



## デバイスの管理

---

- [デバイスの管理に関する情報](#) (1 ページ)
- [デバイスの管理方法](#) (9 ページ)
- [デバイス管理の設定例](#) (32 ページ)
- [デバイス管理に関する追加情報](#) (34 ページ)
- [デバイス管理の機能履歴](#) (34 ページ)

## デバイスの管理に関する情報

### システム日時の管理

デバイスのシステム日時は、自動設定方式 (RTC および NTP) または手動設定方式を使用して管理できます。



---

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

---

### システム クロック

時刻サービスの基本となるのはシステム クロックです。このクロックはシステムがスタートアップした瞬間から稼働し、日時を常時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。

- RTC
- 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。

- `user 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、グリニッジ標準時 (GMT) とも呼ばれる協定世界時 (UTC) に基づいて内部的に時刻を追跡します。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。

## ネットワーク タイム プロトコル

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 はユーザ データグラム プロトコル (UDP) で稼働し、UDP は IP 上で稼働します。NTP は RFC 1305 で規定されています。

NTP ネットワークは通常、タイム サーバに接続されたラジオクロックやアトミッククロックなど、正規の時刻源から時刻を取得します。NTP は、ネットワークにこの時刻を分配します。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 では、信頼できるタイムソースから各マシンが何 NTP ホップ隔たっているかを表すために、ストラタムという概念が使用されます。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同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

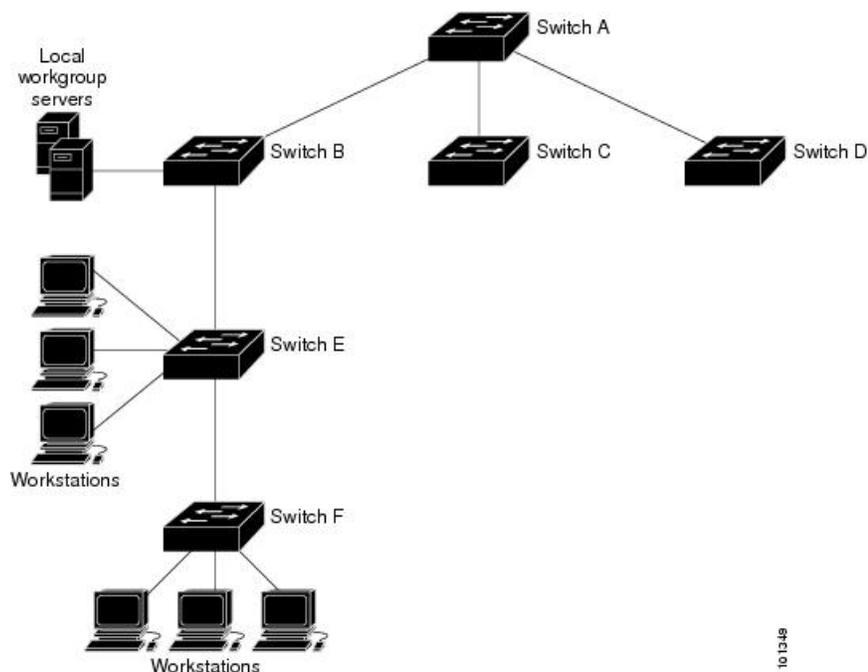
NTP が稼働するデバイス間の通信 (アソシエーション) は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャストメッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

デバイス上で維持される時刻は、重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤って、あるいは意図的に設定されることがないようにしてください。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

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。

次の図に NTP を使用した一般的なネットワークの例を示します。A はプライマリ NTP、デバイス B、C、D が NTP サーバモードに設定されている（デバイス A との間にサーバアソシエーションが設定されている）場合の NTP マスターです。デバイス E は、アップストリームデバイス（デバイス B）とダウンストリームデバイス（デバイス F）の NTP ピアとして設定されます。

図 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、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホストシステムも時間が同期化されます。

## NTP ストラタム

NTP では、信頼できるタイム ソースから各マシンが何 NTP ホップ隔たっているかを表すために、ストラタムという概念が使用されます。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

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 アソシエーション

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、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

## NTP セキュリティ

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ないようにしてください。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

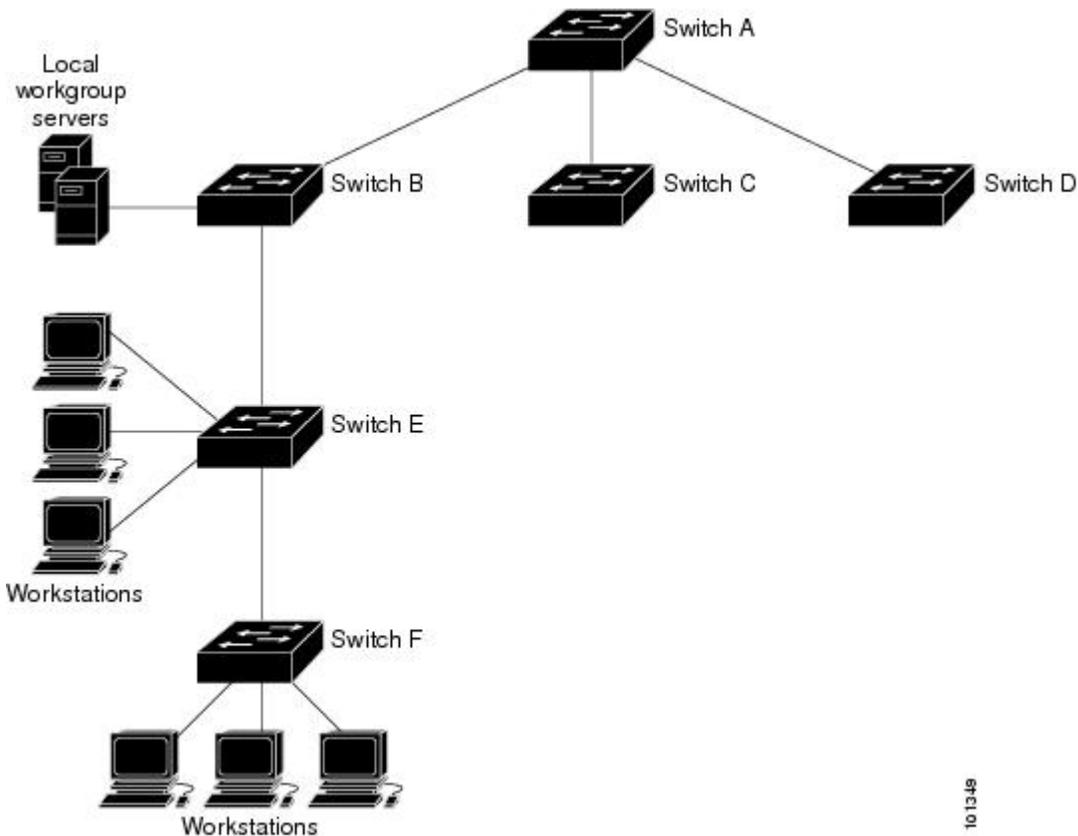
## NTP の実装

NTP の実装では、ストラタム 1 サービスがサポートされないため、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 2: 一般的な NTP ネットワークの構成

次の図は NTP を使用した一般的なネットワークの例を示します。スイッチ A は、スイッチ B、C、D が NTP サーバモードに設定されている（スイッチ A との間にサーバアソシエーションが設定されている）場合のプライマリ NTP です。スイッチ E は、アップストリームスイッチ（ス

スイッチ B) と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ます。



ネットワークがインターネットから切り離されている場合、NTPによって、実際には、他の方法で時刻を取得している場合でも、NTPを使用した同期化と同様にデバイスの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、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホストシステムも時間が同期化されます。

## システム名およびシステム プロンプト

デバイスを識別するシステム名を設定します。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 文字がシステムプロンプトとして使用されます。大なり記号 (>) が付加されます。システム名が変更されると、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 12.4』および『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4』を参照してください。

## スタックのシステム名およびシステム プロンプト

アクティブスイッチを介してスタックメンバにアクセスする場合は、**session stack-member-number** 特権 EXEC コマンドを使用する必要があります。スタックメンバ番号の有効範囲は1～8です。このコマンドを使用すると、スタックメンバの番号がシステムプロンプトの末尾に追加されます。たとえば、Switch-2#はスタックメンバ2の特権EXECモードのプロンプトであり、スイッチスタックのシステムプロンプトはSwitchです。

## デフォルトのシステム名とプロンプトの設定

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。

## DNS

DNS プロトコルは、ドメインネームシステム (DNS) を制御します。DNS とは分散型データベースであり、ホスト名を IP アドレスにマッピングできます。デバイスに DNS を設定すると、**ping**、**telnet**、**connect** などのすべての IP コマンドを使用する場合や、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、たとえばファイル転送プロトコル (FTP) 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。

## DNS のデフォルト設定値

表 1: DNS のデフォルト設定値

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

## ログインバナー

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、接続されたすべての端末に表示されます。すべてのネットワークユーザに影響するメッセージ（差し迫ったシステム シャットダウンの通知など）を送信する場合に便利です。

ログインバナーも接続されたすべての端末に表示されます。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 12.4*』を参照してください。

## 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。

## MAC アドレス テーブル

MAC アドレステーブルには、デバイス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：デバイスが取得し、使用されなくなった時点で期限切れとなる送信元の 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、デバイス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 (仮想 LAN) 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。

## MAC 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 アドレスを使用して、他のネットワークデバイスにデバイス上のすべてのポートを接続できます。デバイスは、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れに関連付けられたポート番号を追加することによって、動的なアドレス指定を行います。ネットワークでデバイスの追加

たは削除が行われると、デバイスによってアドレステーブルが更新され、新しいダイナミックアドレスが追加され、使用されていないアドレスは期限切れになります。

エージング インターバルは、グローバルに設定されています。ただし、デバイスは 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。

デバイスは、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。デバイスは、MAC アドレステーブルを使用することによって、宛先アドレスに関連付けられたポート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。デバイスは、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転送します。

## MAC アドレスおよび VLAN

すべてのアドレスは VLAN と関連付けられます。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。

## MAC アドレスおよびデバイススタック

すべてのスタック メンバにある MAC アドレス テーブルでは、同期が取られます。いかなる時点でも、各スタック メンバには、各 VLAN のアドレス テーブルの同じコピーがあります。アドレスがエージングアウトすると、アドレスは、すべてのスタック メンバにあるアドレス テーブルから削除されます。デバイスがスイッチスタックに参加すると、そのデバイスでは、他のスタックメンバで学習された各 VLAN のアドレスを受信します。スタックメンバがスイッチスタックに残っているときには、残りのスタックメンバは、エージングアウトするか、前のスタックメンバによってラーニングされたすべてのアドレスが削除されます。

## MAC アドレス テーブルのデフォルト設定

次の表に、MAC アドレス テーブルのデフォルト設定を示します。

表 2: MAC アドレスのデフォルト設定

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

## 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、サブネットワークアクセスプロトコル（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）がデフォルトでイーサネット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（コマンドライン インターフェイス）の手順については、*Cisco.com* で Cisco IOS Release 12.4 のマニュアルを参照してください。

## デバイスの管理方法

### 手動による日付と時刻の設定

正確なシステム時刻は再開と再起動により保持されますが、日付と時刻はシステムが再開してから手動で設定できます。

手動設定は必要な場合にのみ使用することを推奨します。デバイスが同期できる外部ソースがある場合は、システムクロックを手動で設定する必要はありません。



---

（注） 手動でシステムクロックを設定している場合は、デバイスに障害が発生して別のスタックメンバがデバイスの役割を引き継ぐ前に、この設定を再設定する必要があります。

---

### 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、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> <li><b>clock set hh:mm:ss day month year</b></li> <li><b>clock set hh:mm:ss month day year</b></li> </ul> <p>例 :</p> <pre>Device# clock set 13:32:00 23 March 2013</pre>	<p>次のいずれかの書式を使ってシステムクロックを手動で設定します。</p> <ul style="list-style-type: none"> <li><b>hh:mm:ss</b> : 時間 (24 時間形式)、分、秒を指定します。指定された時刻は、設定されたタイムゾーンに基づきます。</li> <li><b>day</b> : 月の日で日付を指定します。</li> <li><b>month</b> : 月を名前で指定します。</li> <li><b>year</b> : 年を指定します (略式表記で指定しないでください)。</li> </ul>

## タイムゾーンの設定

タイムゾーンを手動で設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p><b>clock timezone zone hours-offset [minutes-offset]</b></p> <p>例 :</p>	<p>時間帯を設定します。</p> <p>内部時間は、協定世界時 (UTC) で維持されるため、このコマンドは表示専用</p>

	コマンドまたはアクション	目的
	<pre>Device(config)# clock timezone AST -3 30</pre>	<p>で、時刻を手動で設定するときだけに使用されます。</p> <ul style="list-style-type: none"> <li>• <i>zone</i> : 標準時が適用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。デフォルトは UTC です。</li> <li>• <i>hours-offset</i> : UTC からのオフセット時間数を入力します。</li> <li>• (任意) <i>minutes-offset</i> : UTC からのオフセット分数を入力します。ローカルタイムゾーンが UTC と 1 時間の差の割合である場合に指定できます。</li> </ul>
ステップ 4	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 5	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 6	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(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。

## 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。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p>	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> <b>enable</b>	<ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>clock summer-time zone date date month year hh:mm date month year hh:mm [offset]</b> 例： Device(config)# <b>clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00</b>	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。
ステップ 4	<b>clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]</b> 例： Device(config)# <b>clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00</b>	<p>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。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。</p> <p>終了時間は夏時間を基準にしています。夏時間はデフォルトでディセーブルに設定されています。パラメータなしで <b>clock summer-time zone recurring</b> を指定すると、夏時間のルールは米国のルールにデフォルト設定されます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <i>zone</i> : 夏時間が有効な場合に表示される時間帯名 (PDT など) を指定します。</li> <li>• (任意) <i>week</i> : 月の週 (1 ~ 4、<b>first</b>、または <b>last</b>) を指定します。</li> <li>• (任意) <i>day</i> : 曜日 (Sunday、Monday など) を指定します。</li> <li>• (任意) <i>month</i> : 月 (January、February など) を指定します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• (任意) <i>hh:mm</i> : 時および分単位で時間 (24時間形式) を指定します。</li> <li>• (任意) <i>offset</i> : 夏時間中に追加する分数を指定します。デフォルトは 60 です。</li> </ul>
ステップ 5	<b>end</b> 例 : Device (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例 : Device # <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例 : Device # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## システム名の設定

システム名を手動で設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device > <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : Device # <b>configure terminal</b>	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	<p><b>hostname name</b></p> <p>例 :</p> <pre>Device(config)# hostname remote-users</pre>	<p>システム名を設定します。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。</p> <p>デフォルト設定は Switch です。</p> <p>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。</p>
ステップ 4	<p><b>end</b></p> <p>例 :</p> <pre>remote-users(config)#end remote-users#</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 5	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	<p>入力を確認します。</p>
ステップ 6	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	<p>(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。</p>

## DNS の設定

デバイスの IP アドレスをホスト名として使用する場合、この IP アドレスが使用されるため、DNS クエリは発生しません。ピリオド (.) なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホスト名に追加され、その後で DNS クエリが行われ、名前を IP アドレスにマッピングします。デフォルトのドメイン名は、グローバル コンフィギュレーションモードで **ip domain name** 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 を使用するようにスイッチを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p><b>ip domain name name</b></p> <p>例 :</p> <pre>Device(config)# ip domain name Cisco.com</pre>	<p>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。</p> <p>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。</p> <p>ブート時にはドメイン名は設定されていませんが、デバイスの設定が BOOTP または Dynamic Host Configuration Protocol (DHCP) サーバから行われている場合、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（この情報がサーバに設定されている場合）。</p>
ステップ 4	<p><b>ip name-server server-address1 [server-address2 ... server-address6]</b></p> <p>例 :</p> <pre>Device(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300</pre>	<p>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。</p> <p>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。デバイスは、プライマリサーバへ DNS クエリを最初に送信します。そのクエリが失敗した場合は、バックアップサーバにクエリが送信されます。</p>

	コマンドまたはアクション	目的
ステップ 5	<b>ip domain lookup [nsap   source-interface interface]</b> 例： Device(config)# <b>ip domain-lookup</b>	(任意) デバイス上で、DNS に基づくホスト名から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。 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 6	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config</b> 例： Device# <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## Message-of-the-Day ログインバナーの設定

デバイスにログインしたときに画面に表示される 1 行以上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、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
	Device> <b>enable</b>	
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーションモードを開始します。
ステップ 3	<b>banner motd c message c</b> 例： Device(config)# <b>banner motd #</b> This is a secure site. Only authorized users are allowed. For access, contact technical support. #	MoTD を指定します。  <i>c</i> : ポンド記号 (#) など、目的のデリミタを入力して <b>Return</b> 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> : 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 4	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例： Device# <b>show running-config</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## 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、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p><b>banner login c message c</b></p> <p>例 :</p> <pre>Device(config)# banner login \$ Access for authorized users only. Please enter your username and password. \$</pre>	<p>ログイン メッセージを指定します。</p> <p><i>c</i> : ポンド記号 (#) など、目的のデリミタを入力して 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。</p> <p><i>message</i> : 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。</p>
ステップ 4	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 5	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	<p>入力を確認します。</p>
ステップ 6	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	<p>(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。</p>

# MAC アドレス テーブルの管理

## 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テーブルのエージングタイムを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>mac address-table aging-time [0   10-1000000] [routed-mac   vlan vlan-id]</b> 例： Device(config)# <b>mac address-table aging-time 500 vlan 2</b>	ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に保持される時間を設定します。  指定できる範囲は 10 ~ 1000000 秒です。デフォルトは 300 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 : 有効な ID は 1 ~ 4094 です。
ステップ 4	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例： Device# <b>show running-config</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例：	(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。

	コマンドまたはアクション	目的
	Device# <code>copy running-config startup-config</code>	

## MAC アドレス変更通知トラップの設定

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、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <code>enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>snmp-server host <i>host-addr</i> <i>community-string</i> <i>notification-type</i> { <i>informs</i>   <i>traps</i> } { <i>version</i> { <i>1</i>   <i>2c</i>   <i>3</i> } } { <i>vrf</i> <i>vrf instance name</i> }</b> 例： Device(config)# <code>snmp-server host 172.20.10.10 traps private mac-notification</code>	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"> <li><b>host-addr</b> : NMS の名前またはアドレスを指定します。</li> <li><b>traps</b> (デフォルト) : ホストに SNMP トラップを送信します。</li> <li><b>informs</b> : ホストに SNMP 情報を送信します。</li> <li><b>version</b> : サポートする SNMP バージョンを指定します。 <b>informs</b> にはバージョン 1 (デフォルト) を使用できません。</li> <li><b>community-string</b> : 通知処理で送信する文字列を指定します。  <b>snmp-server host</b> コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、<b>snmp-server community</b> グローバ</li> </ul>

	コマンドまたはアクション	目的
		<p>ル コンフィギュレーション コマンドを使用してから、<b>snmp-server host</b> コマンドを使用することを推奨します。</p> <ul style="list-style-type: none"> <li>• <b>notification-type</b> : <b>mac-notification</b> キーワードを使用します。</li> <li>• <b>vrf vrf</b> インスタンス名 : このホストの VPN ルーティング/転送インスタンスを指定します。</li> </ul>
ステップ 4	<p><b>snmp-server enable traps mac-notification change</b></p> <p>例 :</p> <pre>Device(config)# snmp-server enable traps mac-notification change</pre>	<p>デバイスが MAC アドレス変更通知を NMS に送信できるようにします。</p>
ステップ 5	<p><b>mac address-table notification change</b></p> <p>例 :</p> <pre>Device(config)# mac address-table notification change</pre>	<p>MAC アドレス変更通知機能をイネーブルにします。</p>
ステップ 6	<p><b>mac address-table notification change [ interval value] [ history-size value]</b></p> <p>例 :</p> <pre>Device(config)# mac address-table notification change interval 123 Device(config)# mac address-table notification change history-size 100</pre>	<p>トラップ インターバル タイムと履歴テーブルのサイズを入力します。</p> <ul style="list-style-type: none"> <li>• (任意) <b>interval value</b> : NMS に生成されるトラップの各セット間の通知トラップインターバルを秒単位で指定します。指定できる範囲は 0 ~ 2147483647 秒です。デフォルトは 1 秒です。</li> <li>• (任意) <b>history-size value</b> : 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。</li> </ul>
ステップ 7	<p><b>interface interface-id</b></p> <p>例 :</p>	<p>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</p>

	コマンドまたはアクション	目的
	Device(config)# <b>interface</b> gigabitethernet1/0/2	するレイヤ2 インターフェイスを指定します。
ステップ 8	<b>snmp trap mac-notification change</b> {added   removed}  例：  Device(config-if)# <b>snmp trap</b> <b>mac-notification change added</b>	インターフェイス上で 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"> <li>• MAC アドレスがインターフェイスに<b>added</b>された場合にトラップをイネーブルにします。</li> <li>• MAC アドレスがインターフェイスに<b>removed</b>された場合にトラップをイネーブルにします。</li> </ul>
ステップ 9	<b>end</b>  例：  Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 10	<b>show running-config</b>  例：  Device# <b>show running-config</b>	入力を確認します。
ステップ 11	<b>copy running-config startup-config</b>  例：  Device# <b>copy running-config</b> <b>startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## MAC アドレス移動通知トラップの設定

MAC 移動通知を設定する場合は、MAC アドレスが、同じ VLAN 内のあるポートから別のポートに移動すると常に、SNMP 通知が生成されてネットワーク管理システムに送信されます。

次の手順に従い、デバイスを設定し、NMS ホストに MAC アドレス移動通知トラップを送信するようにします。

手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p><b>snmp-server host <i>host-addr</i> {traps   informs} {version {1   2c   3}} <i>community-string notification-type</i></b></p> <p>例 :</p> <pre>Device(config)# snmp-server host 172.20.10.10 traps private mac-notification</pre>	<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"> <li>• <i>host-addr</i> : NMS の名前またはアドレスを指定します。</li> <li>• <b>traps</b> (デフォルト) : ホストに SNMP トラップを送信します。</li> <li>• <b>informs</b> : ホストに SNMP 情報を送信します。</li> <li>• <b>version</b> : 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。</li> <li>• <b>community-string</b> : 通知処理で送信する文字列を指定します。<b>snmp-server host</b> コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、<b>snmp-server community</b> 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から、<b>snmp-server host</b> コマンドを使用することを推奨します。</li> <li>• <b>notification-type</b> : <b>mac-notification</b> キーワードを使用します。</li> </ul>
ステップ 4	<p><b>snmp-server enable traps mac-notification move</b></p> <p>例 :</p>	<p>デバイスが NMS に MAC アドレス移動通知トラップを送信できるようにします。</p>

	コマンドまたはアクション	目的
	<pre>Device(config)# snmp-server enable traps mac-notification move</pre>	
ステップ 5	<p><b>mac address-table notification mac-move</b></p> <p>例 :</p> <pre>Device(config)# mac address-table notification mac-move</pre>	MAC アドレス移動通知機能をイネーブルにします。
ステップ 6	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 8	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(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。

#### 次のタスク

MAC アドレス移動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 アドレス移動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。

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場合は、MAC アドレス テーブルのしきい値の制限値に達するか、その値を超えると、SNMP 通知が生成されて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、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p><b>snmp-server host <i>host-addr</i> { <b>traps</b> / <b>informs</b> } { <b>version</b> { <b>1</b>   <b>2c</b>   <b>3</b> } }</b> <i>community-string notification-type</i></p> <p>例 :</p> <pre>Device(config)# snmp-server host 172.20.10.10 traps private mac-notification</pre>	<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"> <li><i>host-addr</i> : NMS の名前またはアドレスを指定します。</li> <li><b>traps</b> (デフォルト) : ホストに SNMP トラップを送信します。</li> <li><b>informs</b> : ホストに SNMP 情報を送信します。</li> <li><b>version</b> : 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。</li> <li><i>community-string</i> : 通知処理で送信する文字列を指定します。<b>snmp-server host</b> コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、<b>snmp-server community</b> 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から、<b>snmp-server host</b> コマンドを使用することを推奨します。</li> <li><i>notification-type</i> : <b>mac-notification</b> キーワードを使用します。</li> </ul>
ステップ 4	<p><b>snmp-server enable traps mac-notification threshold</b></p> <p>例 :</p>	<p>NMS への MAC しきい値通知トラップをイネーブルにします。</p>

	コマンドまたはアクション	目的
	<pre>Device(config)# snmp-server enable traps mac-notification threshold</pre>	
ステップ 5	<p><b>mac address-table notification threshold</b></p> <p>例 :</p> <pre>Device(config)# mac address-table notification threshold</pre>	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 6	<p><b>mac address-table notification threshold</b> [ <i>limit percentage</i> ]   [ <i>interval time</i> ]</p> <p>例 :</p> <pre>Device(config)# mac address-table notification threshold interval 123 Device(config)# mac address-table notification threshold limit 78</pre>	<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"> <li>• (任意) <b>limit percentage</b> : MAC アドレステーブルの使用率を指定します。有効値は 1 ~ 100% ですデフォルト値は 50% です。</li> <li>• (任意) <b>interval time</b> : 通知の間隔を指定します。有効値は 120 秒以上です。デフォルトは 120 秒です。</li> </ul>
ステップ 7	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 8	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 9	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(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 の MAC アドレスラーニングのディセーブル化

VLAN で MAC アドレスラーニングを制御すると、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。MAC アドレスラーニングをディセーブルにする前に、ネットワークトポロジ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、ネットワークでフラッディング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には、特権 EXEC モードで次の手順を実行します。

### 始める前に

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

- スイッチ仮想インターフェイス (SVI) スイッチを設定済みの 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、十分注意してください。この場合、スイッチはレイヤ 2 ドメインにすべての IP パケットをフラッディングします。
- MAC アドレスラーニングは、2 から 4094 までの 1 つの VLAN ID (例: `no mac address-table learning vlan 223`)、または、ハイフンやカンマで区切られた一連の VLAN ID (例: `no mac address-table learning vlan 1-10, 15`) でディセーブルにできます。
- MAC アドレスラーニングのディセーブル化は、ポートを 2 つ含む VLAN だけで行うことを推奨します。3 つ以上のポートを含む VLAN で MAC アドレスラーニングをディセーブルにした場合は、スイッチに着信するすべてのパケットは、その VLAN ドメインでフラッディングします。
- セキュア ポートを含む VLAN で MAC アドレスラーニングをディセーブルにする場合、そのポートで MAC アドレスラーニングはディセーブルになりません。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : Device# <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	<b>no mac-address-table learning vlan</b> [ <i>vlan-id</i>   <i>vlan-id</i>   - <i>vlan-id</i> .] 例 : Device(config)# <code>no mac-address-table learning {vlan vlan-id [,vlan-id   -vlan-id]}</code>	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。有効な VLAN ID の範囲は 2 ~ 4094 です。内部 VLAN は指定できません。
ステップ 3	<b>end</b> 例 : Device(config)# <code>end</code>	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	<b>show mac-address-table learning</b> <b>vlan[vlan-id]</b> 例： Device# <b>show mac-address-table learning</b> <b>[vlan vlan-id]</b>	設定を確認します。 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できます。
ステップ 5	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config</b> <b>startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 6	<b>default mac address-table learning</b> 例： Device# <b>default mac address-table</b>	(任意) グローバル コンフィギュレーション モードで VLAN の MAC アドレス ラーニング を再度イネーブルにします。

## 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 を追加するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>mac address-table static mac-addr vlan</b> <b>vlan-id interface interface-id</b> 例： Device(config)# <b>mac address-table</b> <b>static c2f3.220a.12f4 vlan 4 interface</b> <b>gigabitethernet 1/0/1</b>	MAC アドレス テーブル にスタティック アドレス を追加します。 <ul style="list-style-type: none"> <li><b>mac-addr</b> : 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。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>vlan-id</i> : 指定された 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。</li> <li>• <i>interface-id</i> : 受信パケットが転送されるインターフェイスを指定します。有効なインターフェイスは、物理ポートまたはポートチャネルです。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。</li> </ul>
ステップ 4	<b>show running-config</b> 例 : Device# <b>show running-config</b>	入力を確認します。
ステップ 5	<b>copy running-config startup-config</b> 例 : Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## ユニキャスト MAC アドレス フィルタリングの設定

デバイス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、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>mac address-table static mac-addr vlan vlan-id drop</b> 例： Device(config)# <b>mac address-table static c2f3.220a.12f4 vlan 4 drop</b>	ユニキャスト MAC アドレスフィルタリングをイネーブルにし、デバイス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"> <li>• <i>mac-addr</i> : 送信元または宛先ユニキャスト MAC アドレス (48 ビット) 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。</li> <li>• <i>vlan-id</i> : 指定された 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。</li> </ul>
ステップ 4	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例： Device# <b>show running-config</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

## デバイスのモニタリングおよび保守の管理

コマンド	目的
<b>clear mac address-table dynamic</b>	すべてのダイナミック エントリを削除します。
<b>clear mac address-table dynamic address mac-address</b>	特定の MAC アドレスを削除します。

コマンド	目的
<b>clear mac address-table dynamic interface</b> <i>interface-id</i>	指定された物理ポートまたはポート チャンネル上のすべてのアドレスを削除します。
<b>clear mac address-table dynamic vlan</b> <i>vlan-id</i>	指定された VLAN 上のすべてのアドレスを削除します。
<b>show clock</b> [ <i>detail</i> ]	時刻と日付の設定を表示します。
<b>show ip igmp snooping groups</b>	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。
<b>show mac address-table address</b> <i>mac-address</i>	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。
<b>show mac address-table aging-time</b>	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。
<b>show mac address-table count</b>	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。
<b>show mac address-table dynamic</b>	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。
<b>show mac address-table interface</b> <i>interface-name</i>	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。
<b>show mac address-table move update</b>	MAC アドレス テーブル 移動更新情報を表示します。
<b>show mac address-table multicast</b>	マルチキャストの MAC アドレスのリストを表示します。
<b>show mac address-table notification {change   mac-move   threshold}</b>	MAC 通知パラメータおよび履歴テーブルを表示します。
<b>show mac address-table secure</b>	セキュア MAC アドレスを表示します。
<b>show mac address-table static</b>	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。
<b>show mac address-table vlan</b> <i>vlan-id</i>	指定された VLAN の MAC アドレス テーブル情報を表示します。

## デバイス管理の設定例

### 例：システムクロックの設定

次の例は、システムクロックを手動で設定する方法を示しています。

```
Device# clock set 13:32:00 23 July 2013
```

### 例：サマータイムの設定

次に、サマータイムが3月10日の02:00に開始し、11月3日の02:00に終了する場合の設定を例として示します。

```
Device(config)# clock summer-time PDT recurring PST date  
10 March 2013 2:00 3 November 2013 2:00
```

次に、サマータイムの開始日と終了日を設定する例を示します。

```
Device(config)#clock summer-time PST date  
20 March 2013 2:00 20 November 2013 2:00
```

### 例：MOTD バナーの設定

次の例は、開始および終了デリミタにポンド記号（#）を使用して、MOTD バナーを設定する方法を示しています。

```
Device(config)# banner motd #  
  
This is a secure site. Only authorized users are allowed.  
For access, contact technical support.  
  
#  
Device(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 192.0.2.15  
  
Trying 192.0.2.15...  
Connected to 192.0.2.15.  
  
Escape character is '^]'.  
  
This is a secure site. Only authorized users are allowed.
```

```
For access, contact technical support.  
  
User Access Verification  
  
Password:
```

## 例：ログインバナーの設定

次の例は、開始および終了デリミタにドル記号 (\$) を使用して、にログインバナーを設定する方法を示しています。

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

## 例：MAC アドレス変更通知トラップの設定

次に、NMS として 172.20.10.10 を指定し、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、インターバルタイムを 123 秒に設定し、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。

```
Device(config)# snmp-server host 172.20.10.10 traps private mac-notification  
Device(config)# snmp-server enable traps mac-notification change  
Device(config)# mac address-table notification change  
Device(config)# mac address-table notification change interval 123  
Device(config)# mac address-table notification change history-size 100  
Device(config)# interface gigabitethernet1/2/1  
Device(config-if)# snmp trap mac-notification change added
```

## 例：MAC しきい値通知トラップの設定

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、インターバルタイムを 123 秒に設定し、制限を 78% に設定する例を示します。

```
Device(config)# snmp-server host 172.20.10.10 traps private mac-notification  
Device(config)# snmp-server enable traps mac-notification threshold  
Device(config)# mac address-table notification threshold  
Device(config)# mac address-table notification threshold interval 123  
Device(config)# mac address-table notification threshold limit 78
```

## 例：MAC アドレス テーブルへのスタティック アドレスの追加

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。VLAN4でこのMACアドレスを宛先アドレスとして持つパケットを受信すると、パケットは指定されたポートに転送されます。



(注) 複数のインターフェイスに同じ静的 MAC アドレスを関連付けることはできません。コマンドを別のインターフェイスで再度実行すると、新しいインターフェイス上で静的 MAC アドレスが上書きされます。

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

## 例：ユニキャスト MAC アドレス フィルタリングの設定

次に、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つドロップパケットを設定する例を示します。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。

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

## デバイス管理に関する追加情報

### 関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9200 Series Switches)</i>

## デバイス管理の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	デバイス管理	デバイス管理では、システムの日時、システム名、ログインバナーを設定し、DNSを設定できます。

Cisco Feature Navigatorを使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigatorには、<http://www.cisco.com/go/cfn> からアクセスします。



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。