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。

- 「機能」（P.1-1）
- 「初期スイッチ設定後のデフォルト設定値」（P.1-13）
- 「スイッチを使用する場合の設計概念」（P.1-16）
- 「次の作業」（P.1-19）

特に記述がない限り、*スイッチ*という用語はスタンドアロン ブレード スイッチを意味しています。

このマニュアルでは、明示的に IP Version 6（IPv6）を指す場合を除き、IP とは IP Version 4（IPv4）のことを指します。

機能

Cisco IOS Release 12.2(44)SE 以降では、スイッチに IP ベース イメージがインストールされており、レイヤ 2+ 機能（エンタープライズクラスのインテリジェント サービス）を備えています。これらの機能としては、Access Control List（ACL; アクセス コントロール リスト）、QoS（Quality of Service）、スタティック ルーティング、EIGRP および PIM スタブ ルーティング、Hot Standby Router Protocol（HSRP）、Routing Information Protocol（RIP）、IPv6 ホスト管理、および IPv6 MLD スヌーピングなどがあります。

この章で説明する一部の機能は、暗号化（暗号化対応）バージョンのソフトウェアでのみ利用可能です。この機能を使用し、Cisco.com から暗号化バージョンの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。

スイッチには次の機能があります。

- 「Ease-of-Deployment および Ease-of-Use 機能」（P.1-2）
- 「パフォーマンス向上機能」（P.1-2）
- 「管理オプション」（P.1-3）
- 「管理の容易さに関する機能」（P.1-4）（暗号化バージョンのソフトウェア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.1-6）
- 「VLAN 機能」（P.1-7）
- 「セキュリティ機能」（P.1-7）（暗号化バージョンのソフトウェアを必要とする機能を含む）
- 「QoS および CoS 機能」（P.1-11）
- 「レイヤ 3 機能」（P.1-12）
- 「モニタリング機能」（P.1-12）

Ease-of-Deployment および Ease-of-Use 機能

スイッチには、単体のスイッチを Web ブラウザから設定し、モニタするための組み込みのデバイス マネージャ GUI（グラフィカル ユーザ インターフェイス）が備えられています。デバイス マネージャの起動の詳細については、『スタートアップ ガイド』を参照してください。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。

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。

- Cisco EnergyWise は Power over Ethernet（PoE）エンティティのエネルギー使用を管理します。

  詳細については、Cisco.com の『*Cisco EnergyWise Version 2 Configuration Guide*』を参照してください。

- すべてのスイッチ ポートの速度自動検知、およびデュプレックス モードの自動ネゴシエーション。帯域幅の利用を最適化します。
- 10/100/1000 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; 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。
- 最大 1546 バイトのルーテッド フレームをサポートします。
- 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）
- 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）全二重の帯域幅を確保します。
- 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
- 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します。
- 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
- Cisco Group Management Protocol（CGMP）サーバのサポートおよび Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）バージョン 1、バージョン 2、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
- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）バージョン 1、バージョン 2、バージョン 3 対応の IGMP スヌーピングにより、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します。
- マルチキャスト ルータ クエリー単位で IGMP レポートを 1 つだけマルチキャスト デバイスへ送信する IGMP レポート抑制（IGMPv1 または IGMPv2 クエリーでだけサポート）
- 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 IP バージョン 6（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 Multicast Listener Discovery（MLD）スヌーピング
- 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 フォワーディング 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 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 リソースが割り当てられます。
- Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）は、Cisco IOS ソフトウェアの一部で、ネットワーク パフォーマンスを測定するアクティブ トラフィック モニタリングを使用します。
- 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
- Cisco Medianet により、多様なビデオ アプリケーションを対象としたネットワーク インフラストラクチャにおけるインテリジェントなサービスが可能になります。Medianet のサービスの 1 つに、Auto Smartport を通じて実行する、Cisco Digital Media Player および Cisco IP Video Surveillance カメラの自動プロビジョニングがあります。
- Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）拡張機能には、スイッチがダイナミック MVR モードの場合に、2000 MVR グループを設定する機能や、リングトポロジでの転送をメンバー ポートに制限させる新しいコマンド（**mvr ringmode flood**）などがあります。
- メモリ整合性検査ルーチンでは、無効な Ternary Content Addressable Memory（TCAM）テーブル エントリが検出され、修正されます。

管理オプション

次のオプションは、スイッチの設定と管理を実行します。

- 組み込みデバイス マネージャ：このデバイス マネージャはソフトウェア イメージに組み込まれた GUI として機能します。このデバイス マネージャは単体のスイッチの設定とモニタリングに使用します。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。
- 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、管理ステーションをスイッチ コンソール ポートに直接接続するか、リモート管理ステーションから Telnet を利用します。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：HP OpenView などの SNMP 管理アプリケーション。HP OpenView または 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; リモート モニタリング）グループをサポートします。SNMP の詳しい使用方法については、第 31 章「SNMP の設定」を参照してください。
- Cisco IOS Configuration Engine（旧 Cisco IOS CNS エージェント）：ネットワーク デバイスおよびサービスの配置と管理を自動化する設定サービスです。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アップデートを自動化できます。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。

（注）　管理インターフェイスの詳細については、「スイッチを使用する場合の設計概念」（P.1-16）を参照してください。

管理の容易さに関する機能

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 組み込みエージェント
- 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、IP アドレス要求など 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
- 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
- 多数のスイッチに指定した設定と新しいイメージをダウンロードするための DHCP ベースの自動設定およびイメージ アップデート
- スイッチ ポートへの IP アドレス事前割り当てのための DHCP サーバのポートベース 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
- VLAN での MAC アドレス学習のディセーブル化
- 設定可能な MAC アドレス スケーリングにより、VLAN での MAC アドレス学習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ます。
- 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 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
- スイッチからのロケーション情報をエンドポイント デバイスに提供する LLDP メディア拡張（LLDP-MED）ロケーション TLV

- 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）、Differentiated Services Code Point（DSCP; Diffserv コード ポイント）、およびタギング モードの各値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。
- CDP および LLDP 拡張機能を使用したビデオ エンド ポイントとのロケーション情報の交換による、サーバからの動的なロケーションベースのコンテンツの配信
- 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
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）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。
- 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
- 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 セッション上のデバイス マネージャを通じてアクセスするインバンド管理アクセス
- 最大 16 の Telnet 接続を同時に使用できるインバンド管理アクセス。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 ベース 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（暗号化バージョンのソフトウェアが必要）
- SNMP バージョン 1、2c、3 の get および set 要求によるインバンド管理アクセス
- アウトオブバンド管理アクセス。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。
- CPU 使用率をモニタリングする CPU 使用率しきい値トラップ
- 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（暗号化バージョンのソフトウェアが必要）
- 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。
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を IPv6 トランスポート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 パケットのオプション 12 のフィールドにホスト名を含める機能のサポート。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。

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。

- Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）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。
- 単一方向リンク検出（UDLD）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 間のロード バランシング
  - Rapid PVST+ による VLAN 間のロード バランシングとスパニングツリー インスタンスの高速コンバージェンス
  - UplinkFast 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
- IEEE 802.1s Multiple Spanning-Tree Protocol（MSTP）が、複数の VLAN をスパニング ツリー インスタンスにグループ化し、データ トラフィックとロード バランシング用の複数の転送パスを提供します。さらに、IEEE802.1w Rapid Spanning-Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）に基づき、Rapid Per-VLAN Spanning-Tree plus（Rapid PVST+）が、ルートと Designated Port（DP; 指定ポート）を即座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を実行します。
- 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 ステートに即時に変更することで転送遅延を解消
  - 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 インターフェイスは、基本リンク冗長性のため STP に対する代替として相互にバックアップします。
- リンクステート トラッキング（レイヤ 2 トランク フェールオーバー）。外部イーサネット リンク状態をミラーリングし、プロセッサ ブレードのトラフィックを個別の Cisco イーサネット スイッチ上の動作する外部リンクにフェールオーバーできます。

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 規格によって許可された 1 ～ 4094 の範囲の VLAN ID をサポートします。
- ダイナミック VLAN メンバシップに対応する VLAN Query Protocol（VQP）
- すべてのポート上で稼動する Inter-Switch Link（ISL; スイッチ間リンク）および IEEE 802.1Q トランキング 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 つのデバイス間のリンクでのトランキングのネゴシエーション、および使用するトランキング カプセル化タイプ（IEEE 802.1Q または ISL）のネゴシエーションを行います。
- 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、制御プロトコル フレームの送受信を引き続き行います。
- 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 冗長性を提供する VLAN Flex Link ロード バランシング。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。
- プライベート VLAN。VLAN スケーラビリティ問題に対処し、制御された IP アドレスを割り当て、レイヤ 2 ポートをスイッチの他のポートから切り離します。
- プライベート VLAN ホストのポート セキュリティ。ポートで学習される MAC アドレス数を制限します。また、ポートで学習される MAC アドレスを定義します。
- 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。

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。

- 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 Agreements（IP SLA; IP サービス レベル契約）のサポート
- 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。
- MAC 認証バイパス（MAB）エージング タイマー。MAB を使用して認証された後に認証された非アクティブなホストを検出します。

- 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。
- 管理インターフェイス（デバイス マネージャおよび不正な設定変更を防止するための 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）
- 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
- 違反が発生したときに、ポート全体をシャットダウンするのではなく、当該ポートの VLAN をシャットダウンする、VLAN 認識ポート セキュリティ オプション
- 音声認識 IEEE 802.1x および mac authentication bypass（MAB; MAC 認証バイパス）のセキュリティ違反機能により、セキュリティ違反の発生時にポート上のデータ VLAN だけ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）により、ルーテッド インターフェイス（ルータ ACL）と VLAN の両方向およびレイヤ 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
- 拡張 MAC ACL により、レイヤ 2 インターフェイスの受信方向に関するセキュリティ ポリシーを定義
- VLAN ACL（VLAN マップ）により、MAC、IP、および TCP/UDP ヘッダー内の情報に基づくトラフィックのフィルタリングを行い VLAN 内のセキュリティを確保
- 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
- スタティック ACL が設定されていないポートでの、auth-default ACL の動的な作成または接続のサポート
- DHCP スヌーピングにより、untrusted 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
- IP ソース ガードにより、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きトラフィックをフィルタリングすることで、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
- ダイナミック ARP インスペクション。同じ VLAN 内の他のポートの無効な ARP 要求や応答を信頼しないことで、スイッチでの悪意のある攻撃を回避します。
- IEEE 802.1Q トンネリングにより、サービス プロバイダーのネットワークをまたがるリモート サイトにユーザがいるカスタマーは、その他のカスタマーから VLAN を分離できます。また、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、CDP、VTP の各情報がカスタマー ネットワークに含まれます。
- レイヤ 2 ポイントツーポイント トンネリング。EtherChannel を自動的に作成します。
- レイヤ 2 プロトコル トンネリングのバイパス機能。サードパーティ ベンダーとの相互運用性を実現します。
- オープン アクセス対応 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。
- 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。

- IEEE 802.1x ポートベースの認証。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。
  - VLAN 割り当て。IEEE 802.1x 認証ユーザを特定の VLAN に制限します。
  - ポート セキュリティ。IEEE 802.1x ポートへのアクセスを制御します。
  - 音声 VLAN。ポートが許可ステートか無許可ステートかにかかわらず、Cisco IP Phone の音声 VLAN へのアクセスを許可します。
  - ゲスト VLAN。IEEE 802.1x 以外の規格に準拠するユーザに制限付きの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 プロセスで認証するための資格情報を持たないユーザに制限つきのサービスを提供します。
  - multi-auth モードに設定されたポートでの VLAN 割り当てをサポートします。RADIUS サーバはポートで最初に認証されたホストに VLAN を割り当て、それ以降のホストが同じ VLAN を使用します。音声 VLAN は 1 台の IP Phone に対してサポートされます。
  - IEEE 802.1x アカウンティングにより、ネットワーク使用をトラッキング
  - IEEE 802.1x と Wake-on-LAN。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。
  - 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 ホストの準備状況を判別します。
  - 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 にのみ違反時の処理を適用します。
  - 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 にのみ違反時の処理を適用します。
  - 802.1x スイッチ サプリカントによる Network Edge Access Topology（NEAT）。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。
  - 複数ユーザの認証機能により、802.1x がイネーブルになっているホストに対し、2 つ以上のホストを認証できます。
- MAC 認証バイパス。クライアントの MAC アドレスに基づいてクライアントを許可します。
- Network Admission Control（NAC）機能
  - デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウィルス対策の状態または*態勢*に関する NAC レイヤ 2 IEEE 802.1x 検証。

    NAC レイヤ 2 IEEE 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 802.1x 検証の設定」（P.8-54）を参照してください。
  - デバイスのネットワークアクセスを許可する前の、エンドポイントシステムまたはクライアントの*態勢*に関する NAC レイヤ 2 IP 検証

    NAC レイヤ 2 IP 検証の設定の詳細については、『*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.8-49）を参照してください。

  - Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）ダウン ポリシー。態勢検証が発生したときに、AAA サーバが利用できない場合のホストの NAC レイヤ 2 IP 検証

    この機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

- TACACS+：TACACS サーバを使用してネットワーク セキュリティを管理する独自仕様の機能
- RADIUS により、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）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
- 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（暗号化バージョンのソフトウェアが必要）
- 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（暗号化バージョンのソフトウェアが必要）
- 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、そのアトリビュートを変更します。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 パケットを送信して認証を再初期化し、新しいポリシーを適用できます。
- IEEE 802.1x ユーザ ディストリビューション。複数の VLAN（ユーザ グループ向け）が配置されている場合、複数の VLAN でユーザをロード バランシングすることで、ネットワークのスケーラビリティを向上できます。認証されたユーザは、RADIUS サーバの割り当てによる、グループで最も空いている VLAN に割り当てられます。
- 複数のホストを認証する重要な VLAN のサポート。この機能により、ポートが multii-auth に設定されているときは、AAA サーバが到達不能になり、重要なリソースに引き続きアクセスするためにこのポートは重要な VLAN に配置されます。
- Web 認証のカスタマイズが可能。これによってローカル Web 認証を行うユーザ定義の Web ページ、*login*、*success*、*failure*、および *expire* の作成ができます。
- Network Edge Access Topology（NEAT）のサポート。これにより、ポートのホスト モードが変更され、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が適用されます。
- VLAN-ID ベースの MAC 認証機能。VLAN と MAC アドレス情報を組み合わせてユーザ認証に使用することにより、無許可の VLAN からのネットワーク アクセスを防止します。
- MAC 移動機能。ホスト（IP Phone の背後に接続されているホストを含む）は、モビリティをイネーブルにするための制限を課されることなく、同じスイッチ内のポート間を移動することができます。MAC 移動機能では、スイッチは、別のポートに再表示された同一 MAC アドレスを、完全に新規の MAC アドレスと同じように処理します。
- バージョン 3 の簡易ネットワーク管理プロトコル（SNMPv3）による 3DES および AES サポート。このリリースは、168 ビット Triple Data Encryption Standard（3DES）および、128 ビット、192 ビット、256 ビットの Advanced Encryption Standard（AES; 高度暗号化規格）暗号化アルゴリズムを SNMPv3 に追加したものです。
- 認証、暗号化、およびアクセス コントロールを使用したセキュリティ アーキテクチャである、Cisco TrustSec の Security Group Tag（SCT）Exchange Protocol（SXP）コンポーネントのサポート。

QoS および CoS 機能

次に、QoS および CoS 機能を示します。

- auto-QoS（自動 QoS）。トラフィックの分類と出力キューの設定を自動化することで既存の QoS 機能の展開を簡略化します。
- 分類
  - ポート単位の IP Type Of Service/Differentiated Services Code Point（IP ToS/DSCP）および IEEE 802.1p CoS プライオリティ マーキング。ポート単位での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
  - フローベースのパケット分類（MAC、IP、および TCP/UDP ヘッダー内の情報に基づく分類）に基づく IP ToS/DSCP および IEEE 802.1p CoS マーキング。ネットワーク エッジでの高性能な QoS を実現し、各種ネットワーク トラフィックに応じて区別化したサービス レベルを可能にし、ネットワーク内のミッションクリティカルなトラフィックを優先
  - 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
- ポリシング
  - スイッチ ポートに関するトラフィックポリシング ポリシー。特定のトラフィック フローに割り当てるポート帯域幅を管理
  - 階層型のポリシー マップで複数のクラスマップを作成する場合、各クラスマップを自身のポート レベル（第 2 レベル）ポリシー マップと関連付けることができます。第 2 レベルのポリシー マップは、それぞれ異なるポリサーを保有できます。
  - トラフィック フローのポリシングをまとめて行う集約ポリシング。特定のアプリケーションまたはトラフィック フローをあらかじめ定義された特定のレートに制限します。
- 不適合
  - 帯域幅の使用制限を超過したパケットの不適合マークダウン
- 入力キューイングおよびスケジューリング
  - ユーザ トラフィック用に設定可能な 2 つの入力キュー（一方のキューをプライオリティ キューにできます）
  - 輻輳回避メカニズムとしての Weighted Tail Drop（WTD）。キュー長を管理し、トラフィックの分類ごとに異なるドロップ優先順位を設定します。
  - Shaped Round Robin（SRR; シェイプド ラウンド ロビン）。パケットがキューから内部リングへ送出されるときのレートを指定するスケジューリング サービス（入力キューでサポートされる唯一のモードはシェアリング）
- 出力キューおよびスケジューリング
  - 1 ポートに 4 つの出力キュー
  - 輻輳回避メカニズムとしての WTD。キュー長を管理し、トラフィックの分類ごとに異なるドロップ優先順位を設定します。
  - SRR パケットがキューから出力インターフェイスへ送出されるときのレートを指定するスケジューリング サービス（出力キューでは、シェーピングまたはシェアリングがサポートされる）。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 信頼機能のサポート
- Auto-QoS 拡張機能では、Cisco Telepresence System や Cisco Surveillance Camera などのビデオ デバイスからのトラフィック フローを、自動的にコンフィギュレーション分類できるようになります。

レイヤ 3 機能

次に、レイヤ 3 機能について説明します。

- レイヤ 3 ルータの冗長構成用の HSRP Version 1（HSRPv1）および HSRP Version 2（HSRPv2）
- RIP バージョン 1 および 2 などの 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
- ルーテッド アクセス用の OSPF によって、アクセスまたはワイヤリング クローゼットへのレイヤ 3 ルーティング機能を拡張可能
- 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
- 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; インターネット制御メッセージ プロトコル）および ICMP Router Discovery Protocol（IRDP）。ルータのアドバタイズおよびルータ送信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
- 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
- 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）
- IPv6 ユニキャスト ホスト管理
- SVI ラインステート アップまたはダウンの計算から VLAN 内のポートを除外する機能

モニタリング機能

次に、モニタリング機能を示します。

- スイッチ LED によるポートレベルおよびスイッチレベルのステータス確認
- MAC アドレス通知トラップおよび RADIUS アカウンティング。スイッチが学習または削除した MAC アドレスをストアすることによって、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）による、任意のポートまたは VLAN のトラフィック モニタリング
- 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リング、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リングし、トラフィック解析を行うことができます。
- Syslog ファシリティ。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。

- SFP モジュール診断管理インターフェイス。SFP モジュールの物理ステータスまたは動作ステータスをモニタします。
- スイッチが稼動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 Generic Online Diagnostics
- HSRP の拡張オブジェクト トラッキング
- Cisco IOS デバイスおよび EEM 3.2 内でのイベント検出と回復のための Embedded Event Manager（EEM; 組み込みイベント マネージャ）をサポートし、ネイバー ディスカバリ、ID、および MAC アドレス テーブルに対するイベント ディテクタが導入されます。

初期スイッチ設定後のデフォルト設定値

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）　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は、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 21 章「DHCP 機能および IP ソース ガードの設定」を参照してください。
- デフォルトのドメイン名は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、イネーブルの場合だけ）。DHCP リレー エージェントはイネーブルに設定されています（DHCP リレー エージェントとして動作するデバイスが設定されていて、イネーブルの場合だけ）。詳細については、第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」、および第 21 章「DHCP 機能および IP ソース ガードの設定」を参照してください。
- 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 7 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 7 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。詳細については、第 7 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 8 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 10 章「インターフェイス特性の設定」を参照してください。
  - インターフェイス速度およびデュプレックス モードが自動ネゴシエーションに設定されています。詳細については、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、イネーブルです。詳細については、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。詳細については、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。
  - PortFast は 10 個の内部ギガビット イーサネットでイネーブルにされています。詳細については、第 19 章「オプションのスパニング ツリー機能の設定」を参照してください。
- Smartport マクロは定義されていません。詳細については、第 11 章「SmartPort マクロの設定」を参照してください。
- VLAN
  - デフォルト VLAN は VLAN 1 です。詳細については、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。詳細については、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。詳細については、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。詳細については、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。詳細については、第 13 章「VTP の設定」を参照してください。
  - プライベート VLAN は設定されていません。詳細については、第 15 章「プライベート VLAN の設定」を参照してください。
  - 音声 VLAN はディセーブルに設定されています。詳細については、第 14 章「音声 VLAN の設定」を参照してください。
- IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングはディセーブルに設定されています。詳細については、第 16 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 の場合、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 17 章「STP の設定」を参照してください。
- MSTP はディセーブルに設定されています。詳細については、第 18 章「MSTP の設定」を参照してください。
- オプションのスパニングツリー機能はディセーブルに設定されています。詳細については、第 19 章「オプションのスパニング ツリー機能の設定」を参照してください。
- Flex Link は設定されていません。詳細については、第 20 章「Flex Link および MAC アドレステーブル移動更新機能の設定」を参照してください。
- DHCP スヌーピングは、ディセーブルです。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 21 章「DHCP 機能および IP ソース ガードの設定」を参照してください。

- IP ソース ガードはディセーブルです。詳細については、第 21 章「DHCP 機能および IP ソース ガードの設定」を参照してください。
- 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設定されています。詳細については、第 22 章「ダイナミック ARP インスペクションの設定」を参照してください。
- IGMP スヌーピングはイネーブルに設定されています。IGMP のフィルタは適用されていません。詳細については、第 23 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スロットリング設定は拒否されます。詳細については、第 23 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スヌーピング クエリア機能はディセーブルに設定されています。詳細については、第 23 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- MVR はディセーブルに設定されています。詳細については、第 23 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- ポートベース トラフィック
  - ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルに設定されています。詳細については、第 24 章「ポートベース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 24 章「ポートベース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 24 章「ポートベース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 24 章「ポートベース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 25 章「CDP の設定」を参照してください。
- UDLD はディセーブルに設定されています。詳細については、第 27 章「UDLD の設定」を参照してください。
- SPAN および RSPAN はディセーブルに設定されています。詳細については、第 28 章「SPAN および RSPAN の設定」を参照してください。
- RMON はディセーブルに設定されています。詳細については、第 29 章「RMON の設定」を参照してください。
- Syslog メッセージはイネーブルに設定され、コンソール上に表示されます。詳細については、第 30 章「システム メッセージ ロギングの設定」を参照してください。
- SNMP はイネーブルに設定されています（バージョン 1）。詳細については、第 31 章「SNMP の設定」を参照してください。
- ACL は設定されていません。詳細については、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。
- EtherChannels は設定されていません。詳細については、第 36 章「EtherChannel およびレイヤ 2 トランク フェールオーバーの設定」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 37 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 と拡張オブジェクト トラッキングの設定」を参照してください。

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。ネットワークを構成する時点で、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が増大している。 • ネットワーク アプリケーション（大容量の添付ファイル付き電子メールなど）および帯域幅を多用するアプリケーション（マルチメディアなど）による帯域幅需要が増大している。	• 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つれ、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重要なアプリケーションに対する帯域幅保証	• IGMP スヌーピングを使用して、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、帯域幅およびセキュリティ上の理由から、そ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需要の高さ	• Hot Standby Router Protocol（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プライオリティ設定し、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 に基づく高プライオリティまたは低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、音声とラフィックに別個の VLAN を用意します。

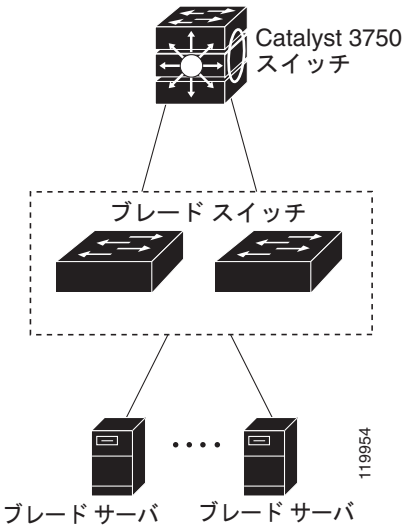
スイッチを使用して、次を作成できます。

- High-Performance ワークグループ向けの費用効果が高い Gigabit-to-the-Blade サーバ（図 1-1）：ネットワーク リソースに高速アクセスするために、アクセス レイヤで Cisco Catalyst Blade Switch 3030 for Dell 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。輻輳を回避するには、これらのスイッチ上で 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 3750 スイッチなどのルーティング機能を持つギガビット マルチレイヤ スイッチまたはルータに接続します。

  最初の図は、ブレード 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た独立した High-Performance ワークグループの図です。

  この構成の各ブレード スイッチは、ネットワーク リソースへの専用 1 Gb/s 接続を提供します。SFP モジュールは、光ファイバ接続によって、メディアと距離を柔軟に選択することもできます。

図 1-1　High-Performance ワークグループ（Gigabit-to-the-Blade サーバ）



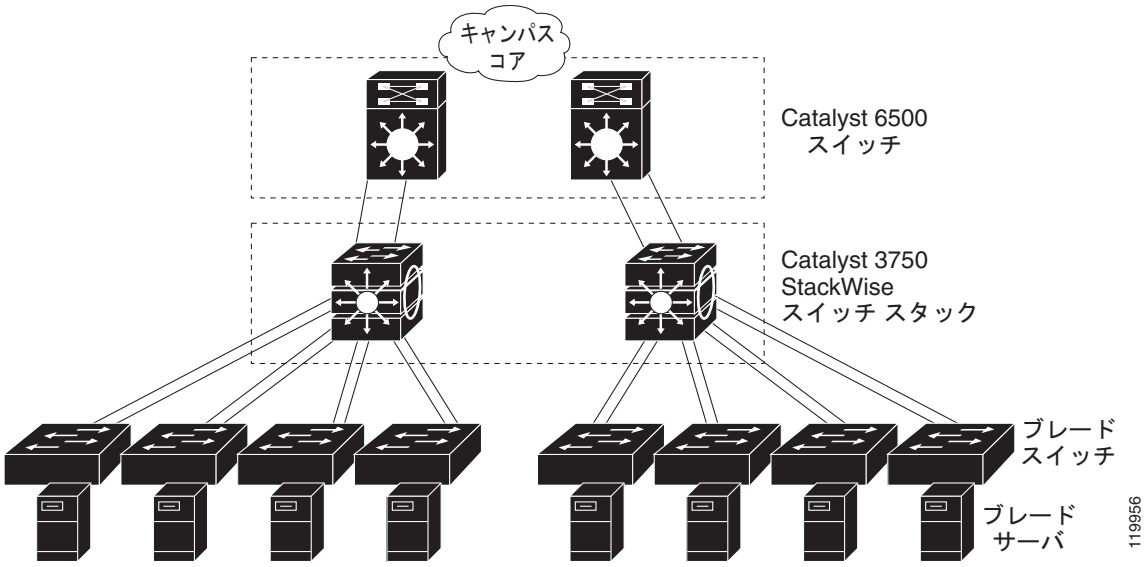
- サーバ集約（図 1-2）：スイッチを使用してサーバ グループを相互に接続し、ネットワークの物理的なセキュリティと管理を一元化できます。ディストリビューション レイヤで高速 IP 転送を実現するには、アクセス レイヤ スイッチを、ルーティング機能を備えたマルチレイヤ スイッチに接続します。ギガビットの相互接続によって、データ フローの遅延を最小限に抑えます。

  ブレード 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。ブレード 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対障害性は、冗長ギガビット EtherChannel を持つブレード 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。

  ブレード スイッチのデュアル SFP モジュール アップリンクを使用すると、ネットワーク コアに冗長アップリンクを構築できます。SFP モジュールは、光ファイバ接続によって、メディアと距離を柔軟に選択することができます。

図 1-2　サーバ集約



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」