CHAPTER 7

スイッチの管理

この章では、IE 3000 スイッチを管理するための 1 回限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

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

（注） この項で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference*』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

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、システムが起動した瞬間から動作し、日時を追跡します。

システム クロックは、次のソースから設定できます。

- 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できます。

- ユーザ **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）（または Greenwich Mean Time（GMT; グリニッジ標準時））に基づいて内部で時刻を追跡します。時刻が現地の時間帯に応じて正しく表示されるように、現地の時間帯と夏時間に関する情報を設定できます。

システム クロックは、時刻が*信頼できる*かどうか（時刻が信頼できると見なされる時刻源によって設定されているかどうか）を追跡します。時刻が信頼できない場合、時刻は表示目的でだけ使用でき、再配布されません。設定の詳細については、「手動での日時の設定」（P.7-11）を参照してください。

ネットワーク タイム プロトコルの概要

NTP は、装置のネットワークの時間を同期するように設計されています。NTP は、IP 上で実行される User Datagram Protocol（UDP; ユーザ データグラム プロトコル）で実行されます。NTP については、RFC 1305 で説明されています。

通常、NTP ネットワークは、タイム サーバに接続されているラジオ クロックやアトミック クロックなど信頼できる時刻源から時刻を取得します。NTP は、ネットワークを介して取得した時刻を配布します。NTP は非常に効率的です。1 分あたり 1 つのパケットを使用するだけで、2 台の装置を 1 ミリ秒以内に同期できます。

NTP は、*ストラタム*という概念を使用して、装置と信頼できる時刻源の間にある NTP ホップ数を表します。ストラタム 1 タイム サーバには、ラジオ クロックまたはアトミック クロックが直接接続され、ストラタム 2 タイム サーバは、ストラタム 1 タイム サーバから NTP 経由で時刻を受信するというように、順番に続いていきます。NTP を実行している装置は、その時刻源として、NTP を介して通信するときに使用するストラタム番号が最小の装置を自動的に選択します。この方法によって、NTP スピーカの自己編成型ツリーが効率的に構築されます。

NTP では、同期されていない装置と同期しないようにして、時刻が正確ではない可能性がある装置との同期を回避します。また、複数の装置から報告された時刻を比較し、時刻が他の装置と大幅に異なる装置とは、そのストラタム番号が小さい場合であっても同期しません。

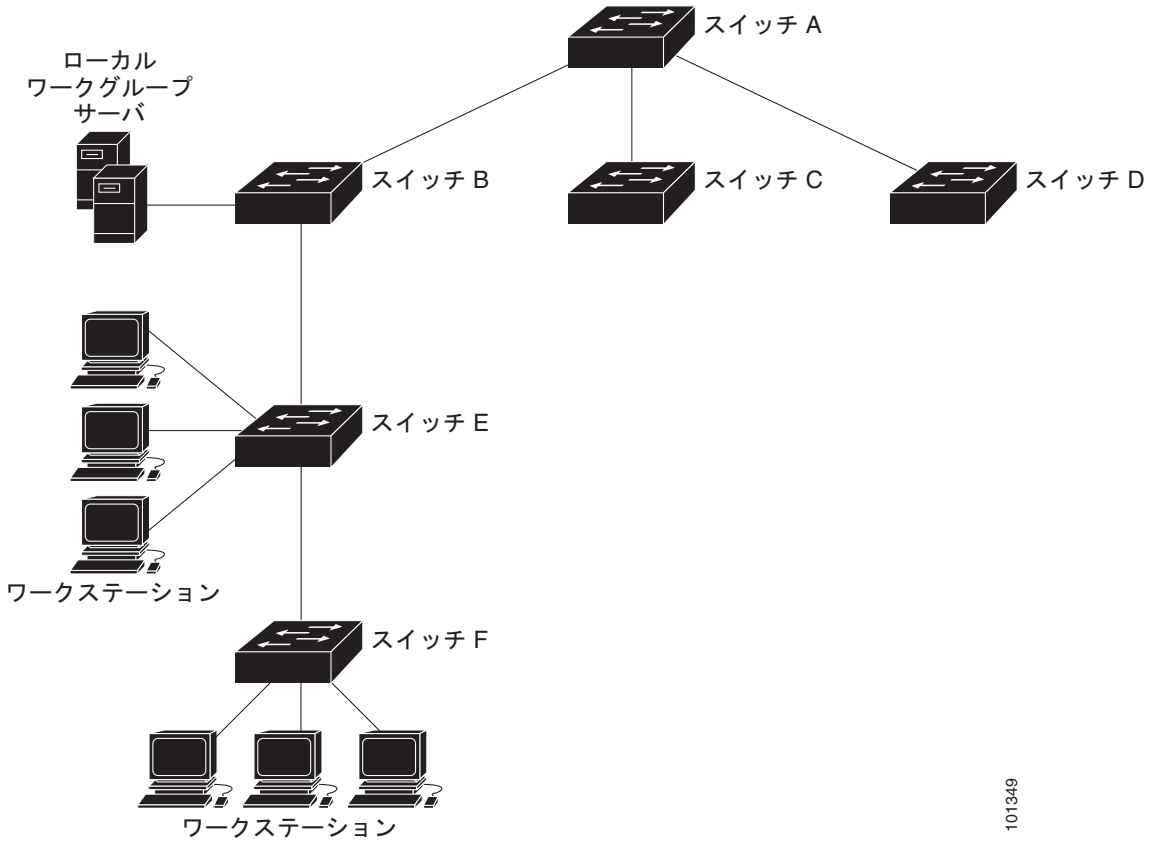
NTP を実行している装置間の通信（*アソシエーション*）は通常、スタティックに設定されます。各装置には、アソシエーションの作成に使用するすべての装置の IP アドレスが与えられます。アソシエーションのペアとなる装置間で NTP メッセージを交換することで、正確なタイムキーピングが実現されます。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。この代替の方法では、ブロードキャスト メッセージを送受信するように各装置を設定するだけなので、設定の複雑さが解消されます。ただし、この場合は、情報の流れが一方向に限定されます。

装置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、誤って指定した設定や悪意ある設定で誤った時刻が設定されないようにする必要があります。2 つのメカニズムを利用できます。1 つはアクセス リストに基づく制限方式で、もう 1 つは暗号化認証メカニズムです。

シスコの NTP の実装では、ストラタム 1 サービスはサポートされていません。そのため、ラジオ クロックやアトミック 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 インターネットで使用できるパブリック NTP サーバから取得することを推奨します。

図 7-1 に、NTP を使用した一般的なネットワークの例を示します。スイッチ A は NTP マスターです。スイッチ B、C、D は NTP サーバ モードで設定され、スイッチ A とのサーバ アソシエーション内にあります。スイッチ E は、アップストリーム スイッチ（スイッチ B）とダウンストリーム スイッチ（スイッチ F）に対する NTP ピアとして設定されています。

図 7-1　一般的な NTP ネットワークの設定



ネットワークがインターネットに接続されていない場合、シスコの NTP の実装では、実際には他の方法で時刻を取得している場合でも、NTP を介して同期されているかのように装置を設定できます。この場合、他の装置は、NTP を介してその装置と同期します。

複数の時刻源が使用できる場合、NTP は常に他の時刻源よりも信頼が高いと見なされます。NTP の時刻は、他の方法で設定された時刻よりも優先されます。

いくつかの製造元では、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ます。また、UNIX を実行しているシステム用の公開バージョンおよびその各種派生バージョンもあります。このソフトウェアでは、ホスト システムの時刻も同期できます。

NTP の設定

スイッチには、ハードウェアでサポートされているクロックはありません。また、スイッチは、外部の NTP ソースが使用できない場合に、ペアが自身を同期する NTP マスター クロックとしても機能しません。スイッチには、カレンダーに対するハードウェアのサポートもありません。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 コマンドは使用できません。

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.7-4）
- 「NTP 認証の設定」（P.7-4）
- 「NTP アソシエーションの設定」（P.7-5）

NTP のデフォルト設定

表 7-1 に、NTP のデフォルト設定を示します。

表 7-1　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。認証キーは指定されていません。
NTP ピアおよびサーバ アソシエーション	設定なし。
NTP ブロードキャスト サービス	ディセーブル。インターフェイスは 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	アクセス制御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設定されます。

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なっています。すべてのインターフェイスが 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、スイッチが時刻を NTP サーバと同期するときに使用するサーバと一致する必要があります。

セキュリティ目的で他の装置とのアソシエーション（正確なタイムキーピングを行うために提供される、NTP を実行している装置間の通信）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	**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	**ntp authenticate**	デフォルトではディセーブルになっている NTP 認証機能をイネーブルにします。
ステップ 3	**ntp authentication-key** *number* **md5** *value*	認証キーを定義します。デフォルトでは、認証キーは定義されていません。 • *number* には、キー番号を指定します。指定できる範囲は 1 ～ 4294967295 です。 • **md5** は、Message Digest Algorithm 5（MD5）を使用してメッセージ認証のサポートが提供されることを指定します。 • *value* には、キーの 8 文字までの任意の文字列を入力します。 スイッチと装置の両方がこれらの認証キーのいずれかを持たない限り、スイッチと装置は同期しません。また、キー番号は、**ntp trusted-key** *key-number* コマンドで指定されます。

	コマンド	目的
ステップ 4	**ntp trusted-key** *key-number*	スイッチが同期するためにピアの NTP 装置がその NTP パケットに提供する必要のある 1 つまたは複数のキー番号（ステップ 3 で定義）を指定します。 デフォルトでは、信頼できるキーは定義されていません。 *key-number* には、ステップ 3 で定義したキーを指定します。 このコマンドを指定すると、スイッチが誤って信頼できない装置と同期することがなくなります。
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）設定をコンフィギュレーション ファイルに保存します。

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。認証キーを削除するには、**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。装置の 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、装置の NTP パケットで認証キー 42 を提供する装置とだけ同期するよう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（スイッチを他の装置に同期することも、他の装置をスイッチに同期することもできる）、またはサーバ アソシエーション（スイッチだけが他の装置に同期でき、他の装置からは同期することができない）として設定できます。

別の装置との NTP アソシエーションを作成するには、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	**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	**ntp peer** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	ピアを同期するか、ピアによって同期される（ピア アソシエーション）ようにスイッチのシステム クロックを設定します。
	または	または
	ntp server *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	タイム サーバで同期される（サーバ アソシエーション）ようにスイッチのシステム クロックを設定します。 デフォルトでは、ピア アソシエーションまたはサーバ アソシエーションは定義されていません。 • ピア アソシエーションの *ip-address* には、クロック同期を提供しているピア、またはクロック同期が提供されているピアの IP アドレスを指定します。サーバ アソシエーションの場合は、クロック同期を提供しているタイム サーバの IP アドレスを指定します。 • （任意）*number* 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）*keyid* には、**ntp authentication-key** グローバル コンフィギュレーション コマンドで定義した認証キーを入力します。 • （任意）*interface* には、IP 送信元アドレスを選択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されます。 • （任意）**prefer** キーワードを入力して、このピアまたはサーバを、同期を提供する優先ピアまたはサーバにします。このキーワードにより、ピアとサーバ間の切り替えが削減されます。
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**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アソシエーションの一端の装置だけ設定する必要があります。もう一方の装置では、アソシエーションは自動的に設定されます。デフォルトの NTP バージョン（バージョン 3）を使用しているときに NTP 同期が行われない場合は、NTP バージョン 2 を使用してみてください。インターネット上の多くの NTP サーバがバージョン 2 を実行しています。

ピア アソシエーションまたはサーバ 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 にあるピアのクロックとシステム クロックを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 server 172.16.22.44 version 2
```

NTP ブロードキャスト サービスの設定

NTP を実行している装置間の通信（*アソシエーション*）は通常、スタティックに設定されます。各装置には、アソシエーションの作成に使用するすべての装置の 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装置間で NTP メッセージを交換することで、正確なタイムキーピングが実現されます。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。この代替の方法では、ブロードキャスト メッセージを送受信するように各装置を設定するだけなので、設定の複雑さが解消されます。ただし、情報の流れは一方向に限定されます。

ルータなどの NTP ブロードキャスト サーバがあり、ネットワーク上で時刻の情報をブロードキャストしている場合、スイッチはインターフェイス単位で 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 パケットをピアに送信して、ピアがスイッチと同期できるようにします。また、スイッチは NTP ブロードキャスト パケットを受信して独自のクロックを同期することもできます。ここでは、NTP ブロードキャスト パケットを送受信する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、ピアがそれぞれのクロックをスイッチと同期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	**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*	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	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]	NTP ブロードキャス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になっています。 • （任意）*number* 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い場合、バージョン 3 が使用されます。 • （任意）*keyid* には、パケットをピアに送信するときに使用する認証キーを指定します。 • （任意）*destination-address* には、そのクロックをこのスイッチと同期しているピアの IP アドレスを指定します。
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）設定をコンフィギュレーション ファイルに保存します。
ステップ 7		次の手順で説明するように NTP ブロードキャスト パケットを受信するよう、接続されているピアを設定します。

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

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

接続されているピアから 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	**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*	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	**ntp broadcast client**	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イネーブルにします。 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	**exit**	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	**ntp broadcastdelay** *microseconds*	（任意）スイッチと NTP ブロードキャスト サーバ間の予測されるラウンドトリップ遅延を変更します。 デフォルト値は 3000 マイクロ秒です。範囲は 1 ～ 999999 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスによる NTP ブロードキャストの受信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。予測されるラウンドトリップ遅延をデフォルト値に変更するには、**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、NTP ブロードキャスト パケットを受信するようにポートを設定する例を示します。

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

NTP アクセス制限の設定

- 「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.7-9）
- 「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.7-10）

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	**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	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*	アクセス グループを作成し、基本 IP アクセス リストを適用します。 キーワードの意味は次のとおりです。 • **query-only**：NTP 制御クエリーだけ許可します。 • **serve-only**：時刻の要求だけ許可します。 • **serve**：時刻の要求と NTP 制御クエリーを許可しますが、スイッチはリモート装置と同期できません。 • **peer**：時刻の要求と NTP 制御クエリーを許可し、スイッチはリモート装置と同期できます。 *access-list-number* には、1 ～ 99 までの標準 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* **permit** *source* [*source-wildcard*]	アクセス リストを作成します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • **permit** キーワードを入力し、条件が一致した場合にアクセスを許可します。 • *source* の場合は、スイッチへのアクセスが許可される装置の 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 ビットを入力します。 **（注）** アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれ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**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アクセス グループ キーワードが、次の順序で（最も制限の少ないものから最も制限の大きいものへ）スキャンされます。

1. **peer**：時刻の要求と NTP 制御クエリーを許可し、スイッチはアドレスがアクセス リスト基準を満たしている装置とスイッチを同期できます。
2. **server**：時刻の要求と NTP 制御クエリーを許可しますが、スイッチはアドレスがアクセス リスト基準を満たしている装置とスイッチを同期できません。
3. **serve-only**：アドレスがアドレス リスト基準を満たす装置からの時刻の要求だけ許可します。
4. **query-only**:アドレスがアクセス リスト基準を満たす装置からの NTP 制御クエリーだけ許可します。

送信元 IP アドレスが、複数のアクセス タイプのアクセス リストと一致した場合、最初のタイプが許可されます。アクセス グループが指定されていない場合は、すべてのアクセス タイプがすべての装置に許可されます。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 タイプだけ許可されます。

スイッチの NTP サービスへのアクセス制御を削除するには、**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、アクセス リスト 99 のピアと同期するためのスイッチを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 からの時刻の要求だけ許可するようにアクセスを制限します。

```
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でデフォルトでイネーブルになっています。

NTP パケットのインターフェイス上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**	NTP パケットのインターフェイス上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）設定をコンフィギュレーション ファイルに保存します。

NTP パケットのインターフェイス上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 パケットの送信元 IP アドレスの設定

スイッチで NTP パケットを送信する場合、送信元 IP アドレスは通常、NTP パケットが送信されるときに使用される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 パケットで特定の送信元 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されます。このコマンドは、インターフェイス上のアドレスが、応答パケットの宛先として使用できない場合に役に立ちます。

送信元 IP アドレスが取得され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	**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	**ntp source** *type number*	送信元 IP アドレスが取得され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によって設定されます。
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**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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.7-5）の説明に従って、**ntp peer** または **ntp server** グローバル コンフィギュレーション コマンドで **source** キーワードを使用します。

NTP の設定の表示

NTP 情報を表示するには、次の 2 つの特権 EXEC コマンドを使用します。

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

（注）　この出力に表示されるフィールドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*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、システムを再起動した後に、手動で日時を設定できます。次にシステムを再起動するまで、時刻は正確な状態で維持されます。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。スイッチが同期できる外部の時刻源がある場合、システム クロックを手動で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.7-11）
- 「日時設定の表示」（P.7-12）
- 「時間帯の設定」（P.7-12）
- 「夏時間の設定」（P.7-13）

システム クロックの設定

NTP サーバなど、時刻サービスを提供する外部の時刻源がネットワーク上にある場合、システム クロックを手動で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	**clock set** *hh*:*mm*:*ss day month year* または **clock set** *hh*:*mm*:*ss month day year*	次のフォーマットのいずれか 1 つを使用して、システム クロックを手動で設定します。 • *hh*:*mm*:*ss* には、24 時間形式の時間、分、秒で時刻を指定します。指定された時刻は、設定された時間帯に基づきます。 • *day* には、月の日付を指定します。 • *month* には、月の名前を指定します。 • *year* には、年（省略なし）を指定します。

次に、システム クロックを 2001 年 7 月 23 日の午後 1 時 32 分に手動で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 クロックでは、時刻が信頼できる（正確であると確信できる）かどうかを示す *authoritative* フラグが維持されます。システム クロックが NTP などのタイミング ソースにより設定されている場合、フラグが設定されます。時刻が信頼できない場合、時刻は表示目的でだけ使用されます。クロックが信頼でき、*authoritative* フラグが設定されるまでは、フラグによって、ピアの時刻が無効な場合にピアはクロックと同期されません。

show clock 表示の前にある記号の意味は次のとおりです。

- *****：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 は同期されません。

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	**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 timezone** *zone hours-offset* [*minutes-offset*]	時間帯を設定します。 スイッチでは、UTC の内部時刻が維持されるため、このコマンドは、表示目的および時刻を手動で設定する場合にだけ使用されます。 • *zone* には、標準時間が有効なときに表示される時間帯の名前を入力します。デフォルトは UTC です。 • *hours-offset* には、UTC からの時間のオフセットを入力します。 • （任意）*minutes-offset* には、UTC からの分のオフセットを入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
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）設定をコンフィギュレーション ファイルに保存します。

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、現地の時間帯が UTC との時間差を 1 時間における割合で表す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の Atlantic Standard Time（AST; 大西洋標準時）が UTC-3.5 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

毎年の特定の曜日に夏時間が開始および終了する区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	**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* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年指定された日付に開始および終了する夏時間を設定します。 夏時間はデフォルトではディセーブルになっています。パラメータを指定せずに **clock summer-time** *zone* **recurring** を指定すると、夏時間のルールはデフォルトで米国のルールに設定されます。 • *zone* には、夏時間が有効な場合に表示される時間帯の名前（PDT など）を指定します。 • （任意）*week* には、月の週（1 ～ 5 または **last**）を指定します。 • （任意）*day* には、曜日（Sunday、Monday など）を指定します。 • （任意）*month* には、月（January、February など）を指定します。 • （任意）*hh*:*mm* には、24 時間形式の時間と分を指定します。 • （任意）*offset* には、夏時間の間に追加する分数を指定します。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）設定をコンフィギュレーション ファイルに保存します。

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、夏時間が開始される日時を指定します。2 つ目の部分では終了する日時を指定します。すべての時刻は、現地の時間帯に基づきます。開始時刻は、標準時間に基づきます。終了時刻は、夏時間に基づきます。開始月が終了月よりあとの場合は、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 1 日曜日の 2 時に開始し、10 月の最終日曜日の 2 時に終了するように指定する例を示します。

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

区域の夏時間が定期的なパターンに従わない（次の夏時間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*]]	最初の日付から開始し、2 つ目の日付で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はディセーブルになっています。 • *zone* には、夏時間が有効な場合に表示される時間帯の名前（PDT など）を指定します。 • （任意）*week* には、月の週（1 ～ 5 または **last**）を指定します。 • （任意）*day* には、曜日（Sunday、Monday など）を指定します。 • （任意）*month* には、月（January、February など）を指定します。 • （任意）*hh*:*mm* には、24 時間形式の時間と分を指定します。 • （任意）*offset* には、夏時間の間に追加する分数を指定します。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）設定をコンフィギュレーション ファイルに保存します。

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、夏時間が開始される日時を指定します。2 つ目の部分では終了する日時を指定します。すべての時刻は、現地の時間帯に基づきます。開始時刻は、標準時間に基づきます。終了時刻は、夏時間に基づきます。開始月が終了月よりあとの場合は、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 2000 年 10 月 12 日の 2 時に開始し、2001 年 4 月 26 日の 2 時に終了するように設定する例を示します。

```
Switch(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

システム名とプロンプトの設定

スイッチにシステム名を設定して識別します。デフォルトでは、システム名とプロンプトは *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 文字がシステム プロンプトとして使用されます。大なり記号 [>] が追加されます。システム名が変更されるたびにプロンプトが更新されます。

この項で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Configuration Fundamentals Command Reference*』および『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』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とプロンプトの設定」（P.7-15）
- 「システム名の設定」（P.7-15）
- 「DNS の概要」（P.7-15）

デフォルトのシステム名とプロンプトの設定

デフォルトのスイッチ システム名とプロンプトは *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	**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	**hostname** *name*	手動でシステム名を設定します。 デフォルト設定は *switch* です。 名前は、ARPANET ホスト名のルールに従う必要があります。名前の先頭は文字で始まり、文字または数字で終わり、その間には文字、数字、およびハイフンしか使用できません。名前には最大 63 文字を使用できます。
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**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

システム名を設定すると、その名前はシステム 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、DNS を制御します。DNS は、ホスト名を IP アドレスにマッピングできる分散データベースです。スイッチ上に DNS を設定すると、**ping**、**telnet**、**connect** などのすべての IP コマンドおよび関連の 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 は、場所やドメインによって装置を識別できる階層型の命名方式を定義します。ドメイン名は、デリミタにピリオド (.) を使用して連結できます。たとえば、シスコシステムズは、IP が *com* というドメイン名で識別される商業組織なので、ドメイン名は *cisco.com* となります。このドメインの特定の装置、たとえば File Transfer Protocol（FTP; ファイル転送プロトコル）システムは *ftp.cisco.com* として識別されます。

ドメイン名を継続的に追跡するために、IP はドメイン ネーム サーバの概念を定義しています。このサーバには、IP アドレスにマッピングされる名前のキャッシュ（またはデータベース）が保持されます。ドメイン名を IP アドレスにマッピングするには、まずホスト名を識別し、ネットワーク上にあるネーム 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.7-16）
- 「DNS の設定」（P.7-16）
- 「DNS の設定の表示」（P.7-17）

DNS のデフォルト設定

表 7-2 に、DNS のデフォルト設定を示します。

表 7-2　DNS のデフォルト設定

機能	デフォルト設定
DNS イネーブル ステート	イネーブル
DNS デフォルト ドメイン名	設定なし
DNS サーバ	ネーム サーバ アドレスの設定なし

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	**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	**ip domain-name** *name*	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、ドメイン名は設定されませんが、BOOTP または Dynamic Host Configuration Protocol（DHCP）サーバからスイッチの設定を取得している場合は、BOOTP または DHCP サーバでデフォルトのドメイン名が設定されている可能性があります（サーバがこの情報を使用して設定されている場合）。
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	名前とアドレスの解決に使用する、1 つまたは複数のネーム サーバのアドレスを指定します。 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。
ステップ 4	**ip domain-lookup**	（任意）スイッチで、DNS ベースのホスト名から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なっています。 使用するネットワーク装置が、名前の割り当てを制御していないネットワーク内の装置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、装置を一意に識別する装置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）設定をコンフィギュレーション ファイルに保存します。

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 クエリーは発生しません。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に追加され、そのあとで DNS クエリーが行われ、名前が IP アドレスにマッピングされます。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 の設定の表示

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）とログイン バナーを設定できます。MOTD バナーは、ログイン時に接続されているすべての端末に表示され、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）を送信するのに役立ちます。

ログイン バナーも、接続され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）　この項で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*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.7-17）
- 「Message-Of-The-Day ログイン バナーの設定」（P.7-17）
- 「ログイン バナーの設定」（P.7-19）

バナーのデフォルト設定

MOTD バナーとログイン バナーは設定されません。

Message-Of-The-Day 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	**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	**banner motd** *c message c*	該当の日のメッセージを指定します。 *c* には、任意のデリミタ、たとえばポンド記号（#）を入力して、Return キーを押します。デリミタは、バナー テキストの始まりと終わりを表します。終わりのデリミタのあとの文字は廃棄されます。 *message* には、最大 255 文字のバナー メッセージを入力します。メッセージにはデリミタを使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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（#）を始まりのデリミタおよび終わりのデリミタとして使用し、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の例を示します。

```
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

接続されている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	**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	**banner login** *c message c*	ログイン メッセージを指定します。 *c* には、任意のデリミタ、たとえばポンド記号（#）を入力して、Return キーを押します。デリミタは、バナー テキストの始まりと終わりを表します。終わりのデリミタのあとの文字は廃棄されます。 *message* には、最大 255 文字のログイン メッセージを入力します。メッセージにはデリミタを使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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（$）を始まりのデリミタおよび終わりのデリミタとして使用し、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

Media Access Control（MAC; メディア アクセス制御）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。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関連付けられます。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 アドレス。

アドレス テーブルは、宛先 MAC アドレス、関連付けられている VLAN ID、アドレスとタイプ（スタティックまたはダイナミック）に関連付けられているポート番号を示します。

（注） この項で使用しているコマンドの構文と使用方法の詳細については、このリリースのコマンド 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

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、その他のネットワーク装置に接続できます。各ポートで受信するパケットの送信元アドレスを学習し、アドレス テーブルにアドレスと関連付けられているポート番号を追加することにより、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 テーブルを更新し、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を期限切れにします。

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、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）によって VLAN 単位でエージング インターバルを短縮できます。

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、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 テーブルを使用して、スイッチは宛先アドレスに関連付けられているポートにだけ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。つまり、完全なパケットを保管して、エラーがないかチェックしてから転送されます。

MAC アドレスと VLAN

すべてのアドレスは VLAN に関連付けられています。1 つのアドレスを複数の VLAN に関連付け、それぞれに異なる宛先を設定できます。たとえば、ユニキャスト アドレスを VLAN 1 のポート 1 および VLAN 5 のポート 9、10、および 1 に転送できます。

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 で既知のアドレスが別の 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、スタティックに関連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は、アドレス学習は MAC アドレスのタイプによって異なります。

- プライベート VLAN の 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連する 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 VLAN またはセカンダリ VLAN で設定されたスタティック MAC アドレスは、関連付けられている VLAN には複製されません。プライベート VLAN のプライマリ VLAN またはセカンダリ VLAN にスタティック MAC アドレスを設定するときは、同じスタティック MAC アドレスを、関連付けられているすべての VLAN にも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 19 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 テーブルのデフォルト設定

表 7-3 に、MAC アドレス テーブルのデフォルト設定を示します。

表 7-3　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	自動的に学習
スタティック アドレス	設定なし

アドレスのエージング 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、使用されなくなった時点で期限切れとなる送信元 MAC アドレスです。すべての VLAN または指定された VLAN のエージング タイムの設定を変更できます。

エージング タイムの設定が短すぎると、アドレスがテーブルから削除されるのが早くなります。また、スイッチで不明な宛先のパケットを受信すると、受信ポートと同じ VLAN 内のすべてのポートにパケットがフラッディングします。この不要なフラッディングによって、パフォーマンスに影響を与える可能性があります。エージング タイムの設定が長すぎると、アドレス テーブルは未使用のアドレスで一杯になり、新しいアドレスが学習されなくなります。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影響を与える可能性があります。

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	**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	**mac address-table aging-time** [**0** | *10-1000000*] [**vlan** *vlan-id*]	ダイナミック エントリが使用または更新されたあと、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。 *vlan-id* に指定できる有効な ID は 1 ～ 4094 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show mac address-table aging-time**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

すべてのダイナミック エントリを削除するには、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 アドレス変更通知では、MAC アドレスの変更アクティビティを保存して、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きに、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）通知トラップを Network Management System（NMS; ネットワーク管理システム）に送信できます。多くのユーザがネットワークに出入りしている場合は、トラップの間隔を設定して通知トラップをバンドルし、ネットワーク トラフィックを削減できます。MAC 通知履歴テーブルには、トラップが設定されている各ポートの MAC アドレス アクティビティが保存されます。MAC アドレス変更通知は、ダイナミック MAC アドレスまたはセキュア MAC アドレスについて許可されます。自アドレス、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、通知は生成されません。

MAC アドレス変更通知トラップを NMS ホストに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	**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 host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* には、NMS の名前または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。情報の場合は、デフォルトのバージョン 1 を使用できません。 • *community-string* には、通知処理で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。 • *notification-type* には、**mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification change**	MAC アドレス変更通知トラップを NMS に送信するようにスイッチをイネーブルにします。
ステップ 4	**mac address-table notification change**	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	**mac address-table notification change** [**interval** *value*] [**history-size** *value*]	トラップの間隔と履歴テーブルのサイズを入力します。 • （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間隔を秒単位で指定します。指定できる範囲は 0 ～ 2147483647 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エントリの最大数を指定します。指定できる範囲は 0 ～ 500 です。デフォルトは 1 です。
ステップ 6	**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、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。
ステップ 7	**snmp trap mac-notification change** {**added** | **removed**}	インターフェイス上で MAC アドレス変更通知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に**追加された**ときに、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**削除された**ときに、トラップをイネーブルにします。

	コマンド	目的
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mac address-table notification change interface** **show running-config**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、172.20.10.10 を NMS として指定し、MAC アドレス通知トラップを NMS に送信するようにスイッチをイネーブルにし、MAC アドレス変更通知機能をイネーブルにし、間隔を 123 秒に設定し、履歴サイズを 100 エントリまでとし、MAC アドレスが指定されたポートに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 gigabitethernet1/2
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 アドレス移行通知トラップの設定

MAC 移行通知を設定すると、MAC アドレスが同じ VLAN 内の別のポートに移行するたびに、SNMP 通知が生成されて、ネットワーク管理システムに送信されます。

MAC アドレス移行通知トラップを NMS ホストに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	**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 host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* には、NMS の名前または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。情報の場合は、デフォルトのバージョン 1 を使用できません。 • *community-string* には、通知処理で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。 • *notification-type* には、**mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification move**	MAC アドレス移行通知トラップを NMS に送信するようにスイッチをイネーブルにします。
ステップ 4	**mac address-table notification mac-move**	MAC アドレス移行通知機能をイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show mac address-table notification mac-move** **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

MAC アドレス移行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 アドレス移行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、172.20.10.10 を NMS として設定し、MAC アドレス移行通知トラップを NMS に送信するようにスイッチをイネーブルにし、MAC アドレス移行通知機能をイネーブルにし、MAC アドレスが別のポートに移行したとき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 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 スレッシュホールド通知トラップの設定

MAC スレッシュホールド通知を設定すると、MAC アドレス テーブルのスレッシュホールド制限に達するか、スレッシュホールド制限を超えると、SNMP 通知が生成されて、ネットワーク管理システムに送信されます。

MAC アドレス テーブル スレッシュホールド通知トラップを NMS ホストに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	**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 host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* には、NMS の名前または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。情報の場合は、デフォルトのバージョン 1 を使用できません。 • *community-string* には、通知処理で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。 • *notification-type* には、**mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification threshold**	MAC スレッシュホールド通知トラップを NMS に送信するようにスイッチをイネーブルにします。
ステップ 4	**mac address-table notification threshold**	MAC アドレススレッシュホールド通知機能をイネーブルにします。
ステップ 5	**mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]	MAC アドレス スレッシュホールド使用状況のモニタリングのスレッシュホールドを入力します。 • （任意）limit percentage には、MAC アドレステーブルの使用割合を指定します。有効値は 1 ～ 100% です。デフォルト値は 50% です。 • （任意）interval time には、通知間隔を指定します。有効値は 120 秒以上です。デフォルト値は 120 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mac address-table notification threshold** **show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

MAC アドレス スレッシュホールド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 スレッシュホールド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、172.20.10.10 を NMS として設定し、MAC アドレス スレッシュホールド通知機能をイネーブルにし、間隔を 123 秒に設定し、制限を 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 エントリの追加と削除

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 テーブルに手動で入力し、手動で削除する必要があります。
- ユニキャスト アドレスまたはマルチキャスト アドレスとして使用できます。
- 期限切れにならず、スイッチの再起動時に保持されます。

スタティック アドレスを追加および削除し、それらのアドレスの転送動作を定義できます。転送動作では、パケットを受信するポートがパケットを別の伝送用ポートに転送する方法を定義します。すべてのポートは少なくとも 1 つの VLAN に関連付けられているため、スイッチは指定したポートからアドレスの VLAN ID を取得します。送信元ポートごとに異なる宛先ポート リストを指定できます。

スタティックに入力されていない VLAN に、スタティック アドレスを持つパケットが着信した場合、そのパケットはすべてのポートにフラッディングされ、学習されません。

宛先 MAC ユニキャスト アドレスと受信元の VLAN を指定して、スタティック アドレスをアドレス テーブルに追加します。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 VLAN またはセカンダリ VLAN にスタティック MAC アドレスを設定するときは、同じスタティック MAC アドレスを、関連付けられているすべての VLAN にも設定する必要があります。プライベート VLAN のプライマリ VLAN またはセカンダリ VLAN で設定されたスタティック MAC アドレスは、関連付けられている 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 19 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	**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	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	スタティック アドレスを MAC アドレス テーブルに追加します。 • *mac-addr* 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。 • *vlan-id* 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。 • *interface-id* には、受信されたパケットを転送するインターフェイスを指定します。有効なインターフェイスは、物理ポートまたはポート チャネルです。スタティック マルチキャスト アドレスの場合は、複数のインターフェイス ID を入力できます。スタティック ユニキャスト アドレスの場合は、一度に 1 つのインターフェイスだけ入力できます。ただし、同じ MAC アドレスと VLAN ID を使用してコマンドを複数回入力できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table static**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スタティック エントリをアドレス テーブルから削除するには、**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パケットを受信すると、パケットは指定されたポートに転送されます。

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

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、特定の送信元または宛先 MAC アドレスのパケットを廃棄します。この機能はデフォルトではディセーブルになっています。また、この機能ではユニキャスト スタティック アドレスだけサポートされます。

この機能を使用する場合、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、これらのいずれかのアドレスを指定すると、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廃棄します。2 番め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廃棄します。

  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、送信元または宛先のユニキャスト MAC アドレスと受信元の VLAN を指定して、特定のアドレスのパケットを廃棄するようにスイッチを設定します。

送信元または宛先のユニキャスト スタティック アドレスを廃棄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	**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	**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**	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、指定された送信元または宛先のユニキャスト スタティック アドレスのパケットを廃棄するようにスイッチを設定します。 • *mac-addr* には、送信元または宛先のユニキャスト 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廃棄されます。 • *vlan-id* 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	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table static**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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廃棄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、パケットが廃棄されます。

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

VLAN での MAC アドレス学習のディセーブル化

デフォルトでは、MAC アドレス学習はスイッチのすべての VLAN でイネーブルです。VLAN で MAC アドレス学習を制御して、MAC アドレスを学習できる VLAN、さらにポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。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。

VLAN で MAC アドレス学習をディセーブルにする場合、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）を設定済みの VLAN で MAC アドレス学習をディセーブルにする場合は十分注意してください。この場合、スイッチは、レイヤ 2 ドメインにすべての IP パケットをフラッディングします。
- MAC アドレス学習は、1 つの VLAN ID（例 : **no mac address-table learning vlan 223**）または一連の VLAN ID（例 : **no mac address-table learning vlan 1-20, 15**）でディセーブルにできます。
- MAC アドレス学習のディセーブル化はポートを 2 つ含む VLAN だけで行うことを推奨します。3 つ以上のポートを含む VLAN で MAC アドレス学習をディセーブルにした場合、スイッチに着信するすべてのパケットは、その VLAN ドメインでフラッディングします。
- スイッチが内部的に使用する VLAN で MAC アドレス学習をディセーブルにできません。入力する VLAN ID が内部 VLAN である場合、スイッチはエラー メッセージを生成してコマンドを拒否します。使用している内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを使用します。
- プライベート VLAN のプライマリ VLAN として設定された VLAN で MAC アドレス学習をディセーブルにする場合、MAC アドレスは、そのプライベート VLAN に属するセカンダリ VLAN 上で引き続き学習され、プライマリ VLAN に複製されます。プライベート VLAN のプライマリ VLAN ではなくセカンダリ VLAN で MAC アドレス学習をディセーブルにする場合、プライマリ VLAN で MAC アドレス学習が実行され、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 MAC アドレス学習をディセーブルにする場合、セキュア ポートで MAC アドレス学習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する場合、設定した MAC アドレス学習の状態がイネーブルになります。

VLAN で MAC アドレス学習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** *vlan-id*	指定された 1 つまたは複数の VLAN で MAC アドレス学習をディセーブルにします。1 つの VLAN ID を指定するか、一連の VLAN ID をハイフンまたはカンマで区切って指定できます。指定できる VLAN ID は、1 ～ 4094 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 mac address-table learning** [**vlan** *vlan-id*]	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN で MAC アドレス学習を再び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。**mac address-table learning vlan** *vlan-id* グローバル コンフィギュレーション コマンドを入力して、VLAN で MAC アドレス学習を再びイネーブルにすることもできます。1 つ目（**デフォルト**）のコマンドでは、デフォルト設定の状態に戻るため、**show running-config** コマンドを実行しても出力に表示されません。2 つ目のコマンドでは、**show running-config** 特権 EXEC コマンドの表示に設定が表示されます。

次に、VLAN 200 で MAC アドレス学習をディセーブルにする例を示します。

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

すべての VLAN、または指定された VLAN の MAC アドレス学習のステータスを表示するには、**show mac-address-table learning** [**vlan** *vlan-id*] 特権 EXEC コマンドを入力します。

アドレス テーブル エントリの表示

表 7-4 で説明されている 1 つまたは複数の特権 EXEC コマンドを使用して、MAC アドレス テーブルを表示できます。

表 7-4　MAC アドレス テーブルを表示するためのコマンド

コマンド	説明
show ip igmp snooping groups	すべての VLAN または指定された VLAN のレイヤ 2 マルチキャスト エントリを表示します。
show mac address-table 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 または指定された VLAN の MAC アドレス学習のステータスを表示します。
show mac address-table notification	MAC 通知パラメータと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 エントリだけを表示します。
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

イーサネットなどを介して装置と通信するために、ソフトウェアは最初にその装置の 48 ビットの MAC アドレスまたはローカル データ リンク アドレスを学習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 アドレスを学習するプロセスは、*アドレス解決*と呼ばれます。

Address Resolution Protocol（ARP; アドレス解決プロトコル）は、ホストの IP アドレスを対応するメディアまたは MAC アドレスおよび VLAN ID に関連付けます。ARP は、IP アドレスを使用して、関連付けられた MAC アドレスを検索します。MAC アドレスが見つかると、IP と MAC アドレスの関連付けが ARP キャッシュに保存され、すぐに取得できます。次に、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、ネットワーク上で送信されます。イーサネット以外の IEEE 802 ネットワークでの IP データグラムおよび ARP 要求および応答のカプセル化は、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）で指定されます。デフォルトでは、IP インターフェイスで標準の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）はイネーブルになっています。

テーブルに手動で追加された ARP エントリは期限切れがないため、手動で削除する必要があります。

（注） CLI の手順の詳細については、Cisco.com のページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] にある Cisco IOS Release 12.2 のマニュアルを参照してください。