



## 概要

---

この章では、Catalyst 3560 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 \(p.1-2\)](#)
- [スイッチ初期設定後のデフォルト値 \(p.1-13\)](#)
- [ネットワークの構成例 \(p.1-16\)](#)
- [次の作業 \(p.1-23\)](#)

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。

## 機能

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

- IP ベース イメージ (以前の Standard Multilayer Image [SMI; 標準マルチレイヤ イメージ]) — レイヤ 2+ 機能を提供します (エンタープライズ クラスのインテリジェント サービス)。これらの機能としては、Access Control List (ACL; アクセス コントロール リスト)、QoS (Quality of Service)、スタティック ルーティング、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; ホットスタンバイ ルータ プロトコル)、Routing Information Protocol (RIP) などがあります。IP ベース イメージがインストールされたスイッチは、IP サービス イメージ (以前の Enhanced Multilayer Image [EMI; 拡張マルチレイヤ イメージ]) にアップグレードできます。
- IP サービス イメージ — 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 セットを提供します。それには、すべての IP ベース イメージ機能と完全なレイヤ 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) が含まれます。IP サービス イメージには、レイヤ 2+ スタティック ルーティングや RIP と区別される特長として、Enhanced Interior Gateway Routing Protocol (EIGRP) や Open Shortest Path First (OSPF) などのプロトコルが含まれています。

IP サービス イメージのみに対応するレイヤ 3 機能については、「[レイヤ 3 機能](#)」(p.1-10) に記載されています。



(注) 特に注記がないかぎり、このマニュアルで取り上げる機能はすべて、IP ベース イメージと IP サービス イメージでサポートされています。

IPv6 Multicast Listener Discovery (MLD) スヌーピングは、すべての Catalyst 3560 および 3750 イメージでサポートされます。詳細については、[第 37 章「IPv6 MLD スヌーピングの設定」](#)を参照してください。IPv6 ルーティングおよび IPv6 ACL を含む IPv6 のフルサポートでは、拡張 IP サービス イメージが必要です。シスコからこのイメージのアップグレード ライセンスを入手できます。IPv6 ルーティングの詳細については、[第 36 章「IPv6 ユニキャスト ルーティングの設定」](#)を参照してください。IPv6 ACL の詳細については、[第 38 章「IPv6 ACL の設定」](#)を参照してください。

この章で取り上げる一部の機能は、ソフトウェアの IP ベース イメージと IP サービス イメージの暗号化バージョン (つまり、暗号化をサポートするバージョン) のみに対応しています。この機能を使用し、Cisco.com から暗号化ソフトウェアをダウンロードするには許可を得る必要があります。詳細については、このリリースのリリース ノートを参照してください。

スイッチの機能は次のとおりです。

- [使用および導入を簡素化する機能](#) (p.1-3)
- [パフォーマンス向上機能](#) (p.1-4)
- [管理オプション](#) (p.1-5)
- [管理の簡易性に関する機能](#) (p.1-5) (ソフトウェアの IP ベース イメージと IP サービス イメージの暗号化バージョンが必要な機能を含む)
- [アベイラビリティおよび冗長性に関する機能](#) (p.1-6)
- [VLAN 機能](#) (p.1-7)
- [セキュリティ機能](#) (p.1-7) (ソフトウェアの IP ベース イメージと IP サービス イメージの暗号化バージョンが必要な機能を含む)
- [QoS および CoS 機能](#) (p.1-9)
- [レイヤ 3 機能](#) (p.1-10) (IP サービス イメージが必要な機能を含む)
- [PoE 機能](#) (p.1-11)
- [モニタ機能](#) (p.1-12)

## 使用および導入を簡素化する機能

スイッチには、使用と導入を容易にするため、次の機能が搭載されています。

- 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 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。
- 組み込みのデバイス マネージャ GUI (グラフィカル ユーザ インターフェイス) — 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 (以降、*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 (コマンドライン インターフェイス) 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、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すみます。
  - スイッチ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。
- 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、Small Form-Factor Pluggable (SFP) モジュール、ギガビット イーサネット、Gigabit 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。

## パフォーマンス向上機能

スイッチには、次の機能が搭載されています。

- 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 10/100/1000 BASE-TX SFP モジュール インターフェイス上の Auto MDIX 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。
- ルーテッド フレームの場合は最大 1546 バイト、ハードウェアでブリッジングされるフレームの場合は最大 9000 バイト、ソフトウェアでブリッジングされるフレームの場合は最大 2000 バイトのサポート
- 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。）
- 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（Fast EtherChannel）全二重の帯域幅を確保
- 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。
- ギガビット回線レートでのレイヤ 2 およびレイヤ 3 パケットの転送
- 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。
- 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。
- Web Cache Communication Protocol (WCCP)。トラフィックのローカル広域アプリケーション 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 (IP サービス イメージが必要) を行います。

## 管理オプション

次のオプションは、スイッチの設定と管理を実行します。

- 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 にアクセスするには、スイッチのコンソール ポートに管理ステーションを直接接続するか、リモート管理ステーションから Telnet を使用します。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。
- SNMP — 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。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31章「SNMP の設定」を参照してください。
- CNS — Cisco Networking Services は、ネットワーク管理ソフトウェアで、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ためのコンフィギュレーション サービスとして機能します。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 CNS エージェントの設定」を参照してください。

## 管理の簡易性に関する機能

次に、管理の簡易性に関する機能を示します。

- 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
- 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
- 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 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廃棄するユニキャスト 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製デバイスとのマッピングを行います。
- Link Layer Discovery Protocol (LLDP) および LLDP Media Endpoint Discovery (LLDP-MED) によるサードパーティ製 IP 電話との相互運用性の確保
- 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 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。
- 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が可能です(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)。
- 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。
- Secure Copy Protocol (SCP) 機能では、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できます(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)。

## アベイラビリティおよび冗長性に関する機能

アベイラビリティおよび冗長性に関する機能を次に示します。

- HSRP により、コマンドスイッチとレイヤ 3 ルータの冗長性を確立します。
- Unidirectional Link Detection (UDLD; 単一方向リンク検出) およびアグレッシブ UDLD。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
  - スパニングツリー トポロジ変更のあとの迅速なコンバージェンス、およびギガビット アップリンクを含む冗長アップリンク間のロード バランシングを実現する UplinkFast および BackboneFast
- 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更迭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 トラフィックを送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ヘサーバ トラフィックをフェールオーバーすることができます。
- Cisco RPS 300 および Cisco RPS 675 による RPS サポート。電源の信頼性が向上します。

## VLAN 機能

次に、VLAN に関する機能を示します。

- 最大 1005 個の 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働する 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グ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。
- VLAN 1 の最小化 — VLAN 1 を任意の個々の VLAN トランク リンクでディセーブル化することで、スパニング ツリー ループまたはストームのリスクを軽減。この機能をイネーブルに設定すると、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。
- PVLAN ホスト上のポート セキュリティ — ポートで学習する MAC アドレスの数を制限したり、ポートで学習可能な MAC アドレスを指定します。
- VLAN Flex Link ロード バランシング — STP を必要としないレイヤ 2 冗長性を提供。プライマリおよびバックアップ リンクとして設定したインターフェイスのペアを使用して、VLAN ベースによるトラフィックのロード バランシングが可能です。

## セキュリティ機能

スイッチには、次のセキュリティ機能が搭載されています。

- Web 認証。IEEE 802.1x 機能をサポートしないサブリカント (クライアント) を Web ブラウザを使用して認証可能になります。
- MAC authentication bypass (MAB; MAC 認証バイパス) エージング タイマー。MAB を使用して認証したあとに認証された非アクティブのホストを検出します。
- 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
- VLAN 認識ポート セキュリティ オプション。違反の発生時にポート全体をシャットダウンするのではなく、そのポート上の VLAN をシャットダウンします。
- 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。
- 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。
- 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 検査。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。
- 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; マルチドメイン認証)。データ デバイスと (シスコまたはシスコ以外の) IP 電話のような音声デバイスの両方が、独立して同一の IEEE 802.1x 対応スイッチ ポートを認証することができます。
  - VLAN 割り当て。802.1x 認証ユーザを特定の VLAN に制限します。
  - 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。
  - IP Phone 検出の機能拡張。Cisco IP Phone を検出し識別します。
  - 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 で認証するための証明書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トラッキングします。
  - 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。



- MAC 認証バイパス。クライアント MAC アドレスに基づいてクライアントを許可します。
- 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イルス対策の状態または態勢に関する 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.9-40) 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態勢に関する 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.9-36) を参照してください。
  - Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) ダウン ポリシー。態勢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。
- 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。
- RADIUS。AAA 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トラッキングします。
- 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 (ソフトウェアの IP ベース イメージと IP サービス イメージの暗号化バージョンが必要)。
- HTTP 1.1 サーバ認証、暗号化、メッセージ整合性、HTTP クライアント認証用に Secure Socket Layer (SSL) バージョン 3.0 がサポートされ、安全な HTTP 通信が可能になります (ソフトウェアの IP ベース イメージと IP サービス イメージの暗号化バージョンが必要)。

## QoS および CoS 機能

次に、QoS および CoS 機能を示します。

- 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
  - 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)
  - 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

- Cisco IOS Release 12.2(25)SED 以降では、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廃棄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) — パケットがキューから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廃棄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。

## レイヤ 3 機能

次に、レイヤ 3 機能について説明します。



(注)

ここで取り上げる一部の機能は IP サービス イメージのみに対応しています。

- HSRP — レイヤ 3 ルータの冗長性
- IP ルーティング プロトコルによるロードバランシングとスケーラブルなルーテッド バックボーンの構築
  - RIP バージョン 1 および 2
  - OSPF (IP サービス イメージが必要)
  - EIGRP (IP サービス イメージが必要)
  - Border Gateway Protocol (BGP) バージョン 4 (IP サービス イメージが必要)
- 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 (マルチ 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; パ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 イメージが必要)
- 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 イメージが必要)
- 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およびルータ 請求メッセージによる直接接続サブネット上のルータのアドレス検索
- Protocol-Independent Multicast (PIM) によるネットワーク内マルチキャスト ルーティング。これにより、ネットワーク内のデバイスは要求されたマルチキャスト フィードの受信が可能になり、マルチキャストに参加しないスイッチのプルーニングが可能になります。PIM sparse mode (PIM-SM; PIM sparse [希薄] モード)、PIM dense mode (PIM-DM; PIM dense [稠密] モード)、および PIM sparse-dense モードのサポートも含まれます (IP サービス イメージが必要)。
- Multicast Source Discovery Protocol (MSDP) — 複数の PIM-SM ドメインを接続 (IP サービス イメージが必要)
- 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 イメージが必要)
- 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
- 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 (拡張 IP サービス イメージが必要)
- 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、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 対応近接ルータからのパケットを継続して転送することが可能

## PoE 機能

次に、Power over Ethernet (PoE) 機能について説明します。

- 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。
- 電力消費を含む 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。
- シスコの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 バジレット。スイッチはパワー バジレットを維持し、電力要求をモニタおよびトラッキングし、利用できる場合にのみ電力を供給します。

## モニタ機能

次に、モニタ機能を示します。

- 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
- 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トラッキングします。
- Switched Port Analyzer (SPAN; スイッチドポートアナライザ) および Remote SPAN (RSPAN)。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（履歴、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)。10/100/1000 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。
- 汎用オンライン診断。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。
- HSRP に対する拡張オブジェクトのトラッキング

## 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 21 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のみ)。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のみ)。詳細は、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 21 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 クラスタはディセーブルに設定されています。スイッチ クラスタの詳細は、第 5 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。詳細は、第 6 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。詳細は、第 6 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。詳細は、第 6 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。詳細は、第 6 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。詳細は、第 8 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。詳細は、第 8 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。詳細は、第 8 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。詳細は、第 9 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。詳細は、第 10 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。詳細は、第 10 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。詳細は、第 10 章「インターフェイス特性の設定」を参照してください。



(注) Cisco IOS Release 12.2(20)SE より前のリリースでは、auto-MDIX のデフォルト設定はディセーブルです。

- フロー制御はディセーブルに設定されています。詳細は、第 10 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。詳細は、第 10 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。詳細は、第 11 章「SmartPort マクロの設定」を参照してください。
- VLAN
  - デフォルト VLAN は VLAN 1 です。詳細は、第 12 章「VLAN の設定」を参照してください。
  - VLAN トランキン設定は dynamic auto (DTP) です。詳細は、第 12 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。詳細は、第 12 章「VLAN の設定」を参照してください。
  - VTP モードはサーバです。詳細は、第 13 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。詳細は、第 13 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。詳細は、第 15 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。詳細は、第 14 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。詳細は、第 16 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。詳細は、第 17 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。詳細は、第 18 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。詳細は、第 19 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。詳細は、第 20 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。詳細は、第 21 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。詳細は、第 21 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 検査はすべての VLAN でディセーブルに設定されています。詳細は、第 22 章「ダイナミック ARP 検査の設定」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。詳細は、第 23 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されます。詳細は、第 23 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。詳細は、第 23 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。詳細は、第 23 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。詳細は、[第24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。詳細は、[第24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。詳細は、[第24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。詳細は、[第24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。詳細は、[第25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。詳細は、[第27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。詳細は、[第28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。詳細は、[第29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。詳細は、[第30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)。詳細は、[第31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。詳細は、[第32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。詳細は、[第33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。詳細は、[第34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。詳細は、[第35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す。詳細は、[第39章「HSRP および拡張オブジェクト トラッキングの設定」](#)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。詳細は、[第41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。詳細は、[第42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。詳細は、[第43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。

- [スイッチを使用する場合の設計概念 \(p.1-16\)](#)
- [Catalyst 3560 スイッチを使用する中小規模ネットワーク \(p.1-19\)](#)
- [Catalyst 3560 スイッチを使用する大規模ネットワーク \(p.1-21\)](#)
- [長距離広帯域トランスポートの構成 \(p.1-23\)](#)

## 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の増大</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) による帯域幅需要の増大</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>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。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 15 MB の IP 接続を提供します。</p> <p> (注) 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。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>

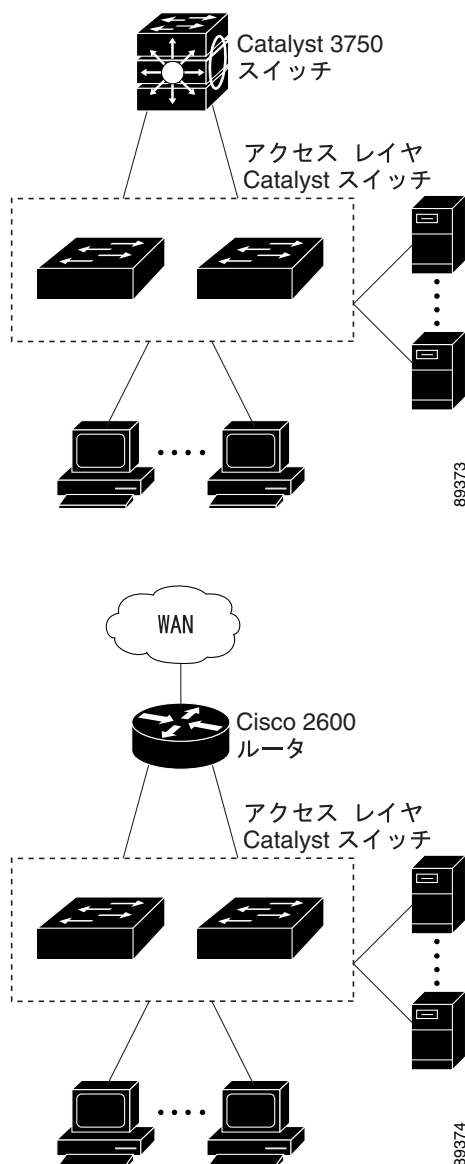
スイッチを使用して、以下を作成できます。

- 高性能なワークグループ向けの、費用効率に優れた Gigabit-To-The-Desktop (GTTD) (図 1-1) — ネットワーク リソースへの高速アクセス用に、アクセス レイヤ上の Cisco Catalyst 3560 スイッチを使用できます。これにより、デスクトップ上でギガビット イーサネットを実現できます。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層で高速 IP 転送を実現するには、アクセス層のスイッチを、Catalyst 3750 ギガビット スイッチやルータなどのルーティング機能を備えたギガビット マルチレイヤ スイッチに接続します。

最初の図は、分離された高性能なワークグループを示します。ここでは、ディストリビューション レイヤ内の Catalyst 3750 スイッチに Catalyst 3560 スイッチが接続されています。2 番目の図は、ブランチ オフィス内の高性能なワークグループを示します。ここでは、Catalyst 3560 スイッチがディストリビューション レイヤ内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。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 1-1 高性能なワークグループ (GHHD)



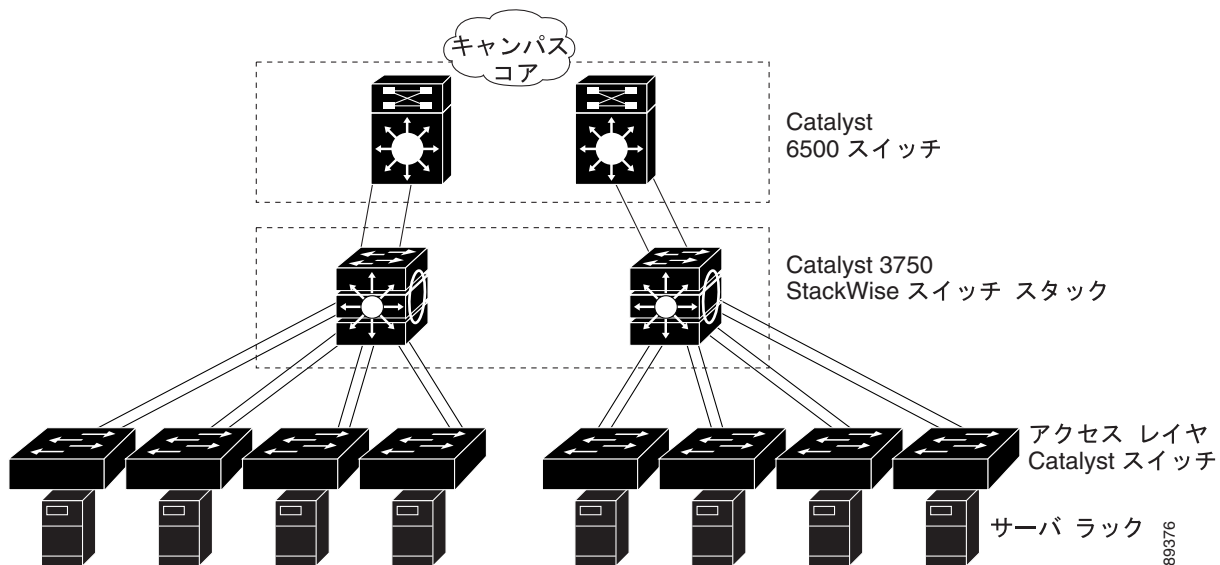
- サーバ集約(図 1-2) — ネットワークの物理的なセキュリティおよび管理の集中化のためにサーバグループを相互接続する場合にスイッチを使用できます。ディストリビューションレイヤで高速 IP 転送を実現するには、アクセスレイヤスイッチを、ルーティング機能を備えたマルチレイヤスイッチに接続します。ギガビットの相互接続によって、データフローの遅延を最小限に抑えることができます。

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 を持つ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が提供されます。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。

図 1-2 サーバ集約



## Catalyst 3560 スイッチを使用する中小規模ネットワーク

図 1-3 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、2 つのルータへの高速接続を実現する Catalyst 3560 レイヤ 3 スイッチを使用します。ネットワークの信頼性とロード バランシングのために、このネットワークでは HSRP をルータとスイッチでイネーブルにしています。これにより、万が一ルータやスイッチの 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。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 シェアリ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。

スイッチは、ワークステーション、ローカルサーバ、および IEEE 802.3af 準拠（および非準拠）の受電装置（Cisco IP Phone など）に接続されています。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 VVID 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、スイッチが VLAN 間ルーティングを行います。スイッチ上の 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、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 がロー プライオリティ トラフィックを廃棄し、ハイ プライオリティ トラフィックを伝送できるようにします。

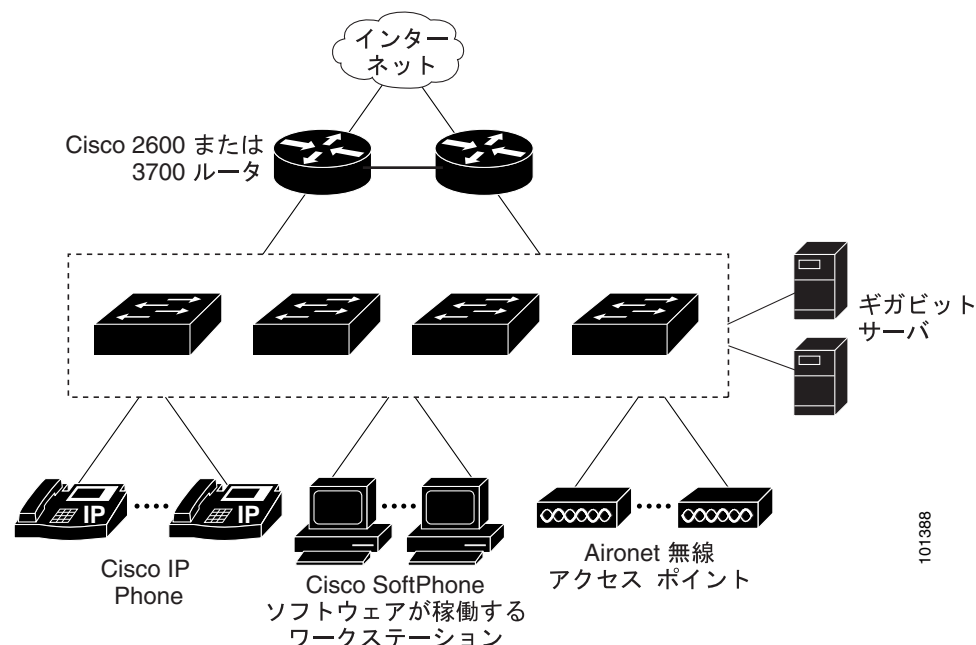
Catalyst PoE スイッチと接続している先行標準の受電装置および IEEE 802.3af 準拠の受電装置では、IEEE 802.1p/Q QoS を使用することにより、音声トラフィックをデータ トラフィックよりも優先的に転送できます。

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 1-3 コラプスト バックボーン構成の Catalyst 3560 スイッチ



## Catalyst 3560 スイッチを使用する大規模ネットワーク

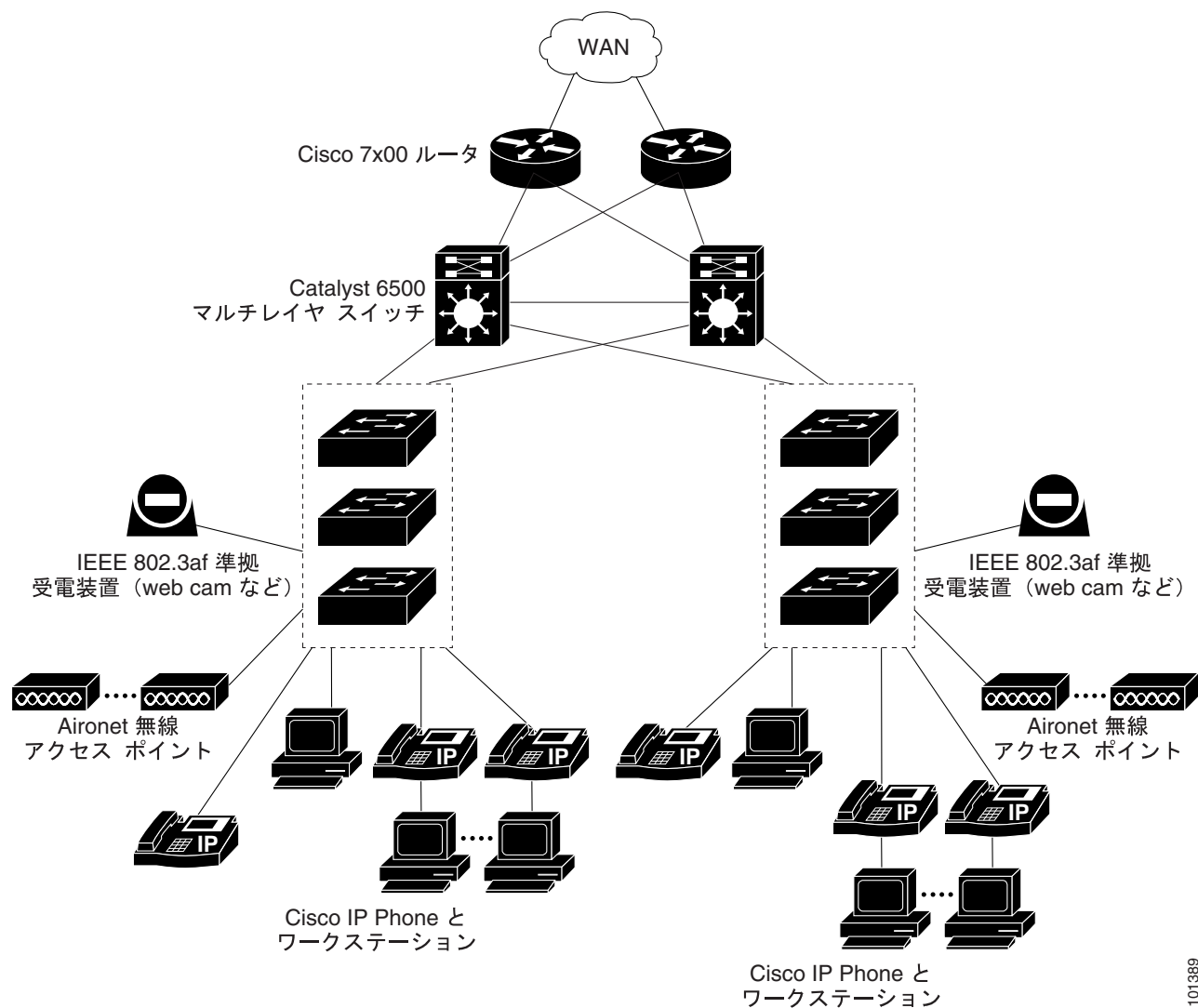
ワイヤリング クローゼット内のスイッチは、これまでレイヤ2 専用デバイスでしたが、ネットワークトラフィック プロファイルの改善に伴い、ますますマルチキャスト管理やトラフィック分類などのマルチレイヤ サービスを採用するようになっていきます。図 1-4 に、ワイヤリング クローゼットに Catalyst 3560 マルチレイヤ スイッチと、最大 10 のワイヤリング クローゼットを集約する Catalyst 6500 スイッチなどの 2 台のバックボーン スイッチのみを使用するネットワークの構成を示します。

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、スイッチは、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 1-4 バックボーン構成でのワイヤリング クローゼットの Catalyst 3560 スイッチ



101389

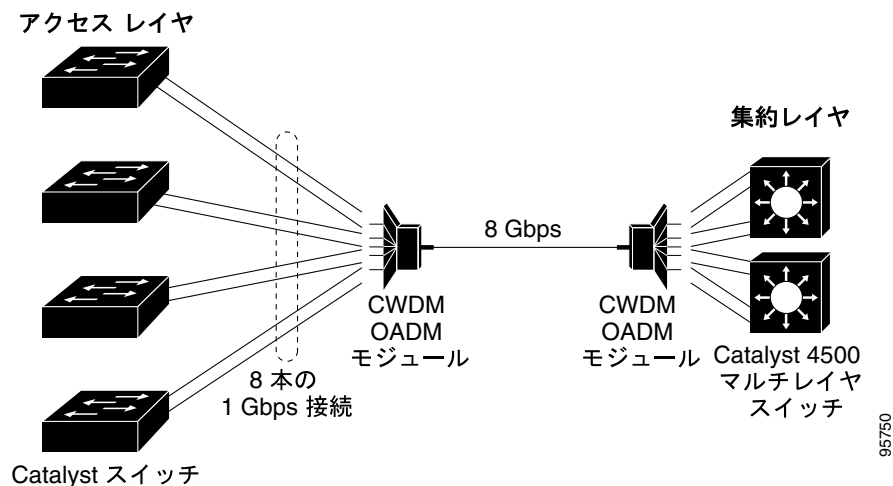
## 長距離広帯域トランスポートの構成

図 1-5 に、8 Gb 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 3560 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; オプティカル Add/Drop マルチプレクサ) 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 1-5 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「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」](#)

