



CHAPTER 5

スイッチの管理

この章では、Catalyst 3750 Metro スイッチを管理するための 1 回かぎりの手順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。

- 「システム日時の管理」(P.5-1)
- 「システム名およびプロンプトの設定」(P.5-14)
- 「バナーの作成」(P.5-17)
- 「MAC アドレス テーブルの管理」(P.5-19)
- 「ARP テーブルの管理」(P.5-31)

システム日時の管理

Network Time Protocol (NTP; ネットワーク タイム プロトコル) などの自動設定方式、または手動設定方式を使用して、スイッチのシステム日時を管理します。



(注) ここで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Configuration Fundamentals Command Reference, Release 12.2』を参照してください。

ここでは、次の設定情報について説明します。

- 「システム クロックの概要」(P.5-1)
- 「NTP の概要」(P.5-2)
- 「NTP の設定」(P.5-3)
- 「手動での日時の設定」(P.5-11)

システム クロックの概要

時刻サービスの中核となるのはシステム クロックです。このクロックはシステムがスタートアップした瞬間から稼動し、日時を常時トラッキングします。

システム クロックは、次のソースにより設定できます。

- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供します。

- ユーザの **show** コマンド
- ログおよびデバッグ メッセージ

システム クロックは、**Universal Time Coordinated (UTC; 協定世界時)** (別名 **Greenwich Mean Time (GMT; グリニッジ標準時)**) に基づいてシステム内部の時刻を常時トラッキングします。ローカルの時間帯および夏時間に関する情報を設定することにより、時刻がローカルの時間帯に応じて正確に表示されるようになります。

システム クロックは、時刻に**信頼性**があるかどうか (つまり、信頼できると見なされる時刻源によって時刻が設定されているか) を常時トラッキングします。信頼性のない場合は、時刻は表示目的でだけ使用され、再配信されません。設定の詳細については、「**手動での日時の設定 (P.5-11)**」を参照してください。

NTP の概要

NTP は、ネットワーク上のデバイス間の時刻の同期化を目的に設計されています。NTP は **User Datagram Protocol (UDP; ユーザ データグラム プロトコル)** で稼動し、UDP は IP 上で稼動します。NTP は RFC 1305 に規定されています。

NTP ネットワークは通常、電波時計やタイム サーバに接続されたアトミック クロックなど、信頼できる時刻源からその時刻を取得します。そのあと、NTP はネットワークにこの時刻を配信します。NTP はきわめて効率的で、1 分間に 1 パケットを使用するだけで、2 台のデバイスを 1 ミリ秒以内に同期化できます。

NTP は、**ストラタム (層)** という概念を使用して、信頼できる時刻源とデバイスが離れている NTP ホップを記述します。ストラタム 1 タイム サーバには、電波時計またはアトミック クロックが直接接続されており、ストラタム 2 タイム サーバは、NTP を使用してストラタム 1 タイム サーバから時刻を取得します (以降のストラタムも同様です)。NTP が稼動するデバイスは、時刻源として、NTP を使用して通信するストラタム番号が最小のデバイスを自動的に選択します。この方法によって、NTP 時刻配信の自動編成型ツリーが効率的に構築されます。

NTP では、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

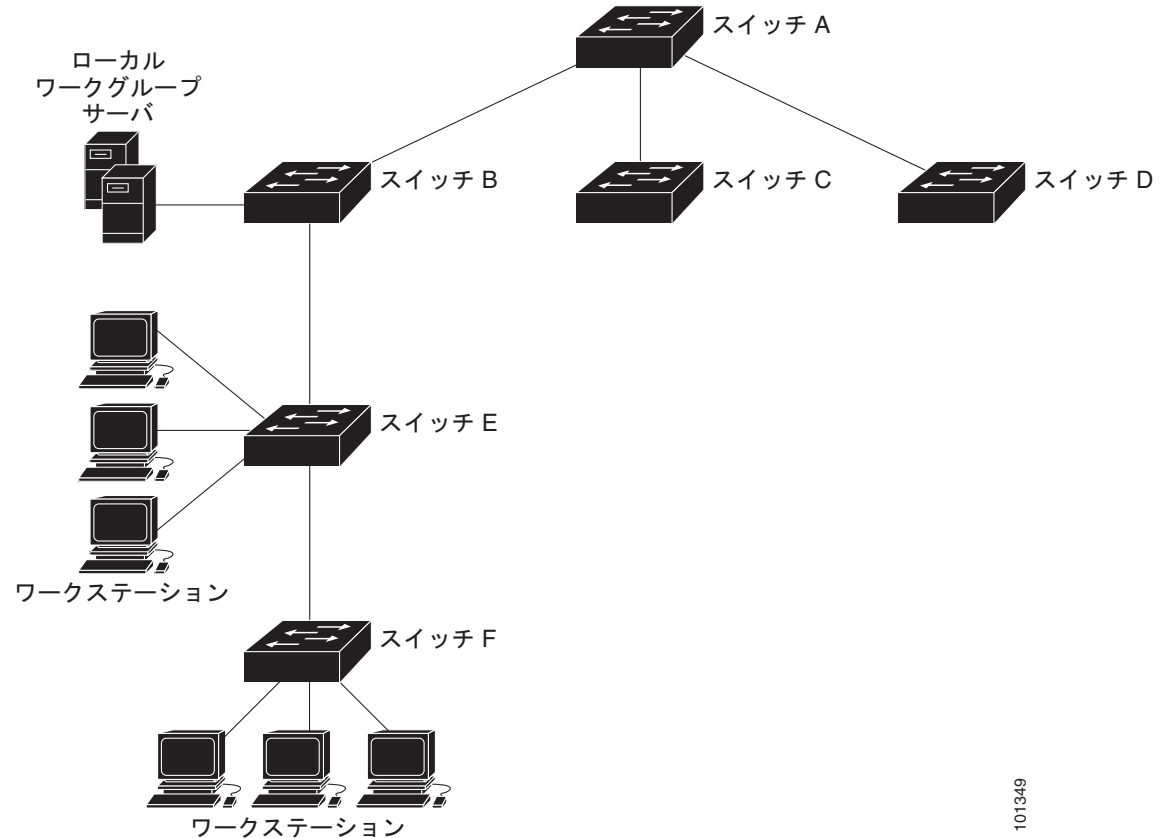
通常、NTP が稼動するデバイス間の通信 (**アソシエーション**) はスタティックに設定されます。各デバイスには、アソシエーションを作成する必要があるすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確なタイムキーピングが可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、この場合は、情報の流れは一方向にかぎられます。

デバイス上で維持される時刻は、重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤って、または意図的に設定されることを防止してください。アクセスリストを使用して制限する方式および暗号化認証メカニズムの、2 種類のメカニズムを使用できます。

シスコの NTP ではストラタム 1 サービスをサポートしていないので、電波時計またはアトミック クロックに接続できません。ネットワークの時刻サービスは、IP インターネット上のパブリック NTP サーバから取得することを推奨します。

図 5-1 に、NTP を使用する一般的なネットワーク例を示します。スイッチ A は、NTP サーバ モードで設定したスイッチ B、C、D の NTP マスターです。スイッチ B、C、D とスイッチ A との間にはサーバアソシエーションが設定されています。スイッチ E は、アップストリーム スイッチ (スイッチ B) およびダウンストリーム スイッチ (スイッチ F) の NTP ピアとして設定されています。

図 5-1 一般的な NTP ネットワークの設定



101349

ネットワークがインターネットから切り離されている場合、シスコの NTP によって、実際には、他の方法で時刻が決定されているにもかかわらず、デバイスが NTP を使用して同期しているように動作できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

複数の時刻源がある場合は、NTP は常に、より信頼性があると見なされます。NTP の時刻は、他の方法による時刻を無効にします。

自社のホスト システムに NTP ソフトウェアを組み込んでいるメーカーが数社あり、また、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホスト システムも時間が同期化されます。

NTP の設定

スイッチはハードウェアサポート クロックを備えておらず、外部 NTP ソースが利用できないときに、ピアが自身を同期化するための NTP マスター クロックとして機能することはできません。これらのスイッチは、カレンダーに対するハードウェア サポートも備えていません。そのため、**ntp update-calendar** および **ntp master** グローバル コンフィギュレーション コマンドが使用できません。ここでは、次の設定情報について説明します。

- 「NTP のデフォルト設定」(P.5-4)
- 「NTP 認証の設定」(P.5-4)
- 「NTP アソシエーションの設定」(P.5-5)

- 「NTP ブロードキャスト サービスの設定」 (P.5-7)
- 「NTP アクセス制限の設定」 (P.5-8)
- 「NTP パケット用の送信元 IP アドレスの設定」 (P.5-10)
- 「NTP 設定の表示」 (P.5-11)

NTP のデフォルト設定

表 5-1 に、NTP のデフォルト設定を示します。

表 5-1 NTP のデフォルト設定

機能	デフォルト設定
NTP 認証	ディセーブル。認証鍵は指定されていません。
NTP ピアまたはサーバ アソシエーション	未設定。
NTP ブロードキャスト サービス	ディセーブル。どのインターフェイスも NTP ブロードキャスト パケットを送受信しません。
NTP アクセス制限	アクセス コントロールは指定されていません。
NTP パケット送信元 IP アドレス	送信元アドレスは、発信インターフェイスによって決定されます。

NTP は、すべてのインターフェイスでデフォルトでイネーブルに設定されています。すべてのインターフェイスは、NTP パケットを受信します。

NTP 認証の設定

この手順は、NTP サーバの管理者と調整する必要があります。この手順で設定する情報は、時刻を NTP サーバと同期化するためにスイッチが使用するサーバに対応している必要があります。

セキュリティ目的で他のデバイスとのアソシエーション（正確なタイムキーピングを行う NTP 稼動デバイス間の通信）を認証するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>ntp authenticate</code>	デフォルトではディセーブルに設定されている NTP 認証機能をイネーブルにします。

	コマンド	目的
ステップ 3	<code>ntp authentication-key number md5 value</code>	<p>認証鍵を定義します。デフォルトでは何も定義されていません。</p> <ul style="list-style-type: none"> <code>number</code> には、鍵の番号を指定します。指定できる範囲は 1 ~ 4294967295 です。 <code>md5</code> は、Message Digest Algorithm 5 (MD5; メッセージダイジェストアルゴリズム 5) を使用してメッセージ認証サポートが行われるように指定します。 <code>value</code> には、鍵に対する 8 文字までの任意のストリングを入力します。 <p>スイッチとデバイスの双方がいずれかの認証鍵を持ち、<code>ntp trusted-key key-number</code> コマンドによって鍵番号が指定されていないかぎり、スイッチはデバイスと同期化しません。</p>
ステップ 4	<code>ntp trusted-key key-number</code>	<p>1 つまたは複数の鍵番号 (ステップ 3 で定義したもの) を指定します。ピア NTP デバイスは、このスイッチと同期化するため、このスイッチへの NTP パケット内にこの鍵番号を設定しなければなりません。</p> <p>デフォルト設定では、信頼される鍵は定義されていません。</p> <p><code>key-number</code> には、ステップ 3 で定義された鍵を指定します。</p> <p>このコマンドは、スイッチが、信頼されていないデバイスと誤って同期化することを防ぎます。</p>
ステップ 5	<code>end</code>	特権 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。

NTP 認証をディセーブルにするには、`no ntp authenticate` 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。認証鍵を削除するには、`no ntp authentication-key number` 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。デバイス ID の認証をディセーブルにするには、`no ntp trusted-key key-number` 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、NTP パケットに認証鍵 42 を設定しているデバイスとだけ同期するようにスイッチを設定する例を示します。

```
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 42 md5 aNiceKey
Switch(config)# ntp trusted-key 42
```

NTP アソシエーションの設定

NTP アソシエーションは、ピア アソシエーション (スイッチを他のデバイスに同期化するか、スイッチに対して他のデバイスを同期化させるかのどちらかが可能) に設定することも、サーバ アソシエーション (スイッチを他のデバイスに同期化させるだけで、その逆はできない) に設定することもできます。

別のデバイスとの NTP アソシエーションを形成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>ntp peer ip-address [version number] [key keyid] [source interface] [prefer]</code> または <code>ntp server ip-address [version number] [key keyid] [source interface] [prefer]</code>	スイッチのシステム クロックをピアに同期化するか、ピアによって同期化する（ピア アソシエーション）ように設定します。 または スイッチのシステム クロックをタイム サーバによって同期化する（サーバ アソシエーション）ように設定します。 ピアまたはサーバ アソシエーションはデフォルトでは定義されていません。 <ul style="list-style-type: none"> ピア アソシエーションの <i>ip-address</i> には、クロックの同期化を行う、または同期化の対象となるピアの IP アドレスを指定します。サーバ アソシエーションでは、クロックの同期化を行うタイム サーバの IP アドレスを指定します。 （任意）<i>number</i> には、NTP のバージョン番号を指定します。指定できる範囲は 1～3 です。デフォルトではバージョン 3 が選択されています。 （任意）<i>keyid</i> には、<code>ntp authentication-key</code> グローバル コンフィギュレーション コマンドで定義された認証鍵を入力します。 （任意）<i>interface</i> には、IP の送信元アドレスを取得するインターフェイスを指定します。デフォルトでは、送信元 IP アドレスは発信インターフェイスから取得します。 （任意）prefer キーワードを指定すると、このピアまたはサーバが同期化を行う優先ピアまたはサーバになります。このキーワードは、ピアとサーバ間の切り替えを減らします。
ステップ 3	<code>end</code>	特権 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。

アソシエーションの一端しか設定する必要がありません。もう一方のデバイスには自動的にアソシエーションが設定されます。デフォルトの NTP バージョン（バージョン 3）を使用していて、同期化が発生しない場合は、NTP のバージョン 2 を使用してください。インターネット上の多くの NTP サーバは、バージョン 2 で稼動しています。

ピアまたはサーバ アソシエーションを削除するには、`no ntp peer ip-address` または `no ntp server ip-address` 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、NTP バージョン 2 を使用して、IP アドレス 172.16.22.44 のピアのクロックにシステム クロックを同期化するようにスイッチを設定する例を示します。

```
Switch(config)# ntp server 172.16.22.44 version 2
```

NTP ブロードキャスト サービスの設定

通常、NTP が稼動するデバイス間の通信（アソシエーション）はスタティックに設定されます。各デバイスには、アソシエーションを作成する必要があるすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確なタイムキーピングが可能になります。ただし、LAN 環境では、代わりに IP ブロードキャストメッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方方向にかぎられます。

ルータのようにネットワーク上で時刻情報をブロードキャストする NTP ブロードキャスト サーバがある場合、スイッチはインターフェイスごとに NTP ブロードキャスト パケットを送受信できます。スイッチは NTP ブロードキャスト パケットをピアへ送信できるので、ピアはそのスイッチに同期化できます。スイッチは、NTP ブロードキャスト パケットを受信して自身のクロックを同期化することもできます。ここでは、NTP ブロードキャスト パケットの送信と受信の両方の手順について説明します。

NTP ブロードキャスト パケットをピアに送信して、ピアが自身のクロックをスイッチに同期化するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>interface interface-id</code>	NTP ブロードキャスト パケットを送信するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ntp broadcast [version number] [key keyid] [destination-address]</code>	NTP ブロードキャスト パケットをピアに送信するインターフェイスをイネーブルにします。 デフォルトでは、この機能はすべてのインターフェイスでディセーブルです。 <ul style="list-style-type: none"> （任意）<i>number</i> には、NTP のバージョン番号を指定します。指定できる範囲は 1 ～ 3 です。バージョンを指定しなかった場合は、バージョン 3 が使用されます。 （任意）<i>keyid</i> には、ピアにパケットを送信するときに使用する認証鍵を指定します。 （任意）<i>destination-address</i> には、スイッチにクロックを同期化しているピアの IP アドレスを指定します。
ステップ 4	<code>end</code>	特権 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。
ステップ 7		次の手順で説明するように、接続されているピアが NTP ブロードキャスト パケットを受信するように設定します。

インターフェイスによる NTP ブロードキャスト パケットの送信をディセーブルにするには、`no ntp broadcast` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが NTP バージョン 2 パケットを送信するように設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ntp broadcast version 2
```

接続したピアから NTP ブロードキャスト パケットを受信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>interface interface-id</code>	NTP ブロードキャスト パケットを受信するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ntp broadcast client</code>	インターフェイスが NTP ブロードキャスト パケットを受信できるようにします。 デフォルトでは、インターフェイスは NTP ブロードキャスト パケットを受信しません。
ステップ 4	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	<code>ntp broadcastdelay microseconds</code>	(任意) スイッチと NTP ブロードキャスト サーバとの間の予測される往復遅延を変更します。 デフォルトは 3000 マイクロ秒です。指定できる範囲は 1 ~ 999999 です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	設定を確認します。
ステップ 8	<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。

ポートが NTP ブロードキャスト パケットを受信する機能をディセーブルにするには、**no ntp broadcast client** インターフェイス コンフィギュレーション コマンドを使用します。予測される往復遅延をデフォルト設定に変更するには、**no ntp broadcastdelay** 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、ポートが NTP ブロードキャスト パケットを受信するように設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ntp broadcast client
```

NTP アクセス制限の設定

以降で説明するように、2つのレベルで NTP アクセスを制御できます。

- ・「アクセス グループの作成と基本 IP アクセス リストの割り当て」(P.5-8)
- ・「特定のインターフェイスでの NTP サービスのディセーブル化」(P.5-10)

アクセス グループの作成と基本 IP アクセス リストの割り当て

アクセス リストを使用して NTP サービスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>ntp access-group {query-only serve-only serve peer} access-list-number</code>	<p>アクセス グループを作成し、基本 IP アクセス リストを割り当てます。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • query-only : NTP 制御クエリーにかぎり許可します。 • serve-only : 時刻要求にかぎり許可します。 • serve : 時刻要求と NTP 制御クエリーは許可しますが、スイッチがリモート デバイスと同期化することは許可しません。 • peer : 時刻要求と NTP 制御クエリーを許可し、スイッチがリモート デバイスと同期化することを許可します。 <p><i>access-list-number</i> には、1 ~ 99 の範囲で標準の IP アクセス リスト番号を入力します。</p>
ステップ 3	<code>access-list access-list-number permit source [source-wildcard]</code>	<p>アクセス リストを作成します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定した番号を入力します。 • permit キーワードを入力すると、条件が一致した場合にアクセスを許可します。 • <i>source</i> には、スイッチへのアクセスが許可されたデバイスの IP アドレスを入力します。 • (任意) <i>source-wildcard</i> には、送信元に適用するワイルドカードビットを入力します。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ 4	<code>end</code>	特権 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。

アクセス グループのキーワードは、最小の制限から最大の制限に、次の順序でスキャンされます。

1. **peer** : 時刻要求と NTP 制御クエリーを許可し、さらに、スイッチがアクセス リストの基準を満たすアドレスを持つデバイスと同期化することを許可します。
2. **serve** : 時刻要求と NTP 制御クエリーを許可しますが、スイッチがアクセス リストの基準を満たすアドレスを持つデバイスと同期化することを許可しません。
3. **serve-only** : アクセス リストの基準を満たすアドレスを持つデバイスからの時刻要求にかぎり許可します。
4. **query-only** : アクセス リストの基準を満たすアドレスを持つデバイスからの NTP 制御クエリーにかぎり許可します。

複数のアクセス タイプについて送信元 IP アドレスがアクセス リストに一致する場合は、最初のタイプが認可されます。アクセス グループが指定されなかった場合は、すべてのアクセス タイプがすべてのデバイスに認可されます。いずれかのアクセス グループが指定されている場合は、指定されたアクセス タイプにかぎり認可されます。

スイッチ NTP サービスに対するアクセス コントロールを削除するには、**no ntp access-group {query-only | serve-only | serve | peer}** 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、スイッチがアクセス リスト 99 からのピアに同期化できるように設定する例を示します。ただし、スイッチはアクセス リスト 42 に対してはアクセスを制限し、時刻要求にかぎり許可します。

```
Switch# configure terminal
Switch(config)# ntp access-group peer 99
Switch(config)# ntp access-group serve-only 42
Switch(config)# access-list 99 permit 172.20.130.5
Switch(config)# access list 42 permit 172.20.130.6
```

特定のインターフェイスでの NTP サービスのディセーブル化

NTP サービスは、すべてのインターフェイス上でデフォルトでイネーブルに設定されています。

インターフェイス上で NTP パケットの受信をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	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	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、ディセーブルにするインターフェイスを指定します。
ステップ 3	ntp disable	インターフェイス上で NTP パケットの受信をディセーブルにします。 デフォルトでは、すべてのインターフェイスは NTP パケットを受信します。
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	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイス上で NTP パケットの受信を再びイネーブルにするには、**no ntp disable** インターフェイス コンフィギュレーション コマンドを使用します。

NTP パケット用の送信元 IP アドレスの設定

スイッチが NTP パケットを送信すると、送信元 IP アドレスは、通常 NTP パケットが送信されたインターフェイスのアドレスに設定されます。すべての NTP パケットに特定の送信元 IP アドレスを使用する場合は、**ntp source** 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。アドレスは指定されたインターフェイスから取得します。インターフェイス上のアドレスを返信パケット用の宛先として使用できない場合に、このコマンドは便利です。

送信元 IP アドレスを取得する特定のインターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>ntp source type number</code>	IP 送信元アドレスを取得するインターフェイスのタイプと番号を指定します。 デフォルトでは、送信元アドレスは、発信インターフェイスから取得されます。
ステップ 3	<code>end</code>	特権 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。

指定されたインターフェイスは、すべての宛先に送信されるすべてのパケットの送信元アドレスに使用されます。送信元アドレスを特定のアソシエーションに使用する場合は、「[NTP アソシエーションの設定](#)」(P.5-5) に説明したように、`ntp peer` または `ntp server` グローバル コンフィギュレーション コマンド内で `source` キーワードを使用します。

NTP 設定の表示

次の 2 つの特権 EXEC コマンドを使用して NTP 情報を表示できます。

- `show ntp associations [detail]`
- `show ntp status`

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。

手動での日時の設定

他の時刻源が使用できない場合は、システムの再起動後、手動で日時を設定できます。時刻は、次にシステムを再起動するまで正確です。手動設定は最後の手段としてだけ使用することを推奨します。スイッチを同期化できる外部ソースがある場合は、手動でシステム クロックを設定する必要はありません。

ここでは、次の設定情報について説明します。

- 「[システム クロックの設定](#)」(P.5-11)
- 「[日時設定の表示](#)」(P.5-12)
- 「[時間帯の設定](#)」(P.5-12)
- 「[夏時間の設定](#)」(P.5-13)

システム クロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合、手動でシステム クロックを設定する必要はありません。

システム クロックを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>clock set hh:mm:ss day month year</code> または <code>clock set hh:mm:ss month day year</code>	次のいずれかのフォーマットで、手動でシステム クロックを設定します。 <ul style="list-style-type: none"><code>hh:mm:ss</code> には、時刻を時間 (24 時間形式)、分、秒で指定します。指定された時刻は、設定された時間帯に基づきます。<code>day</code> には、当月の日付で日を指定します。<code>month</code> には、月を名前で指定します。<code>year</code> には、年を指定します (常に 4 桁で指定)。
ステップ 2	<code>show running-config</code>	設定を確認します。
ステップ 3	<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。

次に、システム クロックを手動で 2001 年 7 月 23 日午後 1 時 32 分に設定する例を示します。

```
Switch# clock set 13:32:00 23 July 2001
```

日時設定の表示

日時の設定を表示するには、`show clock [detail]` 特権 EXEC コマンドを使用します。

システム クロックは、信頼性がある (正確であると信じられる) かどうかを示す *authoritative* フラグを維持します。システム クロックがタイミング ソースによって設定されている場合は、フラグを設定します。時刻が信頼性のないものである場合は、表示目的でだけ使用されます。クロックが信頼できず、*authoritative* フラグも設定されていないければ、ピアの時刻が無効でも、フラグはピアがクロックと同期しないようにします。

`show clock` の表示の前にある記号は、次の意味があります。

- * : 時刻は信頼できません。
- (空白) : 時刻は信頼できます。
- . : 時刻は信頼できますが、NTP は同期していません。

時間帯の設定

手動で時間帯を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>clock timezone zone hours-offset</code> <code>[minutes-offset]</code>	時間帯を設定します。 スイッチは内部時刻を UTC で管理するので、このコマンドは表示目的の場合および手動で時刻を設定した場合にかぎって使用します。 <ul style="list-style-type: none"><code>zone</code> には、標準時間が施行されているときに表示される時間帯の名前を入力します。デフォルトの設定は UTC です。<code>hours-offset</code> には、UTC からの時差を入力します。(任意) <code>minutes-offset</code> には、UTC からの分差を入力します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
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。

`clock timezone` グローバル コンフィギュレーション コマンドの **minutes-offset** 変数は、現地の時間帯と UTC との時差が分単位である場合に使用できます。たとえば、カナダ大西洋沿岸のある区域の時間帯 (Atlantic Standard Time (AST; 大西洋標準時)) は UTC-3.5 です。この場合、3 は 3 時間、.5 は 50% を意味します。この場合、必要なコマンドは **clock timezone AST -3 30** です。

時刻を UTC に設定するには、**no clock timezone** 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。

夏時間の設定

毎年特定の曜日に夏時間が開始して終了する地域に夏時間を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>clock summer-time zone recurring</code> [<i>week day month hh:mm week day month hh:mm [offset]</i>]	毎年指定した日に開始および終了するように夏時間を設定します。 夏時間はデフォルトでディセーブルに設定されています。パラメータなしで clock summer-time zone recurring を指定すると、夏時間の規則は米国の規則をデフォルトにします。 <ul style="list-style-type: none"> zone には、夏時間が施行されているときに表示される時間帯の名前 (たとえば PDT) を入力します。 (任意) week には、月の何週めかを指定します (1 ~ 5、または last)。 (任意) day には、曜日を指定します (Sunday、Monday など)。 (任意) month には、月を指定します (January、February など)。 (任意) hh:mm には、時刻を時間 (24 時間形式) と分で指定します。 (任意) offset には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。
ステップ 3	<code>end</code>	特権 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。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地の時間帯を基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月よりもあとの場合は、システムでは南半球にいると見なされます。

次に、夏時間が 4 月の第一日曜の 2 時に始まり、10 月の最終日曜の 2 時に終わるように指定する例を示します。

■ システム名およびプロンプトの設定

```
Switch(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

ユーザの居住地の夏時間が定期的なパターンに従わない（次の夏時間のイベントの正確な日時を設定する）場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	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	clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]] または clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]	最初の日付で夏時間開始の日付を、2 番目の日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 <ul style="list-style-type: none"> • <i>zone</i> には、夏時間が施行されているときに表示される時間帯の名前（たとえば PDT）を入力します。 • (任意) <i>week</i> には、月の何週めかを指定します（1 ~ 5、または last）。 • (任意) <i>day</i> には、曜日を指定します（Sunday、Monday など）。 • (任意) <i>month</i> には、月を指定します（January、February など）。 • (任意) <i>hh:mm</i> には、時刻を時間（24 時間形式）と分で指定します。 • (任意) <i>offset</i> には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。
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	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地の時間帯を基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月よりもあとの場合は、システムでは南半球にいると見なされます。

夏時間をディセーブルにするには、**no clock summer-time** 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、夏時間が 2003 年 10 月 12 日の 2 時に始まり、2004 年 4 月 26 日の 2 時に終わるよう設定する例を示します。

```
Switch(config)# clock summer-time pdt date 12 October 2003 2:00 26 April 2004 2:00
```

システム名およびプロンプトの設定

スイッチにシステム名を設定して特定します。デフォルトでは、システム名およびプロンプトは *Switch* です。

システム プロンプトを設定していない場合は、システム名の最初の 20 文字をシステム プロンプトとして使用します。大なり記号 (>) が付加されます。システム名が変更されると、プロンプトはアップデートされます。



(注) ここで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Configuration Fundamentals Command Reference, Release 12.2』および『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2』を参照してください。

ここでは、次の設定情報について説明します。

- 「デフォルトのシステム名およびプロンプトの設定」(P.5-15)
- 「システム名の設定」(P.5-15)
- 「DNS の概要」(P.5-15)

デフォルトのシステム名およびプロンプトの設定

デフォルトのスイッチのシステム名およびプロンプトは *Switch* です。

システム名の設定

手動でシステム名を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>hostname name</code>	手動でシステム名を設定します。 デフォルト設定は <i>switch</i> です。 名前は ARPANET ホスト名の規則に従う必要があります。この規則ではホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、またはハイフンしか使用できません。名前には 63 文字まで使用できます。
ステップ 3	<code>end</code>	特権 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。

システム名を設定すると、システム プロンプトとしても使用されます。

デフォルトのホスト名に戻すには、**no hostname** 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。

DNS の概要

Domain Name System (DNS; ドメイン ネーム システム) プロトコルは、分散型データベース DNS を制御し、これによりホスト名を IP アドレスにマッピングできます。スイッチ上に DNS を設定すると、**ping**、**telnet**、**connect** などのすべての IP コマンドや、関連する Telnet サポート操作時に、IP アドレスの代わりにホスト名を使用できます。

IP によって定義される階層型のネーミング方式では、デバイスを場所またはドメインで特定できます。ドメイン名の区切りとしては、ピリオド (.) を使用します。たとえば、シスコシステムズは、IP で *com* というドメイン名に分類される商業組織なので、ドメイン名は *cisco.com* となります。このドメイン内の特定のデバイス、たとえば FTP システムは、*ftp.cisco.com* で表されます。

IP ではドメイン名をトラッキングするために、ドメイン ネーム サーバという概念が定義されています。ドメイン ネーム サーバの役割は、名前から IP アドレスへのマッピングをキャッシュ（またはデータベース）に保存することです。ドメイン名を IP アドレスにマッピングするには、まず、ホスト名を明示し、ネットワーク上に存在するネーム サーバを指定し、DNS をイネーブルにします。

ここでは、次の設定情報について説明します。

- 「DNS のデフォルト設定」(P.5-16)
- 「DNS の設定」(P.5-16)
- 「DNS 設定の表示」(P.5-17)

DNS のデフォルト設定

表 5-2 に、DNS のデフォルト設定を示します。

表 5-2 DNS のデフォルト設定

機能	デフォルト設定
DNS イネーブル ステータス	イネーブル。
DNS デフォルト ドメイン名	未設定。
DNS サーバ	ネーム サーバのアドレスが未設定。

DNS の設定

DNS を使用するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>ip domain-name name</code>	未修飾のホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 起動時にはドメイン名は設定されていませんが、BOOTP または DHCP サーバからスイッチ コンフィギュレーションを取得している場合は、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（サーバにこの情報が設定されている場合）。
ステップ 3	<code>ip name-server server-address1 [server-address2 ... server-address6]</code>	1 つまたは複数のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。 最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。スイッチは、最初にプライマリ サーバに DNS クエリーを送信します。そのクエリーが失敗した場合は、バックアップサーバにクエリーが送信されます。

	コマンド	目的
ステップ 4	ip domain-lookup	(任意) スイッチ上で、DNS ベースのホスト名のアドレスへの変換をイネーブルにします。この機能は、デフォルトでイネーブルに設定されています。 ユーザのネットワーク デバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式 (DNS) を使用して、ユーザのデバイスを一意に識別するデバイス名をダイナミックに割り当てることができます。
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	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチの IP アドレスをそのホスト名として使用する場合は、IP アドレスが使用され、DNS クエリは発生しません。ピリオド (.) なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホスト名に追加され、そのあとで DNS クエリが行われ、名前を IP アドレスにマッピングします。デフォルトのドメイン名は、**ip domain-name** グローバル コンフィギュレーション コマンドによって設定される値です。ホスト名にピリオド (.) がある場合は、Cisco IOS ソフトウェアは、ホスト名にデフォルトのドメイン名を追加せずに IP アドレスを検索します。

ドメイン名を削除するには、**no ip domain-name name** 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。ネーム サーバのアドレスを削除するには、**no ip name-server server-address** 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。スイッチ上の DNS をディセーブルにするには、**no ip domain-lookup** 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。

DNS 設定の表示

DNS 設定情報を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

バナーの作成

Message-of-The-Day (MoTD) バナーおよびログイン バナーを作成できます。MoTD バナーはログイン時に接続しているすべての端末で表示され、すべてのネットワーク ユーザに影響のあるメッセージ (システムのシャットダウン予告など) を送信するのに便利です。

ログイン バナーも、接続しているすべての端末で表示されます。表示されるのは、MoTD バナーのあとで、ログイン プロンプトが表示される前です。



(注) ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。

ここでは、次の設定情報について説明します。

- 「バナーのデフォルト設定」(P.5-18)
- 「MoTD ログイン バナーの設定」(P.5-18)
- 「ログイン バナーの設定」(P.5-19)

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MoTD ログイン バナーの設定

ユーザがスイッチにログインしたときに、画面に表示される 1 行または複数行のメッセージ バナーを作成できます。

MoTD ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>banner motd c message c</code>	MoTD バナーを指定します。 <i>c</i> には、任意の区切り文字、たとえばポンド記号 (#) を入力して、 Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 <i>message</i> には、255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 3	<code>end</code>	特権 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。

MoTD バナーを削除するには、`no banner motd` 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、ポンド記号 (#) を開始および終了の区切り文字として使用し、スイッチの MoTD バナーを設定する例を示します。

```
Switch(config)# banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
Switch(config)#
```

次に、前の設定により表示されたバナーを示します。

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

User Access Verification

Password:
```

ログイン バナーの設定

接続されたすべての端末でログイン バナーが表示されるように設定できます。バナーが表示されるのは、MoTD バナーのあとで、ログインプロンプトが表示される前です。

ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>banner login c message c</code>	ログイン メッセージを指定します。 <i>c</i> には、任意の区切り文字、たとえばポンド記号 (#) を入力して、 Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されません。 <i>message</i> には、255 文字までのログイン メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 3	<code>end</code>	特権 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。

ログイン バナーを削除するには、`no banner login` 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、ドル記号 (\$) を開始および終了の区切り文字として使用し、スイッチのログイン バナーを設定する例を示します。

```
Switch(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
Switch(config)#
```

MAC アドレス テーブルの管理

MAC アドレス テーブルには、スイッチがポート間のトラフィック転送に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- ダイナミック アドレス：スイッチが学習し、使用されなくなった時点で期限切れとなる送信元 MAC アドレス
- スタティック アドレス：手動で入力され、期限切れにならず、スイッチのリセット時にも消去されないユニキャストまたはマルチキャスト アドレス

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN ID、アドレスに対応付けられたポート番号、およびタイプ (スタティックまたはダイナミック) のリストです。



(注) ここで使用す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コマンド リファレンスを参照してください。

ここでは、次の設定情報について説明します。

- 「アドレス テーブルの作成」 (P.5-20)
- 「MAC アドレスおよび VLAN」 (P.5-20)
- 「MAC アドレス テーブルのデフォルト設定」 (P.5-21)
- 「アドレス エージング タイムの変更」 (P.5-21)
- 「ダイナミック アドレス エントリの削除」 (P.5-22)
- 「MAC アドレス変更通知トラップの設定」 (P.5-22)
- 「MAC アドレス移動通知トラップの設定」 (P.5-24)
- 「MAC しきい値通知トラップの設定」 (P.5-26)
- 「スタティック アドレス エントリの追加および削除」 (P.5-27)
- 「ユニキャスト MAC アドレス フィルタリングの設定」 (P.5-28)
- 「VLAN での MAC アドレス ラーニングのディセーブル化」 (P.5-29)
- 「アドレス テーブル エントリの表示」 (P.5-31)

アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスによって、スイッチの任意のポートを各ワークステーション、リピータ、スイッチ、ルータ、またはその他のネットワーク デバイスに接続できます。各ポートで受信するパケットの送信元アドレスを取得し、アドレス テーブルにアドレスとその対応するポート番号を追加することによって、スイッチはダイナミックなアドレス指定を行います。ネットワークでステーションの増設または取り外しが行われると、スイッチはアドレス テーブルをアップデートし、新しいダイナミック アドレスを追加し、使用されていないアドレスはエージングアウトにします。

エージング インターバルはグローバルに設定されています。ただし、スイッチは VLAN ごとにアドレス テーブルを維持し、STP によって VLAN 単位で有効期間を短縮できます。

スイッチは、受信したパケットの宛先アドレスに基づいて、任意の組み合わせのポート間でパケットを送信します。MAC アドレス テーブルを使用することによって、スイッチは、宛先アドレスに対応付けられたポート（複数可）に限定してパケットを転送します。宛先アドレスがパケットを送信したポート上にある場合は、パケットはフィルタリング処理され、転送されません。スイッチは、常にストア アンド フォワード方式を使用します。このため、完全なパケットをいったん保存してエラーがないか検査してから転送します。

MAC アドレスおよび VLAN

アドレスはすべて、VLAN と対応付けられます。1 つのアドレスを複数の VLAN に対応付け、それぞれで異なる宛先を設定できます。たとえば、ユニキャスト アドレスは、VLAN 1 内のポート 1 および VLAN 5 内のポート 9、10、1 へ転送できます。



(注) マルチポート スタティック アドレスはサポートされていません。

VLAN ごとに、独自の論理アドレス テーブルが維持されます。ある VLAN で認識されているアドレスが別の VLAN で認識されるには、別の VLAN 内のポートによって学習されるか、または別の VLAN 内のポートにスタティックに対応付けられる必要があります。

プライベート VLAN が設定されている場合、アドレス学習は MAC アドレス タイプによって異なります。

- プライベート VLAN 上にある 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連 VLAN に複製されます。たとえば、プライベート VLAN のセカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN に複製されます。
- プライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは関連 VLAN には複製されません。プライベート VLAN のプライマリまたはセカンダリ VLAN 内にスタティック MAC アドレスを設定した場合、同じスタティック MAC アドレスをすべての関連 VLAN に設定する必要があります。

プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。

MAC アドレス ラーニングは、各 VLAN ごとにディセーブルにすることができます。サービスプロバイダー ネットワーク上のカスタマーは、ネットワーク経由で多数の MAC アドレスをトンネリングし、使用可能な MAC アドレス テーブル スペースを満たすことができます。VLAN 上の MAC アドレス ラーニングを制御したり、どの VLAN（つまり、ポート）で MAC アドレス ラーニングが可能であるかを指定することにより、スイッチで使用可能な MAC アドレス テーブル スペースを管理したりすることができます。

MAC アドレス学習をディセーブルにする前に、ネットワーク トポロジとスイッチ システム設定に詳しいことを確認してください。VLAN で MAC アドレス学習をディセーブルにすると、ネットワークでフラッディングを引き起こす可能性があります。詳細については、「VLAN での MAC アドレス ラーニングのディセーブル化」(P.5-29) を参照してください。

MAC アドレス テーブルのデフォルト設定

表 5-3 に、MAC アドレス テーブルのデフォルト設定を示します。

表 5-3 MAC アドレス テーブルのデフォルト設定

機能	デフォルト設定
エージング タイム	300 秒
ダイナミック アドレス	自動学習
スタティック アドレス	未設定
VLAN での MAC アドレス ラーニング	イネーブル

アドレス エージング タイムの変更

ダイナミック アドレスは、スイッチが学習し、使用されなくなると期限切れになる送信元 MAC アドレスです。すべての VLAN または指定された VLAN に対して、エージング タイムの設定を変更できます。

エージング タイムを短く設定しすぎると、アドレスが活用されないままテーブルから削除される可能性があります。その場合、スイッチは宛先が不明の packets を受信すると、受信ポートと同じ VLAN 内のすべてのポートに、その packets をフラッディングさせます。この不必要なフラッディングによって、パフォーマンスに悪影響を及ぼす可能性があります。また、エージング タイムを長く設定しすぎると、アドレス テーブルが未使用のアドレスでいっぱいになり、これによって新しいアドレスを学習できなくなります。この結果フラッディングとなり、スイッチのパフォーマンスに悪影響を及ぼす可能性があります。

ダイナミック アドレス テーブルのエージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>mac address-table aging-time [0 10-1000000] [vlan vlan-id]</code>	ダイナミック エントリが使用またはアップデートされたあと、MAC アドレス テーブル内に保持される時間を設定します。 指定できる範囲は 10 ~ 1000000 秒です。デフォルト値は 300 です。0 を入力してエージングをディセーブルにすることもできます。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。 <i>vlan-id</i> では、指定できる範囲は 1 ~ 4094 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mac address-table aging-time</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。

デフォルト値に戻すには、`no mac address-table aging-time` 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。

ダイナミック アドレス エントリの削除

ダイナミック エントリをすべて削除するには、特権 EXEC モードで `clear mac address-table dynamic` コマンドを使用します。特定の MAC アドレス (`clear mac address-table dynamic address mac-address`)、指定された物理ポートまたはポートチャネル上のすべてのアドレス (`clear mac address-table dynamic interface interface-id`)、または指定された VLAN 上のすべてのアドレス (`clear mac address-table dynamic vlan vlan-id`) の削除もできます。

ダイナミック エントリが削除されたことを確認するには、`show mac address-table dynamic` 特権 EXEC コマンドを使用します。

MAC アドレス変更通知トラップの設定

MAC アドレス変更通知は、MAC アドレス変更アクティビティを保存することでネットワーク上のユーザを追跡します。スイッチが MAC アドレスを学習または削除すると、SNMP 通知トラップが NMS (Network Management System; ネットワーク管理システム) に送信されます。ネットワークから多数のユーザの出入りがある場合は、トラップ インターバル タイムを設定して通知トラップを組み込み、ネットワーク トラフィックを削減できます。MAC 通知履歴テーブルは、トラップが設定されたポートごとの MAC アドレス アクティビティを保存します。MAC アドレス変更通知は、ダイナミックまたはセキュア MAC アドレスについてだけ生成されます。自身のアドレス、マルチキャストアドレス、または他のスタティック アドレスについては生成されません。

NMS ホストに MAC アドレス変更通知トラップを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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 host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 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。SNMP 情報をホストに送信するには、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 にはバージョン 1 (デフォルト) を使用できません。 <code>community-string</code> には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できませんが、このストリングを定義するには、snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ 3	<code>snmp-server enable traps mac-notification change</code>	スイッチが MAC アドレス変更通知トラップを NMS に送信できるようにします。
ステップ 4	<code>mac address-table notification change</code>	MAC アドレス変更通知機能をイネーブルにします。
ステップ 5	<code>mac address-table notification change [interval value] [history-size value]</code>	<p>トラップ インターバル タイムと履歴テーブルのサイズを入力します。</p> <ul style="list-style-type: none"> (任意) interval value には、NMS に対して生成される各トラップ セット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は 0 ~ 2147483647 秒です。デフォルトは 1 秒です。 (任意) history-size value には、MAC 通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は 0 ~ 500 です。デフォルト値は 1 です。
ステップ 6	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。

	コマンド	目的
ステップ 7	<code>snmp trap mac-notification change {added removed}</code>	インターフェイスの MAC アドレス変更通知トラップをイネーブルにします。 <ul style="list-style-type: none"> • MAC アドレスがインターフェイスに追加されると、トラップをイネーブルにします。 • MAC アドレスがインターフェイスから削除されると、トラップをイネーブルにします。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show mac address-table notification change interface</code> <code>show running-config</code>	設定を確認します。
ステップ 10	<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。

MAC アドレス変更通知トラップをディセーブルにするには、**no snmp-server enable traps mac-notification change** 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。特定のインターフェイス上で MAC アドレス変更通知トラップをディセーブルにするには、**no snmp trap mac-notification change {added | removed}** インターフェイス コンフィギュレーション コマンドを使用します。MAC アドレス変更通知機能をディセーブルにするには、**no mac address-table notification change** 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、NMS として 172.20.10.10 を指定し、スイッチによる NMS への MAC アドレス通知トラップの送信をイネーブルにして、MAC アドレス変更通知機能をイネーブルにし、インターバル タイムを 123 秒、履歴サイズを 100 エントリに設定し、指定されたポートに MAC アドレスが追加されるたびにトラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet1/1/2
Switch(config-if)# snmp trap mac-notification change added
```

設定を確認するには、**show mac address-table notification change interface** および **show mac address-table notification change** 特権 EXEC コマンドを入力します。

MAC アドレス移動通知トラップの設定

MAC 移動通知を設定すると、あるポートから同じ VLAN 内の別のポートに MAC アドレスが移動するたびに、SNMP 通知が生成され、ネットワーク管理システムに送信されます。

NMS ホストに MAC アドレス移動通知トラップを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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 host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 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。SNMP 情報をホストに送信するには、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 にはバージョン 1 (デフォルト) を使用できません。 <code>community-string</code> には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できませんが、このストリングを定義するには、snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ 3	<code>snmp-server enable traps mac-notification move</code>	スイッチが MAC アドレス移動通知トラップを NMS に送信できるようにします。
ステップ 4	<code>mac address-table notification mac-move</code>	MAC アドレス移動通知機能をイネーブルにします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show mac address-table notification mac-move</code> <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。

MAC アドレス移動通知トラップをディセーブルにするには、**no snmp-server enable traps mac-notification move** 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。MAC アドレス移動通知機能をディセーブルにするには、**no mac address-table notification mac-move** 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、NMS として 172.20.10.10 を指定し、スイッチによる NMS への MAC アドレス移動通知トラップの送信をイネーブルにして、MAC アドレス移動通知機能をイネーブルにし、あるポートから別のポートに MAC アドレスが移動するとトラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification move
Switch(config)# mac address-table notification mac-move
```

設定を確認するには、**show mac address-table notification mac-move** 特権 EXEC コマンドを入力します。

MAC しきい値通知トラップの設定

MAC しきい値通知を設定すると、MAC アドレス テーブルのしきい値が上限に達するか、または上限を超えた時点で、SNMP 通知が生成され、ネットワーク管理システムに送信されます。

NMS ホストに MAC アドレス テーブルしきい値通知を送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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 host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 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。SNMP 情報をホストに送信するには、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 にはバージョン 1 (デフォルト) を使用できません。 <code>community-string</code> には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ 3	<code>snmp-server enable traps mac-notification threshold</code>	スイッチが MAC しきい値通知トラップを NMS に送信できるようにします。
ステップ 4	<code>mac address-table notification threshold</code>	MAC アドレスしきい値通知機能をイネーブルにします。
ステップ 5	<code>mac address-table notification threshold [limit percentage] [interval time]</code>	<p>MAC アドレスしきい値の使用状況のモニタリングに使用するしきい値を入力します。</p> <ul style="list-style-type: none"> (任意) <code>limit percentage</code> には、MAC アドレス テーブル使用の割合を指定します。有効な値は 1 ~ 100% です。デフォルト値は 50% です。 (任意) <code>interval time</code> には、通知する間隔を指定します。有効な値は 120 秒以上です。デフォルト値は 120 秒です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show mac address-table notification threshold</code> <code>show running-config</code>	設定を確認します。
ステップ 8	<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。

MAC アドレスしきい値通知トラップをディセーブルにするには、**no snmp-server enable traps mac-notification threshold** 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。MAC アドレスしきい値通知機能をディセーブルにするには、**no mac address-table notification threshold** 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、NMS として 172.20.10.10 を指定し、MAC アドレスしきい値通知機能をイネーブルにし、インターバル タイムを 123 秒、上限を 78% に設定する例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification threshold
Switch(config)# mac address-table notification threshold
Switch(config)# mac address-table notification threshold interval 123
Switch(config)# mac address-table notification threshold limit 78
```

設定を確認するには、**show mac address-table notification threshold** 特権 EXEC コマンドを入力します。

スタティック アドレス エントリの追加および削除

スタティック アドレスには、次の特性があります。

- アドレス テーブルへの追加およびアドレス テーブルからの削除は、手動で行う必要があります。
- ユニキャスト アドレスとして設定できます。
- 期限切れになることはなく、スイッチが再起動しても維持されます。

スタティック アドレスを追加および削除でき、また、スタティック アドレスの転送動作を定義できます。転送動作とは、パケットを受信したポートが、そのパケットを他のポートに転送する方法のことです。ポートは必ず少なくとも 1 つの VLAN と対応しているので、スイッチは指定されたポートから、アドレスに対応する VLAN ID を取得します。

特定のアドレスがスタティックとして入力されていない VLAN に、そのスタティック アドレスを持つパケットが到着すると、すべてのポートにパケットがフラッディングされ、学習されません。

アドレス テーブルにスタティック アドレスを追加するには、宛先 MAC ユニキャスト アドレスと、その送信元 VLAN を指定します。この宛先アドレスで受信したパケットは、*interface-id* オプションで指定されたインターフェイスに転送されます。

プライベート VLAN のプライマリまたはセカンダリ VLAN のスタティック MAC アドレスを設定する場合、同じスタティック MAC アドレスを対応付けられた VLAN すべてで設定します。プライベート VLAN のプライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは関連 VLAN には複製されません。プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。

スタティック アドレスを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>mac address-table static mac-addr vlan vlan-id interface interface-id</code>	MAC アドレス テーブルにスタティック アドレスを追加します。 <ul style="list-style-type: none"> <code>mac-addr</code> には、アドレス テーブルに追加する宛先 MAC ユニキャスト アドレスを指定します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 <code>vlan-id</code> には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる範囲は 1 ~ 4094 です。 <code>interface-id</code> には、受信したパケットの転送先インターフェイスを指定します。指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mac address-table static</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。

アドレス テーブルからスタティック エントリを削除するには、`no mac address-table static mac-addr vlan vlan-id interface interface-id` 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。

次の例では、MAC アドレス テーブルにスタティック アドレス `c2f3.220a.12f4` を追加する方法を示します。VLAN 4 で、この MAC アドレスを宛先アドレスとして持つパケットを受信すると、パケットは指定されたインターフェイスに転送されます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet1/0/1
```

ユニキャスト MAC アドレス フィルタリングの設定

ユニキャスト MAC アドレス フィルタリングがイネーブルの場合、スイッチは、特定の送信元 MAC アドレスまたは宛先 MAC アドレスを持つパケットをドロップします。この機能はデフォルトではディセーブルで、ユニキャスト スタティック アドレスだけをサポートしています。

この機能を使用する場合は、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされません。`mac address-table static mac-addr vlan vlan-id drop` グローバル コンフィギュレーション コマンドを入力するときに、これらのアドレスのいずれかを指定すると、次のいずれかのメッセージが表示されます。

```
% Only unicast addresses can be configured to be dropped
% CPU destined address cannot be configured as drop address
```
- CPU に転送されるパケットもサポートされません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定する場合は、最後に入力されたコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、またはその MAC アドレスを持つパケットをドロップします。2 番目に入力したコマンドは、最初のコマンドを上書きします。

たとえば、`mac address-table static mac-addr vlan vlan-id interface interface-id` グローバル コンフィギュレーション コマンドのあとに `mac address-table static mac-addr vlan vlan-id drop` コマンドを入力した場合は、スイッチは送信元または宛先として指定された MAC アドレスを持つパケットをドロップします。

`mac address-table static mac-addr vlan vlan-id drop` グローバル コンフィギュレーション コマンドのあとに `mac address-table static mac-addr vlan vlan-id interface interface-id` コマンドを入力した場合は、スイッチがその MAC アドレスをスタティック アドレスとして追加します。

ユニキャスト MAC アドレス フィルタリングをイネーブルにして、スイッチが特定のアドレスを持つパケットをドロップするように設定するには、送信元または宛先ユニキャスト MAC アドレスおよび受信側の VLAN を指定します。

スイッチが送信元または宛先ユニキャスト スタティック アドレスをドロップするよう設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>mac address-table static mac-addr vlan vlan-id drop</code>	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、スイッチが指定した送信元または宛先ユニキャスト スタティック アドレスを持つパケットをドロップするように設定します。 <ul style="list-style-type: none"> <code>mac-addr</code> には、送信元または宛先ユニキャスト MAC アドレスを指定します。この MAC アドレスを持つパケットはドロップされます。 <code>vlan-id</code> には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID は、1 ~ 4094 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mac address-table static</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。

ユニキャスト MAC アドレス フィルタリングをディセーブルにするには、`no mac address-table static mac-addr vlan vlan-id` 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。

次の例では、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、`c2f3.220a.12f4` の送信元または宛先アドレスを持つパケットをドロップするようにスイッチを設定する方法を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

VLAN での MAC アドレス ラーニングのディセーブル化

デフォルトでは、MAC アドレス ラーニングがスイッチのすべての VLAN でイネーブルです。VLAN 上の MAC アドレス ラーニングを制御したり、どの VLAN (つまり、ポート) で MAC アドレス ラーニングが可能であるかを指定することにより、MAC アドレス テーブル スペースを管理したりすることができます。MAC アドレス ラーニングをディセーブルにする前に必ず、ネットワーク トポロジとスイッチ システム設定をよく理解しておいてください。VLAN で MAC アドレス学習をディセーブルにすると、ネットワークでフラッドを引き起こす可能性があります。

VLAN で MAC アドレス ラーニングをディセーブルにするときは、次の注意事項に従ってください。

- Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) が設定された VLAN で MAC アドレス ラーニングをディセーブルにするときは、注意が必要です。この場合、スイッチはレイヤ 2 ドメイン内のすべての IP パケットをフラッディングします。
- MAC アドレス ラーニングは、1 つの VLAN (例 : **no mac address-table learning vlan 223**) または VLAN の範囲 (例 : **no mac address-table learning vlan 1-10, 15**) でディセーブルにすることができます。
- MAC アドレス ラーニングは、2 つのポートを備えた VLAN でだけディセーブルにすることを推奨します。3 つ以上のポートを備えた VLAN で MAC アドレス ラーニングをディセーブルにすると、スイッチが受信するすべてのパケットが VLAN ドメインでフラッディングされます。
- スイッチにより内部的に使用される VLAN では、MAC アドレス ラーニングをディセーブルにすることはできません。入力した VLAN ID が内部 VLAN である場合は、スイッチがエラー メッセージを生成し、そのコマンドを拒否します。使用する内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを入力します。
- プライベート VLAN、プライマリ VLAN として設定された VLAN で MAC アドレス ラーニングをディセーブルにしても、MAC アドレスは、プライマリ VLAN に属しており、プライマリ VLAN に複製されたセカンダリ VLAN で学習されます。プライベート VLAN のプライマリ VLAN ではないセカンダリ VLAN で MAC アドレス ラーニングをディセーブルにすると、MAC アドレス ラーニングは、プライマリ VLAN 上で発生する VLAN で実行され、セカンダリ VLAN に複製されます。
- RSPAN VLAN で MAC アドレス学習はディセーブルにできません。設定すること自体できません。
- セキュア ポートを含む VLAN での MAC アドレス ラーニングをディセーブルにしても、ポートでは MAC アドレス ラーニングはディセーブルになりません。ポートセキュリティをディセーブルにした場合、設定済みの MAC アドレス ラーニング ステートはイネーブルです。

VLAN で MAC アドレス ラーニングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	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 mac address-table learning vlan <i>vlan-id</i>	<ul style="list-style-type: none"> • 特定の VLAN で MAC アドレス ラーニングをディセーブルにします。1 つの VLAN を指定するか、VLAN の範囲をハイフンまたはカンマで区切って指定します。指定できる VLAN ID は、1 ~ 4094 です。VLAN を内部 VLAN にすることはできません。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mac address-table learning [vlan <i>vlan-id</i>]	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN で MAC アドレス ラーニングを再度イネーブルにするには、**default mac address-table learning vlan *vlan-id*** 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。また、**mac address-table learning vlan *vlan-id*** 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、VLAN で MAC アドレス ラーニングを再度イネーブルにすることもできます。前者の (**default**) コマンドを使用すると、デフォルトの状態に戻るようになるため、設定は **show running-config** コマンドによる出力には含まれません。後者のコマンドを使用すると、設定が **show running-config** 特権 EXEC コマンドの表示に含まれます。

次に、VLAN 200 で MAC アドレス ラーニングをディセーブルにする方法の例を示します。

```
Switch(config)# no mac address-table learning vlan 200
```

show mac-address-table learning [vlan vlan-id] 特権 EXEC コマンドを入力すると、すべての VLAN または特定の VLAN の MAC アドレス ラーニングのステータスを表示することができます。

アドレス テーブル エントリの表示

表 5-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用すると、MAC アドレス テーブルを表示できます。

表 5-4 MAC アドレス テーブル表示用のコマンド

コマンド	説明
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリだけを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table learning	すべての VLAN または特定の VLAN での MAC アドレス ラーニングのステータスを表示します。
show mac address-table multicast	すべての VLAN または指定された VLAN に対するレイヤ 2 マルチキャスト エントリを表示します。
show mac address-table notification	MAC 通知パラメータおよび履歴テーブルを表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

ARP テーブルの管理

デバイスと通信するには（イーサネット経由など）、ソフトウェアは最初に、そのデバイスの 48 ビット MAC アドレスまたはローカルデータ リンク アドレスを識別する必要があります。IP アドレスからローカルデータ リンク アドレスを識別するプロセスを、「アドレス解決」と呼びます。

Address Resolution Protocol (ARP; アドレス解決プロトコル) は、ホスト IP アドレスを、対応する MAC アドレス (メディア) と VLAN ID に関連付けます。IP アドレスが入力されると、ARP はそれに関連付けられた MAC アドレスを識別します。MAC アドレスが識別されると、それ以降迅速に検索できるように、IP-MAC アドレス アソシエーションが ARP キャッシュにストアされます。そのあと、IP データグラムがリンク レイヤ フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化および ARP 要求/応答については、Subnetwork Access Protocol (SNAP; サブネットワーク アクセス プロトコル) で規定されています。IP インターフェイスでは、標準的なイーサネット形式の ARP カプセル化 (**arpa** キーワードで表される) がデフォルトでイネーブルに設定されています。

手動でテーブルに追加された ARP エントリは期限切れにならないので、手動で削除する必要があります。

詳細については、Cisco.com で Cisco IOS リリース 12.2 のマニュアルを参照してください。

