



## スイッチの管理

---

この章では、Catalyst 3550 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 \( p.7-2 \)](#)
- [システム名およびプロンプトの設定 \( p.7-15 \)](#)
- [バナーの作成 \( p.7-19 \)](#)
- [MAC アドレス テーブルの管理 \( p.7-21 \)](#)
- [ユーザが選択した機能に対するシステム リソースの最適化 \( p.7-29 \)](#)

## 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 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。

- [システムクロックの概要 \(p.7-2\)](#)
- [NTP の概要 \(p.7-2\)](#)
- [NTP の設定 \(p.7-4\)](#)
- [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 Greenwich Mean Time [GMT; グリニッジ標準時])に基づいてシステム内部の時刻を常時監視します。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 User Datagram Protocol (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することができます。

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止します。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、時刻がほか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。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、情報の流れは単方向に限られます。

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 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。

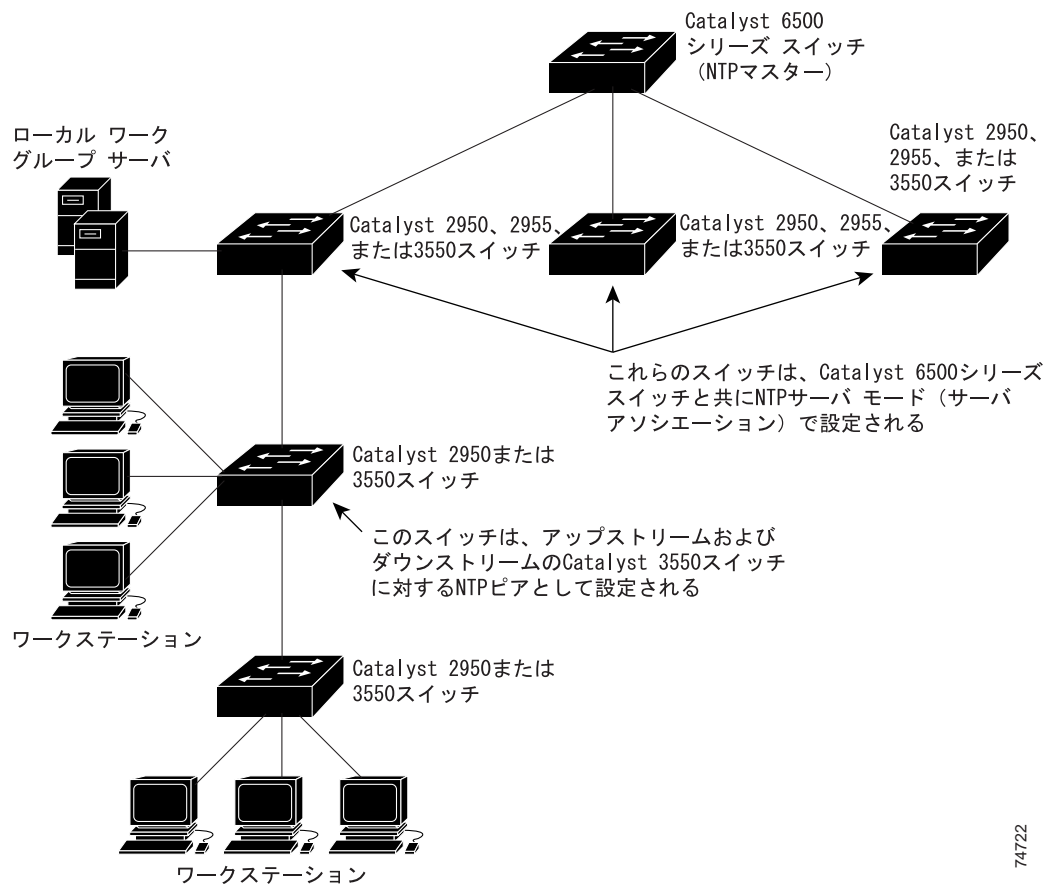
シスコの NTP ではストラタム 1 サービスをサポートしていないので、ラジオ クロックまたは原子時計に接続できません。ネットワークの時刻サービスは、IP インターネット上のパブリック NTP サーバから取得することを推奨します。図 7-1 に、NTP を使用する一般的なネットワーク例を示します。

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、ほか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、常に NTP はより信頼できるとみなされます。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。

図 7-1 一般的な NTP ネットワーク構成



74722

## 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 \(p.7-5\)](#)
- [NTP アソシエーションの設定 \(p.7-6\)](#)
- [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 \(p.7-9\)](#)
- [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 \(p.7-11\)](#)

## 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	ディセーブルです。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	設定されていません。
NTP ブロードキャスト サービス	ディセーブルです。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ほか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	<i>configure terminal</i>	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	<i>ntp authenticate</i>	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	<i>ntp authentication-key number md5 value</i>	<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"> <li><b>number</b> には、鍵の番号を指定します。指定できる範囲は 1 ~ 4294967295 です。</li> <li><b>md5</b> 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。</li> <li><b>value</b> 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。</li> </ul> <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、<i>ntp trusted-key key-number</i> 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	<i>ntp trusted-key key-number</i>	<p>1 つまたは複数の鍵番号（ステップ 3 で定義したもの）を指定します。ピア NTP デバイスは、このスイッチと同期化するため、このスイッチへの NTP パケット内にこの鍵番号を設定しなければなりません。</p> <p>デフォルト設定では、信頼される鍵は定義されていません。</p> <p><b>key-number</b> 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止します。</p>
ステップ 5	<i>end</i>	イネーブル EXEC モードに戻ります。

	コマンド	説明
ステップ 6	<b><i>show running-config</i></b>	設定を確認します。
ステップ 7	<b><i>copy running-config startup-config</i></b>	(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	<b><i>configure terminal</i></b>	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	<b><i>ntp peer ip-address [version number] [key keyid] [source interface] [prefer]</i></b> または <b><i>ntp server ip-address [version number] [key keyid] [source interface] [prefer]</i></b>	<p>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ように設定します (ピア アソシエーション)。</p> <p>または</p> <p>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ように設定します (サーバ アソシエーション)。</p> <p>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。</p> <ul style="list-style-type: none"> <li>ピア アソシエーションの <b><i>ip-address</i></b> 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。</li> <li>(任意) <b><i>number</i></b> 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。</li> <li>(任意) <b><i>keyid</i></b> には、<b><i>ntp authentication-key</i></b> 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。</li> <li>(任意) <b><i>interface</i></b> 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。</li> <li>(任意) <b><i>prefer</i></b> 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。</li> </ul>

	コマンド	説明
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	設定を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(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 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 アソシエーションまたはサーバ アソシエーションを削除するには、**no ntp peer ip-address** または **no ntp server ip-address** グローバル コンフィギュレーション コマンドを使用します。

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。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、情報の流れは単方向に限られます。

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	<b>configure terminal</b>	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	<b>interface interface-id</b>	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。

	コマンド	説明
ステップ 3	<b><i>ntp broadcast [version number] [key keyid] [destination-address]</i></b>	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"> <li>（任意）<b><i>number</i></b>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。</li> <li>（任意）<b><i>keyid</i></b>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。</li> <li>（任意）<b><i>destination-address</i></b>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。</li> </ul>
ステップ 4	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b><i>show running-config</i></b>	設定を確認します。
ステップ 6	<b><i>copy running-config startup-config</i></b>	（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、インターフェイスが 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、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	<b><i>configure terminal</i></b>	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	<b><i>interface interface-id</i></b>	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	<b><i>ntp broadcast client</i></b>	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	<b><i>exit</i></b>	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	<b><i>ntp broadcastdelay microseconds</i></b>	（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 マイクロ秒です。
ステップ 6	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 7	<b><i>show running-config</i></b>	設定を確認します。
ステップ 8	<b><i>copy running-config startup-config</i></b>	（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、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 \(p.7-9\)](#)
- [特定のインターフェイスでの NTP サービスのディセーブル化 \(p.7-10\)](#)

### アクセスグループの作成と基本 IP アクセスリストの割り当て

アクセスリストを使用して NTP サービスへのアクセスを制御するには、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	<b>configure terminal</b>	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	<b>ntp access-group {query-only   serve-only   serve   peer} access-list-number</b>	<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"> <li>• <b>query-only</b> NTP 制御クエリに限り許可します。</li> <li>• <b>serve-only</b> 時刻要求に限り許可します。</li> <li>• <b>serve</b> 時刻要求と NTP 制御クエリは許可しますが、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。</li> <li>• <b>peer</b> 時刻要求と NTP 制御クエリを許可し、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。</li> </ul> <p><b>access-list-number</b> 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	<b>access-list access-list-number permit source [source-wildcard]</b>	<p>アクセスリストを作成します。</p> <ul style="list-style-type: none"> <li>• <b>access-list-number</b> を指定する場合は、ステップ 2 で指定した番号を入力します。</li> <li>• <b>permit</b> 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。</li> <li>• <b>source</b> 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。</li> <li>• (任意) <b>source-wildcard</b> 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。</li> </ul> <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>

	コマンド	説明
ステップ 4	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(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 制御クエリに限り許可します。

送信元 IP アドレスが複数のアクセス タイプのアクセス リストに一致する場合は、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	<b>configure terminal</b>	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	<b>interface interface-id</b>	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	<b>ntp disable</b>	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	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(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	<b><i>configure terminal</i></b>	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	<b><i>ntp source type number</i></b>	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	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b><i>show running-config</i></b>	設定を確認します。
ステップ 5	<b><i>copy running-config startup-config</i></b>	(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.7-6)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 for Cisco IOS Release 12.1](#)』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。

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 \(p.7-12\)](#)
- [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、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	<b><i>clock set hh:mm:ss day month year</i></b> または <b><i>clock set hh:mm:ss month day year</i></b>	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"> <li>• <b><i>hh:mm:ss</i></b> 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。</li> <li>• <b><i>day</i></b> には、当月の日付で日を指定します。</li> <li>• <b><i>month</i></b> には、月を名前で指定します。</li> <li>• <b><i>year</i></b> には、年を指定します (短縮不可)。</li> </ul>
ステップ 2	<b><i>show running-config</i></b>	設定を確認します。
ステップ 3	<b><i>copy running-config startup-config</i></b>	(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]*** 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 (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 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	<b><i>configure terminal</i></b>	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	<b><i>clock timezone zone hours-offset</i></b> <b>[<i>minutes-offset</i>]</b>	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"> <li>• <b><i>zone</i></b> 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。</li> <li>• <b><i>hours-offset</i></b> には、UTC からの時差（時間単位）を入力します。</li> <li>• （任意）<b><i>minutes-offset</i></b> には、UTC からの時差（分単位）を入力します。</li> </ul>
ステップ 3	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b><i>show running-config</i></b>	設定を確認します。
ステップ 5	<b><i>copy running-config startup-config</i></b>	（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地域のタイムゾーン（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 パーセントを意味します。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	<b><i>configure terminal</i></b>	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	<b><i>clock summer-time zone recurring</i></b> [ <b><i>week</i></b> <b><i>day month hh:mm week day month hh:mm</i></b> <b>[<i>offset</i>]</b> ]	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 <b><i>clock summer-time zone recurring</i></b> 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"> <li>• <b><i>zone</i></b> 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。</li> <li>• （任意）<b><i>week</i></b> には、月の何番目の週かを指定します（1 ~ 5、または <b><i>last</i></b>）。</li> <li>• （任意）<b><i>day</i></b> には、曜日を指定します（Sunday、Monday など）。</li> <li>• （任意）<b><i>month</i></b> には、月を指定します（January、February など）。</li> <li>• （任意）<b><i>hh:mm</i></b> には、時刻を時間（24 時間制）と分で指定します。</li> <li>• （任意）<b><i>offset</i></b> 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 分です。</li> </ul>

	コマンド	説明
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	設定を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(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	<b>configure terminal</b>	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	<b>clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]]</b> または <b>clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]</b>	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"> <li><b>zone</b> 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。</li> <li>(任意) <b>week</b> には、月の何番目の週かを指定します (1 ~ 5、または <b>last</b>)。</li> <li>(任意) <b>day</b> には、曜日を指定します ( Sunday, Monday など )。</li> <li>(任意) <b>month</b> には、月を指定します ( January, February など )。</li> <li>(任意) <b>hh:mm</b> には、時刻を時間 ( 24 時間制 ) と分で指定します。</li> <li>(任意) <b>offset</b> 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 分です。</li> </ul>
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	設定を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(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と、**prompt** 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手動でプロンプトを設定している場合以外、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 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 \(p.7-15\)](#)
- [システム プロンプトの設定 \(p.7-16\)](#)
- [DNS の概要 \(p.7-16\)](#)

### 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	<b>configure terminal</b>	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	<b>hostname name</b>	手動でシステム名を設定します。  デフォルト設定は、 <b>switch</b> 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	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	設定を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(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。**prompt** グローバル コンフィギュレーション コマンドを使用すると、プロンプトの設定を上書きできます。

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。

## システム プロンプトの設定

手動でシステム プロンプトを設定するには、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	<b><i>configure terminal</i></b>	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	<b><i>prompt string</i></b>	<p>コマンドライン プロンプトを設定して、<b><i>hostname</i></b> コマンドでの設定を上書きします。</p> <p>デフォルトのプロンプトは、<b><i>switch</i></b>または <b><i>hostname</i></b> 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名前です。そのあとにユーザ EXEC モードの場合はかぎカッコ (&gt;)、イネーブル EXEC モードの場合はポンド記号 (#) が続きます。</p> <p>プロンプトは、すべての印刷文字およびエスケープシーケンスで構成できます。</p>
ステップ 3	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b><i>show running-config</i></b>	設定を確認します。
ステップ 5	<b><i>copy running-config startup-config</i></b>	(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。

デフォルトのプロンプトに戻すには、***no prompt [string]*** 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 アドレスに対応づけることができます。スイッチに 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することができます。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 File Transfer Protocol (FTP) 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、次の設定情報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	イネーブルです。
DNS デフォルト ドメイン名	設定されていません。
DNS サーバ	ネーム サーバ アドレスは設定されていません。

## 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	<b><i>configure terminal</i></b>	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	<b><i>ip domain-name name</i></b>	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; 動的ホスト制御プロトコル) サーバからスイッチ コンフィギュレーションを取得している場合は、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります (サーバにこの情報が設定されている場合)。
ステップ 3	<b><i>ip name-server server-address1 [server-address2 ... server-address6]</i></b>	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 クエリを送信します。そのクエリが失敗した場合は、バックアップサーバがクエリされます。
ステップ 4	<b><i>ip domain-lookup</i></b>	(任意) スイッチで、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	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 6	<b><i>show running-config</i></b>	設定を確認します。
ステップ 7	<b><i>copy running-config startup-config</i></b>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

MoTD (Message-of-The-Day) 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 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。

- [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

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、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	<b><i>configure terminal</i></b>	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	<b><i>banner motd c message c</i></b>	MoTD 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、 <b>Return</b> 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	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b><i>show running-config</i></b>	設定を確認します。
ステップ 5	<b><i>copy running-config startup-config</i></b>	(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、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	<b><i>configure terminal</i></b>	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	<b><i>banner login c message c</i></b>	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、 <b>Return</b> 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。  <b>message</b> 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	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b><i>show running-config</i></b>	設定を確認します。
ステップ 5	<b><i>copy running-config startup-config</i></b>	(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。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またはマルチキャスト 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 ID、およびアドレスに対応づ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 \(p.7-21\)](#)
- [MAC アドレスおよび VLAN \(p.7-22\)](#)
- [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 \(p.7-27\)](#)

### アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスによって、スイッチの任意のポートを各ワークステーション、リピータ、スイッチ、ルータ、またはその他のネットワーク デバイスに接続できます。各ポートで受信するパケットの送信元アドレスを学習し、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。

有効期間はスイッチごとに設定します。ただし、スイッチは VLAN ごとにアドレス テーブルをメンテナンスし、STP によって VLAN ごとの有効期間を短縮することができます。

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づ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、完全なパケットを一度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 と対応づけられます。1 つのアドレスを複数の VLAN に対応づけ、それぞれで異なる宛先を設定できます。たとえば、VLAN 1 のポート 1、および VLAN 5 のポート 9、10、11 を宛先とするマルチキャスト アドレスを設定できます。

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づ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 アドレスで設定するか、他の VLAN で認識されない状態のままではなりません。

## 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、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。  <code>vlan-id</code> に指定できる有効な 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。

	コマンド	説明
ステップ 4	<b><i>show mac address-table aging-time</i></b>	設定を確認します。
ステップ 5	<b><i>copy running-config startup-config</i></b>	(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 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、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	<i>configure terminal</i>	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	<i>snmp-server host host-addr { traps   informs } { version { 1   2c   3 } } community-string notification-type</i>	<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"> <li>• <i>hos-addr</i> には、NMS の名前または IP アドレスを指定します。</li> <li>• SNMP トラップをホストに送信するには、<i>traps</i> (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、<i>informs</i> を指定します。</li> <li>• 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。</li> <li>• <i>community-string</i> 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、<i>snmp-server host</i> コマンドで設定できますが、<i>snmp-server community</i> コマンドでこのストリングを定義してから <i>snmp-server host</i> コマンドを使用することを推奨します。</li> <li>• <i>notification-type</i> には、<i>mac-notification</i> キーワードを使用します。</li> </ul>
ステップ 3	<i>snmp-server enable traps mac-notification</i>	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	<i>mac address-table notification</i>	MAC アドレス通知機能をイネーブルにします。
ステップ 5	<i>mac address-table notification [interval value]   [history-size value]</i>	<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"> <li>• (任意) <i>interval value</i> 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。</li> <li>• (任意) <i>history-size value</i> 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。</li> </ul>
ステップ 6	<i>interface 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レイヤ 2 インターフェイスを指定します。
ステップ 7	<i>snmp trap mac-notification { added   removed }</i>	<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"> <li>• このインターフェイスに MAC アドレスが追加 (<i>added</i>) されたときはいつでも、MAC アドレス通知トラップをイネーブルにします。</li> <li>• このインターフェイスから MAC アドレスが削除 (<i>removed</i>) されたときはいつでも、MAC アドレス通知トラップをイネーブルにします。</li> </ul>
ステップ 8	<i>end</i>	イネーブル EXEC モードに戻ります。
ステップ 9	<i>show mac address-table notification interface show running-config</i>	設定を確認します。
ステップ 10	<i>copy running-config startup-config</i>	(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、インターフェイス FastEthernet 0/4 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 fastethernet0/4
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** 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 アドレス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、転送動作を定義することができます。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 に関連づけられているので、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のリストを指定できます。

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 アドレスでなければなりません。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 アドレス (ユニキャストまたはマルチキャスト) およびその受信先となる 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。

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	<b><i>configure terminal</i></b>	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	<b><i>mac address-table static mac-addr vlan vlan-id interface interface-id</i></b>	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"> <li>• <b><i>mac-addr</i></b> 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。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。</li> <li>• <b><i>vlan-id</i></b> 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。</li> <li>• <b><i>interface-id...</i></b> 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。</li> </ul>
ステップ 3	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b><i>show mac address-table static</i></b>	設定を確認します。
ステップ 5	<b><i>copy running-config startup-config</i></b>	(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、およびルータ MAC アドレスは、サポートされません。***mac address-table static mac-addr vlan vlan-id drop*** グローバル コンフィギュレーション コマンドを入力するときに、このアドレスの 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、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したコマンドによって、MAC アドレスをスタティック アドレスとして追加するか、MAC アドレスが指定されたパケットを廃棄します。2 番めに入力したコマンドは、最初に入力したコマンドを無効にして、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。

たとえば、**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。

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、送信元または宛先ユニキャスト MAC アドレスと、パケットを受信する VLAN を指定することにより、特定のアドレスを持つパケットを廃棄するようスイッチを設定します。

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	<b>configure terminal</b>	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	<b>mac address-table static mac-addr vlan vlan-id drop</b>	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、指定された送信元または宛先ユニキャスト スタティック アドレスを持つパケットを廃棄するようスイッチを設定します。 <ul style="list-style-type: none"> <li>• <b>mac-addr</b> 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 アドレスのあるパケットは、廃棄されます。</li> <li>• <b>vlan-id</b> 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。</li> </ul>
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>show mac address-table static</b>	設定を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(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、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スイッチを設定する例を示します。送信元または宛先アドレスとして、この MAC アドレスを持つ VLAN 4 にパケットが受信された場合、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
<b>show mac address-table address</b>	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。
<b>show mac address-table aging-time</b>	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。

表 7-4 MAC アドレス テーブル表示用のコマンド (続き)

コマンド	説明
<i>show mac address-table count</i>	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。
<i>show mac address-table dynamic</i>	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。
<i>show mac address-table interface</i>	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。
<i>show mac address-table multicast</i>	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。
<i>show mac address-table static</i>	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。
<i>show mac address-table vlan</i>	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。

## ユーザが選択した機能に対するシステム リソースの最適化

ネットワークでのスイッチの使用状況に応じて、Switch Database Management (SDM) テンプレートを使用して、特定の機能に対するサポートを最適化するようにスイッチのメモリ リソースを設定できます。4つのテンプレートのいずれかを使用して、どのようにシステム リソースを割り当てるかを指定できます。これによって、このスイッチで設定できる、ユニキャスト MAC アドレス、Internet Group Management Protocol (IGMP) グループ、Quality of Service (QoS; サービス品質) Access Control Entry (ACE; アクセス制御エントリ)、セキュリティ ACE、ユニキャスト ルート、マルチキャスト ルート、サブネット VLAN (ルーテッド インターフェイス)、およびレイヤ 2 VLAN の最大数を概算できます。

4つのテンプレートは、システム メモリに優先順位をつけて、次の機能タイプのサポートを最適化します。

- QoS およびセキュリティ ACE    アクセス テンプレートは、通常、ネットワーク エッジにあり、ルート テーブルのサイズがあまり大きくないアクセス スイッチで使用されます。アクセス スイッチがネットワーク全体の入口になるので、フィルタリングと QoS がより重要となります。
- ルーティング    ルーティング テンプレートは、通常、ネットワークの中心にあるルータまたはアグリゲータが必要となります。ユニキャスト ルーティングに対して、システム リソースを最大化します。
- VLAN    VLAN テンプレートは、ルーティングをディセーブルにし、最大数のユニキャスト MAC アドレスをサポートします。通常、レイヤ 2 スイッチとして使用される Catalyst 3550 用を選択されます。
- デフォルト    デフォルト テンプレートは、すべての機能 (QoS、ACL、ユニキャスト ルーティング、マルチキャスト ルーティング、VLAN、および MAC アドレス) のバランスをとります。

144 ビットのレイヤ 3 TCAM をサポートできるようにスイッチを設定すると、ルーティング テーブル メモリの割り当てを再フォーマットすることにより、スイッチ内部のルーティング テーブルにフィールドを追加できます。**extended-match** キーワードをデフォルト、アクセス、またはルーティング テンプレートで使用すると、使用できるユニキャスト ルート数が減り、レイヤ 3 TCAM の下位 72 ビットに追加のルーティング情報が保存されます。割り当てられた TCAM が再フォーマットされます。スイッチの Customer Edge (CE; カスタマー エッジ) デバイスで Web Cache Communication Protocol (WCCP)、または multiple VPN Routing/Forwarding (multi-VRP) インスタンス (multi-VRP CE) を実行している場合は、144 ビットのレイヤ 3 TCAM が必要です。

表 7-5 に、Catalyst 3550 ギガビット イーサネット スイッチに対する 4つのテンプレートそれぞれでサポートされる各リソースの概数を示します。表 7-6 では、Catalyst 3550 スイッチの 4つのテンプレートをプライマリ ファスト イーサネット ポートと比較します。

表の最初の 6 行 (ユニキャスト MAC アドレスからマルチキャスト ルートまで) は、各テンプレートが選択されたときに設定されるハードウェアのおおよその限度を表します。ハードウェア リソースのある部分がいっぱいの場合、処理のオーバーフローはすべて CPU に送られ、スイッチのパフォーマンスに重大な影響が出ます。

最後の 2 行は、ルーテッド ポートと SVI の合計数、およびレイヤ 2 VLAN の数で、ほかのリソース パラメータに関連してハードウェア リソースの消費量を計算する際の指針となります。

サブネット VLAN (ルーテッド ポートおよび SVI) の数はソフトウェアによって制限されず、この表に示されているものより大きな数値に設定できます。サブネット VLAN の数をこの表の値以下に設定すると、テンプレートごとの各カテゴリ (ユニキャスト アドレス、IGMP グループなど) のエントリ数は表示されているものになります。サブネット VLAN の数が増えるにつれて、一般的に CPU の利用率が上がります。サブネット VLAN 数が表に示される数を超えると、イネーブルになっている機能に応じて、各カテゴリのサポートされているエントリ数が減ります。たとえば、16 を超えるサブネット VLAN で PIM-DVMRP がイネーブルになっている場合は、アクセス テンプレートに対するマルチキャスト ルートのエントリ数は、1 ~ 5 K の範囲です。

表 7-5 ギガビット イーサネット スイッチの各テンプレートで可能なリソースの概数

リソース	デフォルト テンプレート	アクセス テンプレート	ルーティング テンプレート	VLANテンプレート
ユニキャスト MAC アドレス	6 K	2 K	6 K	12 K
IGMP グループ (MVR や IGMP ス ヌーピングなどのレイヤ2 マルチ キャスト機能によって管理)	6 K	8 K	6 K	6 K
QoS 分類 ACE	2 K	2 K	1 K	2 K
セキュリティ ACE	2 K	4 K	1 K	2 K
ユニキャスト ルート	12 K または 6 K <sup>1</sup>	4 K または 2 K <sup>1</sup>	24 K または 12 K <sup>1</sup>	0
マルチキャスト ルート	6 K	8 K	6 K	0
サブネット VLAN (ルーテッド ポートおよび SVI)	16	16	16	16
レイヤ 2 VLAN	1 K	1 K	1 K	1 K

1. 指定されたテンプレートで *extended-match* キーワードを使用した場合。このキーワードは、使用できるユニキャスト ルート数にだけ影響します。

表 7-6 ファスト イーサネット スイッチの各テンプレートで可能なリソースの概数

リソース	デフォルト テンプレート	アクセス テンプレート	ルーティング テンプレート	VLANテンプレート
ユニキャスト MAC アドレス	5 K	1 K	5 K	8 K
IGMP グループ (MVR や IGMP ス ヌーピングなどのレイヤ2 マルチ キャスト機能によって管理)	1 K	2 K	1 K	1 K
QoS 分類 ACE	1 K	1 K	512	1 K
セキュリティ ACE	1 K	2 K	512	1 K
ユニキャスト ルート	8 K または 4 K <sup>1</sup>	2 K または 1 K <sup>1</sup>	16 K または 8 K <sup>1</sup>	0
マルチキャスト ルート	1 K	2 K	1 K	0
サブネット VLAN (ルーテッド ポートおよび SVI)	8	8	8	8
レイヤ 2 VLAN	1 K	1 K	1 K	1 K

1. 指定されたテンプレートで *extended-match* キーワードを使用した場合。このキーワードは、使用できるユニキャスト ルート数にだけ影響します。

## テンプレートの使用方法

SDM テンプレートを使用するときは、次の注意事項に従ってください。

- 各テンプレートで可能なリソースの最大数は概数で、設定されているほかの機能の実数によって異なります。たとえば、Catalyst 3550-12T のデフォルトテンプレートで、ご使用のスイッチに 16 を超えるルーテッド インターフェイスが設定されている場合は、ハードウェアが対応できるマルチキャストまたはユニキャスト ルートの数は、表の値より少なくなります。
- sdm prefer vlan* グローバル コンフィギュレーション コマンドを使用すると、スイッチのルーティング機能がディセーブルになります。リロード後は、どのようなルーティング設定も拒否され、以前に設定したルーティング オプションが失われることがあります。ルーティングをサポートしていないレイヤ 2 スイッチング専用スイッチに限り、*sdm prefer vlan* 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ください。

- スイッチでのルーティングをイネーブルにしない場合は、ルーティングテンプレートを 사용하지 ないでください。スイッチに **sdm prefer routing** グローバル コンフィギュレーション コマンド を入力しても、ルーティングはイネーブルになりませんが、ルーティングテンプレート内のユニキャストおよびマルチキャスト ルーティングに割り当てられたメモリがほかの機能で使用されなくなります。このメモリは、ギガビット イーサネット スイッチでは最大 30 K、ファスト イーサネット スイッチでは最大 17 K になります。
- WCCP または multi-VRF CE がスイッチでイネーブルになっている場合は、**extended-match** キーワードを使用して、144 ビットのレイヤ 3 TCAM をサポートする必要があります。このキーワードは、VLAN テンプレートではサポートされません。

ここでは、SDM テンプレートをデフォルトから変更する手順を示します。設定を有効にするには、スイッチをリロードする必要があります。スイッチをリロードする前に **show sdm prefer** イネーブル EXEC コマンドを使用すると、以前の設定（この場合はデフォルト）が表示されます。

SDM テンプレートを使用して機能動作を最適にサポートするには、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	<b>configure terminal</b>	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	<b>sdm prefer {access [extended-match]   extended-match   routing [extended-match]   vlan}</b>	<p>スイッチで使用する SDM テンプレートを指定します。</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"> <li>• <b>access</b> スイッチでの QoS 分類 ACE およびセキュリティ ACE の使用状況を最適化します。</li> <li>• <b>routing</b> スイッチでのルーティングを最適化します。</li> <li>• <b>vlan</b> ルーティングを行わないスイッチでの VLAN 設定を最適化します。</li> <li>• <b>extended-match</b> ルーティング メモリ スペースを再フォーマットし、デフォルト、アクセス、ルーティングの各テンプレートで 144 ビットのレイヤ 3 TCAM が、WCCP または multi-VRF CE をサポートするようにします。</li> </ul> <p>デフォルトのテンプレート（上記のいずれも設定されていない場合）では、ユニキャスト MAC アドレス、IGMP グループ、QoS ACE、セキュリティ ACE、ユニキャストおよびマルチキャスト ルート、ルーテッドインターフェイス、レイヤ 2 VLAN の使用状況が最適化されています。</p>
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>reload</b>	オペレーティング システムをリロードします。

システムの再起動後、**show sdm prefer** イネーブル EXEC コマンドを使用して、新しいテンプレート設定を確認できます。**reload** イネーブル EXEC コマンドの前に **show sdm prefer** コマンドを使用すると、新しいテンプレートではなく前のテンプレートが表示されます。

デフォルトのテンプレートに戻すには、**no sdm prefer** 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、スイッチにルーティングテンプレートを設定し、その設定を確認する例を示します。

```
Switch(config)# sdm prefer routing
Switch(config)# end
Switch# reload
Proceed with reload? [confirm]
```

