



CHAPTER 7

スイッチの管理

この章では、Catalyst 3750 スイッチを管理するための 1 回限りの手順について説明します。特に明記しない限り、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

この章で説明する内容は、次のとおりです。

- 「システム日時の管理」(P.7-1)
- 「システム名とプロンプトの設定」(P.7-7)
- 「バナーの作成」(P.7-10)
- 「MAC アドレス テーブルの管理」(P.7-12)
- 「ARP テーブルの管理」(P.7-24)

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.com で入手可能な『Cisco IOS Configuration Fundamentals Command Reference, Release』を参照してください。

ここでは、次の設定情報について説明します。

- 「システム クロックの概要」(P.7-1)
- 「ネットワーク タイム プロトコルの概要」(P.7-2)
- 「NTP バージョン 4」(P.7-3)
- 「手動での日時の設定」(P.7-4)

システム クロックの概要

時刻サービスの中核となるのはシステム クロックです。このクロックはシステムがスタートアップした瞬間から稼動し、日時を常時トラッキングします。

システム クロックは、次のソースにより設定できます。

- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供します。

- ユーザの **show** コマンド
- ログおよびデバッグ メッセージ

システム クロックは、**Universal Time Coordinated (UTC; 協定世界時)** (別名 **GMT (グリニッジ標準時)**) に基づいてシステム内部の時刻を常時トラッキングします。ローカルのタイムゾーンおよび夏時間に関する情報を設定することにより、時刻がローカルのタイムゾーンに応じて正確に表示されるようになります。

システム クロックは、時刻に**信頼性**があるかどうか (つまり、信頼できると見なされるタイムソースによって時刻が設定されているか) を常時トラッキングします。信頼性のない場合は、時刻は表示目的でのみ使用され、再配信されません。設定手順については、「**手動での日時の設定**」(P.7-4) を参照してください。

ネットワーク タイム プロトコルの概要

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; ユーザ データグラム プロトコル)** で稼動し、UDP は IP 上で稼動します。NTP は RFC 1305 に規定されています。

NTP ネットワークは通常、ラジオクロックやタイムサーバに接続された原子時計など、信頼できるタイムソースからその時刻を取得します。その後、NTP はネットワークにこの時刻を配信します。NTP はきわめて効率的で、1 分間に 1 パケットを使用するだけで、2 台のデバイスを 1 ミリ秒以内に同期化できます。

NTP は、**ストラタム (階層)** という概念を使用して、信頼できる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 が稼動するデバイスは、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同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

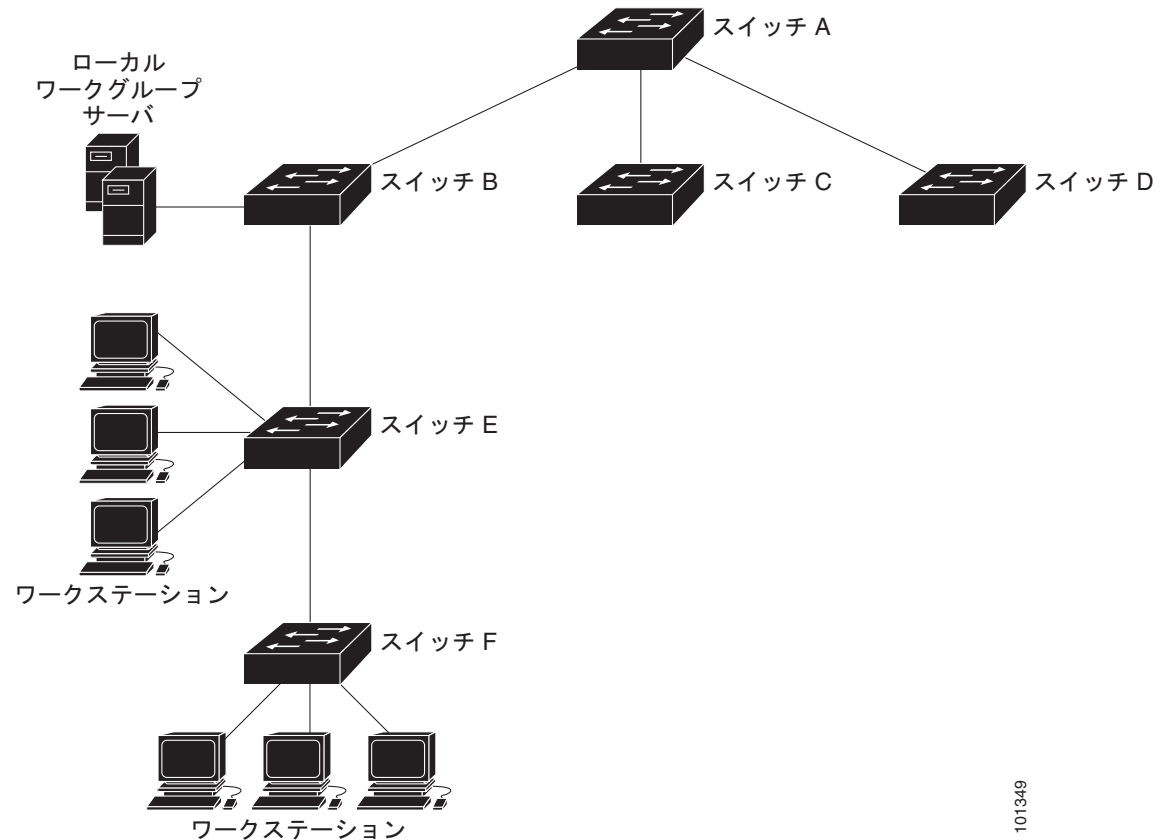
NTP が稼動するデバイス間の通信 (アソシエーション) は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャストメッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、この場合は、情報の流れは一方に限られます。

デバイス上で維持される時刻は、重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤ってあるいは意図的に設定されることを防止してください。アクセスリストを使用して制限する方式および暗号化認証メカニズムの、2 種類のメカニズムを使用できます。

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

図 7-1 に、NTP を使用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 7-1 一般的な NTP ネットワークの構成



101349

ネットワークがインターネットから切り離されている場合、シスコの NTP によって、実際には、他の方法で時刻を学習しているにもかかわらず、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。

複数のタイムソースがある場合は、NTP は常に、より信頼性があると見なされます。NTP の時刻は、他の方法による時刻に優先します。

自社のホストシステムに NTP ソフトウェアを組み込んでいるメーカーが数社あり、また、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホストシステムの時間も同期化されます。

NTP バージョン 4

NTP バージョン 4 は、スイッチに実装されています。NTPv4 は、NTP バージョン 3 の拡張です。NTPv4 は IPv4 および IPv6 をサポートし、NTPv3 と下位互換性があります。

NTPv4 は次の機能を提供します。

- IPv6 のサポート。

- NTPv3 と比較して向上したセキュリティ。NTPv4 プロトコルは、公開キー暗号化および標準の X509 証明書に基づくセキュリティ フレームワークを提供します。
- ネットワークに対する時刻配信の階層の自動計算。特定のマルチキャスト グループの使用によって、NTPv4 は、最低の帯域幅コストで最高の時刻精度を得るためのサーバの階層を自動的に設定します。この機能では、サイトローカル IPv6 マルチキャスト アドレスが活用されます。

NTPv4 の設定の詳細については、『[Cisco IOS IPv6 Configuration Guide, Release 12.4T](#)』の「[Implementing NTPv4 in IPv6](#)」の章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。



(注)

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

ここでは、次の設定情報について説明します。

- 「[システム クロックの設定](#)」(P.7-4)
- 「[日時設定の表示](#)」(P.7-5)
- 「[タイム ゾーンの設定](#)」(P.7-5)
- 「[夏時間の設定](#)」(P.7-6)

システム クロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合、手動でシステム クロックを設定する必要はありません。

システム クロックを設定するには、特権 EXEC モードで次の手順を実行します。

| コマンド | 目的 |
|--|--|
| ステップ1 <code>clock set hh:mm:ss day month year</code> または <code>clock set hh:mm:ss month day year</code> | 次のいずれかのフォーマットで、手動でシステム クロックを設定します。 <ul style="list-style-type: none"> • <code>hh:mm:ss</code> には、時刻を時間 (24 時間形式)、分、秒で指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • <code>day</code> には、当月の日付で日を指定します。 • <code>month</code> には、月を名前で指定します。 • <code>year</code> には、年を指定します (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 クロックがタイミグ ソースによって設定されている場合は、フラグを設定します。時刻が信頼性のないものである場合は、表示目的でのみ使用されます。クロックが信頼できず、*authoritative* フラグも設定されていなければ、ピアの時刻が無効でも、フラグはピアがクロックと同期しないようにします。

show clock の表示の前にある記号は、次の意味があります。

- * : 時刻は信頼できません。
- (空白) : 時刻は信頼できます。
- . : 時刻は信頼できますが、NTP は同期していません。

タイム ゾーンの設定

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

| | コマンド | 目的 |
|-------|---|--|
| ステップ1 | configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | clock timezone zone hours-offset [minutes-offset] | タイム ゾーンを設定します。 スイッチは内部時刻を UTC で管理するので、このコマンドは表示目的の場合および手動で時刻を設定した場合に限って使用します。 <ul style="list-style-type: none"> • <i>zone</i> には、標準時間が施行されているときに表示されるタイムゾーンの名前を入力します。デフォルトの設定は UTC です。 • <i>hours-offset</i> には、UTC からの時差を入力します。 • (任意) <i>minutes-offset</i> 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。 |
| ステップ4 | show running-config | 設定を確認します。 |
| ステップ5 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

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

時刻を UTC に設定するには、**no clock timezone** グローバル コンフィギュレーション コマンドを使用します。

夏時間の設定

毎年特定の曜日に夏時間が開始して終了する地域に夏時間を設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|--|---|
| ステップ1 | 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]] | 毎年指定した日に開始および終了するように夏時間を設定します。 夏時間はデフォルトでディセーブルに設定されています。パラメータなしで clock summer-time zone recurring を指定すると、夏時間ルールは米国のルールをデフォルトにします。 <ul style="list-style-type: none"> • <i>zone</i> には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • (任意) <i>week</i> には、月の何週めかを指定します（1～5、または last）。 • (任意) <i>day</i> には、曜日を指定します（Sunday、Monday など）。 • (任意) <i>month</i> には、月を指定します（January、February など）。 • (任意) <i>hh:mm</i> には、時刻を時間（24 時間形式）と分で指定します。 • (任意) <i>offset</i> には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。 |
| ステップ3 | end | 特権 EXEC モードに戻ります。 |
| ステップ4 | show running-config | 設定を確認します。 |
| ステップ5 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

次に、夏時間が 4 月の第 1 日曜の 2 時に始まり、10 月の最終日曜の 2 時に終わるように指定する例を示します。

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

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

| | コマンド | 目的 |
|-------|---|---|
| ステップ1 | 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]] または 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"> • zone には、夏時間が施行されているときに表示されるタイムゾーンの名前（たとえば PDT）を入力します。 • （任意）week には、月の何週めかを指定します（1 ~ 5、または last）。 • （任意）day には、曜日を指定します（Sunday、Monday など）。 • （任意）month には、月を指定します（January、February など）。 • （任意）hh:mm には、時刻を時間（24 時間形式）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。デフォルト値は 60 です。 |
| ステップ3 | end | 特権 EXEC モードに戻ります。 |
| ステップ4 | show running-config | 設定を確認します。 |
| ステップ5 | copy running-config startup-config | （任意）コンフィギュレーションファイルに設定を保存します。 |

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイムゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

夏時間をディセーブルにするには、**no clock summer-time** グローバル コンフィギュレーション コマンドを使用します。

次に、夏時間が 2000 年 10 月 12 日の 2 時に始まり、2001 年 4 月 26 日の 2 時に終わるように設定する例を示します。

```
Switch(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

システム名とプロンプトの設定

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。

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

ここで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』および『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』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.7-8)
- 「システム名の設定」(P.7-8)
- 「DNS の概要」(P.7-8)

デフォルトのシステム名およびプロンプトの設定

デフォルトのスイッチのシステム名およびプロンプトは *Switch* です。

システム名の設定

手動でシステム名を設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|---|--|
| ステップ1 | configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | hostname name | 手動でシステム名を設定します。 デフォルト設定は <i>switch</i> です。 名前は ARPANET ホスト名のルールに従う必要があります。このルールではホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、またはハイフンしか使用できません。名前には 63 文字まで使用できます。 |
| ステップ3 | end | 特権 EXEC モードに戻ります。 |
| ステップ4 | show running-config | 設定を確認します。 |
| ステップ5 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

システム名を設定すると、システム プロンプトとしても使用されます。

デフォルトのホスト名に戻すには、**no hostname** グローバル コンフィギュレーション コマンドを使用します。

DNS の概要

Domain Name System (DNS; ドメイン ネーム システム) プロトコルは、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* となります。このドメイン内の特定のデバイス、たとえば File Transfer Protocol (FTP; ファイル転送プロトコル) システムは、*ftp.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、次の設定情報について説明します。

- 「DNS のデフォルト設定」 (P.7-9)
- 「DNS の設定」 (P.7-9)
- 「DNS の設定の表示」 (P.7-10)

DNS のデフォルト設定

表 7-1 に、DNS のデフォルト設定を示します。

表 7-1 DNS のデフォルト設定

| 機能 | デフォルト設定 |
|-----------------|------------------|
| DNS イネーブル ステート | イネーブル |
| DNS デフォルト ドメイン名 | 未設定 |
| DNS サーバ | ネーム サーバのアドレスが未設定 |

DNS の設定

DNS を使用するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|---|--|
| ステップ1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | <code>ip domain-name name</code> | 未修飾のホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 起動時にはドメイン名は設定されていませんが、BOOTP または Dynamic Host Configuration Protocol (DHCP) サーバからスイッチ コンフィギュレーションを取得している場合は、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（サーバにこの情報が設定されている場合）。 |
| ステップ3 | <code>ip name-server server-address1 [server-address2 ... server-address6]</code> | 1 つまたは複数のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。 最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。スイッチは、最初にプライマリ サーバに DNS クエリーを送信します。そのクエリーが失敗した場合は、バックアップ サーバにクエリーが送信されます。 |

| | コマンド | 目的 |
|-------|---|--|
| ステップ4 | <code>ip domain-lookup</code> | (任意) スイッチ上で、DNS ベースのホスト名のアドレスへの変換をイネーブルにします。この機能は、デフォルトでイネーブルに設定されています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式 (DNS) を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。 |
| ステップ5 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ6 | <code>show running-config</code> | 設定を確認します。 |
| ステップ7 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

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

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

DNS 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 バナーの後に、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.com で入手可能な『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*』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.7-11)
- 「Message-of-The-Day ログイン バナーの設定」(P.7-11)
- 「ログイン バナーの設定」(P.7-12)

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。

Message-of-The-Day ログイン バナーの設定

ユーザがスイッチにログインしたときに、画面に表示される 1 行または複数行のメッセージバナーを作成できます。

MoTD ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|---|---|
| ステップ1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | <code>banner motd c message c</code> | MoTD バナーを指定します。 <i>c</i> には、任意の区切り文字、たとえばポンド記号 (#) を入力して、Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 <i>message</i> には、255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。 |
| ステップ3 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ4 | <code>show running-config</code> | 設定を確認します。 |
| ステップ5 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

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 '^]'.

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

User Access Verification

Password:
```

ログイン バナーの設定

接続されたすべての端末でログイン バナーが表示されるように設定できます。バナーが表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|---|--|
| ステップ1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | <code>banner login c message c</code> | ログイン メッセージを指定します。 <i>c</i> には、任意の区切り文字、たとえばポンド記号 (#) を入力して、Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 <i>message</i> には、255 文字までのログイン メッセージを入力します。メッセージ内には区切り文字を使用できません。 |
| ステップ3 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ4 | <code>show running-config</code> | 設定を確認します。 |
| ステップ5 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

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

次に、ドル記号 (\$) を開始および終了の区切り文字として使用し、スイッチのログイン バナーを設定する例を示します。

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

MAC アドレス テーブルの管理

MAC アドレス テーブルには、スイッチがポート間のトラフィック転送に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- ダイナミック アドレス：スイッチが学習し、使用されなくなった時点で期限切れとなる送信元 MAC アドレス
- スタティック アドレス：手動で入力され、期限切れにならず、スイッチのリセット時にも消去されないユニキャスト 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、次の設定情報について説明します。

- 「アドレス テーブルの作成」 (P.7-13)
- 「MAC アドレスおよび VLAN」 (P.7-13)
- 「MAC アドレスおよびスイッチ スタック」 (P.7-14)
- 「MAC アドレス テーブルのデフォルト設定」 (P.7-14)
- 「アドレス エージング タイムの変更」 (P.7-14)
- 「ダイナミック アドレス エントリの削除」 (P.7-15)
- 「MAC アドレス変更通知トラップの設定」 (P.7-15)
- 「MAC アドレス移行通知トラップの設定」 (P.7-17)
- 「MAC しきい値通知トラップの設定」 (P.7-19)
- 「スタティック アドレス エントリの追加および削除」 (P.7-20)
- 「ユニキャスト MAC アドレス フィルタリングの設定」 (P.7-21)
- 「VLAN での MAC アドレス ラーニングのディセーブル化」 (P.7-22)
- 「アドレス テーブル エントリの表示」 (P.7-24)

アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスによって、スイッチの任意のポートを各ワークステーション、リピータ、スイッチ、ルータ、あるいはその他のネットワークデバイスに接続できます。各ポートで受信するパケットの送信元アドレスを取得し、アドレス テーブルにアドレスとその対応するポート番号を追加することによって、スイッチは動的なアドレス指定を行います。ネットワークでステーションの増設または取り外しが行われると、スイッチはアドレス テーブルを更新し、新しいダイナミック アドレスを追加し、使用されていないアドレスは期限切れにします。

有効期間は、スタンドアロン スイッチまたはスイッチ スタックにグローバルに設定されます。ただし、スイッチは VLAN ごとにアドレス テーブルを維持し、STP によって VLAN 単位で有効期間を短縮できます。

スイッチは、受信したパケットの宛先アドレスに基づいて、任意の組み合わせのポート間でパケットを送信します。MAC アドレス テーブルを使用することによって、スイッチは、宛先アドレスに対応付けられたポート（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。

プライベート VLAN が設定されている場合、アドレス学習は次のように MAC アドレスのタイプに左右されます。

- プライベート LAN 上にある 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連 VLAN に複製されます。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。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 の詳細については、第 16 章「プライベート VLAN の設定」を参照してください。

MAC アドレスおよびスイッチ スタック

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

MAC アドレス テーブルのデフォルト設定

表 7-2 に、MAC アドレス テーブルのデフォルト設定を示します。

表 7-2 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。その場合、宛先が不明のペケットをスイッチが受信すると、受信ポートと同じ VLAN 内のすべてのポートに、そのペケットをフラッドさせます。この不必要なフラッドによって、パフォーマンスに悪影響を及ぼす可能性があります。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。この結果フラッドとなり、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、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|---|--|
| ステップ1 | configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | mac address-table 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。 指定できる範囲は 10 ~ 1000000 秒です。デフォルト値は 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。 <i>vlan-id</i> 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 | 設定を確認します。 |
| ステップ5 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

デフォルト値に戻すには、**no mac address-table aging-time** グローバル コンフィギュレーション コマンドを使用します。

ダイナミック アドレス エントリの削除

ダイナミック エントリをすべて削除するには、特権 EXEC モードで **clear mac address-table dynamic** コマンドを使用します。特定の MAC アドレス (**clear mac address-table dynamic address mac-address**)、指定された物理ポートまたはポートチャネル上のすべてのアドレス (**clear mac address-table dynamic interface interface-id**)、または指定された VLAN 上のすべてのアドレス (**clear mac address-table dynamic vlan vlan-id**) の削除もできます。

ダイナミック エントリが削除されたことを確認するには、**show mac address-table dynamic** 特権 EXEC コマンドを使用します。

MAC アドレス変更通知トラップの設定

ネットワークの MAC アドレス変更通知は、MAC アドレス変更アクティビティを保存することで、ネットワーク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きに、SNMP 通知トラップを NMS に送信させることができます。ネットワークから多数のユーザの出入りがある場合は、トラップ インターバル タイムを設定して通知トラップを組み込み、ネットワーク トラフィックを削減できます。MAC 通知履歴テーブルは、トラップが設定されたポートごとの MAC アドレス アクティビティを保存します。MAC アドレス変更通知は、ダイナミック MAC アドレスまたはセキュア MAC アドレスについて生成されます。自身のアドレス、マルチキャスト アドレス、または他のスタティック アドレスについては、通知は生成されません。

NMS ホストに MAC アドレス変更通知トラップを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|--|--|
| ステップ1 | configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | snmp-server host <i>host-addr</i> { traps informs } { version { 1 2c 3 }} <i>community-string notification-type</i> | <p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <i>host-addr</i> には、NMS の名前または IP アドレスを指定します。 SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 情報をホストに送信するには、informs を指定します。 サポートする SNMP バージョンを指定します。informs にはバージョン 1 (デフォルト) を使用できません。 <i>community-string</i> には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。 <i>notification-type</i> には、mac-notification キーワードを使用します。 |
| ステップ3 | snmp-server enable traps mac-notification change | スイッチが MAC アドレス変更通知トラップを NMS に送信できるようにします。 |
| ステップ4 | mac address-table notification 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 [<i>interval value</i>] [<i>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"> (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。 (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 です。デフォルトは 1 です。 |
| ステップ6 | interface <i>interface-id</i> | インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。 |

| | コマンド | 目的 |
|--------|---|--|
| ステップ7 | <code>snmp trap mac-notification change {added removed}</code> | インターフェイスの MAC アドレス変更通知トラップをイネーブルにします。 <ul style="list-style-type: none"> このインターフェイスに MAC アドレスが追加されると、トラップをイネーブルにします。 このインターフェイスから MAC アドレスが削除されると、トラップをイネーブルにします。 |
| ステップ8 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ9 | <code>show mac address-table notification change interface</code> <code>show running-config</code> | 設定を確認します。 |
| ステップ10 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

MAC アドレス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。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 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。MAC アドレス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。

次に、NMS として 172.20.10.10 を指定し、スイッチによる NMS への MAC アドレス通知トラップの送信をイネーブルにし、MAC アドレス変更通知機能をイネーブルにし、インターバルを 123 秒、履歴サイズを 100 エントリに設定し、特定のポートで MAC アドレスが追加された場合のトラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private 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 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# snmp trap mac-notification change added
```

設定を確認するには、**show mac address-table notification change interface** および **show mac address-table notification change** 特権 EXEC コマンドを入力します。

MAC アドレス移行通知トラップの設定

MAC 移行通知を設定すると、同一の VLAN 内であるポートから別のポートへ MAC アドレスが移行したときに 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。

NMS ホストに MAC アドレス移行通知トラップを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|--|--|
| ステップ1 | configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | snmp-server host <i>host-addr</i> { traps informs } { version { 1 2c 3 }} <i>community-string notification-type</i> | トラップ メッセージの受信側を指定します。 <ul style="list-style-type: none"> • <i>host-addr</i> には、NMS の名前または IP アドレスを指定します。 • SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 情報をホストに送信するには、informs を指定します。 • サポートする SNMP バージョンを指定します。informs にはバージョン 1 (デフォルト) を使用できません。 • <i>community-string</i> には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できませんが、このストリングを定義するには、snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。 • <i>notification-type</i> には、mac-notification キーワードを使用します。 |
| ステップ3 | snmp-server enable traps mac-notification move | スイッチが MAC アドレス移行通知トラップを NMS に送信できるようにします。 |
| ステップ4 | mac address-table notification mac-move | MAC アドレス移行通知機能をイネーブルにします。 |
| ステップ5 | end | 特権 EXEC モードに戻ります。 |
| ステップ6 | show mac address-table notification mac-move show running-config | 設定を確認します。 |
| ステップ7 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

MAC アドレス移行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。MAC アドレス移行通知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 アドレス移行通知トラップの送信をイネーブルにし、MAC アドレス移行通知機能をイネーブルにし、あるポートから別のポートへ MAC アドレスが移行された場合のトラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification move
Switch(config)# mac address-table notification mac-move
```

設定を確認するには、**show mac address-table notification mac-move** 特権 EXEC コマンドを入力します。

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 アドレス テーブルしきい値制限に達したか、またはそれを越えたときに、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。

NMS ホストに MAC アドレステーブルしきい値通知トラップを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|---|---|
| ステップ1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | <code>snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code> | <p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 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。 <code>community-string</code> 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せんが、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。 <code>notification-type</code> には、mac-notification キーワードを使用します。 |
| ステップ3 | <code>snmp-server enable traps mac-notification threshold</code> | スイッチが MAC しきい値通知トラップを NMS に送信できるようにします。 |
| ステップ4 | <code>mac address-table notification threshold</code> | MAC アドレスしきい値通知機能をイネーブルにします。 |
| ステップ5 | <code>mac address-table notification threshold [limit percentage] [interval time]</code> | <p>MAC アドレスしきい値使用状況モニタリングのしきい値を入力します。</p> <ul style="list-style-type: none"> (任意) <code>limit percentage</code> には、MAC アドレス テーブル使用の割合を指定します。有効な値は 1 ~ 100% です。デフォルト値は 50% です。 (任意) <code>interval time</code> には、通知の間隔の時間を指定します。有効な値は 120 秒以上です。デフォルトは 120 秒です。 |
| ステップ6 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ7 | <code>show mac address-table notification threshold</code> <code>show running-config</code> | 設定を確認します。 |
| ステップ8 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

MAC アドレス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。MAC アドレスしきい値通知機能をディセーブルにするには、**no mac 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。

次に、NMS として 172.20.10.10 を指定し、MAC アドレスしきい値通知機能をイネーブルにし、インターバルを 123 秒に設定し、限界を 78% に設定する例を示します。

```
Switch(config)# snmp-server host 172.20.10.10 traps 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
```

設定を確認するには、**show mac address-table notification threshold** 特権 EXEC コマンドを入力します。

スタティック アドレス エントリの追加および削除

スタティック アドレスには、次の特性があります。

- アドレス テーブルへの追加およびアドレス テーブルからの削除は、手動で行う必要があります。
- ユニキャストまたはマルチキャスト アドレスとして設定できます。
- 期限切れになることはなく、スイッチが再起動しても維持されます。

スタティック アドレスを追加および削除でき、また、スタティック アドレスの転送動作を定義できます。転送動作は、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 と対応しているため、スイッチは指定されたポートから、アドレスに対応する VLAN ID を取得します。送信元ポートごとに、宛先ポートのリストを別々に指定できます。

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

スタティック アドレスを追加するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|--|---|
| ステップ1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ2 | <code>mac address-table static mac-addr vlan vlan-id interface interface-id</code> | <p>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。</p> <ul style="list-style-type: none"> <code>mac-addr</code> には、アドレス テーブルに追加する宛先 MAC ユニキャスト アドレスを指定します。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。 <code>vlan-id</code> には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。有効な VLAN ID は 1 ~ 4094 です。 <code>interface-id</code> には、受信したパケットの転送先インターフェイスを指定します。有効なインターフェイスには、物理ポートまたはポートチャネルがあります。スタティック マルチキャスト アドレスの場合、複数のインターフェイス ID を入力できます。スタティック ユニキャスト アドレスの場合、インターフェイスは同時に 1 つしか入力できません。ただし、同じ MAC アドレスおよび VLAN ID を指定すると、コマンドを複数回入力できます。 |
| ステップ3 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ4 | <code>show mac address-table static</code> | 設定を確認します。 |
| ステップ5 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

アドレス テーブルからスタティック エントリを削除するには、`no mac address-table static mac-addr vlan vlan-id [interface interface-id]` グローバル コンフィギュレーション コマンドを使用します。

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

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

ユニキャスト MAC アドレス フィルタリングの設定

ユニキャスト MAC アドレス フィルタリングがイネーブルの場合、スイッチは、特定の送信元 MAC アドレスまたは宛先 MAC アドレスを持つパケットをドロップします。この機能はデフォルトではディセーブルで、ユニキャスト スタティック アドレスだけをサポートしています。

この機能を使用する場合は、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされていません。`mac address-table static mac-addr vlan vlan-id drop` グローバル コンフィギュレーション コマンドを入力するときに、これらのアドレスのいずれかを指定すると、次のいずれかのメッセージが表示されます。

```
% Only unicast addresses can be configured to be dropped
```

```
% CPU destined address cannot be configured as drop address
```

- CPU に転送されるパケットもサポートされていません。

- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定すると、最後に入力したコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、MAC アドレスを持つパケットをドロップします。2 番めに入力したコマンドは、1 番目のコマンドより優先されます。

たとえば、**mac address-table static mac-addr vlan vlan-id interface interface-id** グローバル コンフィギュレーション コマンドに続けて、**mac address-table static mac-addr vlan vlan-id drop** コマンドを入力すると、スイッチは、送信元または宛先として MAC アドレスを持つパケットをドロップします。

mac address-table static mac-addr vlan vlan-id drop グローバル コンフィギュレーション コマンドに続けて、**mac address-table static mac-addr vlan vlan-id interface interface-id** コマンドを入力すると、スイッチは、スタティック アドレスとして MAC アドレスを追加します。

ユニキャスト MAC アドレス フィルタリングをイネーブルにして、スイッチが特定のアドレスを持つパケットをドロップするように設定するには、送信元または宛先ユニキャスト MAC アドレスおよび受信側の VLAN を指定します。

スイッチが送信元または宛先ユニキャスト スタティック アドレスを廃棄するよう設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|--|--|
| ステップ 1 | configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | mac address-table static mac-addr vlan vlan-id drop | ユニキャスト MAC アドレス フィルタリングをイネーブルにし、スイッチが指定した送信元または宛先ユニキャスト スタティック アドレスを持つパケットをドロップするように設定します。 <ul style="list-style-type: none"> <i>mac-addr</i> には、送信元または宛先ユニキャスト MAC アドレスを指定します。この MAC アドレスを持つパケットはドロップされます。 <i>vlan-id</i> には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。有効な VLAN ID は 1 ~ 4094 です。 |
| ステップ 3 | end | 特権 EXEC モードに戻ります。 |
| ステップ 4 | show mac address-table static | 設定を確認します。 |
| ステップ 5 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

ユニキャスト MAC アドレス フィルタリングをディセーブルにするには、**no mac address-table static mac-addr vlan vlan-id** グローバル コンフィギュレーション コマンドを使用します。

次にユニキャスト MAC アドレス フィルタリングをイネーブルにし、送信元または宛先アドレスが c2f3.220a.12f4 であるパケットをスイッチがドロップするように設定する例を示します。この MAC アドレスを送信元または宛先アドレスとしたパケットを VLAN 4 で受信すると、パケットはドロップされます。

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

VLAN での MAC アドレス ラーニングのディセーブル化

デフォルトでは、MAC アドレス ラーニングがスイッチのすべての VLAN でイネーブルです。VLAN 上の MAC アドレス ラーニングを制御して、どの VLAN (つまり、ポート) で MAC アドレス ラーニングが可能であるかを指定することにより、使用可能な MAC アドレス テーブル スペースを管理できます。MAC アドレス ラーニングをディセーブルにする前に必ず、ネットワーク トポロジとスイッチ システム設定をよく理解しておいてください。VLAN で MAC アドレス ラーニングをディセーブルにすると、ネットワーク上でフラッドを引き起こす可能性があります。

VLAN で MAC アドレス ラーニングをディセーブルにするときは、次の注意事項に従ってください。

- Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) が設定された VLAN で MAC アドレス ラーニングをディセーブルにするときは、注意が必要です。スイッチはレイヤ 2 ドメインのすべての IP パケットをフラッドします。
- MAC アドレス学習は、1 つの VLAN ID (例: **no mac address-table learning vlan 223**) または一連の VLAN ID (例: **no mac address-table learning vlan 1-20, 15**) でディセーブルにすることができます。
- MAC アドレス ラーニングは、2 つのポートを備えた VLAN でのみディセーブルにすることを推奨します。3 つ以上のポートを備えた VLAN で MAC アドレス ラーニングをディセーブルにすると、スイッチが受信するすべてのパケットが VLAN ドメインでフラッディングされます。
- スイッチにより内部的に使用される VLAN では、MAC アドレス ラーニングをディセーブルにすることはできません。入力した VLAN ID が内部 VLAN である場合は、スイッチがエラーメッセージを生成し、そのコマンドを拒否します。使用中の内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを入力します。
- プライベート VLAN、プライマリ VLAN として設定された VLAN で MAC アドレス ラーニングをディセーブルにしても、MAC アドレスは、プライマリ VLAN に属しており、プライマリ VLAN に複製されたセカンダリ VLAN で学習されます。プライベート VLAN のプライマリ VLAN ではないセカンダリ VLAN で MAC アドレス ラーニングをディセーブルにすると、MAC アドレス ラーニングは、プライマリ VLAN 上で発生する VLAN で実行され、セカンダリ VLAN に複製されます。
- RSPAN VLAN で MAC アドレス ラーニングをディセーブルにすることはできません。その設定は許可されていません。
- セキュア ポートを含む VLAN での MAC アドレス ラーニングをディセーブルにしても、そのポートでは MAC アドレス ラーニングはディセーブルになりません。ポート セキュリティをディセーブルにした場合、設定済みの MAC アドレス ラーニング ステータスはイネーブルです。

VLAN で MAC アドレス ラーニングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 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 | no mac address-table learning vlan vlan-id | 特定の VLAN で MAC アドレス ラーニングをディセーブルにします。単一の VLAN ID または VLAN ID 範囲を、ハイフンまたはカンマで区切って指定できます。有効な VLAN ID は 1 ~ 4094 です。 |
| ステップ 3 | end | 特権 EXEC モードに戻ります。 |
| ステップ 4 | show mac address-table learning [vlan vlan-id] | 設定を確認します。 |
| ステップ 5 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

VLAN で MAC アドレス ラーニングを再度イネーブルにするには、**default mac address-table learning vlan vlan-id** グローバル コンフィギュレーション コマンドを使用します。また、**mac address-table learning vlan vlan-id** グローバル コンフィギュレーション コマンドを使用して、VLAN で MAC アドレス ラーニングを再度イネーブルにすることもできます。前者の (**default**) コマンドを使用すると、デフォルトの状態に戻るようになるため、設定は **show running-config** コマンドによる出力には含まれません。後者のコマンドを使用すると、設定が **show running-config** 特権 EXEC コマンドの表示に含まれます。

次に、VLAN 200 で MAC アドレス ラーニングをディセーブルにする方法の例を示します。

```
Switch(config)# no mac address-table learning vlan 200
```

show mac-address-table learning [vlan vlan-id] 特権 EXEC コマンドを入力すると、すべての VLAN または特定の VLAN の MAC アドレス ラーニングのステータスを表示することができます。

アドレス テーブル エントリの表示

表 7-3 に示す 1 つまたは複数の特権 EXEC コマンドを使用すると、MAC アドレス テーブルを表示できます。

表 7-3 MAC アドレス テーブル表示用のコマンド

| コマンド | 説明 |
|-------------------------------------|---|
| show ip igmp snooping groups | すべての VLAN または指定された VLAN に対するレイヤ 2 マルチキャスト エントリを表示します。 |
| show mac address-table address | 指定された MAC アドレスに対する MAC アドレス テーブル情報を表示します。 |
| show mac address-table aging-time | すべての VLAN または指定された VLAN のエージング タイムを表示します。 |
| show mac address-table count | すべての VLAN または指定された VLAN に存在するアドレスの数を表示します。 |
| show mac address-table dynamic | ダイナミック MAC アドレス テーブル エントリのみを表示します。 |
| show mac address-table interface | 指定されたインターフェイスに対する MAC アドレス テーブル情報を表示します。 |
| show mac address-table learning | すべての VLAN または特定の VLAN での MAC アドレス ラーニングのステータスを表示します。 |
| show mac address-table 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 エントリのみを表示します。 |
| show mac address-table vlan | 指定された VLAN に対する MAC アドレス テーブル情報を表示します。 |

ARP テーブルの管理

デバイスと通信するには（イーサネット上のデバイスなど）、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。

Address Resolution Protocol (ARP; アドレス解決プロトコル) は、ホスト IP アドレスを、該当するメディアまたは MAC アドレスおよび VLAN ID に対応付けます。IP アドレスを使用して、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、IP と MAC アドレスとの対応を ARP キャッシュに格納し、すばやく検索できるようにします。その後、IP データグラムがリンク レイヤ フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化および ARP 要求/応答については、Subnetwork Access Protocol (SNAP) 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。



(注) CLI の手順については、Cisco.com で入手可能な Cisco IOS Release 12.4 のマニュアルを参照してください。