgroup および mygroup のメンバーとして guestuser1 および guestuser2 を設定する例を示します。

```
Console> (enable) set snmp group guestgroup user guestuser1 security-model v3
Snmp group was set to guestgroup user guestuser1 and version v3, nonvolatile.

Console> (enable) set snmp group mygroup user guestuser1 security-model v3
Snmp group was set to mygroup user guestuser1 and version v3, nonvolatile.

Console> (enable) set snmp group mygroup user guestuser2 security-model v3
Snmp group was set to mygroup user guestuser2 and version v3, nonvolatile.
```

次に、ワークステーションで guestuser1 に対する SNMPv3 セットアップを確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser1 ifDescr.0
Enter Authentication password :guestuser1password
Enter Privacy password        :privacypasswd1
ifDescr.1 = sc0
```

次に、ワークステーションで snmpEngineID MIB の guestgroup に対する SNMPv3 セットアップを確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser1 snmpEngineID
Enter Authentication password :guestuser1pasword
Enter Privacy password        :privacypasswd1
snmpEngineID = END_OF_MIB_VIEW_EXCEPTION
```

次に、ワークステーションで公開アクセスに対する SNMPv2c セットアップを確認する例を示します。

```
workstation% getnext -v2c 10.6.4.201 public snmpEngineID
snmpEngineID.0 =
00 00  00 09   00 10  7b f2    82 00  00 00
```

次に、guestgroup のアクセス権を引き上げて、snmpEngineMibView の読み取り権限を設定する例を示します。

```
Console> (enable) set snmp view snmpEngineMibView 1.3.6.1.6.3.10.2.1 included
Snmp view name was set to snmpEngineMibView with subtree 1.3.6.1.6.3.10.2.1 included,
nonvolatile

Console> (enable) set snmp access guestgroup security-model v3 authentication read
snmpEngineMibView
Snmp access group was set to guestgroup version v3 level authentication,
readview snmpEngineMibView, nonvolatile.
```

次に、ワークステーションで guestuser1 に対する SNMPv3 アクセス権を確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser1 snmpEngineID
Enter Authentication password :guestuser1password
Enter Privacy password        :privacypasswd1
snmpEngineID.0 =
00 00  00 09   00 10  7b f2    82 00  00 00
```

次に、guestgroup のアクセス権を削除する例を示します。

```
Console> (enable) clear snmp acc guestgroup security-model v3 authentication
Cleared snmp access guestgroup version v3 level authentication.
```

次に、ワークステーションで guestuser1 のアクセス権が削除されたことを確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser1 ifDescr.1
Enter Authentication password :guestuser1password
Enter Privacy password        :privacypasswd1
Error code set in packet - AUTHORIZATION_ERROR:1.
```

次に、ワークステーションで guestuser2 のアクセス権を確認する例を示します。

```
workstation% getnext -v3 10.6.4.201 guestuser2 ifDescr.1
Enter Authentication password :guestuser2password
Enter Privacy password        :privacypasswd2
REPORT received, cannot recover:
usmStatsUnsupportedSecLevels.0 = 1
```