CHAPTER 1

概要

この章では、Cisco Metro Ethernet（ME）3400E シリーズ イーサネット アクセス スイッチ ソフトウェアについて説明します。具体的な内容は次のとおりです。

このマニュアル内では、「IP」と表記した場合は IP バージョン 4（IPv4）を表すものとし、IP バージョン 6 を表す場合は「IPv6」と明記します。

機能

スイッチには、次のいずれかのソフトウェア イメージがインストールされています。

- メトロ アクセス イメージは、IEEE 802.1Q トンネリング、レイヤ 2 プロトコル トンネリング、ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査、IP ソース ガードなどの追加機能を備えています。
- メトロ IP アクセス イメージは、Routing Information Protocol（RIP）、Open Shortest Path First（OSPF）プロトコル、Border Gateway Protocol（BGP）、および Enhanced Interior Gateway Routing Protocol（EIGRP）に対する IP ルーティングのサポート、Intermediate System-to-Intermediate System（IS-IS）ダイナミック ルーティング、Bidirectional Forwarding Detection （BFD; 双方向フォワーディング検出）プロトコル、Customer Edge（CE; カスタマーエッジ）デバイスの Multiple VPN Routing/Forwarding（マルチ VRF）インスタンス（マルチ VRF CE）、および IP マルチキャスト ルーティングの Protocol-Independent Multicast（PIM）の sparse（希薄）モード（SM）および dense（稠密）モード（DM）などのレイヤ 3 機能が追加されています。

（注） 特記されていないかぎり、この章およびこのマニュアルで説明されている機能はいずれも、すべてのイメージでサポートされています。

この章で特記されている機能の中には、スイッチ ソフトウェア イメージの暗号化（暗号化をサポートしている）バージョンでだけ使用可能なものもあります。こうした機能を使用するには、その使用権限を取得し、Cisco.com からソフトウェアの暗号化バージョンをダウンロードする必要があります。詳細については、このリリースのリリース ノートを参照してください。

Cisco ME スイッチには、Network Node Interface（NNI; ネットワーク ノード インターフェイス）および User Network Interface（UNI; ユーザ ネットワーク インターフェイス）という 2 つのタイプのインターフェイスがデフォルトで用意されています。NNI はサービス プロバイダー ネットワークへの接続に使用され、UNI は顧客ネットワークへの接続に使用されます。一部の機能は、このいずれかのポート タイプでだけサポートされます。また、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）を設定することもできます。ENI は通常、ユーザ ネットワーク側インターフェイスとして使用され、そのデフォルト設定および機能は UNI と同じです。ただし、設定により Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）、Link Layer Discovery Protocol（LLDP; リンク レイヤ検出プロトコル）、および EtherChannel の Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）または Port Aggregation Protocol（PAgP; ポート集約プロトコル）用のプロトコル制御パケットをサポートできます。

パフォーマンスの特長

- すべてのスイッチ ポートにおけるポート速度の自動検知とデュプレックス モードの自動ネゴシエーションにより、帯域利用が最適化されます。
- 10/100 Mbps インターフェイスと 10/100/1000 Mbps インターフェイス、および 10/100/1000 BASE-T/TX Small Form-factor Pluggable（SFP）モジュール インターフェイス上の Automatic Medium-Dependent Interface crossover（Auto MDIX）機能によって、インターフェイスは必要なケーブル接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定できます。
- ルーテッド フレームの場合は最大 1998 バイト、ハードウェアでブリッジングされるフレームの場合は最大 9000 バイト、ソフトウェアでブリッジングされるフレームの場合は最大 2000 バイトのサポートを実現します。
- すべてのポートで IEEE 802.3x フロー制御（スイッチは、ポーズ フレームを送信しない）を行います。
- EtherChannel により、耐障害性を高め、スイッチ、ルータ、およびサーバ間に最大 8 Gbps（ギガビット EtherChannel）または 800 Mbps（ファスト EtherChannel）の全二重の帯域幅を確保します。
- PAgP および LACP により EtherChannel リンク（NNI または ENI に限りサポート）が自動的に作成されます。
- レイヤ 2 およびレイヤ 3 パケットをギガビット回線レートで転送します。

- ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストーム防止用のポート単位のストーム制御を行います。
- レイヤ 2 の不明なユニキャスト トラフィック、マルチキャスト トラフィック、およびブリッジド ブロードキャスト トラフィックの転送時にポート ブロッキングを行います。
- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）バージョン 1、2、および 3 の IGMP スヌーピングにより、マルチメディア トラフィックおよびマルチキャスト トラフィックを効率的に転送できます。
- IGMP レポート抑制により、マルチキャスト ルータのクエリーごとに 1 つの IGMP レポートがマルチキャスト デバイスに送信されます（IGMPv1 クエリーまたは IGMPv2 クエリーに限りサポート）。
- IGMP スヌーピング クエリアのサポートにより、IGMP 一般クエリー メッセージが定期的に生成されるようにスイッチを設定できます。
- IGMP ヘルパーにより、マルチキャスト ストリームへのホスト加入要求を、スイッチから特定の IP 宛先アドレスへ転送できます（メトロ IP アクセス イメージが必要）。
- Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）により、マルチキャスト VLAN 内でマルチキャスト ストリームを継続的に送信し、かつ帯域幅およびセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離できます。各スイッチ上では最大 512 のマルチキャスト エントリがサポートされています。
- MVR over trunk port（MVRoT）のサポートにより、トランク ポートを MVR 受信ポートとして設定できます。
- IGMP フィルタリングにより、スイッチ ポート上のホストが所属できるマルチキャスト グループ セットを管理できます。
- IGMP スロットリングにより、IGMP 転送テーブル内のエントリ数が上限に達した場合のアクションを設定できます。
- 設定可能な IGMP 脱退タイマーにより、ネットワークの脱退遅延を設定します。
- Switch Database Management（SDM; スイッチ データベース管理）テンプレートにより、ユーザが選択した機能を最大限サポートできるようなシステム リソースの割り当てを行えます。また、IPv6 アドレスのサポート用として、デュアル IPv4/IPv6 テンプレートが用意されています。
- RADIUS サーバのロード バランシングにより、アクセス要求や認証要求がサーバ グループ全体で均等に分散されます。
- MVR の拡張機能として、スイッチがダイナミック MVR モードの場合には最大 2000 の MVR グループを設定できるだけでなく、新たに追加されたコマンド（**mvr ringmode flood**）を使用することで、リング トポロジでの転送をメンバー ポートに制限できます。

管理オプション

- Command Line Interface（CLI; コマンドライン インターフェイス）: Cisco IOS ソフトウェアでは、デスクトップ スイッチング機能および Multilayer Switching（MLS; マルチレイヤ スイッチング）機能がサポートされています。CLI には、スイッチのコンソール ポートに直接管理ステーションを接続するか、リモート管理ステーションから Telnet を使用してアクセスできます。CLI の詳細については、第 2 章「CLI の使用方法」を参照してください。
- Cisco Configuration Engine : Cisco Configuration Engine は、スイッチ ソフトウェアに組み込まれた Cisco IOS CNS エージェントと連携するネットワーク管理デバイスです。スイッチ固有の設定変更を生成してスイッチに送信し、設定変更を実行して結果をロギングすることで、初期設定および設定更新を自動化できます。Cisco IOS エージェントの使用に関する詳細については、第 4 章「Cisco IOS Configuration Engine の設定」を参照してください。

- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）: SNMP 管理アプリケーションには、CiscoWorks2000 LAN Management Suite（LMS）や HP OpenView などがあります。HP OpenView や SunNet Manager などのプラットフォームが稼動している SNMP 対応管理ステーションを使用してスイッチを管理できます。スイッチは、広範囲の拡張 Management Information Base（MIB; 管理情報ベース）セットおよび 4 種類の （RMON; リモート モニタリング）グループをサポートしています。SNMP の詳細については、第 30 章「SNMP の設定」を参照してください。

管理機能

（注）　ここに列挙した暗号化 Secure Shell（SSH ; セキュア シェル）機能は、スイッチ ソフトウェア イメージの暗号化バージョンでだけ使用できます。

- IP アドレス、デフォルト ゲートウェイ、ホスト名、Domain Name System（DNS; ドメイン ネーム システム）、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ名などのスイッチ情報の設定に関して、Dynamic Host Configuration Protocol（DHCP）をサポートします。
- DHCP リレーにより、IP アドレス要求など DHCP クライアントからの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ブロードキャストが転送されます。
- DHCP サーバにより、IP アドレスおよびその他の DHCP オプションが IP ホストに自動で割り当てられます。
- DHCP ベースの自動設定およびイメージ アップデートにより、指定された設定および新しいイメージが多数のスイッチにダウンロードされます。
- DHCP サーバによるポート ベースのアドレス割り当てにより、スイッチ ポートには IP アドレスが事前に割り当てられます。
- DNS サーバへの有向ユニキャスト要求により、IP アドレスおよび対応ホスト名からスイッチを特定できるほか、TFTP サーバへの有向ユニキャスト要求により、ソフトウェア アップグレードを TFTP サーバから管理できます。
- ARP によって、IP アドレスおよび対応 MAC アドレスからスイッチを特定できます。
- ユニキャスト MAC アドレス フィルタリングにより、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廃棄できます。
- 設定可能な MAC アドレス スケーリングにより、VLAN 上での MAC アドレス学習をディセーブルにして、MAC アドレス テーブルのサイズを制限できます。
- CDP バージョン 1 および 2 により、ネットワーク トポロジを検出できるだけでなく、そのネットワーク上にあるスイッチやその他のシスコ製デバイスを相互にマッピングできます（NNI ではデフォルトでサポート、ENI ではイネーブル化可能、UNI ではサポートなし）。
- LLDP および LLDP Media Endpoint Discovery（LLDP-MED）により、サードパーティ製の IP 電話との相互運用性が実現されます（NNI または ENI でだけサポート）。
- LLDP-MED ロケーション TLV のサポートにより、スイッチからエンドポイント デバイスへロケーション情報が送信されます。
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）により、外部ソースから全スイッチへ一貫したタイム スタンプが提供されます。
- Cisco IOS File System（IFS）により、スイッチが使用するすべてのファイル システムに対して共通のインターフェイスを使用できます。

- 帯域内管理アクセスにより、ネットワーク上の複数の CLI ベース セッションに対して、最大 16 の Telnet 接続を同時に行えます。
- 帯域内管理アクセスにより、ネットワーク上の複数の CLI ベース セッションに対して、最大 5 つの暗号化 SSH 接続を同時に行えます（スイッチ ソフトウェアの暗号化バージョンが必要）。
- SNMP バージョン 1、2c、3 の get 要求および set 要求を介した帯域内管理アクセスが可能です。
- スイッチのコンソール ポートから、直接接続された端末への帯域外管理アクセスや、シリアル接続またはモデムを経由したリモート ターミナルへの帯域外管理アクセスが可能です。
- イーサネット管理ポートから PC への帯域外管理アクセスが可能です。
- ユーザ定義のコマンド マクロにより、複数のスイッチ間の配置を単純化するカスタム スイッチ設定を作成できます。
- メトロ イーサネットの Operation, Administration, and Maintenance（OAM; 運用管理および保守）IEEE 802.1ag Connectivity Fault Management（CFM）、カスタマーエッジ スイッチおよびプロバイダーエッジ スイッチにおける Ethernet Line Management Interface（E-LMI）、IEEE 802.3ah イーサネット OAM ディスカバリ、リンク モニタリング、リモート障害検知、およびリモート ループバックをサポートしています。
- イーサネット ループバック機能のサポートにより、リモート デバイスへの接続をテストできます。無停止ループバック テストを行うための VLAN ループバックと、全パスの QoS（Quality Of Service）を双方向でテストするための端末ループバックがあります（メトロ IP アクセス イメージが必要）。
- コンフィギュレーションの置換およびロールバックにより、スイッチ上の実行コンフィギュレーションを、保存されている Cisco IOS コンフィギュレーション ファイルで置換できます。
- Source Specific Multicast（SSM）マッピングにより、マルチキャスト アプリケーションでは送信元のマッピングが可能になります。これにより、IGMPv2 クライアントは SSM を利用できるようになり、リスナーはマルチキャストの送信元にダイナミックに接続できるようになります。またアプリケーションへの依存度も軽減されます。
- Cisco IOS でサポートされている HTTP クライアントは、IPv4 HTTP サーバおよび IPv6 HTTP サーバのどちらに対しても要求を送信できます。また Cisco IOS でサポートされている HTTP サーバは、IPv4 HTTP クライアントおよび IPv6 HTTP クライアントのどちらから送信された HTTP 要求も処理できます（メトロ IP アクセス イメージが必要）。
- IPv6 では、ステートレス自動設定がサポートされています。これにより、リンク、サブネット、およびサイトのアドレス指定変更を管理できます。ホスト IP アドレスやモバイル IP アドレスの管理に有用です（メトロ IP アクセス イメージが必要）。
- CPU 利用率のしきい値トラップにより、CPU の利用率をモニタできます。
- DHCPDISCOVER パケットの Option 12 フィールドにホスト名を指定できます。これにより、DHCP プロトコルを使用して同一のコンフィギュレーション ファイルを送信できます。
- DHCP スヌーピングの機能拡張として、DHCP の Option 82 フィールドの回線 ID サブオプションに対して固定型ストリング ベース フォーマットを選択できるようになっています。

アベイラビリティ機能

- UniDirectional Link Detection（UDLD; 単方向リンク検出）およびアグレッシブ UDLD により、不適切な光ファイバ配線またはポート障害によって生じる光ファイバ インターフェイス上の単方向リンクを検出してディセーブル化できます。
- IEEE 802.1D Spanning Tree Protocol（STP; スパニング ツリー プロトコル）により、冗長バックボーン接続とループのないネットワークを実現できます（NNI ではデフォルトでサポート、ENI ではイネーブル化可能、UNI ではサポートなし）。STP には次の機能があります。
  - 最大 128 のスパニング ツリー インスタンスをサポート
  - Per-VLAN Spanning-Tree Plus（PVST+）による VLAN 間のロード バランシング
  - Rapid Per-VLAN Spanning-Tree Plus（rapid-PVST+）による VLAN 間のロード バランシングとスパニング ツリー インスタンスの高速コンバージェンス
- NNI または ENI で動作する IEEE 802.1s Multiple Spanning-Tree Protocol（MSTP; マルチ スパニング ツリー プロトコル）により、複数の VLAN をスパニング ツリー インスタンスにグループ化できるほか、データ トラフィックとロード バランシングに使用するフォワーディング パスを複数構成できます。さらに、IEEE802.1w Rapid Spanning-Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）をベースにした rapid PVST+ により、ルートおよび指定ポートの NNI またはスパニング ツリー対応の ENI を即座にフォワーディング ステートへ移行することでスパニング ツリーの高速コンバージェンスが可能です。
- スパニング ツリーがイネーブルになっている NNI および ENI では、Optional spanning-tree features available in PVST+ モード、rapid-PVST+ モード、および MSTP モードで、次のようなオプションのスパニング ツリー機能を使用できます。
  - PortFast：スパニング ツリー ポートをブロッキング ステートからフォワーディング ステートに即時に移行することで転送遅延を解消
  - Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）ガード：BPDU を受信する PortFast 対応のポートをシャット ダウン
  - BPDU フィルタリング：PortFast 対応のポートで BPDU が送受信されるのを防止
  - ルート ガード機能：ネットワーク コア外のスイッチがスパニング ツリー ルートとして使用されるのを防止
  - ループ ガード：単方向リンクを引き起こす障害によって代替ポートまたはルート ポートである NNI または ENI が指定ポートとして使用されるのを防止
- STP の代替手段として相互にバックアップする Flex Link レイヤ 2 インターフェイスと、プリエンプションされるスイッチオーバーおよび双方向高速コンバージェンスにより、ループのないネットワークでの基本的なリンク冗長性が確保されます。MAC アドレス テーブル移行更新機能とも呼ばれます。
- Flex Link マルチキャスト高速コンバージェンスにより、Flex Link に障害が発生したあとのマルチキャスト トラフィックのコンバージェンス時間が短縮されます。
- リンクステート トラッキングにより、接続されたホストおよびサーバからのアップストリーム トラフィックを伝送するポートのステートをミラーリングし、他の Cisco Ethernet スイッチ上の動作リンクにサーバ トラフィックをフェールオーバーできます。
- Resilient Ethernet Protocol（REP; レジリエント イーサネット プロトコル）により、スパニング ツリーを使用しないコンバージェンス時間の短縮とネットワーク ループ防止が可能です。
- REP のサポートに合せてカウンタおよびタイマーの機能が拡張されています。ネイバー ポートが REP に対応していない場合に REP エッジ ポートを使用できます。
- Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）により、レイヤ 3 ルータの冗長性が確保されます（メトロ IP アクセス イメージが必要）。

- 等価コスト ルーティングにより、リンク レベルおよびスイッチ レベルでの冗長性が確保されます（メトロ IP アクセス イメージが必要）。
- Shorter REP hello により、REP Link Status Layer（LSL; リンク ステータス レイヤ）の経過時間タイマーの範囲が 3000 ～ 10000 ミリ秒（500 ミリ秒間隔）から 120 ～ 10000 ミリ秒（40 ミリ秒間隔）に変更されています。

VLAN 機能

- 最大 1005 の VLAN がサポートされているため、ユーザを適切なネットワーク リソース、トラフィック パターン、および帯域に対応付けられた VLAN に割り当てることが可能です。
- IEEE 802.1Q 標準によって許可された 1 ～ 4094 の範囲の VLAN ID が完全にサポートされています。
- VLAN Query Protocol（VQP; VLAN クエリー プロトコル）により、ダイナミック VLAN メンバーシップがサポートされています。
- 全ポートでの IEEE 802.1Q トランキング カプセル化により、ネットワークの移動、追加、および変更、ブロードキャストおよびマルチキャスト トラフィックの管理と制御、高度なセキュリティを要するユーザやネットワーク リソースに対して VLAN グループを作成することによるネットワーク セキュリティが実現されています。
- VLAN 1 の最小化によって、VLAN 1 を個々の VLAN トランク リンクでディセーブル化できます。これにより、スパニング ツリー ループまたはストームのリスクが軽減されます。この機能をイネーブルにすると、ユーザ トラフィックはトランク上では送受信されません。スイッチ CPU は、これまでどおり制御プロトコル フレームを送受信します。
- UNI-ENI 独立 VLAN により、カスタマー VLAN を、同一スイッチ上の他のカスタマー VLAN から分離できます。同一の UNI-ENI 独立 VLAN に属するスイッチでは、UNI または ENI 間のローカル スイッチングが実行されません。
- プライベート VLAN により、VLAN のスケーラビリティの問題に対処できるほか、IP アドレスの割り当てをより細かく制御したり、レイヤ 2 ポートを他のスイッチ上のポートから分離したりできます。
- PVLAN ホストのポート セキュリティにより、ポートで学習される MAC アドレスの数を制限できるほか、ポートで学習できる MAC アドレスを定義できます。
- VLAN Flex Link ロード バランシングにより、STP を使用することなく、レイヤ 2 の冗長性を確保できます。プライマリ リンクおよびバックアップ リンクとして設定されるインターフェイスのペアにより、VLAN に基づいてトラフィックの負荷を分散できます。
- カスタマー ネットワークに接続されたトランク ポート上での VLAN マッピング（または VLAN ID 変換）により、Customer VLAN（C-VLAN; カスタマー VLAN）を Service Provider VLAN（S-VLAN; サービス プロバイダー VLAN）にマッピングできます。

セキュリティ機能

スイッチは、加入者、スイッチ、およびネットワークに対するセキュリティ機能を備えています。

加入者に対するセキュリティ

- デフォルトでは、各加入者の独立性を確保するため、加入者ポート間のローカル スイッチングはディセーブルに設定されています。

- DHCP スヌーピングにより、信頼できないホストと DHCP サーバの間で、信頼できない DHCP メッセージのフィルタリング処理を行えます。
- DHCP スヌーピング統計情報の **show** コマンドにより、DHCP スヌーピング統計情報をサマリー形式または詳細形式で表示できます。また **clear** コマンドにより、DHCP スヌーピング統計情報を削除できます。
- IP ソース ガードにより、DHCP スヌーピング データベースおよび IP 送信元バインディングに基づいて、ルーティングされないインターフェイス上でトラフィックを制限できます。
- ダイナミック ARP 検査により、無効な ARP 要求や応答を同じ VLAN 内の他のポートにリレーしないことで、スイッチに対する悪意のある攻撃を防御できます。

スイッチ セキュリティ

（注） ここに示した Kerberos 機能は、スイッチ ソフトウェア イメージの暗号化バージョンでだけ使用できます。

- パスワードによって保護された管理インターフェイスへのアクセス（読み取り専用および読み取り/書き込み）により、不正な設定変更を防止できます。
- 認証および許可されたユーザに限ってコンフィギュレーション ファイルにアクセスできるようにしたコンフィギュレーション ファイル セキュリティ機能によって、ユーザがパスワード回復プロセスを使用してコンフィギュレーション ファイルにアクセスするのを防止できます。
- マルチレベルのセキュリティにより、セキュリティ レベル、通知、および対応動作を選択できます。
- ポート セキュリティ オプションにより、ポートへのアクセスを許可するステーションの MAC アドレスを制限したり識別したりできます。
- ポート セキュリティ エージングにより、ポート上のセキュア アドレスに対してエージング タイムを設定できます。
- LLDP および LLDP-Media Extensions（LLDP-MED; LLDP メディア拡張）により、マルチベンダー ネットワークでの相互運用性に対して IEEE 802.1AB リンク レイヤ検出プロトコルがサポートされます。スイッチは、速度、デュプレックス、および電力の設定を IP 電話などのエンド デバイスと交換します。
- UNI および ENI のデフォルト ポート ステートはディセーブルです。
- 自動コントロール プレーン保護機能により、UNI または ENI 上のレイヤ 2 制御トラフィックによって偶発的または意図的に生じる過負荷から CPU が保護されます。
- サービス プロバイダーの柔軟な対応を可能にする設定可能コントロール プレーン セキュリティ機能により、カスタマーのコントロール プレーン トラフィックをポート単位およびプロトコル単位で廃棄できます。CDP、STP、LLDP、LACP、または PAgP に対して ENI プロトコル制御パケットを設定できます。
- Terminal Access Controller Access Control System Plus（TACACS+）は、TACACS サーバを介してネットワーク セキュリティを管理するシスコ独自の機能です。
- Remote Authentication Dial-In User Service（RADIUS）により、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）サービスを使用して、リモート ユーザの ID の検証、アクセスの許可、およびアクションの追跡を実行できます。
- Kerberos セキュリティ システムにより、信頼できる第三者を通じてネットワーク リソースの要求を認証できます（スイッチ ソフトウェアの暗号化バージョンが必要）。

ネットワーク セキュリティ

- スタティック MAC アドレス指定を使用することで、セキュリティを確保できます。
- 標準および拡張 IP Access Control List（ACL; アクセス制御リスト）により、ルーテッド インターフェイス（ルータ ACL）と VLAN の両方向およびレイヤ 2 インターフェイス（ポート ACL）の受信方向に関するセキュリティ ポリシーを定義できます。
- インターフェイスに適用される IPv6 ACL により、IPv6 トラフィックのフィルタリングを行えます。
- 拡張 MAC ACL により、レイヤ 2 インターフェイスの受信方向に関するセキュリティ ポリシーを定義できます。
- VLAN ACL（VLAN マップ）により、MAC ヘッダー、IP ヘッダー、および TCP/UDP ヘッダー内の情報を基にしたトラフィックのフィルタリングを行い、VLAN 内のセキュリティを確保できます。
- 送信元および宛先 MAC ベースの ACL により、非 IP トラフィックのフィルタリングを行えます。
- IEEE 802.1X ポートベースの認証により、不正なデバイス（クライアント）がネットワークにアクセスするのを防止できます。次の機能がサポートされています。
  - VLAN 割り当て：IEEE 802.1X 認証ユーザを特定の VLAN に制限できます。
  - ポート セキュリティ：IEEE 802.1X ポートへのアクセスを制御できます。
  - IEEE 802.1X アカウンティング：ネットワークの使用状況を追跡できます。
  - 802.1x 準備状態チェック：スイッチ上で 802.1x の設定を行う前に、接続されているエンド ホストの準備状態を判定できます。
  - 802.1x スイッチ サプリカントによる Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）、Client Information Signalling Protocol（CISP; クライアント情報シグナリング プロトコル）によるホスト許可、および自動イネーブル化：ワイヤリング クローゼット外部のスイッチを、他のスイッチに対するサプリカントとして認証できます。
- スタティック ホスト上では、IP ソース ガードがサポートされています。
- IEEE 802.1x ユーザ分散により、複数の VLAN でユーザのロードバランシングを行えます。これにより、複数の VLAN が配置されたネットワークのスケーラビリティを向上させることが可能です。認可されたユーザは、RADIUS サーバにより割り当てられたグループ内でメンバーが最も少ない VLAN に割り当てられます。
- SNMP バージョン 3（SNMPv3）で Triple Data Encryption Standard（3DES; トリプル DES）および Advanced Encryption Standard（AES; 高度暗号化規格）がサポートされています。このリリースでは、SNMPv3 に対する暗号化アルゴリズムとして、168 ビットの 3DES および 128 ビット、192 ビット、および 256 ビットの AES が新たにサポートされています。
- IPv6 MLD スヌーピング、IPv6 eBGP、IPv6 SNMP、syslog、HTTP を含め、IPv6 が追加サポートされています。

QoS 機能および CoS 機能

- 設定可能コントロール プレーン キュー割り当てにより、CPU で生成されたトラフィックのコントロール プレーン トラフィックを、特定の出力キューに割り当てることが可能です。
- Cisco Modular Quality of Service Command Line Interface（MQC; モジュラ QoS コマンドライン インターフェイス）が実装されています。

- IP precedence、Differential Service Code（DSCP）、および IEEE 802.1p Class of Service（CoS; サービス クラス）パケット フィールドに基づく分類、ACL 検索、または出力分類への QoS ラベルの割り当てが可能です。
- ポリシング
  - 平均レートおよびバースト レートに基づく 1 レート ポリシング：1 つのポリサーが対象
  - 2 カラー ポリシング：レートに適合するパケットまたはレートを超過するパケットにより異なる動作を許可
  - 集約ポリシング：複数のトラフィック クラスで共有されるポリサーが対象
  - 入力 2 レート、3 カラー ポリシング：個別のポリサーまたは集約ポリサーが対象
- 輻輳回避メカニズムである Weighted Tail Drop（WTD; 重み付きテール ドロップ）により、キューの長さを管理し、異なるトラフィック分類ごとに廃棄優先順位を決定できます。
- テーブル マップにより、DSCP、CoS、IP precedence の各値をマッピングできます。
- キューイングおよびスケジューリング。
  - Shaped Round Robin（SRR; シェイプド ラウンド ロビン）トラフィック シェーピングにより、すべてのキューのパケットを混在させて、トラフィック バーストを最小化できます。
  - クラスベース トラフィック シェーピングにより、トラフィック クラスの最大許容平均レートを指定できます。
  - ポート シェーピングにより、ポートの最大許容平均レートを指定できます。
  - Class-based Weight Queuing（CBWFQ; クラス ベース均等化キューイング）により、トラフィック クラスに合せて帯域幅を制御できます。
  - WTD により、指定されたトラフィック クラスのキュー サイズを調整できます。
  - 低遅延プライオリティ キューイングにより、特定のトラフィックへの優先処理を許可できます。
- ポート単位、VLAN 単位 QoS により、所定のインターフェイスのユーザ指定 VLAN で伝送されるトラフィックを制御できます。IOS ソフトウェア リリース 12.2（25）SEG 以降では、VLAN 単位の分類に階層型ポリシーマップを使用して、トランク ポートにポート単位、VLAN 単位の階層型ポリシー マップを適用できます。
- CPU 保護をディセーブルにするオプションにより、使用できる QoS ポリシング機能が、1 ポートにつき 45 から 64 （4 ポートごとに 63）に増加しました。

レイヤ 2 VPN サービス

- IEEE 802.1Q トンネリングにより、サービス プロバイダーはカスタマーに複数のポイント レイヤ 2 VPN サービスを提供できます。
- レイヤ 2 プロトコル トンネリングにより、カスタマーは BPDU、CDP、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）、PAgP、LACP、および UDLD などのプロトコルを制御して、サービス プロバイダー ネットワーク間でトンネリングを行えます。
- カスタマー ネットワークに接続されたトランク ポート上での VLAN マッピング（または VLAN ID 変換）により、Customer VLAN（C-VLAN; カスタマー VLAN）を Service Provider VLAN（S-VLAN; サービス プロバイダー VLAN）にマッピングできます。

レイヤ 3 機能

（注）　レイヤ 3 機能は、スイッチでメトロ IP アクセス イメージが稼動している場合に限り使用できます。

- HSRP バージョン 1（HSRPv1）および HSRP バージョン 2（HSRPv2）により、レイヤ 3 ルータの冗長性が確保されます。
- 次の IP ルーティング プロトコルにより、ロード バランシングとスケーラブルなルーテッド バックボーンを構築できます。
  - RIP バージョン 1 および 2
  - OSPF
  - EIGRP
  - BGP バージョン 4
  - IS-IS ダイナミック ルーティング
  - BFD プロトコル：OSPF、IS-IS、BGP、EIGRP、または HSRP の各ルーティング プロトコルのフォワーディング パス障害を検出できます。
- 2 つ以上の VLAN 間における完全レイヤ 3 ルーティングに対応した IP ルーティング（VLAN 間ルーティング）により、各 VLAN は独自の自律データリンク ドメインを維持できます。
- Policy-Based Routing（PBR; ポリシー ベース ルーティング）により、トラフィック フローに定義済みポリシーを設定できます。
- スタティック IP ルーティングにより、ネットワーク パス情報のルーティング テーブルを手動で作成できます。
- 等価コスト ルーティングにより、ロード バランシングおよび冗長構成が可能です。
- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）および ICMP Router Discovery Protocol（IRDP）により、ルータのアドバタイズメントおよびルータ請求メッセージを使用して、直接接続されたサブネット上にあるルータのアドレスを検出できます。
- PIM により、ネットワーク内でのマルチキャスト ルーティングが可能です。これにより、ネットワーク内のデバイスは要求されたマルチキャスト フィードを受信できるほか、マルチキャストに参加しないスイッチをプルーニングできます。PIM-SM モード、PIM-DM モード、および PIM sparse-dense モードもサポートされています。
- SSM PIM プロトコルのサポート：ビデオなどのマルチキャスト アプリケーションを最適化できます。
- Multicast Source Discovery Protocol（MSDP）により、複数の PIM-SM ドメインを接続できます。
- DHCP リレーにより、IP アドレス要求など DHCP クライアントからの UDP ブロードキャストを転送できます。
- DHCP for IPv6 のリレー、クライアント、サーバ アドレス割り当て、およびプレフィクス委任がサポートされています。
- IPv6 ユニキャスト ルーティング機能により、スタティック ルーティング、RIP、または OSPF を使用し、設定済みインターフェイスを介して IPv6 トラフィックを転送できます。
- IPv6 Default Router Preference（DRP; デフォルト ルータ プリファレンス）により、ホストが適切なルータを選択するための機能が向上しています。
- IPv6 トランスポートを利用する EIGRP IPv6 のサポートにより、IPv6 ピアとの通信および IPv6 ルートのアドバタイズが可能です。

レイヤ 3 VPN サービス

ここで説明する機能は、スイッチでメトロ IP アクセス イメージが稼動している場合にだけ使用できます。

- マルチ VRF CE により、サービス プロバイダーは、複数の VPN をサポートし、VPN 間で 重複した IP アドレスを使用できます。
- マルチ VRF Lite により、ネットワーク バーチャライゼーション用のプライベート ルーティング ドメインや、バーチャル プライベート マルチキャスト ネットワークを構成できます。
- VRF と EIGRP には互換性があります。

モニタリング機能

- スイッチ LED により、ポート レベルおよびスイッチ レベルのステータスを確認できます。
- 設定可能外部アラーム入力により、アラームの場合と同様、取り外された電源や故障した電源、入力のない電源を特定できます。
- MAC アドレス通知トラップおよび RADIUS アカウンティングにより、スイッチが学習または削除した MAC アドレスを保存して、ネットワークのユーザを追跡できます。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN; リモート SPAN）により、任意のポートまたは VLAN のトラフィックをモニタリングできます。
- Intrusion Detection System（IDS; 侵入検知システム）における SPAN および RSPAN のサポートにより、ネットワーク セキュリティ違反のモニタリング、対処、および報告を行えます。
- 組み込み RMON エージェントの 4 つのグループ（履歴、統計、アラーム、イベント）により、ネットワークのモニタリングとトラフィックの分析が可能です。
- Syslog 機能により、認証エラーまたは許可エラー、リソースの問題、およびタイムアウト イベントに関してシステム メッセージをロギングできます。
- レイヤ 2 traceroute により、パケットが送信元デバイスから宛先デバイスへ送られる物理パスを特定できます。
- Time Domain Reflector（TDR; タイム ドメイン反射率計）により、銅線イーサネット 10/100 ポートにおけるケーブル配線の問題の診断と解決を行います。
- SFP モジュール診断管理インターフェイスにより、SFP モジュールの物理ステータスおよび動作ステータスをモニタリングできます。
- オンライン診断により、稼動中のネットワークにスイッチを接続したまま、そのスイッチのハードウェア機能をテストできます。
- On-Board Failure Logging（OBFL; オンボード障害ロギング）により、スイッチおよびそれに接続されている電源についての情報を収集できます。
- HSRP クライアントの拡張オブジェクト トラッキング（メトロ IP アクセス イメージが必要）。
- IP Service Level Agreement（IP SLA; IP サービス レベル契約）のサポート：アクティブなトラフィック モニタリングによりネットワーク パフォーマンスを測定できます。
- IP SLA EOT により、遅延、ジッタ、パケット損失などのアクションによってトリガされる IP SLA トラッキング動作からの出力に基づいて、フェールオーバーによるスタンバイ ルータへの引き継ぎが行われます。
- EOT および IP SLA EOT スタティック ルートのサポートにより、事前設定されたスタティック ルートまたは DHCP ルートがダウンした場合に、それを検出できます。

- メトロ イーサネット対応の IP SLA により、IEEE 802.1ag イーサネット OAM 機能を使用して、メトロ イーサネット ネットワークにおける接続性、ジッタ、および遅延の検証を行えます。
- Embedded Event Manager（EEM）により、主要なシステム イベントのモニタリングとポリシーに基づいたイベント処理を行うことで、デバイスおよびシステムを管理できます。
- EEM 3.2 のサポートにより、近隣探索、ID、および MAC アドレス テーブルに関するイベントの検出が可能です。
- TWAMP 基準のサポートにより、このプロトコルをサポートする 2 つのデバイス間でラウンドトリップ ネットワーク パフォーマンスを測定できます。

スイッチ初期設定後のデフォルト設定値

スイッチはプラグアンドプレイ対応として設計されているため、基本的な IP 情報をスイッチに割り当て、そのスイッチをネットワーク内の他のデバイスに接続する以外、ユーザが行うべき作業はありません。ただし、ネットワークに対するさまざまな必要性に応じて、インターフェイス固有の設定値やシステム全体の設定値を変更できます。

（注）　CLI ベースのセットアップ プログラムを使用して IP アドレスを割り当てる方法については、ハードウェア インストール ガイドを参照してください。

スイッチの設定をまったく行わない場合、Cisco ME 3400E スイッチはデフォルト設定（表 1-1 を参照）で動作します。

表 1-1　スイッチ初期設定後のデフォルト設定値

機能	デフォルト設定	詳細
スイッチの IP アドレス、サブネット マスク、およびデフォルト ゲートウェイ	0.0.0.0	第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」
ドメイン名	なし	
パスワード	定義なし	第 5 章「スイッチの管理」
TACACS+	ディセーブル	
RADIUS	ディセーブル	
システム名およびプロンプト	*スイッチ*	
NTP	イネーブル	
DNS	イネーブル	
IEEE 802.1x	ディセーブル	第 9 章「IEEE 802.1x ポートベースの認証の設定」
DHCP		
• DHCP クライアント	イネーブル	第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」 第 20 章「DHCP 機能および IP ソース ガードの設定」
• DHCP サーバ	イネーブル（DHCP サーバとして動作するデバイスが設定されており、かつイネーブルである場合）	
• DHCP リレー エージェント	イネーブル（DHCP リレー エージェントとして動作するデバイスが設定されており、かつイネーブルである場合）	

表 1-1　スイッチ初期設定後のデフォルト設定値 （続き）

機能	デフォルト設定	詳細
ポート パラメータ		
• ポート タイプ	ギガビット イーサネット：NNI、ファスト イーサネット ポート：UNI	第 10 章「インターフェイスの設定」
• 動作モード	レイヤ 2（スイッチ ポート）	
• ポート イネーブル ステート	NNI：イネーブル、UNI および ENI：ディセーブル	
• インターフェイス速度およびデュプレックス モード	自動ネゴシエーション	
• 自動 MDIX	イネーブル	
• フロー制御	消灯	
コマンド マクロ	設定なし	第 11 章「コマンド マクロの設定」
VLAN		
• デフォルト VLAN	VLAN 1	第 12 章「VLAN の設定」
• VLAN インターフェイス モード	アクセス	
• VLAN タイプ	UNI 独立	
• プライベート VLAN	設定なし	第 13 章「プライベート VLAN の設定」
ダイナミック ARP インスペクション	すべての VLAN でディセーブル	第 21 章「ダイナミック ARP 検査の設定」
トンネリング		
• 802.1Q トンネリング	ディセーブル	第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」
• レイヤ 2 プロトコル トンネリング	ディセーブル	
スパニング ツリー プロトコル		
• STP	Rapid PVST+（VLAN 1 の NNI でイネーブル）	第 15 章「STP の設定」
• MSTP	ディセーブル（UNI ではサポートなし、ENI では設定可能）	第 16 章「MSTP の設定」
• オプションのスパニング ツリー機能	ディセーブル（UNI ではサポートなし、ENI では設定可能）	第 17 章「オプションのスパニング ツリー機能の設定方法」
レジリエント イーサネット プロトコル	設定なし	第 18 章「レジリエント イーサネット プロトコルの設定」
Flex Link	設定なし	第 19 章「Flex Link および MAC アドレス テーブル移行更新機能の設定」
DHCP スヌーピング	ディセーブル	第 20 章「DHCP 機能および IP ソース ガードの設定」
IP ソース ガード	ディセーブル	第 20 章「DHCP 機能および IP ソース ガードの設定」
IGMP スヌーピング		
• IGMP スヌーピング	イネーブル	第 22 章「IGMP スヌーピングおよび MVR の設定」
• IGMP フィルタリング	適用なし	
• IGMP クエリア	ディセーブル	
• MVR	ディセーブル	

表 1-1　スイッチ初期設定後のデフォルト設定値 （続き）

機能	デフォルト設定	詳細
IGMP スロットリング	拒否	第 22 章「IGMP スヌーピングおよび MVR の設定」
ポートベースのトラフィック制御		
• ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームの制御	ディセーブル	第 23 章「ポートベースのトラフィック制御の設定」
• 保護ポート	定義なし	
• ユニキャスト トラフィック フラッディングおよびマルチキャスト トラフィック フラッディング	ブロックなし	
• セキュア ポート	設定なし	
CDP	NNI ではイネーブル、ENI ではディセーブル、UNI ではサポートなし	第 24 章「CDP の設定」
LLDP	ディセーブル（UNI ではサポートなし）	第 25 章「LLDP および LLDP-MED の設定」
UDLD	ディセーブル	第 26 章「UDLD の設定」
SPAN および RSPAN	ディセーブル	第 27 章「SPAN および RSPAN の設定」
RMON	ディセーブル	第 28 章「RMON の設定」
syslog メッセージ	イネーブル（コンソールでのみ表示）	第 29 章「システム メッセージ ロギングの設定」
SNMP	イネーブル（バージョン 1）	第 30 章「SNMP の設定」
ACL	設定なし	第 32 章「ACL によるネットワーク セキュリティの設定」
QoS	設定なし	第 34 章「QoS の設定」
EtherChannel	設定なし	第 35 章「EtherChannel およびリンクステート トラッキングの設定」
IP ユニキャスト ルーティング		
• IP ルーティングおよび IP ルーティング プロトコル	ディセーブル	第 36 章「IP ユニキャスト ルーティングの設定」
• マルチ VRF CE	ディセーブル	
HSRP グループ（メトロ IP アクセス イメージが必要）	設定なし	第 40 章「HSRP の設定」
Cisco IOS IP SLA	設定なし	第 41 章「Cisco IOS IP SLA 動作の設定」
拡張オブジェクト トラッキング	追跡対象のオブジェクトおよびリストは未設定	第 42 章「拡張オブジェクト トラッキングの設定」
IP マルチキャスト ルーティング（メトロ IP アクセス イメージが必要）	全インターフェイスでディセーブル	第 44 章「IP マルチキャスト ルーティングの設定」
MSDP（メトロ IP アクセス イメージが必要）	ディセーブル	第 45 章「MSDP の設定」

表 1-1　スイッチ初期設定後のデフォルト設定値 （続き）

機能	デフォルト設定	詳細
イーサネット OAM		
• CFM	グローバルでディセーブル、インターフェイス単位でイネーブル	第 43 章「イーサネット OAM、CFM、および E-LMI の設定」
• E-LMI	グローバルでディセーブル	
• イーサネット OAM プロトコル（IEEE 802.3ah）	全インターフェイスでディセーブル	

ネットワークの構成例

ここでは、ネットワーク構成の概要について説明します。また、スイッチを使用して専用ネットワークセグメントを作成し、ファスト イーサネット接続およびギガビット イーサネット接続を介してそれらのセグメントを相互接続する具体例についても説明します。

- 「集合住宅のネットワークまたはイーサネット/加入者ネットワーク」（P.1-16）
- 「レイヤ 2 VPN アプリケーション」（P.1-17）
- 「マルチ VRF CE アプリケーション」（P.1-18）

集合住宅のネットワークまたはイーサネット/加入者ネットワーク

メトロ イーサネットは、都市圏で音声サービス、ビデオ サービス、およびインターネット アクセス サービスを提供するサービス プロバイダー向けのアクセス テクノロジーです。メトロ イーサネット User-facing Provider Edge（UPE; ユーザ側プロバイダー エッジ）スイッチを使用すると、帯域幅を効率的に利用できるほか、これらのサービスに必要となるセキュリティや QoS が確保されます。

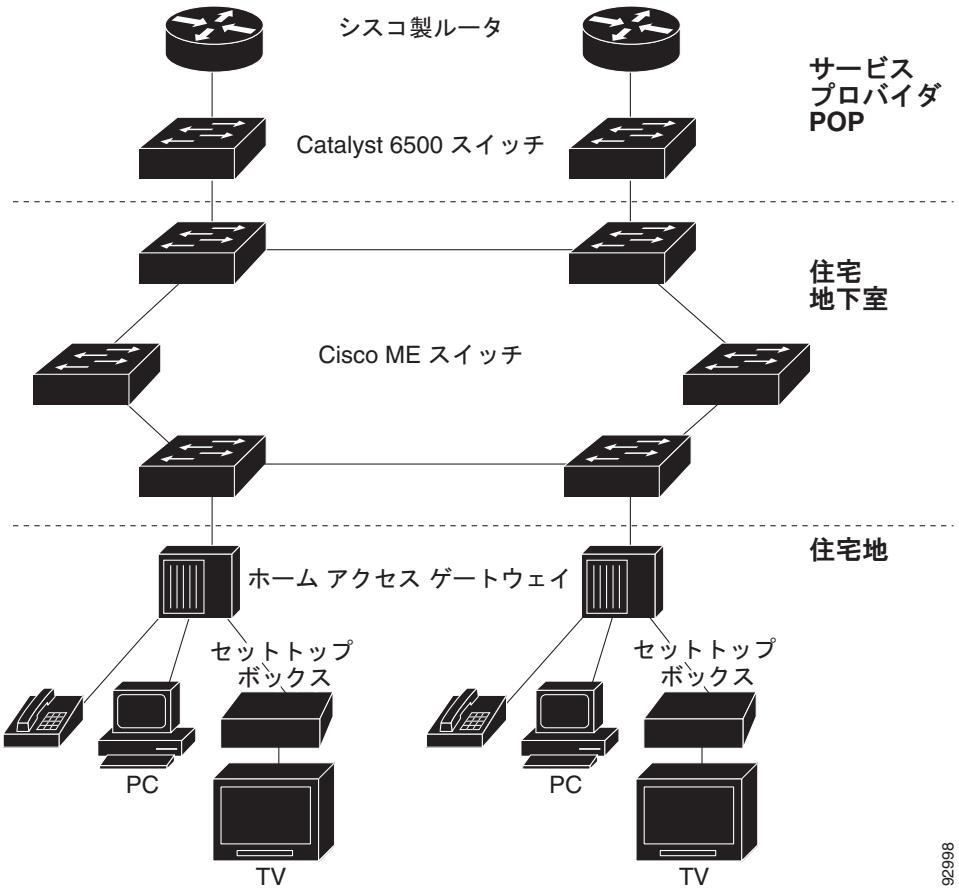
図 1-1 は、1000BASE-X SFP モジュール ポートを介して接続された Cisco ME 3400E イーサネット アクセス スイッチを使用してマルチテナント ユニットを処理する、住宅地でのギガビット イーサネット リングを示したものです。住宅側のスイッチとして Cisco ME スイッチを使用することで、カスタマーとサービス プロバイダーの Point-of Presence（POP; アクセス ポイント）との間で高速接続が実現されます。

ホーム アクセス ゲートウェイは、802.1Q トランクとして設定された UNI または ENI を介して ME スイッチに接続されます。これらのポートのデフォルト動作では、ポート間のローカル スイッチングは行えないため、加入者は相互に保護されます。また、UNI ではカスタマーからの制御プロトコルが処理されないため、DoS 攻撃を回避できます。Cisco ME スイッチは、MAC スプーフィングや IP スプーフィングを防ぐために、ポート セキュリティや IP ソース ガードなどのメカニズムも備えています。サービス プロバイダーは、高度な ACL を使用することにより、ネットワークに着信するトラフィックのタイプを細かく制御できます。

トラフィック タイプごとに異なる QoS を実現するため、Cisco ME スイッチでは、レイヤ 2 ～レイヤ 4 の情報に基づいてトラフィック タイプの特定、ポリシング、マーキング、およびスケジューリングを行えます。Cisco ME スイッチの Cisco MQC を使用することで、QoS を効率的に設定できます。入力 UNI 上でポリシング機能を設定すると、カスタマーが送信に使用できる帯域幅量を常に課金対象の範囲内に収めることができます。出力 NNI では、4 種類のキューを使用して、トラフィック タイプごとに異なるプライオリティ レベルを設定できます。1 つのキューを低遅延キューとして割り当てることにより、音声など遅延に影響されやすいトラフィックを迅速に処理できます。また、低遅延キューにレート制限を設定することにより、誤設定のために他のキューの処理が阻害されるのを回避できます。

ある VLAN のエンド ステーションが別の VLAN のエンド ステーションと通信する必要がある場合は、ルータまたはスイッチにより VLAN 内ルーティングが行われ、該当する宛先 VLAN にトラフィックがルーティングされます。VLAN ACL（VLAN マップ）を使用すると、VLAN 内セキュリティが確保され、ネットワークの重要なエリアに対する不正ユーザのアクセスを防止できます。ルータは、ファイアウォール サービス、Network Address Translation（NAT; ネットワーク アドレス変換）サービス、Voice-over-IP（VoIP）ゲートウェイ サービス、WAN アクセス、およびインターネット アクセスも提供します。

図 1-1　集合住宅構成での Cisco ME スイッチ



レイヤ 2 VPN アプリケーション

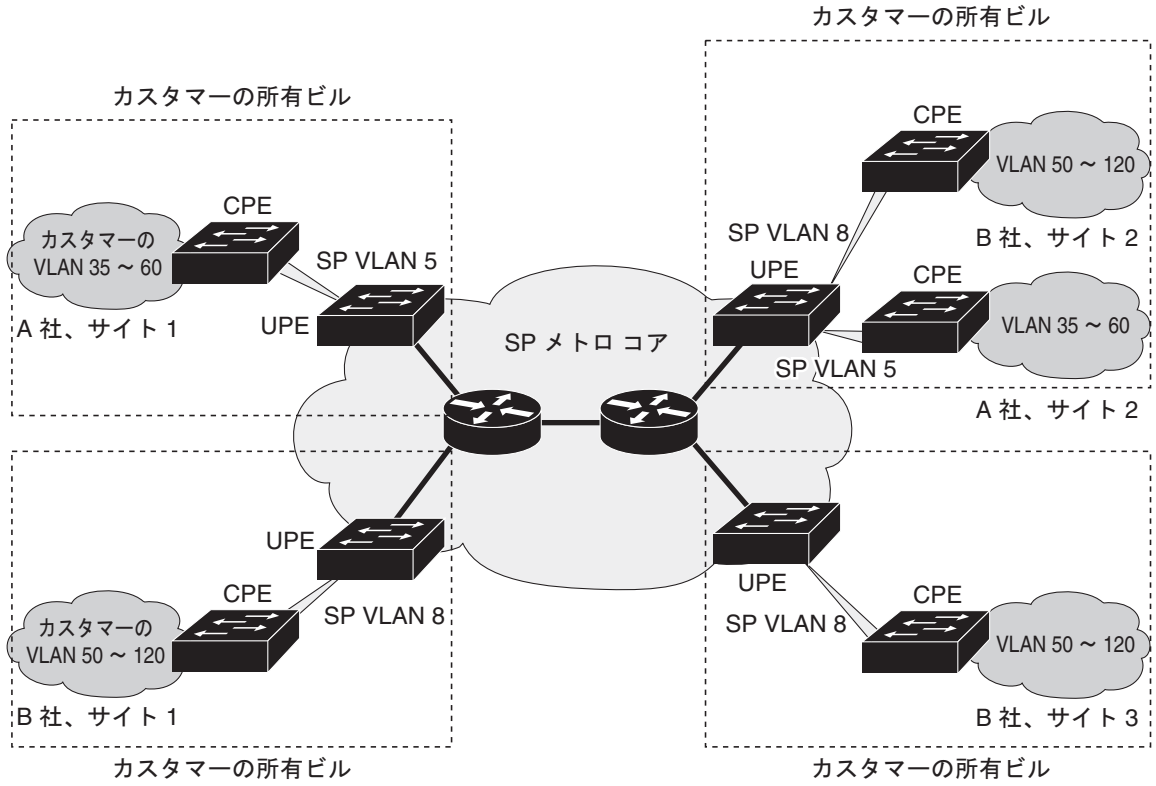
企業カスタマーは、高帯域を利用するだけでなく、プライベート ネットワークをサービス プロバイダーの共有インフラストラクチャ全体にまで拡張する必要があります。サービス プロバイダーは、WAN ネットワーク内でイーサネットを使用することにより、企業カスタマーの帯域幅要件を満たすと同時に、VPN 機能を使用してカスタマー ネットワークを拡張できます。

企業カスタマーは、レイヤ 2 VPN を使用して、サービス プロバイダーのネットワーク上に任意タイプのトラフィック を透過的に移行し、サービス プロバイダーのインフラストラクチャ上で仮想パイプを作成できます。レイヤ 3 VPN サービスとは対照的に、レイヤ 2 VPN では、企業の UPE スイッチの設定および管理を最小化することにより、運用コストが抑えられます。Cisco ME 3400 スイッチを使用してレイヤ 2 VPN を確立すれば、所在地が異なるカスタマーは互いにサービス プロバイダー ネットワークを介して情報を交換できるため、専用回線は必要なくなります。

図 1-2 では、Customer-Premises Equipment（CPE; 顧客宅内機器）スイッチに接続されたカスタマー サイトで、Cisco ME 3400E スイッチが UPE として使用されています。スイッチでは、カスタマーの IEEE 802.1Q タグの先頭にあるサービス プロバイダーの VLAN ID で、カスタマー トラフィックをタグ付けできます。Cisco ME 3400 スイッチは、二重タグをサポートすることで、カスタマーごとの仮想トンネルを実現し、カスタマー間で VLAN ID が重複しないようにします。Cisco ME 3400E スイッチは、データ プレーンを分離できるだけでなく、カスタマーの制御プロトコルをトンネリングすることもできます。スイッチは、レイヤ 2 プロトコル トンネリングを使用して、各カスタマーのコントロール プレーン トラフィックをカプセル化し、サービス プロバイダー ネットワーク上で透過的に送信します。

これらの機能の設定に関する詳細は、第 14 章「IEEE 802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

図 1-2　　レイヤ 2 VPN の構成



UPE = Cisco ME 3400 スイッチ

マルチ VRF CE アプリケーション

VPN は、共通ルーティング テーブルを共有するサイトの集合です。カスタマー サイトは、1 つまたは複数のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーでは、VPN Routing/Forwarding（VRF; VPN ルーティングおよび転送）テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスが関連付けられます。サービス プロバイダーは、マルチ VRF CE を使用することで、IP アドレスが重複した複数の VPN をサポートできます。

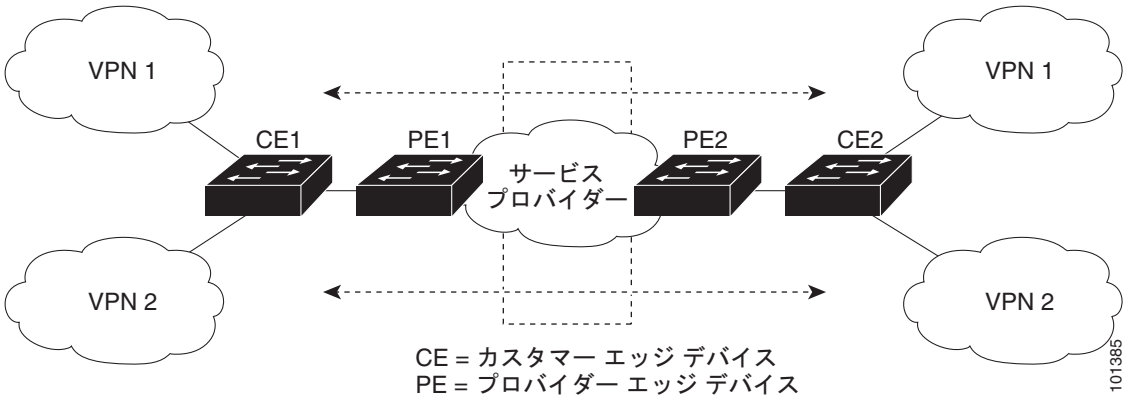
マルチ VRF CE には、次のようなデバイスがあります。

- Customer edge（CE; カスタマー エッジ）：カスタマーは、CE デバイスにより、1 つまたは複数の Provider Edge（PE; プロバイダー エッジ）ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカル ルートをルータにアドバタイズし、そのルータからリモート VPN ルートを学習します。Cisco ME 3400 スイッチは CE デバイスとして使用できます。
- Provider edge（PE; プロバイダー エッジ）：PE ルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CE デバイスとルーティング情報を交換します。PE は、直接接続された VPN の VPN ルートを維持するためだけに必要です。サービス プロバイダー VPN ルートのすべてを維持する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。
- CE デバイスに接続していないサービス プロバイダー ネットワークのルータは、プロバイダー ルータやコア ルータになります。

マルチ VRF CE では、複数のカスタマーが 1 つの CE を共有でき、CE と PE の間ではただ 1 つの物理リンクが使用されます。共有 CE は、カスタマーごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、カスタマーごとにパケットをスイッチングまたはルーティングします。マルチ VRF CE は、制限付きの PE 機能を CE デバイスに拡張して、別々の VRF テーブルを維持し、VPN のプライバシおよびセキュリティを支店に拡張します。

図 1-3 は、Cisco ME 3400E スイッチを複数の仮想 CE として使用した構成を示したものです。このシナリオは、中小企業など、VPN サービスの帯域幅要件が低いカスタマーに適しています。このような場合、Cisco ME スイッチではマルチ VRF CE のサポートが必要です。マルチ VRF CE はレイヤ 3 機能であるため、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスであることが必要です。

図 1-3　　複数の仮想 CE



マルチ VRF CE の詳細は、「マルチ VRF CE の設定」（P.36-88）を参照してください。

次の作業

スイッチの設定の前に、スタートアップ情報について次の章を参照してください。

- 第 2 章「CLI の使用方法」
- 第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」
- 第 4 章「Cisco IOS Configuration Engine の設定」