CHAPTER 1

概要

この章では、スイッチ ソフトウェアに関する次のトピックについて説明します。

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 スイッチとスイッチ 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、スタッキング対応スイッチのものです。コマンドライン インターフェイス（CLI）でコマンドを指定する場合、スタッキング対応スイッチでのインターフェイスは、たとえば *gigabitethernet 1/0/5* となります。

この例は、スタッキング非対応スイッチにも適用されます。前の例では、スタッキング非対応スイッチで指定するインターフェイスは、*gigabitethernet0/5*（スタック メンバーの *1/*はなし）となります。

機能

Catalyst Switch Module 3110 および Catalyst Switch Module 3012 は、暗号化（暗号化対応）または非暗号化のユニバーサル ソフトウェア イメージをサポートしています。Catalyst Switch Module 3110 は複数のフィーチャ セットをサポートしています。Catalyst Switch Module 3012 は IP ベース フィーチャ セットだけをサポートしています。

Catalyst Switch Module 3110 では、暗号化および非暗号化のユニバーサル ソフトウェア イメージによる IP ベースおよび IP サービスのフィーチャ セットをサポートしています。特定のフィーチャ セットをイネーブルにするには、対象のフィーチャ セットについての 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 Software Activation for IBM*』を参照してください。

Catalyst Switch Module 3012 を使用する場合はソフトウェア ライセンスは不要です。

この章で説明する機能のいくつかは、暗号化ソフトウェア イメージでだけ利用可能です。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。

- IP ベース フィーチャ セット：基本的なフィーチャ セットで、レイヤ 2+ フィーチャを提供します（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、Enhanced Interior Gateway Routing Protocol（EIGRP）スタブ ルーティング、ホットスタンバイ ルータ プロトコル（HSRP）、Routing Information Protocol（RIP）、および基本 IPv6 管理などがあります。IP ベース フィーチャ セットを備えたスイッチは、IP サービス フィーチャ セットにアップグレードできます。
- 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、Enhanced Interior Gateway Routing Protocol（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。

  IP サービスだけのレイヤ 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。

  詳細については、第 25 章「IPv6 MLD スヌーピングの設定」および第 36 章「IPv6 ACL の設定」を参照してください。

  IPv6 ルーティングの詳細については、第 40 章「IPv6 ホスト機能とユニキャスト 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 36 章「IPv6 ACL の設定」を参照してください。

（注） 特に注記がない限り、この章およびこのマニュアルで取り上げるすべての機能は、IP ベース フィーチャ セットおよび IP サービス フィーチャ セットの両方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.1-3）
- 「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.1-6）（暗号化ユニバーサル ソフトウェア イメージを必要とする機能を含む）
- 「アベイラビリティおよび冗長性に関する機能」（P.1-8）
- 「VLAN 機能」（P.1-9）
- 「セキュリティ機能」（P.1-10）（暗号化ユニバーサル ソフトウェア イメージを必要とする機能を含む）
- 「QoS および CoS 機能」（P.1-14）
- 「レイヤ 3 機能」（P.1-15）（IP サービス フィーチャ セットを必要とする機能を含む）
- 「モニタ機能」（P.1-17）

導入機能

スイッチには、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、および簡易ネットワーク管理プロトコル（SNMP）に関する情報を使用し、スイッチ スタックにだけ用意されている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。
- ローカル Web 認証バナー：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できます。
- 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（*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、スイッチおよびスイッチ スタックを簡単に、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）、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、ポート LED の色は実際の LED の色と同じです。
- スタッキング対応スイッチで使用する Cisco StackWise Plus テクノロジーの機能は、次のとおりです。
  - 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。
- スタックのトラブルシューティング機能の拡張
- 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

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 インターフェイス上の Automatic Medium-Dependent Interface Crossover（Auto-MDIX; 自動メディア 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 タイプの最大伝送単位（MTU）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（スイッチはポーズ フレームを送信しません）
- スイッチ スタックでは最大 64 Gbs 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 Gbs（ギガビット EtherChannel）または 80 Gbs（10 ギガビット EtherChannel）全二重の帯域幅を確保
- ポート集約プロトコル（PAgP）および Link Aggregation Control Protocol（LACP）により、EtherChannel リンクを自動的に作成
- 最大 64 の EtherChannel をサポート
- 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
- 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 のパケットをギガビット ラインレートで転送
- ポート単位のストーム制御。ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームを防止します。
- 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
- 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。

- 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
- 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 クエリア 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 ヘルパーにより、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。
- 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 レジストレーション）により、マルチキャスト VLAN 内でマルチキャスト ストリームを継続的に送信しながら、帯域幅およびセキュリティ上の理由から、加入者 VLAN からストリームを分離します。
- IGMP フィルタリングにより、スイッチ ポート上のホストが所属できるマルチキャスト グループセットを管理します。
- 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。
- ネットワーク終了の待ち時間を設定できる IGMP の Leave 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。
- 新しい Switch Database Management（SDM）デュアル IPv4/IPv6 テンプレートの導入。より多くの間接ルートをサポートします。
- Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）による、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、ローカルでのコンテンツ要求の実行、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を行います（IP サービス フィーチャ セットが稼働する Catalyst Switch Module 3110 に限る）
- Web Cache Communication Protocol（WCCP）リダイレクト リスト内での deny ACL エントリのサポート。それ以前は、permit エントリのみがサポートされていました。
- 設定可能なスモールフレーム着信しきい値により、スモール フレーム（64 バイト以下）が指定されたレート（しきい値）でインターフェイスに着信した場合のストーム制御を防止します。
- RADIUS サーバのロード バランシングにより、サーバ グループにおける認証要求の均等な配信が可能
- ダイナミックなロケーションベースのコンテンツをサーバから配信するために、ビデオ エンド ポイントとの間でロケーション情報を交換する CDP および LLDP 拡張機能です。

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、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 33 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。
- Advanced Management Module（AMM）GUI : スイッチの内部イーサネット管理ポート（*Fa0 または fastethernet0 ポート*とも呼ばれます）が、スイッチと AMM との間で管理トラフィックだけを送受信します。ポートはバックプレーン コネクタを通じて AMM と接続します。

管理の簡易性に関する機能

次に、管理の容易さ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。
- 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。
- 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。
- スイッチからエンドポイント デバイスにロケーション情報を提供する LLDP-MED ロケーション TLV のサポート。
- ロケーションに基づいてサーバからダイナミックにコンテンツを配布するために、ビデオ エンドポイントとの間でロケーション情報を交換する CDP および LLDP 拡張。
- ネットワーク タイム プロトコル（NTP）により、外部ソースから全スイッチに一貫したタイムスタンプを提供します。
- IPv4 と IPv6 の両方をサポートし、NTPv3 と互換性のある Network Time Protocol version 4（NTPv4）。
- 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。
- 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。
- 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 つの暗号化された同時 Secure Shell（SSH; セキュア シェル）接続によるインバンド管理アクセス（スイッチ ソフトウェア 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。
- スイッチ コンフィギュレーション ファイルまたはスイッチ イメージ ファイルをコピーするためのセキュアで認証された方法を提供する Secure Copy Protocol（SCP）機能（暗号化ユニバーサル ソフトウェア イメージが必要）
- 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
- LLDP-MED ネットワークポリシー プロファイル時間、長さ、値（TLV）。これにより、VLAN、サービス クラス（CoS）、DiffServ コード ポイント（DSCP）の各値、および CPU 使用率をモニタリングするタギング モードの CPU 使用率しきい値トラップを指定して音声と音声信号のプロファイルを作成できます。
- Cisco IOS の HTTP クライアントは IPv4 および IPv6 の両 HTTP サーバに要求を送信でき、Cisco IOS の HTTP サーバは IPv4 および IPv6 の両 HTTP クライアントからの HTTP 要求を処理できます。

- SNMP を IPv6 転送上で設定できるため、IPv6 ホストは SNMP クエリーを送信でき、IPv6 を実行するデバイスから SNMP 通知を受信できます。
- IPv6 がサポートするステートレス自動設定により、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ことができます。
- 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。これにより、DHCP プロトコルを使用して同一のコンフィギュレーション ファイルを複数送信できます。
- DHCP スヌーピング拡張機能。これにより、Option 82 DHCP フィールドで指定する回線 ID サブオプションに、固定文字列ベースのフォーマットを選択できるようになります。
- Cisco EnergyWise により、power over Ethernet（PoE）デバイスなどの EnergyWise エンティティおよびデーモンが動作するエンド ポイントの電力消費量を管理します。

（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.1-22）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

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。
- （フェールオーバー サポート）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（Catalyst Switch Module だけ）

  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。
- 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 Switch Module 3110 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 Switch Module 3110 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 アップリンクを含む冗長アップリンク間でのロード バランシングの実行（Catalyst Switch Module 3110 だけ）
- 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 高速スパニングツリー プロトコル（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できます。
- VTP バージョン 3 のサポート。具体的には、任意の VTP モードによる拡張範囲 VLAN（VLAN 1006 ～ 4094）設定のサポート、認証の拡張機能（非表示パスワードまたはシークレット パスワード）、VTP に加えて他のデータベースの伝播、VTP プライマリ サーバおよびセカンダリ サーバ、VTP のポートによるオン / オフの切り替えオプションがあります。

VLAN 機能

次に、VLAN に関する機能を示します。

- 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 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。
- 2 つのデバイス間のライン上で、トランキングとカプセル化のネゴシエーションを行う Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）
- 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。
- Multidomain authentication（MDA）対応ポート上のダイナミック音声仮想 LAN（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。

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 機能をサポートしていないサプリカント（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 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 アクセス コントロール リスト（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。
- 設定済みのスタティック ACL を持たないポート上で、auth-default ACL のダイナミックな作成または添付をサポート。
- ACL で拒否された IP パケットに関する Syslog メッセージを生成する VACL ロギング。
- 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。
- 柔軟な認証シーケンス機能。新規ホストの認証時にポートが試みる認証方式の順序を設定します。
- オープン アクセス対応 IEEE 802.1x により、ホストは認証される前にネットワークにアクセスできます。
- 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）。
  - 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 電話について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。
  - 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。
  - 802.1x サプリカント スイッチを持つ Network Edge Access Topology（NEAT）。Client Information Signalling Protocol（CISP）を使用してホスト認証を行い、ワイヤリング クローゼット外部のスイッチを別のスイッチに対するサプリカントとしての認証を自動的にイネーブルにします。

  - IEEE 802.1x 認証機能。ACL のダウンロードおよび URL のリダイレクトが可能で、これによって Cisco Secure ACS サーバから認証対象のスイッチにユーザ単位で ACL をダウンロードできます。
  - 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。
- 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。
- 「NAC レイヤ 2 802.1x 検証の設定」（P.9-58）ネットワーク アドミッション コントロール（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 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 2 802.1x 検証の設定」（P.9-58）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.9-53）を参照してください。
  - 認証、許可、アカウンティング（AAA）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。
- RADIUS により、AAA サービスを使用して、リモートユーザの ID の検証、アクセスの許可、アクションのトラッキングを実行
- 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 システムにより、信頼できるサード パーティを使用して、ネットワーク リソースへの要求を認証（暗号化ユニバーサル ソフトウェア イメージが必要）
- Secure Socket Layer（SSL）バージョン 3.0 では、HTTP 1.1 サーバ認証、暗号化、メッセージ整合性をサポート。HTTP クライアント認証によりセキュア HTTP 通信が可能（暗号化ソフトウェア イメージが必要）
- 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、ポートが複数認証用に設定され、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。

- 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。
- 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。

QoS および CoS 機能

次に、QoS および CoS 機能を示します。

- 自動 QoS（auto-QoS）。トラフィックの分類と出力キューの設定を自動化することで既存の 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 Switch Module 3110 だけ）
- 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。
  - シェイプド ラウンドロビン（SRR）。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。
- 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 Quality of Service（QoS）Voice over IP（VoIP）拡張機能
- IPv6 トラフィックの完全な QoS 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 フローに対する自動設定分類を追加する自動 QoS 拡張です。

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 フィーチャ セットにだけ対応しています。

- 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）
- IPv6 用の HSRP（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）。
- 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 サポート（IP サービス フィーチャ セットが動作する Catalyst Switch Module 3110 だけ）

    IP Base イメージでは、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。
  - IPv6 用 HSRP（IP サービス フィーチャ セットが動作する Catalyst Switch Module 3110 だけ）
  - Enhanced IGRP（EIGRP）（IP サービス フィーチャ セットが動作する Catalyst Switch Module 3110 だけ）
  - 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 フィーチャ セットが動作する Catalyst Switch Module 3110 だけ）
- 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（Catalyst Switch Module 3110 だけ）
- カスタマー エッジ（CE）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バーチャル プライベート ネットワーク（VPN）をサポートし、VPN 間で IP アドレスを重複できるようにする（IP サービス フィーチャ セットが動作する Catalyst Switch Module 3110 だけ）

- 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（Catalyst Switch Module 3110 だけ）
- 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 セットが動作する Catalyst Switch Module 3110 だけ）
- 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 スパース モード（PIM-SM）、PIM デンス モード（PIM-DM）、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 セットが動作する Catalyst Switch Module 3110 だけ）
- Multicast Source Discovery Protocol（MSDP）。複数の PIM-SM ドメインを接続します（IP サービス フィーチャ セットが動作する Catalyst Switch Module 3110 だけ）
- Distance Vector Multicast Routing Protocol（DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル）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 セットが動作する Catalyst Switch Module 3110 だけ）
- 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 IPv6 ユニキャスト ルーティング機能（拡張 IP サービス フィーチャ セットが必要）
- 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。
- IPv6 ユニキャスト ホスト管理
- 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 セットが動作する Catalyst Switch Module 3110 だけ）
- 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できます（Catalyst Switch Module 3110 だけ）
- 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 Reverse Path Forwarding（ユニキャスト RPF）（Catalyst Switch Module 3110 だけ）

- Nonstop Forwarding（NSF）認識。プライマリ ルート プロセッサ（RP）が障害を起こしていて、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 セットが動作する Catalyst Switch Module 3110 だけ）
- 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 Switch Module 3110 だけ）
- OSPFv2 用の NSF IETF モード : IPv4 に対する 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 セット専用）
- OSPFv3 用の NSF IETF モード **:** IPv6 に対する 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 セット専用）
- 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。Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）ネットワーク向けのダイナミック プロトコルをサポートします（IP サービス フィーチャ セットが動作する Catalyst Switch Module 3110 だけ）
- IPv4 に対する Virtual Router Redundancy Protocol（VRRP）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。

モニタ機能

次に、モニタリング機能を示します。

- Catalyst Switch Module 3012 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 Switch Module 3110 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でのステータス確認
- 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 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。
- 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、スイッチのハードウェア機能をテストするオンライン診断。

- 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。
- Digital Optical Monitoring（DOM; デジタル オプティカル モニタリング）。X2 Small Form-Factor Pluggable（SFP）モジュールのステータスを確認します。
- 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 テーブルの状態をトラッキングすることで 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（Catalyst Switch Module 3110 だけ）。
- 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。
- Cisco IOS デバイス内のイベント検出と回復のための Embedded Event Manager（EEM）と、ネイバー探索、アイデンティティ、MAC-Address-Table 用のイベント ディテクタを導入する EEM 3.2 のサポート。
- メモリ整合性検査ルーチン拡張機能。スイッチのパフォーマンスに影響を与える可能性のある無効な Ternary Content Addressable Memory（TCAM）テーブル エントリを検出し、修正します。
- IP version 6（IPv6）専用オブジェクトとテーブル、および Protocol-Version Independent（PVI）オブジェクトとテーブルの IPv6 部分をサポートする IETF IP-MIB および IP-FORWARD-MIB（RFC4292 および RFC4293）アップデート。

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 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 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 7 章「スイッチ スタックの管理」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 5 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 5 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 5 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 5 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 6 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 6 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 6 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 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。詳細については、第 11 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 11 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 11 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 11 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、第 12 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 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 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 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 機能および IP ソースガードの設定」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 26 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 26 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 26 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 26 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 はディセーブルです。詳細については、第 29 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 30 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 31 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 32 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 33 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 35 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 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 38 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 39 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 41 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（Catalyst Switch Module 3110 に限定）。詳細については、第 45 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（Catalyst Switch Module 3110 に限定）。詳細については、第 46 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（Catalyst Switch Module 3110 に限定）。詳細については、第 47 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

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。

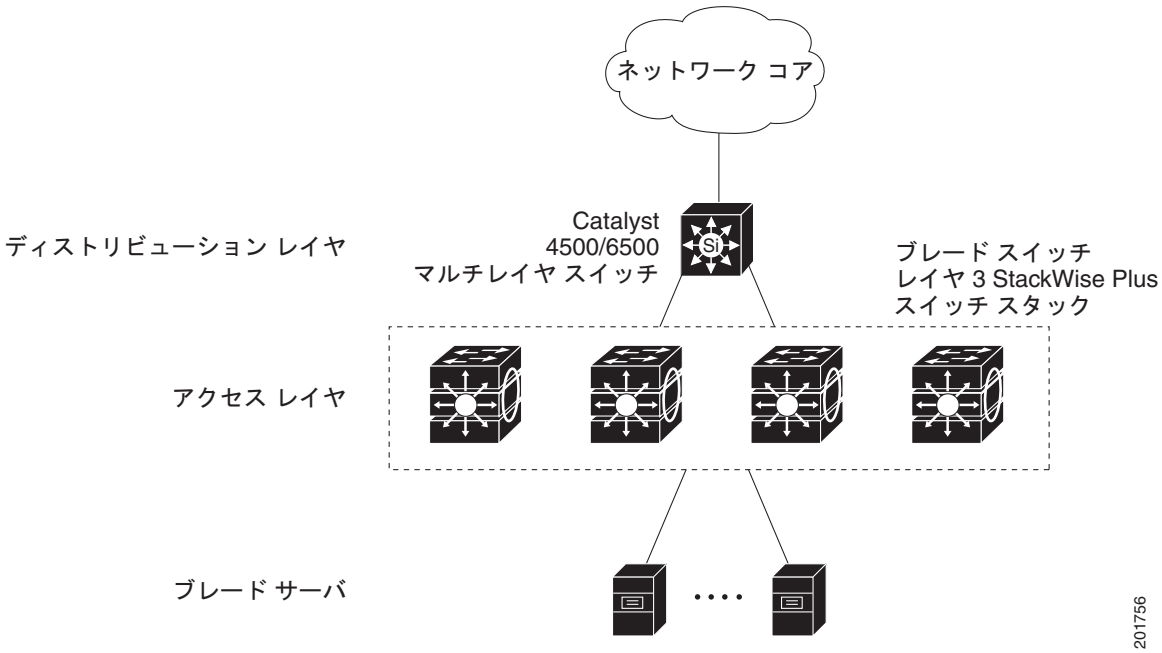
表 1-2　ネットワーク サービスの提供

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。 • ホットスタンバイ ルータ プロトコル（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 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。

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。

- データセンター（図 1-1）：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 レイヤでスイッチとスイッチ スタックを使用すると、ブレード サーバへのギガビット イーサネット アクセスを提供できます。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。

図 1-1　　データセンター



- 拡張データセンター（図 1-2）：スタンドアロンのスイッチおよびスイッチ スタックを使用してサーバ グループを相互に接続し、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。

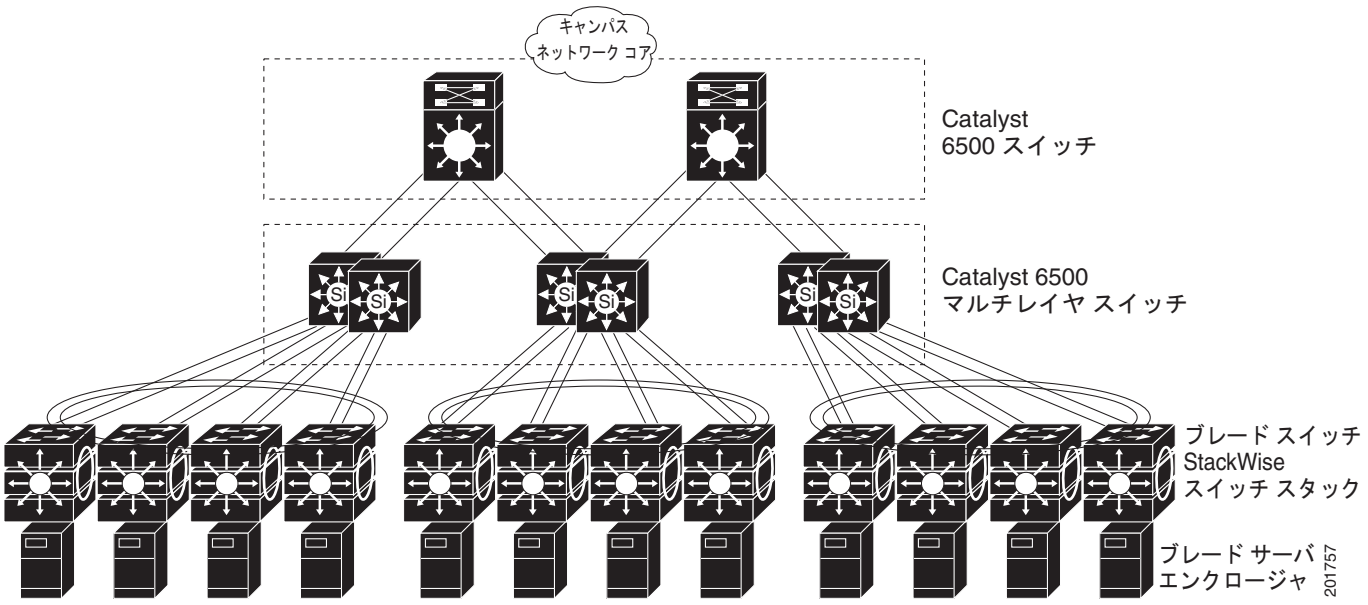
  スイッチ上の QoS およびポリシングによって、特定のデータ ストリームが優先的に処理されます。トラフィック ストリームはいくつかの経路に分けられて処理されます。スイッチのセキュリティ機能によって、パケットの高速処理が保証されます。

  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 10 ギガビット イーサネット 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。

  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 1-2　拡張データセンター



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、レイヤ 3 スイッチ スタックを使用し、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 シェアリングにクロススタック EtherChannel を使用できます。

スイッチには、ローカル サーバが接続されます。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。Cisco CallManager は、コール処理およびルーティングを制御します。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。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。

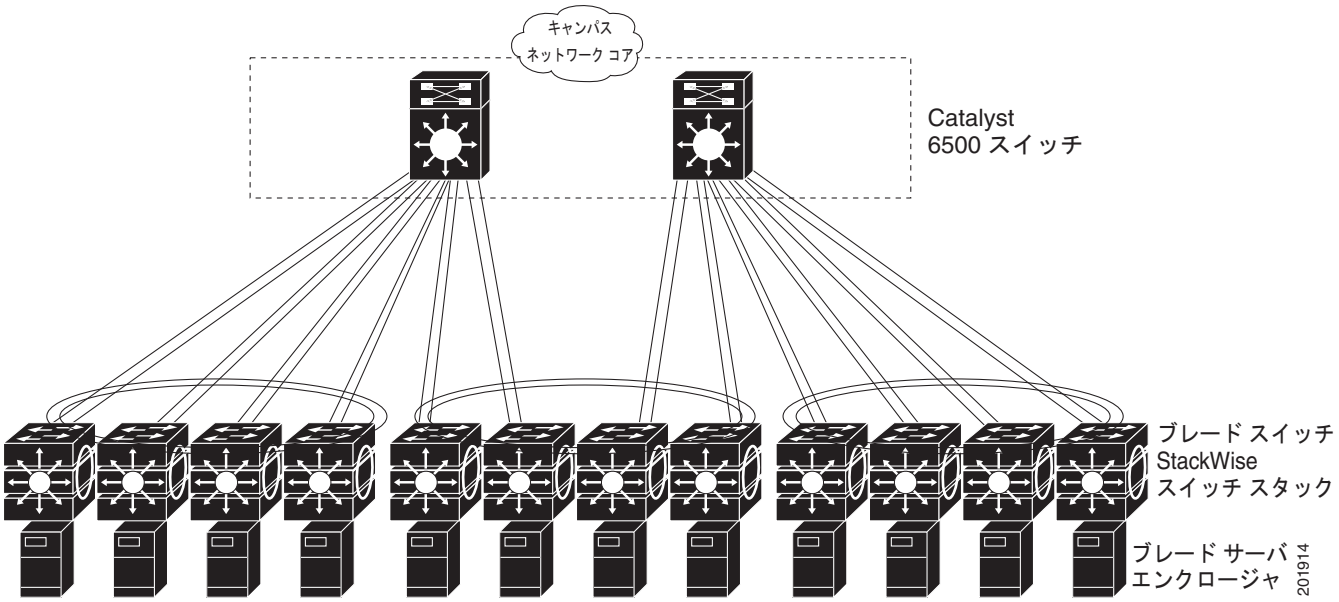
ある VLAN のエンド ステーションが別の VLAN にあるエンド ステーションと通信する必要がある場合、ルータ、またはレイヤ 3 スイッチが宛先 VLAN にトラフィックをルーティングします。このネットワークでは、スイッチ スタックが VLAN 間ルーティングを行います。スイッチ スタック上の VLAN ACL（VLAN マップ）が VLAN 内セキュリティを設定し、不正ユーザがネットワークの重要な領域にアクセスしないようにします。

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、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。

Cisco CallManager は、コール処理およびルーティングを制御します。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 CallManager 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の両方をサポートします。

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 1-3　縮小バックボーンのスイッチ スタック



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.