



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 (12 ページ)
- デバイス管理の設定例 (43 ページ)
- デバイス管理に関する追加情報 (45 ページ)
- デバイス管理の機能履歴 (45 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はユーザー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 サーバー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 サーバーには、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 サーバーは、NTP を使用してストラタム 1 タイム サーバー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。

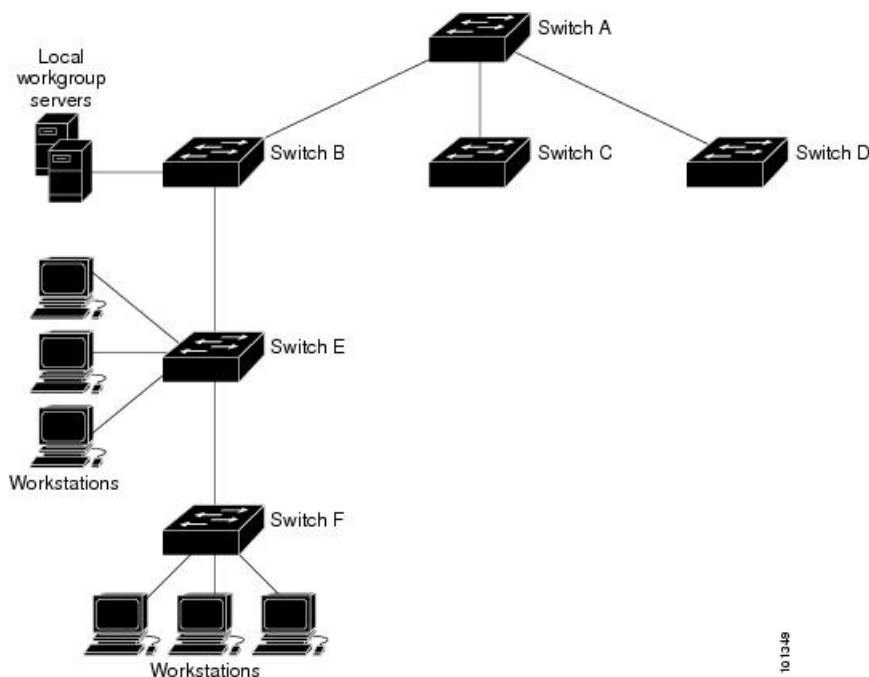
NTPが稼働するデバイス間の通信（アソシエーション）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャストメッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

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 サーバー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 サーバーモードに設定されている（デバイス A との間にサーバー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 タイムサーバーには、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 タイムサーバーは、NTP を使用して

ストラタム 1 タイム サーバー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。

ポーリング ベースの NTP アソシエーション

NTP を実行しているネットワーク デバイスは、時刻を基準時刻源と同期する際にさまざまなアソシエーションモードで動作するように設定できます。ネットワーク デバイスは、2つの方法でネットワーク上の時刻情報を取得できます。それらは、ホストサービスのポーリングと NTP ブロードキャストのリスニングです。ここでは、ポーリングベースのアソシエーションモードを中心に説明します。ブロードキャストベースの NTP アソシエーションの詳細については、「ブロードキャスト ベースの NTP アソシエーション」を参照してください。

最も一般的に使用される 2 つのポーリングベースのアソシエーション モードは次のとおりです。

- クライアント モード
- 対称アクティブ モード

クライアント モードと対称アクティブ モードは、高レベルの時刻の精度と信頼性を提供するために NTP が必要になる場合に使用します。

クライアント モードで動作しているネットワーク デバイスは、自身に割り当てられている時刻提供ホストをポーリングして現在の時刻を取得します。次に、ネットワーク デバイスは、ポーリングされたすべてのタイムサーバーから、同期に使用するホストを選択します。この場合は、確立された関係がクライアントホスト関係なので、ホストがローカルクライアントデバイスから送信された時刻情報をキャプチャしたり使用したりすることはありません。このモードが最も適しているのは、他のローカルクライアントにどのような形式の時刻同期も提供する必要のない、ファイルサーバーおよびワークステーションのクライアントです。ネットワーク デバイスを同期させるタイムサーバーを個別に指定し、クライアントモードで動作するようにネットワーク デバイスを設定するには、**ntp server** コマンドを使用します。

対称アクティブ モードで動作しているネットワーキング デバイスは、自身に割り当てられている時刻提供ホストをポーリングして現在の時刻を取得し、そのホストによるポーリングに応答します。これはピアツーピアの関係なので、ホストは、通信相手のローカルネットワーキング デバイスの時刻関連情報も保持します。このモードは、さまざまなネットワーク パスを経由で多数の冗長サーバーが相互接続されている場合に使用します。インターネット上のほとんどの **Stratum 1** および **Stratum 2** サーバーは、この形式のネットワーク設定を採用しています。ネットワーキングデバイスを同期させる時刻提供ホストを個別に指定し、対称アクティブモードで動作するようにネットワーキングデバイスを設定するには、**ntp peer** コマンドを使用します。

各ネットワーキング デバイスの設定モードを決定する際には、タイムキーピング デバイスとしてのそのデバイスの役割（サーバーかクライアントか）と、そのデバイスが **Stratum 1** タイムキーピング サーバーにどれだけ近いかを主に考慮してください。

ネットワーキング デバイスは、クライアント モードでクライアントまたはホストとして動作する場合、または対称アクティブ モードでピアとして動作する場合にポーリングに関与します。通常、ポーリングによってメモリおよび CPU リソース（帯域幅など）に負荷が生じることはありませんが、システム上で進行または同時実行しているポーリングの数がきわめて多い場合には、システムのパフォーマンスに深刻な影響があったり、特定のネットワークのパフォーマンスが低下したりする可能性があります。過剰な数のポーリングがネットワーク上で進行することを防止するには、直接的なピアツーピアアソシエーションまたはクライアントからサーバーへのアソシエーションを制限する必要があります。代わりに、NTPブロードキャストを使用して、ローカライズされたネットワーク内で時刻情報を伝播することを検討します。

ブロードキャストベースの NTP アソシエーション

ブロードキャストベースの NTP アソシエーションは、時刻の精度および信頼性要件が適度であり、ネットワークがローカライズされ、クライアント数が 20 を超える場合に使用します。また、帯域幅、システム メモリ、または CPU リソースが制限されているネットワークにおいても、ブロードキャストベースの NTP アソシエーションの使用をお勧めします。

ブロードキャスト クライアント モードで動作しているネットワーキング デバイスはポーリングに関与しません。代わりに、ブロードキャスト タイム サーバーによって転送される NTP ブロードキャスト パケットをリスンします。その結果、時刻情報の流れが一方向に限られるため、時刻の精度がわずかに低下する可能性があります。

ネットワークを通じて伝播される NTP ブロードキャスト パケットをリスンするようにネットワーキングデバイスを設定するには、**ntp broadcast client** コマンドを使用します。ブロードキャスト クライアント モードが動作するためには、ブロードキャスト サーバーとそのクライアントが同じサブネット上に存在する必要があります。**ntp broadcast** コマンドを使用して、特定のデバイスのインターフェイスで NTP ブロードキャスト パケットを送信するタイムサーバーを有効にする必要があります。

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。



- (注) Message Direct 5 (MD5) 認証の設定は推奨しません。より強力な暗号化のためにサポートされている他の認証方式を使用できます。

NTP アクセス グループ

アクセスリストベースの制限スキームを使用すると、ネットワーク全体、ネットワーク内のサブネット、またはサブネット内のホストに対し、特定のアクセス権限を許可または拒否できます。NTP アクセスグループを定義するには、グローバル コンフィギュレーションモードで `ntp access-group` コマンドを使用します。

アクセスグループのオプションは、次の順序で制限の緩いものから厳しいものへとスキャンされます。

1. `ipv4` : IPv4 アクセスリストを設定します。
2. `ipv6` : IPv6 アクセスリストを設定します。
3. `peer` : 時刻要求と NTP 制御クエリを許可し、システムがアクセスリストの基準を満たすアドレスを持つ別のシステムに同期することを許可します。
4. `serve` : 時刻要求と NTP 制御クエリを許可しますが、システムがアクセスリストの基準を満たすアドレスを持つ別のシステムに同期することは許可しません。
5. `serve-only` : アクセスリストの条件を満たすアドレスを持つシステムからの時刻要求のみを許可します。
6. `query-only` : アクセスリストの基準を満たすアドレスを持つ別のシステムからの NTP 制御クエリのみを許可します。

送信元 IP アドレスが複数のアクセス タイプのアクセス リストに一致する場合は、最初のアクセス タイプのアクセスが認可されます。アクセス グループが指定されていない場合は、すべてのシステムへのアクセスがすべてのアクセス タイプに対して認可されます。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 タイプに対してのみアクセスが認可されます。

NTP 制御クエリーの詳細については、RFC 1305 (NTP バージョン 3) を参照してください。

信頼できる形式のアクセス コントロールが必要な場合は、暗号化された NTP 認証方式を使用する必要があります。IP アドレスに基づくアクセス リスト ベースの制約方式とは異なり、暗号化認証方式では、認証キーと認証プロセスを使用して、ローカルネットワーク上の指定されたピアまたはサーバーによって送信された NTP 同期パケットが信頼できると見なされるかどうかを、一緒に伝送された時刻情報を受け入れる前に判断します。

認証プロセスは、NTP パケットが作成されるとすぐに開始されます。暗号チェックサム キーは、Message-Digest Algorithm 5 (MD5) を使用して生成され、受信側クライアントに送信される NTP 同期パケットに埋め込まれます。パケットがクライアントによって受信されると、暗号チェックサム キーが復号され、信頼できるキーのリストに対してチェックされます。一致する認証キーがパケットに含まれる場合、受信側クライアントは、パケットに含まれるタイムス

タンブ情報を受け入れます。一致するオーセンティケーター キーが含まれていない NTP 同期パケットは無視されます。



- (注) 信頼できるキーを多数設定する必要がある大規模なネットワークでは、信頼できるキーの範囲設定機能を使用して複数のキーを同時にイネーブルにすることができます。

NTP 認証で使用される暗号化および復号化プロセスでは、CPU に非常に大きな負荷がかかる場合があります。ネットワーク内で伝播される時刻の精度が大きく低下する可能性があることに注意してください。より包括的なアクセス コントロール モデルを使用できるネットワーク構成の場合は、アクセス リスト ベースのコントロール方式を使用することを検討してください。

NTP 認証が適切に設定されると、ネットワーキングデバイスは、信頼できる時刻源と同期し、信頼できる時刻源だけに同期を提供します。

特定のインターフェイス上の NTP サービス

Network Time Protocol (NTP) サービスは、デフォルトではすべてのインターフェイスでディセーブルになっています。なんらかの NTP コマンドを入力すると、NTP がグローバルにイネーブルになります。特定のインターフェイスを通じて特定の NTP パケットを受信しないように設定するには、インターフェイス コンフィギュレーション モードで **ntp disable** コマンドを使用します。

NTP パケットの送信元 IP アドレス

システムが NTP パケットを送信すると、通常、送信元 IP アドレスは、その NTP パケットの送信元であるインターフェイスのアドレスに設定されます。IP 送信元アドレスの取得元のインターフェイスを設定するには、グローバル コンフィギュレーション モードで **ntp source interface** コマンドを使用します。

この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。特定のアソシエーションに送信元アドレスを使用する場合は、**ntp peer** コマンドまたは **ntp server** コマンドで **source** キーワードを使用します。

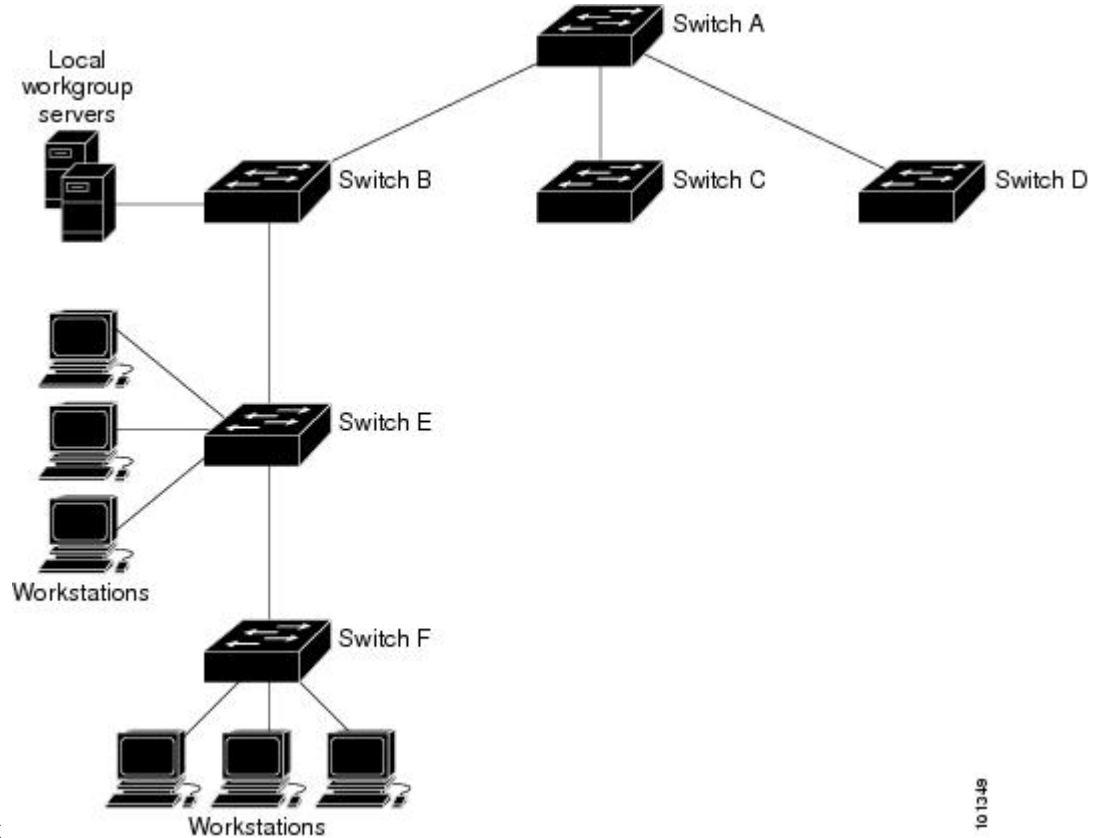
NTP の実装

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 サーバー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 サーバーモードに設定されている（スイッチ A との間にサーバー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

チ（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。

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ーという概念が定義されています。ドメインネームサーバーの役割は、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ーを指定し、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 サーバー	ネーム サーバー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ー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ま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 と関連付けされます。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 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（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 サーバー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	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかを使用します。 <ul style="list-style-type: none"> clock set hh:mm:ss day month year clock set hh:mm:ss month day year 例 : Device# clock set 13:32:00 23 March 2013	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。 <ul style="list-style-type: none"> hh:mm:ss : 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。 day : 月の日で日付を指定します。 month : 月を名前で指定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>year</i> : 年を指定します（略式表記で指定しないでください）。

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	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	clock timezone zone hours-offset [minutes-offset] 例 : Device(config)# clock timezone AST -3 30	時間帯を設定します。 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で、時刻を手動で設定するときだけに使用されます。 <ul style="list-style-type: none"> • <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。 • <i>hours-offset</i> : UTC からのオフセット時間数を入力します。 • （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。
ステップ 4	end 例 :	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
	Device(config)# end	
ステップ 5	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例 : Device# 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。

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	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	clock summer-time zone date date month year hh:mm date month year hh:mm [offset] 例 : Device(config)# clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00	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。

	コマンドまたはアクション	目的
ステップ 4	<p>clock summer-time zone recurring [<i>week day month hh:mm week day month hh:mm [offset]</i>]</p> <p>例 :</p> <pre>Device(config)# clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00</pre>	<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 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"> • <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。 • (任意) <i>week</i> : 月の週 (1 ~ 4、first、または last) を指定します。 • (任意) <i>day</i> : 曜日 (Sunday、Monday など) を指定します。 • (任意) <i>month</i> : 月 (January、February など) を指定します。 • (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。 • (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。
ステップ 5	<p>end</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 6	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	<p>入力を確認します。</p>

	コマンドまたはアクション	目的
ステップ 7	copy running-config startup-config 例 : <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。

NTP の設定

デバイスはハードウェアサポート クロックを備えておらず、外部 NTP ソースが利用できないときに、ピアが自身を同期化するための NTP プライマリクロックとして機能することはできません。デバイスは、カレンダーに対するハードウェアサポートも備えていません。そのため、グローバル コンフィギュレーション モードで **ntp update-calendar** コマンドと **ntp master** コマンドを使用することはできません。

NTP の設定情報については、次のセクションを参照してください。

NTP のデフォルト設定

NTP のデフォルト設定を示します。

表 3: 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 ピアまたはサーバー 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

NTP 認証を設定するには、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	enable 例 : Device> enable	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	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	[no] ntp authenticate 例 : Device(config)# ntp authenticate	NTP 認証をイネーブルにします。 NTP 認証を無効にするには、このコマンドの no 形式を使用します。
ステップ 4	[no] ntp authentication-key number {md5 cmac-aes-128 hmac-sha1 hmac-sha2-256} value 例 : Device(config)# ntp authentication-key 42 md5 aNiceKey	認証キーを定義します。 <ul style="list-style-type: none"> • キーごとに、キー番号、タイプ、および値を 1 つずつ指定します。 • キーは次のいずれかのタイプになります。 <ul style="list-style-type: none"> • md5 : MD5 アルゴリズムを使用した認証。 • cmac-aes-128 : AES-128 アルゴリズムによる暗号ベースメッセージ承認コード (CMAC) を使用した認証。ダイジェストの長さは 128 ビットで、キーの長さは 16 バイトまたは 32 バイトです。 • hmac-sha1 : SHA1 ハッシュ関数を使用したハッシュベースメッセージ承認コード (HMAC) を使用した認証。ダイジェストの長さは 128 ビットで、キーの長さは 1 ～ 32 バイトです。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • hmac-sha2-256 : SHA2 ハッシュ関数を使用した HMAC を使用した認証。ダイジェストの長さは 256 ビットで、キーの長さは 1 ～ 32 バイトです。 <p>SNTP の認証キーを削除する場合は、このコマンドの no 形式を使用します。</p>
ステップ 5	[no] ntp trusted-key key-number 例 : Device(config)# ntp trusted-key 42	<p>このデバイスと同期できるようにするために、ピア NTP デバイスが NTP パケットで提供する必要がある信頼できる認証キーを定義します。</p> <p>信頼できる認証を無効にするには、このコマンドの no 形式を使用します。</p>
ステップ 6	[no] ntp server ip-address key key-id [prefer] 例 : Device(config)# ntp server 172.16.22.44 key 42	<p>NTP タイムサーバーによってソフトウェアクロックが同期されるように設定します。</p> <ul style="list-style-type: none"> • ip-address : クロック同期を提供するタイムサーバーの IP アドレス。 • key-id : ntp authentication-key コマンドで定義された認証キー。 • prefer : このピアを、同期を提供する優先ピアにします。このキーワードは、ピア間のクロックホップを減らします。 <p>サーバーアソシエーションを解除するには、このコマンドの no 形式を入力します。</p>
ステップ 7	end 例 : Device(config)# end	<p>特権 EXEC モードに戻ります。</p>

ポーリングベースの NTP アソシエーションの設定

ポーリングベースの NTP アソシエーションを設定するには、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	enable 例 : Device> enable	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	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	[no] ntp peer ip-address [version number] [key key-id] [source interface] [prefer] 例 : Device(config)# ntp peer 172.16.22.44 version 2	ピアを同期化するか、またはピアによって同期化されるように、デバイスのシステムクロックを設定します（ピアアソシエーション）。 <ul style="list-style-type: none"> • ip-address : クロック同期を提供する、またはクロック同期を提供されるピアの IP アドレス。 • number : NTP バージョン番号。範囲は、1 ～ 3 です。デフォルトでは、バージョン 3 が選択されています。 • key-id : ntp authentication-key コマンドで定義された認証キー。 • interface : IP の送信元アドレスを取得するインターフェイス。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。 • prefer : このピアを、同期を提供する優先ピアにします。このキーワードにより、ピア間の切り替えが減少します。 ピアアソシエーションを解除するには、このコマンドの no 形式を使用します。
ステップ 4	[no] ntp server ip-address [version number] [key key-id] [source interface] [prefer] 例 :	タイムサーバーによって同期化されるように、デバイスのシステムクロックを設定します（サーバーアソシエーション）。

	コマンドまたはアクション	目的
	<pre>Device(config)# ntp server 172.16.22.44 version 2</pre>	<ul style="list-style-type: none"> • ip-address : クロック同期を提供するタイムサーバーの IP アドレス。 • number : NTP バージョン番号。範囲は、1 ～ 3 です。デフォルトでは、バージョン3が選択されています。 • key-id : ntp authentication-key コマンドで定義された認証キー。 • interface : IP の送信元アドレスを取得するインターフェイス。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。 • prefer : このピアを、同期を提供する優先ピアにします。このキーワードは、ピア間のクロックホップを減らします。 <p>サーバーアソシエーションを解除するには、このコマンドの no 形式を入力します。</p>
ステップ 5	<pre>end</pre> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。

ブロードキャストベースの NTP アソシエーションの設定

ブロードキャストベースの NTP アソシエーションを設定するには、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	<pre>enable</pre> <p>例 :</p> <pre>Device> enable</pre>	<p>特権 EXEC モードを有効にします。</p> <p>パスワードを入力します（要求された場合）。</p>
ステップ 2	<pre>configure terminal</pre> <p>例 :</p>	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet1/0/1	インターフェイスを設定し、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 4	[no] ntp broadcast [version number] [key key-id] [destination-address] 例 : Device(config-if)# ntp broadcast version 2	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。 <ul style="list-style-type: none"> • number : NTP バージョン番号。範囲は、1 ～ 3 です。デフォルトでは、バージョン 3 が使用されます。 • key-id : 認証キー。 • destination-address : このスイッチに対してクロックを同期しているピアの IP アドレス。 インターフェイスでの NTP ブロードキャスト パケットの送信を無効にするには、このコマンドの no 形式を使用します。
ステップ 5	[no] ntp broadcast client 例 : Device(config-if)# 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。 インターフェイスでの NTP ブロードキャスト パケットの受信を無効にするには、このコマンドの no 形式を使用します。
ステップ 6	exit 例 : Device(config-if)# exit	特権 EXEC モードに戻ります。
ステップ 7	[no] ntp broadcastdelay microseconds 例 : Device(config)# ntp broadcastdelay 100	(任意) デバイスと NTP ブロードキャストサーバー間のラウンドトリップ遅延の予測値を変更します。 デフォルトは 3000 マイクロ秒です。範囲は 1 ～ 999999 です。

	コマンドまたはアクション	目的
		インターフェイスでのNTPブロードキャストパケットの受信を無効にするには、このコマンドの no 形式を使用します。
ステップ 8	end 例 : Device(config)# end	特権 EXEC モードに戻ります。

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

アクセスグループを作成して基本IPアクセスリストを割り当てるには、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	enable 例 : Device> enable	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	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	[no] ntp access-group {query-only serve-only serve peer} access-list-number 例 : Device(config)# ntp access-group peer 99	アクセスグループを作成し、基本IPアクセスリストを割り当てます。 <ul style="list-style-type: none"> • query-only : NTP 制御クエリ。 • serve-only : 時間要求。 • serve : 時刻要求と NTP 制御クエリは許可しますが、リモートデバイスに対するデバイスの同期化は許可しません。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • peer : 時刻要求と NTP 制御クエリ、およびリモートデバイスに対するデバイスの同期化を許可します。 • access-list-number : IP アクセスリスト番号。指定できる範囲は 1 ～ 99 です。 <p>スイッチ NTP サービスに対するアクセス制御を削除するには、このコマンドの no 形式を使用します。</p>
ステップ 4	access-list access-list-number permit source [source-wildcard] 例 : <pre>Device(config)# access-list 99 permit 172.20.130.5</pre>	<p>アクセスリストを作成します。</p> <ul style="list-style-type: none"> • access-list-number : IP アクセスリスト番号。指定できる範囲は 1 ～ 99 です。 • permit : 条件が一致した場合にアクセスを許可します。 • source : デバイスへのアクセスが許可されているデバイスの IP アドレス。 • source-wildcard : 送信元アドレスに適用されるワイルドカードビット。 <p>(注) アクセスリストを作成する際は、アクセスリストの末尾に暗黙の deny ステートメントがデフォルトで存在し、ACL の終わりに到達するまで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p> <p>SNTP の認証キーを削除する場合は、このコマンドの no 形式を使用します。</p>
ステップ 5	end 例 : <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>

特定のインターフェイス上の NTP サービスのディセーブル化

インターフェイスで NTP パケットの受信を無効にするには、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	enable 例 : Device> enable	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	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet1/0/1	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 4	[no] ntp disable 例 : Device(config-if)# 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。 インターフェイスで NTP パケットの受信を再度有効にするには、このコマンドの no 形式を使用します。
ステップ 5	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。

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	enable 例 : Device> enable	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	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	hostname name 例 : Device(config)# hostname remote-users	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。 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。
ステップ 4	end 例 : remote-users(config)# end remote-users#	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例 : Device# 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。

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、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	enable 例 : Device> enable	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	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	ip domain name name 例 : Device(config)# ip domain name Cisco.com	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。 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) サーバーから行われている場合、BOOTP または DHCP サーバー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（この情報がサーバーに設定されている場合）。
ステップ 4	ip name-server server-address1 [server-address2 ... server-address6] 例 :	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 サーバーのアドレスを指定します。

	コマンドまたはアクション	目的
	<pre>Device(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300</pre>	<p>最大 6 つのネーム サーバーを指定できます。各サーバー 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ーが、プライマリ サーバーです。デバイスは、プライマリサーバーへ 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 サーバーにクエリが送信されます。</p>
ステップ 5	<p>ip domain lookup [nsap source-interface interface]</p> <p>例 :</p> <pre>Device(config)# ip domain-lookup</pre>	<p>(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。</p> <p>ユーザー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、ユーザー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。</p>
ステップ 6	<p>end</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 7	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	<p>入力を確認します。</p>
ステップ 8	<p>copy running-config startup-config</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>

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	enable 例 : Device> enable	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	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	banner motd c message c 例 : Device(config)# banner motd # 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 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> : 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	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ログイン バナーの設定

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	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	banner login c message c 例 : Device(config)# banner login \$ Access for authorized users only. Please enter your username and password. \$	ログイン メッセージを指定します。 c : 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。 message : 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 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 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
	<pre>Device# copy running-config startup-config</pre>	

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	enable 例 : <pre>Device> enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : <pre>Device# configure terminal</pre>	グローバル設定モードを開始します。
ステップ 3	mac address-table aging-time [0 10-1000000] [routed-mac vlan vlan-id] 例 : <pre>Device(config)# mac address-table aging-time 500 vlan 2</pre>	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	end 例 : <pre>Device(config)# end</pre>	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 5	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例 : Device# 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	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	snmp-server host host-addr community-string notification-type { informs traps } { version { 1 2c 3 } } { vrf vrf instance name } 例 : Device(config)# snmp-server host 172.20.10.10 traps private mac-notification	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"> host-addr : NMS の名前またはアドレスを指定します。 traps (デフォルト) : ホストに SNMP トラップを送信します。 informs : ホストに SNMP 情報を送信します。 version : サポートする SNMP バージョンを指定します。informs には

	コマンドまたはアクション	目的
		<p>バージョン 1（デフォルト）を使用できません。</p> <ul style="list-style-type: none"> • community-string : 通知処理で送信する文字列を指定します。 snmp-server host 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、snmp-server community 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、snmp-server host コマンドを使用することを推奨します。 • notification-type : mac-notification キーワードを使用します。 • vrf vrf 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。
ステップ 4	snmp-server enable traps mac-notification change 例 : Device(config)# snmp-server enable traps mac-notification change	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。
ステップ 5	mac address-table notification change 例 : Device(config)# 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 6	mac address-table notification change [interval value] [history-size value] 例 : Device(config)# mac address-table notification change interval 123 Device(config)# mac address-table notification change history-size 100	<p>トラップ インターバル タイムと履歴テーブルのサイズを入力します。</p> <ul style="list-style-type: none"> • （任意） interval value : 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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) history-size value : 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 7	interface interface-id 例 : Device(config)# interface gigabitethernet1/0/2	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。
ステップ 8	snmp trap mac-notification change {added removed} 例 : Device(config-if)# snmp trap mac-notification change added	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"> • MAC アドレスがインターフェイスにaddedされた場合にトラップをイネーブルにします。 • MAC アドレスがインターフェイスにremovedされた場合にトラップをイネーブルにします。
ステップ 9	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 10	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 11	copy running-config startup-config 例 : Device# 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	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type 例 : Device(config)# snmp-server host 172.20.10.10 traps private mac-notification	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"> host-addr : NMS の名前またはアドレスを指定します。 traps (デフォルト) : ホストに SNMP トラップを送信します。 informs : ホストに SNMP 情報を送信します。 version : 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 : 通知処理で送信する文字列を指定します。snmp-server host 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、snmp-server community 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、snmp-server host コマンドを使用することを推奨します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>notification-type</i> : mac-notification キーワードを使用します。
ステップ 4	snmp-server enable traps mac-notification move 例 : <pre>Device(config)# snmp-server enable traps mac-notification move</pre>	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。
ステップ 5	mac address-table notification mac-move 例 : <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	end 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : <pre>Device# show running-config</pre>	入力を確認します。
ステップ 8	copy running-config startup-config 例 : <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	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	snmp-server host host-addr { traps / informs } { version { 1 2c 3 } } community-string notification-type 例 : Device(config)# snmp-server host 172.20.10.10 traps private mac-notification	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"> host-addr : NMS の名前またはアドレスを指定します。 traps (デフォルト) : ホストに SNMP トラップを送信します。 informs : ホストに SNMP 情報を送信します。 version : 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 : 通知処理で送信する文字列を指定します。snmp-server host 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、snmp-server community 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、snmp-server host コマンドを使用することを推奨します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>notification-type</i> : mac-notification キーワードを使用します。
ステップ 4	snmp-server enable traps mac-notification threshold 例 : <pre>Device(config)# snmp-server enable traps mac-notification threshold</pre>	NMS への MAC しきい値通知トラップをイネーブルにします。
ステップ 5	mac address-table notification threshold 例 : <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	mac address-table notification threshold [limit percentage] [interval time] 例 : <pre>Device(config)# mac address-table notification threshold interval 123 Device(config)# mac address-table notification threshold limit 78</pre>	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。 <ul style="list-style-type: none"> • (任意) limit percentage : 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。 • (任意) interval time : 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。
ステップ 7	end 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : <pre>Device# show running-config</pre>	入力を確認します。
ステップ 9	copy running-config startup-config 例 : <pre>Device# copy running-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。

	コマンドまたはアクション	目的
	startup-config	

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ドイ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 パケットをフラッドイングします。
- 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 ドメインでフラッドイングします。
- 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	configure terminal 例： Device# 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 [,vlan-id -vlan-id,] 例：	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。

	コマンドまたはアクション	目的
	Device(config)# no mac-address-table learning {vlan vlan-id [,vlan-id -vlan-id]}	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	end 例 : Device(config)# 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] 例 : Device# show mac-address-table learning [vlan vlan-id]	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	copy running-config startup-config 例 : Device# 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。
ステップ 6	default mac address-table learning 例 : Device# default mac address-table	(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	enable 例 : Device> enable	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	configure terminal 例 : Device# configure terminal	グローバル設定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	mac address-table static mac-addr vlan vlan-id interface interface-id 例 : <pre>Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1</pre>	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"> • mac-addr : 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 : 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。 • interface-id : 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。
ステップ 4	show running-config 例 : <pre>Device# show running-config</pre>	入力を確認します。
ステップ 5	copy running-config startup-config 例 : <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。

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	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル設定モードを開始します。
ステップ 3	mac address-table static mac-addr vlan vlan-id drop 例 : Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 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、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"> mac-addr : 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。 vlan-id : 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。
ステップ 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例 : Device# 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。

デバイスのモニターリングおよび保守の管理

コマンド	目的
clear mac address-table dynamic	すべてのダイナミックエントリを削除します。
clear mac address-table dynamic address <i>mac-address</i>	特定の MAC アドレスを削除します。
clear mac address-table dynamic interface <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。
clear mac address-table dynamic vlan <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。
show clock [<i>detail</i>]	時刻と日付の設定を表示します。
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 <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。
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 <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。
show mac address-table move update	MAC アドレス テーブル移動更新情報を表示します。
show mac address-table multicast	マルチキャストの MAC アドレスのリストを表示します。
show mac address-table notification {change mac-move threshold}	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 secure	セキュア MAC アドレスを表示します。
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。

コマンド	目的
show mac address-table vlan <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
```

例：ログインバナーの設定

```
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</i> (Catalyst 9300 シリーズ スイッチ)

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 Everest 16.5.1a	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。