CHAPTER 1

設定の概要

機能

スイッチは暗号化イメージ（暗号化対応）をサポートするために Cisco IOS ソフトウェア ライセンス（CISL）アーキテクチャを使用しています。このイメージは、スイッチ モデルによって LAN Base または LAN Lite 機能を実装しています。

- LAN Base イメージは、Quality Of Service (QoS)、ポート セキュリティ、1588v2 PTP、およびスタティック ルーティング機能を提供します。
- LAN Lite イメージは、SSH や SNMPv3 などの重要なセキュリティ機能を除き、レイヤ 2 機能が制限されて提供されます。

フィーチャ ソフトウェア ライセンス

フィーチャ ライセンスは、ソフトウェア ライセンスによって LAN Base または LAN Lite 機能を実装する、単一のユニバーサル イメージでサポートされます。

- LAN Base 機能には、Quality Of Service（QoS）、ポート セキュリティ、PTP およびスタティック ルーティングが含まれます。
- LAN Lite 機能は、SSH や SNMPv3 などの重要なセキュリティ機能を除き、レイヤ 2 機能が制限されて提供されます。

暗号化機能はユニバーサル イメージに含まれています。

これらのガイドラインは、スイッチ上でどのイメージが動作しているかを特定することができます。

- **show version** 特権 EXEC コマンドを入力します。たとえば、IE-2000-8TC-G-E はデフォルトで LAN Base イメージを実行し、IE-2000-4T-G-L は LAN Lite イメージを実行します。
- **show license** 特権 EXEC コマンドを入力し、アクティブなイメージを確認します。

```
Switch# show license
Index 1 Feature: lanbase
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Priority: Medium
        License Count: Non-Counted

Index 2 Feature: lanlite
        Period left: 0  minute  0  second
```

使用および導入を簡素化する機能

- Express Setup : 基本的な IP 情報、コンタクト情報、スイッチおよび Telnet のパスワード、および Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）に関する情報を使用し、ブラウザ ベースのプログラムを通じて、スイッチの初回設定を迅速に行うことができます。Express Setup の詳細については、スタートアップ ガイドを参照してください。
- ユーザ定義およびデフォルト設定の SmartPort マクロ：ネットワークへの配置を簡単にするためにカスタム スイッチ設定を作成します。
- 着脱式の SD フラッシュ カードに、Cisco IOS ソフトウェア イメージと、スイッチのコンフィギュレーション ファイルが格納されています。ソフトウェア機能を再設定せずに、スイッチの交換やアップグレードを実行できます。
- 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。

パフォーマンス向上機能

- すべてのスイッチ ポートの速度自動検知、およびデュプレックス モードの自動ネゴシエーション。帯域幅の利用を最適化します。
- 10/100 Mbps インターフェイス、10/100/1000 Mbps インターフェイス、および 10/100/1000 BASE-TX SFP モジュール インターフェイス上の Auto MDIX 機能により、インターフェイスが必要なケーブル接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定します。
- ルーテッド フレームの場合は最大 1546 バイト、ハードウェアでブリッジングされるフレームの場合は最大 9000 バイト、ソフトウェアでブリッジングされるフレームの場合は最大 2000 バイトのサポート。
- すべてのポートにおける IEEE 802.3x フロー制御（スイッチはポーズ フレームを送信しません）。
- 最大 6 個の EtherChannel グループのサポート。
- 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。
- 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）バージョン 1、バージョン 2、およびバージョン 3 対応の IGMP スヌーピング。
  - （CGMP デバイスの場合）CGMP が特定のエンド ステーションへのマルチキャスト トラフィックを制限し、ネットワーク全般のトラフィックを軽減
  - （IGMP デバイスの場合）IGMP スヌーピングによってマルチメディア トラフィックとマルチキャスト トラフィックを転送
- IGMP レポート抑制。1 つのマルチキャスト ルータ クエリーにつき 1 つの IGMP レポートだけをマルチキャスト デバイスへ送信します（IGMPv1 または IGMPv2 クエリーだけをサポート）。
- IGMP スヌーピング クエリー サポート。IGMP 一般クエリー メッセージを定期的に生成するように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可能。
- 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。
- Cisco IOS IP サービス レベル契約（SLA）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。
- FlexLink に障害が発生したあとのマルチキャスト トラフィックのコンバージェンス時間を短縮するための FlexLink マルチキャスト高速コンバージェンス。
- 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 。
- CPU 生成トラフィックの QoS マーキングのサポートと、出力ネットワーク ポートへの CPU 生成トラフィックのキュー。

管理オプション

- 組み込みデバイス マネージャ：GUI アプリケーションのデバイス マネージャがソフトウェア イメージに組み込まれています。このデバイス マネージャは、単体のスイッチの設定、管理に使用します。デバイス マネージャの起動については、スタートアップ ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- Network Assistant：Network Assistant は、Cisco.com からダウンロードできるネットワーク管理アプリケーションです。単一のスイッチ、スイッチ クラスタ、デバイスのコミュニティの管理に使用します。Network Assistant の詳細については、Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。
- CLI：Cisco IOS ソフトウェアは、デスクトップ スイッチングおよびマルチレイヤ スイッチング機能をサポートします。CLI にアクセスするには、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「コマンドライン インターフェイスの使用」を参照してください。
- SNMP：CiscoWorks 2000 LAN Management Suite（LMS）および HP OpenView などの SNMP 管理アプリケーション。HP OpenView、SunNet Manager などのプラットフォームが稼働している SNMP 対応管理ステーションから管理できます。スイッチは豊富な MIB 拡張機能および 4 つの Remote Monitoring（RMON）グループをサポートします。SNMP の詳しい使用方法については、第 36 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 5 章「Cisco IOS Configuration Engine の設定」を参照してください。

工業用アプリケーション

- CIP：Common Industrial Protocol（CIP）はピアツーピアのアプリケーション プロトコルであり、スイッチと工業用装置（I/O コントローラ、センサー、リレーなど）間でアプリケーション レベルの接続を実現します。CIP ベースの管理ツール（RSLogix など）を使用してスイッチを管理できます。スイッチでサポートされる CIP コマンドの詳細については、コマンド リファレンスを参照してください。
- PROFINET Version 2：PROFINET IO（分散型オートメーション アプリケーション用のモジュラ通信フレームワーク）をサポートします。スイッチから I/O コントローラへの PROFINET 管理接続が可能です。

管理の簡易性に関する機能

- スイッチ管理、設定ストレージ、および配信を自動化するための CNS の組み込み型エージェント。
- Dynamic Host Configuration Protocol（DHCP）によるスイッチ情報（IP アドレス、デフォルト ゲートウェイ、ホスト名、ドメイン ネーム システム（DNS）、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ユーザ データグラム プロトコル（UDP）ブロードキャストの転送（IP アドレス要求を含む）。
- DHCP サーバによる IP アドレスおよびその他の DHCP オプションの IP ホストへの自動割り当て。
- 新しいイメージの指定された設定を多数のスイッチにダウンロードするために、DHCP ベースの自動設定およびイメージをアップデート。
- 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。
- 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。
- アドレス解決プロトコル（ARP）。IP アドレスおよび対応する MAC アドレスによってスイッチを特定します。
- 特定の送信元 MAC アドレスおよび宛先 MAC アドレスを持ったパケットをドロップするユニキャスト MAC アドレス フィルタリング。
- 設定可能な MAC アドレス スケーリング。これにより、VLAN で MAC アドレス ラーニングをディセーブルにし、MAC アドレス テーブルのサイズを制限することができます。
- Cisco Discovery Protocol（CDP）バージョン 1 および 2。ネットワーク トポロジを検出し、ネットワーク上のスイッチと他のシスコ デバイスとのマッピングを行います。
- リンク層検出プロトコル（LLDP）および LLDP Media Endpoint Discovery（LLDP-MED）によるサードパーティ製 IP 電話との相互運用性の確保。
- スイッチからエンドポイント デバイスへロケーション情報を提供する LLDP メディア拡張（LLDP-MED）ロケーション TLV。
- 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）。
- IEEE 1588 標準で定められた高精度時間プロトコル（PTP）により、ネットワーク内の装置のリアルタイム クロックをナノ秒精度で同期できます。
  - 拡張モジュール ポートの PTP メッセージをサポートする PTP 拡張機能。
- 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。
- ビデオなどのマルチキャスト アプリケーションを最適化するための SSM PIM プロトコルのサポート。
- スイッチの設定変更を記録して表示させるコンフィギュレーション ロギング。
- 一意のデバイス ID。**show inventory** ユーザ EXEC コマンドで製品の ID 情報が表示されます。
- Netscape Communicator または Microsoft Internet Explorer ブラウザ セッションでデバイス マネージャを使用した帯域内管理アクセス。
- 最大 16 の Telnet 接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベース セッションを実行できます。
- ネットワーク上の複数の CLI セッションに対する、最大 5 つの同時暗号化セキュア シェル（SSH）接続の確立によって帯域内管理アクセス。
- 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）機能により、セキュアかつ認証済みの方法でスイッチ設定またはスイッチ イメージ ファイルをコピーできます（暗号化バージョンのソフトウェアが必要）。
- 設定の交換およびロールバックは、スイッチ上で一意の保存された Cisco IOS コンフィギュレーション ファイルで稼働している設定を交換します。
- Cisco IOS の HTTP クライアントは、IPv4 と IPv6 の両方の HTTP サーバに要求を送信することができます。また、Cisco IOS の HTTP サーバは、IPv4 と IPv6 の両方の HTTP クライアントから、HTTP 要求にサービスを提供することができます。
- 簡易ネットワーク管理プロトコル（SNMP）を IPv6 トランスポートを介して設定できるため、IPv6 ホストは SNMP クエリーを送信し、IPv6 を実行中のデバイスから SNMP 通知を受信できます。
- ホストやモバイル IP アドレスの管理など、リンク、サブネット、およびサイト アドレス指定の変更を管理するための IPv6 ステートレス自動設定。
- VLAN の MAC アドレス ラーニングをディセーブルにします。
- スイッチ ポートに IP アドレスを前もって割り当てるための DHCP サーバ ポートをベースにしたアドレス割り当て。
- CPU 使用率しきい値トラップによる CPU 使用率の監視。
- VLAN、サービス クラス（CoS）、DiffServ コード ポイント（DSCP）、およびタグ付けモードを指定して音声と音声シグナリングのプロファイルを作成する LLDP-MED ネットワークポリシー プロファイル Time、Length、Value（TLV; 時間、長さ、時間）。
- 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。

- PROFINET IO（分散型オートメーション アプリケーション用のモジュラ通信フレームワーク）をサポートします。スイッチから I/O コントローラへの PROFINET 管理接続が可能です。

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。
  - 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。
- IEEE 802.1s Multiple Spanning-Tree Protocol（MSTP）により、VLAN をスパニングツリー インスタンスに分類、またデータ トラフィックおよびロード バランシング用に複数の転送パスを確保します。また、IEEE 802.1w Rapid Spanning-Tree Protocol（RSTP）に基づいた Rapid Per-VLAN Spanning-Tree plus（Rapid PVST+）により、ルートと指定ポートをただちにフォワーディング ステートに変更することで、スパニングツリーの高速コンバージェンスが実現されます。
- PVST+、Rapid-PVST+、および MSTP モードで使用できるスパニングツリーのオプション機能は次のとおりです。
  - PortFast。ポートをブロッキング ステートからフォワーディング ステートへただちに変更させることによって、転送遅延を防ぎます。
  - BPDU ガード。Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を受信する PortFast 対応ポートをシャットダウンします。
  - BPDU フィルタリング。PortFast 対応ポートで BPDU の送受信ができなくなります。
  - ルート ガード。ネットワーク コア外のスイッチがスパニングツリー ルートになることを防ぎます。
  - ループ ガード。代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。
- FlexLink 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。（LAN Base イメージが必要）
- 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。

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。
- IEEE 802.1Q 規格で認められている 1 ～ 4096 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。
- ダイナミック トランキング プロトコル（DTP）。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 トランキング プロトコル（VTP）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 FlexLink 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。
- 制限付き VLAN（*認証失敗 VLAN* とも呼ばれる）による 802.1X 認証のサポート。
- 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 ～ 4096）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

- 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 サービス レベル契約（IP SLA）のサポート。
- LAN SLA EOT により、スタンバイ ルータのフェールオーバー引き継ぎを行うために、遅延、ジッター、パケット損失などのアクションによってトリガーされる IP SLA 追跡動作からの出力を使用できます（LAN Base イメージが必要）。
- Web 認証。IEEE 802.1x 機能をサポートしないサプリカント（クライアント）に Web ブラウザを使用して認証可能になります。
- ローカル Web 認証バナー。これにより、カスタム バナー、またはイメージ ファイルを Web 認証ログイン画面に表示することができます。
- MAC authentication bypass（MAB; MAC 認証バイパス）エージング タイマー。MAB を使用して認証した後に認証された非アクティブのホストを検出します。
- 管理インターフェイス（デバイス マネージャ、Network Assistant、CLI）へのパスワード保護付きアクセス（読み取り専用および読み書きアクセス）。不正な設定変更を防止します。
- セキュリティ レベル、通知、および対応するアクションを選択できる、マルチレベル セキュリティ。
- セキュリティを確保できるスタティック MAC アドレッシング。
- 保護ポート オプション。同一スイッチ上の指定ポートへのトラフィック転送を制限します。
- ポートにアクセスできるステーションの MAC アドレスを制限または特定するポート セキュリティ オプション。

- 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。
- 指定した入力割合を超えたパケットをドロップして、スイッチへの着信プロトコル トラフィックの割合を制御する、プロトコル ストーム プロテクション。
- BPDU ガード。無効なコンフィギュレーションが発生した場合に、PortFast が設定されているポートをシャットダウンします。
- 標準および拡張 IP ACL。ルーテッド インターフェイス（ルータ ACL）と VLAN の双方向およびレイヤ 2 インターフェイス（ポート ACL）の受信方向に関するセキュリティ ポリシーを定義します。
- MAC 拡張アクセス コントロール リスト。レイヤ 2 インターフェイスの着信方向のセキュリティ ポリシーを定義します。
- 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、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。
- レイヤ 2 プロトコル トンネリングのバイパス機能。サードパーティ ベンダーとの相互運用性を実現します。
- IEEE 802.1x ポートベース認証。不正なデバイス（クライアント）によるネットワーク アクセスを防止します。次の機能がサポートされています。
  - データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が、同じ IEEE 802.1x 対応スイッチ ポートにおいて、単独で認証できるようにする Multidomain Authentication（MDA; マルチドメイン認証）。
  - MDA のダイナミック音声 VLAN（仮想 LAN）。ダイナミック音声 VLAN が MDA 対応ポートで可能になります。
  - VLAN 割り当て。802.1x 認証ユーザを特定の VLAN に制限します。
  - 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。
  - 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。802.1x に準拠はしているが、標準の 802.1x で認証するためのクレデンシャルを持っていないユーザに制限付きのサービスを提供します。
  - 802.1x アカウンティング。ネットワーク使用をトラッキングします。
  - 802.1x と LAN の Wake-on-LAN（WoL）機能。休止状態の PC に、特定のイーサネット フレームを送信して起動させます。
  - 802.1x 準備状態チェック。スイッチで IEEE 802.1x を設定する前に、接続されたエンド ホストの準備状態を判断します。

  - セキュリティ違反が発生した VLAN だけでトラフィック違反アクションを適用するための音声認識 802.1x セキュリティ。
  - MAC 認証バイパス。クライアントの MAC アドレスに基づいてクライアントを許可します。
  - 802.1X スイッチ サプリカントを使用する Network Edge Access Topology（NEAT）、CISP を使用するホスト許可、および自動イネーブル。ワイヤリング クローゼットの外にあるスイッチを別のスイッチのサプリカントとして認証します。
  - 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 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。
  - 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。
  - 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。

- Network Admission Control（NAC）機能：
  - デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウイルス対策の状態またはポスチャに関する NAC レイヤ 2 802.1x 検証

    NAC レイヤ 2 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 802.1x 検証の設定」（P.13-46）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の設定」（P.13-44）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 サービスを通じてリモート ユーザの ID の確認、アクセス権の付与、アクションの追跡を実行できます。
- IPv6 上での機能向けに、RADIUS、TACACS+、および SSH を拡張。
- Kerberos セキュリティ システム。信頼できるサードパーティを使用して、ネットワーク リソースに対する要求を認証します（ソフトウェアの暗号化バージョンが必要）。
- HTTP 1.1 サーバ認証、暗号化、メッセージ整合性、HTTP クライアント認証用に Secure Socket Layer（SSL）バージョン 3.0 がサポートされ、安全な HTTP 通信が可能になります（ソフトウェアの暗号化バージョンが必要）。
- 音声認識 IEEE 802.1X および MAB セキュリティ違反。セキュリティ違反が発生すると、ポートのデータ VLAN だけがシャットダウンされます。
- スタティック ホストでの IP ソース ガードのサポート。

- RADIUS 認証の変更（CoA）。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 ユーザ ディストリビューション。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。
- 複数のホスト認証を行うクリティカル VLAN では、ポートがマルチ認証用に設定されており、AAA サーバが到達不能となった場合でも、重要なリソースにアクセスできるように、ポートがクリティカル VLAN に配置されます。
- ローカル Web 認証のために、ユーザ定義の *login*、*success*、*failure* および *expire* Web ページを作成できるカスタマイズ可能な Web 認証拡張。
- ポート ホスト モードの変更および認証スイッチ ポート上の標準ポート設定の適用を行う Network Edge Access Topology（NEAT）のサポート。
- 認証されていない VLAN からのネットワーク アクセスを回避するためのユーザ認証に、VLAN および MAC のアドレス情報の組み合わせを使用する VLAN ID ベースの MAC 認証。
- MAC Move。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 Move 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。

QoS および CoS 機能

（注）　これらの機能には、LAN Base イメージが必要です。

- 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。
- ポートベースの信頼の自動 Quality of Service（QoS）VoIP 拡張と DSCP および出トラフィックのプライオリティ キューイング
- 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）。パケットがキューから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。

モニタ機能

- EOT および IP SLA EOT スタティック ルートのサポート。事前に設定したスタティック ルートまたは DHCP ルートがダウンした場合に特定します。
- 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。
- スイッチド ポート アナライザ（スイッチド ポート アナライザ（SPAN）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。（RSPAN には LAN Base イメージが必要です）
- 侵入検知システム（IDS）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。（RSPAN には LAN Base イメージが必要です）

- 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。
- 温度、電源状態、イーサネット ポートのステータスに関するアラームの処理機能が備わっています。
- 外部のリレー システムに使用できるアラーム リレー接点が備わっています。
- Digital Optical Monitoring（DOM; デジタル オプティカル モニタリング）。X2 SFP モジュールのステータスを確認します。

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、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 4 章「スイッチ セットアップの設定」および第 25 章「DHCP 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 4 章「スイッチ セットアップの設定」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 4 章「スイッチ セットアップの設定」および第 25 章「DHCP 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 6 章「スイッチ クラスタの設定」および Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。
- パスワードは定義されていません。詳細については、第 7 章「スイッチ管理の実行」を参照してください。
- システム名とプロンプトは *Switch* です。詳細については、第 7 章「スイッチ管理の実行」を参照してください。
- NTP はイネーブルに設定されています。詳細については、第 7 章「スイッチ管理の実行」を参照してください。

- DNS はイネーブルに設定されています。詳細については、第 7 章「スイッチ管理の実行」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 12 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 12 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 12 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 13 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 15 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 15 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 15 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 15 章「インターフェイス特性の設定」を参照してください。
- VLAN
  - デフォルト VLAN は VLAN 1 です。詳細については、第 17 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 17 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 17 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 18 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 18 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。詳細については、第 19 章「音声 VLAN 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 20 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 21 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 22 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。
- FlexLink は設定されていません。詳細については、第 24 章「FlexLink および MAC アドレステーブル移動更新の設定」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 25 章「DHCP 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 25 章「DHCP の設定」を参照してください。

- DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。詳細については、第 25 章「DHCP 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 26 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 28 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 28 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 28 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 28 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 29 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 29 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 29 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 29 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 32 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 33 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 34 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 35 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 36 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 37 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 38 章「標準 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 40 章「EtherChannel 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 41 章「スタティック 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。

（注）

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」（P.1-15）
- 「Ethernet-to-the-Factory アーキテクチャ」（P.1-16）

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ー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。

Ethernet-to-the-Factory アーキテクチャ

ここでは、Ethernet-to-the-Factory（EttF）アーキテクチャについて概説します。EttF は、オートメーション システムや制御システム内の装置やアプリケーションにネットワーク サービスとセキュリティ サービスを提供します。そして、それらをより大規模な企業ネットワークに統合します。

EttF アーキテクチャはさまざまなタイプの製造環境に応用できますが、産業タイプ、製造タイプ、および生産施設の規模に合わせて調整する必要があります。また、小規模ネットワーク（装置が 50 台未満）から中規模ネットワーク（装置が 200 台未満）および大規模ネットワーク（装置が最大 1000 台およびそれ以上）まで、さまざまな規模での配置が可能です。

EttF アーキテクチャには*ゾーン*と呼ばれる概念構造が含まれています。ゾーンとは、最上位となる企業レベルのスイッチおよびプロセスから、より詳細なプロセスを制御する最小の装置、あるいは工場のフロアにある装置に至るまでのさまざまな機能を区分するものです。図 1-1 を参照してください。

EttF アーキテクチャの詳細については、次の URL を参照してください。

http://www.cisco.com/web/strategy/manufacturing/ettf_overview.html

企業ゾーン

*企業ゾーン*は、一元管理されている IT システムと機能で構成されます。企業リソース管理サービス、企業間（B2B）サービス、企業/顧客間（B2C）サービスなどの企業ネットワーク サービスへの有線およびワイヤレス アクセスが可能です。サイト ビジネス プランニングやロジスティクスなどの基本的な

ビジネス管理作業はここで実行され、標準の IT サービスに依存します。ゲスト アクセス システムは多くの場合ここに置かれますが、企業レベルでは実現しにくい柔軟性を得るために、より下位レベルのフレームワークに置かれることも珍しくありません。

非武装ゾーン

非武装ゾーン（DMZ）は、企業ゾーンと製造ゾーンの間でデータやサービスを共有するためのバッファを提供します。DMZ では、可用性の維持、セキュリティ上の脆弱性への対処、および適合認定の義務の遵守を行います。DMZ は、たとえば IT 部門と生産部門を分けるなど、組織的な管理区分を提供します。組織ごとに異なるポリシーの適用や組み込みが可能です。たとえば、製造部門では、IT 部門と異なるセキュリティ ポリシーを製造ゾーンに適用できます。

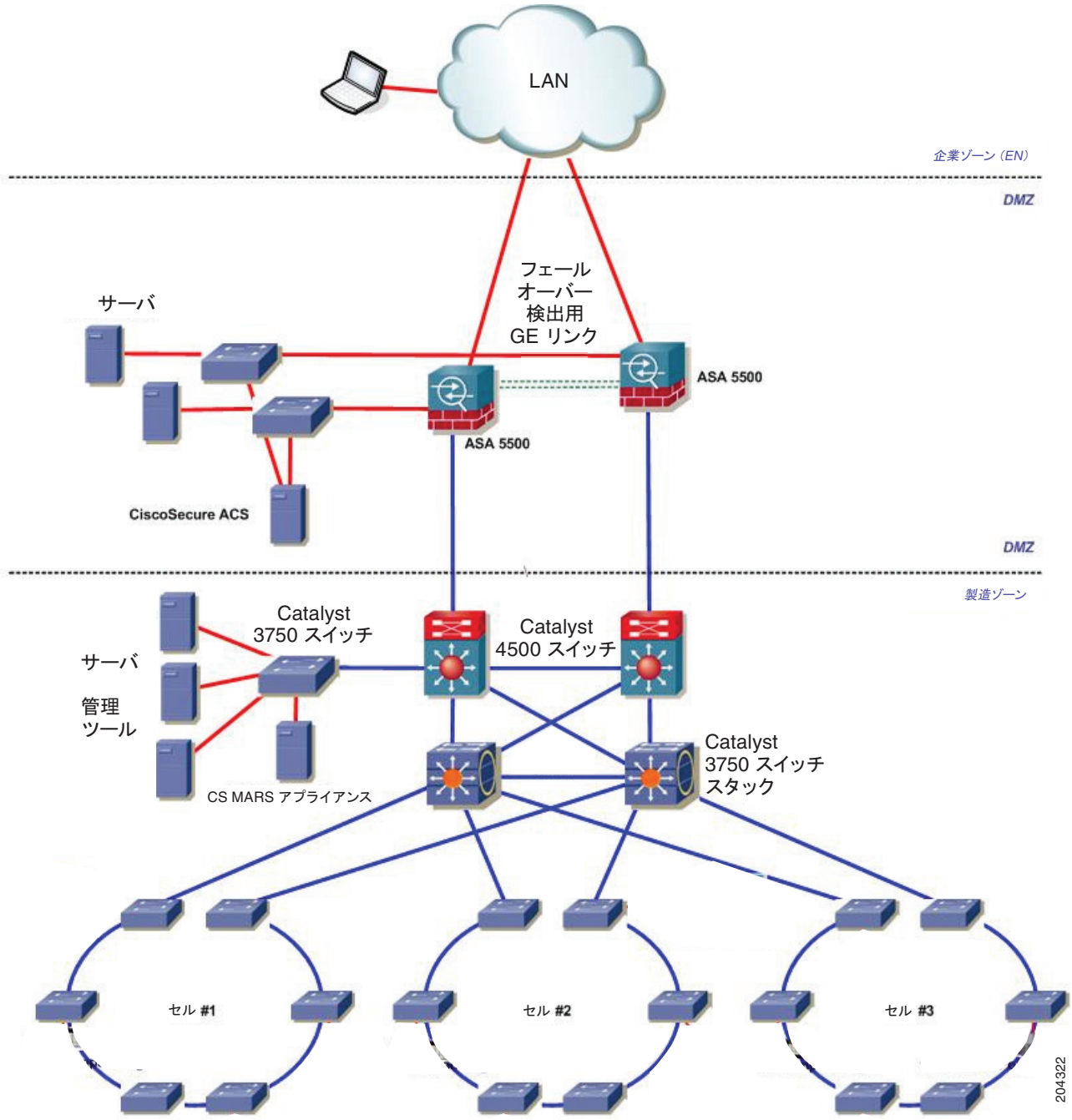
製造ゾーン

*製造ゾーン*は、セル ネットワークとサイトレベルのアクティビティで構成されます。工場のオペレーションをモニタするシステム、装置、コントローラはすべてこのゾーンに置かれます。生産施設内の 1 つの機能エリアを表すのが、セル ゾーンです。

セル ゾーンは、オートメーション プロセスの機能面をリアルタイムで制御する装置やコントローラなどで構成されます。これらはすべて互いにリアルタイム通信を行います。このゾーンは、工場や企業における他のレベルのオペレーションから明確に分離し、保護する必要があります。

図 1-1 に、EttF アーキテクチャを示します。

図 1-1　Ethernet-to-the-Factory アーキテクチャ



トポロジのオプション

トポロジの設計ではまず、装置をネットワークに接続する方法を検討します。セル ネットワークでは、生産フロアの物理的な制約に応じた物理トポロジも必要です。ここでは、トポロジの設計に関する注意事項を示し、トランク廃棄トポロジ、リング トポロジ、および冗長構成のスター トポロジについて説明します。

- 物理レイアウト：トポロジの設計は、生産環境のレイアウトに左右されます。たとえば、長いコンベアベルト システムにはトランク廃棄トポロジやリング トポロジが適していますが、冗長構成のスター トポロジは適していません。
- リアルタイム通信：遅延やジッターの主な発生原因は、トラフィックの量や、パケットが宛先に到達するまでに必要とするホップの数です。レイヤ 2 ネットワーク内のトラフィックの量はさまざまな要因に左右されますが、装置の数が重要となります。リアルタイム通信については、次の注意事項に従ってください。
  - レイヤ 2 ホップごとに生じる遅延の量を考慮してください。たとえば、100 Mb のインターフェイスを使用した場合は、1 ギガビットのインターフェイスを使用した場合に比べて遅延が大きくなります。
  - どのスイッチでも常に、帯域幅がインターフェイス キャパシティの 50% を継続的に超えることがないようにしてください。
  - CPU の使用率は、50 ～ 70% を継続的に超えることがないようにしてください。このレベルを超えると、スイッチが制御パケットを正しく処理できない可能性や、異常な動作をする可能性があります。

接続に関する主な考慮事項は次のとおりです。

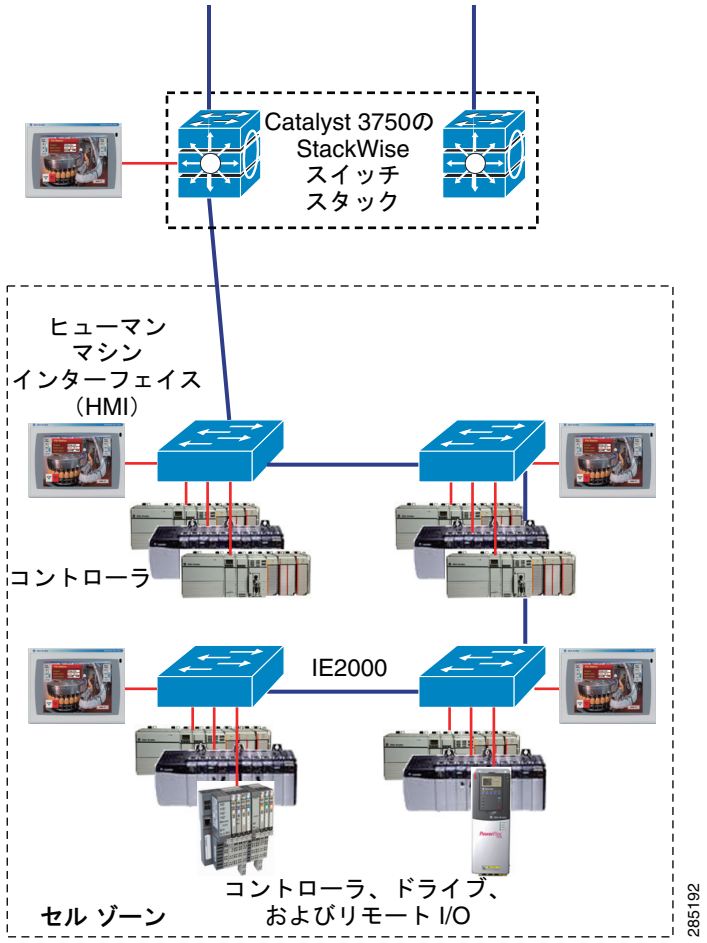
- 装置は、単一のネットワーク接続または IP 対応の I/O ブロックやリンク装置（イーサネットがサポートされていない場合）を通じてスイッチに接続されます。大半の装置にはフェールオーバー機能がないか、あっても機能が制限されているため、冗長構成のネットワーク接続を効果的に利用できません。
- 冗長構成の接続は、基幹インフラストラクチャに該当するプロセス関連の産業など、特定の産業やアプリケーションで利用されます。

セル ネットワーク：トランク廃棄トポロジ

*トランク廃棄*トポロジ（*カスケード*トポロジとも呼ばれる）では、スイッチが互いに接続され、スイッチ チェーンが形成されます。図 1-2 を参照してください。

- レイヤ 3 スイッチと最初のレイヤ 2 スイッチ間の接続はオーバーサブスクリプションの影響を受けやすく、これが発生するとネットワーク パフォーマンスが低下する可能性があります。
- 接続損失に対する冗長構成はありません。

図 1-2　セル ネットワーク：トランク廃棄トポロジ

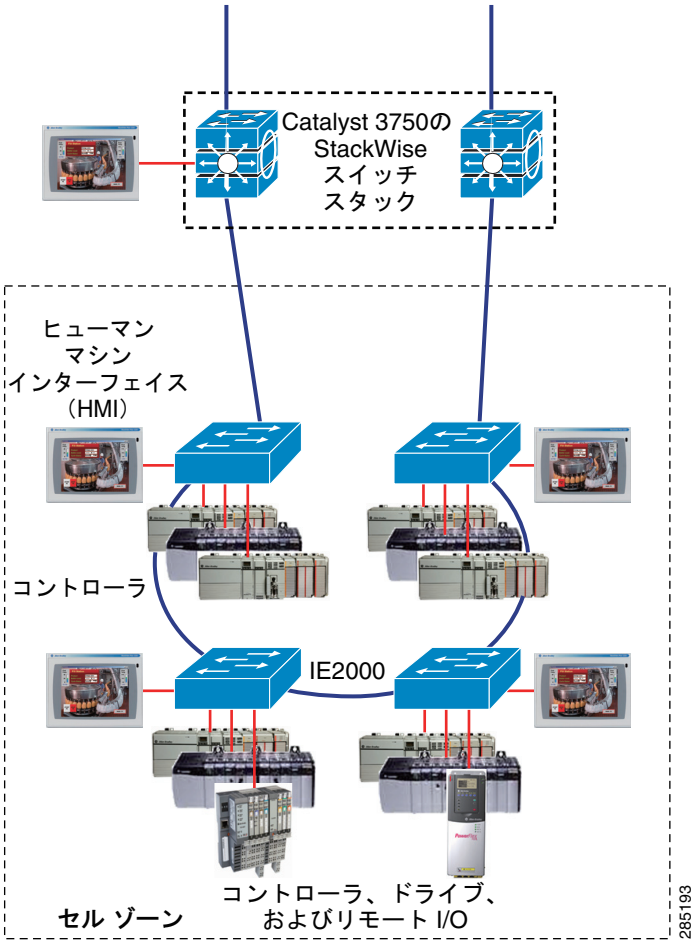


セル ネットワーク：リング トポロジ

リング トポロジはトランク廃棄トポロジと似ていますが、チェーンの最後のスイッチがレイヤ 3 スイッチに接続され、ネットワーク リングが形成される点が異なります。リング内で接続損失が発生しても、各スイッチは他のスイッチとの接続を維持します。図 1-3 を参照してください。

- ネットワークは、単一の接続損失からだけ回復できます。
- 追加プロトコルの実装と高速スパニングツリー プロトコル（RSTP）を必要とするため、このトポロジの実装は比較的難しくなります。
- トランク廃棄よりも優れていますが、リングの最上部（レイヤ 3 スイッチとの接続）がボトルネックになる可能性があります。この部分はオーバーサブスクリプションの影響を受けやすく、これが発生するとネットワーク パフォーマンスが低下する可能性があります。

図 1-3　セル ネットワーク：リング トポロジ

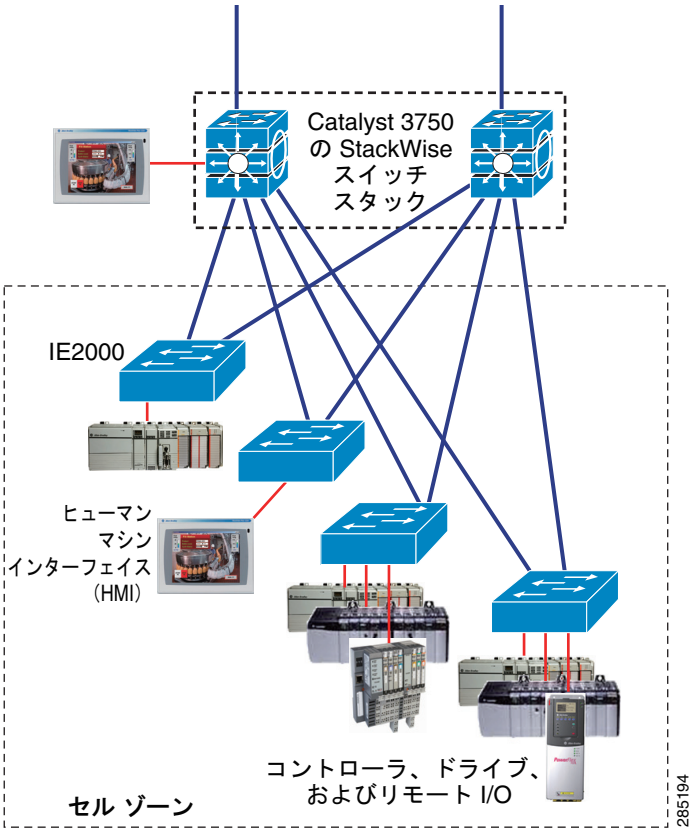


セル ネットワーク：冗長構成のスター トポロジ

冗長構成のスター トポロジでは、各レイヤ 2 アクセス スイッチがレイヤ 3 ディストリビューション スイッチにデュアル接続します。装置はレイヤ 2 スイッチに接続されます。図 1-4 を参照してください。

- どのレイヤ 2 スイッチでも、他のレイヤ 2 スイッチまでのホップ カウントは常に 2 つだけです。
- レイヤ 2 ネットワークでは、各スイッチがレイヤ 3 装置にデュアル接続します。
- 複数の接続損失が発生した場合でも、レイヤ 2 ネットワークは維持されます。

図 1-4　セル ネットワーク：冗長構成のスター トポロジ



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」
- 第 4 章「スイッチ セットアップの設定」

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