概要

この章の内容は、次のとおりです。

- SAN スイッチングの概要, 1 ページ

SAN スイッチングの概要

この章では、Cisco NX-OS デバイスの SAN スイッチングの概要について説明します。 この章の内容は、次のとおりです。

ファイバ チャネル インターフェイス

ファイバ チャネル ポートは、Cisco Nexus 5000 シリーズ スイッチではオプションです。 拡張モジュールを使用した場合、使用可能なファイバ チャネル ポートは、Cisco Nexus 5010 スイッチで最大 8 個、Cisco Nexus 5020 スイッチで最大 16 個です。

それぞれのファイバチャネルポートは、サーバに接続されたダウンリンクとして、またはデータセンター SAN ファブリックへのアップリンクとして使用できます。

ドメイン パラメータ

Fibre Channel domain（fcdomain; ファイバ チャネル ドメイン）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。 ドメインは VSAN 単位で設定されます。 ドメイン ID を設定しない場合、ローカル スイッチはランダムな ID を使用します。

N ポート バーチャライゼーション

Cisco NX-OS ソフトウェアは業界標準の N Port Identifier Virtualization（NPIV; N ポート ID バーチャライゼーション）をサポートします。NPIV を使用すると、単一の物理ファイバ チャネル リンクで複数の N ポート ファブリックが同時にログインできます。 NPIV をサポートする HBA では、ホスト上の各仮想マシン（OS パーティション）についてゾーン分割とポート セキュリティを個別に設定できるようにすることで、SAN セキュリティを改善できます。 NPIV はサーバ接続に有効なだけでなく、コアおよびエッジの SAN スイッチ間の接続にも有効です。

N Port Virtualizer（NPV; N ポート バーチャライザ）は、コアエッジ SAN のファイバ チャネル ドメイン ID 数を減らすことができる補完的な機能です。 NPV モードで動作する Cisco MDS 9000

ファミリ ファブリック スイッチはファブリックに参加せず、コア スイッチ リンクとエンド デバイス間でトラフィックを通過させるだけです。このため、スイッチのドメイン ID は不要です。NPIV は、NPV コア スイッチへのリンクを共有する複数のエンド デバイスにログインするために、NPV モードのエッジ スイッチで使用されます。 この機能を使用できるのは、Cisco MDS ブレード スイッチ シリーズ、Cisco MDS 9124 マルチレイヤ ファブリック スイッチ、および Cisco MDS 9134 マルチレイヤ ファブリック スイッチだけです。

VSAN トランキング

トランキングは、「VSAN トランキング」とも呼ばれ、複数の VSAN 内で、同一の物理リンクを介して、ポートが相互接続してフレームを送受信することを可能にします。 トランキングは E ポートおよび F ポートでサポートされます。

SAN ポート チャネル

ポートチャネルは、ファイバ チャネルと FICON トラフィックの両方について、複数の物理 ISL を帯域幅が大きく、またポートの耐障害性が高い 1 つの論理リンクに集約します。 この機能を使用すると、最大 16 の拡張ポート（E ポート）またはトランキング E ポート（TE ポート）をポートチャネルにバンドルできます。 ISL ポートは任意のスイッチング モジュールに配置できるため、特定のマスター ポートは必要ありません。 ポートまたはスイッチング モジュールに障害が発生した場合、ファブリックを再設定しなくても、ポートチャネルは引き続き正常に機能します。

Cisco NX-OS ソフトウェアでは、隣接するスイッチ間でポートチャネル設定情報を交換するときにプロトコルを使用するので、ポートチャネル管理が簡易化されます。たとえば、誤設定の検出や、互換性のある ISL でのポートチャネルの自動作成などの管理機能です。 自動設定モードでは、互換性のあるパラメータを使用する ISL によって、チャネル グループが自動的に構成されます。手動操作は必要ありません。

ポートチャネルでは、発信元 FC-ID と宛先 FC-ID のハッシュ、さらにオプションで交換 ID を使用して、ファイバ チャネル トラフィックのロード バランスが実行されます。 ポートチャネルを使用するロード バランシングは、ファイバ チャネル リンクと FCIP リンクの両方で実行されます。 また、Cisco NX-OS ソフトウェアを設定して、コストが同じ複数の FSPF ルート間でロード バランスを実行することもできます。

仮想 SAN

仮想 SAN（VSAN）は、単一の物理 SAN を複数の VSAN に分割します。 VSAN を使用すると、Cisco NX-OS ソフトウェアで、大規模な物理ファブリックを個々の分離された環境に論理的に分割して、ファイバ チャネル SAN の拡張性、可用性、管理性、およびネットワーク セキュリティを高めることができます。

FICON の場合、VSAN により、FICON およびオープン システムのハードウェアベースの分離が容易になります。

それぞれの VSAN は、独自の一連のファイバ チャネル ファブリック サービスを持つ論理的および機能的に別個の SAN です。 ファブリック サービスのこの分割は、個々の VSAN 内にファブリック再設定およびエラー条件を含めることにより、ネットワークの不安定さを大幅に軽減します。 VSAN が実現する厳密なトラフィック分離は、特定の VSAN の制御およびデータ トラフィックを VSAN 独自のドメイン内に限定することにより、SAN セキュリティを高めることができます。 VSAN は、可用性を低下させることなく、分離された SAN アイランドを共通のインフラストラクチャに容易に統合できるようにすることで、コストを削減できます。

ユーザは、特定の VSAN の範囲内に限定される管理者ロールを作成できます。 たとえば、すべてのプラットフォーム固有の機能を設定できるネットワーク管理者ロールを設定する一方で、特定の VSAN 内のみで設定および管理ができるその他のロールを設定できます。 この手法は、スイッチ ポートまたは接続されたデバイスの WWN（World Wide Name）に基づいてメンバーシップを割り当てることができる、特定の VSAN に対するユーザ操作の効果を分離することにより、SAN の管理性を高め、人為的エラーを原因とする中断を減らします。

VSAN は、離れた場所にあるデバイスを含めるために VSAN を拡張する、SAN 間の Fibre Channel over IP（FCIP）リンク全体にわたりサポートされます。 Cisco SAN スイッチは、VSAN のトランキングも実装します。 トランキングでは、ISL（スイッチ間リンク）によって、同じ物理リンク上で複数の VSAN のトラフィックを伝送できます。

ゾーン分割

ゾーン分割は、SAN 内のデバイスのアクセス コントロールを提供します。 Cisco NX-OS ソフトウェアは、次の種類のゾーン分割をサポートしています。

- N ポート ゾーン分割：エンドデバイス（ホストおよびストレージ）ポートに基づいてゾーン メンバを定義します。
  - WWN
  - ファイバ チャネル ID（FC-ID）
- Fx ポート ゾーン分割：スイッチ ポートに基づいてゾーン メンバを定義します。
  - WWN
  - WWN およびインターフェイス インデックス、またはドメイン ID およびインターフェイス インデックス
- ドメイン ID およびポート番号（Brocade の相互運用性用）。
- iSCSI ゾーン分割：ホスト ゾーンに基づいてゾーン メンバを定義します。
  - iSCSI 名
  - IP アドレス
- LUN ゾーン分割：N ポート ゾーン分割、論理ユニット番号（LUN）ゾーン分割と組み合わせて、特定のホストのみが LUN にアクセスできるようにし、異種ストレージ サブシステム アクセスを管理するための制御のシングル ポイントを提供します。
- 読み取り専用ゾーン：属性を設定して、任意のゾーン タイプでの I/O 操作を SCSI 読み取り専用コマンドに制限できます。 この機能は、バックアップ、データ ウェアハウジングなど、サーバ間でボリュームを共有する場合に役立ちます。
- ブロードキャスト ゾーン：任意のゾーン タイプ用の属性を設定して、ブロードキャスト フレームを特定のゾーンのメンバに制限できます。

厳密なネットワーク セキュリティを実現するため、入力スイッチで適用されるアクセス コントロール リスト（ACL）を使用して、ゾーン分割はフレームごとに常に適用されます。 すべての

ゾーン分割ポリシーはハードウェアで適用され、パフォーマンスの低下を引き起こすことはありません。 拡張ゾーン分割セッション管理機能では、一度に 1 人のユーザだけがゾーンを変更できるようにすることで、セキュリティがさらに高まります。

デバイス エイリアス サービス

ソフトウェアでは、VSAN 単位およびファブリック全体のデバイス エイリアス サービス（デバイス エイリアス）がサポートされます。 デバイス エイリアス配信により、エイリアス名を手動で再度入力することなく、VSAN 間で HBA（ホスト バス アダプタ）を移動できます。

ファイバ チャネル ルーティング

Fabric Shortest Path First（FSPF）は、ファイバ チャネル ファブリックで使用されるプロトコルです。 FSPF は、どのファイバ チャネル スイッチでも、デフォルトでイネーブルになっています。特に考慮が必要な設定を除いて、FSPF サービスを設定する必要はありません。 FSPF はファブリック内の任意の 2 つのスイッチ間の最適パスを自動的に計算します。 特に、FSPF は次の機能を実行するために使用されます。

- 任意の 2 つのスイッチ間の最短かつ最速のパスを確立して、ファブリック内のルートを動的に計算します。
- 特定のパスで障害が発生した場合は、代替パスを選択します。 FSPF は複数のパスをサポートし、障害リンクを迂回する代替パスを自動的に計算します。 2 つの同等パスを使用できる場合は、推奨ルートを設定します。

SCSI ターゲット

SCSI ターゲットにはディスク、テープ、およびその他のストレージ デバイスが含まれます。 これらのターゲットは、ネーム サーバに論理ユニット番号（LUN）を登録しません。 SCSI LUN 検出機能は、CLI（コマンドライン インターフェイス）または SNMP（簡易ネットワーク管理プロトコル）を通して、オンデマンドで開始されます。 隣接スイッチが Cisco Nexus 5000 シリーズに含まれる場合、この情報はこれらのスイッチとも同期されます。

拡張ファイバ チャネル機能

分散サービス、エラー検出、およびリソース割り当てのためにファイバチャネルプロトコル関連タイマーの値を設定できます。

単一のスイッチに WWN を一意に関連付ける必要があります。 主要スイッチの選択およびドメイン ID の割り当ては、WWN に依存します。Cisco Nexus 5000 シリーズ スイッチは、3 つの Network Address Authority（NAA）アドレス フォーマットをサポートします。

ファイバ チャネル標準では、任意のスイッチの F ポートに接続された N ポートに、一意の FC ID を割り当てる必要があります。 使用する FC ID 数を節約するために、Cisco Nexus 5000 シリーズ スイッチは特殊な割り当て方式を使用します。

FC-SP および DHCHAP

Fibre Channel Security Protocol（FC-SP）は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。 Diffie-Hellman チャレンジ ハンドシェイク認証プロトコル（DHCHAP）は、Cisco SAN スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。 DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

FC-SP により、スイッチ、ストレージ デバイス、およびホストは、信頼性の高い管理可能な認証メカニズムを使用して、それぞれのアイデンティティを証明できます。 FC-SP の使用により、ファイバチャネル トラフィックをフレーム単位で保護することで、信頼できないリンクであってもスヌーピングやハイジャックを防止できます。 ポリシーと管理アクションの一貫した組み合わせがファブリックを介して伝播されて、ファブリック全体での均一なレベルのセキュリティが実現します。

ポート セキュリティ

ポート セキュリティ機能は、1 つ以上の所定のスイッチ ポートへのアクセス権を持つ特定の World-Wide Name（WWN）をバインドすることによって、スイッチ ポートへの不正なアクセスを防止します。

スイッチ ポートでポート セキュリティをイネーブルにしている場合は、そのポートに接続するすべてのデバイスがポート セキュリティ データベースになければならず、所定のポートにバインドされているものとしてデータベースに記されている必要があります。 これらの両方の基準を満たしていないと、ポートは動作上アクティブな状態にならず、ポートに接続しているデバイスは SAN へのアクセスを拒否されます。

ファブリック バインディング

ファブリック バインディングは、ファブリック バインディング設定で指定されたスイッチ間のみでスイッチ間リンク（ISL）がイネーブルにされるようにします。これによって、無許可のスイッチが、ファブリックに参加したり、現在のファブリック処理が中断したりできないようにします。この機能では、Exchange Fabric Membership Data（EEMD）プロトコルを使用することによって、許可されたスイッチのリストがファブリック内の全スイッチで同一になります。

Fabric Configuration Server

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素のコンフィギュレーション情報リポジトリを維持したりすることができます。 通常、管理アプリケーションは N ポートを通してスイッチの FCS に接続されます。 複数の VSAN がファブリックを構成し、VSAN ごとに 1 つの FCS インスタンスが存在します。