CHAPTER 1

概要

この章では、Catalyst 3750 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。

特に明記しない限り、*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 スタックを指します。

このマニュアルでは、IP Version 6（IPv6）に関して特に記載がない限り、IP は IP Version 4（IPv4）を指します。

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：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、アクセス コントロール リスト（ACL）、Quality of Service（QoS）、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 イメージだけに対応するレイヤ 3 機能については、「レイヤ 3 機能」（P.1-15）に記載されています。

（注） 特に注記がない限り、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 41 章「IPv6 MLD スヌーピングの設定」を参照してください。

IPv6 のフルサポートでは、IP サービス イメージが必要です。IPv6 ルーティングの詳細については、第 39 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 40 章「IPv6 ACL の設定」を参照してください。

使用および導入を簡素化する機能

- 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、スタートアップ ガイド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：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、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。
- 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。
  - イントラ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コマンドライン インターフェイス（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（仮想 LAN）、アクセス コントロール リスト（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、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リングできます。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。

  Network Assistant は、必ず、cisco.com/go/cna からダウンロードしてください。

- LAN Base イメージが実行されている Catalyst 2960-S スイッチの Cisco FlexStack テクノロジーの機能概要
- Cisco StackWise テクノロジーの機能概要
  - StackWise 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。
  - スイッチ スタック全体で、双方向 32 Gbps スイッチング 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 アドレスおよび設定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。
  - 新しいスタック メンバの自動 Cisco IOS バージョン チェックを行うことができ、オプションで、スタック マスターまたは TFTP サーバからイメージを自動的にロードできます。
  - スタックの動作を妨げることなく、スタック上でスイッチの追加、削除、および置き換えを行うことができます。
  - オフライン設定機能付きのスイッチ スタックで、新しいメンバをプロビジョニングできます。ユーザは、特定のスタック メンバ番号、および、スタックの一部ではない新しいスイッチの特定のスイッチ タイプに対して、事前にインターフェイスを設定できます。スイッチ スタックでは、プロビジョニングされたスイッチがスタックの一部かどうかに関係なく、スタックのリロード時にこの情報が残されます。
  - スタック リング アクティビティ統計情報（各スタック メンバからリングに送信されたフレームの数）を表示できます。
- 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、Small Form-Factor Pluggable 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。
- スタックのトラブルシューティング機能の拡張
- Auto Smartport
  - ポートで検出されたデバイス タイプに基づいてポートを動的に設定するシスコのデフォルトおよびユーザ定義マクロ。

  - 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 の自動 QoS、および IP 電話のサポートを強化する拡張機能。
  - マクロの永続性、LLDP ベースのトリガー、MAC アドレスおよび OUI ベースのトリガー、リモート マクロに対するサポート、および Cisco Digital Media Player（Cisco DMP）と Cisco IP Video Surveillance Camera（Cisco IPVSC）という 2 つの新しいデバイス タイプに基づく自動設定に対するサポートを追加する拡張機能。
  - Auto Smartport は、CDP 対応の Cisco Digital Media Player 上で自動 QoS をイネーブルにする拡張機能です。
  - デバイスの分類機能と精度が改善され、デバイス可視性が向上し、マクロ管理が機能強化されています。デバイス分類子はデフォルトでイネーブルになっており、DHCP オプションに基づいてデバイスを分類できます。

  詳細については、『*Auto Smartports Configuration Guide*』を参照してください。

- ネットワークの 1 箇所（ディレクタ）からの管理を可能にする Smart Install。Smart Install を使用して、新しく配置されたスイッチのゼロ タッチ イメージとコンフィギュレーションのアップグレード、およびクライアント スイッチに対するイメージとコンフィギュレーションのダウンロードを提供することができます。詳細については、『*Cisco Smart Install Configuration Guide*』を参照してください。
  - Smart Install の拡張では、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。
  - Cisco IOS Release 12.2(58)SE の Smart Install の拡張では､クライアントのスイッチ ヘルス ステートを拒否から許可に手動で変更する機能、オンデマンド アップグレードを保留にする機能、ディレクタのデータベースから選択したクライアントを削除する機能、複数のクライアントの同時オンデマンド アップグレードを許可する機能、およびクライアント デバイスに関して、デバイスのステータス、ヘルス ステータス、およびアップグレードのステータスなどを含むより多くの情報を提供する機能を含みます。
- Call Home を使用すると、E メールベースおよび Web ベースで重大なシステム イベントの通知を行えます。シスコと直接サービス契約を結んでいるお客様は、Call Home デバイスを TAC へのサービス要求を自動で生成する Cisco Smart Call Home サービスに登録できます。

パフォーマンス向上機能

- Cisco EnergyWise は、ドメイン メンバーに接続されているエンドポイントのエネルギーを管理します。詳細については、Cisco.com で Cisco EnergyWise のマニュアルを参照してください。
- EnergyWise Phase 2.5 拡張は、Wake on LAN（WoL）対応の PC の電源をリモート投入するため、ドメイン情報および WoL を分析し表示するクエリーのサポートを追加します。
- 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 インターフェイスと 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 Automatic-Medium-Dependent Interface Crossover（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）。
- スイッチ スタック内で最大 32 Gbps の転送レート。
- 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 Gb/s（ギガビット EtherChannel）または 800 Mb/s（Fast 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; リンク集約制御プロトコル）により、EtherChannel リンクを自動的に作成します。
- 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。
- マルチキャスト Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）Lite。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 ネットワーク用に複数のプライベート ルーティング ドメインを設定します。
- 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 トラフィックを転送。
- 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）。
- 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。
- IGMP ヘルパー。スイッチでホスト要求を転送して、特定の IP 宛先アドレスにマルチキャスト ストリームを加入させることができます。
- 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 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。
- IGMP の脱退タイマー。ネットワーク終了の待ち時間を設定できます。
- Switch Database Management（SDM）テンプレート。ユーザ側で選択する機能へのサポートを最大化するようにシステム リソースを割り当てます。
- 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。
  - WCCP リダイレクト リストの拒否または許可 ACL エントリのサポート

- 小さいフレームの着信しきい値。これは、小さいフレーム（64 バイト以下）が指定された伝送速度（しきい値）でインターフェイスに到着したときに、ストーム制御を回避するためのもので、設定が可能です。
- Flex Link マルチキャスト高速コンバージェンスにより、Flex Link で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が短縮化。
- サーバ グループに均等にアクセスおよび認証要求を分散できるようにするための RADIUS サーバ ロード バランシング。
- CPU 生成トラフィックの QoS マーキングのサポートと、出力ネットワーク ポートへの CPU 生成トラフィックのキュー。
- メモリの整合性検査ルーチン。無効な Ternary Content Addressable Memory（TCAM; 3 値連想メモリ）テーブル エントリの検出と修正を行います。

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、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：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。スイッチ スタックは、任意のスタック メンバのコンソール 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って、管理できます。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 32 章「SNMP の設定」を参照してください。
- Cisco IOS Configuration Engine（旧称 Cisco IOS CNS エージェント）：コンフィギュレーション サービスは、ネットワーク デバイスおよびサービスの導入と管理を自動化します。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。

  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

- 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。
- 新しいイメージの指定された設定を多数のスイッチにダウンロードするために、DHCP ベースの自動設定およびイメージをアップデート。
- スイッチ ポートに IP アドレスを前もって割り当てるための DHCP サーバ ポートをベースにしたアドレス割り当て。
- 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; 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ドロップするユニキャスト MAC アドレス フィルタリング。
- 設定可能な MAC アドレス スケーリング。これにより、VLAN で MAC アドレス ラーニングをディセーブルにし、MAC アドレス テーブルのサイズを制限することができます。
- Cisco Discovery Protocol（CDP）バージョン 1 および 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。
- リンク層検出プロトコル（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。
- スイッチからエンドポイント デバイスへロケーション情報を提供する LLDP メディア拡張（LLDP-MED）ロケーション TLV。
- サーバからのダイナミック ロケーションベースのコンテンツ配布のためのビデオ エンド ポイントとのロケーション情報を交換するための CDP および LLDP 拡張機能のサポート
- IPv4 および IPv6 対応の Network Time Protocol（NTP; ネットワーク タイム プロトコル）時間同期向けの NTP バージョン 4
- 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。
- SSM PIM プロトコル。マルチキャスト アプリケーション（ビデオなど）を最適化します。
- マルチキャスト アプリケーションに対する Source Specific Multicast（SSM）マッピング。グループへ送信元をマッピングしてリスナーをマルチキャスト ソースへ動的に接続させ、アプリケーションの依存性を軽減します。
- IPv6 トランスポートを利用し、IPv6 ピアと通信し、IPv6 ルートをアドバタイズするための Enhanced Interior Gateway Routing Protocol（EIGRPIP）v6 のサポート
- IP サービス（HSRP、ARP、SNMP、IP SLA、TFTP、FTP、Syslog、traceroute、ping）をサポート。これらのサービスを VRF 認識にすることで、複数のルーティング インスタンスで動作させます。
- 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。
- 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アクセス。
- IPv6 向け SSH のサポート。
- 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。IPv4 および IPv6 対応の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（ソフトウェアの暗号化バージョンが必要）。
- 設定の交換およびロールバックは、スイッチ上で一意の保存された Cisco IOS コンフィギュレーション ファイルで稼働している設定を交換します。
- Cisco IOS サポートの HTTP クライアントは、IPv4 と IPv6 の両方の HTTP サーバに要求を送信することができます。また、Cisco IOS の HTTP サーバは、IPv4 と IPv6 の両方の HTTP クライアントから、HTTP 要求にサービスを提供することができます。
- Simple Network and Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を IPv6 トランスポート経由で設定し、IPv6 ホストが SNMP クエリーを送信し、IPv6 を実行しているデバイスから SNMP 通知を受信できるようにすることができます。
- 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するための IPv6 ステートレス自動設定。
- VLAN の MAC アドレス ラーニングをディセーブルにします。
- スイッチ ポートに IP アドレスを前もって割り当てるための DHCP サーバ ポートをベースにしたアドレス割り当て。
- Cisco Mobility Services Engine（MSE; モビリティ サービス エンジン）に接続するデバイスにロケーションと接続トラッキング情報を送信するワイヤード ロケーション サービス。
- CPU の使用率をモニタする CPU 使用率しきい値トラップ。
- LLDP-MED ネットワーク ポリシー プロファイル Type-Length-Value（TLV）。VLAN、サービス クラス（CoS）、DiffServ コード ポイント（DSCP）、およびタギング モードの値を指定して、音声と音声信号のプロファイルを作成します。
- DHCPDISCOVER パケットの Option 12 フィールドにホスト名の入力をサポート。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、Option 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、スイッチで電力デバイス（PD）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。

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。
- Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）は、マルチアクセス リンク上の複数のルータで同じ仮想 IP アドレスを利用できるようにします。
- 拡張オブジェクト トラッキングは HSRP とトラッキング メカニズムを分離し、HSRP 以外のプロセスで使用可能な個別のスタンドアロン型トラッキング プロセスを作成します。

- 自動スタック マスターの再選択。使用できなくなったスタック マスターを置き換えます（フェールオーバー サポート）。

  新たに選択されたスタック マスターでは、1 秒未満でレイヤ 2 トラフィックを受信し始め、3 ～ 5 秒の間でレイヤ 3 トラフィックを受信し始めます。

- クロススタック EtherChannel。スイッチ スタック全体で冗長リンクのプロビジョニングを行います。
- 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。
  - 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 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変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することができます。
- Cisco Redundant Power System 2300（RPS 2300）を使用した RPS サポートによって、冗長電源システムの設定および管理をはじめ、電力の信頼性を向上させます。RPS 2300 の詳細については、デバイスに付属している『*Cisco Redundant Power System 2300 Hardware Installation Guide*』を参照してください。このマニュアルは、Cisco.com からも利用できます。

VLAN 機能

- 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 Trunking Protocol（VTP; VLAN トランキング プロトコル）および VTP プルーニング。トラフィックのフラッ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。
- 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。
- VLAN Flex Link ロード バランシング : Spanning Tree Protocol（STP; スパニングツリー プロトコル）を必要としないレイヤ 2 冗長性を提供。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。
- 制限付き VLAN（別名、*認証失敗 VLAN*）を使用した 802.1x 認証のサポート
- 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 機能をサポートしないサプリカント（クライアント）に Web ブラウザを使用して認証可能になります。
- ローカル Web 認証バナー。これにより、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ことができます。
- 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後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。
- 指定した入力割合を超えたパケットをドロップして、スイッチへの着信プロトコル トラフィックの割合を制御する、プロトコル ストーム プロテクション。
- 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/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。
- 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。
- 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 インスペクション。
- 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ぐリモート 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。
  - データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が、同じ IEEE 802.1x 対応スイッチ ポートにおいて、単独で認証できるようにする Multidomain Authentication（MDA; マルチドメイン認証）。
  - MDA のダイナミック音声 VLAN（仮想 LAN）。ダイナミック音声 VLAN が MDA 対応ポートで可能になります。
  - 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 割り当ては、1 つの IP 電話に対してサポートされます。
- ポート セキュリティ。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。802.1x に準拠はしているが、標準の 802.1x で認証するためのクレデンシャル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。
- 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。
- 802.1x と LAN の Wake-on-LAN（WoL）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。
- 802.1x 準備状態チェック。スイッチで 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。
- セキュリティ違反が発生した VLAN だけでトラフィック違反アクションを適用するための音声認識 802.1x セキュリティ。
- 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。
- 802.1X スイッチ サプリカントを持つ Network Edge Access Topology（NEAT）、CISP を使ったホスト認証、および自動イネーブル化。これらにより、別のスイッチへのサプリカントとして、配線クローゼットの外のスイッチが認証されます。
- 認証される前にネットワークへのアクセスをホストに許可するための、オープン アクセスを使用した IEEE 802.1x。
- ダウンロード可能な ACL とリダイレクト URL を使用した IEEE 802.1x 認証。Cisco Secure ACS サーバから認証されたスイッチへのユーザ単位の ACL ダウンロードを使用できるようになります。
- スタティック ACL が設定されていないポートでの認証デフォルト ACL のダイナミックな作成または接続のサポート。
- 新しいホストを認証するときに、ポートが思考する認証メソッドの順序を設定するための柔軟な認証シーケンス。
- マルチユーザ認証。複数のホストが、802.1x 対応ポートを認証できるようになります。

- 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*ポスチャ*に関する NAC レイヤ 2 802.1x 検証

    NAC レイヤ 2 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 802.1x 検証の設定」（P.10-71）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およびクリティカル音声 VLAN の設定」（P.10-66）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。

- TACACS+。IPv4 および IPv6 対応の 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。
- RADIUS。IPv4 および IPv6 の 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追跡します。
- IPv6 上での機能向けに、RADIUS、TACACS+、および SSH を拡張。
- 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（ソフトウェアの暗号化バージョンが必要）。
- 音声認識 IEEE 802.1X および MAB セキュリティ違反。セキュリティ違反が発生すると、ポートのデータ VLAN だけがシャットダウンされます。
- スタティック ホストでの IP ソース ガードのサポート。
- RADIUS Change of Authorization（CoA; 認証の変更）。特定のセッション認証された後で、その属性を変更します。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管理者は AAA サーバから、Cisco Secure ACS などの RADIUS CoA パケットを送信し、新しいポリシーに適用することができます。
- IEEE 802.1x User Distribution。さまざまな VLAN にわたってユーザをロード バランシングすることにより、（ユーザ グループに対して）複数の VLAN を使った配置で、ネットワークのスケーラビリティを向上させることができます。認証されたユーザは、RADIUS サーバにより割り当てられた、グループ内で最も空いている VLAN に割り当てられます。
- マルチ ホスト認証を使った、重要な VLAN のサポート。これにより、ポートがマルチ認証用に設定され、AAA サーバが到達不能になった場合でも、重要なリソースへのアクセスができるように、このポートが重要な VLAN に配置されます。
- クリティカル音声 VLAN のサポート。認証がイネーブルになっていて、アクセス コントロール サーバが使用できない場合、音声 VLAN でタグ付けされたホストからのトラフィックは、ポートに対して設定された音声 VLAN に配置されます。
- カスタマイズ可能な Web 認証機能強化。ローカル Web 認証で、ユーザ定義の *login*、*success*、*failure*、および *expire* Web ページの作成ができるようになります。
- ポート ホスト モードを変更し、オーセンティケータのスイッチ ポートに標準ポート設定を適用するために Network Edge Access Topology（NEAT）をサポート。
- 認証中のサプリカント ポートへのアクセスを制御する NEAT 機能拡張。
- VLAN-ID ベースの MAC 認証。ユーザ認証のために VLAN と MAC のアドレス情報を結合して、許可されていない VLAN からのネットワーク アクセスを阻止します。
- MAC 移動。モビリティのイネーブル化を制約することなく、ホスト（IP 電話の背後で接続されたホストを含む）が同じスイッチ内のポート間を移動できるようになります。MAC 移動では、もう 1 つのポートに同じ MAC アドレスが再登場した場合、スイッチはこれをまったく新しい MAC アドレスと同様に扱います。

- Simple Network Management Protocol バージョン 3（SNMPv3; 簡易ネットワーク管理プロトコル バージョン 3）を使った 3DES および AES のサポート。このリリースでは、168 ビット Triple Data Encryption Standard（3DES）と、SNMPv3 への 128 ビット、192 ビット、および 256 ビットの Advanced Encryption Standard（AES; 高度暗号化規格）暗号化アルゴリズムに対するサポートが追加されます。
- Cisco TrustSec の Security Group Tag（SGT）Exchange Protocol（SXP）コンポーネントのサポート。このコンポーネントは、認証、暗号化、およびアクセス コントロールを使用するセキュリティ アーキテクチャです。
- SXP バージョン 2、Cisco TrustSec Security Group Tag（SGT）Exchange Protocol（SxP）の Syslog メッセージおよび SNMP サポート。

  Cisco TrustSec の詳細については、次の URL にある『*Cisco TrustSec Switch Configuration Guide*』の「SGT Exchange Protocol over TCP (SXP)」の章を参照してください。
  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/sxp_config.html

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。
- ポートベースの信頼の自動 Quality of Service（QoS）VoIP 拡張と DSCP および出トラフィックのプライオリティ キューイング
- 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。
- 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スタック リングへ送出されるときのレートを決定するスケジューリング サービス（入力キューでサポートされる唯一のモードはシェアリング）。
- 出力キュー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はなく、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。
- IPv6 QoS trust 機能のサポート。
- 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 フローの自動設定分類を追加する自動 QoS 拡張機能。

レイヤ 3 機能

（注）　ここで取り上げる一部の機能は IP サービス イメージ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
  - 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、IP ベース フィーチャ セットで、OSPF for Routed Access がサポートされているので、お客様はレイヤ 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。
  - OSPFv2 の NSF IETF モード: IPv4 の OSPFv2 グレースフル リスタートのサポート（IP サービス フィーチャ セットのみ）
  - OSPFv3 の NSF IETF モード: IPv6 の OSPFv3 グレースフル リスタートのサポート（IP サービス フィーチャ セットのみ）
  - Enhanced Interior Gateway Routing Protocol（EIGRPIP）IPv6。IPv6 トランスポートを利用し、IPv6 ピアと通信し、IPv6 ルートをアドバタイズします。
  - IPv6 対応 HSRP（IP サービス イメージが必要）

  - 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（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
- 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。
- カスタマー エッジ デバイスの Multiple VPN Routing/Forwarding（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します（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。2 つ以上の VLAN 間で非 IP トラフィックを転送します（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 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 モードのサポートが含まれます（IP サービス イメージが必要）。
- Multicast Source Discovery Protocol（MSDP）による複数の PIM-SM ドメインの接続（IP サービス イメージが必要）
- Distance Vector Multicast Routing Protocol（DVMRP）トンネリングによる非マルチキャスト ネットワークでの 2 つのマルチキャスト対応ネットワークの相互接続（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
- IPv6 のリレー、クライアント、サーバ アドレス割り当て、プレフィックス委任に対応した DHCP
- 新しいバルク リース クエリー タイプ（RFC5460 で定義）をサポートする DHCPv6 バルクリース クエリー。
- DHCPv6 リレー エージェントの送信元アドレスを設定する DHCPv6 リレー送信元設定機能。
- 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 イメージが必要）。
- IPv6 Default Router Preference（DRP; デフォルト ルータの初期設定）。ホスト性能を改善することで、適切なルータを選択します。
- Nonstop Forwarding（NSF）認識。プライマリ ルート プロセッサ（RP）で障害が発生していて、バックアップ RP が引き継ぐ場合、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る場合、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）。
- OSPF および EIGRP の NSF 対応ルーティング。NSF 認識および NSF 対応ネイバーからの情報に基づいてスイッチがルーティング テーブルを再構築することができます。
- Switched Virtual Interface（SVI）ラインステートのアップまたはダウンの計算から VLAN 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
- IPv4 に対する Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）のサポート。マルチアクセス リンク上の複数のルータが同じ仮想 IP アドレスを使用できるようにして、1 台以上の仮想ルータの役割を LAN 上の VRRP ルータに動的に割り当てます。

Power over Ethernet の機能

- 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。
- 自動検出およびパワー バジェット。スイッチは、パワー 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。

モニタ機能

- EOT および IP SLA EOT スタティック ルートのサポート。事前に設定したスタティック ルートまたは DHCP ルートがダウンした場合に特定します。
- 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）。
- EEM 3.2 のサポート。ネイバー探索、ID、MAC アドレス テーブルのイベント検出器が導入されます。
- 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。
- 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。
- スマート ロギング。パケット フローを取り込み、NetFlow 収集装置にエクスポートします。このリリースでは、DHCP スヌーピングまたはダイナミック ARP インスペクション違反、IP ソースガード拒否トラフィック、および ACL のスマート ロギングがサポートされています。
- VACL ロギングは、ACL 拒否 IP パケットの Syslog メッセージを生成します。
- レイヤ 2 ポートで許可または拒否されるトラフィック。

- 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 トラッキング
- Digital Optical Monitoring（DOM; デジタル オプティカル モニタリング）。X2 SFP モジュールのステータスを確認します。
- 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。
- 組み込みのトラフィック シミュレータのサポート。Cisco IOS IP SLA ビデオ動作を使用して、Telepresence、IPTV、IP ビデオ サーベイランス カメラなど、さまざまなビデオ アプリケーションの合成トラフィックを生成します。次の目的のために、このシミュレータ ツールを使用できます。
  - ネットワーク パフォーマンス要件の厳しいアプリケーションを導入する前にネットワーク アセスメントを行うため。
  - 導入後のネットワーク関連のパフォーマンスの問題を Cisco Mediatrace と連携してトラブルシューティングするため。

このトラフィック シミュレータには、複数のテストを同時または定期的に、長期にわたって実行できる高性能なスケジューラが含まれています。詳細については、次の URL にある『*Configuring Cisco IOS IP SLAs Video Operations*』を参照してください。
http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/12-2se/Configuring_IP_SLAs_Video_Operations.html

- 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。
- Cisco Mediatrace とパフォーマンス モニタ
  - Cisco Mediatrace。トラフィック ストリーム内でのネットワークまたはアプリケーションに関する問題をトラブルシューティングし、特定します。ビデオ トラフィックを伝送する IPv4 ネットワークにおいて、一方向遅延、一方向パケット損失、一方向ジッタ、および接続性を詳しく分析するのに役立ちます。このツールは、UDP ベースのビデオまたはビデオ以外のトラフィック ストリームに使用できます。

    詳細については、次を参照してください。
    http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/15_1m_and_t/mm_15_1m_and_t.html
  - Cisco Application Performance Monitor。ビデオ パケット フローを追跡します。また、トラフィック ストリーム内でのパフォーマンスの低下をトラブルシューティングし、特定します。パフォーマンス モニタは、ビデオおよびビデオ以外のトラフィックに使用できます。

    詳細については、次を参照してください。
    http://www.cisco.com/en/US/docs/ios/media_monitoring/command/reference/mm_book.html

- Mediatrace とパフォーマンス モニタの設定時の注意事項：

  ビデオ モニタリングは、物理ポート上でのみサポートされます。EtherChannel 上ではサポートされません。

  スイッチで過剰なトラフィックが受信されると、パケットはドロップされます。

  このスイッチでは、入力ポート上でのみポリシー マップとポートベースの信頼性がサポートされます。

- Mediatrace とパフォーマンス モニタの制限：

  ビデオ モニタリングとルータまたは VLAN ACL を同じインターフェイス上に設定できません。
  ビデオ モニタリングを設定した後に ACL を設定すると、ACL 設定がビデオ モニタリング設定よりも優先され、メッセージが表示されます。
  ACL を設定した後にビデオ モニタリングを設定すると、それらのビデオ モニタリング コマンドはスイッチで拒否され、メッセージが表示されます。

  ビデオ モニタリング パケットは、ネットワーク キューを通過するので、ドロップされる可能性があります。

  スイッチでは、ソフトウェアで転送されるパケットに QoS 設定を適用できません。

  スイッチでは、消失またはドロップされたパケットを特定のトラフィックまたはデータ フローに照合できません。これらのパケットに関する情報については、入力と出力の QoS カウンタを参照してください。

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、スタートアップ ガイド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 インストレーション 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 22 章「DHCP および IP ソース ガード機能の設定」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 22 章「DHCP および IP ソース ガード機能の設定」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 9 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 9 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 9 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 10 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 12 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 12 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、イネーブルです。詳細については、第 12 章「インターフェイス特性の設定」を参照してください。
  - フロー制御はディセーブルに設定されています。詳細については、第 12 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 12 章「インターフェイス特性の設定」を参照してください。
- VLAN
  - デフォルト VLAN は VLAN 1 です。詳細については、第 13 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 13 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 13 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 14 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 14 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 16 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 15 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 17 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 18 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 19 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 20 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 21 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、ディセーブルです。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 22 章「DHCP および IP ソース ガード機能の設定」を参照してください。
- IP 送信元ガードはディセーブルです。詳細については、第 22 章「DHCP および IP ソース ガード機能の設定」を参照してください。
- DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。詳細については、第 22 章「DHCP および IP ソース ガード機能の設定」を参照してください。
- すべての VLAN 上でダイナミック ARP インスペクションがディセーブルになっています。詳細については、第 23 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です。IGMP のフィルタは適用されていません。詳細については、第 24 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。詳細については、第 24 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 24 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 24 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 25 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 25 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 25 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 25 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 26 章「CDP の設定」を参照してください。
- UDLD はディセーブルです。詳細については、第 28 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 29 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 30 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 31 章「システム メッセージ ロギングおよびスマート 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 32 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 34 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 はディセーブルです。詳細については、第 35 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 36 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 38 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。
- IPv6 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 39 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。
- HSRP グループは設定されていません。詳細については、第 42 章「HSRP および VRRP 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 46 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 47 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 48 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

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	• 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。
• 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	• 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

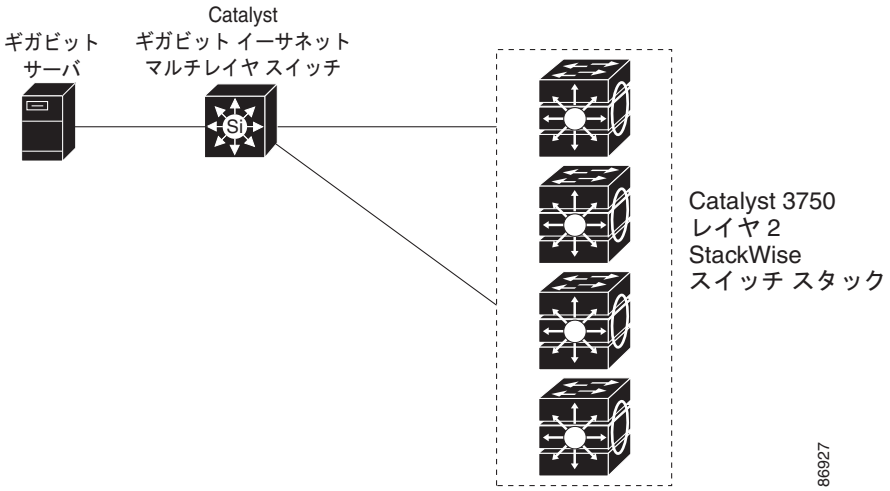
ネットワークに対する需要	推奨する設計方式
マルチメディア アプリケーションにおける帯域幅の効率的な利用およびミッション クリティカルなアプリケーションに対する帯域幅保証	• IGMP スヌーピングを利用して、マルチメディアおよびマルチキャスト トラフィックを効率的に転送します。 • パケット分類、マーキング、スケジューリング、輻輳回避など、他の QoS メカニズムを使用し、適切なプライオリティ レベルを指定してトラフィックを分類し、最大限の柔軟性を得ながら、ミッション クリティカルなユニキャスト、マルチキャスト、およびマルチメディア アプリケーションをサポートできるようにします。 • オプションの 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、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。
*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	• スタック マスターに障害が発生した場合に、すべてのスタック メンバが適格なスタック マスターである、スイッチ スタックを使用します。すべてのスタック メンバで、保存済みで実行中のスイッチ スタックの設定ファイルのコピーとの同期が取られます。 • クロススタック EtherChannel を使用して、スイッチ スタック全体で冗長リンクのプロビジョニングを行います。 • 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。 • 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	• 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。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。 • 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。
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	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。 **（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。

スイッチおよびスイッチ スタックを使用して、次のものを作成できます。

- 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 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。スタックにある 1 つのスイッチでスイッチの接続性を保つには、ハードウェア インストレーション ガイドで推奨されてい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 スタックにある SFP モジュールを使用すると、Catalyst 4500 ギガビット スイッチまたは Catalyst 3750-12S ギガビット スイッチなどの、ギガビット バックボーン スイッチへの冗長アップリンク接続を設定できます。ファスト イーサネット 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。ギガビット スイッチがクラスタ対応の場合、ギガビット スイッチとスイッチ スタックをスイッチ クラスタとして設定し、単一の IP アドレス経由で管理できます。ギガビット スイッチは、1000 BASE-T 接続経由でギガビット サーバに接続できます。

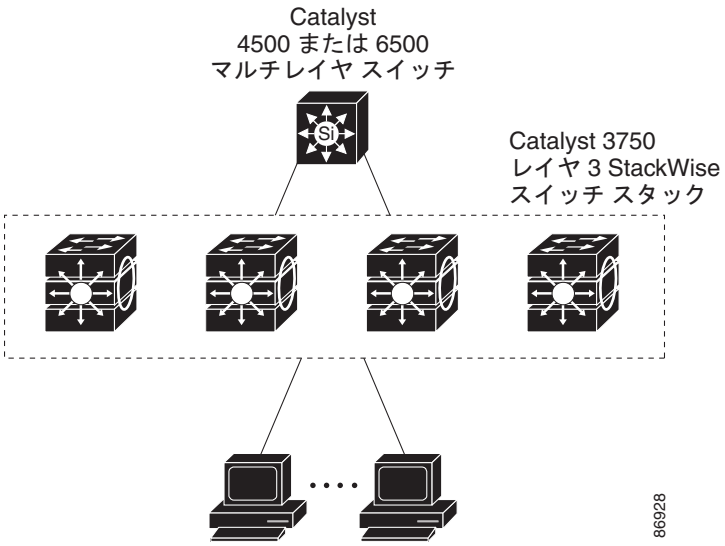
図 1-1　　費用対効果が高いワイヤリング クローゼット



- 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 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。

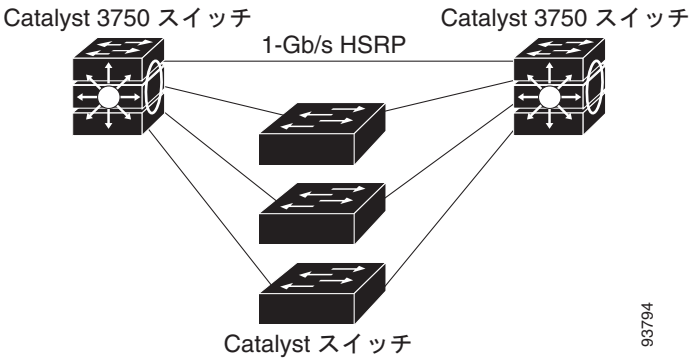
  この構成では、各スイッチはネットワーク リソースにアクセスするための、専用の 1 Gbps 接続をユーザに提供します。また、SFP モジュールを使用すると、光ファイバ接続におけるメディアおよび距離のオプションに柔軟性が提供されます。

図 1-2　高性能ワイヤリング クローゼット



- 冗長ギガビット バックボーン：HSRP によって、2 つの Catalyst 3750G マルチレイヤ 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 3750G 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、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 1-3　冗長ギガビット バックボーン



- サーバ集約（図 1-4）と Linux サーバ クラスタ（図 1-5）：スイッチとスイッチ 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。

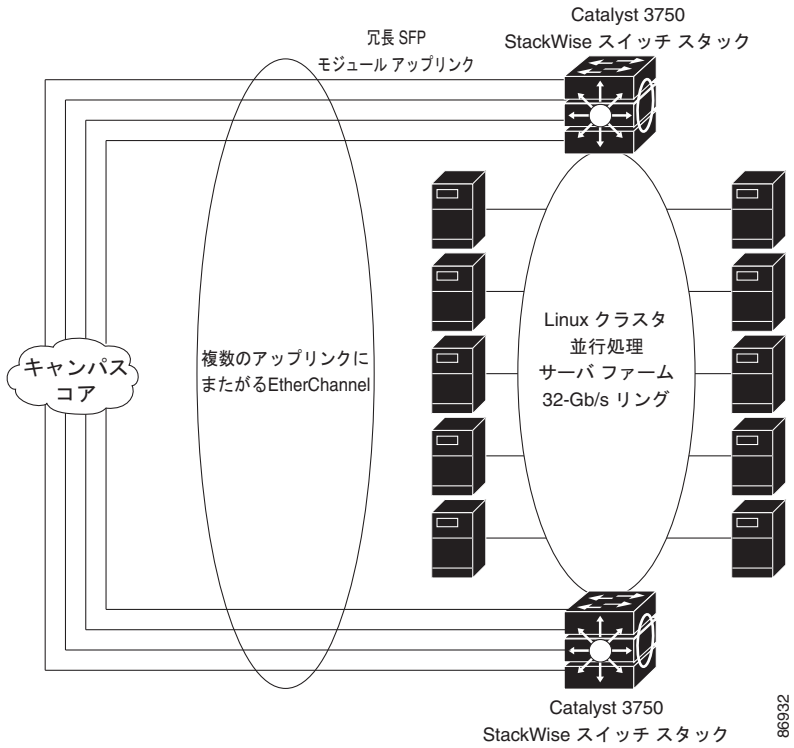
サーバ ラックからコアへの耐障害性は、冗長ギガビット EtherChannel とクロススタック EtherChannel を持つデュアル スイッチ スタックに接続されたサーバのデュアル ホーミングによって実現されます。

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。

0.5 メートルから 3 メートルまで、さまざまな長さのスタック ケーブルを使用できます。これによって、複数スタックを集約する目的で、複数サーバ ラック間でスイッチ スタックを拡張接続できます。

図 1-4　サーバ集約

図 1-5　Linux サーバ クラスタ



Catalyst 3750 スイッチを使用した中小規模のネットワーク

図 1-6 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 3750 レイヤ 3 スイッチ スタックを使用します。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 バランシングと冗長構成用に等コスト ルーティングが設定されています （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）の受電デバイス（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 スタックが VLAN 間ルーティングを行います。スタック上の VLAN アクセス コントロール リスト（VLAN マップ）により、VLAN 内セキュリティが提供され、不正ユーザがネットワークの重要な領域にアクセスできなくなります。

VLAN 間ルーティング以外に、マルチレイヤ スイッチまたはルータが 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。

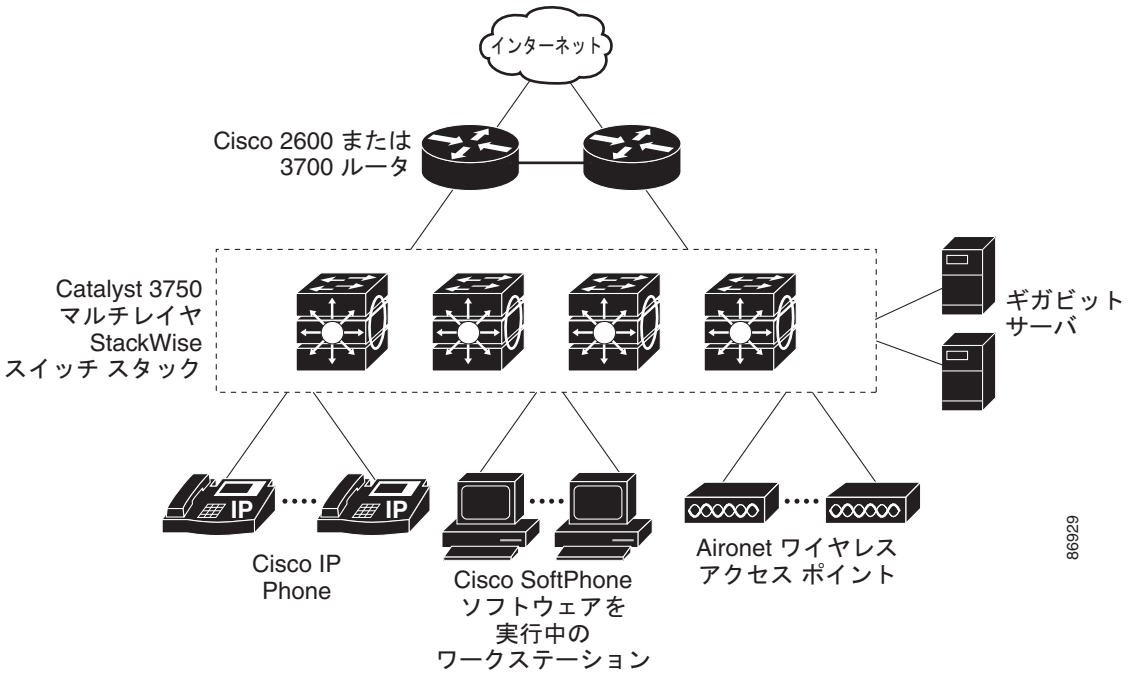
Catalyst PoE スイッチと接続している先行標準の受電デバイスおよび IEEE 802.3af 準拠の受電デバイスでは、IEEE 802.1p/Q QoS を使用することにより、音声トラフィックをデータ トラフィックよりも優先的に転送できます。

Catalyst PoE スイッチ ポートは、シスコの先行標準の受電デバイスおよび IEEE 802.3af 準拠の受電デバイス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。受電デバイス（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デバイスは、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。

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、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 1-6　　コラプスト バックボーン構成



Catalyst 3750 スイッチによる大規模ネットワーク

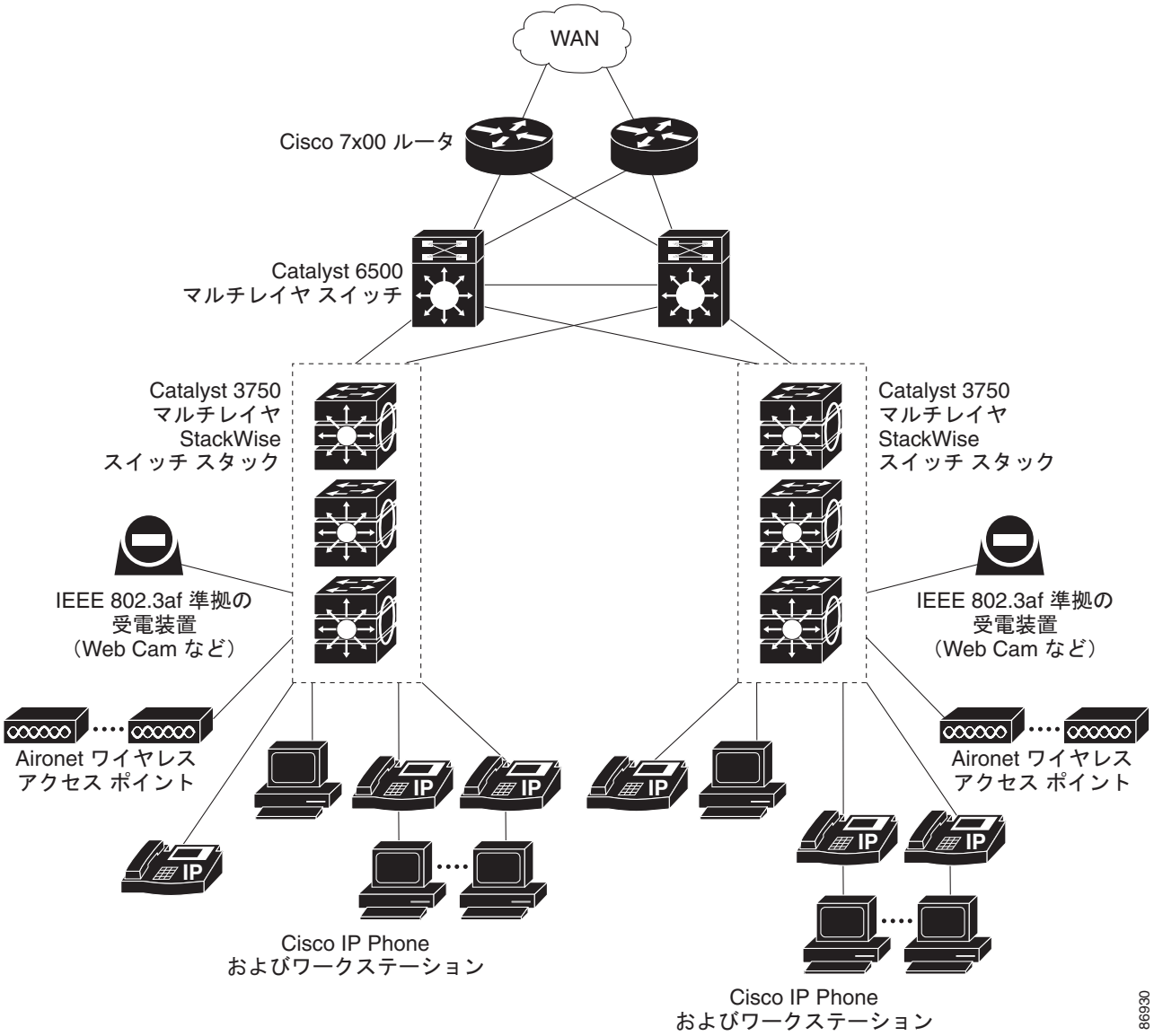
ワイヤリング クローゼット内のスイッチは、従来、レイヤ 2 デバイスだけでしたが、ネットワーク トラフィック プロファイルが拡大するにつれ、ワイヤリング クローゼット内のスイッチでマルチキャスト管理やトラフィック分類などのマルチレイヤ サービスがますます採用されつつあります。図 1-7 に、ワイヤリング クローゼットの Catalyst 3750 マルチレイヤ スイッチ スタックと、最大 10 のワイヤリング クローゼットを集約する 2 台のバックボーン スイッチ（Catalyst 6500 スイッチなど）だけを使用するネットワークの構成を示します。

ワイヤリング クローゼットの各スタックは、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、各スタック上で設定されます。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。

各スタックは、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、これらのスタックは各アップリンク 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 1-7　バックボーン構成でのワイヤリング クローゼットのスイッチ



Catalyst 3750 スイッチによる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 1-8 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 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 Catalyst 2950 LRE スイッチを使用できます。Catalyst 2900 LRE XL および 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 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 スイッチを使用した中小規模のネットワーク」（P.1-28）および「Catalyst 3750 スイッチによる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 1-8　MAN 構成の Catalyst 3750 スイッチ

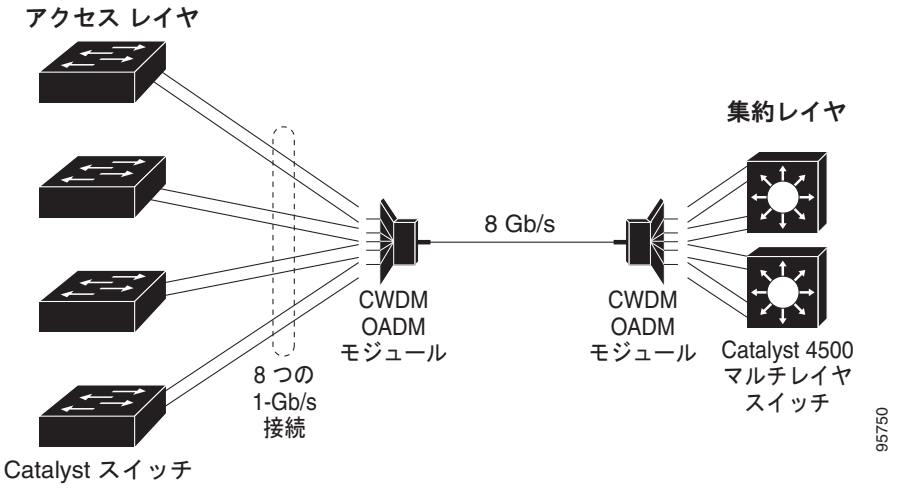
長距離広帯域トランスポートの構成

図 1-9 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 スイッチには、Coarse Wavelength-Division Multiplexing（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 1-9　　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」

特定のシスコ製品およびリリースに対する MIB の検索とダウンロードには、Cisco MIB Locator を使用します。
http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.