概要

この章では、Catalyst 3750 Metro スイッチ ソフトウェアの概要を説明します。具体的な内容は次のとおりです。

機能

（注）　この章で取り上げる一部の機能は、スイッチ ソフトウェア イメージの暗号化バージョン（つまり、暗号化をサポートするバージョン）のみに対応しています。この機能を使用するには、その許可を取得し、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、現リリースのリリースノートを参照してください。

Catalyst 3750 Metro スイッチには、次の機能があります。

パフォーマンスの特長

- ポートの速度を自動検出し、すべてのスイッチ ポートでデュプレックス モードの自動ネゴシエーションを実行して、帯域利用を最適化
- 10/100 Mbps インターフェイスおよび 10/100/1000 BASE-T/TX Small Form-Factor Pluggable（SFP）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オーバー）を自動的に検出し、適切に接続を設定
- 最大 1546 バイトでフレームのルーティングをサポート。ハードウェアでブリッジングされたフレームでは最大 9000 バイト、ソフトウェアでブリッジングされたフレームでは最大 2000 バイトをサポート
- すべてのポートでの 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）
- EtherChannel により、フォールトトレランスを高め、スイッチ、ルータ、およびサーバ間に最大 2 Gbps（Gigabit EtherChannel）または 800 Mbps（Fast EtherChannel）全二重の帯域幅を確保
- EtherChannel リンク自動作成用 Link Aggregation Control Protocol（LACP）および Port Aggregation Protocol（PAgP）
- ブロードキャスト、マルチキャスト、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
- 不明のレイヤ 2 ユニキャスト、マルチキャスト、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のポート ブロッキング
- Cisco Group Management Protocol（CGMP）サーバのサポートおよび Internet Group Management Protocol（IGMP）バージョン 1、バージョン 2、バージョン 3 対応の IGMP スヌーピング
  - （CGMP デバイスの場合）CGMP が特定のエンド ステーションへのマルチキャスト トラフィックを制限し、ネットワーク全般のトラフィックを軽減

- （IGMP デバイスの場合）IGMP スヌーピングによってマルチメディア トラフィックとマルチキャスト トラフィックを効率的に転送

- Multicast VLAN Registration（MVR）により、マルチキャスト VLAN（仮想 LAN）内でマルチキャスト ストリームを継続的に送信しながら、加入者 VLAN からストリームを隔離して帯域およびセキュリティを確保
- 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
- IGMP 転送テーブルにエントリの最大数が存在する場合のアクションを設定する IGMP スロットリング
- マルチキャスト ルータ クエリー単位で IGMP レポート 1 つのみをマルチキャスト デバイスへ送信する IGMP レポート抑制（IGMPv1 または IGMPv2 クエリーでのみサポート）
- Switch Database Management（SDM）テンプレートによる、ユーザ側で選択する機能へのサポートを最大化するシステム リソースの割り当て

管理オプション

- CLI — Catalyst 3750 Metro スイッチの機能をサポートするように、Cisco IOS CLI（コマンドライン インターフェイス）ソフトウェアが機能拡張されています。CLI にアクセスするには、管理ステーションをスイッチのコンソール ポートに直接接続するか、リモート管理ステーションから Telnet 経由で接続します。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。
- CNS — Cisco Configuration Engine は、ネットワーク デバイスおよびサービスの展開と管理を自動化するためのコンフィギュレーション サービスとして動作するネットワーク管理ソフトウェアです。スイッチ固有の設定変更を生成し、その変更をスイッチに送信し、設定変更を実行して結果をロギングすることによって、初期設定および設定のアップデートを自動的に実行できます。

  CNS の詳細については、第 5 章「Cisco IOS CNS エージェントの設定」を参照してください。
- SNMP — CiscoWorks2000 LAN Management Suite（LMS）や HP OpenView などの SNMP（簡易ネットワーク管理プロトコル）管理アプリケーション。HP OpenView や SunNet Manager などのプラットフォームが稼働している 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 MIB（管理情報ベース）セットおよび 4 種類の Remote Monitoring（RMON）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）　ここで説明する暗号化 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のみ使用可能です。

- Cisco IE2100 シリーズ CNS 組み込みエージェントは、スイッチ管理、コンフィギュレーションの保存および配布を自動化します。
- Dynamic Host Configuration Protocol（DHCP）は、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を自動化します。
- 加入者 ID および IP アドレス管理の DHCP リレー エージェント情報（Option 82）
- DHCP サーバは、IP アドレスおよびその他 DHCP オプションを IP ホストへ自動的に割り当てます。

- ユニキャスト要求を DNS サーバへ転送し、IP アドレスおよび対応ホスト名からスイッチを識別したり、ユニキャスト要求を TFTP サーバへ転送し、TFTP サーバからソフトウェア アップグレードを管理したりします。
- Web ブラウザ（HTTP）を使用して、ソフトウェア イメージのダウンロードをサポートします。
- Address Resolution Protocol（ARP）により、IP アドレスおよび対応 MAC（メディア アクセス制御）アドレスからスイッチを識別します。
- ユニキャスト MAC アドレス フィルタリングは、特定の送信元または宛先 MAC アドレスを使用して、パケットを廃棄します。
- 設定可能な MAC アドレス スケーリングにより、VLAN 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することができます。
- Cisco Discovery Protocol（CDP）バージョン 1 およびバージョン 2 により、ネットワーク トポロジーの検出と、ネットワーク上の他のシスコ デバイスとスイッチ間のマッピングを行います。
- Network Time Protocol（NTP）により、外部ソースから全スイッチに一貫したタイムスタンプを提供します。
- 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 システムに対する単一のインターフェイスを実現します。
- ネットワーク上の複数の CLI セッションに対する、最大 16 の同時 Telnet 接続によって帯域内管理が可能です。
- ネットワーク上の複数の CLI セッションに対する、最大 5 つの暗号化された同時 SSH 接続によって帯域内管理が可能です（スイッチ ソフトウェア イメージの暗号化バージョンが必要です）。
- SNMP バージョン 1、2、3 の get および set 要求を使用して帯域内管理が可能です。
- スイッチのコンソール ポートから、直接接続された端末、またはシリアル接続またはモデム経由でのリモート端末へのアクセスによって帯域外管理が可能です。
- Metro イーサネットの Operation, Administration, and Maintenance（OAM; 操作、管理、メンテナンス）、IEEE 802.1ag Connectivity Fault Management（CFM; 接続障害の管理）、および Ethernet Line Management Interface（E-LMI; イーサネット回線管理インターフェイス）のサポート

アベイラビリティ機能

- HSRP により、コマンド スイッチとレイヤ 3 ルータの冗長性を確立します。
- UniDirectional Link Detection（UDLD; 単一方向リンク検出）およびアグレッシブ UDLD が、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一方向リンクを検出しディセーブル化します。
- 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およびループフリー ネットワークを実現します。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 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
  - UplinkFast および BackboneFast によって、スパニングツリー トポロジーの変更後に高速コンバージェンスを実行し、ギガビット アップリンクなどの冗長アップリンク間のロードバランシングを実現
- IEEE 802.1s Multiple Spanning-Tree Protocol（MSTP）が、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し、データ トラフィックとロード バランシング用の複数の転送パスを提供します。さらに、IEEE 802.1w Rapid Spanning-Tree Protocol（RSTP）に基づき、Rapid Per-VLAN Spanning-Tree plus（Rapid PVST+）が、ルートと Designated Port（DP; 指定ポート）を即座にフォワーディング ステートに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を実行します。

- PVST+、Rapid-PVST+、および MSTP モードで利用できるオプションのスパニングツリー機能は次のとおりです。
  - PortFast — 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
  - BPDU ガード — Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を受信する PortFast 対応ポートをシャットダウン
  - BPDU フィルタリング — PortFast 対応ポートが BPDU を送受信するのを防止
  - 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 — 単一方向リンクとなる障害によって代替ポートまたはルート ポートが DP として使用されるのを防止
- 等価コスト ルーティングにより、リンクレベルとスイッチレベルの冗長性を確立します。
- Flex Link レイヤ 2 インターフェイスは、基本リンク冗長性のため STP に対する代替として相互にバックアップします。
- リンクステート トラッキングで、接続されたホスト、サーバ、および他のダウンストリーム デバイスからのアップストリーム トラフィックを搬送するポートのステートをミラーリングします。この機能で、他のシスコ製イーサネット スイッチで動作しているリンクへのダウンストリーム トラフィックのフェールオーバーが可能となります。

VLAN 機能

- 最大 1005 の VLAN をサポートし、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 にユーザを割り当てます。
- IEEE 802.1Q 規格によって許可された 1 ～ 4094 の全範囲の VLAN ID をサポートします。
- VLAN Query Protocol（VQP）— ダイナミック VLAN メンバーシップ対応
- 全ポートでの ISL（スイッチ間リンク）および IEEE 802.1Q トランキング カプセル化によるネットワークの移動、追加、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 セキュリティを実現します。
- Dynamic Trunking Protocol（DTP）— 2 つのデバイス間のリンクでのトランキングのネゴシエーション、および使用するトランキング カプセル化タイプ（802.1Q または ISL）のネゴシエーションを行います。
- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）および VTP プルーニング — フラッディングしたトラフィックをそのトラフィックの受信先に通じるリンクに限定することにより、ネットワーク トラフィックを削減します。
- 音声 VLAN — Cisco IP Phone からの音声トラフィック用のサブネットを作成します。
- VLAN 1 の最小化 — VLAN 1 を任意の個々の VLAN トランク リンクでディセーブル化することで、スパニングツリー ループまたはストームのリスクを軽減。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、引き続き制御プロトコル フレームを送受信します。
- プライベート VLAN — VLAN スケーラビリティ問題に対処し、制御された IP アドレスを割り当て、レイヤ 2 ポートをスイッチの他のポートから切り離します。
- Enhanced-Services（ES）ポート上の VLAN マッピング — カスタマー VLAN をサービス プロバイダー VLAN に変換し、カスタマー VLAN ID に影響を与えずにサービス プロバイダー ネットワーク経由でパケットをトランスポートできるようにします。
- カスタム ethertype — タグ付きおよびタグなしトラフィックをさまざまな VLAN に転送できるよう、ユーザ側でポートの ethertype 値を任意の値に変更できます（ES ポートのみ）。

レイヤ 2 VPN サービス

- 802.1Q トンネリングにより、サービス プロバイダー ネットワーク経由でリモート サイトにユーザを擁するカスタマーの VLAN を、他のカスタマーから隔離された状態に保つことができます。また、トランク ポート、アクセス ポート、またはトンネル ポートでのレイヤ 2 プロトコル トンネリングにより、カスタマー ネットワークの全ユーザに関する完全な STP、CDP、VTP 情報が確保されます。
- レイヤ 2 ポイントツーポイント トンネリング — EtherChannel を自動的に作成できます。
- レイヤ 2 プロトコル トンネリング バイパス機能により、サード パーティ ベンダーとのインターオペラビリティが提供されます。
- インテリジェント 802.1Q トンネリング QoS — 802.1Q トンネリング用に、内部の Cost-of-Service（CoS）値を外部の CoS 値にコピーする機能です。
- Ethernet over Multiprotocol Layer Switching（EoMPLS）トンネリング メカニズムのサポート — サービス プロバイダー MPLS ネットワーク経由でイーサネット フレームをトランスポートします。
- 階層構造の仮想プライベート LAN サービス（H-VPLS）のサポート — IEEE 802.1Q トンネリングまたは Ethernet over MPLS（EoMPLS）を使用します。

レイヤ 3 VPN サービス

- MPLS Virtual Private Network（VPN; 仮想私設網）のサポート — ビジネス カスタマー向けにスケーラブルなレイヤ 3 VPN サービスを展開および管理するための機能を提供します。各 VPN は、VPN メンバーシップを定義するルーティング テーブルおよびフォワーディング テーブルを含む 1 つまたは複数の VPN Routing/Forwarding（VRF）インスタンスに対応付けられます（MPLS VPN は、ES ポート上でのみサポートされます）。
- Customer Edge（CE; カスタマー エッジ）デバイス上の複数 VPN マルチ VRF インスタンスによって、サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複させることができます。

セキュリティ機能

（注）　ここで説明する 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のみ使用可能です。

- パスワードによって保護される管理インターフェイスへの読み取り専用および読み書きアクセス（設定の不正変更を防止するため）
- セキュリティ レベル、通知、および対応動作を選択できるマルチレベルのセキュリティ
- セキュリティ確保のためのスタティック MAC（メディア アクセス制御）アドレス指定
- 同一スイッチ上の DP へのトラフィック転送を制限する保護ポート オプション
- 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されたステーションの MAC アドレスを制限および識別
- ポート上のセキュア　アドレス用にエージング　タイムを設定するためのポート　セキュリティ　エージング
- BPDU ガードが、無効な設定の発生時に PortFast が設定されたポートをシャットダウン
- 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

- 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
- VLAN ACL（VLAN マップ）により、MAC、IP、および TCP/UDP ヘッダー内の情報に基づく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
- 送信元および宛先 MAC ベースの ACL により、非 IP トラフィックをフィルタリング処理
- 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
  - 802.1x と VLAN 割り当てにより、802.1x 認証ユーザを指定した VLAN に制限
  - 802.1x とポート セキュリティにより、802.1x ポートへのアクセスを制限
  - 802.1x と音声 VLAN により、ポートの許可または無許可ステートに関係なく、IP Phone は音声 VLAN にアクセス可能
  - 802.1x とゲスト VLAN により、非 802.1x 準拠のユーザに限定されたサービスを提供
  - 802.1x アカウンティングにより、ネットワーク使用を監視
- TACACS+ — TACACS サーバを使用してネットワーク セキュリティを管理する独自仕様の機能
- 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、アクションの追跡を実行
- Kerberos セキュリティ システムにより、信頼できるサードパーティを使用して、ネットワーク リソースへの要求を認証（スイッチ ソフトウェア イメージの暗号化［つまり、暗号化をサポートする］バージョンが必要）
- パスワード回復ディセーブル機能により、カスタマー サイトのスイッチへのアクセスを保護
- DHCP スヌーピングにより、untrusted ホストと DHCP サーバの間の untrusted DHCP メッセージをフィルタリング
- 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 ソース バインディングに基づきトラフィックをフィルタリングすることで、非ルーテッド インターフェイス上のトラフィックを制限
- Dynamic ARP Inspection（DAI）により、無効な ARP 要求および応答を同じ VLAN 内の他のポートにリレーしないことで、スイッチ上の意図的な攻撃を排除
- Secure Socket Layer（SSL）バージョン 3.0 では、HTTP 1.1 サーバ認証、暗号化、メッセージ整合性をサポート。HTTP クライアント認証によりセキュア HTTP 通信が可能（スイッチ イメージの暗号化バージョンが必要）

QoS 機能

- 標準 Quality of Service（QoS; サービス品質）による、標準ポートまたは ES ポート上での着信トラフィックの分類、ポリシング、マーキング、キューイング、およびスケジューリングと、標準ポート上での発信トラフィックのキューイングおよびスケジューリング

  分類
  - ポート単位の IP Type Of Service/Differentiated Services Code Point（IP ToS/DSCP）および 802.1p CoS プライオリティ マーキング — ポート単位でのミッションクリティカルなアプリケーションのパフォーマンスを保護
  - フローベースのパケット分類（MAC、IP、および TCP/UDP ヘッダー内の情報に基づく分類）に基づく IP ToS/DSCP および 802.1p CoS マーキング — ネットワーク エッジでの高性能な QoS を実現し、各種ネットワーク トラフィックに応じて区別化したサービス レベルを可能にし、ネットワーク内のミッションクリティカルなトラフィックを優先
  - ポート信頼状態 — QoS ドメイン内のポート、および別の QoS ドメインとの境界ポートにおける状態（CoS、DSCP、および IP precedence）
  - 信頼境界機能 — Cisco IP Phone の存在を検出し、受信した CoS 値を信頼して、ポート セキュリティを確保

- DSCP トランスペアレンシ — QoS がイネーブルの場合にスイッチがユーザ IP パケットの DSCP フィールドを書き換えるのを防止

ポリシングおよび不適合パケットのマーキング

- スイッチ ポートに関するトラフィックポリシング ポリシー — 特定のトラフィック フローに割り当てるポート帯域幅を管理（シングルレート トラフィック ポリシング）
- 集約ポリシング — 特定のアプリケーションまたはトラフィック フローを規定または事前定義されたレートに制限する、全体でのトラフィック フローのポリシング
- 帯域利用限度を超える不適合パケットに対するマークダウン（廃棄ポリシー　アクションは、パケットを変更なしで通過させる、パケットに割り当てられた DSCP 値をマークダウンする、またはパケットを廃棄する）

入力キューイングおよびスケジューリング

- ユーザ トラフィック用の 2 つの設定可能な入力キュー（1 つはプライオリティキューとして使用できる）
- Weighted Tail Drop（WTD）— 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する輻輳回避メカニズム
- Shaped Round Robin（SRR）— パケットがキューから内部リングへ送出されるときのレートを決定するスケジューリング サービス（入力キューでサポートされる唯一のモードはシェアリング）

出力キューとスケジューリング

- ポートあたり 4 つの出力キュー
- 標準ポート上の出力プライオリティ キュー。SRR はこのキューを空になるまで処理してから、ほかの 3 個のキューを処理します。
- WTD — 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する輻輳回避メカニズム
- SRR — パケットがキューから出力インターフェイスへ送出されるときのレートを決定するスケジューリング サービス（出力キューでは、シェーピングまたはシェアリングがサポートされる）。シェイプド出力キューは保証されるが、割り当てられたポート帯域幅の使用に制限されています。また、シェアド出力キューも設定済みの帯域幅の割り当てが保証されているが、他のキューが空でその帯域幅の割り当て分を使用していない場合には保証以上の帯域幅を使用できます。

- ES ポート上の階層型 QoS — 着信または発信トラフィックの分類、ポリシング、マーキング、キューイング、およびスケジューリング

分類

- 階層構造の 3 レベルの QoS 設定：クラス、VLAN、および物理インターフェイス
- CoS 値、DSCP 値、IP precedence 値、MPLS Experimental（EXP）ビット、または VLAN に基づく分類

ポリシングおよび不適合パケットのマーキング

- Committed Information Rate（CIR; 認定情報速度）および Peak Information Rate（PIR）に基づく 2 レートのトラフィック ポリシング
- 帯域利用限度を超える不適合パケットに対するマークダウン（ポリシー アクションは、適合するパケットを変更なしで送信する、超過したパケットのプライオリティをマークダウンする、または違反したパケットを廃棄する）

出力キューイングおよびスケジューリング

- 各パケットをトラフィック クラスおよび VLAN に基づいて出力キューに割り当て
- 輻輳回避メカニズムとしての Weighted Random Early Detection（WRED; 重み付きランダム早期検出）
- キュー スケジューリング管理機能としての Class-Based Weighted Fair Queueing（CBWFQ; クラス ベース均等化キューイング）— 遅延に影響されやすい特定のトラフィック クラス（音声など）への帯域を保証し、ネットワーク上の他の全トラフィックを公平に処理

  - スケジューリング輻輳管理機能としての Low-Latency Queueing（LLQ）— 特定のトラフィック クラスに完全優先キューイングを提供し、遅延に影響されやすいデータ（音声など）を他のキューのパケットよりも先に送信
  - トラフィック シェーピングにより、インターネット トラフィックのバースト性を軽減
- Automatic QoS（Auto-QoS）により、トラフィックの分類と出力キューの設定により既存の QoS 機能の展開を簡略化

レイヤ 3 機能

- HSRP — レイヤ 3 ルータの冗長性
- IP ルーティング　プロトコルによるロードバランシングとスケーラブルなルーテッド　バックボーンの構築
  - RIP バージョン 1 および 2
  - OSPF
  - Enhanced Interior Gateway Routing Protocol（EIGRP）
  - Border Gateway Protocol（BGP）バージョン 4
  - International Organization for Standardization（ISO; 国際標準化機構）Connectionless Network Service（CLNS）。スイッチは ISO IGRP および Intermediate System-to-Intermediate System（IS-IS）ルーティングをサポートしています。
- 2 つ以上の VLAN 間の完全レイヤ 3 ルーティング対応の IP ルーティング（VLAN 間ルーティング）により、各 VLAN が独自の自律データリンク ドメインのメンテナンスが可能
- Policy-Based Routing（PBR）— トラフィック フローに定義済みポリシーを設定
- Customer Edge（CE; カスタマー エッジ）デバイス上の複数の multiple VPN Routing/Forwarding（multi-VRF）インスタンスによって、サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複させることができます（EMI が必要）。
- 代替ブリッジングによる 2 つ以上の VLAN 間での非 IP トラフィックの転送
- スタティック IP ルーティングによるネットワーク パス情報のルーティング テーブル手動作成
- 等コスト ルーティングによるロードバランシングおよび冗長構成
- Internet Control Message Protocol（ICMP）および ICMP Router Discovery Protocol（IRDP）— ルータのアドバタイズおよびルータ請求メッセージによる直接接続サブネット上のルータのアドレス検索
- Protocol-Independent Multicast（PIM）によるネットワーク内マルチキャスト ルーティング。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 フィードの受信が可能になり、マルチキャストに参加しないスイッチのプルーニングが可能になります。PIM Sparse Mode（PIM-SM）、PIM Dense Mode（PIM-DM）、および PIM Sparse-Dense モードのサポートも含まれます
- Multicast Source Discovery Protocol（MSDP）— 複数の PIM-SM ドメインを接続
- Distance Vector Multicast Routing Protocol（DVMRP）トンネリング — 非マルチキャスト ネットワークでの 2 つのマルチキャスト対応ネットワークの相互接続
- DHCP リレーによる、IP アドレス要求など DHCP クライアントからの UDP ブロードキャストの転送

モニタ機能

- 各種スイッチ LED による、ポート レベルおよびスイッチ レベルでのステータス表示
- MAC アドレス通知トラップと RADIUS アカウンティング — スイッチが確認または削除した MAC アドレスの保存による、ネットワークのユーザ追跡
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN）による、任意の標準ポートまたは VLAN のトラフィック モニタリング

（注）　ES ポートを SPAN 送信元にすることはできません。

- Intrusion Detection System（IDS）における SPAN および RSPAN のサポート — ネットワーク セキュリティ違反のモニタ、撃退、およびレポート
- 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）による、ネットワーク モニタとトラフィック分析
- Syslog 機能による、認証または許可エラー、リソースの問題、およびタイムアウト イベントに関するシステム メッセージのロギング
- レイヤ 2 traceroute — 送信元デバイスから宛先デバイスまでにパケットが通過する物理パスを識別
- SFP モジュール診断管理インターフェイス — SFP モジュールの物理または動作ステータスをモニタ

初期スイッチ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、ユーザが必要なのは基本 IP 情報をスイッチに割り当て、それをネットワーク内の他のデバイスに接続するだけです。特定のネットワーク ニーズがある場合には、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。

スイッチを全く設定しなかった場合は、スイッチは表 1-1 に記されたデフォルト設定で動作します。この表は、主要なソフトウェア機能、それらのデフォルト値、その機能に関する情報の参照先を一覧にしたものです。

表 1-1　初期スイッチ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、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 6 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	*Switch*	
NTP	イネーブル	
DNS	イネーブル	
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（DHCP サーバとして動作するデバイスが設定されていてイネーブルである場合のみ）	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 21 章「DHCP 機能および IP ソース ガードの設定」
DHCP サーバ		
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いてイネーブルである場合のみ）	
ポート パラメータ		
動作モード	レイヤ 2（スイッチポート）	第 10 章「インターフェイス特性の設定」
ポート イネーブル ステート	すべてのポートでイネーブル	
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	
Auto-MDIX	ディセーブル	
フロー制御	オフ	
VLAN		
デフォルト VLAN	VLAN 1	第 12 章「VLAN の設定」
VLAN トランキング	ダイナミック自動（DTP）	
トランク カプセル化	ネゴシエーション	
VTP モード	サーバ	第 13 章「VTP の設定」
VTP バージョン	1	
音声 VLAN	ディセーブル	第 15 章「音声 VLAN の設定」
プライベート VLAN	設定なし	第 14 章「プライベート VLAN の設定」

表 1-1　初期スイッチ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
ダイナミック ARP 検査	全 VLAN でディセーブル	第 22 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 16 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」
VLAN マッピング	ディセーブル	
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	PVST+ が VLAN 1 でイネーブル	第 17 章「STP の設定」
MSTP	ディセーブル	第 18 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	第 19 章「オプションのスパニングツリー機能の設定」
Flex Link	設定なし	第 20 章「Flex Link および MAC Address-Table Move Update Feature の設定」
DHCP スヌーピング	ディセーブル	第 21 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 21 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 23 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	
MVR	ディセーブル	
IGMP スロットリング		
IGMP スロットリング	拒否	第 23 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		
ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御	ディセーブル	第 24 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	
ユニキャストおよびマルチキャスト フラッディング	ブロックされない	
セキュア ポート	設定なし	
CDP	イネーブル	第 25 章「CDP 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、コンソール上に表示	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 31 章「ACL によるネットワーク セキュリティの設定」
QoS	ディセーブル	第 32 章「QoS の設定」
EtherChannels	設定なし	第 33 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		

表 1-1　初期スイッチ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
IP ルーティング（およびルーティングプロトコル）	ディセーブル	第 34 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	
MPLS サービス		
ラベル スイッチング	グローバルではイネーブル、インターフェイス単位ではディセーブル	第 37 章「MPLS および EoMPLS の設定」
EoMPLS	設定なし	
MPLS QoS	ディセーブル	
H-VPLS	VFI は設定なし	
HSRP グループ	設定なし	第 35 章「HSRP の設定」
IP マルチキャスト ルーティング	全インターフェイスでディセーブル	第 38 章「IP マルチキャスト ルーティングの設定」
MSDP	ディセーブル	第 39 章「MSDP の設定」
代替ブリッジング	設定なし	第 40 章「代替ブリッジングの設定」
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 36 章「イーサネット CFM および E-LMI の設定」
E-LMI	グローバルでディセーブル	

ネットワーク構成の例

ここでは、ネットワーク構成の概要について説明し、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 イーサネットおよびギガビット イーサネット接続でセグメントを相互接続する例を示します。

集合住宅用または Ethernet-to-the Subscriber ネットワーク

図 1-1 は、複数のテナントがある集合住宅向けに、1000BASE-X SFP モジュール ポート経由で接続した Catalyst 3750 Metro スイッチで構成されるギガビット イーサネット リングを示しています。住宅用スイッチとして使用する Catalyst 3750 Metro スイッチによって、サービス プロバイダーの POP への高速接続をユーザに提供します。既存の電話回線を使用した接続が必要なユーザの場合には、住宅用スイッチとして Catalyst 2950 Long-Reach Ethernet（LRE）スイッチを使用することもできます。その場合、Catalyst 2950 LRE スイッチを別の住宅用スイッチ（Catalyst 3750 Metro スイッチなど）に接続できます。Catalyst LRE スイッチおよび LRE の詳細については、Catalyst 2950 LRE マニュアル セットを参照してください。

住宅用スイッチ（および使用されている場合、Catalyst 2950 LRE スイッチ）上のすべてのポートは、プライベート VLAN エッジ（保護ポート）および STP ルート ガード機能がイネーブルに設定された 802.1Q トランクとして設定されています。保護ポート機能は、加入者が他の加入者宛パケットを表示できないように、スイッチ上の各ポートを分離して、セキュリティを確保します。STP ルート ガードは、許可されていないデバイスが STP ルート スイッチとして使用されるのを防止します。マルチキャスト トラフィックを管理するために、すべてのポートで IGMP スヌーピングまたは CGMP をイネーブルに設定します。集約スイッチへのアップリンク ポート上の ACL が、セキュリティと帯域幅の管理を行います。

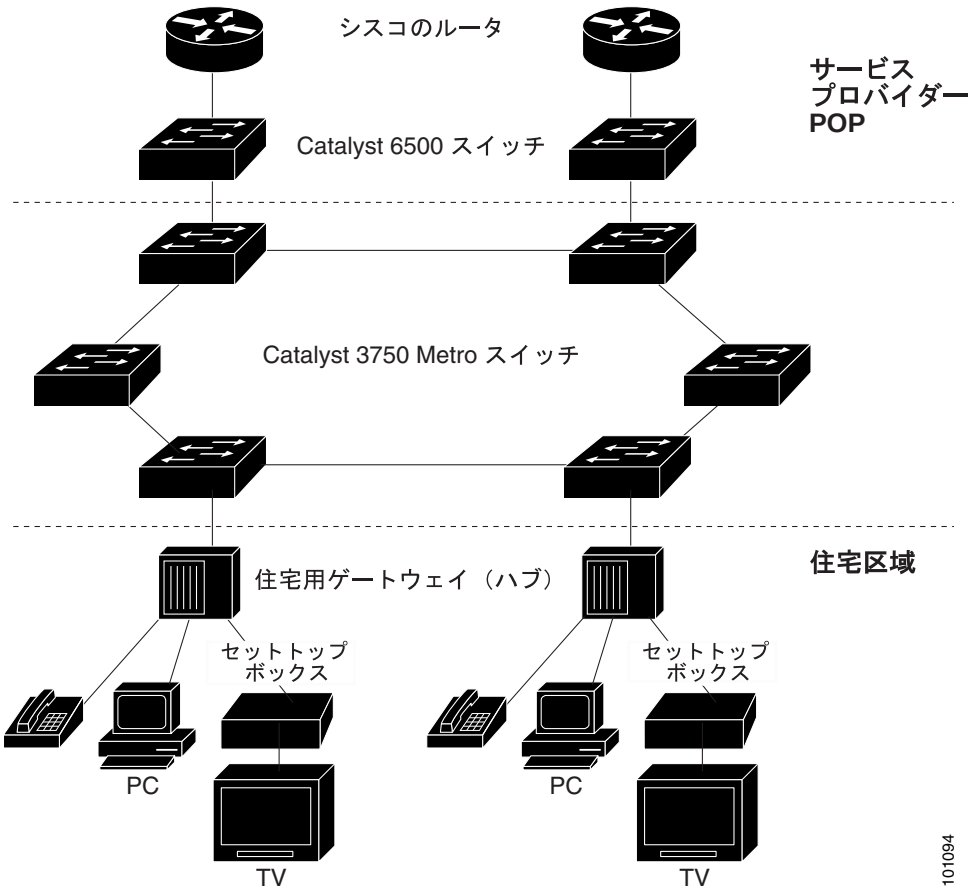
集約スイッチおよびルータには、ロードバランシングおよび冗長接続がイネーブルになるよう HSRP を設定して、ミッションクリティカルなトラフィックを保証します。これにより、ルータまたはスイッチの 1 つに障害が発生した場合でも、インターネット、WAN、およびミッションクリティカルなネットワーク リソースへの接続が保証されます。

1 つの VLAN のエンド ステーションが別の VLAN にあるエンド ステーションと通信する必要がある場合、ルータまたはスイッチが該当する宛先 VLAN にトラフィックをルーティングし、VLAN 間ルーティングを提供します。VLAN ACL（VLAN マップ）は VLAN 内セキュリティを設定し、不正ユーザがネットワークの重要な部分にアクセスしないようにします。

VLAN 間ルーティングのほかに、DSCP などのスイッチ QoS メカニズムを使用して各種ネットワーク トラフィックに優先順位を付け、予測可能な方法でハイ プライオリティ トラフィックを配信します。輻輳が発生した場合、QoS はロー プライオリティ トラフィックを廃棄してハイ プライオリティ トラフィックを配信できるようにします。

ルータはさらに、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 およびインターネットのアクセスも提供します。

図 1-1　集合住宅用構成の Catalyst 3750 Metro スイッチ



レイヤ 2 VPN アプリケーション

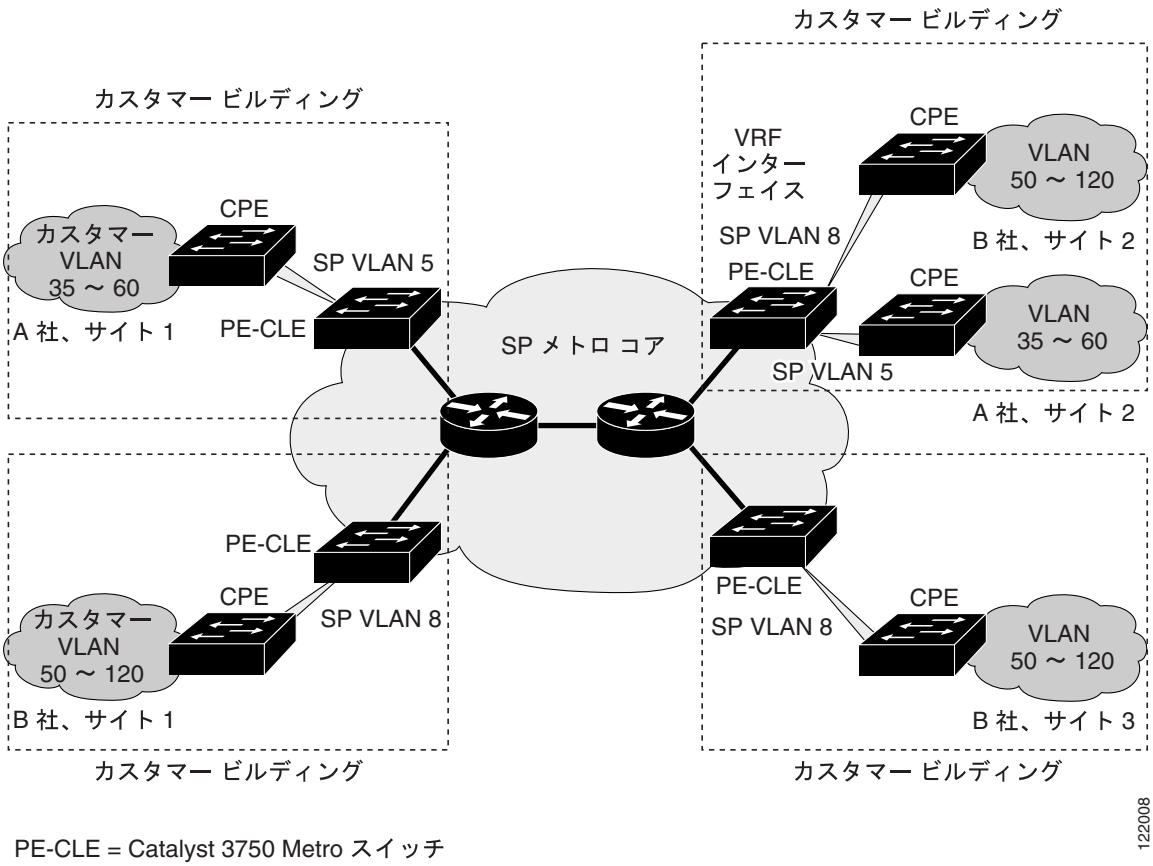
Catalyst 3750 Metro スイッチを使用してレイヤ 2 VPN を構成し、さまざまな場所にいるユーザ同士が専用接続なしでサービス プロバイダー ネットワークを通じて情報を交換可能にできます。IEEE 802.1Q およびレイヤ 2 プロトコル トンネリング機能は、ネットワーク上で複数のカスタマー トラフィックを伝送し、各カスタマーの VLAN およびレイヤ 2 プロトコル設定を他のカスタマー トラフィックへの影響なしで維持する必要のあるサービス プロバイダー向けに設計された機能です。

Customer Premises Equipment（CPE; カスタマー側装置）スイッチに接続するプロバイダー ネットワークの両エッジで、Catalyst 3750 Metro スイッチをカスタマー サイトの Provider Edge Customer-located Equipment（PE-CLE）として使用します。PE スイッチは、サービス プロバイダー ネットワークに着信するパケットをカスタマー VLAN ID でタグ付けします。VLAN マッピングによって各カスタマー VLAN ID がサービス プロバイダー VLAN ID に変換され、サービス プロバイダー ネットワーク経由でのトランスポートが可能になります。出力側の PE インターフェイスでは、出力 PE スイッチがカスタマー ネットワーク用に元の VLAN ID 番号を復元します。

サービス プロバイダーは 802.1Q トンネリングまたは EoMPLS を使用して、レイヤ 2 VPN サービスを提供できます。サービス プロバイダー ネットワークが MPLS クラウドであり、なおかつ EoMPLS をポイントツーポイント プロトコルとして設定した場合、MPLS ネットワークに接続する PE-CLE ES ポートで、MPLS タグが追加されます。この MPLS タグは、リモート PE-CLE デバイスの ES ポートで削除されます。

これらの機能の設定手順については、第 16 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」および第 37 章「MPLS および EoMPLS の設定」を参照してください。

図 1-2　レイヤ 2 VPN 構成



PE-CLE = Catalyst 3750 Metro スイッチ

レイヤ 3 VPN アプリケーション

レイヤ 3 VPN サービスでマルチ VRF-CE または MPLS VPN を使用して、ビジネス カスタマー向けのスケーラブルなレイヤ 3 VPN サービスを展開および管理できます。レイヤ 3 VPN は、1 つまたは複数の物理ネットワーク上でリソースを共有する、セキュア IP ベースのネットワークです。地域的に分散したサイトを対象に、共有バックボーン上での安全な通信を実現します。

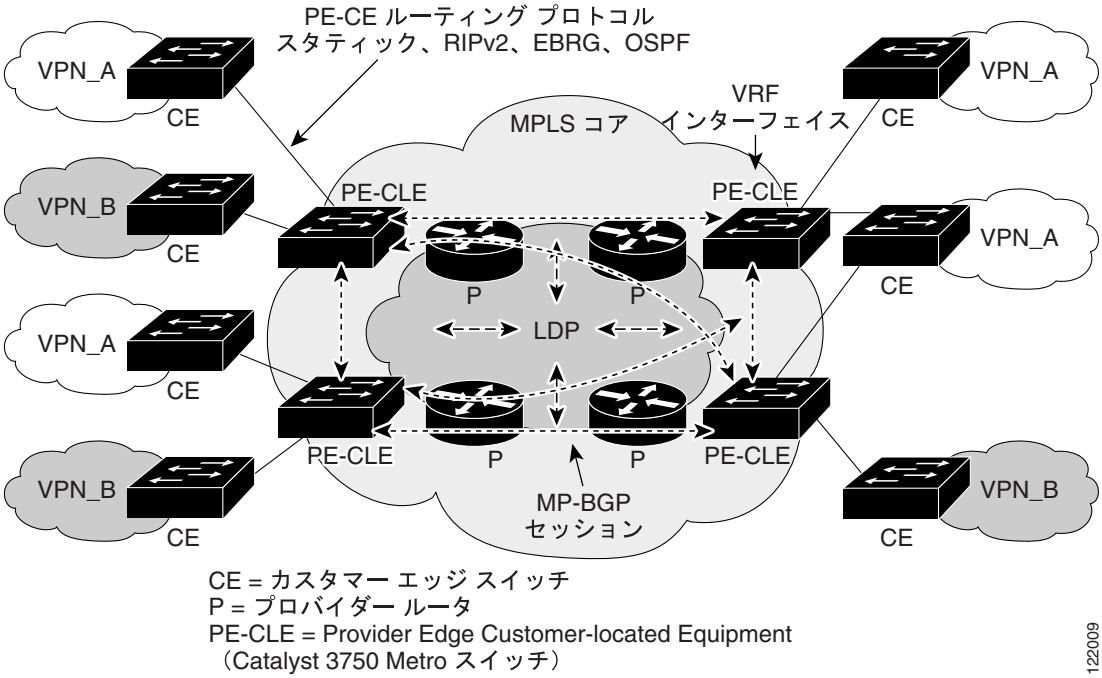
図 1-3 に、カスタマー サイトの間で MPLS 拡張したエンドツーエンドの MPLS VPN ネットワークを示します。CE デバイス（Catalyst 3750 Metro スイッチまたはその他のレイヤ 3 スイッチ）は、RIP、EBGP、OSPF、IS-IS などのルーティング プロトコルまたはスタティック ルーティングを使用して、カスタマー VPN から MPLS ネットワークのエッジにある Catalyst 3750 Metro PE-CLE デバイスに、パケットを転送できます。PE-CLE デバイスには Multiprotocol BGP（MP-BGP）と、カスタマーの VPN に対応するルート識別子が設定されています。PE-CLE デバイスはこの情報を VPN-IPv4 フォーマットに変換し、Layer Distribution Protocol（LDP）ラベルを追加して、VPN ルートを確立します。

VPN ルートは MP-BGP を使用して MPLS ネットワーク上で配布されます。MP-BGP は各 VPN ルートに対応するラベルも配布します。MPLS VPN は VPN Routing/Forwarding（VRF）サポートを使用して、ルーティング ドメインを相互に隔離します。

ポート上で MPLS-VPN パケットを受信すると、CE スイッチはそのラベルをルーティング テーブルで検索してパケットの取り扱い方法を判別します。PE-CLE ルータは CE デバイスから学習した各カスタマー プレフィクスにラベルをバインドし、他の PE-CLE ルータにアドバタイズするプレフィクスにそのラベルを含めます。PE-CLE ルータがプロバイダー ネットワーク経由でパケットを転送する場合、宛先ルータから学習したラベルをパケットに付加します。宛先ルータは、ラベルの付いたパケットを受信すると、ラベルを調べて、正しい CE デバイスにパケットを転送するために使用します。

各 VPN メンバーに対応する VPN ルートを維持するのは、MPLS ネットワークの各終端にある PE-CLE ルータのみです。コア ネットワークに存在するプロバイダー ルータは、VPN ルートを維持しません。その結果、カスタマー VPN のセキュリティが確保され、サービス プロバイダー MPLS ネットワーク経由で伝送される他のカスタマー パケットから分離されます。

図 1-3　MPLS VPN 構成



MPLS VPN の設定手順については、第 37 章「MPLS および EoMPLS の設定」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 5 章「Cisco IOS CNS エージェントの設定」