



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.1-1)
- 「管理オプション」 (P.1-9)
- 「ネットワークの構成例」 (P.1-10)
- 「次の作業」 (P.1-20)

このマニュアルでは、IP は IP Version 4 (IPv4) を意味します。レイヤ 3 IP Version 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

本ソフトウェアは、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 スイッチには、以前は拡張マルチレイヤ イメージ (EMI) と呼ばれていた IP サービス イメージが付属しており、これによって、レイヤ 2+ 機能、完全なレイヤ 3 ルーティング、および拡張サービスが提供されます。Catalyst 3550 ファスト イーサネット スイッチは、以前標準マルチレイヤ ソフトウェア イメージ (SMI) と呼ばれていた IP ベース イメージか、IP サービス イメージがインストールされて出荷されます。IP ベース イメージによって、レイヤ 2+ 機能および基本レイヤ 3 ルーティングを使用できるようになります。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するために、IP サービス イメージ アップグレード キットを注文できます。

使いやすさと簡単な導入

- Express Setup : 基本的な IP 情報、コンタクト情報、スイッチおよび Telnet のパスワード、および簡易ネットワーク管理プロトコル (SNMP) に関する情報を使用し、ブラウザ ベースのプログラムを通じて、スイッチの初回設定を迅速に行うことができます
- ユーザ定義の SmartPort マクロ : ネットワークへの配置を簡単にするためにカスタム スイッチ設定を作成します。

- 組み込み式デバイス マネージャ：単体のスイッチを Web ブラウザから設定および管理します。デバイス マネージャの起動については、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 を使用して、次を行えます。
 - 複数スイッチの統一的な設定、モニタリング、認証、およびソフトウェアのアップグレードを行えます（対応するクラスタ メンバのリストのリリース ノートを参照してください）。
 - 候補スイッチの自動検出と、最大 16 台のスイッチからなるクラスタの作成機能。1 つの IP アドレスを使用してクラスタを管理できます。
 - 拡張検出機能により、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検出できます。
 - イメージを HTTP または TFTP を使用してスイッチにダウンロードします。

パフォーマンス

- すべてのスイッチ ポートの速度自動検知、およびデュプレックス モードの自動ネゴシエーション。帯域幅の利用を最適化します。
- すべてのイーサネット ポート上での IEEE 802.3x フロー制御
- 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。
- Port Aggregation Protocol (PAgP) および Link Aggregation Control Protocol (LACP) により、EtherChannel リンクを自動的に作成します。
- ポート単位のストーム制御。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 ストームを防止します。
- 不明なユニキャストおよびマルチキャスト トラフィックの転送に対するポート 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) マルチキャスト トラフィックのフラッディングを制限するための IGMP スヌーピング
- IGMP レポート抑制。1 つのマルチキャスト ルータ クエリーにつき 1 つの IGMP レポートだけをマルチキャスト デバイスへ送信します (IGMPv1 または IGMPv2 クエリーだけをサポート)。
- 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ながら、帯域幅およびセキュリティ上の理由から、加入者 VLAN からストリームを分離します。
- IGMP フィルタリング。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 セットを管理します。
- IGMP スロットリング。IGMP 転送テーブルのエントリ数が最大になったときのアクションを設定します。
- 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。
- System Database Management (SDM) テンプレートにより、ユーザ側で選択する機能へのサポートを最大化するようにシステム リソースを割り当てられます。

- Web Cache Communication Protocol (WCCP)。トラフィックのローカル キャッシュ エンジンへのリダイレクト、コンテンツ要求のローカルでの対処、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 (拡張マルチレイヤ ソフトウェア イメージが必要) を行います。

管理性

- Cisco Intelligence Engine 2100 (IE2100) シリーズ Cisco Networking Services (CNS) が組み込まれたエージェント。スイッチ管理、ストレージの設定および配信を自動化します。
- Dynamic Host Configuration Protocol (DHCP) によるスイッチ情報 (IP アドレス、デフォルト ゲートウェイ、ホスト名、ドメイン ネーム システム (DNS)、TFTP サーバ名) の自動設定。
- DHCP サーバによる IP アドレスおよびその他の DHCP オプションの IP ホストへの自動割り当て。
- 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)。
- IP アドレスおよび対応するホスト名からスイッチを特定することを目的とした、ユニキャスト要求の DNS サーバへの転送、および TFTP サーバからソフトウェア アップグレードを管理することを目的とした、ユニキャスト要求の TFTP サーバへの転送。
- Address Resolution Protocol (ARP; アドレス解決プロトコル)。IP アドレスおよび対応するメディア アクセス コントロール (MAC) アドレスによってスイッチを特定します。
- 特定の送信元 MAC アドレスおよび宛先 MAC アドレスを持ったパケットをドロップするユニキャスト MAC アドレス フィルタリング。
- Cisco Discovery Protocol (CDP) バージョン 1 および 2。ネットワーク トポロジを検出し、ネットワーク上のスイッチと他のシスコ デバイスとのマッピングを行います。
- ネットワーク タイム プロトコル (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。
- Cisco IOS File System (IFS)。スイッチが使用するすべてのファイル システムに対して単一インターフェイスを提供します。
- スwitchの設定変更を記録して表示させるコンフィギュレーション ロギング。
- 一意のデバイス ID。 **show inventory** ユーザ EXEC コマンドで製品の ID 情報が表示されます。
- Netscape Navigator または Internet Explorer セッションからの組み込みデバイス マネージャ、または Network Assistant アプリケーションにより、インバンド管理にアクセスできます。
- 最大 16 の Telnet 接続を同時に使用できるインバンド管理アクセス。ネットワーク上で複数のコマンドライン インターフェイス (CLI) ベース セッションを実行できます。
- ネットワーク上の複数の CLI セッションに対する、最大 5 つの同時暗号化 Secure Shell (SSH; セキュア シェル) 接続の確立によって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。
- アウトオブバンド管理アクセス。スイッチのコンソール ポートに端末を直接接続するか、またはシリアル接続またはモデム経由でリモート端末に接続します。
- Secure Copy Protocol (SCP) 機能。スイッチ設定またはスイッチ イメージ ファイルをセキュアな認証方法でコピーします (ソフトウェア IP ベースおよび 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

- コマンド スイッチとレイヤ 3 ルータの冗長性のためのホット スタンバイ ルータ プロトコル (HSRP)
- すべてのイーサネット ポート上の単方向リンク検出 (UDLD) およびアグレッシブ UDLD。不正な光ファイバ配線またはポート障害によって発生した光ファイバ インターフェイス上で、単一方向リンクを検出し、ディセーブル化します。
- IEEE 802.1D スパニングツリー プロトコル (STP) による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。STP には次の機能があります。
 - Per-VLAN Spanning-Tree Plus (PVST+) による VLAN 間でのロード バランシング。
 - Rapid PVST+ による VLAN 間でのロード バランシング
 - UplinkFast、クロススタック 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 アップリンクやクロススタック 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 マルチ スパニングツリー プロトコル (MSTP)。複数の VLAN を 1 つのスパニングツリー インスタンスにまとめ、データ トラフィックとロード バランシングを行うための転送パスを複数提供します。
- IEEE 802.1w 高速スパニングツリー プロトコル (RSTP)。ルート ポートおよび指定ポートをただちにフォワーディング ステートに移行することにより、スパニングツリーの高速コンバージェンスを可能にします。
- PVST+、Rapid-PVST+、および MSTP モードで使用できるスパニングツリーのオプション機能は、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します。
 - BPDU ガード。BPDU を受信する PortFast 対応ポートをシャットダウンします。
 - BPDU フィルタリング。PortFast 対応ポートで BPDU の送受信ができなくなります。
 - ルート ガード。ネットワーク コア外のスイッチがスパニングツリー ルートになることを防ぎます。
 - ループ ガード。代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。



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

VLAN のサポート

- 最大 1005 の VLAN をサポート。適切なネットワーク リソース、トラフィック パターン、および帯域幅を対応付けて、VLAN にユーザを割り当てることができます。
- 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。
- ダイナミック VLAN メンバーシップに対応する VLAN Query Protocol (VQP)。

- すべてのポート上で稼働する 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。ネットワークの移動、追加、変更や、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および制御、さらに、ハイセキュリティ ユーザおよびネットワーク リソース別の VLAN グループの確立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; ダイナミック トランキング プロトコル)**。2 台のデバイス間のリンク上でトランキングをネゴシエートするだけでなく、使用するトランキング カプセル化のタイプ (IEEE 802.1Q または ISL) もネゴシエートします。
- **VLAN トランキング プロトコル (VTP) および VTP プルーニング**。トラフィックのフラッドイングをそのトラフィックを受信するステーションへのリンクだけに制限することによって、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、スパンニングツリーループまたはストームのリスクを軽減します。この機能をイネーブルにすると、ユーザトラフィックは送受信されません。スイッチの CPU は、引き続き制御プロトコルフレームの送受信を行います。

セキュリティ

- 管理インターフェイス (デバイス マネージャ、Network Assistant、CLI) へのパスワード保護付きアクセス (読み取り専用および読み書きアクセス)。不正な設定変更を防止します。
- セキュリティ レベル、通知、および対応するアクションを選択できる、マルチレベル セキュリティ。
- セキュリティを確保できるスタティック MAC アドレッシング。
- 保護ポート オプション。同一スイッチ上の指定ポートへのトラフィック転送を制限します。
- ポートにアクセスできるステーションの MAC アドレスを制限または特定するポートセキュリティ オプション。
- VLAN にアクセスできるステーションの MAC アドレスを制限または特定するトランク ポート上のポートセキュリティ。
- ポートセキュリティ エージング。ポートのセキュア アドレスにエージング タイムを設定します。
- 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 インターフェイスでのトラフィックを制限する IP ソース ガード。
- untrusted (信頼性のない) 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する DHCP スヌーピング。
- 不正な ARP 要求や応答を同じ VLAN 上のその他のポートにリレーしないことにより、スイッチに対する悪意のある攻撃を回避するためのダイナミック ARP インспекション。
- ブリッジプロトコルデータ ユニット (BPDU) ガード。無効なコンフィギュレーションが発生した場合に、PortFast が設定されているポートをシャットダウンします。
- 標準および拡張 IP ACL。ルーテッド インターフェイス (ルータ ACL) と双方向およびレイヤ 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 ポリシーを定義します。
- MAC 拡張アクセス コントロール リスト。レイヤ 2 インターフェイスの着信方向のセキュリティ ポリシーを定義します。
- VLAN ACL (VLAN マップ)。MAC、IP、および TCP/User Datagram Protocol (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します。

- 非 IP トラフィックをフィルタリングする、送信元および宛先 MAC ベースの ACL。
- IEEE 802.1x ポートベース認証。不正なデバイス（クライアント）によるネットワーク アクセスを防止します。
- IEEE 802.1x とユーザ単位のアクセス コントロール リスト（ACL）。IEEE 802.1x 認証ユーザに対して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提供します
- IEEE 802.1x と VLAN 割り当てにより、IEEE 802.1x 認証ユーザを指定した VLAN に制限
- IEEE 802.1x とポート セキュリティにより、IEEE 802.1x マルチホスト ポートへのアクセスを制御
- IEEE 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
- IEEE 802.1x とゲスト VLAN により、非 IEEE 802.1x 準拠のユーザに限定されたサービスを提供
- IEEE 802.1x アカウンティング。ネットワーク使用を追跡します。
- IEEE 802.1x と LAN のウェイクアップ機能。休止状態の PC に、特定のイーサネット フレームを送信して起動させます。
- Terminal Access Controller Access Control System Plus（TACACS+）。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独自の機能です。
- 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する Kerberos セキュリティ システム。
- RADIUS を使用すると、アカウンティングの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます
- Secure Socket Layer (SSL) バージョン 3.0 による、HTTP 1.1 サーバ認証、暗号化、メッセージ 整合性のサポート。HTTP クライアント認証によりセキュア HTTP 通信が確保されます。
- IEEE 802.1Q トンネリングにより、サービス プロバイダーのネットワークをまたがるリモート サイトにユーザがいるカスタマーは、その他のカスタマーから VLAN を分離できます。レイヤ 2 プロトコル トンネリングにより、すべてのユーザに関する完全な STP 情報、CDP 情報、VTP 情報が、カスタマー ネットワークに含まれるようになります。
- レイヤ 2 ポイントツーポイント トンネリング。EtherChannel を自動的に作成します。

Quality of Service (QoS) およびサービス クラス (CoS)

- auto-QoS（自動 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 QoS 機能の展開を簡略化します。
- 分類
 - 物理インターフェイスまたはポート単位 VLAN 単位での分類。
 - IP Type of Service/Differentiated Services Code Point (IP ToS/DSCP) および IEEE 802.1p CoS のポート単位でのプライオリティ設定。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します。
 - IP TOS/DSCP および IEEE 802.1P CoS（サービス クラス）のフローベースのパケット分類（MAC、IP、および TCP/UDP ヘッダーに含まれる情報に基づく）によるマーキング。ネットワーク エッジで高性能な QoS 機能を提供し、ネットワーク トラフィックのタイプ別に差別化されたサービス レベルを可能にするとともに、ネットワーク上のミッション クリティカルなトラフィックにプライオリティを設定します。
 - QoS ドメイン内および別の QoS ドメインとの境界ポートにおける、trusted（信頼性のある）ポート ステート（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。
- ポリシング
 - 物理インターフェイスまたはポート単位 VLAN 単位でのポリシング。
 - 特定のトラフィック フローに対してどの程度のポート帯域幅を割り当てるかを管理する、スイッチ ポート上のトラフィック ポリシング ポリシー。
 - トラフィック フローのポリシングをまとめて行う集約ポリシング。特定のアプリケーションまたはトラフィック フローをあらかじめ定義された特定のレートに制限します。
 - 入力ギガビット対応イーサネット ポート上で、最大 128 のポリサー
入力 10/100 ポート上で、最大 8 つのポリサー
出力ポート（集約ポリサーのみ）ごとに最大 8 個のポリサー
- 不適合
 - 帯域幅の使用制限を超過したパケットの不適合マークダウン。
- 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 ポートの 4 個の出力キュー。これらのキューは、重み付けラウンドロビン（WRR）スケジューリング アルゴリズムを使用して設定するか、1 個のキューを完全プライオリティ キューとし、他の 3 個のキューを WRR 用に設定できます。完全プライオリティ キューは、他の 3 個のキューが処理される前に空になっていることが必要です。ミッション クリティカルおよび時間依存のトラフィックに完全プライオリティ キューを使用できます。
 - ギガビットイーサネット ポートの輻輳を回避するためのテール ドロップと重み付けランダム 早期検出（WRED）テクノロジー。ファストイーサネット ポートの輻輳回避のためのテール ドロップ

レイヤ 3 のサポート

一部の機能およびプロトコルには、拡張マルチレイヤ ソフトウェア イメージが必要です。

- レイヤ 3 ルータの冗長性のためのホット スタンバイ ルータ プロトコル（HSRP）
- 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 2
 - Open Shortest Path First（OSPF）
 - Enhanced IGRP（EIGRP）
 - Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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
- カスタマー エッジ（CE）装置内の Multiple VPN Routing/Forwarding（multi-VRF）インスタンス により、サービス プロバイダーが複数のバーチャル プライベート ネットワーク（VPN）をサポート し、VPN 間で IP アドレスが重複できるようにします。
- ポリシーベース ルーティング（PBR）。トラフィック フローに定義済みポリシーを設定。
- フォールバック ブリッジングにより、2 つ以上の VLAN 間で非 IP トラフィックを転送できます。
- 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。
- ディスタンスベクトルマルチキャストルーティングプロトコル (DVMRP) トンネリング。非マルチキャストネットワークで 2 つのマルチキャスト対応ネットワークを相互接続。
- 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) 認識。プライマリルートプロセッサ (RP) がクラッシュしており、バックアップ RP が引き継いでいる間、またはプライマリ RP で無停止のソフトウェアアップグレードのリロードが手動で行われている間、レイヤ 3 スイッチは NSF 対応隣接ルータからのパケットを継続して転送することができます (IP サービスイメージが必要)。

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。
- Switched Port Analyzer (SPAN; スイッチドポートアナライザ) および Remote SPAN (RSPAN)。任意のポートまたは VLAN について、トラフィックモニタリングが可能です。
- 侵入検知システム (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をモニタ、撃退、およびレポートします。
- 組み込み Remote Monitoring (RMON; リモートモニタリング) エージェントの 4 つのグループ (履歴、統計、アラーム、およびイベント)。ネットワークをモニタリングし、トラフィック解析を行います。
- Syslog 機能。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を記録します。
- MAC アドレス通知。スイッチが学習または削除した MAC アドレスを保存することによって、ネットワーク上のユーザをトラッキングします。
- 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します。

Catalyst 3550-24PWR スイッチでの Power over Ethernet のサポート

- 回路に電気が流れていないことがスイッチにより検出されたときに、PoE 対応ポートから、接続された Cisco 準規格の受電デバイス、および IEEE 802.3af 準拠の受電デバイスに電力を提供することができます。
- 電力消費を伴う CDP のサポート。受電デバイスは、スイッチが消費している電力量を、このスイッチに知らせます。
- Cisco インテリジェント電力管理のサポート。受電デバイスとスイッチは、電力消費レベルの合意に向け、電力ネゴシエーション CDP メッセージを通じてネゴシエーションします。このネゴシエーションにより、高性能の Cisco 受電デバイスが最高の電力モードで動作できるようになります。

- 自動検出および電力バジェット。スイッチは、電力バジェットの維持、電力要求のモニタおよび追跡を行いながら、電力が使用可能である場合だけ電力を許可します。
- デバイスマネージャと Network Assistant を通じた冷却ファン障害と過熱検出

管理オプション

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、スイッチの基本的な IP 情報を設定し、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。特定のネットワーク要件があれば、その多彩な管理インターフェイスを通して、スイッチを個別にまたはスイッチ クラスタの一部として設定およびモニタできます。

管理インターフェイス オプション

これらのインターフェイスを使用して、個々のスイッチおよびスイッチ クラスタを設定および監視できます。

- **組み込みデバイス マネージャ** : GUI のデバイス マネージャがソフトウェア イメージに組み込まれています。このデバイス マネージャは、単体のスイッチの設定、管理に使用します。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。単一のスイッチまたはスイッチのクラスタを管理するのに使用します。Network Assistant の詳細については、Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。
- **CLI** : スwitchの Cisco IOS ソフトウェアは、デスクトップ スイッチングおよびマルチレイヤ スイッチング機能をサポートします。CLI にアクセスするには、管理ステーションをスイッチ 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 を利用します。

CLI の詳細については、第 2 章「[コマンドライン インターフェイスの使用](#)」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 ソフトウェア内蔵の CNS エージェントとともに動作するネットワーク管理デバイスです。スイッチごとに設定変更の内容を生成してスイッチに送信し、その設定変更を適用した後、その結果を記録することで初期設定および設定の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 を使用して、スイッチおよびスイッチ クラスタ メンバをモニタおよび制御できます。CiscoWorks2000 LAN Management Suite (LMS) や 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、セキュリティを管理し、また統計情報を収集できます。

HP OpenView、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からスイッチを管理できます。スイッチは豊富な MIB 拡張機能および 4 つの RMON グループをサポートします。

SNMP の詳しい使用方法については、第 27 章「[SNMP の設定](#)」を参照してください。

Network Assistant およびクラスタリング スイッチを使用する利点

Network Assistant とスイッチ クラスタを使用することにより、設計タスクとモニタリング タスクを簡潔にし、また最少にできます。最大 16 台の相互接続されたサポートされている Catalyst スイッチを 1 つの IP アドレスから管理するために、Cisco スイッチ クラスタリング テクノロジーを使用できます。

これにより、IP アドレスの数が制限されている場合に、IP アドレスを節約できます。Network Assistant は最も使いやすいインターフェイスであり、権限を持つユーザは、このインターフェイスを使用することにより、ネットワーク上の任意の PC からスイッチおよびスイッチ クラスタの管理を行います。

スイッチ クラスタと Network Assistant を使用して、次のことが可能です。

- 地理的な近さや、イーサネット、ファストイーサネット、Fast EtherChannel、Cisco ギガスタック ギガビット インターフェイス コンバータ (GBIC)、ギガビットイーサネットおよびギガビット EtherChannel 接続を含む相互接続メディアに関係なく、相互接続されている Catalyst スイッチ (サポート対象スイッチのリストについては、リリース ノートを参照してください) を管理および監視します。
- 1 つの Network Assistant ウィンドウを使用して、複数の設定作業を行うことができます。特定の処理を実行するための CLI コマンドを覚える必要はありません。
- Network Assistant から複数のポートと複数のスイッチに、アクションを同時に適用します。複数のポートとスイッチを設定および管理するいくつかの例を示します。
 - 速度やデュプレックス設定などのポート設定
 - 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 と QoS 設定
 - インベントリおよび統計情報の報告、およびリンクおよびスイッチ レベルのモニタリングとトラブルシューティング
 - グループのソフトウェア アップグレード
- 既存のスイッチ クラスタおよびクラスタに参加できる適格なスイッチを識別するために、相互接続されたデバイスのトポロジを表示します。また、トポロジを使用して、スイッチ間のリンク情報を簡単に確認することもできます。
- 前面パネル イメージに表示される LED によって、単独または複数のスイッチの状態をリアルタイムでモニタできます。このイメージに表示されるシステム LED、冗長電源システム (RPS) LED、およびポート LED の色は、実際の LED の色と同じです。
- インタラクティブ モードを使用して、VLAN、ACL、および QoS などの複雑な機能を設定する手順を一歩ずつ進めます。
- ウィザードを使用して、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、セキュリティといった複雑な機能を設定するために必要な最小限の情報のみを、プロンプトの指示に従って入力します。

Network Assistant ソフトウェアとブラウザの要件、クラスタ化の詳細については、Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。サポートされた Cisco IOS リリースを含むクラスタ化の要件については、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。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て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も示します。

- 「スイッチを使用する場合の設計概念」 (P.1-11)
- 「混合スイッチを使用した中小規模のネットワーク」 (P.1-15)
- 「Catalyst 3550 スイッチのみを使用する大規模ネットワーク」 (P.1-17)

- 「Catalyst 3550 スイッチによる集合ネットワーク」 (P.1-18)
- 「長距離広帯域トランスポートの構成」 (P.1-20)

スイッチを使用する場合の設計概念

ネットワーク帯域幅をめぐってネットワーク ユーザが競合すると、データの送受信に要する時間が長くなります。ネットワークを設計する時点で、ネットワーク ユーザが必要とする帯域幅を考慮するとともに、ユーザが使用する各種ネットワーク アプリケーションの相対的な優先順位について検討する必要があります。

表 1-1 に、ネットワーク パフォーマンスが低下する原因を説明するとともに、ネットワーク ユーザが使用できる帯域幅を増加させるための、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

ネットワークに対する需要	推奨する設計方式
1つのネットワーク セグメントに多くのユーザが集中しすぎ、インターネットへアクセスするユーザが増加している	<ul style="list-style-type: none"> • 帯域幅を共有するユーザ数が少なくなるように、より小さいネットワーク セグメントを作成します。さらに VLAN および IP サブネットを使用して、ネットワーク リソースに頻繁にアクセスするユーザと同じ論理ネットワーク上に、そのリソースを配置します。 • スイッチと接続先ワークステーションとの間で、全二重通信を使用します。
<ul style="list-style-type: none"> • 新しい PC、ワークステーション、およびサーバのパワーの増大 • ネットワーク アプリケーション (大容量の添付ファイル付き電子メールなど) 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) による帯域幅需要の増大 	<ul style="list-style-type: none"> • ネットワーク ユーザが等しくアクセスする必要があるサーバ、ルータなどのグローバル リソースを高速スイッチ ポートに直接接続し、各ユーザに専用の高速セグメントを与えます。 • スイッチと接続先サーバおよびルータ間で EtherChannel 機能を使用します。

ネットワーク設計では、帯域幅が唯一の考慮事項というわけではありません。ネットワークトラフィックのプロファイルが発展するにしたがって、音声とデータの統合、マルチメディアの統合、アプリケーションのプライオリティ処理、およびセキュリティに対応するアプリケーションをサポートできるようなネットワークサービスの提供を検討してください。表 1-2 で、ネットワークに対する需要について説明し、その需要を満たす方法を示します。

表 1-2 ネットワーク サービスの提供

ネットワークに対する需要	推奨する設計方式
マルチメディアアプリケーションにおける帯域幅の効率的な利用およびミッションクリティカルなアプリケーションに対する帯域幅保証	<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、他の QoS メカニズムを使用し、適切なプライオリティレベルを指定してトラフィックを分類し、最大限の柔軟性を得ながら、ミッションクリティカルなユニキャスト、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できるようにします。 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 上でマルチキャストストリームを継続的に送信しますが、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 から分離します。
常時オンのミッションクリティカルなアプリケーションを実現するための、ネットワークの冗長性に対する高い需要	<ul style="list-style-type: none"> ルータの冗長性のために HSRP を使用します。 VLAN トランク、クロススタック 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 テレフォニーに対する新しい需要	<ul style="list-style-type: none"> QoS を使用して、輻輳の発生時に IP テレフォニーなどのアプリケーションを優先順位付けし、ネットワーク内で発生する遅延およびジッタを制御できるようにします。 1 ポートあたり少なくとも 2 つのキューをサポートするスイッチを使用して、音声およびデータトラフィックのプライオリティを IEEE 802.1p/Q に基づくハイプライオリティまたはロープライオリティのいずれかに設定します。 音声トラフィックに個別の VLAN を使用するには、Catalyst 2900 XL スイッチおよび 3500 XL スイッチで音声 VLAN ID (VVID) を使用します。
既存のインフラストラクチャを利用して、自宅または会社からインターネットまたはイントラネットへデータおよび音声を高速で伝送する需要の増大	<p>既存の電話回線など、既存のインフラストラクチャ上での最大 15 Mb の IP 接続を提供するには、Catalyst 2900 LRE XL および Catalyst 2950 LRE スイッチを使用します。</p> <p>(注) Long-Reach Ethernet (LRE) は、Catalyst 2900 LRE XL および Catalyst 2950 LRE スイッチに採用されているテクノロジーです。これらのスイッチと LRE テクノロジーについては、スイッチのマニュアルセットを参照してください。</p>

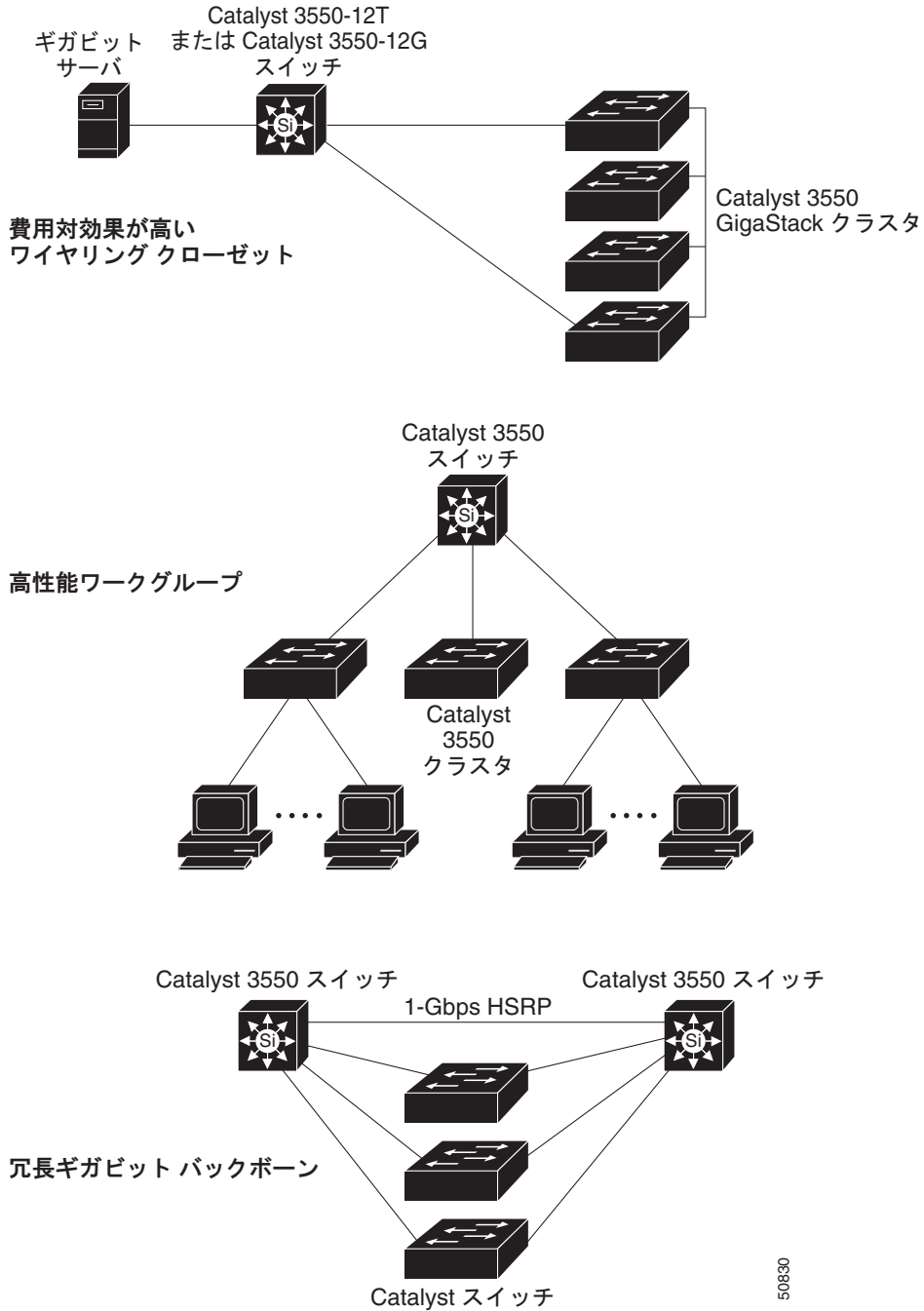
図 1-1 には、Catalyst スイッチを使用して次を作成する際の、3 つの設定例が示されています。

- コスト効率の高いワイヤリングクローゼット：ワイヤリングクローゼットに多数のユーザを接続するコスト効率の高い手法は、GigaStack GBIC 接続を介して最大 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 スイッチの組み合わせ）の Catalyst スイッチクラスタを接続することです。スタック内の 1 台のスイッチに

障害が発生した場合、スイッチの接続を維持するには、最下部のスイッチを最上部の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 アップリンク上でクロススタック UplinkFast をイネーブルにします。

ギガビット GBIC モジュールを使用して、GigaStack クラスタから Catalyst 3550-12T や Catalyst 3550-12G スイッチなどのギガビット バックボーン スイッチへの冗長なアップリンク接続を使用できます。ファスト イーサネット リンク、ギガビット リンク、または EtherChannel リンクを使用することによって、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発生しても、もう一方がバックアップ パスとして機能します。単一の IP アドレスを使用してスタック メンバを管理するために、Catalyst 3550-12T または Catalyst 3550-12G スイッチをスイッチ クラスタ マネージャとして設定できます。Catalyst 3550-12T または Catalyst 3550-12G スイッチは、1000BASE-T 接続を介してギガビット サーバに接続できます。

図 1-1 設定例



- 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。輻輳を回避するために、各スイッチ上で QoS DSCP マーキングによるプライオリティ設定を使用します。ディストリビューション レイヤで高速 IP 転送を実現するには、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。

50830

この構成では、各スイッチはバックボーンのネットワーク リソースにアクセスするための、専用の 1 Gbps 接続をユーザに提供します。これを、1 Gbps 接続がスタック内のスイッチ間で共有される GigaStack 設定のスイッチと比較してください。また、これらのギガビット GBIC モジュールにより、media および distance オプションでの柔軟性が高まります。

- 1000BASE-T GBIC : 最大 328 フィート (100 m) の銅線接続
 - 1000BASE-SX GBIC : 最大 1804 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、ネットワーク障害発生時のネットワーク コンバージェンスも高速化されます。Catalyst スイッチは再びスター型構成で、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。

混合スイッチを使用した中小規模のネットワーク

図 1-2 に、最大 500 人の社員を対象とするネットワークの構成例を示します。このネットワークは、Catalyst 3550 マルチレイヤ スイッチを使用して、最大 10 個のワイヤリング クローゼットを、高速アップリンクを介して集約します。ネットワークの信頼性を確保し、ロードバランシングを行うために、このネットワークは 2 台のルータと 2 台の Catalyst 3550 マルチレイヤ スイッチが、すべて HSRP がイネーブルにされた状態で含まれます。これにより、万ルータや Catalyst 3550 マルチレイヤ 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。

ワイヤリング クローゼットには、Catalyst 3550、Catalyst 3500 XL、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチなどのスイッチの組み合わせがあります。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されています。これらのスイッチは、図に示されているように複数のクラスタにするか、単一のクラスタにできます。クラスタメンバの地理的な位置に関係なく、プライマリおよびセカンダリ コマンド スイッチの IP アドレスでクラスタを管理できます。

このネットワークでは、VLAN を使用してネットワークを明確なブロードキャスト グループとして論理的に分割し、セキュリティ管理を行っています。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は同じ VLAN 上で設定されます。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。ワイヤリング クローゼットごとに最大 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を同じ VLAN に割り当てる場合は、ワイヤリング クローゼットごとに 1 つの VLAN しか設定できません。Cisco IP Phone に接続されているスイッチポートでは、IEEE 802.1P/Q QoS が、データトラフィックよりも音声トラフィックの転送を優先させます。

Cisco IP Phone は、Catalyst 3550-24PWR スイッチ上の 10/100 PoE ポートと Catalyst 3550 スイッチの 10/100 ポートに接続されています (標準のストレート ケーブル、RJ-45 コネクタを備えたツイストペア ケーブルを使用)。これらのマルチサービス スイッチポートは、接続されているすべての 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 機能とその設定を制御します。Cisco SoftPhone ソフトウェアを実行しているワークステーションを使用するユーザは、PC からのコールを配置、受信、および制御できます。Cisco IP Phone、CCM ソフトウェア、および Cisco SoftPhone ソフトウェアを使用することで、テレフォニーと IP ネットワークを統合でき、IP ネットワークが音声とデータをサポートします。

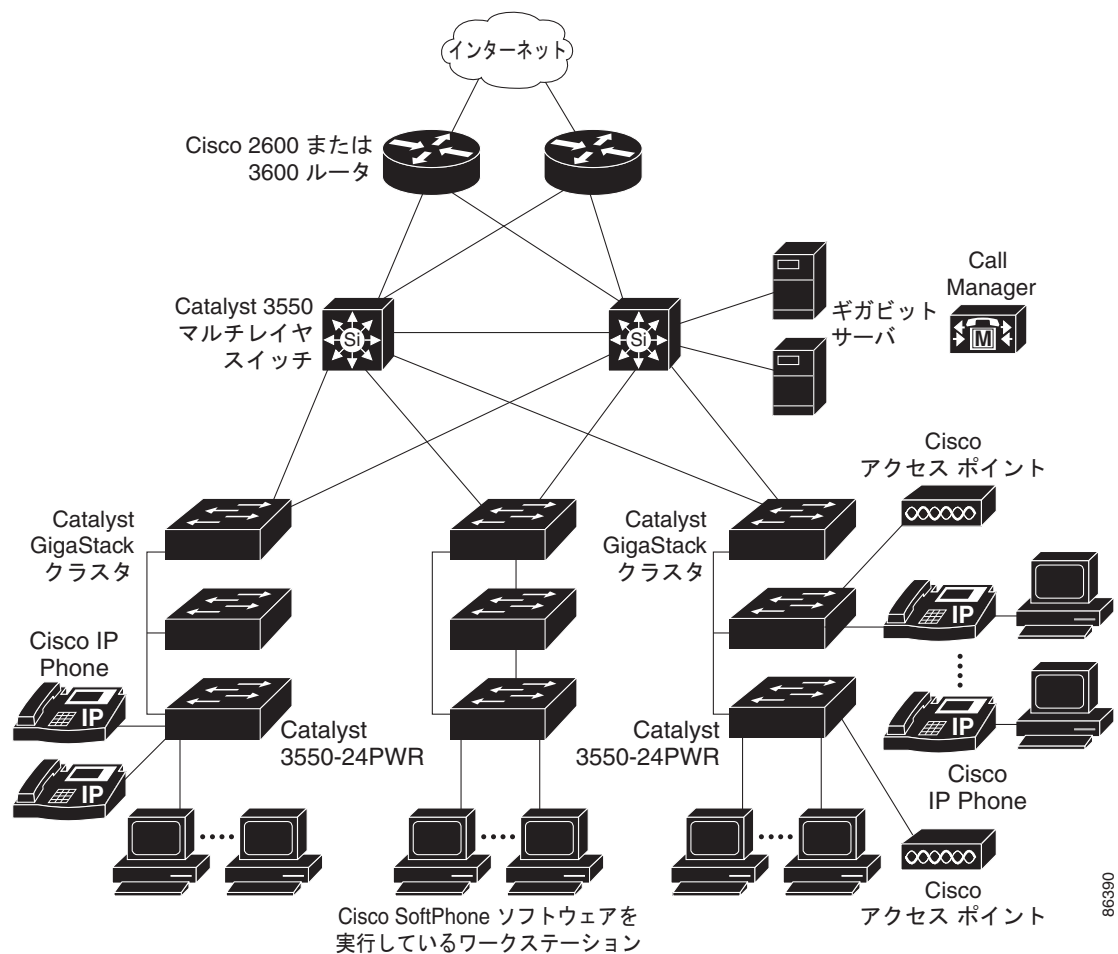
Catalyst 3550-24PWR スイッチの各 10/100 PoE ポートはポートあたり 15.4 W の電力を供給します。IP 電話が AC 電源にも接続されている場合、冗長電力を受け取ることができます。Catalyst 3550-24PWR スイッチに接続されていない IP Phone は、AC 電源から電力を供給されます。

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適切な宛先 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は、VLAN 間ルーティングを提供します。Catalyst 3550 スイッチ上の VLAN アクセスコントロールリスト (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領域にアクセスしないようにします。

VLAN 間ルーティング以外に、Catalyst 3550 マルチレイヤスイッチが 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、ハイプライオリティトラフィックを予測可能な方法で配信します。輻輳が発生した場合、QoS が低優先順位トラフィックをドロップし、高優先順位トラフィックを伝送できるようにします。

VLAN 間ルーティングや他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、ルータが重点を置くのは、ファイアウォールサービス、ネットワークアドレス変換 (NAT) 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アクセスです。

図 1-2 Catalyst 3550 スイッチ (コラプスト バックボーン設定)



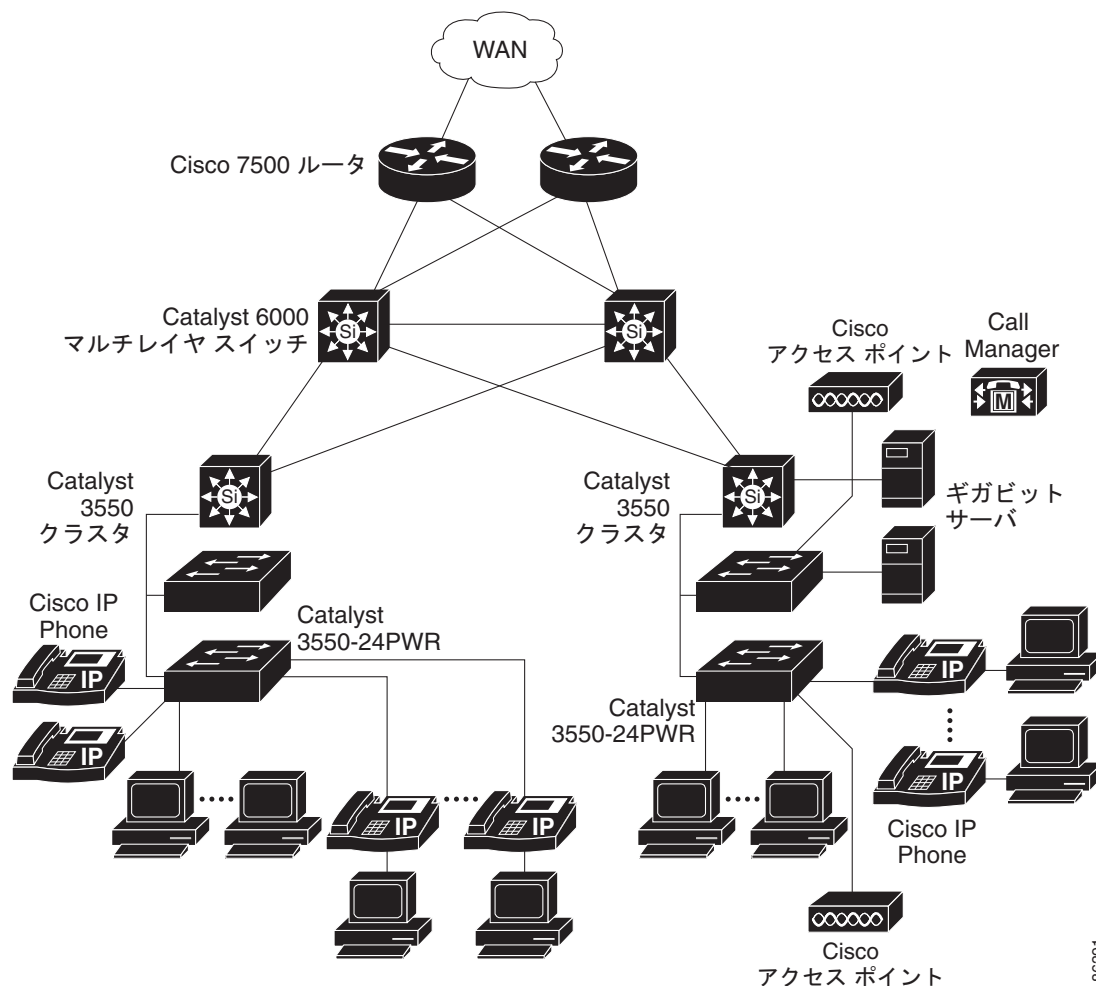
06390

Catalyst 3550 スイッチのみを使用する大規模ネットワーク

ワイヤリング クローゼット内のスイッチは、従来、レイヤ 2 専用のデバイスでしたが、ネットワークトラフィック プロファイルが拡大するにつれ、ワイヤリング クローゼット内のスイッチで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 サービスがますます採用されつつあります。図 1-3 に、ワイヤリング クローゼットで Catalyst 3550 マルチレイヤ スイッチのみを使用し、バックボーンに最大 10 のワイヤリング クローゼットを集約する Catalyst 6000 スイッチを使用するネットワークの構成を示します。

ワイヤリング クローゼットの各 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る、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、各スイッチ上で設定されます。VLAN マップは VLAN 内セキュリティを提供し、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ワイヤリング クローゼットの Catalyst 3550 スイッチ



1698

各ワイヤリング クローゼット内には、VLAN 間ルーティングのための Catalyst 3550 マルチレイヤ スイッチがあります。これらのスイッチは、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 スイッチでは、HSRP をイネーブルにすることで、ロード バランシングおよび冗長接続を実行可能にし、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 スイッチにより、ワークグループに次コア リソースへのギガビット アクセスが提供されます。サーバファームには、Cisco CallManager (CCM) ソフトウェアを実行するコール処理サーバが含まれます。Cisco CallManager は、コール処理、ルーティング、および IP Phone 機能とその設定を制御します。

Catalyst 3550 スイッチによる集合ネットワーク

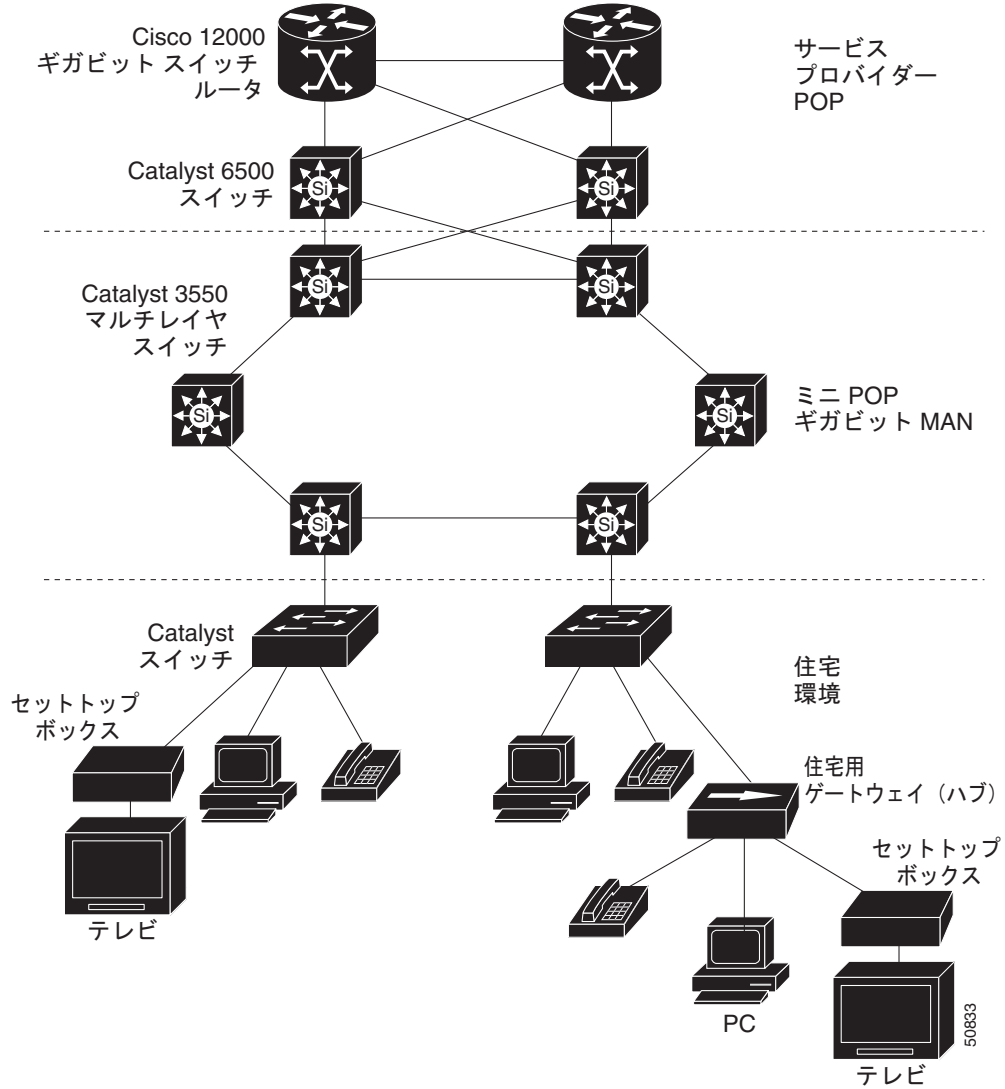
住宅地域および商業地域で、イーサネット Metropolitan-Area Networking (MAN; メトロポリタン エリア ネットワーク) への高速アクセスを必要とするユーザが増加しています。図 1-4 に、Catalyst 3550 マルチレイヤ スイッチをミニ Point Of Presence (POP) ロケーションの集約スイッチとして使用する、ギガビットイーサネット MAN リングの設定を示します。これらのスイッチは、1000BASE-X GBIC ポート経由で接続しています。

住宅用スイッチとして Catalyst 3550 スイッチを使用し、ユーザが MAN に高速接続できるようにします。既存の電話回線による接続が必要なユーザの場合は、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できます。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。保護ポート機能はスイッチ上の各ポートを孤立させることで、加入者が他の加入者宛てにパケットを見ることができないようにして、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 がイネーブルに設定されています。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。

集約スイッチとルータは、「混合スイッチを使用した中小規模のネットワーク」(P.1-15) と「Catalyst 3550 スイッチのみを使用する大規模ネットワーク」(P.1-17) で前に紹介した例で説明したサービスなどを提供します。

図 1-4 MAN 構成の Catalyst 3550 スイッチ



長距離広帯域トランスポートの構成

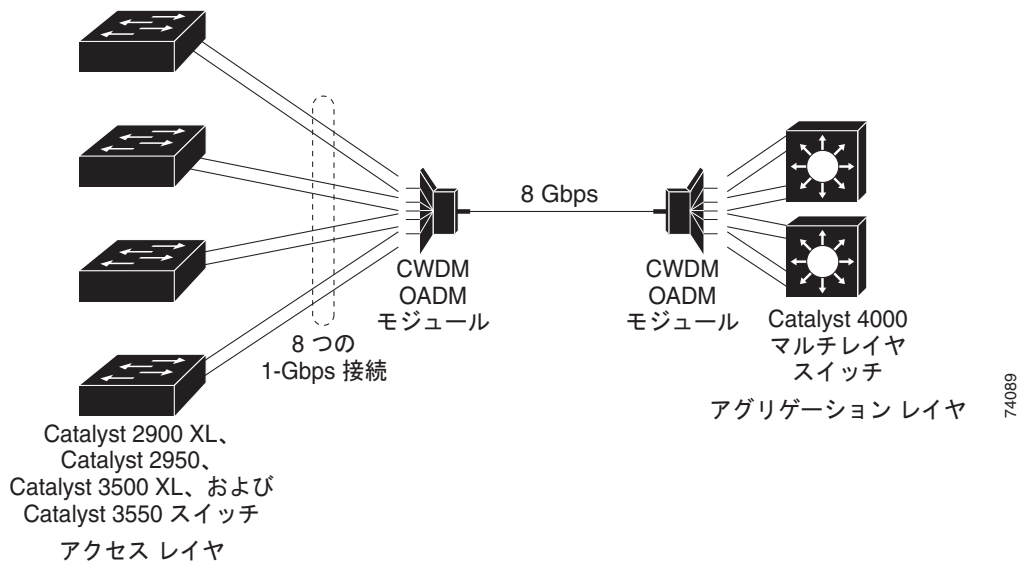
図 1-5 に、8 Gbps のデータを 1 本の光ファイバ ケーブルで転送する構成を示します。Catalyst スイッチには、Coarse Wavelength-Division Multiplexer (CWDM) 光ファイバ GBIC モジュールが搭載されています。CWDM GBIC モジュールに応じて、データは 1470 ~ 1610 nm の波長で送信されます。波長が高くなるほど、伝送できる距離が長くなります。長距離伝送用に使われる一般的な波長は 1550 nm です。

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 オプティカル Add/Drop マルチプレクサ (OADM) 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 (多重化して)、同じ光ファイバ ケーブル上で同時に伝送できるようにします。受信側エンドの CWDM OADM モジュールは、さまざまな波長を分離 (逆多重化) します。

スイッチとともに CWDM テクノロジーを使用すると、より離れた場所までデータ伝送が行われ、単一の光ファイバ ケーブルでの帯域幅キャパシティが (最大 8 Gbps まで) 増加するように変換されます。

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 長距離広帯域トランスポートの構成



次の作業

スイッチを設定する前に、スタートアップ情報について次の各章を参照してください。

- ・ 第 2 章「コマンドライン インターフェイスの使用」
- ・ 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」