CHAPTER 1

概要

この章では、Catalyst 2960 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。

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

この章で取り上げる一部の機能は、ソフトウェア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）だけに対応しています。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。

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、『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：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*）：
  - 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 クラスタを簡単に最小限の手間で管理できます。
  - 単一のグラフィカルなインターフェイスから複数の設定作業を行うことができます。特定の作業を実行するための command-line interface（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、Quality of Service（QoS; サービス品質）などの複雑な機能をガイドに従って設定できます。

  （注）　スイッチで LAN ライト イメージが稼動している場合、ACL を設定できますが、ACL をインターフェイスや VLAN には適用できません。

  - 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、コンポーネントおよび統計レポート、リンクおよびスイッチ レベルでのモニタリング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。

  （注）　RPS を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

（注）　Network Assistant は、cisco.com/go/cna からダウンロードする必要があります。

- スイッチのクラスタ化テクノロジー：
  - イーサネット、ファスト イーサネット、Fast EtherChannel、Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュール、ギガビット イーサネット、Gigabit EtherChannel 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、モニタリング、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。
- ポート上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ための Cisco のデフォルトおよびユーザ定義の自動 Smartport マクロ

パフォーマンス向上機能

- Power over Ethernet（PoE）エンティティのエネルギー使用状況を管理する Cisco EnergyWise
- 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で、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、接続を適切に設定することが可能になる Automatic-medium-dependent interface crossover（Auto-MDIX）機能
- ハードウェアでの最大 9000 バイトまでのフレームのブリッジング、ソフトウェアでの最大 2000 バイトまでのフレームのブリッジングのサポート
- すべてのポート上での 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）
- 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
- EtherChannel リンクを自動的に作成するための Port Aggregation Protocol（PAgP; ポート集約プロトコル）と Link Aggregation Control Protocol（LACP）
- ギガビット回線レートでのレイヤ 2 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、およびブリッジされたブロードキャスト トラフィックの転送に対するポート ブロッキング
- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング。IGMP バージョン 1、2、および 3 に対応し、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できます。
- 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にスイッチを設定します。
- 基本的な IPv6 管理のための IPv6 ホスト サポート
- スイッチド ネットワーク内のクライアントとルータに IP version 6（IPv6）マルチキャスト データを効率良く配信できるようになる Multicast Listener Discovery（MLD）スヌーピング

（注）　IPv6 機能を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

- 帯域幅とセキュリティ上の理由からマルチキャスト ストリームを加入者 VLAN から分離したまま、マルチキャスト VLAN 内のマルチキャスト ストリームを継続的に送信する Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）

（注）　MVR を使用するには、スイッチで LAN ベース イメージを稼動している必要があります。

- 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 グループのセットを制御するための IGMP フィルタリング
- 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。
- システムに Cisco IOS IP Service Level Aggreements（SLA; サービス レベル契約）要求パケットを予想して応答させることができる Cisco IOS IP SLA 応答側のサポート。応答側の設定については、リリース ノートを参照してください。
- 設定可能なスモール フレーム着信しきい値。スモール フレーム（64 バイト以下）が指定のレート（しきい値）でインターフェイスに着信すると、ストーム制御を防止します。
- Flex Link マルチキャスト高速コンバージェンス。Flex Link が失敗したあとのマルチキャスト トラフィック コンバージェンスの時間を短縮します。

（注）　Flex Link マルチキャスト高速コンバージェンスを使用するには、スイッチで LAN ベース イメージを実行している必要があります。

- アクセス要求と認証要求がサーバ グループ内で均等に配信されるようになる RADIUS サーバ ロード バランシング

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、『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動している 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 29 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）: ネットワーク デバイスとサービスの配置と管理を自動化するコンフィギュレーション サービスです。スイッチごとに設定変更の内容を生成してスイッチに送信し、その設定変更を適用したあと、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 5 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
- 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 サーバ名など）の自動設定
- DHCP リレーによる DHCP クライアントからの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）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
- 特定の設定や新しいイメージを多数のスイッチにダウンロードできる DHCP ベースの自動設定およびイメージ アップデート
- 事前に IP アドレスをスイッチ ポートへ割り当てることができる DHCP サーバのポートベースのアドレス割り当て
- IP アドレスおよび対応するホスト名からスイッチを特定することを目的とした、ユニキャスト要求の DNS サーバへの転送、および TFTP サーバからソフトウェア アップグレードを管理することを目的とした、ユニキャスト要求の TFTP サーバへの転送
- Address Resolution Protocol（ARP; 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
- VLAN での MAC アドレス ラーニングをディセーブルにして、MAC アドレス テーブルのサイズを制限することができる設定可能な MAC アドレス スケーリング
- Cisco Discovery Protocol（CDP; シスコ検出プロトコル）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
- 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

（注）　LLDP-MED を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

- Network Time Protocol（NTP; ネットワーク タイム プロトコル）。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。
- 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（EIGRP）IPv6 のサポート
- IP サービス（HSRP、GLBP、uRPF、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 Navigator または Microsoft Internet Explorer ブラウザ セッションでデバイス マネージャを使用した帯域内管理アクセス
- 最大 16 の Telnet 接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベース セッションを実行できます。
- 最大 5 つの暗号化 Secure Shell（SSH; セキュア シェル）接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベース セッションを実行できます（ソフトウェア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。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）。
- スイッチ上の実行コンフィギュレーションを任意の保存された Cisco IOS コンフィギュレーション ファイルと置き換えるコンフィギュレーション交換およびロールバック
- Cisco IOS の HTTP クライアント サポート。HTTP クライアントが IPv4 HTTP サーバおよび IPv6 HTTP サーバの両方へ要求を送信でき、Cisco IOS の HTTP サーバは同様に両方からの HTTP 要求をサービスできます。
- 簡易ネットワーク管理プロトコル（SNMP）。IPv6 ホストで、SNMP クエリーの送信と、IPv6 を実行しているデバイスからの SNMP 通知の受信ができるように、IPv6 トランスポートで設定できます。
- IPv6 のステートレス自動設定。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。
- VLAN での MAC アドレス ラーニングのディセーブル化
- 事前に IP アドレスをスイッチ ポートへ割り当てることができる DHCP サーバのポートベースのアドレス割り当て
- 接続デバイスのロケーションと接続のトラッキング情報を Cisco Mobility Services Engine（MSE）に送信する有線ロケーション サービス
- CPU 利用率をモニタする CPU 利用率しきい値トラップ
- VLAN、Class of Service（CoS; サービス クラス）、Differentiated Services Code Point（DSCP）、およびタギング モードの値を指定することにより、音声のプロファイルを作成し、音声信号を送信するための LLDP-MED ネットワークポリシー プロファイル time、length、value（TLV）

アベイラビリティおよび冗長性に関する機能

- 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

  （注）　スイッチが LAN Lite イメージを実行中の場合、最大 64 のスパニング ツリー インスタンスがサポートされます。

  - Per-VLAN Spanning-Tree Plus（PVST+）による VLAN 間でのロード バランシング
- Rapid PVST+ による、VLAN 間でのロード バランシングおよびスパニング ツリー インスタンスの高速コンバージェンスの実現
  - UplinkFast および BackboneFast によって、スパニング ツリー トポロジ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
  - 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。
- 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。

（注）　Flex Link を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

- 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。

（注）　リンク ステート トラッキングを使用するには、スイッチで LAN ベース イメージを実行している必要があります。

VLAN 機能

- 最大 255 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。

（注）　スイッチが LAN Lite イメージを実行中の場合、最大 64 の VLAN がサポートされます。

- IEEE 802.1Q 規格で認められている 1 ～ 4094 の範囲で VLAN ID をサポート
- ダイナミック VLAN メンバシップに対応する VLAN Query Protocol（VQP）
- すべてのポート上で稼動する 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）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。
- VLAN Flex Link ロード バランシング。スパニング ツリー プロトコル（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。

（注）　VLAN Flex Link ロード バランシングを使用するには、スイッチで LAN ベース イメージを実行している必要があります。

- すべてのスイッチ イメージでの制限付き VLAN（*認証失敗 VLAN* とも呼ばれます）の 802.1X 認証のサポート

セキュリティ機能

- IP Service Level Agreements（IP SLA; IP サービス レベル契約）応答側のサポート。スイッチを IP SLA アクティブ トラフィック モニタリングのターゲット デバイスにできます。

（注）　IP SLA 機能を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

- 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。

（注）　Web 認証を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

- ローカル Web 認証バナー。カスタム バナーやイメージ ファイルを Web 認証ログイン画面で表示できます。
- ACL および RADIUS の Filter-ID アトリビュートによる IEEE 802.1X 認証

（注）　この機能を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

- 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 Access Control List（ACL; 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（ポート ACL）の着信セキュリティ 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。
- 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
- 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 データベースと送信元 IP の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 インターフェイス上のトラフィックを制限する IP ソースガード
- 無効な ARP 要求と応答を同じ VLAN 内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防ぐダイナミック ARP インスペクション

- 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。

（注）　MDA を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

  - MDA のダイナミック音声 VLAN。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。
  - 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。

（注）　制限付き VLAN による認証を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

  - 802.1X アカウンティング。ネットワーク使用状況をトラッキングします。
  - 特定のイーサネット フレームの受信に基づいて休止状態の PC を起動できる Wake-on-LAN による 802.1X

（注）　Wake-on-LAN による認証を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

  - 802.1X の準備チェック機能。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。

（注）　802.1X の準備チェック機能を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

  - 音声認識 802.1X セキュリティ。セキュリティ違反が発生した VLAN 上でだけトラフィック違反に反応します。

（注）　音声認識 802.1X 認証を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

- 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。

（注）　MAC 認証バイパスを使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

- デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウィルス対策の状態または*ポスチャ*に関する Network Admission Control（NAC; ネットワーク アドミッション制御）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.9-58）を参照してください。

（注）　NAC を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

- 802.1X スイッチ サプリカントによる Network Edge Access Topology（NEAT）、CISP によるホスト認証、およびワイヤリング クローゼット外のスイッチを他のスイッチのサプリカントとして認証する自動イネーブル化
- 認証前のホストがネットワークにアクセスできるオープン アクセスによる IEEE 802.1X
- Cisco Secure ACS サーバから認証済みスイッチへユーザ単位 ACL ダウンロードができる、ダウンロード可能な ACL とリダイレクト URL による IEEE 802.1X 認証
- 新しいホストの認証時にポートで実行される認証方式の順序を設定する柔軟な認証シーケンス
- 複数のホストを 1 つの 802.1X 対応ポート上で認証できる複数ユーザ認証

- 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。Authentication、Authorization、Accounting（AAA; 認証、許可、アカウンティング）サービスによってリモート ユーザの身元を確認し、リモート ユーザにアクセス権を与え、リモート ユーザのアクションをトラッキングします。
- 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）。
- ACL および RADIUS の Filter-ID アトリビュートによる IEEE 802.1X 認証

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。

（注）　自動 QoS を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

- 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。

（注）　DSCP を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

  - IP ToS/DSCP および IEEE 802.1p CoS 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 エッジで高性能なサービス品質を提供し、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。

（注）　フローベースのパケット分類を使用するには、スイッチで LAN ベース イメージを稼動している必要があります。

  - 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

（注）　ポリシー マップを使用するには、スイッチで LAN ベース イメージを稼動している必要があります。

  - 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 マップに複数のクラス マップを設定する場合、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。

（注）　WTD を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

  - スケジューリング サービスとしての Shaped Round Robin（SRR; シェイプド ラウンド ロビン）。パケットが内部リングへ送信されるレートを指定します（共有が入力キューでサポートされる唯一のモード）。

（注）　入力キューを使用するには、スイッチで LAN ベース イメージを稼動している必要があります。

- 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。パケットがキューから取り出されて出力インターフェイスに送信されるレートを指定します（出力キューではシェーピングまたは共有をサポート）。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。

（注）　出力キューを使用するには、スイッチで LAN ベース イメージを稼動している必要があります。

レイヤ 3 機能

- IPv6 Default Router Preference（DRP）。ホストの機能を改善して、適切なルータを選択します（LAN ベース イメージが必要です）。

Power over Ethernet 機能

- 回路上に電力が供給されていないことをスイッチが検出した場合、Power over Ethernet（PoE）対応ポートから、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 バジェット。スイッチはパワー バジェットを維持し、電力要求をモニタおよびトラッキングし、利用できる場合にだけ電力を供給します。
- 電力消費量をリアルタイムにモニタできます。PoE ポート ベースごとに、スイッチは総電力消費量の感知、電力使用量の管理、および電力使用量の報告を行います。

モニタ機能

- 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
- 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; リモート SPAN）。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。
- 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。

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、『Hardware Installation Guide』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 19 章「DHCP 機能および IP 送信元ガードの設定」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（DHCP サーバとして動作するデバイスが設定され、それがイネーブルになっている場合に限る）、DHCP リレー エージェントはイネーブル（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、それがイネーブルになっている場合に限る）に設定されます。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 19 章「DHCP 機能および IP 送信元ガードの設定」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 Secure Socket Layer（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
  - 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。
  - 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。
- VLAN
  - デフォルトの 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 トランキング設定は 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。
  - 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。
- STP、PVST+ は VLAN 1 上でイネーブルに設定されています。詳細は、第 15 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 16 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 17 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 18 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。

（注）　Flex Link を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

- 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 19 章「DHCP 機能および IP 送信元ガードの設定」を参照してください。
- DHCP サーバのポートベースのアドレス割り当てはディセーブルに設定されています。詳細は、第 19 章「DHCP 機能および IP 送信元ガードの設定」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 21 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 deny です。詳細は、第 21 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 21 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 21 章「IGMP スヌーピングおよび MVR の設定」を参照してください。

（注）　MVR を使用するには、スイッチで LAN ベース イメージを稼動している必要があります。

- 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 22 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 22 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 22 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 22 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 23 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 25 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 26 章「SPAN および RSPAN の設定」を参照してください。

（注）　RSPAN を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

- RMON はディセーブルに設定されています。詳細は、第 27 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 28 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 29 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 30 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 32 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 35 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。

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。 • 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	• 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。
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 を使用するには、スイッチで LAN ベース イメージを稼動している必要があります。 **（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。

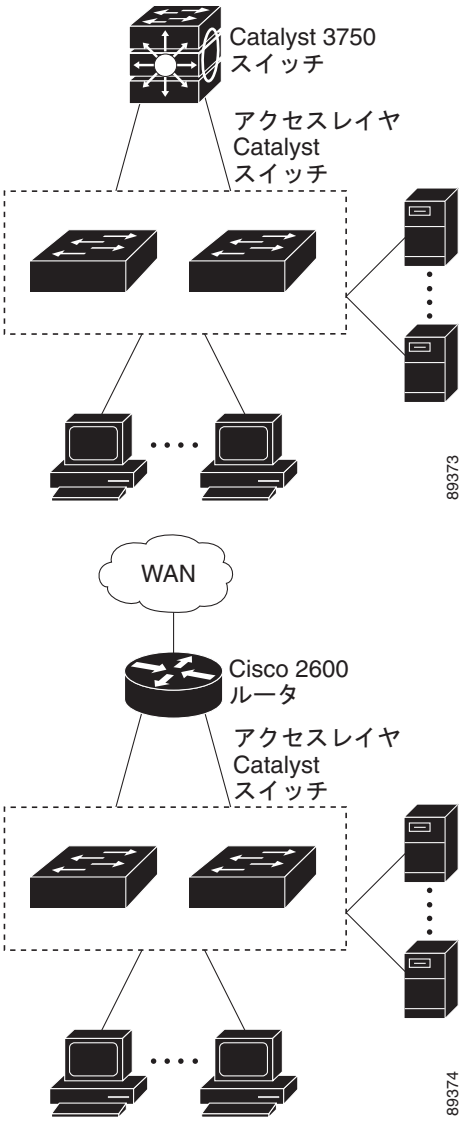
スイッチを使用して、次のものを作成できます。

- 高性能ワークグループに適したコスト効率の高いギガビットツーデスクトップ（図 1-1）：ネットワーク リソースへの高速アクセスを実現するには、Cisco Catalyst 2960 スイッチをアクセス レイヤで使用して、デスクトップにギガビット イーサネットを提供します。輻輳を回避するために、各スイッチ上で QoS DSCP マーキングによるプライオリティ設定を使用します。ディストリビューション レイヤで高速 IP 転送を実現するには、アクセス レイヤのスイッチを、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（Catalyst 3750 スイッチなど）またはルータに接続します。

  最初の図は分離された高性能ワークグループです。Catalyst 2960 スイッチがディストリビューション レイヤの Catalyst 3750 スイッチに接続されています。2 番めの図はブランチ オフィスの高性能ワークグループです。Catalyst 2960 スイッチがディストリビューション レイヤのルータに接続されています。

この構成では、各スイッチはネットワーク リソースにアクセスするための、専用の 1 Gbps 接続をユーザに提供します。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　高性能ワークグループ（ギガビットツーデスクトップ）



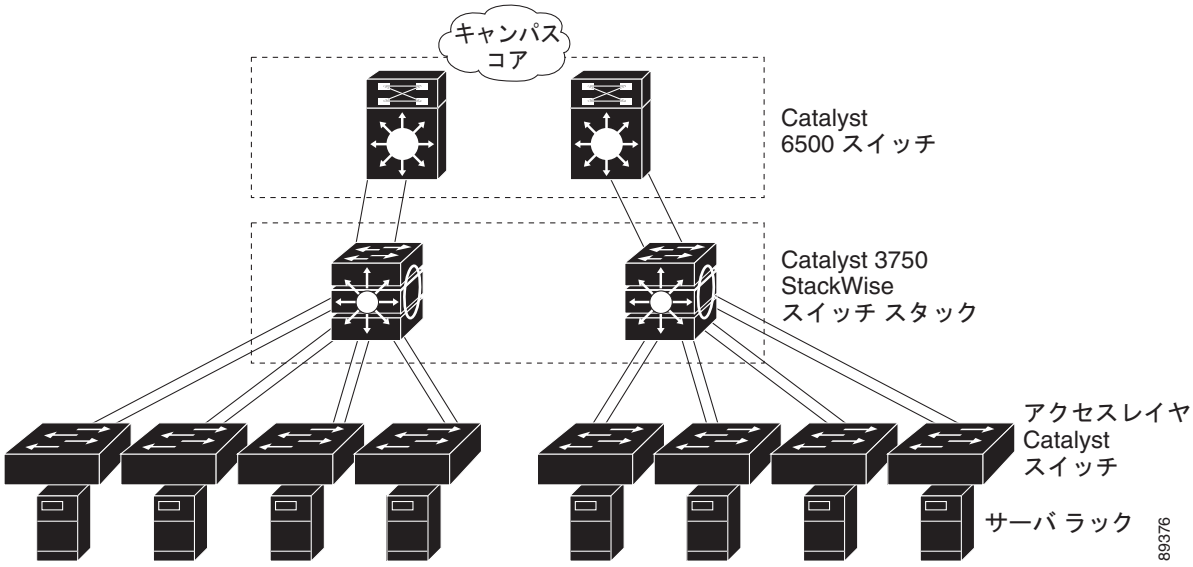
- サーバ集約（図 1-2）：スイッチを使用してサーバ グループを相互接続し、ネットワークの物理的なセキュリティと管理を一元化できます。ディストリビューション レイヤで高速 IP 転送を実現するには、アクセス レイヤ スイッチを、ルーティング機能を備えたマルチレイヤ スイッチに接続します。ギガビットの相互接続によって、データ フローの遅延を最小限に抑えることができます。

  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 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 2960 スイッチを使用した中小規模のネットワーク

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 2960 スイッチを使用します。これにより、いずれかのルータ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。スイッチは負荷分散に EtherChannel を使用しています。

スイッチは、ワークステーションおよびローカル サーバ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。

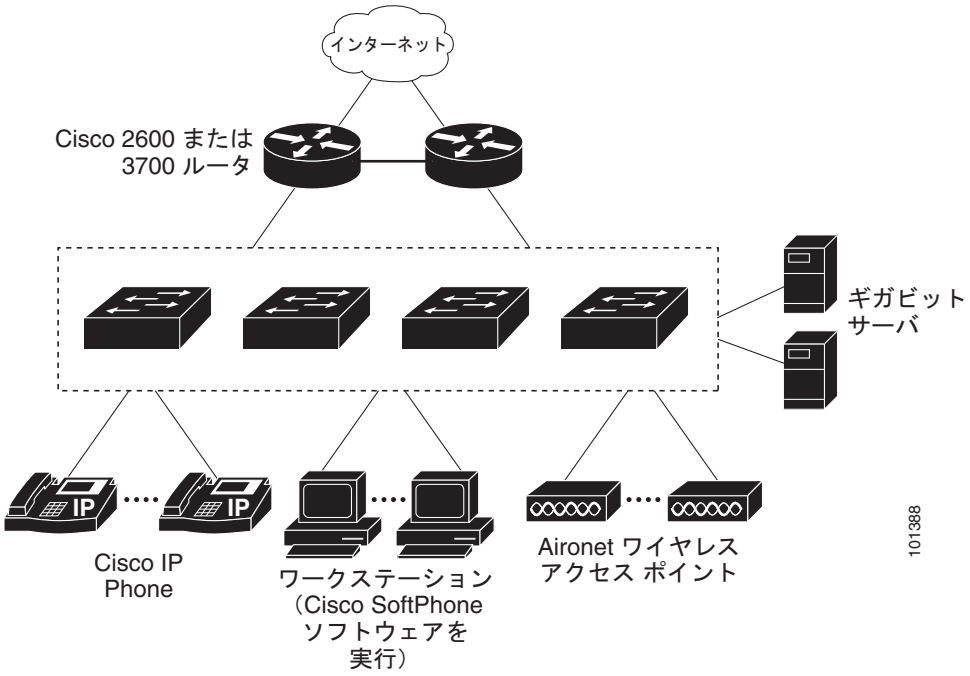
ある VLAN のエンド ステーションが別の VLAN にあるエンド ステーションと通信する必要がある場合、ルータが宛先 VLAN にトラフィックをルーティングします。このネットワークでは、ルータが VLAN 間ルーティングを行います。スイッチ上の VLAN アクセス コントロール リスト（VLAN マップ）が VLAN 内セキュリティを設定し、不正ユーザがネットワークの重要な領域にアクセスしないようにします。

VLAN 間ルーティング以外に、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。

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の両方をサポートします。

ルータ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 アクセスも提供します。

図 1-3　コラプスト バックボーン構成の Catalyst 2960 スイッチ



長距離広帯域トランスポートの構成

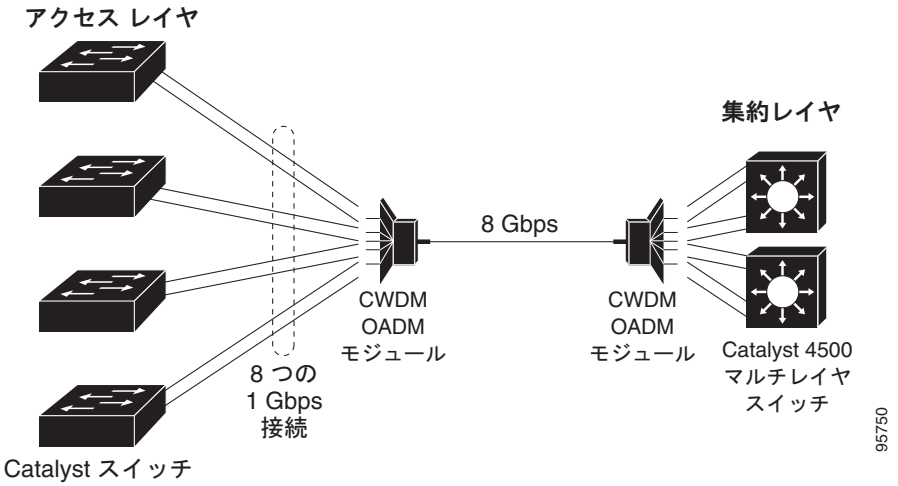
（注）　CWDM SFP を使用するには、スイッチで LAN ベース イメージを実行している必要があります。

図 1-4 に、8 ギガビットのデータを 1 本の光ファイバ ケーブルで送信するための構成を示します。Catalyst 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。2960 CWDM SFP モジュールに応じて、データは 1470 ～ 1610 nm の波長で送信されます。波長が高くなるほど、伝送できる距離が長くなります。長距離伝送用に使われる一般的な波長は 1550 nm です。

CWDM SFP モジュールは、最大 393,701 フィート（74.5 マイルまたは 120 km）の距離で、CWDM Optical Add/Drop Multiplexer（OADM; 光分岐挿入）モジュールに接続します。CWDM OADM モジュールは、さまざまな CWDM 波長を結合（*多重化*）して、同じ光ファイバ ケーブル上で同時に伝送できるようにします。受信側エンドの CWDM OADM モジュールは、さまざまな波長を分離（*逆多重化*）します。

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

図 1-4　　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」