



スイッチの管理

この章では、Catalyst 3750 スイッチを管理するために行う初回のみの手順について説明しています。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

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.7-2)
- システム名およびプロンプトの設定 (p.7-16)
- バナーの作成 (p.7-19)
- MAC アドレス テーブルの管理 (p.7-21)
- ARP テーブルの管理 (p.7-28)

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、『Cisco IOS Configuration Fundamentals Command Reference』Release 12.2 を参照してください。

ここでは、次の設定について説明します。

- システムクロックの概要 (p.7-2)
- NTP の概要 (p.7-3)
- NTP の設定 (p.7-5)
- 手動での日時の設定 (p.7-12)

システムクロックの概要

時刻サービスの中心となるのがシステムクロックです。このクロックはシステム開始時から稼働し、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なります。

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、「手動での日時の設定」(p.7-12) を参照してください。

NTP の概要

NTP は、ネットワーク上にあるデバイス間の時刻の同期をとるため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 ソースとデバイスが離れている 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 が稼働するデバイスは、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。

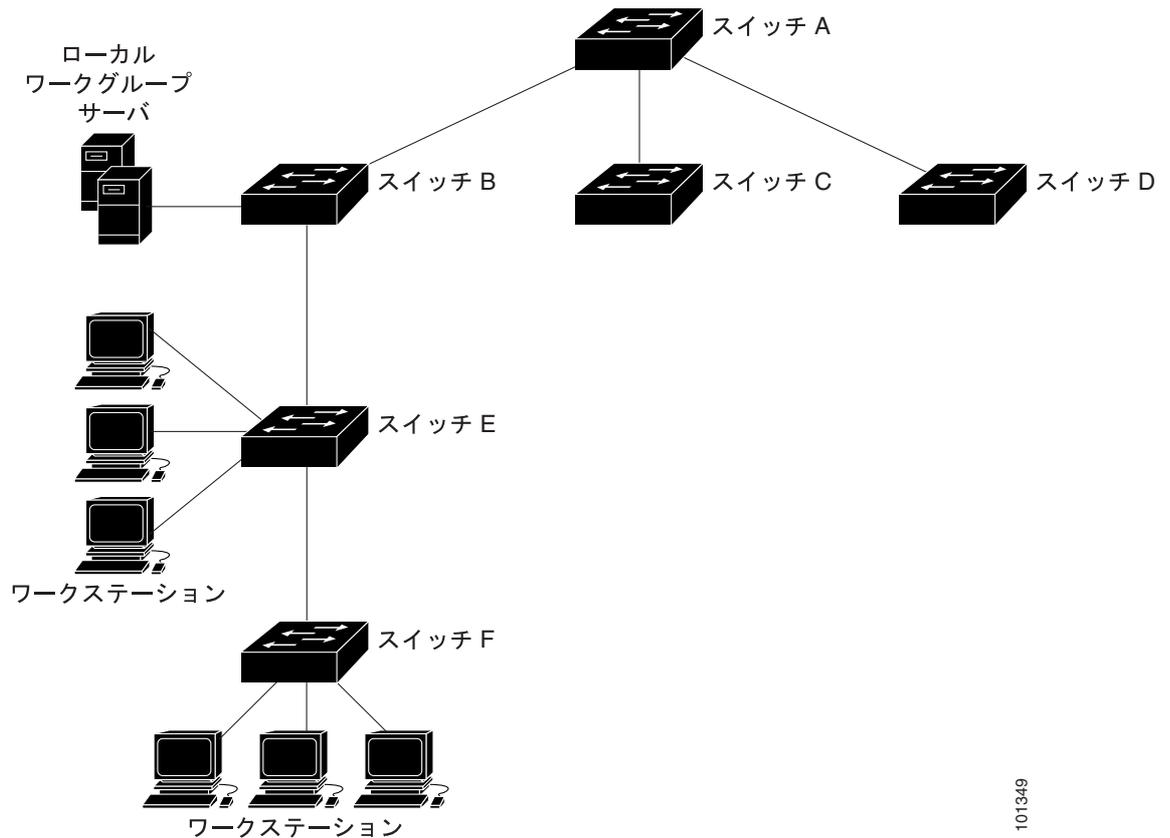
NTP が稼働するデバイス間の通信 (アソシエーション) は、通常スタティックに設定されます。各デバイスには、アソシエーションを作成すべき全デバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャストメッセージを使用するように NTP を設定できます。ブロードキャストメッセージを送受信するように各デバイスを設定すればよいだけなので、この代替手段によって設定作業が容易になります。ただし、この場合は、情報の流れは一方向に限られます。

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ことを防いでください。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 の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 インターネット上で使用可能なパブリック NTP サーバから取得することを推奨します。

図 7-1 に、NTP を使用する一般的なネットワーク例を示します。スイッチ A は NTP マスターで、スイッチ B、C、D は NTP サーバモードに設定されていて、スイッチ A とのサーバアソシエーションにあります。スイッチ E は、スイッチ B およびスイッチ F というアップストリームおよびダウンストリームスイッチの 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 によって、実際には、他の方法で時刻が取得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を設定できます。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、NTP は常に信頼性がより高いものとみなされます。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でサポートされるクロックを備えていないため、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に使用する NTP マスター クロックとして機能できません。このスイッチは、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 コマンドが利用できません。

ここでは、次の設定について説明します。

- [NTP のデフォルト設定 \(p.7-5\)](#)
- [NTP 認証の設定 \(p.7-6\)](#)
- [NTP アソシエーションの設定 \(p.7-7\)](#)
- [NTP ブロードキャスト サービスの設定 \(p.7-8\)](#)
- [NTP アクセス制限の設定 \(p.7-9\)](#)
- [NTP パケット用の送信元 IP アドレスの設定 \(p.7-11\)](#)
- [NTP 設定の表示 \(p.7-12\)](#)

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

この手順を行うには、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、イネーブル 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	<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。</p> <ul style="list-style-type: none"> <code>number</code> には、鍵の番号を指定します。指定できる範囲は 1 ~ 4294967295 です。 <code>md5</code> は、Message Digest Algorithm 5 (MD5) 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。 <code>value</code> には、鍵に対する 8 文字までの任意のストリングを入力します。 <p>スイッチとデバイスの双方がいずれかの認証鍵を持ち、<code>ntp trusted-key key-number</code> コマンドによって鍵番号が指定されていないかぎり、スイッチはデバイスと同期化しません。</p>
ステップ 4	<code>ntp trusted-key key-number</code>	<p>1 つまたは複数の鍵番号（ステップ 3 で定義したもの）を指定します。ピア NTP デバイスは、このスイッチと同期化するため、スイッチの NTP パケット内にこの鍵番号を設定しなければなりません。</p> <p>デフォルト設定では、信頼される鍵は定義されていません。</p> <p><code>key-number</code> には、ステップ 3 で定義された鍵を指定します。</p> <p>このコマンドは、スイッチが、信頼されていないデバイスと誤って同期化するのを防ぎます。</p>
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

NTP 認証をディセーブルにするには、`no ntp authenticate` グローバル コンフィギュレーション コマンドを使用します。認証鍵を削除するには、`no ntp authentication-key number` グローバル コンフィギュレーション コマンドを使用します。デバイス ID の認証をディセーブルにするには、`no ntp trusted-key key-number` グローバル コンフィギュレーション コマンドを使用します。

NTP パケットに認証鍵 42 を設定しているデバイスとだけ同期するようにスイッチを設定する例を以下に示します。

```
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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ntp peer ip-address [version number] [key keyid] [source interface] [prefer]</code> または <code>ntp server ip-address [version number] [key keyid] [source interface] [prefer]</code>	スイッチのシステム クロックをピアに同期化させるか、ピアを同期化させる（ピア アソシエーション）かを設定します。 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 <code>ip-address</code> 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）<code>number</code> 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）<code>keyid</code> には、<code>ntp authentication-key</code> グローバル コンフィギュレーション コマンドで定義された認証鍵を入力します。 （任意）<code>interface</code> 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）<code>prefer</code> 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換えを減らします。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	（任意）コンフィギュレーション ファイルに設定を保存します。

アソシエーションは、一端のデバイスのみを設定します。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 を使用します。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。

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方法を、以下の例に示します。

```
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し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ピ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。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だけなので、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、イネーブル 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	<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に設定されています。 <ul style="list-style-type: none"> （任意）<i>number</i> には、NTP のバージョン番号を指定します。指定できる範囲は 1～3 です。バージョンを指定しなかった場合は、バージョン 3 が使用されます。 （任意）<i>keyid</i> には、ピアにパケットを送信するときに使用する認証鍵を指定します。 （任意）<i>destination-address</i> には、スイッチにクロックを同期化しているピアの IP アドレスを指定します。
ステップ 4	<code>end</code>	イネーブル 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、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 gigabitethernet1/0/1
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、イネーブル 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	<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>	イネーブル 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、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 gigabitethernet1/0/1
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、次の 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 \(p.7-10\)](#)
- [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 \(p.7-11\)](#)

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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ntp access-group {query-only serve-only serve peer} access-list-number</code>	<p>アクセスグループを作成し、基本 IP アクセスリストを割り当てます。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • query-only — NTP 制御クエリーに限り許可します。 • 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><code>access-list-number</code> には、1 ~ 99 の範囲で標準の IP アクセスリスト番号を入力します。</p>
ステップ 3	<code>access-list access-list-number permit source [source-wildcard]</code>	<p>アクセスリストを作成します。</p> <ul style="list-style-type: none"> • <code>access-list-number</code> 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。 • <code>source</code> 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) <code>source-wildcard</code> 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拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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、イネーブル 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	イネーブル 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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ntp source type number</code>	IP 送信元アドレス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によって設定されます。
ステップ 3	<code>end</code>	イネーブル 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全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.7-7) 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 つのイネーブル 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。

手動での日時の設定

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。



(注) システム クロックを手動で設定し、スタック マスターに障害が生じて別のスタック メンバーがスタック マスターの役割を再開した場合は、この設定をリセットする必要があります。

ここでは、次の設定について説明します。

- [システム クロックの設定](#) (p.7-13)
- [日時設定の表示](#) (p.7-13)
- [タイム ゾーンの設定](#) (p.7-13)
- [夏時間の設定](#) (p.7-14)

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、イネーブル 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 <i>hh:mm:ss day month year</i> または clock set <i>hh:mm:ss month day year</i>	次のいずれかのフォーマットで、手動でシステムクロックを設定します。 <ul style="list-style-type: none"> • <i>hh:mm:ss</i> 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。 • <i>day</i> には、当月の日付で日を指定します。 • <i>month</i> には、月を名前で指定します。 • <i>year</i> には、年を指定します (短縮不可)。

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]** イネーブル 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 (確実である) かどうかを示す *authoritative* フラグを維持します。システムクロックがタイミングソース (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、*authoritative* フラグが設定された状態でない場合、ピアの時刻が無効なときは、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、イネーブル 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 <i>zone hours-offset</i> [<i>minutes-offset</i>]	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"> • <i>zone</i> 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。 • <i>hours-offset</i> には、UTC からの時差 (時間単位) を入力します。 • (任意) <i>minutes-offset</i> には、UTC からの時差 (分単位) を入力します。

	コマンド	説明
ステップ 3	<code>end</code>	イネーブル 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 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 [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および終了する地域で夏時間を設定するには、イネーブル 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	<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 [week day month hh:mm week day month hh:mm [offset]]</code>	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。 <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、月の何番めの週かを指定します (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 時間制) と分で指定します。 (任意) <i>offset</i> には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。
ステップ 3	<code>end</code>	イネーブル 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 日曜の午前 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場合（次の夏時間のイベントの正確な日時を設定する）は、イネーブル 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	<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、月の何番目の週かを指定します（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 時間制）と分で指定します。 • (任意) <i>offset</i> には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。
ステップ 3	<code>end</code>	イネーブル 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 2000 年 10 月 12 日の 2 時に始まり、2001 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 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識別します。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。大なり記号 [**>**] が付加されます。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。

スタック マスターを経由してスタック メンバーにアクセスしている場合は、**session stack-member-number** イネーブル EXEC コマンドを使用する必要があります。スタック メンバー番号は 1～9 です。このコマンドを使用すると、スタック メンバー番号がシステム プロンプトに付加されます。たとえば、*switch-2#* はスタック メンバー 2 のイネーブル EXEC モードのプロンプトです。*switch* は、スイッチ スタックのシステム プロンプトです。

ここで説明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、『*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.7-16)
- システム名の設定 (p.7-16)
- DNS の概要 (p.7-17)

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、イネーブル 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、 <i>switch</i> です。 名前は ARPANET ホスト名の規則に従う必要があります。この規則ではホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、またはハイフンしか使用できません。名前には 63 文字まで使用できます。
ステップ 3	end	イネーブル 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、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、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。スイッチ上で 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、IP で *com* というドメイン名に分類される商業組織なので、ドメイン名は *cisco.com* 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) に保管します。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、次の設定について説明します。

- [DNS のデフォルト設定 \(p.7-17\)](#)
- [DNS の設定 \(p.7-17\)](#)
- [DNS 設定の表示 \(p.7-18\)](#)

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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip domain-name name</code>	未修飾のホスト名 (ドット付き 10 進表記ドメイン名のない名前) を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 起動時にはドメイン名は設定されていませんが、BOOTP または Dynamic Host Configuration Protocol (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 <i>server-address1</i> [<i>server-address2 ... server-address6</i>]	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動的に割り当てることができます。
ステップ 5	end	イネーブル 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 (.) がある場合は、Cisco IOS ソフトウェアは、ホスト名にデフォルトのドメイン名を追加せずに IP アドレスを検索します。

ドメイン名を削除するには、**no ip domain-name name** グローバル コンフィギュレーション コマンドを使用します。ネーム サーバのアドレスを削除するには、**no ip name-server server-address** グローバル コンフィギュレーション コマンドを使用します。スイッチ上の DNS をディセーブルにするには、**no ip domain-lookup** グローバル コンフィギュレーション コマンドを使用します。

DNS 設定の表示

DNS 設定情報を表示するには、**show running-config** イネーブル 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。ログインバナーは MoTD バナーのあとに表示され、その次にログインプロンプトが表示されます。



(注)

ここで説明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、『Cisco IOS Configuration Fundamentals Command Reference』Release 12.2 を参照してください。

ここでは、次の設定について説明します。

- バナーのデフォルト設定 (p.7-19)
- MoTD ログイン バナーの設定 (p.7-19)
- ログインバナーの設定 (p.7-20)

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

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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>banner motd c message c</code>	MoTD 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。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。 <i>message</i> には、255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

MoTD バナーを削除するには、`no banner motd` グローバル コンフィギュレーション コマンドを使用します。

次に、ポンド記号 (#) を開始および終了の区切り文字として使用し、スイッチの MoTD バナーを設定する例を示します。

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

次に、前の設定により表示されたバナーを示します。

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

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

User Access Verification

Password:
```

ログインバナーの設定

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。バナーは、MoTD バナーのあとに表示され、その次にログインプロンプトが表示されます。

ログインバナーを設定するには、イネーブル 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。 <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。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。 <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	イネーブル 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 (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、次の設定について説明します。

- [アドレス テーブルの作成 \(p.7-21\)](#)
- [MAC アドレスおよび VLAN \(p.7-22\)](#)
- [MAC アドレスおよびスイッチ スタック \(p.7-22\)](#)
- [MAC アドレス テーブルのデフォルト設定 \(p.7-22\)](#)
- [アドレス エージング タイムの変更 \(p.7-22\)](#)
- [ダイナミック アドレス エントリの削除 \(p.7-23\)](#)
- [MAC アドレス通知トラップの設定 \(p.7-23\)](#)
- [スタティック アドレス エントリの追加および削除 \(p.7-25\)](#)
- [ユニキャスト MAC アドレス フィルタリングの設定 \(p.7-26\)](#)
- [アドレス テーブル エントリの表示 \(p.7-28\)](#)

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、スタンドアロン スイッチまたはスイッチ スタックに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 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。パケットを送信したポート上に宛先アドレスがある場合は、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管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 と VLAN 5 内のポート 9、10 へ伝送できます。

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、対応付けられたすべての VLAN に同じスタティック MAC アドレスを設定します。

プライベート VLAN の詳細については、[第 16 章「プライベート VLAN の設定」](#)を参照してください。

MAC アドレスおよびスイッチ スタック

すべてのスタック メンバーの MAC アドレス テーブルは、同期されています。常に、各スタック メンバーは、各 VLAN に対応するアドレス テーブルの同一のコピーを持っています。アドレスが期限切れになると、そのアドレスはすべてのスタック メンバーのアドレス テーブルから削除されます。スイッチがスイッチ スタックに参加すると、そのスイッチは他のスタック メンバーが学習した各 VLAN に対応するアドレスを受け取ります。スタック メンバーがスイッチ スタックから削除されると、残りのスタック メンバーは、以前のスタック メンバーが学習したアドレスをすべて期限切れにするか削除します。

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	設定なし

アドレス エージング タイムの変更

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

エージング タイムの設定が短かすぎると、アドレスが活用されないままテーブルから削除される可能性があります。その場合、スイッチは宛先が不明の packets を受信すると、受信ポートと同じ VLAN 内のすべてのポートに、その packets をフラッディングさせます。この不必要なフラッディングによって、パフォーマンスに悪影響が出る可能性があります。また、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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mac address-table aging-time [0 10-1000000] [vlan vlan-id]</code>	ダイナミック エントリが使用または更新されたあと、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、期限切れがディセーブルになります。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。 <i>vlan-id</i> の有効な ID は、1 ~ 4094 です。
ステップ 3	<code>end</code>	イネーブル 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、イネーブル 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` イネーブル 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 (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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信デバイスを指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 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。 <code>community-string</code> 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てから snmp-server host コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ 3	<code>snmp-server enable traps mac-notification</code>	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	<code>mac address-table notification</code>	MAC アドレス通知機能をイネーブルにします。
ステップ 5	<code>mac address-table notification [interval value] [history-size value]</code>	<p>トラップ インターバル タイムと履歴テーブルのサイズを入力します。</p> <ul style="list-style-type: none"> (任意) interval value には、NMS に対して生成される各トラップ セット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は 0 ~ 2147483647 秒です。デフォルトは 1 秒です。 (任意) history-size value には、MAC 通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は 0 ~ 500 で、デフォルトは 1 です。
ステップ 6	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。
ステップ 7	<code>snmp trap mac-notification {added removed}</code>	<p>MAC アドレス通知トラップをイネーブルにします。</p> <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)されたときは常に、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)されたときは常に、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>	イネーブル 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、指定したポートで MAC アドレスが追加されたときはいつでも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 gigabitethernet1/0/2
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** イネーブル 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ので、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。送信元ポートごとに、異なる宛先ポートを指定できます。

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 すべてに設定します。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16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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mac address-table static mac-addr vlan vlan-id interface interface-id</code>	MAC アドレス テーブルにスタティック アドレスを追加します。 <ul style="list-style-type: none"> <code>mac-addr</code> には、アドレス テーブルに追加する宛先 MAC ユニキャスト アドレスを指定します。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。 <code>vlan-id</code> には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。有効な VLAN ID は、1 ~ 4094 です。 <code>interface-id</code> 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、物理ポートまたはポート チャネルなどです。スタティック マルチキャスト アドレスには、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 アドレスには、一度に1つのインターフェイスのみを入力できます。ただし、MAC アドレスおよび VLAN ID が同じ場合、コマンドを複数回、入力できます。
ステップ 3	<code>end</code>	イネーブル 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ポートに転送されます。

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

ユニキャスト MAC アドレス フィルタリングの設定

ユニキャスト MAC アドレス フィルタリングがイネーブルの場合、スイッチは特定の送信元または宛先 MAC アドレスを持つパケットを廃棄します。デフォルトでは、この機能はディセーブルで、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には、次の手順を実行してください。

- 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、前述のアドレスのいずれかを指定すると、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 コマンドを入力して、続いて **mac address-table static mac-addr vlan vlan-id drop** コマンドを入力する場合、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。

また、**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 コマンドを入力して、続いて **mac address-table static mac-addr vlan vlan-id interface interface-id** コマンドを入力する場合には、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、イネーブル 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。 <ul style="list-style-type: none"> • <i>mac-addr</i> 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。 • <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。
ステップ 3	end	イネーブル 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つ 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
```

アドレス テーブル エントリの表示

表 7-4 に示す 1 つまたは複数のイネーブル 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
show ip igmp snooping groups	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 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 notification	MAC 通知パラメータとヒストリ 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（たとえば、イーサネットを介して）、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を、「アドレス解決」といいます。

Address Resolution Protocol (ARP) は、ホスト IP アドレスを、対応する MAC アドレスと VLAN ID に関連付けます。ARP は、IP アドレスを使用してそれに関連付けられた MAC アドレスを検索します。MAC アドレスが見つかり、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層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。

CLI の手順については、Cisco.com で Cisco IOS Release 12.2 のマニュアルを参照してください。