CHAPTER 22

SNMP の設定

この章では、ML シリーズ カードと SNMP（簡易ネットワーク管理プロトコル）を連動させるための設定方法について説明します。

（注） この章で使用されている全構文と使用方法の情報については、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。

この章の内容は次のとおりです。

- SNMP の概要（p.22-2）
- SNMP の設定（p.22-7）
- SNMP ステータスの表示（p.22-16）

SNMP の概要

SNMP は、マネージャとエージェント間の通信用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（Management Information Base; 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 NMS（Network Management System; ネットワーク管理システム）に組み込むことができます。SNMP を設定するには、マネージャとエージェントの間の関係を定義します。

SNMP エージェントには MIB 変数があり、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することができます。エージェントは、装置のパラメータとネットワーク データの情報リポジトリである MIB からデータを収集します。エージェントは、マネージャのデータ取得またはデータ設定要求に応じることもできます。

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。トラップは、ネットワークの状態を SNMP マネージャに伝えるメッセージです。トラップは、不正なユーザ認証、再起動、リンク 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 接続の終了、ネイバとの接続の切断、または他の重要なイベントを伝えることができます。

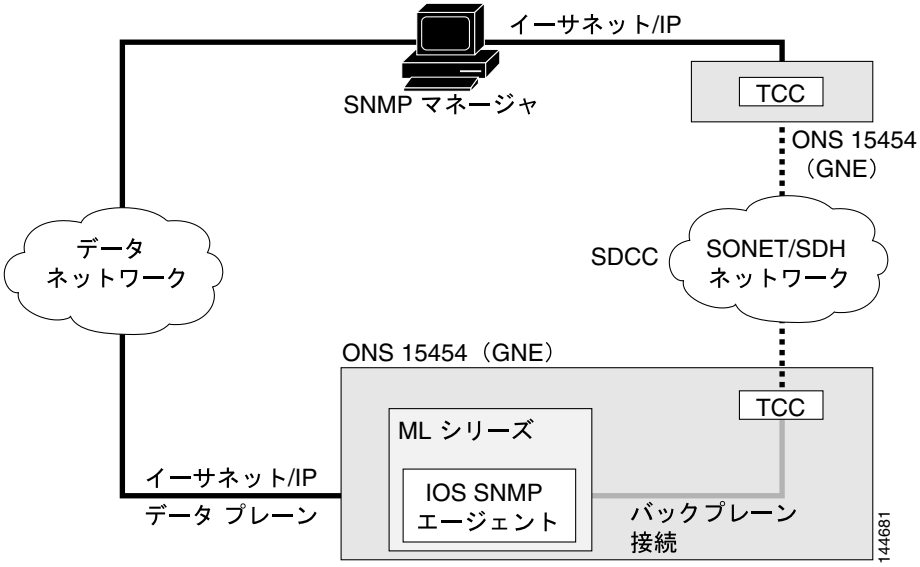
ここでは、次の内容について説明します。

- ML シリーズ カード上の SNMP（p.22-2）
- SNMP のバージョン（p.22-3）
- SNMP マネージャの機能（p.22-4）
- SNMP エージェントの機能（p.22-4）
- SNMP コミュニティ ストリング（p.22-4）
- SNMP による MIB 変数へのアクセス（p.22-5）
- サポート対象の MIB（p.22-5）
- SNMP 通知（p.22-6）

ML シリーズ カード上の SNMP

SNMP は、ONS 15454 SONET/SDH ML シリーズ カード上で、2 種類の方法で動作します。1 つは直接通信する方法です。これも、直接通信、Cisco IOS、データ プレーンを使用して、小さな Catalyst スイッチの SNMP が動作する方法です。ML シリーズ カードと連動する SNMP エージェントも ONS 15454 SONET/SDH および SONET ネットワークを経由して通信できます。両方の方法を 図 22-1 に示します。

図 22-1　ML シリーズ カード上の SNMP の例



ONS 15454 SONET/SDH ノードが ML シリーズ カードの SNMP 通信をリレーする場合、ノードはプロキシ エージェントを使用して get 要求、getNext 要求、set 要求を受信および検証し、ML シリーズ カードに転送します。ML シリーズの要求には、ML シリーズ カードのスロット ID が含まれているので、ONS 15454 SONET/SDH ノードの通常の SNMP 要求と区別できます。ML シリーズ カードからの応答は、ONS 15454 SONET/SDH ノード によって、要求を送信した SNMP エージェントにリレーされます。

SNMP アクセスは、ML シリーズ カードに対し、Cisco IOS データ プレーン イベント、アラーム、統計情報を収集するのに役立ちます。デフォルトでは、ML シリーズ カードで定義された SNMP イベントおよびトラップはすべて TCC2/TCC2P カードの SNMP エージェントに報告されます。TCC2/TCC2P カードの SNMP エージェントがアクティブの場合、このイベントが定義済みの SNMP サーバに送信されます。

SNMP のバージョン

ML シリーズ カードと ONS 15454 SONET/SDH ノードは両方とも SNMP バージョン 1（SNMPv1）と SNMP バージョン 2c（SNMPv2c）をサポートします。定義は次のとおりです。

- SNMPv1 — Request For Comments（RFC; コメント要求）1157 で定義されている、SNMP の完全インターネット標準
- SNMPv2c では、SNMPv2 classic 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変わりましたが、SNMPv2classic のバルク検索機能と改良されたエラー処理機能は残されています。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、さまざまなエラー状態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。これらのエラー状態は、SNMPv1 の単一のエラー コードで報告されます。SNMPv2c のエラー リターン コードはエラー タイプを報告します。

SNMPv1 および SNMPv2C は、次の同じセキュリティ モデルとレベルを使用します。

- レベル — noAuthNoPriv
- 認証 — コミュニティ ストリング

- 暗号化 — なし
- 結果 — 認証にはコミュニティ ストリングの一致を使用

管理ステーションによってサポートされる SNMP バージョンを使用するように、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ので、SNMPv1 プロトコルと SNMPv2 プロトコルを使用する通信をサポートするよう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 の情報を使用して、表 22-1 に示す動作を実行します。

表 22-1　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のある大きなデータ ブロックを取得します。
get-response	NMS から送信された get-request、get-next-request、set-request に応答します。
set-request	特定の変数に値を格納します。
trap	あるイベントが発生したときに、SNMP エージェントから SNMP マネージャに送信される非送信請求メッセージ

1. この動作の場合、SNMP マネージャは正確な変数名を知る必要はありません。順番に検索を実行し、テーブルの中から必要な変数を見つけます。
2. **get-bulk-request** コマンドは、SNMPv2 以降でのみ動作します。

SNMP エージェントの機能

SNMP エージェントは、次の 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。

SNMP エージェントは、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、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、認証エラーが発生した場合などが含まれます。

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 ML シリーズ カードにアクセスするには、NMS 上のコミュニティ ストリング定義が ML シリーズ カード上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致しなければなりません。

コミュニティ ストリングのアトリビュートは、次の 3 つのうちのいずれかです。

- read-only（RO）— 許可し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。

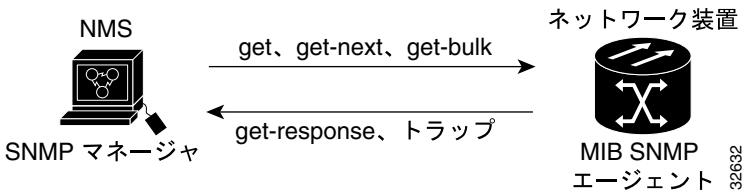
- read-write（RW）— 許可した管理ステーションに、MIB 内のオブジェクトすべてに対する読み取りおよび書き込みアクセス権を与えます。ただし、コミュニティ ストリングへのアクセスは許可しません。
- read-write-all — 許可した管理ステーションに、コミュニティ ストリングも含めた MIB 内のオブジェクトすべてに対する読み取りおよび書き込みアクセス権を与えます。

SNMP による MIB 変数へのアクセス

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 ソフトウェアは、ML シリーズ カードの MIB 変数を使用して、装置の変数を設定し、ネットワーク上の装置をポーリングして特定の情報を入手します。ポーリング結果はグラフとして表示されます。この結果を分析して、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、装置の設定の確認、トラフィック負荷のモデルなどを行うことができます。

図 22-2 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、トラップまたは特定イベントの通知を送信します。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 アドレス追跡などに関する状態を SNMP マネージャに通知します。SNMP エージェントはさらに、get-request、get-next-request、set-request 形式で SNMP マネージャから送信される MIB 関連のクエリに応答します。

図 22-2　SNMP ネットワーク



サポート対象の MIB

サポート対象となる ML シリーズ カードの MIB の完全リストは、使用している ONS ソフトウェア CD の MIBsREADME.txt ファイルにあります。このソフトウェア CD には、必要な MIB モジュールと MIB のロードに関する情報も含まれます。

次の URL の Cisco MIB Locator を使用して、シスコ プラットフォーム、Cisco IOS リリース、およびフィーチャ セットの MIB を指定してダウンロードすることもできます。

http://www.cisco.com/go/mibs

サポート対象となる重要な MIB には次が含まれます。

- Bridge-MIB（RFC 1493）からの Spanning Tree Protocol（STP）のトラップ
- RFC 1157 の認証トラップ
- IF-MIB（RFC 1573）からのイーサネット ポート用リンクアップ トラップとリンクダウン トラップ
- CISCO-PORT-QOS-MIB 拡張による QoS（Quality Of Service）統計のエクスポート

（注） ML シリーズ カードの CISCO-PORT-QOS-MIB 拡張では、Class of Service（CoS; サービス クラス）ベースの QoS 指標がサポートされています。設定オブジェクトは、サポートされません。

SNMP 通知

SNMP を使用すると、ML シリーズ カード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できます。コマンド構文内に、トラップ要求またはインフォーム要求を選択するコマンド オプションが指定されていない場合、キーワード *traps* はトラップ要求、インフォーム要求、またはその両方を表します。SNMP 通知をトラップ要求またはインフォーム要求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 はインフォーム要求をサポートしていません。

レシーバ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、インフォーム要求が再送信されます。このため、インフォーム要求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ので、ML シリーズ カード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は異なり、インフォーム要求は応答を受信するか、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ります。したがって、トラップおよびインフォームを使用する場合は信頼性とリソースのどちらを重視するかの選択が必要となります。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ます。ネットワークのトラフィックまたは ML シリーズ カードのメモリが重要で、通知が必要ない場合は、トラップを使用します。

SNMP の設定

ここでは、ML シリーズ カードに SNMP を設定する方法について説明します。以下の設定情報について説明します。

- SNMP のデフォルト設定（p.22-7）
- SNMP 設定時の注意事項（p.22-7）
- SNMP エージェントのディセーブル化（p.22-8）
- コミュニティ ストリングの設定（p.22-8）
- SNMP グループおよびユーザの設定（p.22-10）
- SNMP 通知の設定（p.22-11）
- 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.22-14）
- SNMP 経由で使用する TFTP サーバの制限（p.22-14）
- SNMP の例（p.22-15）

SNMP のデフォルト設定

表 22-2 にデフォルトの SNMP 設定を示します。

表 22-2　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 コミュニティ ストリング	read-only：パブリック read-write：プライベート read-write-all：シークレット
SNMP トラップ レシーバ	設定なし
SNMP トラップ	TCP 接続のトラップ（tty）以外はディセーブル
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。
SNMP 通知タイプ	タイプを指定しない場合、すべての通知が送信されます。

SNMP 設定時の注意事項

SNMP を設定する場合、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を自動生成し、そのユーザに関連付けられたグループにビューを追加します。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場合については、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。
- 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 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するには、特権 EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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	`no snmp-server`	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	`end`	特権 EXEC モードに戻ります。
ステップ 4	`show running-config`	エントリを確認します。
ステップ 5	`copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

no snmp-server グローバル コンフィギュレーション コマンドは、装置上で実行されているすべてのバージョンをディセーブルにします。SNMP をイネーブルにする特定の 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 ストリングの設定

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 ストリングを使用します。コミュニティ ストリングはパスワードと同様に機能し、ML シリーズ カードのエージェントへのアクセスを許可します。任意で、文字列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。

- 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 アドレスを指定したアクセス リスト
- 特定のコミュニティにアクセス可能な、すべての MIB オブジェクトのサブセットを定義した MIB ビュー
- コミュニティがアクセスできる MIB オブジェクトに対応する読み書きアクセス許可または読み取り専用アクセス許可

ML シリーズ カード上でコミュニティ ストリングを設定するには、特権 EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	**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	**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し、SNMP プロトコルへのアクセスを許可する文字列を指定します。任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 • （任意）**view** *view-name* 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、読み取り専用（**ro**）を指定します。または、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、読み書き（**rw**）を指定します。デフォルトでは、コミュニティ ストリングのアクセス権は、すべてのオブジェクトに対して読み取り専用になっています。 • （任意）*access-list-number* 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	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	（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。 • *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。**permit** 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。 • *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 進表記で入力します。無視するビット位置に 1 を配置します。 アクセス リストは必ず、すべてに対し、暗黙的な拒否ステートメントで終了することに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	エントリを確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルにエントリを保存します。

（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）。

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。

次に、SNMP に comaccess という文字列を割り当て、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 ストリングを使用して ML シリーズ カードの 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。

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

SNMP グループおよびユーザの設定

ML シリーズ カード上のローカルまたはリモート SNMP サーバ エンジンに、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、SNMP グループに新規ユーザを追加できます。

ML シリーズ カード上で SNMP を設定するには、特権 EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	**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	**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*]}	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。 • *engineid-string* は、SNMP のコピー名を含む 24 文字の ID ストリングです。 • **remote** を選択した場合、SNMP のリモート コピーが格納された装置の *ip-address*、およびリモート装置上の任意の UDP ポートを指定します。UDP ポートのデフォルト値は 162 です。
ステップ 3	**snmp-server group** *groupname* {**v1** | **v2c** [**auth** | **noauth** | **priv**]} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	リモート装置に新規の 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。 • セキュリティ モデルを指定します。 — **v1** は、安全性が低いセキュリティ モデルです。 — **v2c** は、安全性が高いセキュリティ モデルです。このモデルを使用すると、インフォーム要求および整数を標準の 2 倍の幅で伝送できます。 （注） **priv** キーワードは、暗号ソフトウェア 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。 • （任意）**read** *readview* には、エージェント内容のみを表示できるビューの名前を示す文字列（64 文字以下）を指定して、入力します。 • （任意）**write** *writeview* には、データを入力してエージェント内容を設定できるビューの名前を示す文字列（64 文字以下）を指定して、入力します。 • （任意）**notify** *notifyview* には、通知、インフォーム要求、またはトラップを指定できるビューの名前を示す文字列（64 文字以下）を指定して、入力します。 • （任意）**access** *access-list* には、アクセス リストの名前を示す文字列（64 文字以下）を指定して、入力します。

	コマンドの説明	目的
ステップ 4	**snmp-server user** *username groupname* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** [**access** *access-list*]}	SNMP グループに新規ユーザを設定します。 • *username* は、エージェントに接続されたホスト上のユーザ名です。 • *groupname* は、ユーザが関連付けられているグループの名前です。 • （任意）ユーザが属するリモート SNMP エンティティを指定するには、**remote** を入力します。このエンティティのホスト名または IP アドレスを指定し、さらに任意の UDP ポート番号を指定します。UDP ポートのデフォルト値は 162 です。 • SNMP バージョン番号（**v1** または **v2c**）を入力します。 • （任意）**access** *access-list* には、アクセス リストの名前を示す文字列（64 文字以下）を指定して、入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	エントリを確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルにエントリを保存します。

SNMP 通知の設定

トラップ マネージャは、通知タイプ（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、ML シリーズ カード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。すべてのトラップをイネーブルにするには、通知タイプ キーワードを指定しないで、**snmp-server enable traps** コマンドを設定します。

表 22-3 に、一般的によく使用され、ML シリーズ カードによってサポートされるトラップの一部を示します。これらのトラップの一部またはすべてをイネーブルにし、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 22-3　ML シリーズ カードの通知タイプ

通知タイプのキーワード	説明
bridge	STP ブリッジ MIB 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。
config-copy	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 トラップを生成します。
rsvp	RSVP フロー変更トラップを生成します。
rtr	SNMP Response Time Reporter（RTR）に対してトラップを生成します。

表 22-3 に示す通知タイプを特定のホストに受信させるには、**snmp-server host** グローバル コンフィギュレーション コマンドをそのホストに対して実行します。

ホストにトラップまたはインフォーム要求を送信するように ML シリーズ カードを設定するには、特権 EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	**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	**snmp-server engineID remote** *ip-address engineid-string*	リモート ホストの IP アドレスおよびエンジン ID を指定します。
ステップ 3	**snmp-server user** *username groupname* **remote** *host* [**udp-port** *port*] {**v1** | **v2c**} [**access** *access-list*]	ステップ 2 で作成したリモート ホストに関連付けるよう SNMP ユーザを設定します。 • *username* は、エージェントに接続されたホスト上のユーザ名です。 • *groupname* は、ユーザが関連付けられているグループの名前です。 • （任意）ユーザが属するリモート SNMP エンティティを指定するには、**remote** を入力します。このエンティティのホスト名または IP アドレスを指定し、さらに任意の UDP ポート番号を指定します。UDP ポートのデフォルト値は 162 です。 • SNMP バージョン番号（**v1** または **v2c**）を入力します。 • （任意）**access** *access-list* には、アクセス リストの名前を示す文字列（64 文字以下）を指定して、入力します。 **（注）** 最初にリモート ホストのエンジン ID を設定しないと、アドレスに対してリモート ユーザを設定できません。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	**snmp-server host** *host-addr* [**traps** | **informs**] [**version** {**1** | **2c**}] *community-string* [**udp-port** *port*] [*notification-type*]	SNMP トラップ動作の受信側を指定します。 • *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）を入力します。 • （任意）SNMP インフォーム要求をホストに送信するには、**informs** を入力します。 • （任意）SNMP バージョン（**1** または **2c**）を指定します。SNMPv1 はインフォーム要求をサポートしていません。 • *community-string* には、通知動作によって送信されたパスワードと同様のコミュニティ ストリングを入力します。 • （任意）**udp-port** *port* には、リモート装置の UDP ポートを入力します。 • （任意）*notification-type* には、表 22-3 に示す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。

	コマンドの説明	目的
ステップ 5	**snmp-server enable traps** *notification-types*	トラップまたはインフォーム要求を送信するよう ML シリーズ カードをイネーブルにし、送信する通知タイプを指定します。通知タイプのリストについては、次を入力します。 **snmp-server enable traps ?** 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	**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。このコマンドにより、インフォーム要求用の送信元 IP アドレスも設定されます。
ステップ 7	**snmp-server queue-length** *length*	（任意）各トラップ ホストが保持できるトラップ メッセージ数（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 です。デフォルトは 10 です。
ステップ 8	**snmp-server trap-timeout** *seconds*	（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 です。デフォルトは 30 秒です。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show running-config**	エントリを確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルにエントリを保存します。

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要求用）のメカニズムをグローバルにイネーブルにします。インフォーム要求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** コマンドを設定して、**snmp-server enable traps** コマンドを使用してインフォーム要求をグローバルにイネーブルにする必要があります。

受信トラップから特定の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。**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、ホストに対して、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。インフォーム要求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。

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、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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	`snmp-server contact` *text*	システム コンタクト ストリングを設定します。 次に、例を示します。 `snmp-server contact Dial System Operator at beeper 21555.`
ステップ 3	`snmp-server location` *text*	システム ロケーション ストリングを設定します。 次に、例を示します。 `snmp-server location Building 3/Room 222`
ステップ 4	`end`	特権 EXEC モードに戻ります。
ステップ 5	`show running-config`	エントリを確認します。
ステップ 6	`copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

SNMP 経由で使用する TFTP サーバの制限

SNMP 経由で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 Trivial File Transfer Protocol（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、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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	`snmp-server tftp-server-list` *access-list-number*	SNMP 経由で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。 *access-list-number* 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	`access-list` *access-list-number* {`deny` | `permit`} *source* [*source-wildcard*]	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。 • *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。**permit** 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。 • *source* には、ML シリーズ カードにアクセスできる TFTP サーバの IP アドレスを入力します。 • （任意）*source-wildcard* には、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 を配置します。 アクセス リストは必ず、すべてに対し、暗黙的な拒否ステートメントで終了することに注意してください。

	コマンドの説明	目的
ステップ 4	`end`	特権 EXEC モードに戻ります。
ステップ 5	`show running-config`	エントリを確認します。
ステップ 6	`copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

SNMP の例

次に、SNMP のすべての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、コミュニティ ストリング「public」を使用し、すべてのオブジェクトに読み取り専用権限でアクセスする許可を SNMP マネージャに与えます。この設定では、ML シリーズ カードはトラップを送信しません。

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

次に、コミュニティ ストリング「public」を使用し、すべてのオブジェクトに読み取り専用権限でアクセスする許可を SNMP マネージャに与える例を示します。ML シリーズ カードは、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 ストリング「public」がトラップとともに送信されます。

```
ML_Series(config)# snmp-server community public
ML_Series(config)# snmp-server host 192.180.1.27 version 2c public
ML_Series(config)# snmp-server host 192.180.1.111 version 1 public
ML_Series(config)# snmp-server host 192.180.1.33 public
```

次に、コミュニティ ストリング 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、オブジェクトへのアクセス権がありません。コミュニティ ストリング「public」を使用し、SNMP 認証失敗トラップが SNMPv2C によってホスト cisco.com に送信されます。

```
ML_Series(config)# snmp-server community comaccess ro 4
ML_Series(config)# snmp-server enable traps snmp authentication
ML_Series(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ています。2 行め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。

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

次に、ML シリーズ カードがコミュニティ 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 に送信できるように設定する例を示します。

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

SNMP ステータスの表示

不正なコミュニティ ストリング エントリ数、エラー数、要求された変数の数を含めた SNMP 入出力の統計情報を表示するには、**show snmp** イネーブル EXEC コマンドを使用します。また、SNMP 情報を表示するには、表 22-4 のイネーブル EXEC コマンドも使用できます。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 22-4　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 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	SNMP 要求のペンディング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 テーブル内の各 SNMP ユーザ名に関する情報を表示します。