



## 概要

この章では、Catalyst 3750-X および 3560-X スイッチ ソフトウェアに関する次の内容について説明します。

- 「機能」 (P.1-1)
- 「スイッチ初期設定後のデフォルト値」 (P.1-18)
- 「ネットワークの構成例」 (P.1-21)
- 「次の作業」 (P.1-35)

スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

このマニュアル内の *IP* という用語は、特に IP Version 6 (IPv6) を参照している場合を除き、IP Version 4 (IPv4) を意味します。



(注)

このマニュアルに掲載している例は、Catalyst 3750-X スイッチのものです。Command-Line Interface (CLI; コマンドライン インターフェイス) でインターフェイスを表示する場合、Catalyst 3750-X スイッチでは、たとえば *gigabitethernet 1/0/5* となります。この例は Catalyst 3560-X スイッチにも適用されます。前の例では、Catalyst 3560-X スイッチで指定するインターフェイスは、*gigabitethernet0/5* (スタック メンバー番号の *1/* はなし) となります。

## 機能

このスイッチは、サービス サポート契約なしで、カスタマーに対して IP ベース ソフトウェア イメージ (ペイロード暗号化付きまたはペイロード暗号化なし) をサポートしています。このイメージは、IP ベースおよび LAN ベースのフィーチャ セットをサポートしています。サービス契約を締結しているカスタマーは、ユニバーサル イメージ (ペイロード暗号化あり、またはなし) を受け取ります。これには、LAN ベース、IP ベース、および IP サービスのフィーチャ セットが含まれます。ペイロード暗号化イメージを実行しているスイッチでは、管理トラフィックとデータ トラフィックを暗号化できます。非ペイロード暗号化イメージを実行しているスイッチでは、SSH 管理セッションなどの管理トラフィックだけを暗号化できます。

特定のフィーチャ セットをイネーブルにするには、Cisco IOS ソフトウェア ライセンスが必要です。ソフトウェア ライセンスの詳細については、Cisco.com の『*Cisco IOS Software Installation*』を参照してください。

スイッチは、次のいずれかのフィーチャ セットをサポートしています。

- 基本的なレイヤ 2+ 機能を提供する LAN ベースのフィーチャ セット。これには、Access Control List (ACL; アクセス コントロール リスト) と Quality of Service (QoS) が含まれます。

- レイヤ 2+ 機能、および基本的なレイヤ 3 機能（エンタープライズ クラス インテリジェント サービス）を提供する IP ベースのフィーチャ セット。これらの機能としては、ACL、QoS、スタティック ルーティング、Enhanced Interior Gateway Routing Protocol (EIGRP) スタブルーティング、PIM スタブルーティング、Hot Standby Router Protocol (HSRP)、Routing Information Protocol (RIP)、基本 IPv6 管理などがあります。
- IP サービス フィーチャ セット：より豊富なエンタープライズクラスのインテリジェント サービス セットを提供し、IPv6 を完全にサポートします。この機能には、すべての IP ベース フィーチャと完全なレイヤ 3 ルーティング（IP ユニキャスト ルーティング、IP マルチキャスト ルーティング、およびフォールバック ブリッジング）があります。IP サービス フィーチャ セットには、EIGRP や Open Shortest Path First (OSPF) などのプロトコルがあります。また、このフィーチャ セットは、IPv6 ルーティングや、IPv6 ACL および Multicast Listener Discovery (MLD) スヌーピングなどのすべての IP サービス フィーチャもサポートします。



**(注)** 特に明記しないかぎり、このマニュアルで取り上げる機能はすべて、すべてのフィーチャ セットでサポートされています。

スイッチの機能は次のとおりです。

- 「導入機能」(P.1-2)
- 「パフォーマンス向上機能」(P.1-4)
- 「管理オプション」(P.1-6)
- 「管理の簡易性に関する機能」(P.1-6)
- 「アベイラビリティおよび冗長性に関する機能」(P.1-8)
- 「VLAN 機能」(P.1-10)
- 「セキュリティ機能」(P.1-10)
- 「QoS および CoS 機能」(P.1-14)
- 「レイヤ 3 機能」(P.1-15)
- 「PoE 機能」(P.1-16)
- 「モニタ機能」(P.1-17)

## 導入機能

- 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 Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 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。Express Setup の詳細については、『Getting Started Guide』を参照してください。
- ユーザ定義およびデフォルト設定の 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。
- ユーザ定義およびデフォルト設定の自動 SmartPort マクロ : ポート上で検出されたデバイス タイプに基づいて動的にポートを設定します。
- AutoSmartPort 拡張では、グローバル マクロ、ラスト リゾート マクロ、イベント トリガー コントロール、アクセス ポイント、EtherChannels、Cisco Medianet を備えた自動 QoS、および IP Phone のサポートが追加されています。

- 組み込みのデバイス マネージャ GUI : 単体のスイッチを Web ブラウザから設定、管理します。デバイス マネージャの起動については、『Getting Started Guide』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。
- Cisco Network Assistant (*Network Assistant*) の機能概要。
  - 管理コミュニティは、ルータやアクセス ポイントを組み込むことができる点や、セキュリティを強化できる点以外は、クラスタと同じようなデバイス グループです。
  - イン트라ネットの任意の場所から、スイッチ、スイッチ スタック、およびスイッチ クラスタを簡単に最小限の手間で管理できます。
  - 1 つの GUI 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。
  - 対話式のガイド モードで、VLAN、ACL、Quality of Service (QoS) などの複雑な機能をガイドに従って設定できます。
  - 設定ウィザードを使用すると、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を、プロンプトの指示に従って入力するだけで済みます。
  - スwitchにイメージをダウンロードできます。
  - VLAN および QoS の設定、目録および統計レポート、リンクおよびスイッチ レベルでのモニタとトラブルシューティング、複数のスイッチのソフトウェア アップグレードといったアクションを、複数のポート、複数のスイッチに対して同時に実行できます。
  - 相互接続されたデバイスのトポロジを表示して、既存のスイッチ クラスタ、クラスタに参加できる適格なスイッチ、およびスイッチ間のリンク情報を確認できます。
  - 前面パネル イメージで表示される 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、Redundant Power System (RPS; 冗長電源システム) LED、およびポート LED の色は、実際の LED の色と同じです。
- Catalyst 3750-X スwitchの Cisco StackWise Plus テクノロジーの概要。
  - StackWise Plus ポートを使用して最大 9 台のスイッチを接続し、ネットワーク内で単一のスイッチまたはスイッチルータとして動作します。
  - スwitch スタック全体で、双方向 32 Gbps スwitchング ファブリックを作成できます。スイッチ スタックでは、すべてのスタック メンバーがシステム帯域にフルにアクセスできます。
  - 単一の IP アドレスとコンフィギュレーション ファイルを使用して、スイッチ スタック全体を管理できます。
  - 新規スタックメンバーの自動 Cisco IOS バージョン検査。スタック マスターまたは TFTP サーバから自動的にイメージをロードするオプションがあります。
  - スタックの動作を中断せずに、スタック内のスイッチを追加、削除、交換します。
  - オフラインの設定機能を使用して、スイッチ スタックに新しいメンバーを割り当てます。特定のスタック メンバー番号、およびスタックに属していない新しいスイッチの特定のスイッチ タイプを、インターフェイス コンフィギュレーションに事前設定します。割り当てられたスイッチがスタックの一部であるかどうかには関係なく、スイッチ スタックはスタック リロードでこの情報を保持します。
  - スタックリング アクティビティ統計情報 (各スタック メンバーからリングに送信されたフレーム数) を表示します。

Catalyst 3750-X、Catalyst 3750-E、および 3750 混合スイッチ スタックでのスタッキングの相互作用については、Cisco.com の『Cisco IOS Software Installation』を参照してください。

- IP ベースまたは IP サービスのフィーチャセットを実行している Catalyst 3750-X スイッチの StackPower テクノロジー。最大 4 台のスイッチにパワースタック ケーブルを接続した場合、スイッチと接続デバイスの電力共有または冗長性のために、単一の電源装置として、個々のスイッチ電源装置を管理できます。
- スイッチのクラスタ化テクノロジーの機能概要。
  - イーサネット、ファストイーサネット、Fast EtherChannel、着脱可能小型フォームファクタモジュール、ギガビットイーサネット、Gigabit EtherChannel、10 ギガビットイーサネット、10 ギガビット EtherChannel 接続を含めて、地理的な近接にも相互接続メディアにも関係なく、複数のクラスタ対応スイッチの設定、モニタ、認証、およびソフトウェアアップグレードをまとめて実行できます。クラスタ対応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。
  - 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。
- ネットワーク内の単一のポイントからの管理（管理者）を可能にするスマートインストール。スマートインストールを使用すると、すべてのクライアントスイッチに対して、新規に展開されたスイッチのゼロタッチイメージおよび設定のアップグレード、イメージおよび設定のダウンロードを行うことができます。詳細については、Cisco.com の『Cisco Smart Install Configuration Guide』を参照してください。
- Cisco IOS Release 12.2(55)SE のスマートインストール拡張では、クライアントバックアップファイル、同じ製品 ID を持つクライアントのゼロタッチ交換、イメージリストファイルの自動生成、設定可能ファイルのリポジトリ、ホスト名の変更、管理者からクライアントへの透過的な接続、およびイメージとシードを設定するための USB ストレージがサポートされています。
- AutoSmartPort 拡張では、Cisco Digital Media Player (Cisco DMP) および Cisco IP Video Surveillance Camera (Cisco IPVSC) の 2 つの新しいデバイスタイプに基づいた自動設定に加えて、マクロ永続性、LLDP に基づくトリガー、MAC アドレスおよび OUI に基づくトリガー、リモートマクロのサポートが追加されています。

## パフォーマンス向上機能

- Cisco EnergyWise は、Power over Ethernet (PoE) エンティティのエネルギー使用量を管理します。詳細については、Cisco.com の『Cisco EnergyWise Version 2 Configuration Guide』を参照してください。
- 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。
- 10/100 Mbps インターフェイス、10/100/1000 Mbps インターフェイス、および 10/100/1000BASE-TX SFP モジュール インターフェイス上の Automatic Media-Dependent Interface Crossover (Auto MDIX; 自動メディア依存型インターフェイスクロスオーバー) 機能により、インターフェイスが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、接続を適切に設定します。
- 次のフレームタイプの Maximum Transmission Unit (MTU; 最大伝送ユニット) サイズをサポートしています。
  - ルーテッドフレームの場合は最大 9216 バイト
  - ギガビットイーサネットポートおよび 10 ギガビットイーサネットポートを通してハードウェアおよび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 9216 バイト
- すべてのポートにおける IEEE 802.3x フロー制御（スイッチは休止フレームを送信しません）。

- Catalyst 3750-X 専用スイッチ スタックでは最大 64 Gbps のスループット。
- 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 80 Gbps (10 ギガビット EtherChannel) 全二重の帯域幅を確保。
- Port Aggregation Protocol (PAgP; ポート集約プロトコル) 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。
- 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。
- スタック内の複数のスイッチ間で、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。
- ポート単位でのストーム制御。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 ストームを防止できます。
- レイヤ 2 の不明なユニキャスト、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) 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
- 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 デバイスへ送信する IGMP レポート抑制 (IGMPv1 または IGMPv2 クエリーだけをサポート)。
- IGMP スヌーピング クエリー サポート。IGMP 一般クエリー メッセージを定期的に生成するようスイッチを設定します。
- IIGMP ヘルパー。スイッチは、マルチキャスト ストリームに加入するためのホスト要求を特定の IP 宛先アドレスに転送できます。
- スイッチド ネットワーク内のクライアントおよびルータへの IPv6 マルチキャスト データの効率的な配信を可能にするための MLD。
- Multicast VLAN Registration (MVR)。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、なお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 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する IGMP スロットリング。
- ネットワーク終了の待ち時間を設定できる IGMP の脱退タイマー。
- Switch 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。
- 広域アプリケーション エンジンへのトラフィックのリダイレクト、コンテンツ要求のローカルでの対応、およびネットワークでの Web トラフィック パターンのローカライズ (IP サービス フィーチャセットが必要) を実現する Web Cache Communication Protocol (WCCP)。
- スモール フレーム (64 バイト以下) が指定したレート (しきい値) でインターフェイスに到達する場合のストーム制御を防ぐ設定可能なスモールフレーム到達しきい値。
- 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を短縮するための Flex Link マルチキャスト高速コンバージェンス。

- IEEE 802.11n 対応のアクセス ポイントのサポート、および 15.4 W を超える電力を使用する受電装置のサポート。
- サーバグループ全体にわたって、アクセスや認証要求を均等に分散できるようにする RADIUS サーバロード バランシング。
- Cisco Medianet では、ネットワーク インフラストラクチャで幅広いビデオ アプリケーションのためのインテリジェント サービスを可能にします。Medianet のサービスの 1 つは、自動 SmartPort による Cisco Digital Media Player および Cisco IP Video Surveillance Camera の自動プロビジョニングです。
- 出力ネットワーク ポート上の CPU によって生成されたトラフィックの QoS マーキングおよび CPU で生成されたトラフィックのキューがサポートされます。

## 管理オプション

- 組み込みデバイス マネージャ : GUI のデバイス マネージャがユニバーサル 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 マネージャの起動については、『Getting Started Guide』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 : Network Assistant は、Cisco.com からダウンロードできるネットワーク管理アプリケーションです。単一のスイッチ、スイッチ クラスタ、デバイスのコミュニティの管理に使用します。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 : 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、イーサネット管理ポートに直接 PC を接続するか、またはリモート管理ステーションか PC から Telnet を使用して、アクセスできます。任意のスタック メンバーのコンソール ポートまたはイーサネット管理ポートに接続することにより、スイッチ スタックを管理できます。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。
- SNMP : CiscoWorks2000 LAN Management Suite (LMS) および HP OpenView などの SNMP 管理アプリケーション。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または PC から管理できます。スイッチは豊富な MIB 拡張機能および 4 つの Remote Monitoring (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 34 章「SNMP の設定」を参照してください。
- Cisco IOS Configuration Engine (旧名 Cisco IOS CNS エージェント) : ネットワーク デバイスおよびサービスの配置と管理を自動化するコンフィギュレーション サービス。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あと、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。
- CNS の詳細については、第 4 章「Cisco IOS Configuration Engine の設定」を参照してください。

## 管理の簡易性に関する機能

- 有線ロケーション サービスは、接続されているデバイスのロケーション情報およびアタッチメント追跡情報を Cisco Mobility Services Engine (MSE) に送信します。
- スイッチ管理、設定ストレージ、および配信を自動化するための CNS の組み込み型エージェント。
- 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、Domain Name System (DNS; ドメイン ネーム システム)、TFTP サーバ名) の自動設定。

- DHCP リレーによる DHCP クライアントからの UDP ブロードキャストの転送 (IP アドレス要求を含む)。
- 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。
- スイッチ ポートへの IP アドレスの事前割り当てのための DHCP サーバ ポートベースのアドレス割り当て。
- 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)。IP アドレスおよび対応する 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。
- VLAN 上の MAC アドレス ラーニング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る設定可能な MAC アドレス スケーリング。
- VLAN 上の MAC アドレス ラーニングのディセーブル化。
- 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。
- 他社製 IP フォンとの相互運用性のための Link Layer Discovery Protocol (LLDP) および LLDP Media Endpoint Discovery (LLDP-MED)。
- スイッチからエンドポイント デバイスに場所情報を提供する LLDP-MED ロケーション TLV のサポート。
- サーバからロケーションベースのダイナミックなコンテンツ配信を行うために、ビデオ エンドポイントでロケーション情報を交換することを目的とした CDP と LLDP の拡張。
- Network Time Protocol (NTP)。すべてのスイッチに外部ソースから同じタイムスタンプを提供します。
- 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。
- スイッチ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。
- スイッチの実行コンフィギュレーションを保存済みの Cisco IOS コンフィギュレーション ファイルで置き換えるための設定の置換とロールバック。
- 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 Communicator または Microsoft Internet Explorer ブラウザセッションでデバイス マネージャを使用した帯域内管理アクセス。
- 最大 16 の Telnet 接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベース セッションを実行できます。
- 最大 5 つの暗号化 Secure Shell (SSH; セキュア シェル) 接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベース セッションを実行できます。
- 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。
- 帯域外管理アクセス。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とモデム経由でリモート端末に接続します。
- イーサネット管理ポートを経由して PC に帯域外管理アクセスします。

- スイッチの設定やイメージファイルのコピーにセキュアな認証方式を提供する Secure Copy Protocol (SCP) 機能。
- 指定した設定と新しいイメージを多数のスイッチにダウンロードするための DHCP ベースの自動設定およびイメージ更新。
- IGMPv2 クライアントが Source Specific Multicast (SSM) を使用できるようにする送信元のマッピングを提供し、受信側のマルチキャスト送信元への動的な接続とアプリケーション上の依存関係の削除を可能にする、マルチキャスト アプリケーション対応の SSM マッピング。
- Cisco IOS がサポートする HTTP クライアントは IPv4 および IPv6 の HTTP サーバに要求を送信でき、Cisco IOS がサポートする HTTP サーバは IPv4 および IPv6 の HTTP クライアントからの HTTP 要求を処理できます。
- Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) を IPv6 トランスポートを介して設定できるため、IPv6 ホストは SNMP クエリーを送信し、IPv6 を実行中のデバイスから SNMP 通知を受信できます。
- IPv6 ではステートレス自動設定がサポートされているため、ホストやモバイル IP アドレスの管理など、リンク、サブネット、およびサイトアドレス指定の変更を管理できます。
- カスタム バナーまたはイメージファイルを Web 認証ログイン画面に表示するローカル Web 認証バナー。
- CPU の使用率をモニタする CPU 使用率しきい値トラップ。
- Class of Service (CoS)、Differentiated Services Code Point (DSCP)、およびタギング モードの値を指定することで音声および音声シグナリング VLAN のプロファイルを作成するための LLDP-MED ネットワーク ポリシー プロファイル時間、長さ、値 (TLV)。
- DHCPDISCOVER パケットのオプション 12 フィールドのホスト名もサポートされます。これによって、DHCP プロトコルを使用して送信される同一の設定ファイルが提供されます。
- DHCP スヌーピング拡張では、オプション 82 DHCP フィールドで circuit-id サブオプションに固定文字列ベースの形式の選択がサポートされます。
- 電力ポリシー TLV 要求に基づいて、スイッチで Power Device (PD; 電力デバイス) への電力供給を可能にすることによって、LLPD-MED のサポートを強化します。
- Power over Ethernet (PoE) デバイスおよびデーモンを実行しているエンドポイントなどの EnergyWise エンティティの電力消費を管理する Cisco EnergyWise。
- 標準 RJ-45 コンソール ポートに加えて、USB mini タイプ B コンソール ポート。コンソール入力は、一度に 1 つのポートだけがアクティブになります。
- 外部 Cisco USB フラッシュ メモリ デバイス (サム ドライブまたは USB キー) 用の USB タイプ A ポート。標準 Cisco CLI コマンドを使用して、フラッシュ メモリの読み取り、書き込み、消去、コピー、またはフラッシュ メモリからの起動を実行できます。



(注) 管理インターフェイスの詳細については、「[ネットワークの構成例](#)」(P.1-21) を参照してください。

## アベイラビリティおよび冗長性に関する機能

- 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。
- (フェールオーバー) Catalyst 3750-X スイッチにおいて利用不可能となったスタック マスターに代わるためのスタック マスターの自動再選択。  
新たに選択されたスタック マスターは、1 秒未満でレイヤ 2 トラフィックの受信を開始し、3 ~ 5 秒以内にレイヤ 3 トラフィックの受信を開始します。



- スイッチ スタック中に冗長リンクを提供するクロススタック EtherChannel (Catalyst 3750-X スイッチだけ)。
- Unidirectional Link Detection (UDLD; 単一方向リンク検出) およびアグレッシブ UDLD。光ファイバ ケーブルの配線ミスまたはポート障害に起因する光ファイバ インターフェイス上の単一方向リンクを検出し、ディセーブルにします。
- 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。
  - 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 バランシングおよびスパニングツリー インスタンスの高速コンバージェンスの実現
- UplinkFast、クロススタック UplinkFast (Catalyst 3750-X スイッチだけ)、および BackboneFast による、スパニングツリー トポロジの変更後の高速コンバージェンスと、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 (Catalyst 3750-X スイッチだけ) など冗長アップリンク間でのロード バランシングの実行
- IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) により、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します。また、IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP) に基づいた Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+) により、ルートと指定ポートをただちにフォワーディング ステートに変更することで、スパニングツリーの高速コンバージェンスが実現されます。
- 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 ステートへただちに變更させることによって、転送遅延を防ぎます。
  - 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。
- 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。基本リンク冗長の STP に代わるものとして、互いにバックアップします。
- リンクステート トラッキング。接続されたホストと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状態をミラーリングします。また、別のシスコ製イーサネット スイッチで動作するリンクへサーバ トラフィックをフェールオーバーできます。
- StackPower 冗長性オプション。冗長モードでスタック内の電源装置を設定して、スタック内の電源装置に障害が発生した場合に、使用されていない電源装置をオンできます。

## VLAN 機能

- 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 規格で認められている 1 ~ 4094 の範囲で VLAN ID をサポート。
- ダイナミック VLAN メンバシップに対応する VLAN Query Protocol (VQP)。
- すべてのポート上で稼動する Inter-Switch Link (ISL; スイッチ間リンク) および IEEE 802.1Q トランッキング 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 トランッキング プロトコル)。2 台のデバイス間のリンク上でトランッキングをネゴシエートするだけでなく、使用するトランッキング 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 Trunking Protocol (VTP; VLAN トランッキング プロトコル) および VTP プルーニング。トラフィックのフラディ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。
- Multidomain authentication (MDA) 対応ポート上のダイナミック音声 VLAN を可能にする MDA 対応のダイナミック音声 VLAN。
- 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。この機能をイネーブルに設定すると、トランク上でユーザ 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。
- プライベート VLAN - VLAN スケーラビリティ問題に対応します。より制限された IP アドレスを割り当て、スイッチ上で、レイヤ 2 ポートを他のポートから切り離します。
- ポートで学習する MAC アドレス数を制限する、またはポートで学習する MAC アドレスを定義する、PVLAN ホストでのポート セキュリティ。
- Spanning Tree Protocol (STP; スパンニング ツリー プロトコル) を必要としない、レイヤ 2 冗長性を提供する VLAN Flex Link ロード バランシング 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た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分散が可能です。
- 任意の VTP モードでの拡張範囲 VLAN (VLAN 1006 ~ 4094) の設定のサポート、拡張認証 (非表示パスワード、またはシークレット パスワード)、VTP に加えてその他のデータベースの伝播、VTP プライマリおよびセカンダリ サーバ、およびポートごとに VTP をオンまたはオフにするオプションなどが含まれる VTP バージョン 3 をサポートします。

## セキュリティ機能

- Web 認証。IEEE 802.1x 機能をサポートしていないサブリカント (クライアント) を Web ブラウザで認証できるようにします。
- 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。
- 違反発生時に、ポート全体をシャットダウンするのではなく、そのポートの VLAN をシャットダウンする VLAN 対応ポート セキュリティ オプション。
- 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。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 VLAN の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 ACL。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/UDP ヘッダーの情報に基づいてトラフィックをフィルタリングし、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。
- インターフェイスに適用される IPv6 ACL。IPv6 トラフィックをフィルタリングします。
- スタティック ACL が設定されていないポートで、認証デフォルト ACL の動的な作成または適用をサポートします（IP ベースまたは IP サービスのフィッチャセットを実行しているスイッチでのみサポートされます）。
- 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。
- IP ソース ガード。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きルーティングされないインターフェイスでトラフィックを制限します。
- ダイナミック ARP インスペクション。同じ VLAN 内の他のポートの無効な ARP 要求や応答を信頼しないことで、スイッチでの悪意のある攻撃を回避します。
- 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。
- レイヤ 2 プロトコル トンネリングのバイパス機能。サードパーティ ベンダーとの相互運用性を実現します。
- オープンアクセスを使用した IEEE 802.1x。認証される前にホストがネットワークにアクセスできるようになります。
- 柔軟な認証シーケンス。新しいホストを認証する際に、ポートが試行する認証方式の順序を設定します。
- 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。次の機能がサポートされています。
  - Multidomain Authentication（MDA）。MDA では IP Phone（シスコまたはシスコ以外の製品）など、データ デバイスと音声デバイスの両方の認証を個々に同じ IEEE 802.1x 対応スイッチポートで行うことができます。
  - VLAN 割り当て。802.1x 認証ユーザを特定の VLAN に制限します。

- マルチ認証モードで設定されたポートでの VLAN 割り当てのサポート。RADIUS サーバは、ポートで最初に認証されるホストに VLAN を割り当て、後続のホストは同じ VLAN を使用します。音声 VLAN の割り当ては、1 つの IP Phone に対してのみサポートされます (IP ベースまたは IP サービスのフィーチャセットを実行しているスイッチでのみサポートされます)。
- ポート セキュリティ。IEEE 802.1x ポートへのアクセスを制御します。
- 音声 VLAN。ポートが許可ステートか無許可ステートかにかかわらず、Cisco IP Phone の音声 VLAN へのアクセスを許可します。
- Cisco IP Phone を検出および認識するための IP Phone 拡張検出機能。
- ゲスト VLAN。802.1x に適合しないユーザに限定的なサービスを提供します。
- 制限付き VLAN。IEEE 802.1x に準拠はしているが、標準の IEEE 802.1x で認証するための資格情報を持っていないユーザに制限付きのサービスを提供します。
- 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。
- 音声対応 IEEE 802.1x セキュリティ。セキュリティ違反の発生した VLAN にだけトラフィック違反アクションを適用します。
- 802.1x スイッチ サプリカントを使用する Network Edge Access Topology (NEAT)、CISP を使用するホスト認可、および自動イネーブル。ワイヤリング クローゼットの外にあるスイッチを別のスイッチのサプリカントとして認証します。
- ダウンロード可能な ACL およびリダイレクト URL を使用する IEEE 802.1x 認証。Cisco Secure ACS サーバから認証されたスイッチへユーザ別の ACL をダウンロードできるようにします。
- 複数ユーザ認証。802.1x 対応ポート上で 2 つ以上のホストを認証できるようにします。
- MAC 認証バイパス。クライアントの MAC アドレスに基づいてクライアントを許可します。
- 音声対応 IEEE 802.1x および MAC Authentication Bypass (MAB; MAC 認証バイパス) セキュリティ違反。セキュリティ違反が発生したときに、ポート上のデータ VLAN だけをシャットダウンします。
- Network Admission Control (NAC) 機能 :
  - デバイスのネットワーク アクセスを許可する前の、エンドポイントシステムやクライアントのウィルス対策の状態またはポスチャに関する NAC レイヤ 2 IEEE 802.1x 検証  
NAC レイヤ 2 IEEE 802.1x 検証の設定に関する詳細については、「[NAC レイヤ 2 IEEE 802.1x 検証の設定](#)」(P.11-63) を参照してください。
  - デバイスのネットワーク アクセスを許可する前の、エンドポイントシステムまたはクライアントのポスチャに関する NAC レイヤ 2 IP 検証  
NAC レイヤ 2 IP 検証の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
  - IEEE 802.1x アクセス不能認証バイパス  
この機能の設定については、「[アクセス不能認証バイパス機能の設定](#)」(P.11-58) を参照してください。
  - Authentication, Authorization, Accounting (AAA; 認証、許可、アカウンティング) ダウンポリシー。ポスチャ検証が発生したときに、AAA サーバが利用できない場合のホストの NAC レイヤ 2 IP 検証  
この機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

- 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。
- Remote Authentication Dial-In User Service (RADIUS)。Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントリング) サービスによってリモート ユーザの身元を確認し、リモート ユーザにアクセス権を与え、リモート ユーザのアクションを追跡します。
- 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します。
- Secure Socket Layer (SSL) バージョン 3.0 のサポート。HTTP 1.1 サーバによる認証、暗号化、およびメッセージ完全性を確保します。また、HTTP クライアント認証により、セキュア HTTP 通信を可能にします。
- IEEE 802.1x 準備チェック。スイッチに IEEE 802.1x を設定する前に接続されたエンドホストの準備状態を判断します。
- スタティックホストでの IP ソースガードのサポート。
- 認証された後に特定のセッションの属性を変更するための RADIUS Change of Authorization (CoA)。AAA のユーザまたはユーザグループのポリシーが変更されると、管理者は Cisco Secure ACS のような AAA サーバから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーに適用できます。
- IEEE 802.1x User Distribution では、複数の VLAN 上のユーザの負荷を分散してネットワークのスケラビリティを向上するために、(ユーザのグループに対して) 複数の VLAN を配置できます。認証されたユーザは、RADIUS サーバによって、グループ内で最も実装数が少ない VLAN に割り当てられます。
- 複数のホスト認証を行うクリティカルな VLAN では、ポートが複数認証用に設定されており、AAA サーバが到達不能となった場合でも、重要なリソースにアクセスできるように、ポートがクリティカルな VLAN に配置されます。
- ローカル Web 認証のために、ユーザ定義の *login*、*success*、*failure* および *expire* Web ページを作成できるカスタマイズ可能な Web 認証拡張。
- ポートホストモードの変更および認証スイッチポート上の標準ポート設定の適用を行う Network Edge Access Topology (NEAT) のサポート。
- 認証されていない VLAN からのネットワークアクセスを回避するためのユーザ認証に、VLAN および MAC のアドレス情報の組み合わせを使用する VLAN ID ベースの MAC 認証。
- MAC 移動では、ホスト (IP 電話の背後で接続されるホストを含む) が同じスイッチ内の複数のポート間を制限なく移動できます。MAC 移動では、スイッチで別のポート上の同じ MAC アドレスの再適用をまったく新しい MAC アドレスと同様の方法で扱います。
- Simple Network Management Protocol のバージョン 3 (SNMPv3) の 3DES および AES をサポートします。このリリースでは、SNMPv3 に 168 ビットの Triple Data Encryption Standard (3DES) および 128 ビット、192 ビット、256 ビットの Advanced Encryption Standard (AES) 暗号化アルゴリズムのサポートが追加されます。
- Cisco TrustSec の Security Group Tag (SCT) Exchange Protocol (SXP) コンポーネントのサポート。認証、暗号化、およびアクセス制御を使用したセキュリティアーキテクチャです (IP ベースまたは IP サービスのフィーチャセットを実行しているスイッチでのみサポートされます)。
- IEEE 802.1AE Media Access Control Security (MACsec) のサポート。暗号化キーのために帯域外方式を使用し、有線ネットワークを通じて MAC レイヤ暗号化を実現します。MACsec Key Agreement (MKA) プロトコルは、セッションキーと管理暗号化キーを提供します (IP ベースまたは IP サービスのフィーチャセットを実行しているスイッチだけでサポートされています)。

## QoS および CoS 機能

- 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。
- クロススタック QoS により、個々のスイッチ単位ではなく、スイッチ スタック内のすべてのスイッチに QoS 機能を設定します (Catalyst 3750-X スイッチだけ)。
- 自動 QoS の拡張では、Cisco Telepresence System や Cisco Surveillance Camera などのビデオ デバイスからのトラフィック フローを自動的に分類設定する機能が追加されています。
- 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 packets 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 - IPv4 と IPv6 の両方)。
  - 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します。
- 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。
  - 階層型のポリシー マップで複数のクラス マップを作成する場合、各クラス マップを自身のポート レベル (第 2 レベル) ポリシー マップと関連付けることができます。第 2 レベルのポリシー マップは、それぞれ異なるポリサーを保有できます。
  - 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。
- 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。
- 入力キューイングおよびスケジューリング
  - ユーザ トラフィック用に設定可能な 2 つの入力キュー (一方のキューをプライオリティ キューにできます)。
  - 輻輳回避メカニズムとしての Weighted Tail Drop (WTD)。キュー長を管理し、トラフィックの分類ごとに異なるドロップ優先順位を設定します。
  - Shaped Round Robin (SRR; シェイプド ラウンド ロビン)。パケットがスタックまたは内部リングへ送出されるときに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)。
- 出力キューおよびスケジューリング
  - 1 ポートに 4 つの出力キュー。
  - 輻輳回避メカニズムとしての WTD。キュー長を管理し、トラフィックの分類ごとに異なるドロップ優先順位を設定します。

- スケジューリング サービスとしての SRR。キューからパケットを出して出力インターフェイスに入れる速度を指定します（出力キューではシェーピングおよび共有がサポートされます）。シェーピング型出力キューは、ポート帯域幅の割り当てが保証されますが、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。共有型出力キューは、設定された帯域幅の割り当てが保証されるだけでなく、他のキューが空になり、その割り当て分の帯域幅が使用されない場合、保証された割り当てより多く使用できます。
- DSCP のポートベースの信頼性と出力トラフィックのプライオリティ キューイングを実現する自動 QoS Voice over IP (VoIP) 拡張機能
- デュアル IPv4/IPv6 SDM テンプレートによる IPv6 ポートベースの信頼性（LAN ベースのフィーチャセットを実行しているスイッチではサポートされません）。
- IPv6 トラフィックに対する QoS の完全サポート（LAN ベースのフィーチャセットを実行しているスイッチではサポートされません）。

## レイヤ 3 機能



(注)

このセクションの機能は、LAN ベースのフィーチャセットを実行しているスイッチではサポートされません。ここで取り上げる一部の機能は IP サービス フィーチャセットだけに対応しています。

- レイヤ 3 ルータの冗長性を確保するための HSRP バージョン 1 (HSRPv1) および HSRP バージョン 2 (HSRPv2)
- 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
  - IPv6 対応 HSRP (IP サービス フィーチャセットが必要)
  - 完全な OSPF (IP サービス フィーチャセットが必要)
 

Cisco IOS Release 12.2(55)SE 以降のリリースでは、IP ベース フィーチャセットで、ルーテッド アクセスの OSPF をサポートするため、レイヤ 3 ルーティング機能をアクセスまたはワイヤリング クローゼットに拡張できます。
  - EIGRP (IP サービス フィーチャセットが必要)
  - Border Gateway Protocol (BGP) バージョン 4 (IP サービス フィーチャセットが必要)
- 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; ポリシーベース ルーティング)。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) デバイスの複数の VPN ルーティング/転送 (Multi-VRF) インスタンス。サービス プロバイダーが、複数の Virtual Private Network (VPN; バーチャルプライベート ネットワーク) をサポートし、VPN 間で IP アドレスを重複できるようにする (IP サービス フィーチャセットが必要)
- ネットワーク バーチャライゼーションおよびバーチャルプライベート マルチキャスト ネットワークを実現するために複数のプライベート ルーティング ドメインを設定できる VRF Lite
- 次の IP サービスが複数のルーティング インスタンス上で動作できるように、これらを VRF 対応にするサポート機能 : HSRP、uRPF、ARP、SNMP、IP SLA、TFTP、FTP、syslog、traceroute、および ping

- フォールバック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 (IP サービス フィーチャセットが必要)
- 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メント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ブルーニングが可能になります。PIM sparse mode (PIM-SM; PIM スパースモード)、PIM dense mode (PIM-DM; PIM デンスモード)、および PIM スパース-デンスモードのサポートも含まれます (IP サービス フィーチャセットが必要)
- 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するための SSM PIM プロトコルのサポート
- Multicast Source Discovery Protocol (MSDP)。複数の PIM-SM ドメインを接続 (IP サービス フィーチャセットが必要)
- 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 (IP サービス フィーチャセットが必要)
- 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
- IPv6 リレー、クライアント、サーバのアドレス割り当て、およびプレフィックス委任を実行する DHCP
- 設定されたインターフェイスを介して IPv6 トラフィックを転送するための IPv6 ユニキャストルーティング機能 (IP サービス フィーチャセットが必要)
- ホストが適切なルータを選択する機能を改善する IPv6 Default Router Preference (DRP; デフォルトルータ初期設定)
- EIGRP IPv6 のサポート。IPv6 トランスポートの使用、IPv6 ピアとの通信、および IPv6 ルートのアドバタイズを実行可能
- ソースパケット IP アドレスを確認するための IP ユニキャスト逆経路転送 (ユニキャスト RPF)
- Nonstop Forwarding (NSF) 認識。プライマリ Route Processor (RP; ルートプロセッサ) が障害を起こしている、バックアップ RP が引き継ぐ間、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 スイッチが NSF 対応ネイバールータからのパケットを継続して転送することが可能 (IP サービス フィーチャセットが必要)
- OSPF および EIGRP 向けの NSF 対応ルーティング。スイッチが NSF 認識および対応ネイバーからの情報に基づいてルーティングテーブルを再構築できるようにします (Catalyst 3750-E、Catalyst 3750-X スイッチだけ)
- SVI ラインステートアップまたはダウンの計算から VLAN 内のポートを除外する機能
- Intermediate System-to-Intermediate System (IS-IS) ルーティングは、Connectionless Network Service (CLNS) ネットワーク用にダイナミックルーティングプロトコルをサポート

## PoE 機能

- 回路上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、Power over Ethernet (PoE) 対応ポートに接続されたシスコ製先行標準および IEEE 802.3af 準拠の受電装置に電力を供給できます。



- 受電装置で利用できる電力が、1 ポートあたり 15.4 W から 30 W に増加する IEEE 802.3at (PoE+) のサポート。
- 消費電力を含む CDP のサポート。受電装置は、消費している電力量をスイッチに通知します。
- シスコ インテリジェント電力管理のサポート。受電装置およびスイッチは、電力ネゴシエーション CDP メッセージによってネゴシエーションを行い、電力消費レベルについて合意します。このネゴシエーションにより、高電力のシスコ受電装置は、最高電力モードで動作できるようになります。
- 自動検出およびパワー バジエツト。スイッチはパワー バジエツトを維持し、電力要求をモニタおよび追跡し、利用できる場合にだけ電力を供給します。
- リアルタイム電力消費をモニタする機能。スイッチは PoE ポート単位で、電力消費を検出し、電力使用にポーリングを行い、電力消費を報告します。
- IP ベースまたは IP サービスのフィーチャ セットを実行している Catalyst 3750-X スwitch の StackPower テクノロジー。

## モニタ機能

- Catalyst 3560-X スwitch での、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。
- Catalyst 3750-X スwitch での、スイッチ LED によるポート レベル、スイッチ レベル、およびスタック レベルのステータス確認。
- MAC アドレス通知トラップおよび RADIUS アカウンティング。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追跡します。
- Switched Port Analyzer (SPAN; スwitch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。
- 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 セキュリティ違反をモニタ、撃退、およびレポートします。
- 組み込み RMON エージェントの 4 つのグループ (ヒストリ、統計、アラーム、およびイベント) を使用して、ネットワークをモニタし、トラフィック解析を行うことができます。
- 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。
- 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。
- Time Domain Reflector (TDR)。10/100 および 10/100/1000 の銅線イーサネット ポートでケーブル接続の問題を診断し、解決します。
- 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します。
- 接続された SFP モジュールの Digital Optical Monitoring (DOM)。
- オンライン診断。スイッチが稼働中のネットワークに接続している間に、スーパーバイザ エンジン、モジュール、およびスイッチのハードウェア機能をテストします。
- On-Board Failure Logging (OBFL)。スイッチとそれに接続されている電源装置の情報を収集します。
- HSRP 対応の Enhanced Object Tracking (EOT; 拡張オブジェクト トラッキング)。ルーティング テーブルの状態を追跡することで LAN 内のサーバの割合を判別したり、スタンバイ ルータ フェールオーバーをトリガーしたりできます。
- アクティブ トラフィック モニタリングを使用してネットワーク パフォーマンスを測定するための IP Service Level Agreement (IP SLA; IP サービス レベル契約) のサポート。

- IP SLA EOT。スタンバイ ルータ フェールオーバーを実行するために、遅延、ジッタ、またはパケット損失などのアクションによってトリガーされた IP SLA 追跡動作の出力を使用します。
- 事前設定されたスタティック ルートまたは DHCP ルートがどの時点でダウンしたかを識別するための EOT および IP SLA EOT スタティック ルートのサポート。
- 分析用のトラフィックをキャプチャするフィルタを定義するための Flow-based Switch Port Analyzer (FSPAN; フローベース スイッチ ポート アナライザ)。
- 主要なシステム イベントをモニタし、ポリシーを使用して処理するためのデバイスおよびシステム管理用の Embedded Event Manager (EEM)。
- ネイバー探索、ID、MAC-Address-Table のイベント検出器を組み込むための EEM 3.2 のサポート。

## スイッチ初期設定後のデフォルト値

スイッチはプラグアンドプレイ動作に対応しているため、必要なのはスイッチに基本的な IP 情報を割り当て、ネットワーク内の他のデバイスに接続することだけです。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およびスタック全体の設定値を変更できます。



(注) ブラウザベースの Express Setup プログラムによる IP アドレスの割り当てについては、『Getting Started Guide』を参照してください。CLI ベースの設定プログラムによる IP アドレスの割り当てについては、ハードウェア インストールガイドを参照してください。

スイッチをまったく設定しなかった場合、スイッチは次のデフォルト設定で動作します。

- デフォルト スイッチ IP アドレス、サブネット マスク、デフォルト ゲートウェイは 0.0.0.0 です。詳細については、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」および第 23 章「DHCP 機能および IP ソース ガードの設定」を参照してください。
- ドメイン名はデフォルトで設定されていません。詳細については、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」を参照してください。
- DHCP クライアントはイネーブル、DHCP サーバはイネーブルに設定されています (DHCP サーバとして動作するデバイスが設定されていて、イネーブルの場合にだけ)。DHCP リレー エージェントはイネーブルに設定されています (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、イネーブルの場合にだけ)。詳細については、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」および第 23 章「DHCP 機能および IP ソース ガードの設定」を参照してください。
- スイッチ スタックはイネーブルに設定されています (設定変更できません)。詳細については、第 5 章「スイッチ スタックの管理」を参照してください。
- スイッチ クラスタはディセーブルに設定されています。スイッチ クラスタの詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com から入手できる『Getting Started with Cisco Network Assistant』を参照してください。
- パスワードは定義されていません。詳細については、第 7 章「スイッチの管理」を参照してください。
- システム名とプロンプトは *Switch* です。詳細については、第 7 章「スイッチの管理」を参照してください。
- NTP はイネーブルに設定されています。詳細については、第 7 章「スイッチの管理」を参照してください。
- DNS はイネーブルに設定されています。詳細については、第 7 章「スイッチの管理」を参照してください。

- TACACS+ はディセーブルに設定されています。詳細については、第 10 章「スイッチベース認証の設定」を参照してください。
- RADIUS はディセーブルに設定されています。詳細については、第 10 章「スイッチベース認証の設定」を参照してください。
- 標準の HTTP サーバおよび SSL HTTPS サーバは両方ともイネーブルに設定されています。詳細については、第 10 章「スイッチベース認証の設定」を参照してください。
- IEEE 802.1x はディセーブルに設定されています。詳細については、第 11 章「IEEE 802.1x ポートベース認証の設定」を参照してください。
- ポート パラメータ
  - 動作モードはレイヤ 2 (スイッチポート) です。詳細については、第 13 章「インターフェイス特性の設定」を参照してください。
  - インターフェイス速度およびデュプレックス モードが自動ネゴシエーションに設定されています。詳細については、第 13 章「インターフェイス特性の設定」を参照してください。
  - Auto-MDIX はイネーブルに設定されています。詳細については、第 13 章「インターフェイス特性の設定」を参照してください。
  - フロー制御はオフに設定されています。詳細については、第 13 章「インターフェイス特性の設定」を参照してください。
  - PoE は自動ネゴシエーションに設定されています。詳細については、第 13 章「インターフェイス特性の設定」を参照してください。
- SmartPort マクロは定義されていません。詳細については、を参照してください。
- VLAN
  - デフォルトの VLAN は VLAN 1 です。詳細については、第 14 章「VLAN の設定」を参照してください。
  - VLAN トランキング設定は dynamic auto (DTP) です。詳細については、第 14 章「VLAN の設定」を参照してください。
  - トランク カプセル化はネゴシエーションです。詳細については、第 14 章「VLAN の設定」を参照してください。
  - VTP モードはサーバです。詳細については、第 15 章「VTP の設定」を参照してください。
  - VTP バージョンは、バージョン 1 です。詳細については、第 15 章「VTP の設定」を参照してください。
  - プライベート VLAN は設定されていません。詳細については、第 17 章「プライベート VLAN の設定」を参照してください。
  - 音声 VLAN はディセーブルに設定されています。詳細については、第 16 章「音声 VLAN の設定」を参照してください。
- IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングはディセーブルに設定されています。詳細については、第 18 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」を参照してください。
- STP、PVST+ は、VLAN 1 でイネーブルに設定されています。詳細については、第 19 章「STP の設定」を参照してください。
- MSTP はディセーブルに設定されています。詳細については、第 20 章「MSTP の設定」を参照してください。
- オプションのスパニングツリー機能はディセーブルに設定されています。詳細については、第 21 章「オプションのスパニングツリー機能の設定」を参照してください。

- Flex Link は設定されていません。詳細については、第 22 章「Flex Link および MAC アドレステーブル移動更新機能の設定」を参照してください。
- DHCP スヌーピングはディセーブルに設定されています。DHCP スヌーピング情報オプションはイネーブルに設定されています。詳細については、第 23 章「DHCP 機能および IP ソース ガードの設定」を参照してください。
- IP ソース ガードはディセーブルに設定されています。詳細については、第 23 章「DHCP 機能および IP ソース ガードの設定」を参照してください。
- ダイナミック ARP インスペクションはすべての VLAN でディセーブルに設定されています。詳細については、第 24 章「ダイナミック ARP インスペクションの設定」を参照してください。
- IGMP スヌーピングはイネーブルに設定されています。IGMP フィルタは適用されていません。詳細については、第 26 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スロットリング設定は拒否です。詳細については、第 26 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スヌーピング クエリア機能はディセーブルに設定されています。詳細については、第 26 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- MVR はディセーブルに設定されています。詳細については、第 26 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- ポートベース 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 ストーム制御はディセーブルに設定されています。詳細については、第 28 章「ポート単位のトラフィック制御の設定」を参照してください。
  - 保護ポートは定義されていません。詳細については、第 28 章「ポート単位のトラフィック制御の設定」を参照してください。
  - ユニキャストおよびマルチキャスト トラフィック フラッディングはブロックされていません。詳細については、第 28 章「ポート単位のトラフィック制御の設定」を参照してください。
  - セキュア ポートは設定されていません。詳細については、第 28 章「ポート単位のトラフィック制御の設定」を参照してください。
- CDP はイネーブルに設定されています。詳細については、第 27 章「CDP の設定」を参照してください。
- UDLD はディセーブルに設定されています。詳細については、第 30 章「UDLD の設定」を参照してください。
- SPAN および RSPAN はディセーブルに設定されています。詳細については、第 31 章「SPAN および RSPAN の設定」を参照してください。
- RMON はディセーブルに設定されています。詳細については、第 32 章「RMON の設定」を参照してください。
- Syslog メッセージはイネーブルに設定され、コンソール上に表示されます。詳細については、第 33 章「システム メッセージ ロギングの設定」を参照してください。
- SNMP はイネーブルに設定されています (バージョン 1)。詳細については、第 34 章「SNMP の設定」を参照してください。
- ACL は設定されていません。詳細については、第 36 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- QoS はディセーブルに設定されています。詳細については、第 37 章「QoS の設定」を参照してください。

- EtherChannel は設定されていません。詳細については、第 39 章「EtherChannel およびリンクステートトラッキングの設定」を参照してください。
- IP ユニキャスト ルーティングはディセーブルに設定されています。詳細については、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。
- HSRP グループは設定されていません。詳細については、第 43 章「HSRP の設定」を参照してください。
- IP マルチキャスト ルーティングはすべてのインターフェイスでディセーブルに設定されています。詳細については、第 47 章「IP マルチキャスト ルーティングの設定」を参照してください。
- MSDP はディセーブルに設定されています。詳細については、第 48 章「MSDP の設定」を参照してください。
- フォールバック ブリッジングは設定されていません。詳細については、第 49 章「フォールバックブリッジングの設定」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、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、ギガビット イーサネット接続および 10 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。

- 「スイッチを使用する場合の設計概念」(P.1-21)
- 「Catalyst 3750-X と 3560-X スイッチを使用した中小規模ネットワーク」(P.1-28)
- 「Catalyst 3750-X と 3560-X スイッチを使用した大規模ネットワーク」(P.1-30)
- 「Catalyst 3750-X スイッチを使用した集合住宅ネットワーク」(P.1-33)
- 「長距離広帯域トランスポートの構成」(P.1-34)

## 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"> <li>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。</li> <li>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。</li> </ul>
<ul style="list-style-type: none"> <li>新しい PC、ワークステーション、およびサーバのパワーが増大します。</li> <li>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) による帯域幅需要が増大します。</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>

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"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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、なお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 から分離します。</li> </ul>
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およびアベイラビリティに対する大きな需要	<ul style="list-style-type: none"> <li>スタック マスターに障害が生じた場合、すべてのスタック メンバーがスタック マスターの代わりに機能できるスイッチ スタックを使用します。すべてのスタック メンバーが、スイッチ スタックの保存済み実行コンフィギュレーション ファイルの同期化されたコピーを持っています。</li> <li>クロススタック EtherChannel を使用すると、スイッチ スタック全体で冗長リンクを提供します。</li> <li>HSRP を使用して、クラスタ コマンドスイッチとルータの冗長構成を確立します。</li> <li>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。</li> </ul>
IP テレフォニーに対する新しい需要	<ul style="list-style-type: none"> <li>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。</li> <li>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 に基づく高優先順位または低優先順位のいずれかに設定します。スイッチは、1 ポートあたり少なくとも 4 つのキューをサポートします。</li> <li>Voice VLAN ID (VVID) を使用して、音声トラフィックに別個の VLAN を用意します。</li> </ul>
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ヘデータおよび音声を高速で伝送する需要の増大	<p>Catalyst Long-Reach Ethernet (LRE) スイッチを使用して、既存のインフラストラクチャ（既存の電話回線など）上で最大 15MB の IP 接続を提供します。</p> <p>(注) LRE は Catalyst 2950 LRE スイッチで使用されているテクノロジーです。LRE については、各スイッチ固有のマニュアルセットを参照してください。</p>

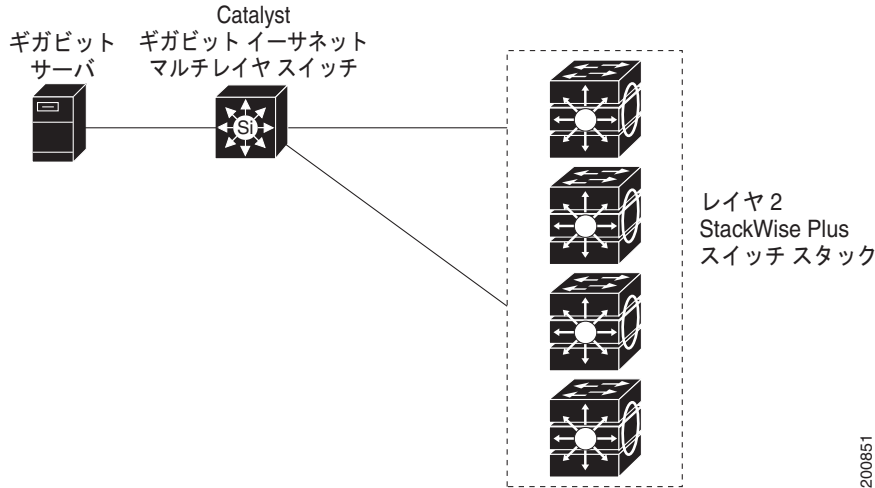
スイッチおよびスイッチ スタックを使用して、次を作成できます。

- コスト効率の高いワイヤリング クローゼット (図 1-1)：多数のユーザをワイヤリング クローゼットに接続するコスト効率の高い手法は、最大 9 台の Catalyst 3750-X スイッチからなるスイッチ スタックを配備することです。スタック内の 1 台のスイッチに障害が生じた場合にスイッチ接続を維持するには、ハードウェア インストールガイドで推奨されるとおりにスイッチを接続し、クロススタック Etherchannel またはクロススタック UplinkFast のいずれかをイネーブルにします。



スイッチ スタック内の SFP モジュールを使用して、Catalyst 4500、Catalyst 3750-X、Catalyst 3750-E、Catalyst 3560E-12D などのギガビット バックボーン スイッチへの冗長アップリンク接続を確立できます。ギガビット リンクまたは EtherChannel 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。ギガビット スイッチがクラスタ対応の場合は、そのスイッチとスイッチ スタックを 1 つのスイッチ クラスタとして設定し、単一の IP アドレスを使ってそれらを管理できます。1000BASE-T 接続を使用して、ギガビット スイッチをギガビット サーバへ接続できます。

図 1-1 コスト効率の高いワイヤリング クローゼット



- 高性能ワイヤリング クローゼット (図 1-2) : 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 3750-X スイッチとスイッチ スタックを使用すると、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 レイヤのスイッチを、Catalyst 4500 ギガビット スイッチや Catalyst 6500 ギガビット スイッチなどのバックボーン内のギガビット マルチレイヤ スイッチに接続します。
- 高性能ワークグループに適したコスト効率の高い Gigabit-to-the-Desktop (GTD; ギガビットツーデスクトップ) (図 1-3) : ネットワーク リソースへの高速アクセスを実現するには、Catalyst 3560-X スイッチをアクセス レイヤで使用して、デスクトップにギガビットイーサネットを提供します。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、ルーティング機能を備えたギガビット スイッチまたはルータに、アクセス レイヤのスイッチを接続します。

最初の図は分離された高性能ワークグループです。Catalyst 3560-X スイッチがディストリビューション レイヤの Catalyst 3750-X スイッチに接続されています。2 番目の図は、ブランチ オフィスの高性能ワークグループです。Catalyst 3560-X スイッチがディストリビューション レイヤのルータに接続されています。

この構成では、各スイッチはネットワーク 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。また、SFP モジュールを使用すると、光ファイバ接続におけるメディアおよび距離のオプションに柔軟性が提供されます。



図 1-2 高性能ワイヤリング クローゼット

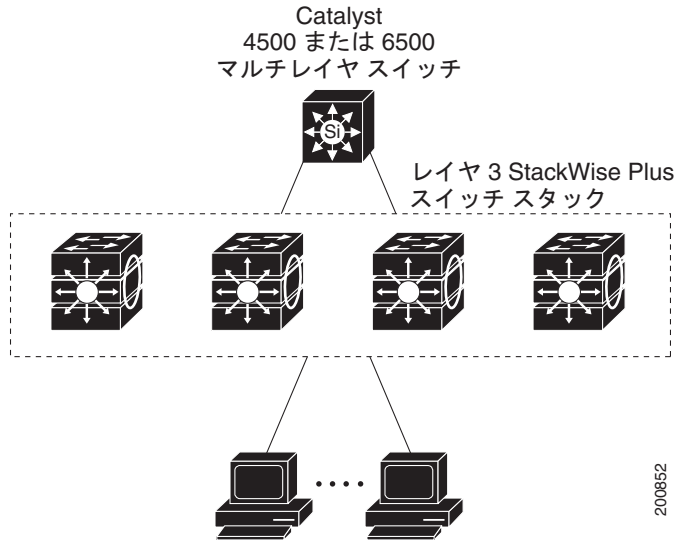
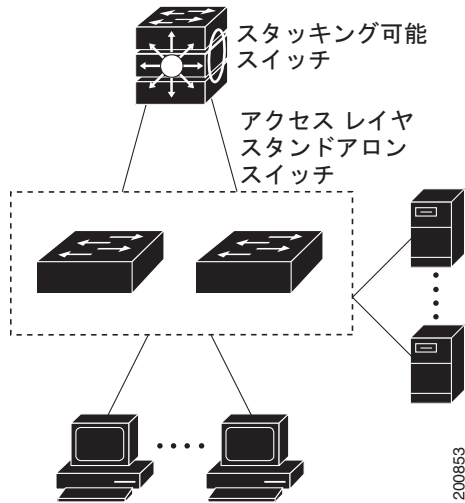
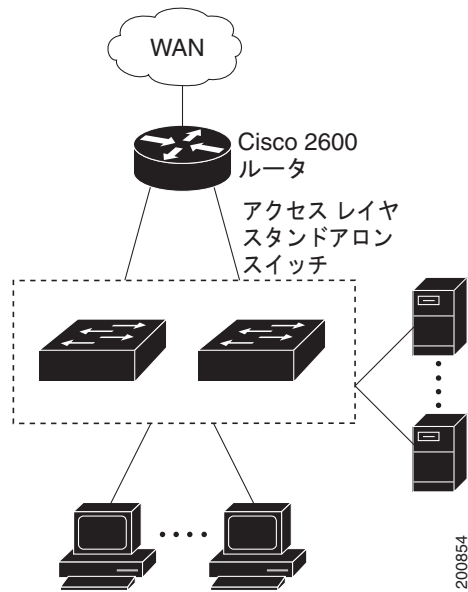


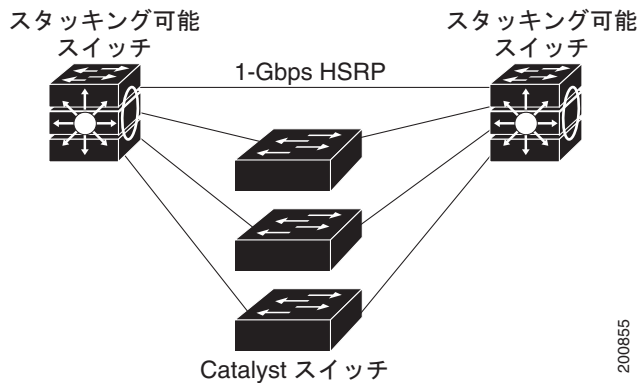
図 1-3 Catalyst 3560-X スタンドアロン スイッチでの高性能ワークグループ (GDT)





- 冗長ギガビット バックボーン (図 1-4) : HSRP によって、2 つの Catalyst 3750-X ギガビット 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 3750-X 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。

図 1-4 冗長ギガビット バックボーン



- サーバ集約 (図 1-5) と Linux サーバクラスタ (図 1-6) : Catalyst 3560-X スイッチと Catalyst 3750-X スイッチ専用スイッチ スタックを使用して、サーバグループを相互接続し、ネットワークの物理的なセキュリティと管理を一元化できます。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 スイッチを、ルーティング機能を備えたマルチレイヤ スイッチに接続します。ギガビットの相互接続によって、データ フローの遅延を最小限に抑えることができます。

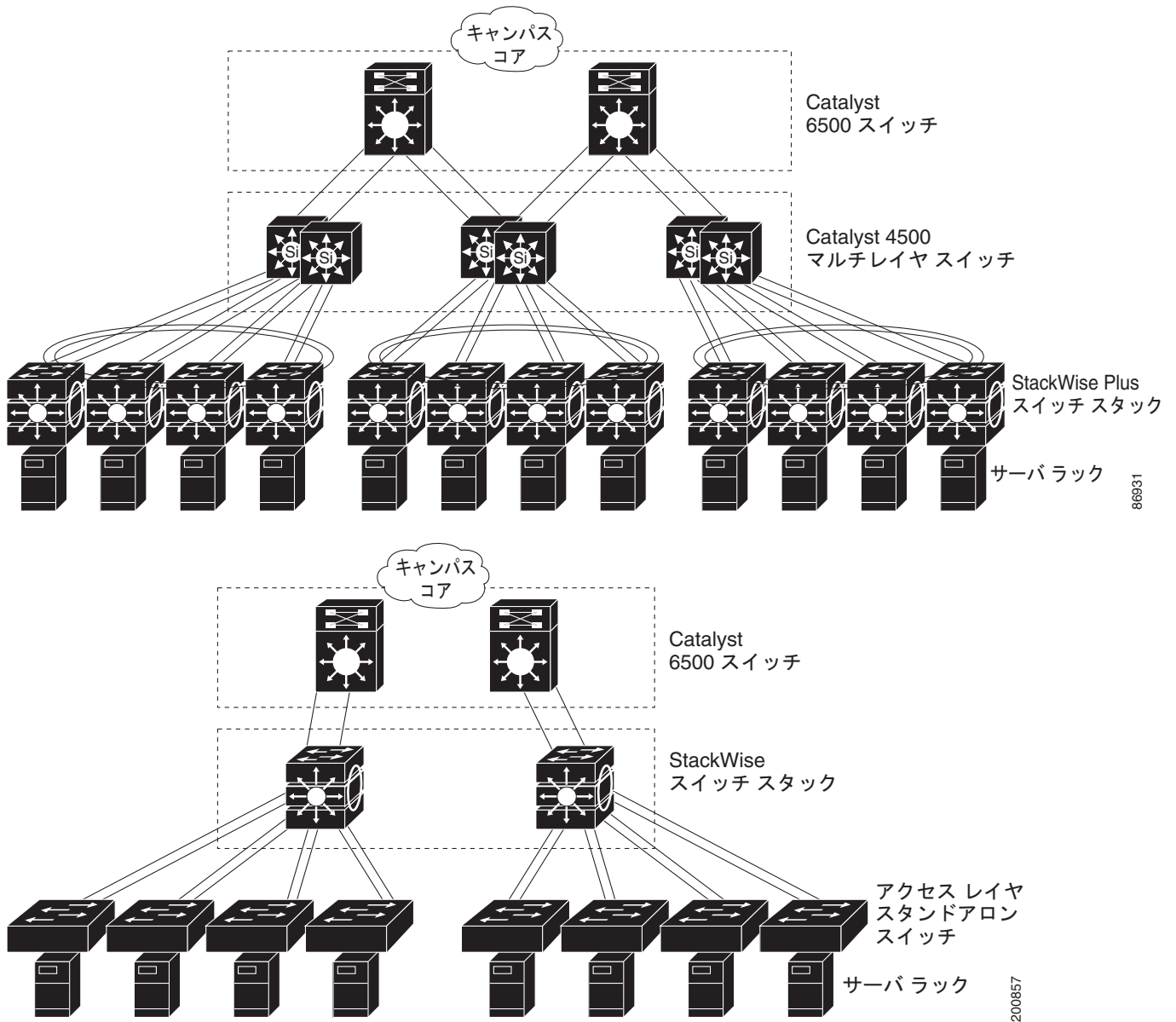
スイッチ上の QoS およびポリシングによって、特定のデータ ストリームが優先的に処理されます。トラフィック ストリームはいくつかの経路に分けられて処理されます。スイッチのセキュリティ機能によって、パケットの高速処理が保証されます。

サーバラックからコアへの耐障害性は、冗長ギガビット EtherChannel とクロススタック EtherChannel を有するデュアルスイッチスタックまたはスイッチに接続された、デュアルホーミングサーバによって達成されます。

スイッチのデュアル SFP モジュールアップリンクを使用すると、ネットワークコアに冗長アップリンクを構築できます。SFP モジュールを使用すると、光ファイバ接続におけるメディアおよび距離のオプションに柔軟性が提供されます。

0.5 ~ 3 m までのさまざまな長さのスタックケーブルが使用可能なため、複数のサーバラック間のスイッチスタックの接続を拡張して、複数のスタック集約を実現できます。

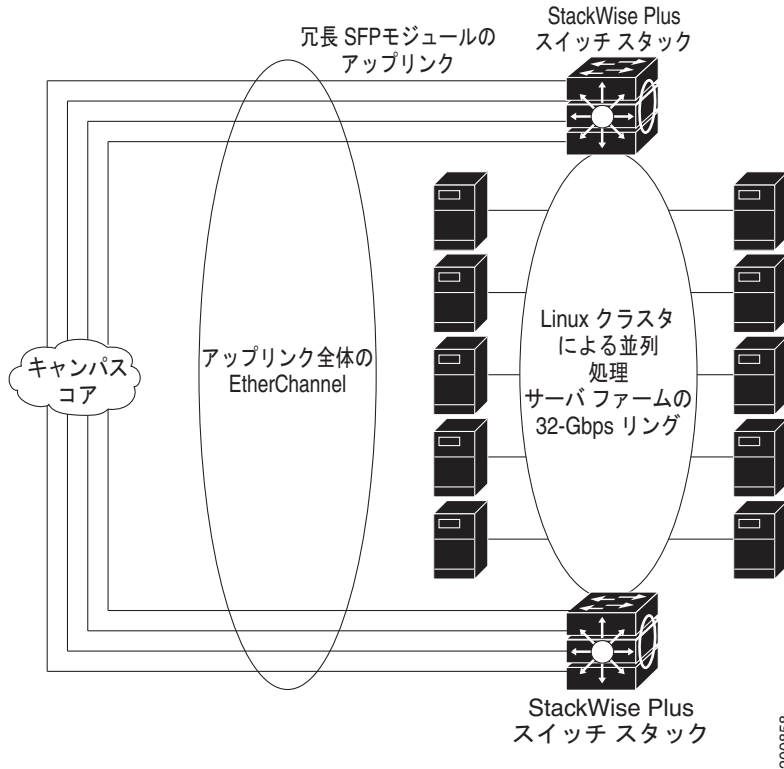
図 1-5 サーバ集約



86931

200857

図 1-6 Linux サーバクラスタ



## Catalyst 3750-X と 3560-X スイッチを使用した中小規模ネットワーク

図 1-7 および図 1-8 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。このネットワークでは、Catalyst 3750-X レイヤ 3 スイッチ スタックまたは Catalyst 3560-X レイヤ 3 スイッチを使用し、2 つのルータに高速接続できるようにします。また、ネットワーク信頼性とロード バランシングを実現するため、ルータとスイッチ上で 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。スイッチは、より高速にフェールオーバーを実行するためにルーテッドアップリンクを使用しています。また、ロード バランシングと冗長構成用に等価コスト ルーティングが設定されています（ネットワークで Catalyst 3750-X スイッチを使用している場合、レイヤ 2 スイッチ スタックは、ロード バランシングにクロススタック EtherChannel を使用できます）。

スイッチには、ワークステーション、ローカル サーバ、および IEEE 802.3af 準拠（または非準拠）の受電装置（Cisco IP Phone など）が接続されます。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。CCM は、コール処理、ルーティング、および Cisco IP Phone 機能とその設定を制御します。スイッチは、ギガビット インターフェイスによって相互接続されています。

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 VVVID 上に設定します。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。

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、ルータまたはレイヤ 3 スイッチが宛先 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 3750-X 専用スイッチ スタックまたは Catalyst 3560-X スイッチが VLAN 間ルーティングを行います。スイッチ スタック上の VLAN ACL (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、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、高優先順位トラフィックを配信します。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送送できるようにします。

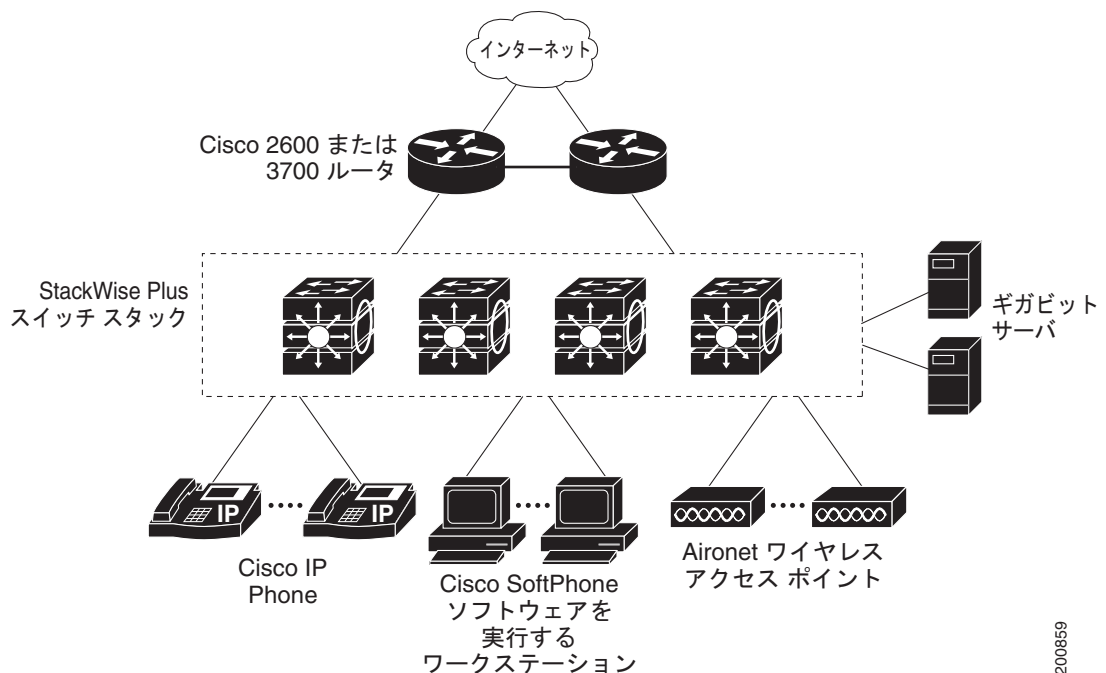
Catalyst PoE スイッチと接続している先行標準の受電装置および IEEE 802.3af 準拠の受電装置では、IEEE 802.1p/Q QoS を使用することにより、音声トラフィックをデータトラフィックよりも優先的に転送できます。

Catalyst PoE スイッチポートは、シスコの先行標準の受電装置および IEEE 802.3af 準拠の受電装置の接続を自動的に検出します。各 PoE スイッチポートは、各ポートに 15.4 W の電力を供給します。受電装置 (Cisco IP Phone など) が AC 電源に接続されている場合、冗長化された電力供給を受けることができます。Catalyst PoE スイッチに接続していない受電装置は、電力を得るために AC 電源に接続する必要があります。

CCM は、コール処理、ルーティング、および Cisco 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持つユーザは、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。

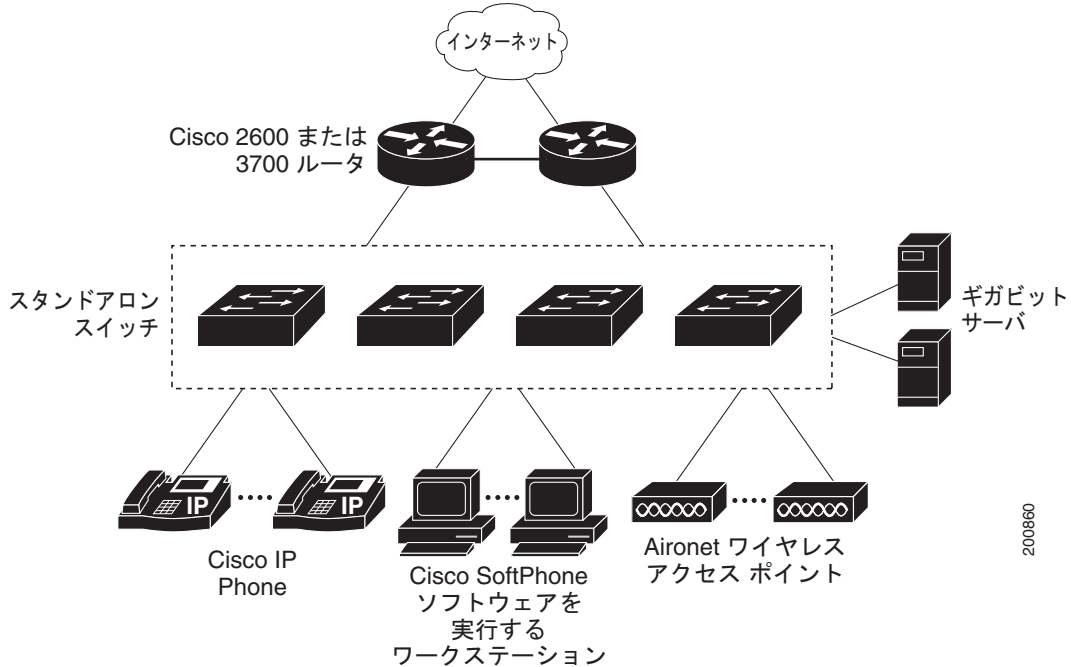
VLAN 間ルーティングや他のネットワークサービスを提供するマルチレイヤ スイッチを使用することで、ルータが重点を置くのは、ファイアウォールサービス、Network Address Translation (NAT; ネットワークアドレス変換) サービス、Voice over IP (VoIP) ゲートウェイサービス、WAN およびインターネットアクセスです。

図 1-7 コラプストバックボーン構成の Catalyst 3750-X 専用スイッチ スタック



200859

図 1-8 コラプスト バックボーン構成の Catalyst 3560-X スイッチ



## Catalyst 3750-X と 3560-X スイッチを使用した大規模ネットワーク

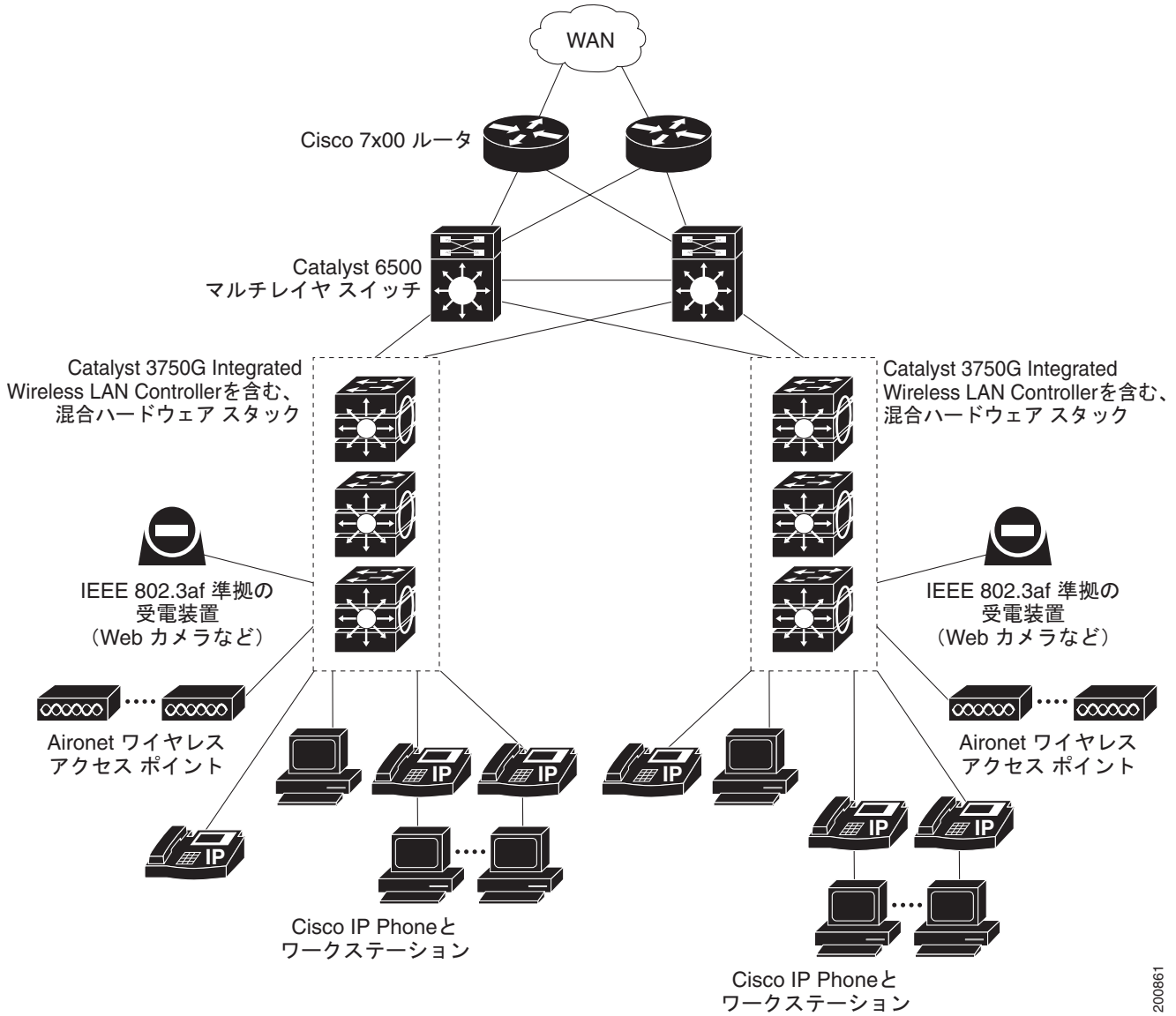
ワイヤリング クローゼット内のスイッチは、従来、レイヤ 2 デバイスだけでしたが、ネットワークトラフィック プロファイルが拡大するにつれ、ワイヤリング クローゼット内のスイッチでマルチキャスト管理やトラフィック分類などのマルチレイヤ サービスがますます採用されつつあります。図 1-9 に、ワイヤリング クローゼット内の Catalyst 3750-X スイッチ スタックと Catalyst 6500 などの 2 つのバックボーン スイッチだけを使用して、最大 10 のワイヤリング クローゼットを集約するネットワークの構成を示します。また、図 1-10 に、ワイヤリング クローゼット内の Catalyst 3560-X スイッチと Catalyst 6500 スイッチなどの 2 つのバックボーン スイッチだけを使用して、最大 10 のワイヤリング クローゼットを集約するネットワークの構成を示します。

ワイヤリング クローゼットの各スイッチ スタックまたはスイッチは、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ドロップまたはマークする QoS ACL も、各スイッチ スタックまたは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。

各スイッチ スタックまたはスイッチは、VLAN 間ルーティングを提供します。これらは、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取得するので、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。

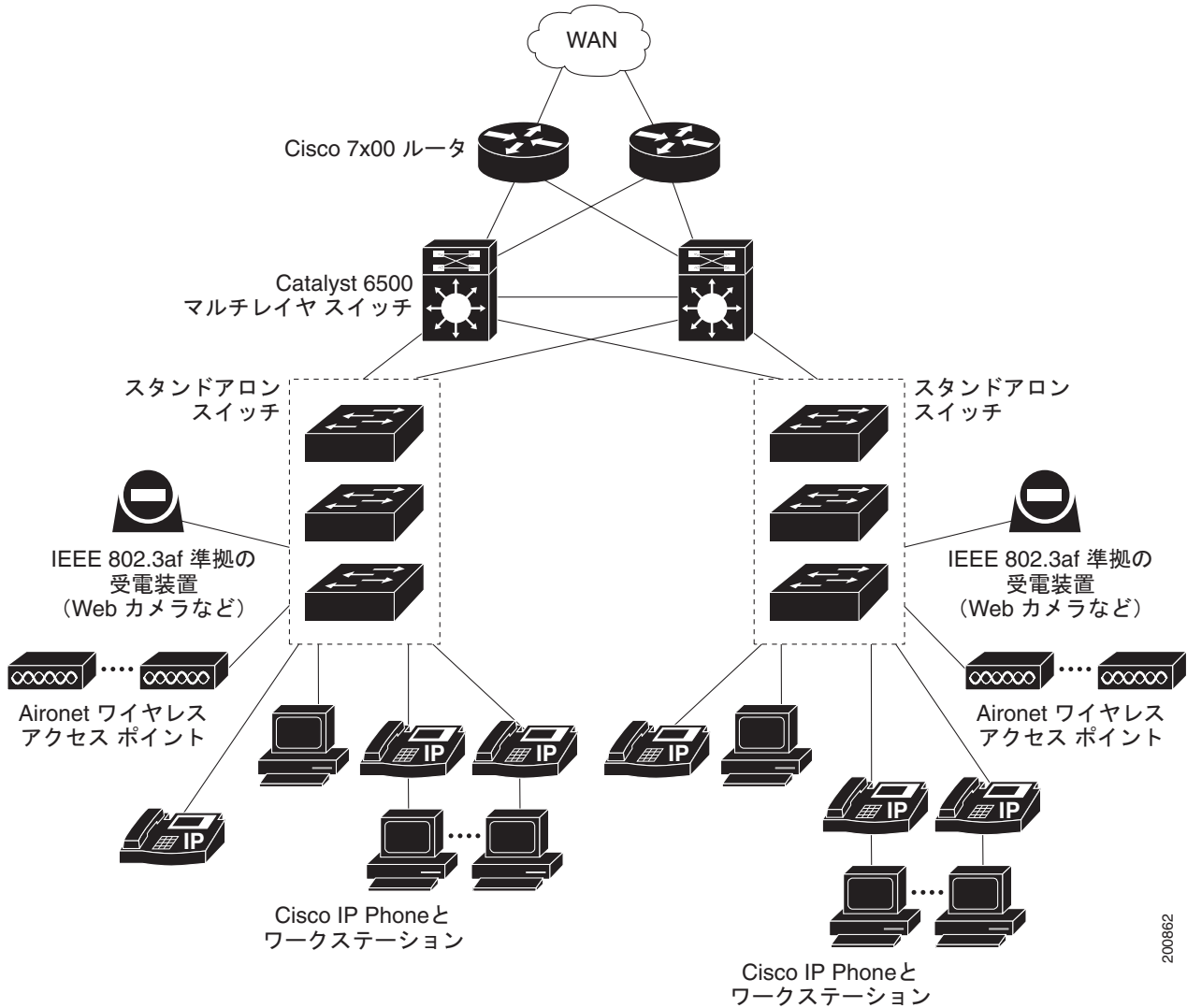
ルータおよびバックボーン スイッチでは、HSRP をイネーブルにして、ロード バランシングおよび冗長接続を実行可能にして、ミッションクリティカルなトラフィックを保証します。

図 1-9 バックボーン構成のワイヤリング クローゼット内の Catalyst 3750-X スイッチ スタック



200861

図 1-10 バックボーン構成のワイヤリング クローゼット内の Catalyst 3560-X スイッチ スタック



200862



## Catalyst 3750-X スイッチを使用した集合住宅ネットワーク

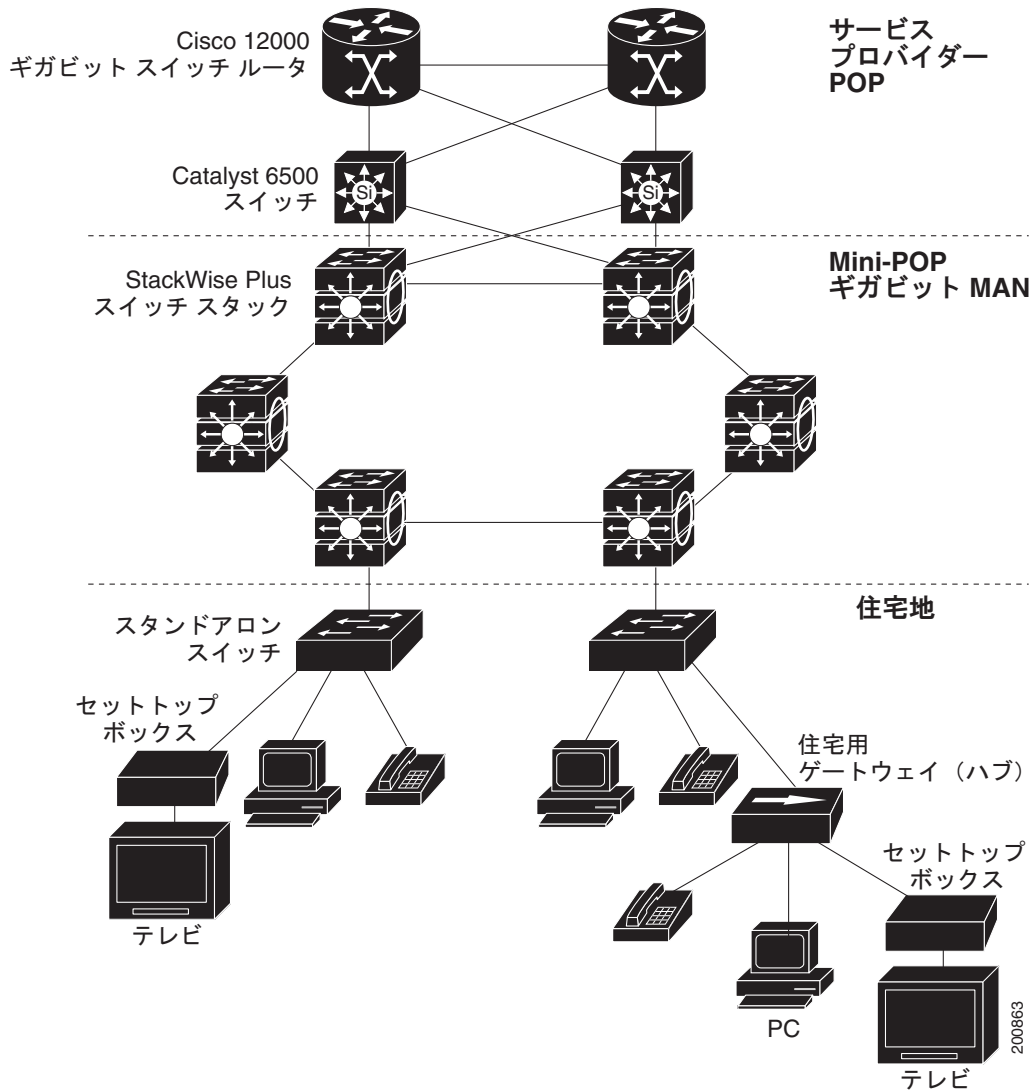
住宅地域および商業地域で、イーサネット Metropolitan-Area Networking (MAN; メトロポリタンエリア ネットワーク) への高速アクセスを必要とするユーザが増加しています。図 1-11 に、Mini-Point-of-Presence (Mini-POP) においてマルチレイヤ スイッチ スタックを集約スイッチとして使用したギガビットイーサネット MAN リング構成を示します。これらのスイッチは、1000BASE-X SFP モジュール ポート経由で接続しています。

住宅用スイッチとして Catalyst 3750-X 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 2950 LRE スイッチも使用できます。Catalyst 2950 LRE スイッチは、別の住宅用スイッチまたは Catalyst 3750 集約スイッチに接続することもできます。Catalyst LRE スイッチの詳細については、これらのスイッチのマニュアルを参照してください。

住宅用 Catalyst 3750-X 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、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 3750 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「Catalyst 3750-X と 3560-X スイッチを使用した中小規模ネットワーク」(P.1-28) および「Catalyst 3750-X と 3560-X スイッチを使用した大規模ネットワーク」(P.1-30) に記載されているようなサービスを提供します。

図 1-11 MAN 構成の Catalyst 3750-X スイッチ



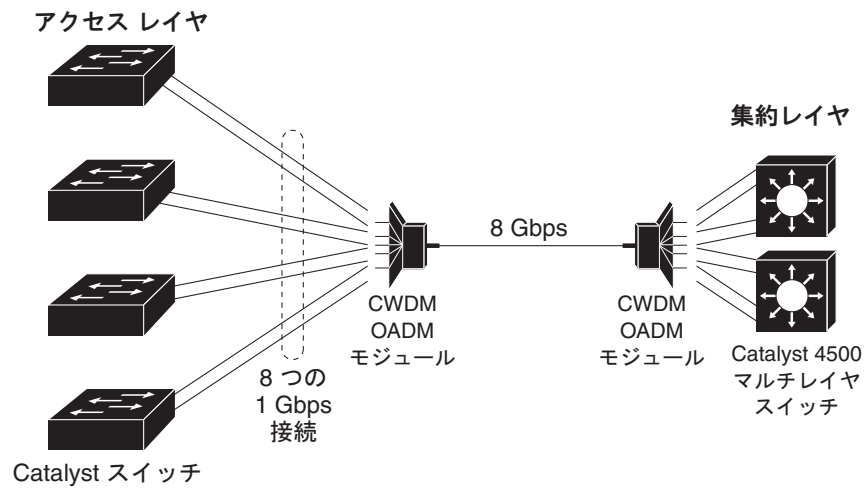
## 長距離広帯域トランスポートの構成

図 1-12 に、8 Gbps のデータを 1 本の光ファイバ ケーブルで伝送する構成を示します。Catalyst 3750-X または 3560-X スイッチには、Coarse Wavelength-Division Multiplexer (CWDM) 光ファイバ SFP モジュールが搭載されています。CWDM SFP 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 SFP 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 (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。

CWDM SFP モジュールおよび CWDM OADM モジュールの詳細については、『Cisco CWDM GBIC and CWDM SFP Installation Note』を参照してください。

図 1-12 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「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」](#)

