データシート

LANスイッチガイド

ネットワーク設計ガイドライン

ビジネスインフラを強固に実現するには、拡張性、安全性、管理性、可用性を考慮したネットワークデザインが重要です。
本章では、構内LANやIDC（Internet Data Center）で標準となっているCisco LANスイッチのモジュラーデザインとその設計のポイントを解説します。

モジュラーデザインによるネットワーク設計

ネットワークの設計は、将来の拡張性と管理の容易性を実現するため、ネットワーク全体を複数の論理階層に分け、階層ごとに機能を分散させる手法をとります。これを“ モジュラーデザイン ”と呼びます。この階層には、コア、ディストリビューション、アクセスの3種類があります。小中規模ネットワークにおいては、1台のスイッチで2つの階層を兼ねる場合があります。

コア

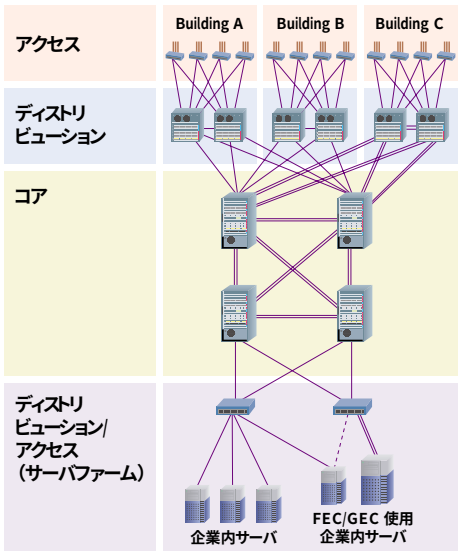
ディストリビューションスイッチを収容し、ネットワークのバックボーンとなります。高速大容量を処理でき、高い信頼性を持ったレイヤ2/3スイッチを設置します。

ディストリビューション

ディストリビューションアクセススイッチを収容し、コアスイッチに接続します。さまざまなサービスを提供できる高機能レイヤ2/3スイッチを設置します。パケットのルーティング、フィルタリング、監視、アクセス制限などの細かいサービスを提供します。

アクセス

アクセスクライアントPCやワークステーションを収容し、ディストリビューションスイッチに接続します。10/100Ethernetを多数収容できる高機能レイヤ2/3スイッチを設置します。



拡張性

―どうやって増え続ける通信量に対応しますか?―

企業のアプリケーションは常に変化をし続けています。また、新たなアプリケーションの登場は、通信量の増大や通信の質の変化をもたらします。したがって、ネットワークの設計時には、将来の拡張性を配慮しなければなりません。

固定型スイッチの拡張

Catalyst 2950シリーズ、Catalyst 3550シリーズは、複数台を組み合わせて仮想的に1台のスイッチとして動作させることができます。段階的に拡張されたいお客様には最適です。

モジュール型スイッチの拡張

Catalyst 6500シリーズは、スイッチファブリックモジュール※や分散フォワーディングカード※を追加することにより、さらに高速なスイッチへと進化させることができます。また、モジュールを交換するだけで、1ギガイーサネットから10ギガイーサネットへと帯域を拡張することが可能です。

※使用する構成に注意が必要です。

安全性 ーどうやってセキュリティを確保しますか?ー

同じ企業内でも部署や役職などによって、アクセスできる情報やサーバなどに制限が必要な場合があります。したがって、社外からのアクセスに対するセキュリティのみならず、企業内のセキュリティも十分考慮のうえ、設計する必要があります。

VLANトランク

VLANトランクを行うことで、単一の物理回線に複数のVLANを多重化することが可能になります。Ciscoが開発したISLの他に標準化されているIEEE802.1Qなどの技術があります。

Private VLAN

1つのVLAN(1つのIPアドレス体系)の中で、他のポートからレイヤ2レベルで隔離されているかのようにアクセスを制限できるVLANです。

アクセスコントロールリスト(ACL)

IPアドレスやポート番号を元に、アクセス制限をかけることができます。これにより、必要な通信だけを通過させることができます。

ファイアウォール

PIXファイアウォールと組み合わせることにより、ネットワークのセキュリティをさらに高めることができます。

不正アクセス検出(IDS)

Catalyst6500シリーズでは、不正アクセス検出用のIDSモジュールを組み込むことにより、シャーシ内の複数セグメントをシームレスに監視することができます。

端末認証

Cisco URT(User Registration Tool)やIEEE802.1xの認証機能を利用すると、ネットワークへのアクセス権を持たない者が、オフィス内のスイッチに端末を接続した場合に、一切の通信を拒否することが可能です。

管理性 ーどうやって管理しますか?ー

障害時の対処の容易性および平常時のネットワーク監視の容易性を考慮し、大規模ネットワークでは、データ系ネットワークと管理系ネットワークは分離させるのが一般的です。また、Ciscoの管理ツールにより、統合されたフレームワークで機器の管理が可能になります。

可用性 ーどうやってネットワークの障害に備えますか?ー

どの企業においても、いまやネットワークのダウンは業務の停止を意味し、ビジネスに多大な損害を与えます。そこで、ネットワークデザインに十分な障害対策を盛り込む必要があります。以下のようなCiscoのテクノロジーを活用すると、エンドツーエンドでネットワークの可用性を保つことができます。

■ スイッチの筐体内の二重化

【電源二重化】

Catalyst 4503/4506とCatalyst 6500シリーズでは、電源モジュールを複数台搭載し、二重化することが可能です。必要とされる電源容量を満たせば、1台の電源がダウンしても、スイッチはまったく問題なく動作し続けます。

【エンジン（CPU）モジュールの二重化】

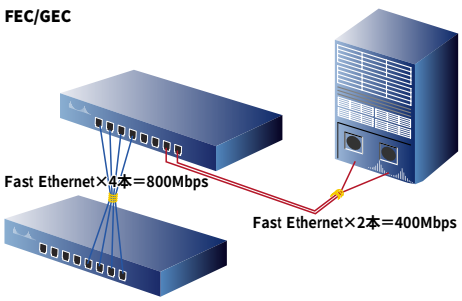
Catalystのエンジンモジュールは、Supervisorエンジンと呼ばれます。Catalyst 6500シリーズでは、このSupervisorエンジンを2枚搭載し、二重化することが可能です。1枚のSupervisorエンジンがダウンした場合、3秒以内にもう1枚のSupervisorエンジンに制御が切り替わり、スイッチは設定情報を引き継いで動作し続けます。

【インターフェイスの二重化】

モジュール型のCatalystは、10/100EthernetやGigabit Ethernetなどのインターフェイスモジュールを複数枚搭載できます。これにより、1枚のインターフェイスモジュールが障害を起こしてもネットワーク全体に影響を及ぼすことはありません。

【リンクの二重化（FEC/GEC/10GEC）】

Fast Ether Channel（FEC）やGiga Ether Channel（GEC）/10 Giga Ether Channel（10GEC）は、スイッチ間、スイッチとルータ間、スイッチとサーバ間でEthernetリンクを複数本束ね、論理的に1本の回線として処理する技術です。たとえば、Fast Ethernetを4本束ねた場合、通信速度は200Mbps（全二重）×4=800Mbpsになると同時に、仮に1本のケーブルが切れても、ネットワークトポロジの変化なしに1秒以内に残り3本で処理されるようになります。IEEEにおいては、802.3adとして標準化されています。



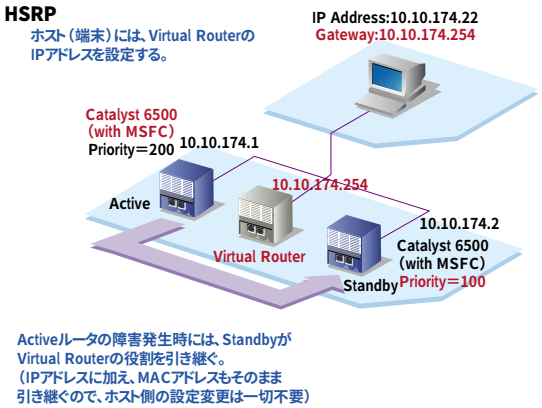
【モジュールのホットスワップ】

モジュール型のCatalystは、システムの稼動中にモジュールの抜き差しをしても、まったく問題なく動作し続けます。したがってシステムが稼動中であっても、モジュール交換などのメンテナンス作業が容易に行えます。

■ デフォルトゲートウェイの二重化

【HSRP】

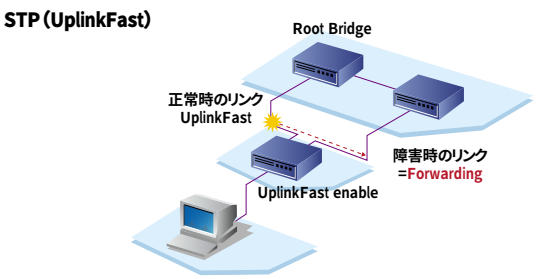
CiscoのHot Standby Router Protocol（HSRP）を使用することにより、2台のスイッチを仮想的に1台に見立て、筐体の二重化を行うことができます。HSRPの設定されたスイッチにつながるPCやルータは、それぞれ1つの仮想IPアドレス／仮想MACアドレスを参照します。スイッチ障害時は、数秒でスタンバイ側スイッチがこの仮想IPアドレス／仮想MACアドレスを引き継ぎ動作しますので、PCやルータなどのホストには設定変更が一切不要です。



■ ネットワーク経路の二重化

【STP】

Spanning Tree Protocol（STP）は、レイヤ2レベルで経路を二重化するのに使用します。LAN環境では主に、アクセススイッチとディストリビューションスイッチの接続で使用されます。通常のSTPは、障害時の切り替えに数十秒の時間がかかりますが、CiscoのUplinkFastの機能をアクセススイッチに設定することにより、アップリンクの障害時に5秒以内で経路を切り替えることができます。これらは、以前はCisco独自の仕様でしたが、近年IEEEにおいて標準化され、802.1w（RSTP:高速スパニングツリー）や802.1s（MSTP:多重スパニングツリー）として定義されています。



【ルーティングプロトコル】

Catalystは、RIPやOSPFといった標準的ルーティングプロトコルのみならず、強力なE-IGRPをサポートしています。これにより、レイヤ3でのネットワーク経路の柔軟で高速な切り替えが可能になります。

■ 負荷の分散

【サーバロードバランシング】

サーバへの極端なアクセス負荷を複数のサーバに分散させることで、1台のサーバのダウンがシステム全体に影響しないようにします。Catalyst 6500シリーズでは、IOSでの負荷分散だけでなく、専用のモジュールによりハードウェアでの負荷分散を実現しています。また、必要に応じてCSSシリーズなどのさらに高機能な負荷分散装置と組み合わせての利用も可能です。

■ 通信の優先制御

【Quality of Service（QoS）】

QoSを最適に設定することで、アプリケーションの特性に応じたネットワークサービスを提供することが可能になります。また、帯域幅の違いなどから発生する輻輳時にも、重要な通信の保護が可能になります。

CISCO SYSTEMS

シスコシステムズ株式会社
URL：http://www.cisco.com/jp/
問合せURL：http://www.cisco.com/jp/service/contactcenter/
〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館
TEL：03-6670-2992
電話でのお問合せは、以下の時間帯で受付けております。
平日10:00～12:00および13:00～17:00

03-11