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 回限りの手順について説明しています。

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）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）　ここで説明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

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働し、日時を常時監視します。

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 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監視します。ローカルのタイム ゾーンおよび夏時間に関する情報を設定することにより、時刻がローカルのタイム ゾーンに応じて正確に表示されるようにできます。

システム クロックは、時刻が*信頼できる*かどうか（つまり、信頼できるとみなされるタイム ソースによって時刻が設定されているか）を常時監視します。信頼できない場合は、時刻は表示目的でのみ利用され、再配信されません。設定の詳細については、「手動による日時の設定」（p.6-12）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 UDP で稼働し、UDP は IP 上で稼働します。NTP は RFC 1305 に規定されています。

NTP ネットワークは通常、ラジオ クロックやタイム サーバに接続された原子時計など、信頼できるタイム ソース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 つのデバイスを 1 ミリ秒以内に同期化できます。

NTP は、*ストラタム*（*階層*）という概念を使用して、信頼できるタイム ソースからデバイスまでの NTP ホップ数を記述します。ストラタム 1 タイム サーバには、ラジオ クロックまたは原子時計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 を実行するデバイスは、タイム ソースとして、NTP を使用して通信するストラタム番号が最少である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。

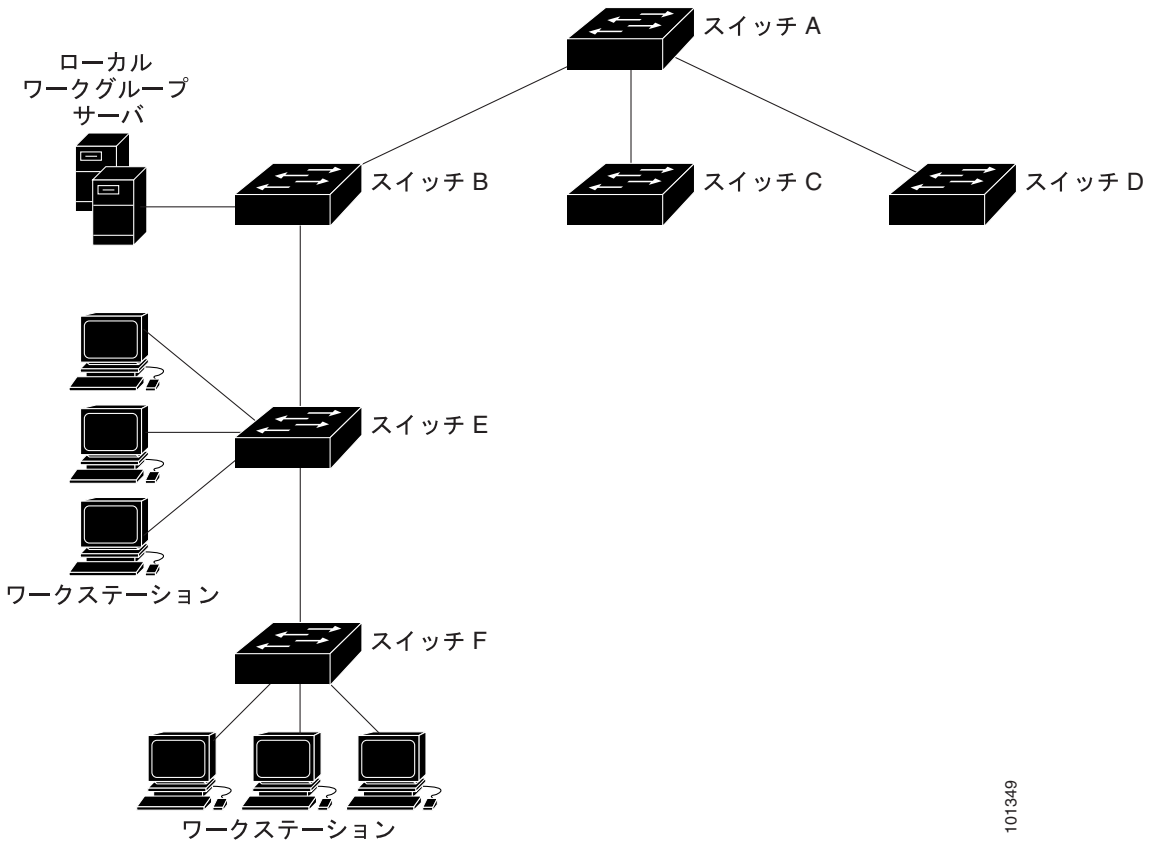
NTP が稼働するデバイス間の通信（*アソシエーション*）は、通常スタティックに設定されます。各デバイスには、アソシエーションを作成すべき全デバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定することができます。単にブロードキャスト メッセージを送受信するように各デバイスを設定すればよいため、この代替手段によって設定作業が容易になります。ただし、この場合は、情報の流れは一方向に限られます。

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あるいは意図的に設定されるのを防止する必要があります。アクセス リストベースの制約方式と、暗号化された認証メカニズムの 2 つのメカニズムが利用できます。

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ため、ラジオ クロックまたは原子時計に接続できません。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 6-1 に、NTP を使用する一般的なネットワークの例を示します。スイッチ A は NTP マスターであり、スイッチ B、C、D は、スイッチ A とのサーバ アソシエーションのある NTP サーバ モードに設定されています。スイッチ E はアップストリームおよびダウンストリーム スイッチ（スイッチ B および F）に対する NTP ピアとして設定されています。

図 6-1　一般的な NTP ネットワーク構成



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。

複数のタイム ソースがある場合は、常に NTP のほうが信頼性が高いとみなされます。NTP の時刻は、他の方法による時刻に優先します。

いくつかのメーカーでは自社のホスト システムに NTP ソフトウェアを組み入れており、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.6-5）
- NTP 認証の設定（p.6-5）
- NTP アソシエーションの設定（p.6-7）

NTP のデフォルト設定

表 6-1 に、NTP のデフォルト設定を示します。

表 6-1　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	設定なし
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（正確な時間の維持を行う NTP 稼働デバイス間の通信）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	説明
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設定されている 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*	認証鍵を定義します。デフォルト設定では何も定義されていません。 • *number* には、鍵の番号を指定します。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サポートが行われることを指定します。 • *value* 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。 スイッチとデバイスの双方がいずれかの認証鍵を持ち、**ntp trusted-key** *key-number* 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。

	コマンド	説明
ステップ 4	**ntp trusted-key** *key-number*	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。 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。 *key-number* には、ステップ 3 で定義された鍵を指定します。 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のを防ぎます。
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。

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 が設定されているデバイスとのみ同期するようにスイッチを設定する例を以下に示します。

```
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、他のデバイスをスイッチに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のみで、その逆は不可）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	説明
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**]	スイッチのシステム クロックにピアを同期化するか、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	または
	ntp server *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	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。 • ピア アソシエーションの *ip-address* 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）*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 コマンドで定義された認証鍵を入力します。 • （任意）*interface* 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。このキーワードを使用すると、ピアとサーバ間の切り換えが少なくなります。
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）コンフィギュレーション ファイルに設定を保存します。

アソシエーションは、一端のデバイスに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 NTP 同期化が発生しない場合は、NTP のバージョン 2 を使用してみてください。インターネット上の多くの NTP サーバは、バージョン 2 で稼働しています。

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

NTP が稼働するデバイス間の通信（*アソシエーション*）は、通常スタティックに設定されます。各デバイスには、アソシエーションを作成すべき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、正確な時刻の維持が可能になります。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 を設定することができます。単にブロードキャスト メッセージを送受信するように各デバイスを設定すればよいため、この代替手段によって設定作業が容易になります。ただし、この場合は、情報の流れは一方向に限られます。

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、ピアはそれに同期化することができます。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、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	説明
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 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に設定されています。 • （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かった場合は、バージョン 3 が使用されます。 • （任意）*keyid* 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）*destination-address* 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	**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。
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	説明
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**	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	**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 サーバとの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	**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）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。予測されるラウンドトリップ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.6-10）
- 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.6-11）

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	説明
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 リストを割り当てます。 キーワードの意味は次のとおりです。 • **query-only —** NTP 制御クエリーに限り許可します。 • **serve-only —** 時刻要求に限り許可します。 • **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。 *access-list-number* 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。
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** キーワードを入力すると、条件が一致した場合にアクセスを許可します。 • *source* 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）*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 リストを作成するときは、アクセス リストの末尾に暗黙的な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。
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。

アクセス グループのキーワードは、制限が小さいほうから大きいほうに、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限り許可します。
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 制御クエリーに限り許可します。

送信元 IP アドレスがアクセス リストの複数のアクセス タイプに一致する場合は、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 タイプがすべてのデバイスに許可されます。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 タイプに限り許可されます。

スイッチ NTP サービスに対する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、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、時刻要求に限り許可します。

```
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	説明
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度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 パケットへの送信元 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 アドレスの取得先とな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	説明
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*	IP 送信元アドレスの取得先とな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	**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。

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.6-7）で説明したように、**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**

この出力に表示されるフィールドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。

手動による日時の設定

他のタイム ソースが利用できない場合は、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のみ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.6-12）
- 日時設定の表示（p.6-13）
- タイム ゾーンの設定（p.6-13）
- 夏時間の設定（p.6-14）

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	説明
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。 • *hh*:*mm*:*ss* には、時刻を時間（24 時間制）、分、秒で指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • *day* には、月単位の日付で日を指定します。 • *month* には、月を名前で指定します。 • *year* には、年を指定します（短縮不可）。
ステップ 2	**show running-config**	設定を確認します。
ステップ 3	**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。

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* フラグを維持します。システム クロックが時刻ソース（NTP など）によって設定されている場合は、フラグを設定します。時刻が信頼できない場合は、表示目的でのみ使用されます。クロックが信頼でき、*authoritative* フラグが設定された状態でないと、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 と同期化していません。

タイム ゾーンの設定

手動でタイム ゾーンを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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*]	タイム ゾーンを設定します。 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限って使用します。 • *zone* には、標準時間が施行されているときに表示されるタイム ゾーンの名前を入力します。デフォルトの設定は UTC です。 • *hours-offset* には、UTC からの時差（時間単位）を入力します。 • （任意）*minutes-offset* には、UTC からの時差（分単位）を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	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 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、現地のタイム ゾーンと UTC との時差が分単位である場合に利用できます。たとえば、カナダ大西洋沿岸のある区域のタイム ゾーン（AST）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および終了する地域で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	説明
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*]]	毎年特定の日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。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（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 時間制）と分で指定します。 • （任意）*offset* には、夏時間の間、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）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 番めの部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーン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あとの場合は、システムでは南半球にいるとみなされます。

次に、夏時間が 4 月の第 1 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。

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

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

	コマンド	説明
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*]]	最初の日付で夏時間開始の日付を、2 番めの日付で終了の日付を設定します。
	または	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。
	clock summer-time *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	• *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（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 時間制）と分で指定します。 • （任意）*offset* には、夏時間の間、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）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 番めの部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーン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あとの場合は、システムでは南半球にいるとみなされます。

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

スイッチをシステム名で識別するようにシステム名を設定します。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 文字がシステム プロンプトとして使用されます。かぎカッコ [>] が付加されます。システム名が変更されると、プロンプトは更新されます。

（注）　ここで説明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

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	説明
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	**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。

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 アドレスに対応付けることができます。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名前指定は、デバイスを場所またはドメインで識別できます。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 *com* というドメイン名によって、IP が商業組織だと認識するため、ドメイン名は *cisco.com* です。このドメイン内の特定のデバイス、たとえば FTP（ファイル転送プロトコル）システムは、*ftp.cisco.com* で表されます。

IP でドメイン名を追跡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。DNS は、名前と IP アドレスのマッピングをキャッシュ（またはデータベース）に保存します。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.6-17）
- DNS の設定（p.6-17）
- DNS 設定の表示（p.6-18）

DNS のデフォルト設定

表 6-2 に、DNS のデフォルト設定を示します。

表 6-2　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	説明
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）。

	コマンド	説明
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	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 サーバがクエリーされます。
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名に追加され、そのあとで DNS クエリーが行われ、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、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、すべての接続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）　ここで説明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.6-19）
- MoTD ログイン バナーの設定（p.6-19）
- ログイン バナーの設定（p.6-20）

バナーのデフォルト設定

MoTD バナーおよびログイン バナーは設定されません。

MoTD ログイン バナーの設定

ある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	説明
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*	MoTD メッセージを指定します。 *c* 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。その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あとの文字は廃棄されます。 *message* 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	**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。

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、スイッチに 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

すべての接続端末でログイン 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	説明
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。その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あとの文字は廃棄されます。 *message* 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	**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。

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、スイッチにログイン 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（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 MAC アドレスはすべて、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：手動で入力するユニキャスト アドレス。これらのアドレスには期限がなく、スイッチがリセットされても失われません。

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN（仮想 LAN）ID、およびアドレスとタイプ（スタティックとダイナミック）に対応付けられたポート番号を保持します。

（注）　ここで使用され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 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学習し、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にアドレスを指定します。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は期限切れにします。

有効期間は、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、STP（スパニングツリー プロトコル）によって VLAN ごとの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にのみ、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伝送します。

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 へ伝送できます。

（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他の VLAN で認識されるには、アドレスが他の VLAN 内のポートによって学習されるか、または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 のある VLAN で学習されたダイナミック MAC アドレスは、対応付けられた VLAN で複製されます。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 で複製されます。
- プライマリまたはセカンダリ VLAN で設定されたスタティック MAC アドレスは、対応付けられた VLAN では複製されません。プライベート VLAN のプライマリまたはセカンダリ VLAN 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 の詳細については、第 14 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 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 ラーニングをディセーブルにすると、ネットワーク上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.6-28）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 6-3 に、MAC アドレス テーブルのデフォルト設定を示します。

表 6-3　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	設定なし
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。

設定されたエージング タイムが短すぎると、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、そのパケット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が出る可能性があります。また、設定されたエージング タイムが長すぎると、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	説明
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。デフォルトは 300 秒です。0 も入力できますが、期限切れをディセーブルにします。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* に指定できる範囲は、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 aging-time**	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。

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*）も削除することができます。

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 アドレス通知トラップの設定

MAC アドレス通知によって、スイッチに MAC アドレス 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できます。スイッチが MAC アドレスを学習または削除すると常に、SNMP（簡易ネットワーク管理プロトコル）通知を生成して Network Management System（NMS; ネットワーク管理システム）に送信させることができます。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、トラップがイネーブルに設定されたハードウェアのポートごとの MAC アドレス アクティビティを保存します。MAC アドレス通知は、セキュアなダイナミック MAC アドレスについて生成されます。自己アドレス、マルチキャスト アドレス、またはその他のスタティック アドレスについては、イベントは生成されません。

NMS ホストに MAC アドレス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	説明
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 メッセージの受信デバイスを指定します。 • *hos-addr* 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 インフォームをホストに送信するには、**informs** を指定します。 • サポートされる SNMP バージョンを指定します。バージョン 1 がデフォルトですが、インフォームでは利用できません。 • *community-string* には、通知作業で送信するストリングを指定します。このストリングは、**snmp-server host** コマンドで設定できますが、**snmp-server community** コマンドでこのストリングを定義したあとに **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**	スイッチが MAC アドレス トラップを NMS に送信できるようにします。
ステップ 4	**mac address-table notification**	MAC アドレス通知機能をイネーブルにします。
ステップ 5	**mac address-table notification** [**interval** *value*] | [**history-size** *value*]	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。 • （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、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。

	コマンド	説明
ステップ 7	**snmp trap mac-notification** {**added** | **removed**}	MAC アドレス通知トラップをイネーブルにします。 • このインターフェイスに MAC アドレスが追加されるたびに MAC アドレス通知トラップをイネーブルにするには、**added** を指定します。 • このインターフェイスから MAC アドレスが削除されるたびに MAC アドレス通知トラップをイネーブルにするには、**removed** を指定します。
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 interface** **show running-config**	設定を確認します。
ステップ 10	**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。

スイッチによる MAC アドレス通知トラップの送信をディセーブルにするには、**no snmp-server enable traps mac-notification** 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 アドレス通知トラップをディセーブルにするには、**no snmp trap mac-notification** {**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 アドレス通知機能をディセーブルにするには、**no mac address-table notification** 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 アドレス通知機能をイネーブルにし、インターバル タイムを 60 秒、履歴サイズを 100 エントリ、ポートに MAC アドレスが追加された時点でのトラップをイネーブルに設定する例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private
Switch(config)# snmp-server enable traps mac-notification
Switch(config)# mac address-table notification
Switch(config)# mac address-table notification interval 60
Switch(config)# mac address-table notification history-size 100
Switch(config)# interface fastethernet1/0/4
Switch(config-if)# snmp trap mac-notification added
```

以前のコマンドを確認するには、**show mac address-table notification interface** および **show mac address-table notification** 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し、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。すべてのポートは 1 つまたは複数の VLAN に関連付けられているため、スイッチは、指定されたポートから、そのアドレスに対応する VLAN ID を取得します。

アドレスがスタティックとして入力されていない VLAN にスタティック アドレスを持った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 アドレスおよびその送信先となる VLAN を指定します。この宛先アドレスとともに受信されたパケットは、*interface-id* オプションで指定されたインターフェイスへ転送されます。

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 で設定されたスタティック MAC アドレスは、対応付けられた VLAN では複製されません。プライベート VLAN の詳細については、第 14 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	説明
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*	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。 • *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。指定した VLAN が、この宛先アドレスを持つパケットを受信すると、指定したインターフェイスへ転送します。 • *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。指定できる範囲は 1 ～ 4094 です。 • *interface-id* には、受信したパケットの転送先とな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などです。
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）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。

次に、MAC アドレス テーブルに、スタティック アドレス c2f3.220a.12f4 を追加する例を示します。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 フィルタリングをイネーブルにすると、スイッチは特定の送信元または宛先 MAC アドレスを持つ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で、ユニキャスト スタティック アドレスのみをサポートします。

この機能を使用するときは、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、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、このアドレスの 1 つを指定した場合、次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は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て、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、スイッチは最後に入力されたコマンドに応じて、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 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 コマンドを入力したあとで、**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** コマンドを入力すると、スイッチは送信元または宛先としての特定の 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 コマンドを入力したあとで、**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* コマンドを入力すると、スイッチはスタティック アドレスとして MAC アドレスを追加します。

送信元または宛先ユニキャスト MAC アドレスおよび受信先の VLAN を指定することにより、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廃棄するように設定します。

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 アドレスを廃棄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	説明
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て、スイッチが特定の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廃棄するように設定します。 • *mac-addr* 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。有効な 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）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。

次に、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 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設定する例を示します。この MAC アドレスを送信元または宛先として持った VLAN 4 で受信されたパケットは、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 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 ラーニングを制御すると、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 ラーニングをディセーブルにすると、ネットワーク上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 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。

- スイッチ仮想インターフェイス（SVI）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。SVI 上で MAC アドレス ラーニングをディセーブルにすると、スイッチはレイヤ 2 ドメインにあるすべての 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、2 つのポートを備えた VLAN でのみ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。スイッチが使用する内部 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 ラーニングをディセーブルにすることはできません。その設定は許可されていません。
- 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、セキュア 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 ステートはアクティブです。

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	説明
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*	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。有効な 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）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。2 番め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。最初の（**default**）コマンドを使用すると、デフォルトの状態に戻ることになるため、設定は **show running-config** コマンドによる出力には含まれません。

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 6-4 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 6-4　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	指定された MAC アドレスに対する 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 に存在するアドレスの数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	指定されたインターフェイスに対する 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 エントリのみを表示します。
show mac address-table vlan	指定された VLAN に対する 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 アドレスを判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 アドレスを判別するプロセスを、「*アドレス解決*」と呼びます。

Address Resolution Protocol（ARP）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 アドレスを判別します。MAC アドレスが判別されると、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 キャッシュに格納されます。その後、IP データグラムはリンク 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 要求や応答については、Subnetwork Access Protocol（SNAP）で規定されています。IP インターフェイスでは、標準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ため、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 Release 12.2 のマニュアルを参照してください。