CHAPTER 17

SNMP の設定

この章では、ブリッジに Simple Network Management Protocol（SNMP）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各コマンドの構文と使用方法の詳細は、このリリース用の『Cisco Aironet アクセス ポイント / ブリッジ Cisco IOS コマンド リファレンス』、およびリリース 12.2 用の『Cisco IOS Configuration Fundamentals Command Reference』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

SNMP は SNMP のマネージャとエージェント間の通信の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 マネージャは、CiscoWorks などのネットワーク管理システム（NMS）に組み込まれています。エージェントと Management Information Base（MIB; 管理情報ベース）は、ブリッジ上に置かれます。ブリッジ上で SNMP を設定する場合、マネージャとエージェント間の関連性を定義します。

SNMP エージェントには、SNMP マネージャが値を要求または変更できる MIB 変数が格納されます。マネージャはエージェントから値を取得し、またエージェントに値を保存します。エージェントは、デバイス パラメータとネットワーク データの情報のリポジトリである 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。

エージェントは要請されていないトラップをマネージャに送信できます。トラップは SNMP マネージャにネットワークの状況を警告するメッセージです。トラップは不適切なユーザ認証や、再起動、リンク ステータス（起動または停止）、MAC アドレスの追跡、TCP 接続の終了、近接との接続の損失、またはその他の重要なイベントを表す場合があります。

この項では次の概念を説明します。

SNMP 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ます。

- SNMPv1：Simple Network Management Protocol。RFC 1157 で定義される完全なインターネット規格。
- SNMPv2C には、次の種類があります。
  - SNMPv2：Simple Network Management Protocol のバージョン 2。RFC 1902 ～ 1907 で定義されるドラフト インターネット規格。
  - SNMPv2C：SNMPv2 のコミュニティ ベースの管理フレームワーク。RFC 1901 で定義される試用段階のインターネット プロトコル。

SNMPv2C はパーティ ベースの管理およびセキュリティ フレームワークの SNMPvClassic を、SNMPv2Classic の一括検索と改良エラー処理を維持しながら、コミュニティ ベースの管理フレームワークの SNMPv2C に置き換えたものです。

SNMPv1 と SNMPv2C はいずれもコミュニティ ベースのセキュリティ形式を使用します。エージェントの MIB にアクセスできるマネージャのコミュニティは、IP アドレス アクセス制御リストとパスワードで定義されます。

SNMPv2C では、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報告機能が使用されます。一括検索メカニズムは、テーブルと大量の情報を取得して、必要なラウンドトリップの回数を最小限に抑えます。SNMPv2C の改良エラー処理機能は、エラー コードの拡張によりエラー状況の種類を区別します。これらの状況は SNMPv1 の 1 つのエラーで報告されます。エラー リターン コードにより、エラーのタイプが報告されます。

SNMP エージェントは、管理ステーションでサポートされる SNMP のバージョンを使用するように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対話できるため、SNMPv1 プロトコルを使用する管理ステーションや、SNMPv2 プロトコルを使用する管理ステーションとの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 内の情報を使用して、表 17-1 に説明する操作を実行します。

表 17-1　SNMP の操作

操作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の特定の変数から値を 1 つ取得します。[1]
get-bulk-request[2]	テーブル内の複数行など、小さなデータ ブロックを数多く送信するような場合に、大きなブロックでデータを取得します。
get-response	NMS が送信した get-request、get-next-request、set-request 要求に返答します。
set-request	特定の変数に値を保存します。
trap	あるイベントが発生したときに、SNMP エージェントが SNMP マネージャに送信する非要請メッセージ。

1. この操作により、SNMP マネージャは正確な変数名を知る必要がなくなります。テーブルから必要な変数を見つけるために、逐次検索が実行されます。
2. **get-bulk** コマンドは、SNMPv2 でのみ機能します。

SNMP エージェントの機能

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

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

また、SNMP エージェントは非要請トラップ メッセージを送信して、エージェントで重要なイベントが発生したことを NMS に伝えます。トラップの状況の例として、ポートまたはモジュールの起動または停止、スパニングツリー トポロジの変更、認証の失敗などが含まれます。

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 オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS がブリッジにアクセスするために、NMS のコミュニティ ストリングの定義は少なくともブリッジの 3 つのコミュニティ ストリング定義のうちの 1 つと一致していなければなりません。

コミュニティ ストリングに次の属性のいずれかを指定できます。

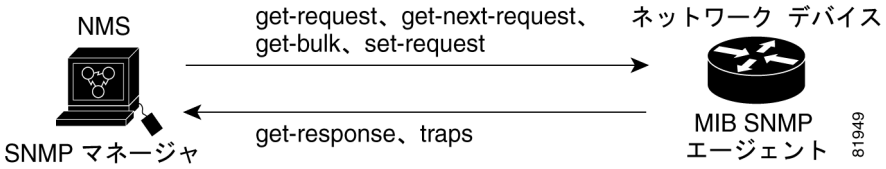
- 読み取り専用：許可された管理ステーションへの読み取りアクセスを、コミュニティ ストリングを除く MIB のすべてのオブジェクトに許可しますが、書き込みアクセスは許可しません。
- 読み取り / 書き込み：許可された管理ステーションへの読み取りおよび書き込みアクセスを、MIB のすべてのオブジェクトに許可しますが、コミュニティ ストリングには許可しません。

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 2000 ソフトウェアは、ブリッジの MIB 変数を使用して、ネットワーク上のデバイスで特定の情報をポーリングします。ポーリングの結果をグラフで表示して、分析し、インターネットワーキング問題のトラブルシューティング、ネットワークのパフォーマンス向上、デバイスの設定の確認、トラフィック負荷の監視などに使用できます。

図 17-1 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 マネージャにトラップ（特定のイベントの通知）を送信することができ、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、不適切なユーザ認証、再起動、リンク ステータス（起動または停止）、MAC アドレスの追跡などの、ネットワーク上の状況を SNMP マネージャに警告するメッセージです。また、SNMP エージェントは、SNMP マネージャが *get-request*、*get-next-request*、および *set-request* の形式で送信する、MIB 関連のクエリーに応答します。

図 17-1　SNMP ネットワーク



サポートされる MIB とそのアクセス方法は、付録 C「サポートされている MIB」を参照してください。

SNMP の設定

この項では、ブリッジで 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。

デフォルトの SNMP 設定

表 17-2 に、デフォルトの SNMP 設定を示します。

表 17-2　デフォルトの SNMP 設定

機能	デフォルト設定
SNMP エージェント	無効
SNMP コミュニティ ストリング	設定されていません。
SNMP トラップ レシーバー	設定されていません。
SNMP トラップ	有効なトラップなし。

SNMP エージェントの有効化

SNMP を有効にするための特定の IOS コマンドはありません。最初に入力したグローバル設定コマンド **snmp-server** を使用すると SNMPv1 と SNMPv2 が有効になります。

また、Web ブラウザ インターフェイスの SNMP Properties ページで SNMP を有効にすることもできます。Web ブラウザ インターフェイスで SNMP を有効にする場合、アクセス ポイントは自動的に、IEEE802dot11 MIB 読み取り専用アクセスで、*public* と呼ばれるコミュニティ ストリングを生成します。

コミュニティ ストリングの設定

SNMP コミュニティ ストリングを使用して、SNMP マネージャとエージェント間の関連性を定義します。コミュニティ ストリングはパスワードと同様に機能し、ブリッジ上のエージェントへのアクセスを許可します。

オプションで、ストリングに関連した次の特性の 1 つまたは複数を指定できます。

- SNMP マネージャの IP アドレスのアクセス リスト。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することが許可された SNMP マネージャが対象です。
- MIB ビュー。特定のコミュニティにアクセスできるすべての MIB オブジェクトを定義します。
- コミュニティにアクセスできる MIB オブジェクトに対する読み取り / 書き込み権限、または読み取り専用の権限。

（注）　現在の IOS MIB エージェント実装では、デフォルトのコミュニティ ストリングは、インターネット MIB オブジェクト サブツリーに対するものです。IEEE802dot11 は、MIB オブジェクト ツリーの別のブランチのもとにあるので、IEEE802dot11 MIB 上の別のコミュニティ ストリングとビュー、あるいは、MIB オブジェクト ツリー内の ISO オブジェクト上の共通のビューとコミュニティ ストリングのいずれかを有効にする必要があります。ISO は、IEEE（IEEE802dot11）およびインターネットの共通の親ノードです。この MIB エージェントの動作は、IOS ソフトウェアを実行していないアクセス ポイントでの MIB エージェントの動作とは異なります。

イネーブル EXEC モードから、次の手順に従ってブリッジにコミュニティ ストリングを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードを開始します。
ステップ 2	**snmp-server community** *string* [*access-list-number*] [**view** *mib-view*] [**ro** | **rw**]	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文字列を指定します。任意の長さの 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。 • （オプション）*access-list-number* には、1 ～ 99 および 1300 ～ 1999 の標準的な IP アクセス リスト番号を入力します。 • （オプション）**view** *mib-view* には、**ieee802dot11** など、このコミュニティがアクセスできる MIB ビューを指定します。IEEE ビューを通じて標準 IEEE 802.11 MIB オブジェクトにアクセスする **snmp-server view** コマンドの使用方法は、「snmp-server view コマンドの使用」の項（P.17-9）を参照してください。 • （オプション）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**）を指定し、許可された管理ステーションを使用して MIB オブジェクトを取得し、修正する場合は、読み取り / 書き込み（**rw**）を指定します。デフォルトでは、コミュニティ ストリングは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。 （注）　IEEE802dot11 MIB にアクセスするには、IEEE802dot11 MIB 上の別のコミュニティ ストリングとビュー、あるいは、MIB オブジェクト ツリー内の ISO オブジェクト上の共通のビューとコミュニティ ストリングを有効にする必要があります。

	コマンド	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	（オプション）ステップ 2 で IP の標準アクセス リストの番号を指定している場合は、このコマンドを必要な回数だけ繰り返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、条件に一致する場合にアクセスを拒否します。**permit** キーワードは、条件に一致する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することが許可された SNMP マネージャの IP アドレスを入力します。 • （オプション）*source-wildcard* には、ソース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ワイルドカードを指定します。 アクセス リストは常に、すべてを暗黙的に否定する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**	イネーブル EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

SNMP コミュニティのアクセスを無効にするには、そのコミュニティのコミュニティ ストリングをヌル文字列に設定します（コミュニティ ストリングに値を入力しない）。特定のコミュニティ ストリングを削除する場合は、グローバル設定コマンド **no snmp-server community** *string* を使用します。

次の例は、コミュニティ ストリング *open* と *ieee* を SNMP に割り当てる方法、両方に対する読み取り / 書き込みアクセスを許可する方法、*open* が非 IEEE802dot11-MIB オブジェクトのクエリーに対するコミュニティ ストリングであり、*ieee* が IEEE802dot11 MIB オブジェクトのクエリーに対するコミュニティ ストリングであることを指定する方法を示します。

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

トラップ マネージャの設定とトラップの有効化

トラップ マネージャは、トラップを受信し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ブリッジ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ておらず、トラップは発行されません。

この IOS リリースを実行するブリッジには、トラップ マネージャを無制限に設定できます。コミュニティ ストリングの長さは任意です。

表 17-3 では、サポートされるブリッジのトラップ（通知タイプ）について説明しています。これらのトラップの一部またはすべてを有効にして、そのトラップ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 17-3　通知タイプ

通知タイプ	説明
authenticate-fail	認証の失敗のトラップを有効にします。
config	SNMP 設定変更のトラップを有効にします。
deauthenticate	クライアント デバイスの認証取り消しのトラップを有効にします。
disassociate	クライアント デバイスのアソシエーション解除のトラップを有効にします。
dot11-qos	QoS 変更のトラップを有効にします。
entity	SNMP のエンティティ変更のトラップを有効にします。
envmon temperature	無線の温度を監視するためのトラップを有効にします。このトラップは、ブリッジの無線温度が作動範囲（摂氏 55 ～ -33 度、華氏 131 ～ -27.4 度）の限界に近づくと送信されます。
snmp	SNMP イベントのトラップを有効にします。
syslog	syslog トラップを有効にします。
wlan-wep	WEP トラップを有効にします。

tty や **udp-port** などの一部の通知タイプは、グローバル設定コマンド **snmp-server enable** で制御できません。これらの通知タイプは、常に有効です。表 17-3 に示す通知タイプを受信する場合は、特定のホストにグローバル設定コマンド **snmp-server host** を使用します。

イネーブル EXEC モードから、次の手順に従ってホストにトラップを送信するようにブリッジを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c**}} *community-string* *notification-type*	トラップ メッセージの受信者を指定します。 • *host-addr* には、（ターゲットの受信者）ホストの名前またはアドレスを指定します。 • ホストに SNMP トラップを送信する場合は、**traps**（デフォルト）を指定します。ホストに SNMP 情報を送信する場合は、**informs** を指定します。 • サポートする SNMP バージョンを指定します。informs を指定した場合は、デフォルトのバージョン 1 は使用できません。 （注）　**version 3** キーワード（SNMPv3）は、コマンドラインのヘルプ文字列には表示されますが、サポートされません。 • *community-string* には、通知操作で送信する文字列を指定します。この文字列は **snmp-server host** コマンドを使用して設定できますが、**snmp-server host** コマンドを使用する前に、**snmp-server community** コマンドを使用してこの文字列を定義することをお勧めします。 • *notification-type* には、表 17-3（P. 17-8）内のキーワードを使用します。

	コマンド	目的
ステップ 3	**snmp-server enable traps** *notification-types*	ブリッジで特定のトラップの送信を有効にします。トラップのリストは、表 17-3（P. 17-8）を参照してください。 複数のタイプのトラップを有効にする場合、各トラップ タイプに **snmp-server enable traps** コマンドを個別に発行します。
ステップ 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

特定のホストに対し、トラップの受信を無効にするには、グローバル設定コマンド **no snmp-server host** *host* を使用します。特定のトラップ タイプを無効にするには、グローバル設定コマンド **no snmp-server enable traps** *notification-types* を使用します。

エージェントの連絡先と場所の情報の設定

イネーブル EXEC モードから、次の手順に従って SNMP エージェントのシステムの連絡先と場所を設定し、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します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードを開始します。
ステップ 2	**snmp-server contact** *text*	システムの連絡先文字列を設定します。 例： `snmp-server contact Dial System Operator at beeper 21555.`
ステップ 3	**snmp-server contact** *text*	システムの場所の文字列を設定します。 例： `snmp-server location Building 3/Room 222`
ステップ 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（オプション）コンフィギュレーション ファイルに入力内容を保存します。

snmp-server view コマンドの使用

グローバル設定モードで **snmp-server view** コマンドを使用して、IEEE ビューおよび dot11 読み取り / 書き込みコミュニティ ストリングを通じて、標準 IEEE 802.11 MIB オブジェクトにアクセスします。

次の例は、IEEE ビューと dot11 読み取り / 書き込みコミュニティ ストリングを有効にする方法を示しています。

```
bridge(config)# snmp-server view ieee ieee802dot11 included
bridge(config)# snmp-server community dot11 view ieee RW
```

SNMP の例

次の例は、SNMPv1 および SNMPv2C を有効にする方法を示しています。この設定により、SNMP マネージャはコミュニティ ストリング *public* を使用した読み取り専用権限ですべてのオブジェクトへのアクセスが許可されます。この設定でブリッジがトラップを送信することはありません。

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

次の例は、コミュニティ ストリング *open* と *ieee* を SNMP に割り当てる方法、両方に対する読み取り / 書き込みアクセスを許可する方法、*open* が非 IEEE802dot11-MIB オブジェクトのクエリーに対するコミュニティ ストリングであり、*ieee* が IEEE802dot11 MIB オブジェクトのクエリーに対するコミュニティ ストリングであることを指定する方法を示します。

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

次の例は、コミュニティ ストリング *public* を使用した読み取り専用権限ですべてのオブジェクトへのアクセスを SNMP マネージャに許可する方法を示します。ブリッジはまた SNMPv1 を使用してホスト 192.180.1.111 と 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に設定トラップを送信します。コミュニティ ストリング *public* はトラップで送信されます。

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

次の例は、すべてのオブジェクトが *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方法を示しています。他の SNMP マネージャはオブジェクトにアクセスできません。SNMP 認証失敗トラップはコミュニティ ストリング *public* を使用して、SNMPv2C がホスト *cisco.com* に送信します。

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

次の例は、エンティティ MIB トラップをホスト *cisco.com* に送信する方法を示しています。コミュニティ ストリングは制限されます。最初の行で、ブリッジはそれまでに有効になったトラップ以外にエンティティ MIB トラップを送信できます。2 行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対してそれまでに発行されたすべての **snmp-server host** コマンドを無効にします。

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

次の例は、ブリッジがコミュニティ ストリング *public* を使用して、ホスト *myhost.cisco.com* にすべてのトラップを送信する動作を有効にする方法を示します。

```
bridge(config)# snmp-server enable traps
bridge(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 ストリングのエントリ数、エラー、要求された変数など SNMP の入出力の統計を表示する場合は、**show snmp** イネーブル EXEC コマンドを使用します。この表示のフィールドについては、『Cisco IOS Configuration Fundamentals Command Reference for Release 12.2』を参照してください。