CHAPTER 4

スイッチの管理

この章では、Catalyst 4500 シリーズ スイッチで 1 回だけ行う管理作業の実行方法について説明します。

またこの章では、Catalyst 4500 シリーズ スイッチのグラフィカル表示と、GUI ベースの管理および設定インターフェイスを提供する組み込み CiscoView ネットワーク管理システムのインストールおよび設定方法についても説明します。

この章の主な内容は、次のとおりです。

（注） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『*Cisco IOS Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

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）を使用して手動または自動でスイッチのシステム日時を設定できます。

ここでは、次の設定について説明します。

- 「NTP の設定」（P.4-3）
- 「手動での日時の設定」（P.4-11）

システム クロック

時刻サービスの中核となるのはシステム クロックで、これによって日時をモニタリングします。このクロックはシステムが起動した瞬間から開始します。

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。現地の時間帯および夏時間に関する情報を設定することにより、時刻が現地の時間帯で正確に表示されるようにできます。

システム クロックは、時刻に*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）を常時モニタリングします。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。設定の詳細については、「手動での日時の設定」（P.4-11）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。NTP は、ネットワーク全体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、信頼できるタイム ソース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。

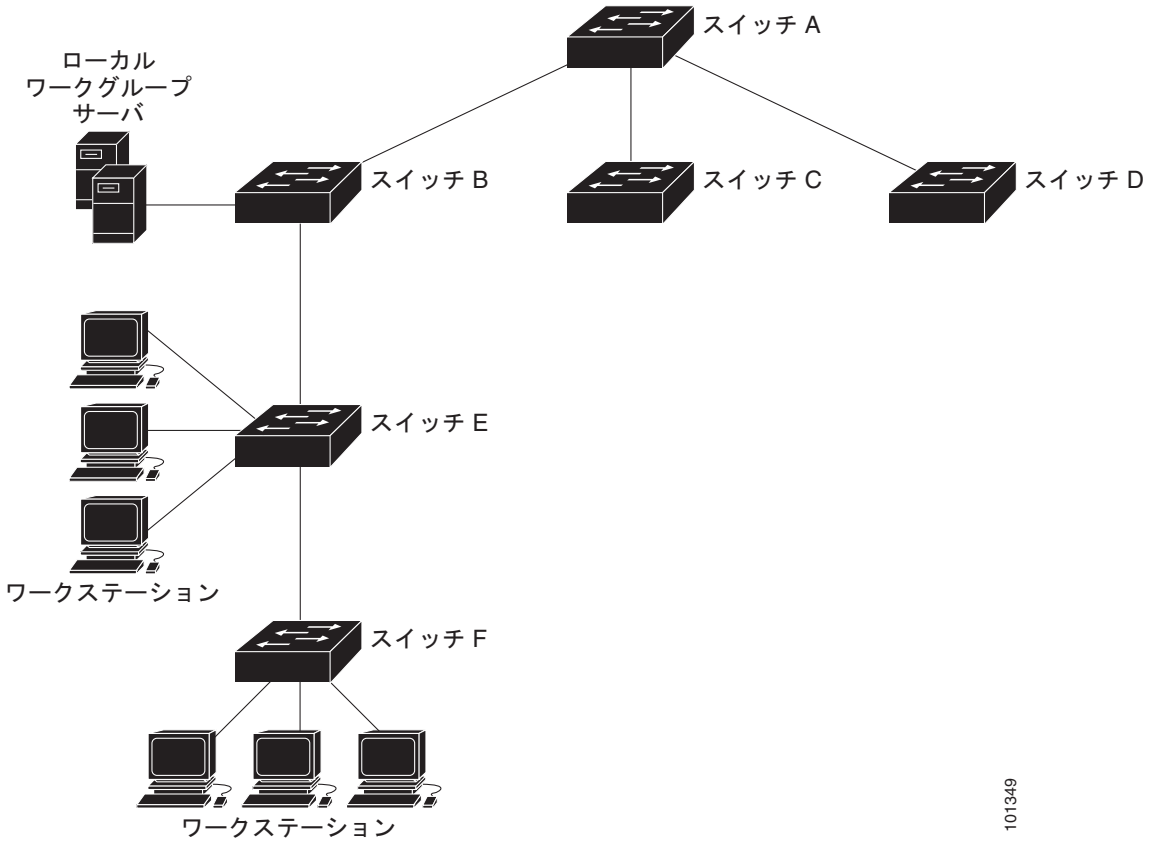
NTP が稼働するデバイス間の通信（*アソシエーション*）は、通常静的に設定されます。各デバイスには、アソシエーションを行う全デバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。各デバイスを、ブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段により設定の複雑さが緩和されます。この場合は、情報の流れは一方向に限られます。

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。

シスコによる NTP の実装では、ストラタム 1 サービスをサポートしていないため、ラジオ クロックまたはアトミック クロックに接続できません。ネットワークの時刻サービスは、IP インターネット上のパブリック NTP サーバから取得することを推奨します。

図 4-1 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 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 スイッチ（スイッチ B）およびダウンストリーム スイッチ（スイッチ F）の NTP ピアとして設定されています。

図 4-1　一般的な NTP ネットワークの構成



ネットワークがインターネットから切り離されている場合、シスコによる NTP 実装では、同期化していなくても、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。

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入れているメーカーもあり、また、UNIX システム用のパブリック バージョンやその派生ソフトウェアも入手できます。このソフトウェアによって、ホスト システムも時刻が同期化されます。

NTP の設定

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.4-4）
- 「NTP 認証の設定」（P.4-4）

NTP のデフォルト設定

表 4-1 に、NTP のデフォルト設定を示します。

表 4-1　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 コントロール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（正確な時刻の維持を行うための NTP を実行するデバイス間の通信）を認証するには、次の作業を行います。

	コマンド	目的
ステップ 1	`configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`ntp authenticate`	デフォルトではディセーブルに設定されている NTP 認証機能をイネーブルにします。

	コマンド	目的
ステップ 3	**ntp authentication-key** *number* **md5** *value*	認証キーを定義します。デフォルトでは何も定義されていません。 • *number* 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。 • *value* 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。 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、**ntp trusted-key** *key-number* 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。
ステップ 4	**ntp trusted-key** *key-number*	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しなければなりません。 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。 *key-number* には、ステップ 3 で定義したキーを指定します。 このコマンドは、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	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

NTP 認証をディセーブルにするには、**no ntp authenticate** グローバル コンフィギュレーション コマンドを使用します。認証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# configure terminal
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 42 md5 aNiceKey
Switch(config)# ntp trusted-key 42
Switch(config)# end
Switch#
```

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、次の作業を行います。

	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**] or **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。 • ピア アソシエーションの *ip-address* には、クロックの同期化を行う、または同期化の対象となるピアの IP アドレスを指定します。サーバ アソシエーションでは、クロックの同期化を行うタイム サーバの IP アドレスを指定します。 • （任意）*number* には、NTP のバージョン番号を指定します。指定できる範囲は 1 ～ 3 です。デフォルトでは、バージョン 3 が選択されます。 • （任意）*keyid* には、**ntp authentication-key** グローバル コンフィギュレーション コマンドで定義された認証キーを入力します。 • （任意）*interface* には、IP の送信元アドレスを取得するインターフェイスを指定します。デフォルトでは、送信元 IP アドレスは発信インターフェイスから取得します。 • （任意）**prefer** キーワードを指定すると、このピアまたはサーバが同期化を行う優先ピアまたはサーバになります。このキーワードは、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**	入力を確認します。
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、NTP 同期化が実行されない場合は、NTP バージョン 2 を使用してみてください。インターネット上の多くの NTP サーバがバージョン 2 で稼働しています。

ピアまたはサーバ アソシエーションを削除するには、**no ntp peer** *ip-address* または **no ntp server** *ip-address* グローバル コンフィギュレーション コマンドを使用します。

次に、NTP バージョン 2 を使用して、IP アドレス 172.16.22.44 のピアのクロックにシステム クロックを同期化するようにスイッチを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ntp server 172.16.22.44 version 2
```

```
Switch(config)# end
Switch#
```

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、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、スイッチを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	NTP ブロードキャスト パケットを送信するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]	NTP ブロードキャスト 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。 • （任意）*number* には、NTP のバージョン番号を指定します。指定できる範囲は 1 ～ 3 です。バージョンを指定しない場合は、バージョン 3 が使用されます。 • （任意）*keyid* には、ピアにパケットを送信するときに使用する認証キーを指定します。 • （任意）*destination-address* には、スイッチにクロックを同期化しているピアの IP アドレスを指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力を確認します。
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# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ntp broadcast version 2
Switch(config-if)# end
```

```
Switch#
```

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、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	NTP ブロードキャスト パケットを受信するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ntp broadcast client**	インターフェイスが NTP ブロードキャスト パケットを受信できるようにします。 デフォルトでは、インターフェイスは NTP ブロードキャスト パケットを受信しません。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ntp broadcastdelay** *microseconds*	（任意）スイッチと NTP ブロードキャスト サーバ間の予測されるラウンドトリップ遅延を変更します。 デフォルトは 3000 マイクロ秒です。指定できる範囲は 1 ～ 999999 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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。ラウンドトリップ遅延の予測値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# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ntp broadcast client
Switch(config-if)# end
Switch#
```

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.4-9）
- 「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.4-10）

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、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*	アクセス グループを作成し、基本 IP アクセス リストを適用します。 キーワードの意味は次のとおりです。 • **query-only**：NTP 制御クエリーに限り許可します。 • **serve-only**：時刻要求に限り許可します。 • **serve**：時刻要求と NTP 制御クエリーは許可しますが、スイッチがリモートデバイスと同期化することは許可しません。 • **peer**：時刻要求と NTP 制御クエリーを許可し、スイッチがリモートデバイスと同期化することを許可します。 *access-list-number* には、1 ～ 99 の範囲で標準の IP アクセス リスト番号を入力します。
ステップ 3	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	アクセス リストを作成します。 • *access-list-number* には、ステップ 2 で指定した番号を入力します。 • **permit** キーワードを入力すると、条件が一致した場合にアクセスを許可します。 • *source* には、スイッチへのアクセスが許可されたデバイスの IP アドレスを入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード ビットを入力します。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力を確認します。
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 コントロールを削除するには、**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
Switch(config)# end
Switch#
```

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。

インターフェイスで NTP パケットの受信をディセーブルにするには、次の作業を行います。

	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。 インターフェイスで 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。
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**	入力を確認します。
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。

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には、**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、次の作業を行います。

	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および番号を指定します。 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設定されます。
ステップ 3	`end`	特権 EXEC モードに戻ります。
ステップ 4	`show running-config`	入力を確認します。
ステップ 5	`copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

指定されたインターフェイスは、すべての宛先に送信されるすべてのパケットの送信元アドレスに使用されます。送信元アドレスを特定のアソシエーションに使用する場合は、「NTP アソシエーションの設定」（P.4-6）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

NTP 情報を表示するには、次の特権 EXEC コマンドを使用します。

- **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 12.3*』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、次の設定について説明します。

- 「システム クロックの設定」（P.4-11）
- 「日時設定の表示」（P.4-12）
- 「タイム ゾーンの設定」（P.4-12）
- 「夏時間の設定」（P.4-13）

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、次の作業を行います。

	コマンド	目的
ステップ 1	**clock set** *hh*:*mm*:*ss day month year* or **clock set** *hh*:*mm*:*ss month day year*	次のいずれかの形式で、手動でシステム クロックを設定します。 • *hh*:*mm*:*ss* には、時刻を時間（24 時間形式）、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。 • *day* には、当月の日付で日を指定します。 • *month* には、月を名前で指定します。 • *year* には、年を指定します（常に 4 桁で指定）。

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 クロックがタイミング ソースによって設定された場合は、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。クロックの信頼性がない間は、*authoritative* フラグが設定され、ピアの時刻が無効でもそのフラグによってピアがクロックと同期しないようにされます。

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

手動で時間帯を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	時間帯を設定します。 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。 スイッチは内部時刻を UTC で管理するので、このコマンドは表示目的の場合および手動で時刻を設定した場合に限って使用します。 • *zone* には、標準時間が施行されているときに表示されるタイムゾーンの名前を入力します。デフォルトの設定は UTC です。 • *hours-offset* には、UTC からの時差を入力します。 • （任意）*minutes-offset* には、UTC からの分差を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	入力を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

clock timezone グローバル コンフィギュレーション コマンドの **minutes-offset** 変数は、現地のタイム ゾーンと UTC との時差が分単位である場合に使用できます。たとえば、カナダ大西洋沿岸のある区域のタイム ゾーン（大西洋標準時（AST））は UTC-3.5 です。この場合、3 は 3 時間、.5 は 50% を意味します。必要なコマンドは、**clock timezone AST -3 30** です。

夏時間の設定

毎年特定の日に夏時間が開始および終了する地域に夏時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年指定された日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、夏時間のルールは米国のルールをデフォルトにします。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • （任意）*week* には、月の何週目かを指定します（1 ～ 5、または **last**）。 • （任意）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh*:*mm* には、時刻を時間（24 時間形式）と分で指定します。 • （任意）*offset* 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 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番めの部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、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# configure terminal
Switch(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October
2:00
Switch(config)# end
Switch#
```

ユーザの居住地域の夏時間が定期的なパターンに従わない（次の夏時間の正確な日時を設定する）場合は、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **date** [*month date year hh:mm month date year hh:mm* [*offset*]] or **clock summer-time** *zone* **date** [*date month year hh:mm date month year hh:mm* [*offset*]]	最初の日付で夏時間開始の日付を、2 番めの日付で終了の日付を設定します。 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。 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。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • （任意）*week* には、月の何週目かを指定します（1 ～ 5、または **last**）。 • （任意）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh*:*mm* には、時刻を時間（24 時間形式）と分で指定します。 • （任意）*offset* 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 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番めの部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、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# configure terminal
Switch(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
Switch#
```

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。

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、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.3*』および『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.3*』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。

- 「システム名の設定」（P.4-15）
- 「DNS の概要」（P.4-15）

システム名の設定

手動でシステム名を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *name*	手動でシステム名を設定します。 デフォルト設定は *switch* です。 名前は ARPANET ホスト名のルールに従う必要があります。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。 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。
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**	入力を確認します。
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。

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 アドレスにマッピングできます。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。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、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* となります。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

表 4-2 に、DNS のデフォルト設定を示します。

表 4-2　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、次の作業を行います。

	コマンド	目的
ステップ 1	`configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip domain-name** *name*	非完全修飾ホスト名（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。 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）。
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 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。 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。

	コマンド	目的
ステップ 4	`ip domain-lookup`	（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されています。 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。 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`	特権 EXEC モードに戻ります。
ステップ 6	`show running-config`	入力を確認します。
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、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。

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、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.3*』を参照してください。

次の設定情報が含まれます。

- 「バナーのデフォルト設定」（P.4-17）
- 「MoTD ログイン バナーの設定」（P.4-18）
- 「ログイン バナーの設定」（P.4-20）

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、次の作業を行います。

	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 を指定します。
		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。
		c には、任意の区切り文字、たとえばポンド記号（#）を入力して、Return キーを押します。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。
		（注） Supervisor Engine 7-E および Supervisor Engine 7L-E で、区切り文字として「#」記号を使用してバナーを設定する場合は、初めに **no shell processing** コマンドでシェル処理をオフにする必要があります。そうしなければ、バナーの設定を終了できません。
		`### With shell processing enabled ###`
		`Sup7# conf t`
		`Enter configuration commands, one per line.  End with CNTL/Z.`
		`Sup7(config)# ban`
		`Sup7(config)# banner lo`
		`Sup7(config)# banner login #`
		`Enter TEXT message.  End with the character '#'`
		`test login banner`
		`#`
		`##`
		`e#`
		`Sup7(config)#`
		`### With shell processing disabled ###`
		`Sup7(config)# banner login #`
		`Enter TEXT message.  End with the character '#'`
		`test login banner`
		`#`
		`Sup7(config)#`
		message には、255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。

ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力を確認します。
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。

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 #
```

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

次に、前の設定により表示されたバナーの例を示します。

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

it 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、次の作業を行います。

	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。
		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。
		c には、任意の区切り文字、たとえばポンド記号（#）を入力して、Return キーを押します。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。
		（注） Supervisor Engine 7-E および Supervisor Engine 7L-E で、区切り文字として「#」記号を使用してバナーを設定する場合は、初めに **no shell processing** コマンドでシェル処理をオフにする必要があります。そうしなければ、バナーの設定を終了できません。
		`### With shell processing enabled ###`
		`Sup7# conf t`
		`Enter configuration commands, one per line.  End with CNTL/Z.`
		`Sup7(config)# ban`
		`Sup7(config)# banner lo`
		`Sup7(config)# banner login #`
		`Enter TEXT message.  End with the character '#'`
		`test login banner`
		`#`
		`##`
		`e#`
		`Sup7(config)#`
		`### With shell processing disabled ###`
		`Sup7(config)# banner login #`
		`Enter TEXT message.  End with the character '#'`
		`test login banner`
		`#`
		`Sup7(config)#`
		message 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**	入力を確認します。
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。

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# configuration terminal
```

```
Switch(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
Switch(config)# end
Switch#
```

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 アドレス

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN ID、アドレスに対応付けられたポート番号、およびタイプ（スタティックまたはダイナミック）のリストです。

（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、次の設定について説明します。

アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスによって、スイッチの任意のポートを各ワークステーション、リピータ、スイッチ、ルータ、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。

エージング間隔はグローバルに設定されます。ただし、スイッチは VLAN ごとにアドレス テーブルを維持し、STP（スパニングツリー プロトコル）によって VLAN 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（複数可）に限定してパケットを転送します。宛先アドレスがパケットを送信したポート上にある場合は、パケットはフィルタリング処理され、転送されません。スイッチは、常にストア アンド フォワード方式を使用します。このため、完全なパケットをいったん保存してエラーがないか検査してから伝送します。

MAC アドレスおよび VLAN

アドレスはすべて、VLAN と対応付けられます。1 つのアドレスを複数の VLAN に対応付け、それぞれで異なる宛先を設定できます。たとえば、ユニキャスト アドレスを VLAN 1 のポート 1 および VLAN 5 のポート 9、10、1 に転送するといったことが可能です。

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。

PVLAN が設定されている場合、アドレス ラーニングは次のように MAC アドレスのタイプに左右されます。

- プライベート PVLAN の 1 つの VLAN で学習したダイナミック MAC アドレスは、関連 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 に複製されます。
- プライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは関連 VLAN には複製されません。PVLAN のプライマリまたはセカンダリ VLAN 内にスタティック MAC アドレスを設定した場合、同じスタティック MAC アドレスをすべての関連 VLAN に設定する必要があります。

PVLAN の詳細については、第 43 章「プライベート VLAN の設定」を参照してください。

MAC アドレス テーブルのデフォルト設定

表 4-3 に、MAC アドレス テーブルのデフォルト設定を示します。

表 4-3　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。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。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を及ぼす可能性があります。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。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及ぼす可能性があります。

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、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table aging-time** [**0** | *10-1000000*] [**vlan** *vlan-id*]	ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に保持される時間を設定します。 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。 指定できる範囲は 10 ～ 1000000 秒です。デフォルトは 300 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。 *vlan-id* の有効範囲は、1 ～ 4094 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table aging-time**	入力を確認します。
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。

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、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 変更通知トラップの設定

MAC 変更通知機能により、スイッチに MAC 変更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たびに、SNMP 通知を生成して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。ネットワークに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まとめ、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、ダイナミックおよびスタティックの MAC アドレスについて生成されます。自己アドレスまたはマルチキャスト 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 変更通知トラップを送信するには、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* [**traps** | **informs**] {**version** {**1**|**2c**|**3**}} [**auth** | **noauth** | **priv**] *community-string* [***udp-port port***] [***notification-type***]	トラップ メッセージの受信側を指定します。 • *host-addr* には、NMS の名前または 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。 • *community-string* 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。 • *notification-type* には、**mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification change**	スイッチによる MAC 変更トラップの NMS への送信をイネーブルにします。 スイッチによる MAC 変更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 change** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**mac address-table notification change**	MAC アドレス変更通知機能をイネーブルにします。
ステップ 5	**mac address-table notification change** [**interval** *value*] | [**history-size** *value*]	トラップ インターバル タイムと履歴テーブルのサイズを入力します。 • （任意）**interval** *value* には、NMS に対して生成される各トラップ セット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は 0 ～ 2147483647 秒です。デフォルトは 1 秒です。 • （任意）**history-size** *value* には、MAC 通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は 0 ～ 500 です。デフォルトは 1 です。 MAC 変更通知機能をディセーブルにするには、**no mac address-table notification change** グローバル コンフィギュレーション コマンドを使用します。

	コマンド	目的
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC 変更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。
ステップ 7	**snmp trap mac-notification change** {**added** | **removed**}	MAC 変更通知トラップをイネーブルにします。 • **added** を指定すると、このインターフェイスに MAC アドレスが追加されるたびに MAC 変更通知トラップが送信されます。 • **removed** を指定すると、このインターフェイスから MAC アドレスが削除されるたびに MAC 変更通知トラップが送信されます。 特定のインターフェイス上で MAC 変更通知トラップをディセーブルにするには、**no snmp trap mac-notification change** {**added** | **removed**} インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mac address-table notification change interface** **show running-config**	入力を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、ネットワーク管理システムとして 172.69.59.93 を指定し、スイッチによるネットワーク管理システムへの MAC 変更通知トラップの送信をイネーブルにし、MAC 変更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# configure terminal
Switch(config)# snmp-server host 172.69.59.93 private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 60
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface fastethernet0/2
Switch(config-if)# snmp trap mac-notification change added
Switch(config-if)# end
Switch# show mac address-table notification change interface
MAC Notification Feature is Enabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
----------------------------------------------------
Interface            MAC Added Trap MAC Removed Trap
---------            -------------- ----------------
GigabitEthernet1/1   Enabled        Enabled
GigabitEthernet1/2   Enabled        Enabled
GigabitEthernet1/3   Enabled        Enabled
GigabitEthernet1/4   Enabled        Enabled
GigabitEthernet1/5   Enabled        Enabled
GigabitEthernet1/6   Enabled        Enabled
GigabitEthernet1/7   Enabled        Enabled
GigabitEthernet1/8   Enabled        Enabled
GigabitEthernet1/9   Enabled        Enabled
GigabitEthernet1/10  Enabled        Enabled
GigabitEthernet1/11  Enabled        Enabled
GigabitEthernet1/12  Enabled        Enabled
```

```
Switch#
```

MAC 移動通知トラップの設定

MAC 移動通知を設定すると、MAC アドレスが同一 VLAN 内の特定のポートから別のポートに移動するたびに、SNMP 通知が生成され、ネットワーク管理システムに送信されます。

MAC 移動通知を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* [**traps** | **informs**] {**version** {**1**|**2c**|**3**}} [**auth** | **noauth** | **priv**] *community-string* [***udp-port port***] [***notification-type***]	トラップ メッセージの受信側を指定します。 • *host-addr* には、NMS の名前または 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。 • *community-string* 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。 • *notification-type* には、**mac-notification** キーワードを使用します。
ステップ 3	**snmp-server enable traps mac-notification move**	スイッチによる MAC 移動通知トラップの NMS への送信をイネーブルにします。 スイッチによる MAC 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 move** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**mac address-table notification mac-move**	MAC 移動通知機能をイネーブルにします。 この機能をディセーブルにするには、**no mac-address-table notification mac-move** グローバル コンフィギュレーション コマンド使用します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show mac address-table notification mac-move** **show running-config**	MAC 移動通知ステータスを表示します。
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。

次に、ネットワーク管理システムとして 172.69.59.93 を指定し、スイッチによる MAC 移動通知トラップの NMS への送信をイネーブルにし、MAC 移動通知機能をイネーブルにし、MAC アドレスが特定のポートから別のポートに移動する場合のトラップをイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# snmp-server host 171.69.59.93 private mac-notification
Switch(config)# snmp-server enable traps mac-notification move
Switch(config)# mac address-table notification mac-move
Switch(config)# end
Switch# show mac address-table notification mac-move
MAC Move Notification: Enabled
```

MAC しきい値通知トラップの設定

MAC しきい値通知を設定すると、MAC Address Table（MAT）しきい値の制限値に達した時点または制限値を超えた時点で、SNMP 通知が生成され、ネットワーク管理システムに送信されます。

MAC アドレスしきい値通知を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* [**traps**|**informs**] {**version** {**1**|**2c**|**3**}} [**auth** | **noauth** | **priv**] *community-string* [***udp-port port***] [***notification-type***]	トラップ メッセージの受信側を指定します。 • *host-addr* には、NMS の名前または 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。 • *community-string* 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。 • *notification-type* には、**mac-notification** キーワードを使用します。

	コマンド	目的
ステップ 3	**snmp-server enable traps mac-notification threshold**	スイッチによる MAC しきい値通知トラップの NMS への送信をイネーブルにします。 スイッチによる MAC しきい値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 threshold** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**mac address-table notification threshold**	MAC アドレスしきい値通知機能をイネーブルにします。 この機能をディセーブルにするには、**no address-table notification threshold** グローバル コンフィギュレーション コマンドを使用します。
ステップ 5	**mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]	MAT 使用率をモニタリングするためのしきい値を入力します。 • （任意）**limit** *percentage* には、MAT 利用率の割合を指定します。指定できる値は、1 ～ 100% です。デフォルト値は 50% です。 • （任意）**interval** *time* には、通知の間隔を指定します。指定できる値は、120 秒以上です。デフォルトは 120 秒です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mac address-table notification threshold** **show running-config**	MAC 利用率しきい値通知ステータスを表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、ネットワーク管理システムとして 172.69.59.93 を指定し、MAC しきい値通知機能をイネーブルにし、スイッチによる MAC しきい値通知トラップの NMS への送信をイネーブルにし、間隔を 123 秒に設定し、制限値を 78% に設定する例を示します。

```
Switch# configure terminal
Switch(config)# snmp-server host 171.69.59.93 private mac-notification
Switch(config)# snmp-server enable traps mac-notification threshold
Switch(config)# mac address-table notification threshold
Switch(config)# mac address-table notification threshold interval 123
Switch(config)# mac address-table notification threshold limit 78
Switch(config)# end
Switch# show mac-address-table notification threshold
     Status       limit        Interval
-------------+-----------+-------------
   enabled        78           123
Switch#
```

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。転送動作は、パケットを受信したポートが、別のポートにパケットを転送する動作を決定します。ポートは必ず少なくとも 1 つの VLAN と対応しているので、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。

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 ユニキャスト アドレスと、その送信元 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。

プライベート VLAN のプライマリまたはセカンダリ VLAN 内にスタティック MAC アドレスを設定した場合、同じスタティック MAC アドレスをすべての関連 VLAN に設定する必要があります。プライベート VLAN のプライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは関連 VLAN には複製されません。PVLAN の詳細については、第 43 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、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	MAC アドレス テーブルにスタティック アドレスを追加します。 • *mac-addr* には、アドレス テーブルに追加する宛先 MAC ユニキャスト アドレスを指定します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 • *vlan-id* には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。 • *interface-id* 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、物理ポートまたはポート チャネルです。 複数のインターフェイス ID にスタティック マルチキャスト アドレスを指定できます。ただし、同じ MAC アドレスと VLAN ID を持つ複数のインターフェイスへスタティック ユニキャスト MAC アドレスを割り当てることはできません 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。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show mac address-table static**	入力を確認します。
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。

次の例では、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する方法を示します。VLAN 4 でこの MAC アドレスを宛先アドレスとしてパケットを受信すると、パケットは指定されたポートに転送されます。

```
Switch# configure terminal
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
Switch(config)# end
Switch#
```

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。

ユニキャスト アドレス フィルタリングを使用する場合、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされません。**mac address-table static vlan 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ません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し､ユニキャスト MAC アドレス フィルタリングを設定する場合は、最後に入力されたコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか､またはその MAC アドレスを持つパケットをドロップします。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 vlan interface** 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 vlan 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指定された MAC アドレスを持つパケットをドロップします。

  mac address-table static vlan 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 vlan interface** 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、次の作業を行います。

	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。 • *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。指定できる VLAN ID の範囲は 1 ～ 4094 です。 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 vlan** グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mac address-table static**	入力を確認します。
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。

次の例では、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つパケットをドロップするようにスイッチを設定する方法を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

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

（注）　セカンダリ VLAN で MAC アドレスをフィルタリングするには、上記の設定で、対応するプライマリ VLAN を指定します。指定した VLAN がプライマリ VLAN の場合、このプライマリ VLAN および関連するセカンダリ VLAN で受信されたすべての一致するパケットはドロップされます。

VLAN の MAC アドレス ラーニングのディセーブル化

デフォルトでは、MAC アドレス ラーニングは、スイッチのすべての VLAN でイネーブルです。MAC アドレスを学習できる VLAN を制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。VLAN でラーニングをディセーブルにすると、この VLAN に表示されるすべての MAC アドレスが学習されていないため、MAC アドレス テーブル スペースを節約できます。

MAC アドレス ラーニングをディセーブルにする前に、配備されているネットワーク トポロジと機能を理解する必要があります。多くのレイヤ 2 機能は MAC アドレスを使用し、ラーニングがディセーブルの場合は、正しく動作しない可能性があります。ラーニングをディセーブルにすることはパケットのフラッディングの原因となるため、ネットワークでのフラッディングの影響を理解する必要があります。

ここでは、次の情報について説明します。

• 「導入シナリオ」（P.4-34）

MAC アドレス ラーニングのディセーブル設定

VLAN で MAC アドレス ラーニングをディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# no mac address-table learning vlan` *vlan-id range*	指定された 1 つまたは複数の VLAN で MAC アドレス ラーニングをディセーブルにします。1 つの VLAN ID を指定、または VLAN ID の範囲をハイフンまたはカンマで区切って指定できます。指定できる VLAN ID の範囲は 1 ～ 4094 です。 **mac address-table learning vlan** グローバル コンフィギュレーション コマンドを入力して VLAN で MAC アドレス ラーニングを再びイネーブルにできます。
ステップ 3	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Switch# show mac address-table learning` [**vlan** *vlan-id range*]	すべての VLAN または指定した VLAN の MAC アドレス ラーニングのステータスを表示します。
ステップ 5	`Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、任意の VLAN または VLAN 範囲でラーニングをディセーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# no mac address-table learning vlan 9-16
Switch(config)# end
Switch#

Switch# show mac address-table learning
Learning disabled on vlans: 9-11,13-16

Switch# show mac address-table learning vlan 10-15
Learning disabled on vlans: 10-11,13-15
```

使用上のガイドライン

（注）　これらのガイドラインは、アドバイスとしてのみ提供されます。特定のソリューションの実装については、シスコのソリューション プロバイダー チームに問い合わせてください。

VLAN で MAC アドレス ラーニングをディセーブルにする場合は、次のガイドラインに従ってください。

- ラーニングが SVI インターフェイスのある VLAN 上でディセーブルである場合、レイヤ 2 ドメイン内のすべての IP パケットがフラッディングされます。このフラッディングが望ましくない場合があるため、SVI VLAN では MAC アドレス ラーニングを慎重にディセーブルにする必要があります。
- 予約済みの VLAN を含む VLAN 範囲（1000 ～ 1006 など）を指定すると、そのコマンドは受け入れられ、ディセーブルのラーニングは 1002 ～ 005 を除くすべての VLAN（つまり、1000 ～ 1001、1006）でイネーブルになります。ただし、無効な範囲（1 ～ 5000 など）を指定した場合、コマンドは失敗し、ディセーブルのラーニングは VLAN でイネーブルになりません。
- PVLAN では、プライマリ VLAN と、そのプライマリ VLAN に関連付けられたすべてのセカンダリ VLAN で、ラーニングをディセーブルにする必要があります。そうしなければ、一方向でトラフィック フラッディング、その他の方向でユニキャスト フラッディングが発生します。
- VLAN で MAC アドレス ラーニングをディセーブルにする場合は、フラッディングの影響を考慮に入れます。

導入シナリオ

ここでは、次の導入シナリオについて取り上げます。

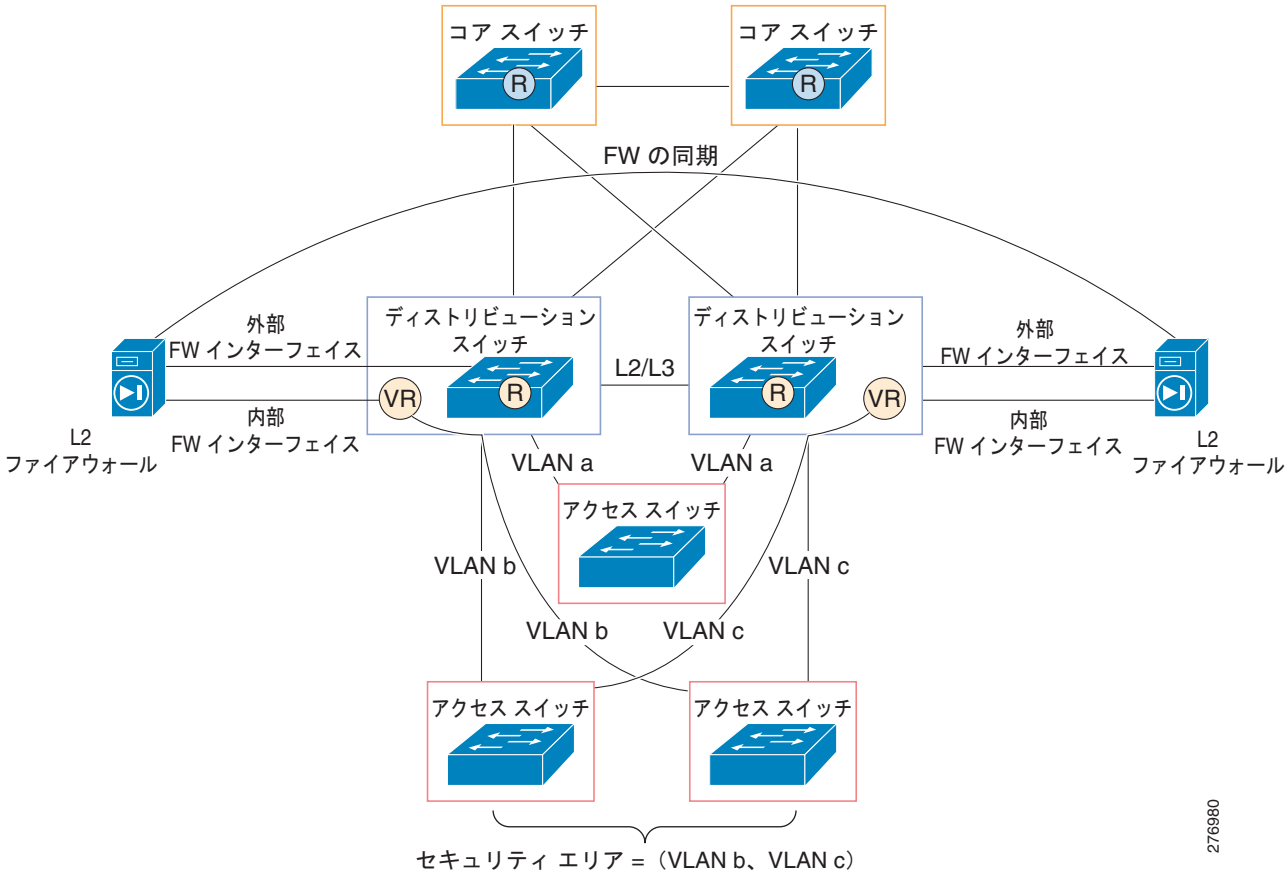
- 「メトロ（ポイント ツー ポイント リンク）」（P.4-34）
- 「ネットワーク ロード バランサ」（P.4-35）
- 「レイヤ 2 ファイアウォールまたはキャッシュ」（P.4-35）

メトロ（ポイント ツー ポイント リンク）

このトポロジでは、VLAN の 2 つのポートがあります。トラフィックは、一方に着信し、他方から発信する必要があります。メトロ ネットワークのポイントツーポイント リンクでは、この 2 つのポートが属する VLAN でラーニングをディセーブルにすることにより、これらのポートのタイプで多数の MAC アドレスが生じ、MAC アドレス テーブル スペースで多数のエントリを節約できます。トラフィック用の出力ポートは 1 つだけであるため、パケットをフラッディングさせ、このポートで認識されるすべての MAC アドレスのラーニングを回避できます。このプロセスによって、MAC アドレス テーブルでかなりのスペースを節約できます。

送信元ラーニングを取得するために、パケットはレイヤ 2 のフラッディング パケットとしてブリッジされます。複製されたパケットは、個別の専用帯域幅を使用します。フラッディング セットのポート数にかかわらず、フラッディング パケットは複製パケット帯域幅を常に消費します。これにより、一部のマルチキャストおよびブロードキャスト パケット処理帯域幅が消費されます（図 4-2）。

図 4-2　MAC アドレス ラーニングのディセーブル化：ポイントツーポイント リンク



ネットワーク ロード バランサ

このトポロジでは、2 台のデバイス（1 台はアクティブ、もう 1 台はスタンバイ）があります。ロード バランシングを実行するには、両方のデバイスがすべてのパケットを受信する必要があります。同じ VLAN に両方のデバイスを配置できます。この VLAN でラーニングをディセーブルにできる場合、パケットはフラッディングされ、両方のデバイスが VLAN 上の MAC アドレスを宛先とするすべてのトラフィックを受信します。または、すべてのパケットが到達するように、両方のロード バランサにマルチキャスト MAC アドレスを割り当てることができます。（図 4-3）。

図 4-3　MAC アドレス ラーニングのディセーブル化：ネットワーク ロード バランサ

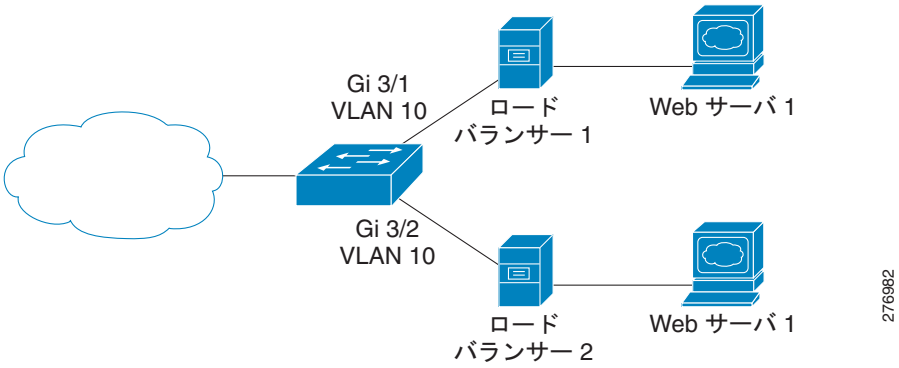
レイヤ 2 ファイアウォールまたはキャッシュ

このトポロジでは、書き換えられたレイヤ 3 パケットは、発信する前に、レイヤ 2 ファイアウォール（またはキャッシュ）に戻ります。パケットがファイアウォールからスイッチに再び着信したときに、パケットは、事前にルーティングされたため、スイッチの MAC アドレスを持っています。入力ポート

がスイッチ ポートである場合、スイッチはルータの MAC アドレスを学習します。ただし、ルーテッド ポートまたは SVI に対して、スイッチはアドレスを学習しません。送信元のエラーはすべての着信データ パケットで継続して発生し、スイッチでは CPU 使用率が非常に高くなります。

ファイアウォールまたはキャッシュの出力が接続されている VLAN でラーニングをディセーブルにすることによって、定期的に送信元のエラーが抑制され、高い CPU 使用率が生じなくなります（図 4-4）。

図 4-4　MAC アドレス ラーニングのディセーブル化：レイヤ 2 ファイアウォール/キャッシュ



機能の互換性

次の機能は、VLAN での MAC アドレス ラーニングのディセーブル化と互換性があります。

- EtherChannel：MAC ラーニング ステートが EtherChannel ポートの VLAN でディセーブルまたはイネーブルの場合、ラーニングのディセーブル化機能は、EtherChannel に影響しません。
- Switch Virtual Interface（SVI、VLAN のレイヤ 3）：ラーニングのディセーブル化機能は、SVI に影響しません。SVI VLAN で MAC アドレス ラーニングをディセーブルにすると、フラッディングが生じますが、レイヤ 3 機能には影響を与えません。
- REP：REP が動作しているポートのアクティブな VLAN で、MAC ラーニング ステートがディセーブルまたはイネーブルの場合、ラーニングのディセーブル化機能は、REP に影響しません。
- ユニキャスト、マルチキャスト、およびブロードキャスト：VLAN でラーニングをイネーブルにすると、ラーニングは、すべてのトラフィック タイプでディセーブルになります。
- DAI、ESMP および IGMP スヌーピング：これらの機能は、ラーニングのディセーブル化機能と相互作用しません。
- 制御パケット：ラーニングがディセーブルになっている場合でも、制御パケットは CPU に到達します。
- RSPAN：VLAN と RSPAN でのラーニングには互換性があります。
- VLAN 変換：変換対象の VLAN でラーニングをディセーブルにするには、変換先 VLAN でラーニングをディセーブルにする必要があります。

機能の非互換性

次の機能は、MAC アドレス ラーニングのディセーブル化と互換性がなく、イネーブルにした場合に正常に動作しません。

- 802.1X：802.1X 機能クラスは、ラーニングがディセーブルな場合は機能しません。これは、一部の機能が、（無視される）送信元のエラーを必要とするためです。
- ポート セキュリティ：ポート セキュリティ VLAN では、ラーニングをイネーブルにする必要があります。MAC アドレスをセキュアにするには、パケットは最初に CPU に着信する必要があります。しかし、VLAN でラーニングをディセーブルにすると、SA の抑制によって、パケットはこのように動作しなくなります。
- ユニキャスト フラッディング ブロック：ユニキャスト フラッディング ブロックがポートでイネーブルの場合、そのポートは、VLAN のフラッディング セットから除外されます。同じ VLAN でラーニングをディセーブルにした場合、そのポートに接続されたホストはトラフィックを受信しません。
- DHCP スヌーピング：DHCP 要求が解決した後にパケットを正しいポートから発信するために、DHCP スヌーピングは MAC アドレスを学習する必要があります。ラーニングをディセーブルにすると、スイッチはパケットを発信するポートを認識しません。つまり、これらの 2 つの機能には、互換性がありません。
- ブロードキャスト ストーム制御：この機能は、ラーニングのディセーブル化機能と相互作用しません。
- PVL を通じて、ラーニングをディセーブルにした VLAN ドメインでのパケットのフラッディング。

部分的な機能の非互換性

次の機能は MAC アドレス ラーニングのディセーブル化と部分的に互換性がありませんが、機能の大部分は保持されます。

- FlexLink：FlexLink は動作し、アップストリーム コンバージェンスは影響を受けません。ただし、ダウンストリーム高速コンバージェンスは、MAC テーブルを使用して、ダウンストリーム コンバージェンスを高速化するために、個々に学習されたアップストリームの MAC アドレスに、ダミーのマルチキャスト パケットを転送します。この状況は、ディセーブルなラーニングをイネーブルにした場合は発生しません。FlexLink のダウンストリーム コンバージェンスは適切に実行されますが、ラーニングがその VLAN でイネーブルの場合は、速度が遅くなります。
- PVLAN：変更の動作を監視するには、プライマリ VLAN と、そのプライマリ VLAN に関連付けられたすべてのセカンダリ VLAN で、ラーニングをディセーブルにする必要があります。

（注）　混乱を避けるために、PVLAN スペース内のプライマリ VLAN とセカンダリ VLAN の両方で、PVLAN を同様に設定します。

- スパニングツリー（STP）：UplinkFast 機能を除いて、VLAN 単位のスパニングツリー機能は影響を受けません。より高速なダウンストリーム コンバージェンスを実現するために、UplinkFast は、学習された MAC アドレスを使用して、ダミーのマルチキャスト パケットを転送します。MAC ラーニングがイネーブルでない場合、このアクションは不可能です。

アドレス テーブル エントリの表示

表 4-4 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 4-4　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 アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	MAC 通知パラメータおよび履歴テーブルを表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan	指定された VLAN の MAC アドレス テーブル情報を表示します。

ARP テーブルの管理

デバイスと通信するには（イーサネット上のデバイスなど）、ソフトウェアは最初にそのデバイスの 48 ビット MAC アドレスまたはローカル データ リンク アドレスを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。

アドレス解決プロトコル（ARP）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 アドレスを使用して、ARP は対応する MAC アドレスを見つけます。MAC アドレスが見つかると、IP と MAC アドレスの関連付けは、高速な検索のために ARP キャッシュに保存され、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/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 で入手可能な Cisco IOS Release 12.3 のマニュアルを参照してください。

組み込み CiscoView サポートの設定

Catalyst 4500 シリーズ スイッチは、Catalyst Web Interface（CWI）ツールを使用した CiscoView Web ベースの管理機能をサポートしています。CiscoView は、スイッチ フラッシュ上に組み込むことができるデバイス管理アプリケーションで、スイッチのダイナミック ステータス、モニタリング、および設定情報を提供します。CiscoView では、モジュールとポートが色分けされたスイッチ シャーシの物理的ビューを表示します。モニタリング機能を使用すると、スイッチのステータス、パフォーマンス、

およびその他の統計情報が表示されます。必要なセキュリティ権限が与えられていれば、設定機能によって、デバイスにさまざまな変更を加えることができます。Catalyst 4500 シリーズ スイッチの設定機能およびモニタリング機能は、CiscoWorks LAN Management Solution（LMS）および CiscoWorks Routed WAN Management Solution（RWAN）を含むすべてのサーバベースの CiscoWorks ソリューションの CiscoView で使用可能な機能と同一です。

ここでは、Cisco IOS Release 12.1(20)EW 以降のリリースで使用できる組み込み CiscoView サポートについて説明します。

組み込み CiscoView の概要

組み込み CiscoView ネットワーク管理システムは、Web ベースのインターフェイスであり、HTTP および SNMP を使用してスイッチをグラフィック表示し、GUI ベースの管理および設定インターフェイスを提供します。

組み込み CiscoView のインストールおよび設定

組み込み CiscoView のインストールおよび設定を行うには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# dir device_name`	デバイスの内容を表示します。 組み込み CiscoView を初めてインストールする場合、または CiscoView ディレクトリが空の場合には、ステップ 5 にスキップしてください。
ステップ 2	`Switch# delete device_name:cv/*`	CiscoView ディレクトリから既存のファイルを削除します。
ステップ 3	`Switch# squeeze device_name:`	ファイル システムのスペースを復元します。
ステップ 4	`Switch# copy tftp bootflash`	tar ファイルをブートフラッシュにコピーします。
ステップ 5	`Switch# archive tar /xtract tftp://ip address of tftp server/ciscoview.tar device_name:cv`	Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ上の tar ファイルから CiscoView ディレクトリに、CiscoView ファイルを抽出します。
ステップ 6	`Switch# dir device_name:`	デバイスの内容を表示します。 冗長構成の場合は、冗長スーパーバイザ エンジンのファイル システムについてステップ 1 ～ステップ 6 を繰り返します。
ステップ 7	`Switch# 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 8	`Switch(config)# ip http server`	HTTP Web サーバをイネーブルにします。
ステップ 9	`Switch(config)# snmp-server community string ro`	読み取り専用動作の SNMP パスワードを設定します。
ステップ 10	`Switch(config)# snmp-server community string rw`	読み取り / 書き込み動作の SNMP パスワードを設定します。

（注）　スイッチ Web ページにアクセスするためのデフォルトのパスワードは、スイッチのイネーブルレベルパスワードです。

次に、スイッチに組み込み CiscoView をインストールおよび設定する例を示します。

```
Switch# dir
Directory of bootflash:/
Directory of bootflash:/
    1  -rw-     9572396  Dec 30 2002 01:05:01 +00:00  cat4000-i9k2s-mz.121-19.EW
    2  -rw-     9604192   Jan 3 2003 07:46:49 +00:00  cat4000-i5k2s-mz.121-19.EW
    3  -rw-     1985024  Jan 21 2003 03:31:20 +00:00  Cat4000IOS.v4-0.tar
    4  -rw-     1910127  Jan 23 2003 04:23:39 +00:00  cv/Cat4000IOS-4.0.sgz
    5  -rw-        7258  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_ace.html
    6  -rw-         405  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_error.html
    7  -rw-        2738  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_install.html
    8  -rw-       20450  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_jks.jar
    9  -rw-       20743  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_nos.jar
   10  -rw-       12383  Jan 23 2003 04:23:46 +00:00  cv/applet.html
   11  -rw-         529  Jan 23 2003 04:23:46 +00:00  cv/cisco.x509
   12  -rw-        2523  Jan 23 2003 04:23:46 +00:00  cv/identitydb.obj
   13  -rw-        1173  Mar 19 2003 05:50:26 +00:00  post-2003.03.19.05.50.07-passed.txt

32578556 bytes total (38199688 bytes free)
Switch#
Switch# del cv/*
Delete filename [cv/*]?
Delete bootflash:cv/Cat4000IOS-4.0.sgz? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_ace.html? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_error.html? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_install.html? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_jks.jar? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_nos.jar? [confirm]y
Delete bootflash:cv/applet.html? [confirm]y
Delete bootflash:cv/cisco.x509? [confirm]y
Delete bootflash:cv/identitydb.obj? [confirm]y
Switch#

Switch# squeeze bootflash:
All deleted files will be removed. Continue? [confirm]y
Squeeze operation may take a while. Continue? [confirm]y
Squeeze of bootflash complete
Switch#
Switch# copy tftp bootflash
Address or name of remote host []? 10.5.5.5
Source filename []? Cat4000IOS.v5-1.tar
Destination filename [Cat4000IOS.v5-1.tar]?
Accessing tftp://10.5.5.5/Cat4000IOS.v5-1.tar...
Loading Cat4000IOS.v5-1.tar from 10.5.5.5 (via FastEthernet2/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 2031616 bytes]

2031616 bytes copied in 11.388 secs (178400 bytes/sec)
Switch#
Switch# dir
Directory of bootflash:/

Directory of bootflash:/
    1  -rw-     9572396  Dec 30 2002 01:05:01 +00:00  cat4000-i9k2s-mz.121-19.EW
    2  -rw-     9604192   Jan 3 2003 07:46:49 +00:00  cat4000-i5k2s-mz.121-19.EW
    3  -rw-     1985024  Jan 21 2003 03:31:20 +00:00  Cat4000IOS.v4-0.tar
    4  -rw-        1173  Mar 19 2003 05:50:26 +00:00  post-2003.03.19.05.50.07-passed.txt
```

```
    5  -rw-     2031616  Mar 26 2003 05:33:12 +00:00  Cat4000IOS.v5-1.tar

32578556 bytes total (38199688 bytes free)

Switch#
Switch# archive tar /xtract Cat4000IOS.v5-1.tar /cv
extracting Cat4000IOS-5.1.sgz (1956591 bytes)
extracting Cat4000IOS-5.1_ace.html (7263 bytes)
extracting Cat4000IOS-5.1_error.html (410 bytes)
extracting Cat4000IOS-5.1_install.html (2743 bytes)
extracting Cat4000IOS-5.1_jks.jar (20450 bytes)
extracting Cat4000IOS-5.1_nos.jar (20782 bytes)
extracting applet.html (12388 bytes)
extracting cisco.x509 (529 bytes)
extracting identitydb.obj (2523 bytes)
Switch#
Switch# dir

Directory of bootflash:/
    1  -rw-     9572396  Dec 30 2002 01:05:01 +00:00  cat4000-i9k2s-mz.121-19.EW
    2  -rw-     9604192   Jan 3 2003 07:46:49 +00:00  cat4000-i5k2s-mz.121-19.EW
    3  -rw-     1985024  Jan 21 2003 03:31:20 +00:00  Cat4000IOS.v4-0.tar
    4  -rw-        1173  Mar 19 2003 05:50:26 +00:00  post-2003.03.19.05.50.07-passed.txt
    5  -rw-     2031616  Mar 26 2003 05:33:12 +00:00  Cat4000IOS.v5-1.tar
    6  -rw-     1956591  Mar 26 2003 05:36:11 +00:00  cv/Cat4000IOS-5.1.sgz
    7  -rw-        7263  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_ace.html
    8  -rw-         410  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_error.html
    9  -rw-        2743  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_install.html
   10  -rw-       20450  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_jks.jar
   11  -rw-       20782  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_nos.jar
   12  -rw-       12388  Mar 26 2003 05:36:19 +00:00  cv/applet.html
   13  -rw-         529  Mar 26 2003 05:36:19 +00:00  cv/cisco.x509
   14  -rw-        2523  Mar 26 2003 05:36:19 +00:00  cv/identitydb.obj

32578556 bytes total (7358284 bytes free)

Switch#
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip http server
Switch(config)# snmp-server community public ro
Switch(config)# snmp-server community public rw
Switch(config)# exit
Switch# wr
Building configuration...
Compressed configuration from 2735 bytes to 1169 bytes[OK]
Switch# show ciscoview ?
  package  ADP Package Details
  version  ADP version
  |        Output modifiers
  <
```

スイッチへの Web アクセスの詳細については、次の URL で『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Using the Cisco Web Browser」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_4t/cf_12_4t_book.html

組み込み CiscoView 情報の表示

組み込み CiscoView 情報を表示するには、次のコマンドを入力します。

コマンド	目的
Switch# **show ciscoview package**	組み込み CiscoView ファイルに関する情報を表示します。
Switch# **show ciscoview version**	組み込み CiscoView のバージョンを表示します。

次に、組み込み CiscoView ファイルおよびバージョン情報を表示する例を示します。

```
Switch# show ciscoview package
File source:
CVFILE                          SIZE(in bytes)
-------------------------------------------------
Cat4000IOS-5.1.sgz               1956591
Cat4000IOS-5.1_ace.html          7263
Cat4000IOS-5.1_error.html        410
Cat4000IOS-5.1_install.html      2743
Cat4000IOS-5.1_jks.jar           20450
Cat4000IOS-5.1_nos.jar           20782
applet.html                      12388
cisco.x509                       529
identitydb.obj                   2523

Switch# show ciscoview version
Engine Version: 5.3.4 ADP Device: Cat4000IOS ADP Version: 5.1 ADK: 49
Switch#
```