



概要

この章では、Catalyst 3550 マルチレイヤ スイッチ ソフトウェアについて説明します。内容は、次のとおりです。

- [機能 \(p.1-2\)](#)
- [管理オプション \(p.1-9\)](#)
- [ネットワーク構成の例 \(p.1-11\)](#)
- [次の作業 \(p.1-20\)](#)

このマニュアルでは、IP は IP バージョン 4 (IPv4) を表します。レイヤ 3 IP バージョン 6 (IPv6) パケットは、非 IP パケットとして取り扱われます。

機能

ソフトウェアは、リリース ノートに記載されているハードウェアをサポートします。ここでは、このリリースでサポートされている機能について説明します。



(注)

すべての Catalyst 3550 ギガビット イーサネット スイッチは、レイヤ 2+ 機能、完全なレイヤ 3 ルーティング、高度なサービスを提供する IP サービス イメージ(以前は Enhanced Multilayer Image [EMI; 拡張マルチレイヤ イメージ]) がインストールされた状態で出荷されます。Catalyst 3550 ファストイーサネット スイッチは、IP ベース イメージ(以前は Standard Multilayer Software Image [SMI; 標準マルチレイヤ ソフトウェア イメージ])、または IP サービス イメージのどちらかがインストールされた状態で出荷されます。IP ベース イメージは、レイヤ 2+ 機能および基本的なレイヤ 3 ルーティングを提供します。IP サービス イメージ アップグレード キットを購入して、IP ベース イメージから IP サービス イメージに Catalyst 3550 ファストイーサネット スイッチをアップグレードできます。

使いやすく簡単な配置

- Express Setup により、ブラウザベースのプログラムを使用して、スイッチを初めて設定するときに、基本的な IP 情報、コンタクト情報、スイッチと Telnet のパスワード、および SNMP (簡易ネットワーク管理プロトコル) 情報を迅速に設定
- ユーザ定義の SmartPort マクロにより、ネットワーク上の展開を簡略化するためのカスタム スイッチ設定を作成
- 組み込みデバイス マネージャにより、Web ブラウザを介して単一のスイッチを設定しモニターする。デバイス マネージャの起動方法については、スタートアップ ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- Network Assistant GUI (グラフィカル ユーザ インターフェイス)
 - 複数のスイッチの設定、モニター、認証、およびソフトウェア アップグレードを一括して実行できます (対象クラスタメンバーのリストはリリース ノートを参照)
 - 1 つの IP アドレスで管理できる候補スイッチを自動検出し、最大 16 台のスイッチ クラスタを作成できます。
 - コマンド スイッチに直接接続されていないクラスタ候補を拡張検出できます。
 - HTTP または TFTP を使用してイメージをスイッチにダウンロードできます。

パフォーマンス

- 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
- すべてのイーサネット ポートでの IEEE 802.3x フロー制御
- 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 8 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
- 不明のユニキャストおよびマルチキャスト トラフィック転送のポート 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、およびバージョン 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キャスト トラフィックのフラグディングを制限
- IGMP レポート抑制は、マルチキャスト ルータ クエリ単位で IGMP レポート 1 つのみをマルチキャスト デバイスに送信 (IGMPv1 または IGMPv2 クエリのみでサポート)
- Multicast VLAN Registration (MVR) 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幅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 スロットリングにより、IGMP 転送テーブルにエントリ最大数が存在するときの動作を設定
- IGMP 設定変更可能な leave タイマーにより、ネットワークの脱退遅延時間を設定
- System Database Management (SDM) テンプレート ユーザ側で選択する機能へのサポートを最大化するためのシステム リソース割り当て
- Web Cache Communication Protocol (WCCP) によるローカル キャッシュ エンジンへのトラフィックのリダイレクト、ローカルに実行されるコンテンツ要求のイネーブル化、およびネットワーク内の Web トラフィック パターンのローカライズ (EMI が必要)

管理機能

- Cisco Intelligence Engine 2100 (IE2100) シリーズ Cisco Networking Services (CNS) 内蔵エージェント スイッチ管理、設定保存、および配信の自動化
- Dynamic Host Configuration Protocol (DHCP) 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)、TFTP (簡易ファイル転送プロトコル) サーバ名などスイッチ情報の設定の自動化
- DHCP サーバ IP アドレスおよびほかの DHCP オプションを IP ホストに自動的に割り当て
- DHCP リレー エージェント情報 (Option 82) 加入者の識別および IP アドレス管理
- 有向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。また有向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
- Address Resolution Protocol (ARP; アドレス解決プロトコル) 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
- ユニキャスト MAC アドレス フィルタリング 特定の送信元または宛先 MAC アドレスを持つパケットを廃棄
- Cisco Discovery Protocol (CDP) バージョン 1 およびバージョン 2 ネットワーク トポロジーの検出と、ネットワーク上のほかのシスコ製デバイスとスイッチ間のマッピング
- Network Time Protocol (NTP) 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付加
- Cisco IOS File System (IFS) 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
- コンフィギュレーション ロギング スイッチ設定への変更を記録および表示
- デバイスの一意識別子 `show inventory` ユーザ EXEC コマンド表示によって製品 ID 情報を提供
- Netscape Navigator または Internet Explorer セッションを通じた組み込みデバイス マネージャによる、または Network Assistant アプリケーションによる帯域内管理アクセス
- ネットワーク上の複数の CLI (コマンドライン インターフェイス) ベースのセッションに対する最大 16 の同時 Telnet 接続確立による帯域内管理アクセス

- ネットワークでの CLI ベース マルチ セッションに対応した、最大 5 つの同時暗号化 Secure Shell (SSH; セキュア シェル) 接続用帯域内管理アクセス
- SNMP のバージョン 1、バージョン 2c、およびバージョン 3 の get および set 要求による帯域内管理アクセス
- 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およびモデム経由でのリモート端末へのアクセスによる帯域外管理アクセス
- Secure Copy Protocol (SCP) 機能 スイッチ コンフィギュレーション ファイルまたはスイッチ イメージ ファイルをコピーする安全な認証方法を提供 (ソフトウェアの IP ベース イメージ および IP サービス イメージの暗号化バージョンが必要) (ソフトウェアの暗号化バージョンが必要)



(注) 管理インターフェイスの詳細については、「[管理オプション](#)」(p.1-9) を参照してください。

冗長性

- Hot Standby Router Protocol (HSRP) によるコマンド スイッチおよびレイヤ 3 ルータの冗長構成
- すべてのイーサネット ポートでの UniDirectional Link Detection (UDLD; 単一方向リンク検出) およびアグレッシブ UDLD 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の検出とディセーブル化
- IEEE 802.1D Spanning-Tree Protocol (STP; スパニングツリー プロトコル) 冗長バックボーン 接続およびループフリー ネットワークの実現。STP には次の機能があります。
 - Per-VLAN Spanning-Tree plus (PVST+) VLAN 間のロードバランシング
 - Rapid PVST+ VLAN 間のロードバランシング
 - UplinkFast、Cross-Stack UplinkFast、および BackboneFast 機能 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 アップリンクおよびクロス タック 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達成
- IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) VLAN をスパニングツリー インスタンスに分類、またデータ トラフィックおよびロードバランシング用に複数の転送パスを確保
- IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP) ルートと Designated Port (DP; 指定ポート) を即時にフォワーディング ステートへ移行することによる、スパニングツリーの高速コンバージェンス
- 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
 - 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
 - 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 ガード機能 単一方向リンクとなる障害のため代替またはルート ポートが DP として使用されるのを防止



(注) スイッチは最大 128 のスパニングツリー インスタンスをサポートします。

VLAN サポート

- 最大 1005 の VLAN のサポートによる、該当するネットワーク 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 へのユーザの割り当て
- IEEE 802.1Q 規格によって許可された 1 ~ 4094 の全範囲の VLAN ID のサポート
- VLAN Query Protocol (VQP) ダイナミック VLAN メンバシップ対応
- 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、および変更。ブロードキャストとマルチキャストトラフィックを管理および制御。また、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
- Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) 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 (IEEE 802.1Q または ISL) のネゴシエーション
- 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
- 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
- VLAN 1 の最小化 個々の VLAN トランク リンクで VLAN 1 をディセーブルにすることにより、スパニングツリーの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の送受信は行われません。スイッチの CPU では、コントロール プロトコル フレームの送受信が継続されます。

セキュリティ

- パスワードによって保護される管理インターフェイス (デバイス マネージャ、Network Assistant、および CLI) 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、および結果の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 アドレス指定
- 同一スイッチの DP へのトラフィック伝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 アクセスを許可されたステーションの MAC アドレスの制限および識別
- トランク ポートのポート セキュリティにより、VLAN アクセスを許可されたステーションの MAC アドレスの制限および識別
- 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
- 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トラフィックをフィルタリングすることにより、非ルーテッド インターフェイスのトラフィックを制限する IP ソース ガード
- DHCP スヌーピングにより、信頼性のないホストと DHCP サーバの間の信頼性のない DHCP メッセージをフィルタリング
- ダイナミック ARP 検査により、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防止
- BPDU ガード 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) ルーテッド インターフェイス (ルータ ACL) 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 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) 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によって 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 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ことを防止
- IEEE 802.1X とユーザ単位のアクセス制御リスト 異なるレベルのネットワーク アクセスおよびサービスを IEEE 802.1X 認証ユーザに提供
- IEEE 802.1X と VLAN 割り当て IEEE 802.1X 認証ユーザを特定の VLAN に制限
- IEEE 802.1X とポート セキュリティ IEEE 802.1X 複数ホスト ポートへのアクセスを制御
- IEEE 802.1X と音声 VLAN ポートが許可ステートか未許可ステートであるかにかかわらず、IP Phone の音声 VLAN へのアクセスを許可
- IEEE 802.1X とゲスト VLAN IEEE 802.1X 非準拠ユーザへのサービスの制限
- ネットワーク使用率を調査する IEEE 802.1X アカウンティング
- Wake-On-LAN 機能を備えた IEEE 802.1X 特定のイーサネット フレームを受信すると休止状態の PC を起動
- TACACS+ TACACS サーバを使用したネットワーク セキュリティの管理
- Kerberos セキュリティ システム 信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証
- RADIUS 認証および許可プロセスにおける詳しいアカウンティング情報とフレキシブルな管理制御を提供
- Secure Socket Layer (SSL) バージョン 3.0 のサポート 安全な HTTP 通信を可能にするための HTTP1.1 サーバ認証、暗号化、メッセージ完全性、および HTTP クライアント認証
- IEEE 802.1Q トンネリング サービス プロバイダー ネットワークのリモート サイトにユーザのいるカスタマーは、VLAN をほかのユーザおよびレイヤ 2 プロトコル トンネリングから分離して、カスタマーのネットワークがすべてのユーザに関する STP、CDP、および VTP の完全な情報を所有することを保証
- レイヤ 2 ポイントツーポイント トンネリング EtherChannel の自動作成を促進

QoS および CoS

- 自動 QoS (auto-QoS) トラフィックの分類と出力キューの設定を自動化することで既存の Quality of Service (QoS; サービス品質) 機能の展開を簡略化
- 分類
 - 物理インターフェイス単位、またはポート単位、VLAN 単位の分類
 - ポート単位の IP Type-of-Service/Differentiated Services Code Point(IP ToS/DSCP)および IEEE 802.1p Class of Service (CoS; サービス クラス) 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 packets 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 IEEE 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差別化したサービス 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
 - 信頼できるポート ステート 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)
 - 信頼できる境界 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
- ポリシング
 - 物理インターフェイス単位、またはポート単位、VLAN 単位のポリシング
 - 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
 - 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

- 入力ギガビット対応イーサネットポートでは最大 128 個のポリサー
入力 10/100 ポートでは、最大 8 個のポリサー
各出力ポートでは、最大 8 個のポリサー（集約ポリサーのみ）
- 不適合パケット
 - 帯域利用率限度を越える（不適合）パケットに対するマークダウン
- 出力ポリシングおよび出力キューのスケジューリング
 - すべてのスイッチポート上の 4 つの出力キュー。このキューは、Weighted Round Robin (WRR; 重み付きラウンドロビン) スケジューリングアルゴリズムで設定することも、WRR に対応する 1 つの完全優先キューとそのほかの 3 つのキューとして設定することもできます。完全優先キューは、ほかの 3 つのキューが処理される前に必ず空にする必要があります。ミッションクリティカルで時間に影響されやすいトラフィックに対して、完全優先キューを使用できます。
 - テールドロップおよび Weighted Random Early Detection (WRED; 重み付きランダム早期検出) 技術 ギガビットイーサネットポートの輻輳を回避。ファストイーサネットポート上の輻輳回避のテールドロップ

レイヤ 3 サポート

機能やプロトコルの中には、EMI が必要なものもあります。

- Hot Standby Router Protocol (HSRP) によるレイヤ 3 ルータの冗長構成
- 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
 - Routing Information Protocol (RIP) バージョン 1 およびバージョン 2
 - Open Shortest Path First (OSPF)
 - Enhanced IGRP (EIGRP)
 - Border Gateway Protocol (BGP) バージョン 4
- 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
- Customer Edge (CE; カスタマー エッジ) デバイス内の multiple VPN Routing/Forwarding (multi-VRF) インスタンスにより、サービスプロバイダーは複数の Virtual Private Network (VPN; 仮想私設網) のサポート、および VPN 間での IP アドレスの共有が可能
- Policy-Based Routing (PBR; ポリシーベースルーティング) によるトラフィックフローへの定義ポリシーの設定
- 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
- 等価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。
- Distance Vector Multicast Routing Protocol (DVMRP) トンネリングによる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

- Nonstop forwarding (NSF; ノンストップ フォワーディング) 認識により、レイヤ 3 スイッチは、プライマリ Route Processor (RP; ルート プロセッサ) がクラッシュしてバックアップ RP が引き継いでいる間、またはスムーズなソフトウェア アップグレードのためプライマリ RP を手動でリロードしている間 (IP サービス イメージが必要) も NSF 対応近接ルータからのパケットを転送し続けることが可能

モニタリング

- スイッチ LED による、ポート レベルおよびスイッチ レベルのステータス確認
- Switch Port Analyzer (SPAN; スイッチ ポート アナライザ) による、任意ポートまたは VLAN のトラフィック モニタリング
- 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
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 Remote Monitoring (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 モニタリングと、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
- MAC アドレス通知 スイッチが学習したかまたは削除した MAC アドレスを保存して、ネットワークのユーザを追跡
- レイヤ 2 traceroute 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識別

Catalyst 3550-24PWR スイッチの PoE のサポート

- 接続されている Cisco の標準化前および IEEE 802.3af 準拠の受電装置の回路に電力が供給されていないことをスイッチが検出した場合に、その装置に Power over Ethernet (PoE) 対応ポートから電力を供給可能
- 消費電力対応 CDP のサポート。受電装置が消費する電力量をスイッチに通知します。
- Cisco Intelligent Power Management のサポート。受電装置とスイッチは、電力ネゴシエーション CDP メッセージを介して、電力消費レベルが一致するようにネゴシエーションを行います。ネゴシエーションにより、大電力のシスコの受電装置が最高の電力モードで動作できます。
- 自動検出およびパワー バジェット機能により、スイッチはパワー バジェットを維持して電力に関する要求のモニタと追跡を行い、必要な場合のみ電力を供給します。
- デバイス マネージャおよび Network Assistant を介したファンの故障や温度超過の検出

管理オプション

スイッチは、プラグアンドプレイ方式で使用できるように設計されています。スイッチに基本的な IP 情報を設定し、ネットワーク上のほかのデバイスに接続するだけで、稼働させることができます。特定のネットワーク要件がある場合には、さまざまな管理インターフェイスを使用して、スイッチ単位で、またはスイッチ クラスタの一部としてスイッチを設定し、モニタできます。

管理インターフェイス オプション

各スイッチおよびスイッチ クラスタは、次のインターフェイスを使用して設定およびモニタできます。

- **組み込みデバイス マネージャ** デバイス マネージャは、ソフトウェア イメージに統合されている GUI です。単一のスイッチの設定とモニタに使用します。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- **Network Assistant** Network Assistant は、Cisco.com からダウンロードできる GUI です。単一のスイッチやスイッチ クラスタの管理に使用できます。Network Assistant の詳細については、Cisco.com の『*Getting Started with Cisco Network Assistant*』を参照してください。
- **CLI** このスイッチの Cisco IOS ソフトウェアは、デスクトップおよびマルチレイヤ スイッチング機能をサポートしています。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。

- **IE2100** Cisco Intelligence Engine 2100 シリーズ Configuration Registrar は、スイッチ ソフトウェアに内蔵の CNS Agent に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、その設定変更を実行した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。

IE2100 の詳細については、第 4 章「IE2100 CNS エージェントの設定」を参照してください。

- **SNMP** SNMP は、スイッチおよびスイッチ クラスタ メンバーをモニタし、制御するためのプロトコルです。CiscoWorks 2000 LAN Management Suite (LMS) および HP OpenView などの SNMP 管理アプリケーションを使用して、スイッチの設定、パフォーマンス、セキュリティの統計情報収集の管理を行うことができます。

また、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 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 27 章「SNMP の設定」を参照してください。

Network Assistant およびスイッチ クラスタの利点

Network Assistant およびスイッチ クラスタを使用することによって、設定およびモニタ作業を簡易化し、最小限に抑えることができます。シスコのスイッチ クラスタ テクノロジーでは、サポート対象の Catalyst スイッチを 16 台まで相互接続し、1 つの IP アドレスで管理できます。したがって、IP アドレスの数量に限りがある場合、IP アドレス数を節約できます。Network Assistant は最も簡単に使用できるインターフェイスで、許可されたユーザは、ネットワーク上の任意の PC からスイッチにアクセスし、スイッチ クラスタを管理できます。

スイッチ クラスタおよび Network Assistant を使用することにより、次の利点があります。

- 設置場所や相互接続メディア (イーサネット、ファストイーサネット、Fast EtherChannel、Cisco GigaStack GBIC [ギガビット インターフェイス コンバータ] ギガビットイーサネット、Gigabit EtherChannel など) に関係なく、相互接続した Catalyst スイッチ (対象スイッチのリストはリリースノートを参照) を管理し、モニタできます。
- 1 つの Network Assistant ウィンドウから複数の設定を実行できます。特定の作業を行うための CLI コマンドを記憶しておく必要はありません。

- Network Assistant から複数のポートと複数のスイッチを同時に設定できます。たとえば、次のように複数のポートと複数のスイッチを設定、管理できます。
 - 速度およびデュプレックスなどのポート設定
 - ポートおよびコンソールポートのセキュリティ設定
 - NTP、STP、VLAN、および QoS の設定
 - 在庫および統計レポート、リンク レベルおよびスイッチ レベルのモニタおよびトラブルシューティング
 - グループソフトウェアのアップグレード
- 相互接続デバイスのトポロジを表示し、既存のスイッチ クラスタや、クラスタに追加できる対象スイッチを識別できます。また、このトポロジを参照して、スイッチ間のリンク情報をすばやく判断できます。
- 前面パネル イメージの LED から、特定または複数のスイッチのリアルタイム ステータスをモニタできます。イメージに表示されるシステム、Redundant Power System (RPS; 冗長電源システム) およびポート LED のカラーは、実際の LED のカラーと同じです。
- 段階を踏んで VLAN、ACL、QoS などの複雑な機能を設定する対話形式モードを使用できます。
- ウィザードを使用できます。このウィザードは、最低限必要な情報のみを提示して、ビデオトラフィックの QoS プライオリティ、データ アプリケーションのプライオリティ レベル、セキュリティなどの複雑な機能を設定するよう要求します。

Network Assistant ソフトウェアおよびブラウザの要件や、クラスタリングの詳細については、Cisco.com の『*Getting Started with Cisco Network Assistant*』を参照してください。サポートされている Cisco IOS リリースを含む、クラスタリングの要件については、このリリースのリリース ノートを参照してください。

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。

- 「[スイッチの使用についての設計概要](#)」(p.1-11)
- 「[各種スイッチを使用する中小規模のネットワーク](#)」(p.1-14)
- 「[Catalyst 3550 スイッチのみを使用する大規模ネットワーク](#)」(p.1-16)
- 「[Catalyst 3550 スイッチによる集合住宅ネットワーク](#)」(p.1-17)
- 「[長距離広帯域幅の転送構成](#)」(p.1-19)

スイッチの使用についての設計概要

ネットワーク帯域に対するネットワーク ユーザの需要が高くなると、データの送受信に時間がかかります。ネットワークを設計する際は、ネットワーク ユーザに必要な帯域幅、およびユーザが使用するネットワーク アプリケーションの相対的なプライオリティを考慮してください。

表 1-1 に、ネットワーク パフォーマンスが低下する原因、およびネットワーク ユーザの使用可能帯域幅が増大するネットワークの設計方法を示します。

表 1-1 ネットワーク パフォーマンスの向上

ネットワークの需要	推奨する設計方法
1 つのネットワーク セグメントのユーザ数 が多すぎ、インターネットにアクセスする ユーザ数が増加している	<ul style="list-style-type: none"> • 小規模なネットワーク セグメントを作成し、帯域幅の共有ユーザ数を減らします。VLAN および IP サブネットを使用して、ネットワーク リソースを、そのリソースを最も多く利用しているユーザの論理ネットワークに位置付けます。 • スイッチおよび接続先ワークステーション間を全二重モードで接続します。
<ul style="list-style-type: none"> • 新しい PC、ワークステーション、およびサーバの消費電力が増加している • ネットワーク アプリケーション (大容量の添付ファイルのある Eメールなど) および帯域幅を多用するアプリケーション (マルチメディアなど) の帯域幅需要が高い 	<ul style="list-style-type: none"> • グローバル リソース (ネットワーク ユーザが同等アクセスを必要とするサーバおよびルータなど) を高速スイッチ ポートに直接接続し、ユーザ独自の高速セグメントを作成します。 • スイッチと接続先のサーバおよびルータ間で EtherChannel の機能を適用します。

ネットワークの設計で考慮しなければならない事項は、帯域幅だけに限りません。ネットワークのトラフィック プロファイルの改善に伴い、音声とデータの統合、マルチキャストメディア統合、アプリケーション優先順位付け、セキュリティなどのアプリケーションをサポートするネットワーク サービスの提供を考慮してください。表 1-2 に、ネットワークの需要例とその需要への対応策を示します。

表 1-2 ネットワーク サービスの提供


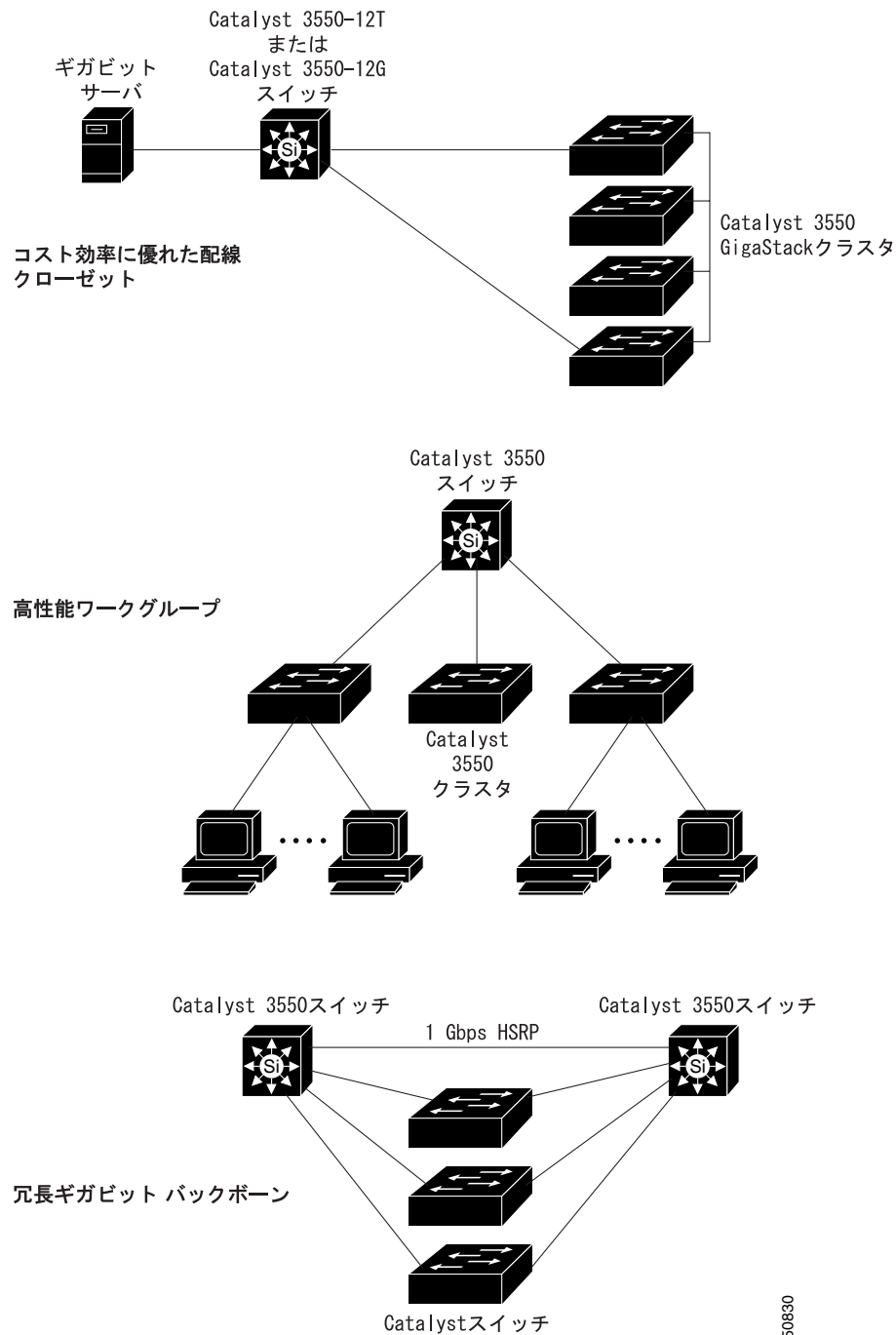
ネットワークの需要	推奨する設計方法
マルチメディア アプリケーション用の効率的な帯域幅の使用と重要なアプリケーション用に保証された帯域幅	<ul style="list-style-type: none"> IGMP スヌーピングを利用して、マルチメディアおよびマルチキャストトラフィックを効率的に転送します。 パケット分類、マーキング、スケジューリング、輻輳回避などの QoS メカニズムを使用して、該当するプライオリティレベルでトラフィックを分類し、これによってフレキシビリティを最大限にし、ミッションクリティカル、ユニキャスト、マルチキャスト、およびマルチメディア アプリケーションをサポートします。 オプションの IP マルチキャストルーティングを使用して、マルチキャストトラフィックにより適したネットワークを設計します。 MVR を使用して、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ながら、帯域幅およびセキュリティを確保するため加入者 VLAN からストリームを隔離します。
ミッションクリティカルなアプリケーションに対してネットワークの冗長性を常に確保することに対する需要が高まっている	<ul style="list-style-type: none"> HSRP を使用してルータを冗長構成にします。 VLAN トランク、Cross-Stack UplinkFast、および BackboneFast を使用して、アップリンク ポート上でトラフィックのロードバランシングを実行し、VLAN トラフィックの転送時にポートコストが低いアップリンクポートが選択されるようにします。
IP テレフォニーの需要が増加している	<ul style="list-style-type: none"> QoS を使用して、輻輳時に IP テレフォニーなどのアプリケーションが優先処理されるようにし、ネットワーク上の遅延およびジッタの両方を制御します。 各ポートで最低 2 つのキューがサポートされるスイッチを使用し、IEEE 802.1p/Q に基づいて、音声トラフィックおよびデータトラフィックにハイプライオリティまたはロープライオリティを適用します。 Catalyst 2900 XL および 3500 XL スイッチに対して Voice VLAN ID (VVID) を使用し、音声トラフィックに対して別個の VLAN を設定します。
既存のインフラを使用した、自宅またはオフィスからインターネットまたはイントラネットへのデータおよび音声の高速伝送の需要が増加している	<p>Catalyst 2900 LRE XL および Catalyst 2950 LRE スイッチを使用して、既存の電話回線などの既存インフラ上で最大 15 Mb の IP 接続を実現します。</p> <p> (注) Long-Reach Ethernet (LRE; 長距離イーサネット) は、Catalyst 2900 LRE XL および Catalyst 2950 LRE スイッチで使用されているテクノロジーです。これらのスイッチおよび LRE のテクノロジーに関しては、スイッチのマニュアルセットを参照してください。</p>

図 1-1 に、Catalyst スイッチを使用した、次の 3 つの構成例を示します。

- コスト効率に優れた配線クローゼット 多数のユーザを優れたコスト効率で配線クローゼットに接続するには、GigaStack GBIC 接続によって、最大 9 台の Catalyst 3550 XL スイッチ (または Catalyst 3550、Catalyst 2950、Catalyst 3500 XL、および Catalyst 2900 XL スイッチの併用) を接続します。スタック内の 1 つのスイッチに障害が生じた場合、スイッチの接続を維持するには、最下位スイッチを最上位スイッチに接続して GigaStack ループバックを作成し、クロススタック ギガビット アップリンク上で Cross-Stack UplinkFast 機能をイネーブルにします。

ギガビット GBIC モジュールを使用すると、GigaStack クラスタから Catalyst 3550-12T または Catalyst 3550-12G スイッチなどのギガビットバックボーンスイッチに冗長アップリンク接続を設定できます。ファストイーサネット、ギガビット、または EtherChannel の各リンクを使用してバックアップパスを作成することもできます。冗長接続のいずれか一方に障害が生じて、もう一方がバックアップパスとして機能します。Catalyst 3550-12T または Catalyst 3550-12G スイッチを 1 つのスイッチ クラスタ マネージャとして設定すると、1 つの IP アドレスでスタックメンバーを管理できます。Catalyst 3550-12T または Catalyst 3550-12G スイッチは、1000BASE-T 接続を使用してギガビットサーバに接続できます。

図 1-1 構成例



50830

- 高性能ワークグループ ネットワーク リソースへ高速アクセスする場合、アクセス レイヤで Catalyst 3550 スイッチを使用すると、デスクトップにギガビットイーサネットを設定できます。輻輳を防止するには、このスイッチに対して QoS DSCP マーキング プライオリティを使用します。ディストリビューション レイヤで高速 IP 転送をする場合は、アクセス レイヤの Catalyst 3550 スイッチをバックボーンのギガビット マルチレイヤ スイッチ (Catalyst 3550 マルチレイヤ スイッチなど) に接続します。

この構成の各スイッチで、ユーザは、バックボーンのネットワーク リソースへの 1 Gbps 専用接続を得られます。これに対して、GigaStack 構成では、1 Gbps 接続がスタックのスイッチ間で共有されます。また、次のギガビット GBIC モジュールを使用することによって、メディアおよび距離に柔軟に対応できます。

- 1000BASE-T GBIC: 最大 328 フィート (100 m) の銅線接続
- 1000BASE-SX GBIC: 最大 1,804 フィート (550 m) の光ファイバ接続
- 1000BASE-LX/LH GBIC: 最大 32,808 フィート (6 マイルまたは 10 km) の光ファイバ接続
- 1000BASE-ZX GBIC: 最大 328,084 フィート (62 マイルまたは 100 km) の光ファイバ接続
- 冗長ギガビット バックボーン HSRP によって、2 つの Catalyst 3550 マルチレイヤ スイッチ間にバックアップ パスを作成して異なる VLAN およびサブネットのネットワーク信頼性とロードバランシングを強化できます。また、HSRP によって、ネットワーク障害が発生した場合のネットワーク コンバージェンスも高速化されます。Catalyst スイッチは、再度スター型構成で 2 つの Catalyst 3550 マルチレイヤ バックボーン スイッチに接続できます。バックボーン スイッチのいずれか一方に障害が生じて、もう一方のバックボーン スイッチが、スイッチとネットワーク リソース間の接続を維持します。

各種スイッチを使用する中小規模のネットワーク

図 1-2 に、最大 500 名の従業員が使用するネットワークの構成を示します。このネットワークでは、Catalyst 3550 マルチレイヤ スイッチを使用し、高速アップリンクを通じて最大 10 の配線クローゼットを集約できます。ネットワークの信頼性とロードバランシングを強化するため、このネットワークには 2 台のルータと 2 台の Catalyst 3550 マルチレイヤ スイッチが含まれ、すべて HSRP がイネーブルになっています。これにより、ルータまたは Catalyst 3550 マルチレイヤ スイッチのいずれか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。

配線クローゼットは、Catalyst 3550、Catalyst 3500 XL、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、Catalyst 1900 など各種のスイッチで構成されています。これらのスイッチはワークステーション、Cisco IP Phone、およびローカル サーバに接続しています。これらのスイッチを、図のように複数のクラスタにまとめることも、1 つのクラスタにまとめることもできます。クラスタは、クラスタメンバーの設置場所に関係なく、プライマリおよびセカンダリのコマンド スイッチの IP アドレスを使用して管理できます。

このネットワークは、VLAN を使用してネットワークを論理的にセグメント化し、詳細に定義したブロードキャスト グループを作成して、セキュリティの管理を行っています。同じ VLAN 上に、データトラフィックおよびマルチメディアトラフィックが設定されています。Cisco IP Phone からの音声トラフィックは、別個の VVID 上に設定します。配線クローゼットあたり最大 4 つの VVID を設定できます。データ、マルチメディア、および音声トラフィックが同じ VLAN に割り当てられている場合、設定できる VLAN は配線クローゼットあたり 1 つだけです。Cisco IP Phone に接続したスイッチポートの場合、IEEE 802.1p/Q QoS はデータトラフィックよりも音声トラフィックに転送プライオリティを与えます。

Cisco IP Phone は、RJ-45 コネクタ付きの標準ツイストペアストレートケーブルを使用して、Catalyst 3550-24PWR スイッチの 10/100 PoE ポートと、Catalyst 3550 の 10/100 ポートに接続されています。これらのマルチサービス スイッチ ポートは、接続されている IP Phone を自動的に検出します。Cisco CallManager は、コール処理、ルーティング、および IP Phone の機能と設定を制御します。ユーザは Cisco SoftPhone ソフトウェアが稼働しているワークステーションを使用して PC から呼び出しを発信、受信、制御できます。Cisco IP Phone、Cisco CallManager ソフトウェア、および Cisco SoftPhone ソフトウェアを使用すると、電話と IP ネットワークを統合でき、IP ネットワークで音声とデータの両方を扱えるようになります。

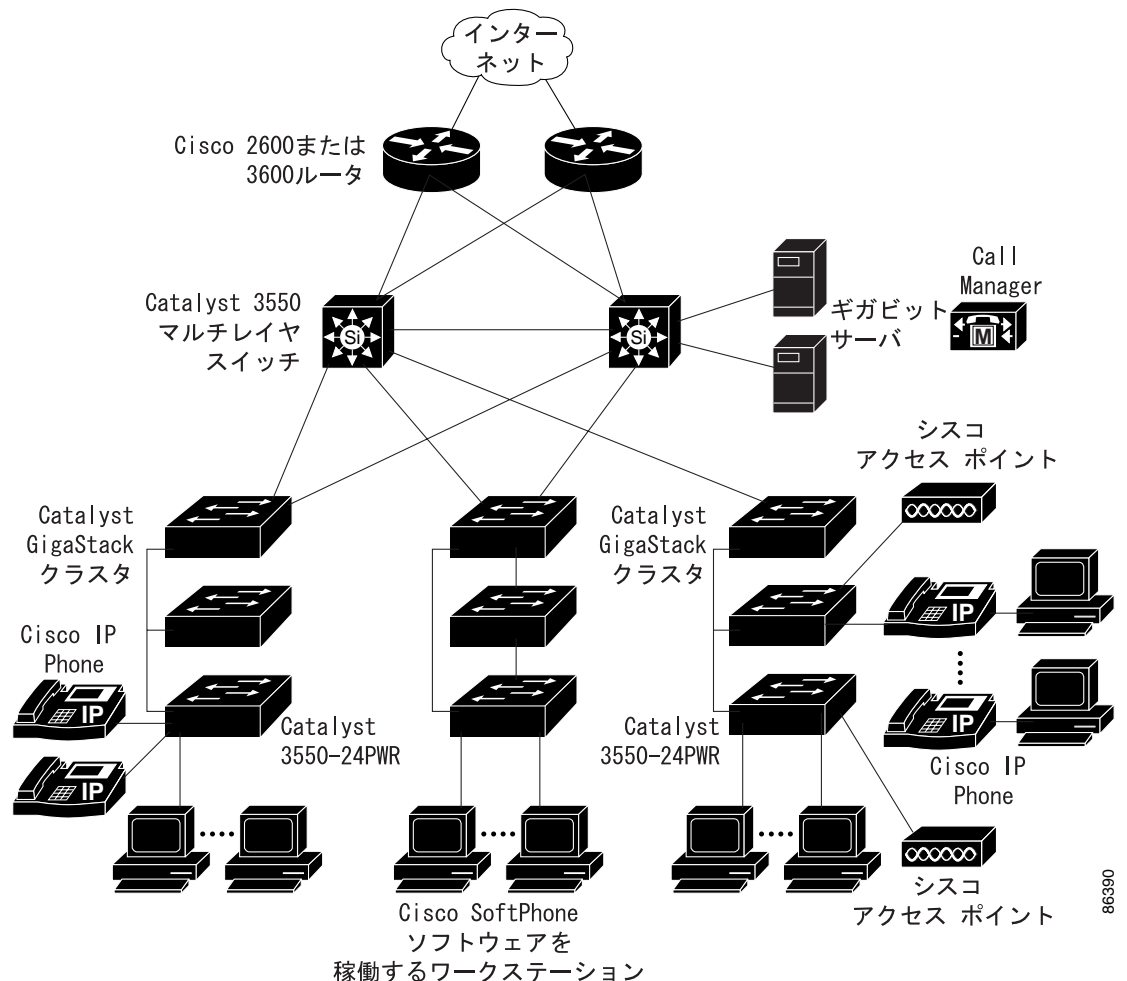
Catalyst 3550-24PWR スイッチの各 10/100 PoE ポートは、ポートあたり 15.4 W の電力を供給します。IP Phone は、AC 電源に接続されている場合も冗長電力を受けられます。Catalyst 3550-24PWR スイッチに接続されていない IP Phone は AC 電源から電力を受けます。

ある 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、ルータまたはマルチレイヤ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ます。このネットワークでは、Catalyst 3550 マルチレイヤスイッチが VLAN 間ルーティングを行います。Catalyst 3550 スイッチの VLAN アクセス制御リスト (VLAN マップ) が 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。

Catalyst 3550 マルチレイヤスイッチは、VLAN 間ルーティング以外に DSCP プライオリティなどの 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。

VLAN 間ルーティングやほかのネットワークサービスを提供する Catalyst 3550 マルチレイヤスイッチを使用することで、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、および WAN とインターネットアクセスに重点を置きます。

図 1-2 バックボーン構成 (略図) の Catalyst 3550 スイッチ

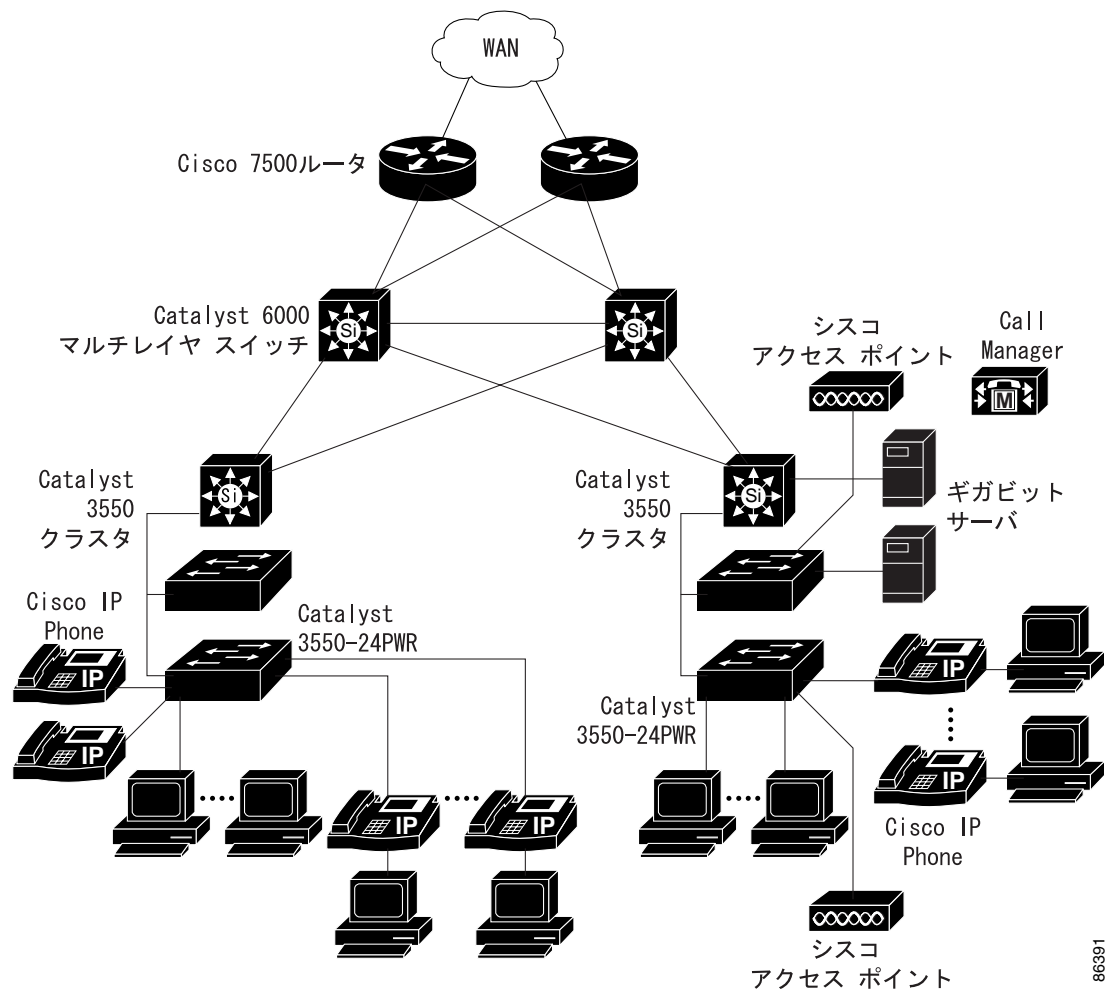


Catalyst 3550 スイッチのみを使用する大規模ネットワーク

配線クローゼット内のスイッチは、これまでレイヤ 2 専用デバイスでしたが、ネットワークトラフィックプロファイルの改善に伴い、ますますマルチキャスト管理やトラフィック分類などのマルチレイヤサービスを採用するようになってきました。図 1-3 に、配線クローゼットに Catalyst 3550 マルチレイヤスイッチのみを使用するネットワークの構成と、最大 10 の配線クローゼットを集約するバックボーンの Catalyst 6000 スイッチを示します。

配線クローゼットでは、各 Catalyst 3550 スイッチは IGMP スヌーピングがイネーブルになっていて、効率的にマルチメディアおよびマルチキャストトラフィックを伝送します。帯域幅制限に基づいて不適合トラフィックを廃棄またはマークする QoS ACL も、各スイッチで設定されます。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。QoS 機能は、ポート単位またはユーザ単位で帯域幅を制限します。スイッチポートは trusted または untrusted で設定します。CoS 値、DSCP 値、または IP precedence を信頼するように trusted ポートを設定できます。untrusted でポートを設定した場合は、ACL を使用し、ネットワークポリシーに従ってフレームをマークできます。

図 1-3 バックボーン構成での配線クローゼットの Catalyst 3550 スイッチ



86391

各配線クローゼット内は、VLAN 内ルーティング用の Catalyst 3550 マルチレイヤ スイッチです。このスイッチは、プロキシ ARP サービスを提供して IP および MAC アドレスのマッピングを決定するので、ルータからこのタスクを取り除き、WAN リンクでのこのタイプのトラフィックを削減します。また、各アップリンク ポートを trusted ルーテッド アップリンクに設定し、アップリンク障害が生じた場合は高速コンバージェンスを行うように設定して、バックボーン スイッチに対して冗長アップリンク接続を行います。

ルータおよび Catalyst 6000 マルチレイヤ バックボーン スイッチは、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。

Catalyst 6000 スイッチにはコア リソースへのギガビット アクセスを実行するワークグループがあります。サーバ ファームには Cisco CallManager ソフトウェアが稼働するコール処理サーバが含まれています。Cisco CallManager は、コール処理、ルーティング、および IP Phone の機能と設定を制御します。

Catalyst 3550 スイッチによる集合住宅ネットワーク

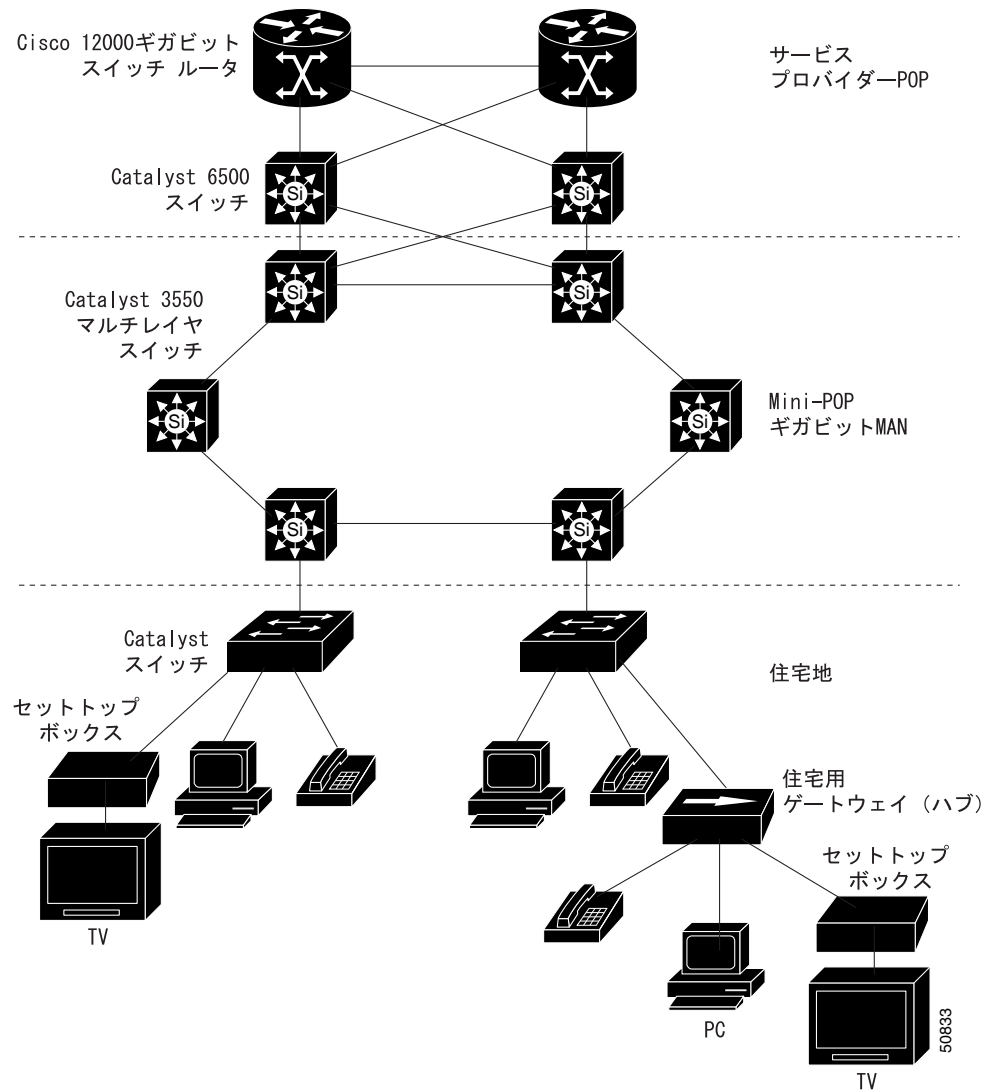
住宅環境および商業環境で、イーサネット Metropolitan-Area Networking (MAN; メトロポリタン エリア ネットワーク) への高速アクセスを必要とするユーザが増加しています。図 1-4 に、Mini-Point-of-Presence (Mini-POP) において Catalyst 3550 マルチレイヤ スイッチを集約スイッチとして使用したギガビット イーサネット MAN リング構成を示します。これらのスイッチは、1000BASE-X GBIC ポート経由で接続しています。

住宅用スイッチとして Catalyst 3550 スイッチを使用し、ユーザがファスト イーサネットまたはギガビット イーサネットで MAN に接続できるようにします。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 2900 LRE XL または 2950 LRE レイヤ 2 専用スイッチを使用することもできます。この場合 Catalyst LRE スイッチは、別の住宅用スイッチまたは集約スイッチに接続できます。

住宅用 Catalyst 3550 スイッチ (および使用されている場合、Catalyst LRE スイッチ) 上のすべてのポートは、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 IEEE 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、加入者がほかの加入者宛パケットを表示できないように、スイッチの各ポートを孤立させることで、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。Catalyst 3550 マルチレイヤ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は、前出の例「[各種スイッチを使用する中小規模のネットワーク](#)」(p.1-14) および「[Catalyst 3550 スイッチのみを使用する大規模ネットワーク](#)」(p.1-16) に記載されているようなサービスを提供します。

図 1-4 MAN 構成の Catalyst 3550 スイッチ



長距離広帯域幅の転送構成

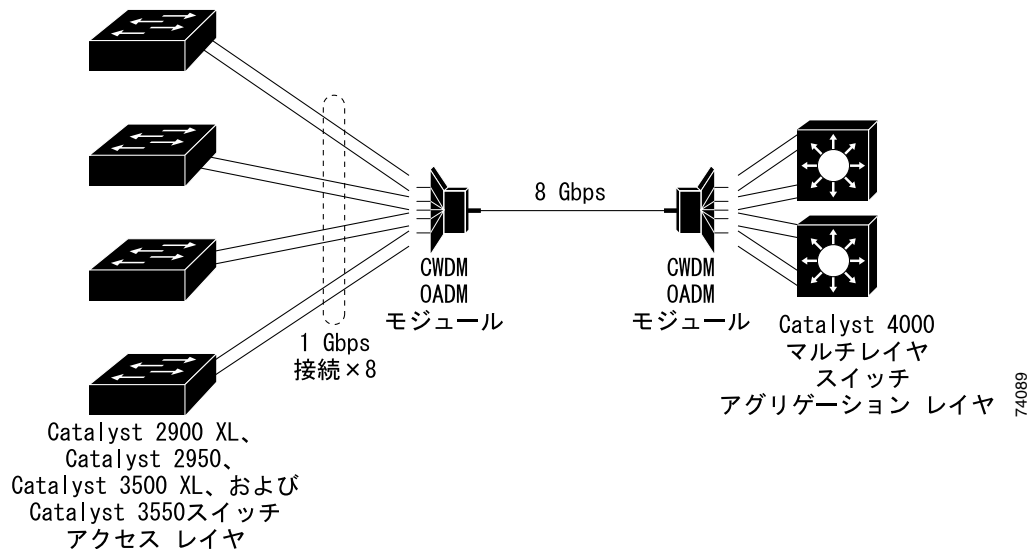
図 1-5 に、1 本の光ファイバケーブルでの 8 ギガビット データ転送用の構成を示します。Catalyst スイッチは、Coarse Wave Division Multiplexer (CWDM; 低密度波長分割多重化) 光ファイバ GBIC モジュールを搭載しています。CWDM GBIC モジュールに応じて、データは 1470 ~ 1610 nm の波長で送信されます。波長が長いほど遠くに伝送できるようになります。長距離伝送に使用される一般的な波長は 1550 nm です。

CWDM GBIC モジュールは、最大 393,701 フィート (74.5 マイルまたは 120 km) の距離で CWDM Optical Add/Drop Multiplexer (OADM; 光分岐挿入) モジュールに接続します。CWDM OADM モジュールは、さまざまな CWDM 波長を結合 (または多重化) して、同じ光ファイバケーブルを同時に移動できるようにします。受信側の CWDM OADM モジュールは、さまざまな波長を分離 (または逆多重化) します。

スイッチで CWDM テクノロジーを使用するという事は、1 本の光ファイバケーブルでのデータ伝送の拡張と帯域幅の拡大を意味します。

CWDM GBIC モジュールおよび CWDM OADM モジュールの詳細については、『*Installation Note for the CWDM Passive Optical System*』を参照してください。

図 1-5 長距離広帯域幅の転送構成



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「IE2100 CNS エージェントの設定」](#)