



CHAPTER 7

スイッチの管理

この章では、Catalyst 2950 または Catalyst 2955 を管理するための一回限りの操作の実行方法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.7-1)
- 「システム名およびプロンプトの設定」(P.7-14)
- 「バナーの作成」(P.7-17)
- 「MAC アドレス テーブルの管理」(P.7-19)
- 「ARP テーブルの管理」(P.7-26)

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)

この章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 for Cisco IOS』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.7-1)
- 「NTP の概要」(P.7-2)
- 「NTP の設定」(P.7-3)
- 「手動での日時の設定」(P.7-11)

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。

- Network Time Protocol (NTP; ネットワーク タイム プロトコル)
- 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トラッキングします。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、時刻は表示目的でのみ使用され、再配信されません。設定情報については、「**手動での日時の設定**」(P.7-11) を参照してください。

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、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、信頼できる時刻源からその時刻を取得します。その後、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 (階層) 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、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 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。

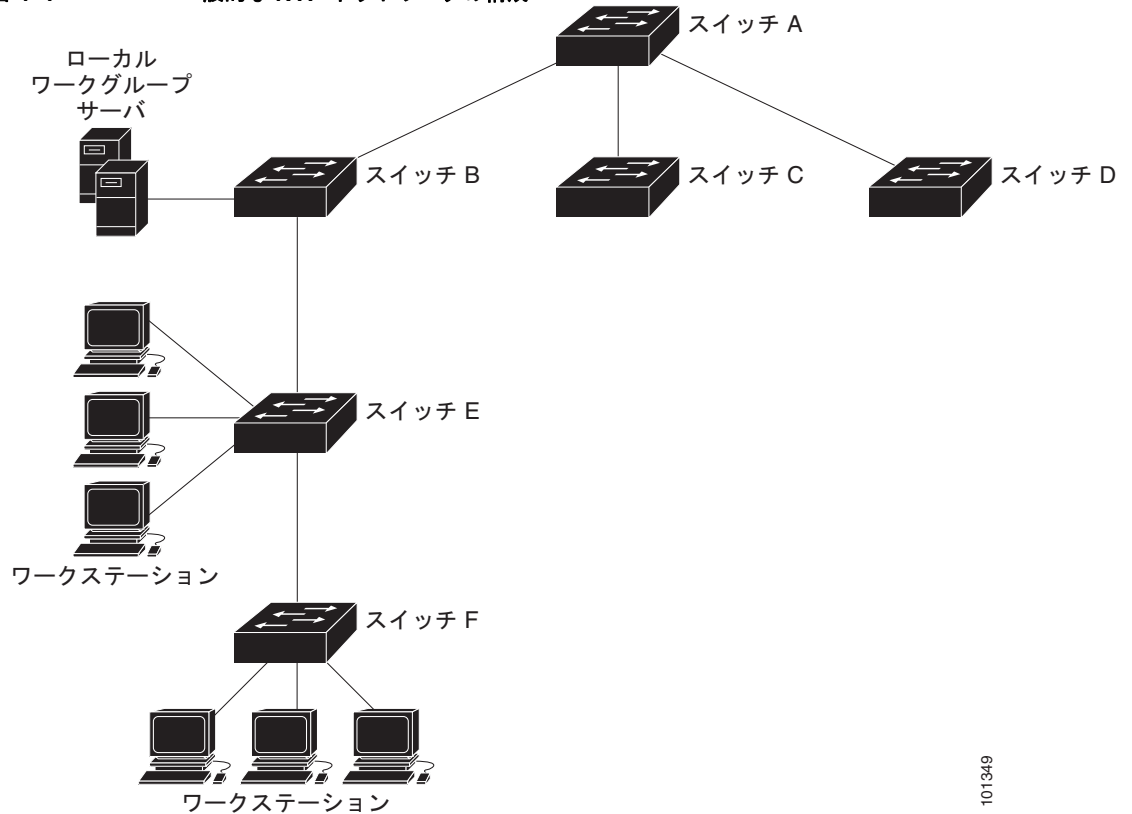
NTP が稼動するデバイス間の通信 (アソシエーション) は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

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、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 7-1 に、NTP を使用した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、アップストリームおよびダウンストリームのスイッチ (スイッチ B およびスイッチ F) への NTP ピアとして設定されます。

図 7-1 一般的な NTP ネットワークの構成



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 実装では、実際には他の方法で時刻が決定されていても、デバイスが NTP を使用して同期化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に優先します。

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は、ピアの同期元としての NTP マスター クロックとして機能できません。また、スイッチは、カレンダーに対するハードウェアの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.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 ブロードキャスト サービスの設定」(P.7-7)

- 「NTP アクセス制限の設定」(P.7-8)
- 「NTP パケット用の送信元 IP アドレスの設定」(P.7-10)
- 「NTP 設定の表示」(P.7-11)

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 サーバの管理者と協調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（正確な時間維持を行う 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。
ステップ 3	<code>ntp authentication-key number md5 value</code>	<p>認証キーを定義します。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"> • <i>number</i> には、キー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ように指定します。 • <i>value</i> には、キーに対する 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キーを持ち、<code>ntp trusted-key key-number</code> コマンドによってキー番号が指定されていない限り、スイッチはデバイスと同期化しません。</p>

	コマンド	目的
ステップ4	<code>ntp trusted-key key-number</code>	1つまたは複数のキー番号（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 パケット内にこのキー番号を設定する必要があります。 デフォルト設定では、信頼されるキーは定義されていません。 <code>key-number</code> 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。
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。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 パケットに認証キー 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のみで、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	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] 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、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キーを入力します。 (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	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 を実行しています。

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 が稼動するデバイス間の通信（アソシエーション）は、通常静的に設定されます。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い場合は、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キーを指定します。 （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 gigabitethernet0/1
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	<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。

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 gigabitethernet0/1
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.7-8)
- 「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.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	<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。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。 <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	access-list access-list-number permit source [source-wildcard]	<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的な deny 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	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、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。

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 タイプに限り認可されます。

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	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によって決定されます。

	コマンド	目的
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.7-5)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`

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 for Cisco IOS*』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.7-11)
- 「[日時設定の表示](#)」(P.7-12)
- 「[タイムゾーンの設定](#)」(P.7-12)
- 「[夏時間の設定](#)」(P.7-13)

システム クロックの設定

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>	次のいずれかの書式で、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、設定されたタイムゾーンに基づきます。 • <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 (必ず 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 年の 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、表示目的でのみ使用されます。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。

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	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>	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。 <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。 • <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、現地のタイムゾーンと 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タイムゾーン (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> [<code>week day month hh:mm week day month</code> <code>hh:mm [offset]</code>]	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 <code>clock summer-time zone recurring</code> を指定すると、夏時間のルールは米国のルールをデフォルトにします。 <ul style="list-style-type: none"> <code>zone</code> 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) <code>week</code> には、月の何週目かを指定します (1 ~ 5、または <code>last</code>)。 (任意) <code>day</code> には、曜日を指定します (Sunday、Monday など)。 (任意) <code>month</code> には、月を指定します (January、February など)。 (任意) <code>hh:mm</code> には、時刻を時間 (24 時間形式) と分で指定します。 (任意) <code>offset</code> には、夏時間の間、追加する分の数を指定します。デフォルトは 60 分です。
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後の場合は、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。

```
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	<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 date [month date year hh:mm month date year hh:mm [offset]]</code> または <code>clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]</code>	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タイム ゾーンの名前（たとえば PDT）を入力します。 • (任意) <i>week</i> には、月の何週目かを指定します（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。デフォルトは 60 分です。
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後の場合は、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 02:00 に始まり、2001 年 4 月 26 日の 02:00 に終わ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、プロンプトは更新されます。



(注)

この章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 for Cisco IOS Release 12.1*』および『*Cisco IOS IP and IP Routing Command Reference for Cisco IOS Release 12.1*』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.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	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 <i>switch</i> です。 名前は ARPANET ホスト名のルールに従う必要があります。このルール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、DNS 分散型データベースを制御し、これによりホスト名を IP アドレスに対応付けできます。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命名方式では、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、は *com* というドメイン名で IP が識別される営利団体であるため、ドメイン名は *.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 File Transfer Protocol (FTP; ファイル転送プロトコル) システムは、*ftp..com* で識別されます。

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、まずホスト名を特定し、ネットワーク上に存在するネーム サーバを指定し、DNS を有効にします。

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	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>	ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成するときに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が設定されません。ただし、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する場合は、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。
ステップ 4	<code>ip domain-lookup</code>	（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動的に割り当てることができます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
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。

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、その後で 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 (.) がある場合は、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) 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 バナーの後で、ログイン プロンプトが表示される前です。



(注)

この章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 for Cisco IOS*』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)
- 「MoTD ログイン バナーの設定」(P.7-17)
- 「ログイン バナーの設定」(P.7-18)

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	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 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	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)#
```

次の例は、上記の設定で表示されるバナーを示しています。

```
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 バナーの後で、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。 <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	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 テーブルには、宛先 MAC アドレスおよび関連付けされた VLAN ID、モジュール、アドレスに関連付けされたポート番号の一覧が表示されます。



(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、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.7-20)
- 「[MAC アドレスおよび VLAN](#)」 (P.7-20)
- 「[MAC アドレス テーブルのデフォルト設定](#)」 (P.7-20)
- 「[アドレス エージング タイムの変更](#)」 (P.7-21)
- 「[ダイナミック アドレス エントリの削除](#)」 (P.7-21)

- 「MAC アドレス通知トラップの設定」 (P.7-21)
- 「スタティック アドレス エントリの追加および削除」 (P.7-23)
- 「ユニキャスト MAC アドレス フィルタリングの設定」 (P.7-24)
- 「アドレス テーブル エントリの表示」 (P.7-26)

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、あるい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、スイッチは動的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は期限切れにします。

有効期間はスイッチごとに設定されます。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 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、マルチキャストアドレスは、VLAN 1 のポート 1 と、VLAN 5 のポート 9、10、11 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。ある VLAN でスタティックとして入力するアドレスは、他のすべての VLAN でもスタティック アドレスとして設定するか、他の VLAN から学習されない状態にしておく必要があります。

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	自動学習
スタティック アドレス	未設定

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。エージング タイム パラメータは、スイッチが未知のアドレスを保持する期間を定義します。このパラメータはすべての VLAN に適用されます。

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ドさせます。この不必要なフラッドによって、パフォーマンスに悪影響を及ぼすおそれがあります。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。

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]</code>	ダイナミック エントリが使用または更新された後、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 を入力して期限切れ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。
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 アドレス通知トラップの設定

MAC アドレス通知は、スイッチに MAC アドレス 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 通知を生成して NMS 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、動的でセキュアな 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	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 <i>host-addr</i> { traps informs } { version { 1 2c 3 } } <i>community-string notification-type</i>	トラップ メッセージの受信側を指定します。 <ul style="list-style-type: none"> • <i>host-addr</i> 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。 • <i>community-string</i> 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。 • <i>notification-type</i> 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。 <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。デフォルトは 1 です。
ステップ 6	interface <i>interface-id</i>	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 {added removed}</code>	MAC アドレス通知トラップをイネーブルにします。 <ul style="list-style-type: none"> このインターフェイスに MAC アドレスが追加 (added) された場合、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から MAC アドレスが削除 (removed) された場合、MAC アドレス通知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 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。

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、MAC アドレス通知機能をイネーブルにし、インターバルを 60 秒、履歴サイズを 100 エントリに設定し、特定のポートで MAC アドレスが追加された場合の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
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 fastethernet0/4
Switch(config-if)# snmp trap mac-notification added
```

これまで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。
- ユニキャストまたはマルチキャスト 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、ポートは必ず少なくとも 1 つの VLAN と対応しているため、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。送信元ポートごとに、宛先ポートのリストを別々に指定できます。

ある VLAN のスタティック アドレスは、他の VLAN でもスタティック アドレスである必要があります。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 アドレス（ユニキャストまたはマルチキャスト）と、その宛先の 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。

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"> <i>mac-addr</i> には、アドレス テーブルに追加する宛先 MAC アドレス（ユニキャストまたはマルチキャスト）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。 <i>vlan-id</i> 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。 <i>interface-id</i> 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。有効なインターフェイスは、物理ポートおよびポートチャンネルです。<i>interface-id</i> 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。有効なインターフェイスには、物理ポートまたはポートチャンネルがあります。スタティック マルチキャストアドレスの場合、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、インターフェイスは同時に 1 つしか入力できません。ただし、同じ MAC アドレスおよび VLAN ID を指定すると、コマンドを複数回入力できます。
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 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
gigabitethernet0/1
```

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。この機能をイネーブルに設定できるのは、スイッチで EI を実行している場合だけです。

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ていません。**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ていません。
- 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と、最後に入力し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、MAC アドレスを持つパケットをドロップします。2 番めに入力したコマンドは、1 番目のコマンドより優先されます。

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 コマンドに続けて、**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 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 コマンドに続けて、**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。

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	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、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"> 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ドロップされます。 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、送信元または宛先アドレスが c2f3.220a.12f4 であるパケットをスイッチがドロップ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アドレスとしたパケットを VLAN 4 で受信すると、パケットはドロップされます。

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

アドレス テーブル エントリの表示

表 7-4 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 7-4 MAC アドレス テーブル表示用のコマンド

コマンド	説明
<code>show mac address-table address</code>	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。
<code>show mac address-table aging-time</code>	すべての VLAN または指定された VLAN のエイジング タイムを表示します。
<code>show mac address-table count</code>	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。
<code>show mac address-table dynamic</code>	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。
<code>show mac address-table interface</code>	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。
<code>show mac address-table multicast</code>	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。
<code>show mac address-table static</code>	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。
<code>show mac address-table vlan</code>	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（イーサネット上のデバイスなど）と通信するには、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、ソフトウェアが特定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 アドレスを特定するプロセスは、**アドレス解決**と呼ばれています。

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、該当するメディアまたは MAC アドレスおよび VLAN ID に対応付けます。IP アドレスを入力として、関連付けされた MAC アドレスが ARP によって特定されます。MAC アドレスが特定されると、IP と MAC アドレスとの対応を ARP キャッシュに格納し、すばやく検索できるようにします。その後、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。

CLI の手順については、Cisco.com にある Cisco IOS Release のマニュアルを参照してください。