

特長

- 小規模サイト用に設計され、さまざまな低コスト 1/10 ギガビット イーサネットプラットフォームで、フル装備のネットワーク仮想化機能を提供
- ネットワーク上のコンパクトなエッジデバイスで、複数の複雑なプロトコルを管理せずに、複数のサービスを提供
- 小規模オフィス向けにネットワーク仮想化テクノロジーを容易に利用でき、規制上またはセキュリティ上の要請に応じてトラフィックを分離
- マルチ・テナント環境で豊富なマルチ・サービス機能を提供し、各テナントのトラフィックの分離や保護を促進
- 従来のルーティング IP とファブリック・ベースのネットワークング配備の両方をサポート



Virtual Services Platform 4000

ファブリック対応のマルチサービス エッジ デバイスが、ネットワークをエンド・トゥ・エンドでシンプルに

Extreme Virtual Services Platform (VSP) 4000 があれば、ネットワークがシンプルになります。VSP 4000 は、Extreme Fabric Connect テクノロジーをブランチやネットワーク エッジに拡張し、しかも、その充実したネットワーク仮想化機能を、小規模エリアに最適な低価格の 1/10 ギガビット プラットフォームで実現します。VSP 4000 は複数のプロトコルを配備せずに、豊富なマルチサービス機能を提供できるため、シンプルかつ効率的にネットワークを構築して管理できます。

小規模オフィスに配備したネットワークを、ファブリック テクノロジーで広域エッジ、メトロ エッジ、またはキャンパス エッジまで拡張する必要がある場合、または法規制やセキュリティ上の理由からあるいは複数の顧客をサポートするために、トラフィックの分離が必要な場合、VSP 4000 は小規模エリア用の費用対効果の高いプラットフォームとして、豊富なマルチサービスとマルチ・テナント機能を実現します。

ネットワーク構築の新しい方法

先ごろエクストリームが IT マネージャーを対象に行った調査では、多くのネットワークが複雑であることを反映し、全回答者の 41% が単純なネットワーク変更の実装に 1 か月以上かかると答えました。これは驚くには当たりません。というのも、たとえば移動、追加、変更でさえ、往々にしてネットワーク全体の構成が必要になるため、簡単には行えないからです。厳格な設計ルールと無数のプロトコルが関係する場合、1 つを修正すると、別のところに支障が生じる可能性があります。必要なのは、スピーディで俊敏かつ柔軟にネットワークを構成できることです。特に、ビデオ、モビリティ、クラウド コンピューティング、ビッグ データ、アプリケーションやエンド デバイスの急速な進化など、巨大なトレンドを取り込む場合はこの点が重要になります。

Switch Cluster: 回復性の向上、可用性の強化

エクストリームは、10 年以上も前に、Switch Cluster テクノロジーの開発により、世界に先駆けて高可用性ネットワークの概念を構築しました。物理的に独立した 2 台のスイッチをクラスタ化して単一の統合された論理的コアを作成すれば、単一障害点が解消されるため、1 か所の障害だけでデュアル / マルチ・ホーム接続が中断することがなくなります。この仕組みは、エンド・トゥ・エンドで常時稼働するための可用性の中核をなします。Switch Cluster テクノロジーをコアに配備すると、ネットワーク エッジで高可用性が実現し、コアやデータ センターでキャンパス ネットワークのワイヤリング クローゼットや、サーバ、ルータなどのネットワーク デバイスがサポートされます。

Switch Cluster テクノロジーは、スプリット マルチ・リンク トランッキング プロトコルを使用して構築されます。このプロトコルは、エクストリーム製品のみにも搭載されていますが、サードパーティのスイッチ、サーバ、アプライアンス、ルータと完全にやり取りすることができます。このことには、現実の価値をもたらすいくつかのメリットがあります。競合他社は特定の個別要素に似た製品を提供することはできるかもしれませんが、当社製品は組み合わせた場合の機能において競合製品の追随を許さず、特にシンプルさと効率性に優れています。

Switch Cluster は、単にスイッチだけでなく、広く拡張できる相互運用可能なソリューションを実現します。そのため、高可用性はスイッチング ネットワーク（スイッチ自体とその直接リンク）に留まることなく、ネットワーク全体に波及します。重要なのは、アタッチされたサーバ、アプライアンス、WAN ルータなどにも高可用性が及ぶことです。これが競合製品との決定的な違いで、競合製品は、純粋にスイッチ ドメイン内の相互作用に基づいており、アプリケーション ホスト自体には効果が及びません。競合製品は、ほとんどが何らかの形のスパンニング ツリー プロトコル (STP) に基づいていますが、STP のサポートはスイッチのみに限られ、他のデバイスがサポートすることはほとんどありません。競合他社のソリューションでは、アクティブな回復性テクノロジーからサーバが除外されているため、高可用性をアプリケーションに拡張することはできません。Switch Cluster テクノロジーは STP に依存せず、基本的でユビキタスな技術であるリンク アグリゲーションを利用するすべてのデバイスにサポートを拡張します。Switch Cluster にアタッチされたデバイスは、複数の物理リンクを使用して仮想接続を形成します。これにより、回復性が向上するとともに、キャパシティが拡大します。

高可用性の実現、およびインサービス メンテナンスと最適化されたパフォーマンスの支援は、Switch Cluster テクノロジーの機能として広く認識されています。1 秒未満のフェイルオーバーや復旧を可能にすることは、今なおきわめて重要であり、おそらくはこれまで以上に重要ですが、必ずしも特定の機能でなければ実現できないわけではありません。STP の拡張機能である高速再構成を積極的に構成すれば、同様のレベルのフェイルオーバー パフォーマンスが得られます。

ただし、STP のすべての機能は、ネットワーク トポロジの変化を検出してそれに反応するという概念に依然として結び付いています。そのため、ネットワークは特定のデバイス（ルート ブリッジなど）の信頼性と可用性にきわめて敏感に左右されます。エクストリームの Switch Cluster テクノロジーは、ミラーリングされたデバイスと仮想化機能の概念を中心に構築されています。

Switch Cluster テクノロジーは、非常に効果的であるため、計画メンテナンスや障害によってすべてのスイッチが停止しても、全体としてアプリケーションの可用性を失うことなく対応できます。

従来のネットワーク	Fabric Connect
複雑: <ul style="list-style-type: none"> 複数のプロトコル (STP, RIP, OSPF, BGP, PIM) ネットワーク設計ルール 追加、移動、変更の手順が複雑 ネットワーク全体の構成 (STP グループ、VLAN、ホップ バイ ホップ) 	シンプル: <ul style="list-style-type: none"> 単一のプロトコル (IS-IS)、設計の柔軟性 (物理的トポロジ独立、どこにでも必要な場所にサービスを追加可能) スピーディに追加、移動、変更 新規サービスやサービスの変更は、1つのコマンドでエンドポイントにプロビジョニング
リソースの利用率が不十分 (ブロックされたポート)	リソースの効率的な使用 (ポートのブロックなし、発信元から宛先まで最適化された最短遅延パスを使用)
復旧に時間がかかる (通常、数秒)	1 秒未満に復旧

Switch Cluster テクノロジーは、従来の手順 (物理的接続) によって実装できますが、テクノロジーの進化により、“仮想 IST” による実装も可能です。これはスイッチ間トランク機能の拡張機能で、従来の物理的リンク経由ではなく、クラスタ メンバー間の仮想接続を利用します。これにより、実装の柔軟性が向上し、高価なバックボーン接続の使用が最適化されるとともに、さらなる開発の基盤が形成されます。このような基盤には、メンバーを 3 台以上に拡大できるクラスタのスケーラビリティや、クラスタ内でさまざまなデバイス タイプを組み合わせ使用できる機能が含まれます。

仮想 IST (vIST) は優れたスケーラビリティを備え、リスクなしに購入を決断できるソリューションです。コアは常時稼働の高可用性を提供します。また、規模を柔軟に調整でき、規模に応じた金額だけを支払って効率的に使用できます。

エクストリームの Switch Cluster テクノロジーは、優れたネットワーク回復性を備えており、これによってもインサービス メンテナンスが容易になります。ネットワーク事業者は、Switch Cluster の決定論的性質を利用してネットワークを区切ることで、重要なサービスの回復性をさらに強化できるとともに、付随するコンポーネントやアプリケーションにサービス復旧作業の影響を及ぼさずに、個々の障害をリアル・タイムで修復できます。

Fabric Connect: 複雑さの軽減と能力の向上

これまで、新しいサービスをプロビジョニングする場合または既存のサービスを変更する場合、エンジニアはサービスパスに含まれるすべてのデバイスを設定し、すべてのデバイスのアクティブリンクと冗長リンクの両方を有効にしなければなりませんでした。ネットワークが大きいほど、この作業は複雑になり、リスクも大きくなります。

Extreme Fabric Connect テクノロジは、IEEE 802.1aq と IETF RFC 6329 の最短パスブリッジング (SPB) 規格に、Extreme Networks による拡張機能 (企業に特化した最適化) を追加した拡張実装に基づいています。このテクノロジにより、要素を動的に仮想化できるシンプルなネットワークを作成でき、効率的なプロビジョニングとリソース利用が可能になります。この結果、ネットワークと IT 担当者のストレスが軽減します。

Fabric Connect テクノロジを利用したネットワークの仮想化は、根本的な変化をもたらします。ネットワークは、個々のデバイスを集めた集合体ではなく、不透明なクラウドとなります。これにより、エンジニアはエンド・ポイントまで直接サービスを提供する単一のユニーク デバイスを設定するだけで済みます。Fabric Connect テクノロジによって、クラウド内の他のすべてのノードに、すべてのサービス属性が自動的にかつ瞬時に伝達され、エンド・トゥ・エンドの接続が実現します。

このようにフォールト・トレラントでパワフル、かつ自己認識型のエンド・トゥ・エンドのファブリックが作成されるため、このテクノロジを採用したソリューションでは、サービスのプロビジョニングが境界での作業だけで完結します。メリットは即座に顕著な効果を及ぼします。管理作業が減少し、エラーが回避され、サービス開始までの所要時間が大幅に改善されます。この基盤テクノロジのメリットは、デバイス、リンク、プロトコルをマスクし、複数のエンド・ポイントに接続性を提供する論理的な拡張イーサネット LAN 実現する点です。これは単純な概念ですが、興味深い、きわめてユニークな方法で実現されています。Fabric Connect は、IS-IS (Intermediate System-to-Intermediate System) という動的リンク状態ルーティング プロトコルを利用し、標準化された拡張機能によって、ドメイン内のすべてのノード間でトポロジ、接続性、デバイス情報が共有されます。各ノードが、宛先までの最適パスを含め、自己認識した独自のネットワーク情報を持つため、高度な分散型で動的に管理するソリューションが構築されます。Fabric Connect テクノロジには、トラフィックを別々のサービス構築に分離および分割できるというメリットもあります。

これにより、クレジット カード決済 (PCI) や医療データの保護 (HIPAA) に対応した特別な取り扱いが必要な場合などの、ビジネス プロセスへの準拠を支援する "ステルス ネットワーキング" ソリューションが可能になります。

トラフィックの分離: 従来のネットワーク	トラフィックの分離: Fabric Connect
<p>MPLS ベースの分離</p> <ul style="list-style-type: none">複雑:<ul style="list-style-type: none">複数のプロトコル (IGP、BGP、MPLS)構成が複雑 (VRF、IGP、iBGP、MPBGP、ルート ターゲット、ルート識別子)テナントの移動、追加、変更が複雑復旧に時間がかかる (通常は数秒) <p>VLAN ベースの分離</p> <ul style="list-style-type: none">真のトラフィック分離ではないセキュリティ侵害に対して脆弱 (VLAN ジャンピング)	<p>Extreme Fabric Connect</p> <ul style="list-style-type: none">シンプル:<ul style="list-style-type: none">単一のプロトコル (IS-IS)構成が容易 (VRF による ISID)テナントの移動、追加、変更が容易迅速な復旧 (1 秒未満)真のトラフィック分離として法規制の要件を充足よりセキュアな (MAC-in-MAC) のカプセル化により、VLAN ジャンピングの防止に役立つ

ネットワーク セグメンテーションとは、各サービスが個別にカプセル化され、他のすべてのサービスから独立して実行されることを意味します。単一の統一プロトコルと併せて統合 IP ルーティングと IP マルチキャスト機能を利用することにより、Fabric Connect は、シンプルでスケーラビリティに優れた、回復性のある IP マルチキャスト・ベースのアプリケーションのための業界最高クラスのソリューションをもたらすことができます。またエッジのみのプロビジョニング モデルによって、ネットワークと仮想マシン モビリティ間の連携が大幅に向上します。レイヤー 2 VLAN は、サイトが 1 か所であっても複数であっても、コアまたはデータ センター全体に簡単かつシームレスに拡張できます。また、トラフィック フローは、利用可能なすべてのリンク全体で自動的に負荷分散され、保護が強化されます。

Fabric Connect デバイスは、複数のユーザ・ネットワーク・インターフェイス (UNI) タイプをサポートして、俊敏な配備機能を提供します。以下にこれらの UNI を示します。

- VLAN UNI (C-VLAN): ノード固有の VLAN ID が L2 仮想サービス ネットワーク (VSN) にマッピングされます。これにより、この VLAN に関連付けられたそのノード上のすべての物理ポートが、サービスに関連付けられます。
- フレックス UNI には、以下のサブ・タイプがあります。
 - スイッチド UNI: VLAN ID とポートの組み合わせが L2 VSN にマッピングされます。この UNI タイプでは、VLAN ID を他のポートで再利用できるため、異なる VSN にマッピングできます。
 - トランスペアレント ポート UNI: 物理ポートが L2 VSN にマッピングされます。そのポートを通過するすべてのトラフィック (802.1Q タグ付きまたはタグなし、入力および出力) がその VSN にマッピングされます。

- E ツリー UNI: プライベート VLAN が1つのノードを超えて拡大し、ネットワーク全体に及ぶ E ツリー サービス インフラストラクチャを形成します。1つの E ツリー UNI が1つの L2 VSN となります。ブロードキャスト トラフィックは、ハブ サイトからスポーク サイトへ、スポークからハブへと伝送されますが、スポーク サイト間では伝送されません。E ツリー ハブは、任意の VLAN UNI で形成できますが、E ツリー スポークはプライベート VLAN UNI として構成する必要があります。
- L3 VSN UNI: ノード固有の VRF が L3 VSN にマッピングされ、すべてのノードが同じ VSN に属する L3 ルートが制御プレーンによって交換されます。同じネットワーク内の同じ L3 VSN を共有するすべての VRF によって、有効に L3 VPN が形成されます。L3 VSN は、IP ユニキャストと IP マルチキャストの両方を同時にサポートするように構成できます。

自律型仮想ネットワークに移行することで、決定的なメリットが得られます。サービスに変更を加えるたびに、ネットワークのコアを構成する必要がなくなります。またサービスはネットワークのエッジで構成するだけで済みます。このことは、変更パラダイム全体に劇的な影響を与えます。

Fabric Connect は、そのシンプルなネットワーク構築方法と優れた運用方法で高い評価を集めています。エクストリームの委託に基づく第三者機関の調査によると、Fabric Connect の配備環境では、実装時間が最大 91%、変更のための待機時間が最大 66%、

構成とトラブルシューティングの両方で、所要時間が 85% 短縮しています。また、Fabric Connect の強力な回復力によってフェイルオーバー時間が 2,500 分の 1 以下に改善され、人的ミスによる機能停止がほとんど皆無になりました。

Fabric Attach: サービス自動化を完成させる最後のピース

サービス自動化は、IT の究極の目標です。ビジネス システムやビジネス プロセスをリアル・タイムで開始、移動、廃止できるソリューションを作成することにより、IT がビジネスの障害ではなく、ビジネスを支援する存在に変わります。エクストリームは、自動化の完成において最後まで残っていた重要部分である、エンド・ポイント デバイスと仮想ネットワークの接続を処理するテクノロジーを開発しました。

Extreme Fabric Connect テクノロジーは、ネットワークに数々重要なメリットをもたらします。エクストリームの委託により第三者機関が実施した "Fabric Connect 顧客エクスペリエンス調査" では、複数の領域で目覚ましい改善が示されており、実装、構成、トラブルシューティング所要時間、復元、エラーによる中断がすべて改善されています。

Fabric Connect は、基盤である最短パス ブリッジング プロトコルの能力を利用して、これらのメリットを提供することができます。

これをはじめとする特徴により、サービスの定義はネットワーク エッジだけで済み、従来のようにリンクごと、デバイスごとに構成を変更する必要はありません。従来のネットワークでサービスの配備に時間がかかり、望ましくないリスクが発生するのは、主として、このような変更が必要なためです。

しかし、まだ課題が残っています。高度に仮想化されたネットワークのシナリオで、拡大を続ける大規模で多様なユーザ ベースとエンド・ポイント デバイスに自動アタッチ機能を提供するという課題です。あらゆるソリューションは柔軟でオープンでなければなりません。また多様なトラフィック フローを最大限に分離し、配慮を要するまたはミッション・クリティカルなネットワークの不必要な露出を最小限に抑えるという要望（場合によっては必須の要件）を満たす必要があります。

IP マルチキャスト: 従来の IP	IP マルチキャスト: Fabric Connect
複雑: • 複数のプロトコル (PIM over OSPF) • 運用とトラブルシューティングが複雑 (独自仕様のツール) • ネットワーク全体の構成 (ブートストラップ ルータ、ランデブーポイント)	シンプル: • 単一のプロトコル (IS-IS) • 運用とトラブルシューティングが容易 (IEEE 802.1 ag 拡張) • 単一のコマンドによるエンドポイントの構成
障害からの復旧に数秒から数分かかる	迅速な復旧 (1 秒未満)
限られた拡張性 (数百のストリーム)	強力な拡張性 (数万のストリーム)

ここで、課題をさらに具体的に説明しましょう。少なくとも何らかのレベルの自動アタッチ機能を実装するという概念は、新しいものではありません。これまでも個別のベンダー レベルで MAC ベースや RADIUS ベースのソリューションが開発され、業界レベルで協力して 802.1X 拡張可能認証プロトコルなどのオープン ソリューションが作成されました。さらに最近では、802.1AB リンク レイヤー検出プロトコル/メディア拡張が、VoIP/ユニファイド コミュニケーション アプリケーションの配備を支援しています。

ただし、それらのアプローチは、ネットワーク エッジにすべてのネットワーク セグメントへのアクセスが既にプロビジョニングされていること (通常、仮想 LAN (VLAN) としての実装) を前提としています。この前提に当てはまらない場合が増加しています。このアプローチは、ネットワークが基本的に単一の "データ" ネットワークであって、その後、単一の "音声" ネットワークが追加された頃には適切であったかもしれません。

この課題に対応するため、エクストリームでは Fabric Attach を開発しました。これは、エンド・ポイント デバイスの自動アタッチメント（規格用語で言うところの "自動アタッチ"）を容易にする標準ベースの機能です。Fabric Attach を利用することで、エンド・ポイントを動的に配備し、必要に応じて一意のネットワーク サービスを一時的にエッジまで拡張できます。自動アタッチされたエンド・ポイント デバイスは、適切なネットワーク リソースに接続されます。これは通常、Fabric Connect 仮想サービス ネットワーク (VSN) が従来の VLAN になります。Fabric Attach 機能は、"イネーブルド エッジ" と呼ばれる Extreme Fabric ベースのアーキテクチャの基本的概念を提供します。

Fabric Attach は、汎用 IT エンド・ポイント デバイス、ネットワーク デバイス、コンピューティング リソース、ビジネス中心型 IoT（モノのインターネット）エンド・ポイント デバイスの配備を効率化するように設計されています。Fabric Attach では、非常に簡単な方法で、これらのデバイスを適切なネットワーク セグメントに割り当てることができ、必要に応じて、アクティブな有効セッションの間のみ、セグメントのプレゼンスがエッジ ノードまで拡張されます。Fabric Attach はまた、詳細なビジネス主導型ポリシーの実装によって、高度なサービス差別化を行うこともできます。

Fabric Attach は、従来のエンド・ポイント デバイスとネットワークの間で "ゲートウェイ" の自動化機能を作成することでその役割を果たします。通常、ネットワークは Fabric Connect プライベート クラウドですが、Fabric Attach は標準ベースであるため、従来の 802.1Q VLAN ベースのネットワークでも同様に機能します。Fabric Attach コンポーネント間のシグナリングの受け渡しには、802.1AB リンク レイヤー検出プロトコルが使用されているため、きわめて柔軟で、拡張性と移植性に優れています。Fabric Attach は、IETF に標準規格としての採用を申請中です。エクストリームはまた Wind River と協力して、Fabric Attach を Open vSwitch オープン ソース開発プロジェクトに提供しています。

自動アタッチを容易にするためには、ネットワーク エッジ、つまりエンド・ポイント デバイスが最初に接続され、最も可視性の高い部分が重要になります。ここには、Fabric Attach クライアント (FA クライアント) エージェントと呼ばれる、複数の方法で柔軟に実装できるソフトウェア コードが配置されます。FA クライアントは、以下の形態で実装できます。

- Extreme イーサネット アクセス スイッチに実装し、従来のエンド・ポイント デバイス（汎用 PC、IP 電話、プリンタ、IP カメラなど）を検出し、カスタマイズされたネットワーク サービス接続と属性を拡張する。
- ExtremeWireless LAN アクセス ポイントに実装し、シンプルなハンズ・フリー配備、サービス提供、デバイス接続を支援する。

- Wind River との協働関係を利用：あらゆる Open vSwitch ベースのデバイス システム (Xen、KVM、VirtualBox ハイパーバイザなど)、新しい Extreme Open Networking Adapter 製品ライン。
- IETF 申請を利用：準拠した実装方法で動作するあらゆるエンド・ポイント デバイスまたはネットワーク デバイス（サードパーティ製スイッチ、任意のイーサネット対応のネットワーク デバイスを含む）。

FA クライアントはそれぞれ、特定のネットワーク サービス（特定の VSN ID、VLAN ID など）を要求することも、単純に汎用の要求のみを行って、一元的ポリシーの割り当てにゆだねることもできます。たとえば、IP 電話はデフォルトで "音声 VLAN" に割り当て、IP カメラはハードウェア アドレッシングによって認識して、"ビデオ セキュリティ VLAN" に割り当てることができます。さらに仮想マシンは、起動時にアプリケーション固有のネットワーク割り当てを要求することができます。Fabric Attach は、MAC ベースや RADIUS ベース、802.1X、802.1AB など、デバイスの認識、認可、認証に使用される既存の手法を補完し、これらを活用してネットワークのプロビジョニングとポリシーの適用に取り入れることができます。

FA クライアント は、LLDP 拡張を使用して、Fabric Attach サーバ (FA サーバ) と直接、または Fabric Attach プロキシ (FA プロキシ) 経由で通信します。FA プロキシは、従来型のネットワーク スイッチです。トポロジの必要に応じて、また必要な場合に配備され、FA クライアントから FA サーバを介して自動アタッチ要求を渡します。FA プロキシとして動作するスイッチが、同時に FA クライアントとして動作することもできます。たとえば、スイッチが、それに直接接続されているエンド・ポイント デバイス (PC や IP 電話) に FA クライアント機能を提供すると同時に、アタッチされた FA クライアント (Extreme 無線 LAN AP など) のプロキシとしても動作することができます。FA プロキシと FA クライアントのエージェント機能は容易に共存するため、きわめて柔軟に配備できます。

FA サーバはネットワーク スイッチですが、FA プロキシと違って、Fabric Connect のプライベート クラウドと従来のイーサネット アクセス ネットワークの間の境界です。FA サーバは、Fabric Connect ノードであり、すべてのネットワークとサービスを認識します。またトポロジ上必要であれば、ここでも FA プロキシを介して、FA クライアントやアタッチされたあらゆるエンド・ポイント デバイスにネットワーク サービスを動的に拡張できます。

言い換えれば、エンド・ポイント デバイスは、FA クライアントによって大きなネットワークに接続されて、FA サーバからサービス拡張を受けるとともに、従来の VLAN を Fabric Connect VSN にマッピングします。VOSS 5.0 は、FA サーバ機能を VSP 4000 シリーズの製品ラインにもたらしめます。現在、さらに VSP 8000 シリーズと VSP 7200 シリーズ製品もサポートしています。

Fabric Attach プロセスは、FA サーバから FA クライアントと FA クライアントがホストするエンド・ポイント デバイスの両方に、動的かつ自動的にネットワーク サービスを拡張します。これにより、ネットワークに "弾力性" が加わり、必要に応じてかつ必要な期間だけ、サービスがエッジに拡張されます。エンド・ポイント デバイスが終了するか切断されると、冗長ネットワーク サービスがエッジから回収されます。このことには、露出と攻撃プロファイルが減少するというさらなるメリットがあります。

このソリューションに重要な付加価値を与える要素が、Extreme Identity Engines ポリシー サーバです。Fabric Attach は、Identity Engines がなくても基本的な接続自動化機能を提供できますが、Identity Engines がユーザとエンド・デバイスに高度な認証サービスを提供することにより、ソリューションが大幅に向上します。Identity Engines は、VSN/VLAN の割り当てに加え、ネットワーク サービスに対してさらに細分化した制御を行うことができます。ユーザ単位やデバイス単位の認証を利用して、カスタム ネットワーク サービスを動的に作成し、オンデマンドで適用できます。

Fabric Attach は、FA サーバ (Fabric Connect ノード / ネットワーク) が存在しない、純粋な従来型の VLAN ベースのネットワークにおける通常の配備にも利用できます。このシナリオでは、FA プロキシ スイッチが "スタンドアロン" モードで動作し、FA クライアントからの VLAN ID の要求に対応します。Identity Engines はこのモデルにも適用して、強力なユーザおよびデバイス認証とポリシー制御を提供できます。この方法で Fabric Attach を実装すると、Fabric Connect をまだ実装していない場合でも自動アタッチ機能を利用できます。

Fabric Attach は、運用上の大きなメリットをもたらします。エンド・ポイント デバイスは、IT 部門の介入や手作業による構成を必要とせず、一元化されたポリシー エンジンが、ビジネス ポリシーに従ってデバイスの自動アタッチを定義・ポリシングすることで、リアル・タイムで配備できます。静的なネットワーク デバイス構成を動的なプログラミングに置き換えることにより、ネットワーク全体の複雑さが減少し、それによってシステム停止のリスクが軽減するというメリットが得られます。

Fabric Extend: より幅広いユーザにメリットをもたらす

Fabric Connect はこれまで多くのお客様に、ほとんど理想的なネットワーク ソリューションを提供してきました。その理想的な Fabric Connect のおそらく唯一の問題は、開発の基盤である最短パス ブリッジング標準が、物理イーサネットの概念を中心に設計されている点です。このためトポロジがイーサネット・ベースに限定され、たとえば、サービス・ベースの接続を広域ネットワーク全体にエンド・トゥ・エンドで拡張できませんでした。技術的に言うと、この制限は、NNI リンク (ネットワーク間インターフェイス リンク) の "確立" に依存して、IS-IS 隣接が形成され、サービスが定義・提供されていることが原因です。そのため、Fabric Connect ネットワーク仮想化クラウドの任意境界は、イーサネットが到達する限界を超えることができませんでした。

この状況は、リモート サイトを自社のプライベート クラウドに完全に統合したいと望む企業にとって、多かれ少なかれ制約となっていました。このようなニーズの背景には、IP マルチキャスト・ベースのアプリケーションを会社全体にわたってサポートする必要がある場合や、IPv6 のスピーディな展開が必要な場合が考えられます。しかし、このインフラストラクチャはそれに十分に対応できません。拡張されたマルチ・テナント / セグメンテーション機能の提供が必要な場合もあれば、おそらくは単に異種ベンダー混合環境に Fabric Connect を外科的に配備することが求められている場合もあります。具体的な要件が何であれ、数多くの理由からルーティング IP 接続のみではソリューションとして完全かつ十分とは言えず、Fabric Connect クラウドが拡張可能であれば多くのメリットがもたらされることが考えられました。

そこでエクストリームが開発したのが Fabric Extend テクノロジーです。これにより、リモート ロケーションを Fabric Connect クラウドに完全に統合できるようになりました。Fabric Extend では、NNI インターフェイスを論理的に定義でき、VXLAN カプセル化により、MPLS や光イーサネットなどの IP ベースのトポロジ全体で、最短パス ブリッジング接続をシームレスにトンネルできます。Fabric Extend は汎用的テクノロジーであり、VLAN および VRF 拡張、レイヤー 2 とレイヤー 3 のハブ・スポーク型ネットワーク、および分散したキャンパスやデータ センター ロケーションのサイト相互接続を提供できます。

Fabric Extend は、Fabric Connect が築き上げたシンプルなネットワークの名声をさらに確固たるものにします。この流れを受け継ぐ Extreme Fabric Orchestrator 管理プラットフォームには、新しい Tunnel Manager ユーティリティが搭載されており、新しいノードを Fabric Extend ドメインに統合する際に、必要な双方向トンネルが自動的に構成されます。

Tunnel Manager では、直感的なグラフィカル機能を使用して、エニー・トゥ・エニー型とハブ・アンド・スポーク型の両方の構成を配備できます。さらに手作業によるセットアップが必要な場合に備えて、コマンド・ライン オプションも用意されています。

製品サポートについては、Fabric Extend は、3 種類のイーサネット スイッチ プラットフォームで使用できます。VSP 4000 シリーズでは、Extreme Open Networking Adaptor と組み合わせて配備する場合に使用でき、VSP 8000 シリーズと VSP 7200 シリーズの製品でもネイティブに使用できます。エクストリームの新しい Fabric Extend テクノロジは、複数のプライベートおよびプロバイダ IP インフラストラクチャにわたってネットワークのどこにでも拡張できる柔軟でスケーラビリティの高いソリューションを提供して、Fabric Connect が現在提供しているきわめて大きなメリットをさらに拡大します。

VSP 4000 モデル：

VSP 4000 モデルには、以下の 6 種類の製品があります。

- **VSP 4450GSX-PWR+**: 36 ポート x 100/1000 Mbps SFP、12 ポート x 10/100/1000BASE-T (PoE+ 搭載)、2 ポート x 1/10 Gigabit SFP+ (MACsec 暗号化機能対応)。
- **VSP 4450GSX-DC**: 36 ポート x 100/1000 Mbps SFP、12 ポート x 10/100/1000BASE-T、2 x SFP+ MACsec 対応のアップリンク ポート、オプションの DC 冗長電源付き。
- **VSP 4850GTS**: 48 ポート x 10/100/1000、2 x コンボ SFP、2 x SFP+ アップリンク ポート、オプションの冗長電源付き。
- **VSP 4850GTS-PWR+**: 48 ポート x 10/100/1000 (PoE+ 搭載)、2 x コンボ SFP、2 x SFP+ アップリンク ポート、オプションの冗長電源付き。
- **VSP 4850GTS-DC**: 48 ポート x 10/100/1000、2 x コンボ SFP、2 x SFP+ アップリンク ポート、オプションの DC 冗長電源付き。
- **VSP 4450GTX-HT-PWR+**: VSP 4000 シリーズの高温対応機種。0 ~ 70 °C の極端な温度範囲の環境に配備可能。48 ポート x 10/100/1000 (PoE+ 搭載)、2 x コンボ SFP、2 x SFP+ アップリンク ポート、オプションの冗長電源付き。

VSP 4000 サービスの概要：

VSP 4000 には、シンプルで配備が容易な広範囲に及ぶネットワーク サービスが用意されています。初回リリースでサポートされる項目は以下のとおりです。

- ファブリック全体 (サブネット全体および長距離を含む) に VLAN を拡張する レイヤー 2 仮想化サービス。
- ファブリック全体で VRF を相互接続し、拡張する レイヤー 3 仮想化サービス。

- 共有サービスにアクセスするためのレイヤー 2 とレイヤー 3 仮想化サービス間のネイティブなルーティング。
- 追加の IGP を配備する必要なしに、個別のエンド・ポイント間の直接レイヤー 3 接続を可能にする IP ショートカットルーティング。
- PIM ベースのプロトコルを配備せずに、スケーラブルで効率的、かつ回復性に優れたマルチキャスト分散を行うための IP マルチキャスト ショートカット。
- レイヤー 2 またはレイヤー 3 仮想サービス ネットワーク内で、PIM 非依存のマルチキャストをサポートするための IP マルチキャスト仮想化。
- スタティック、RIP、OSPF、eBGP、BGP+、ECMP、VRRP、PIM-SM/SSM、VRF などの IP ルーティング方法をサポート。さらに IPv6 配備の Static、RIPng、OSPFv3、ECMP、VRRP もサポート。

VSP 4000 の配備シナリオ：

多様なサービスを提供する VSP 4000 は、以下のような幅広い配備シナリオに適切に対応します。

- 仮想化環境にある中小規模企業
- 分散環境にある企業

配備には、以下のいずれかまたは両方が必要な場合があります (詳細については後述します)。

- マルチ・テナンシーを実現するため、またはセキュリティ / 法令準拠上の理由 (PCI DSS など) によるエンド・トゥ・エンドのトラフィックの分離。
- 統合ビデオ監視、ビデオ配信、デジタル サイネージ (電子看板) のサポート。

VSP 4850 シリーズは、銅ベースの配備に最適化されており、VSP 4450 は、ヘビーファイバーベースの配備に最適化されています。たとえば、各階にギガビット接続を提供するビルのライザー ケーブルなどです。

仮想化環境にある中小規模企業

Extreme Fabric Connect 戦略は、あらゆる規模の会社にファブリックベースのテクノロジーの価値を提供します。中小規模企業に機能豊富で費用対効果の高いソリューションを提供する VSP 4000 は、VSP 8200 とともにコアに配備して、シンプルで俊敏、かつ回復性に富んだネットワークを構築できます。このファブリック対応のエッジと小さくコンパクトなコア オプションのパワフルな組み合わせを一緒に配備することで、小規模企業向けに費用対効果が向上し、主流のファブリック テクノロジーを導入できます。

分散環境にある企業

Extreme Fabric Connect テクノロジーによってネットワークをエンド・トゥ・エンドで真に変革するには、リモート ロケーションにまで拡張する必要があります。VSP 4000 を使用すると、ネットワーク全体で単一のテクノロジーを使用することができ、サービス プロバイダのレイヤー 2 サービス (E-Line と E-Tree) 全体にわたってリモート サイトに接続できます。VSP 4000 は、物理リング ベースのインフラストラクチャ上に配備して、Fabric Connect ネットワークの接続範囲をメトロ全体に拡張することもできます。

マルチ・テナンシーをサポートするためのエンド・トゥ・エンドのトラフィックの分離

企業環境の種類を問わず、マルチ・テナンシーをサポートするために、エンド・トゥ・エンドでトラフィックを分離しなければならないことがあります。たとえば、空港、大学、政府機関、医療機関、および他の法人を買収しようとする企業は、場合によっては、何らかの共有サービスを提供する間、トラフィックを分離します。

Extreme Fabric Connect は、統合 VRF 機能により、シンプルなエンド ポイント プロビジョニングを使用して、ファブリック全体にレイヤー 3 ネットワークを容易に配備できます。VSP 4000 は、低コストのマルチ・テナント境界設定サービスとして、複数のエンティティからのトラフィックをサポートして分離し、環境に対して重要な役割を果たします。

セキュリティまたは規制上の理由によるエンド・トゥ・エンドのトラフィックの分離

セキュリティまたは規制上の理由から、エンド・トゥ・エンドのトラフィックの分離が必要になることがあります。たとえば、クレジット カード取引、医療機器、監視カメラを他のネットワークトラフィックから保護したり、あらゆる業種で、VoIP を分離して、別に管理したりすることがこれに当てはまります。

Extreme Fabric Connect は、統合 VRF 機能により、ファブリック全体にレイヤー 3 ネットワークを容易に配備して、エンド・トゥ・エンドでトラフィックの分離を維持できます。

これは、エッジでの Mac-in-Mac のカプセル化に加えて、複数の必要なネットワークを提供し、VLAN ジャンピングなどのセキュリティ侵害を防止してセキュリティを強化することができます。

統合ビデオ監視、ビデオ配信、デジタル サイネージ

運輸業、政府機関、サービス業などの業界では、人や製品の保護にビデオ監視テクノロジーが多用されています。ビデオ監視はマルチキャストへと発展しつつありますが、いまだユニキャスト トラフィックが広く使用されています。VSP 4000 は、追加の IGP または PIM プロトコルを必要とせずに、両方のタイプの監視ネットワークをサポートします。また VSP 4850GTS-PWR+ デバイスと VSP 4450GSX-PWR+ デバイスは、IEEE 802.3at PoE+ を併せてサポートしており、新型のポイント チルト/ズーム カメラに電源を供給できます。

ブロードキャスト転送およびマルチキャスト転送は、イーサネットに内在する機能であるため、Extreme Fabric Connect テクノロジーは、最初からマルチキャスト ツリーの効率的な処理を目的に構築されています。Extreme Fabric Connect では、ネットワークがポイント・トゥ・ポイント、ポイント・トゥ・マルチ・ポイント、エニイ・トゥ・エニイ接続サービスをオンデマンドでインスタンス化できるため、きわめて効率的でスケーラビリティと回復性に優れた方法でマルチキャスト配信を行って、IPTV、デジタル サイネージ、マルチキャスト対応のビデオ監視ネットワークをサポートできます。

さらに、VOSS は Extreme Fabric Connect-PIM Gateway をサポートします。この機能によって、Fabric Connect と標準ベースの PIM マルチキャスト ルーティング環境の間で、シームレスな双方向の相互運用が可能になります。従来の PIM (プロトコル独立型マルチキャスト) については、制限が多く複雑で不安定だという不評が多いですが、残念なことにネットワークで IP マルチキャスト トラフィックをルーティングする必要がある場合、これが唯一の選択肢でした。しかし Fabric Connect により、マルチキャストのパラダイムが一変します。マルチキャストが、柔軟に計画して簡単に配備でき、安定して動作するようになります。現在、従来型の IP マルチキャスト環境 (PIM-SM または PIM-SSM) を運用している企業は、Fabric Connect を実装した後も、PIM から完全に移行するまでの間、これらをシームレスに共存させることができます。この機能は柔軟性が高く、高可用性オプションをサポートしているため、組織はそれぞれのペースでテクノロジーの配備と廃止を進めることができます。VSP 4000 シリーズは、Fabric Connect-PIM Gateway 機能のインターフェイス機能コンポーネントをサポートします。

システムの互換性

ソフトウェアに関して述べると、VSP 4000 シリーズは、VOSS 4.1 統合ソフトウェア リリースとともに提供が開始されました。したがって、これがこのスイッチの動作に利用できる最低限のソフトウェアとなります。最新の VOSS 7.0 リリースでは、以下の重要な強化機能が追加されました。

- ゼロ・タッチの Fabric Connect 機能の導入
- フェーズ 1 の IPv6 IP ルーティング仮想化
- BGPv6 への IPv6 ピアリングの追加
- Energy Saver 機能の導入
- Extreme Management Center の統合
- 拡張トランシーバの提供とサポート

ゼロ・タッチの Fabric Connect。新しい "ゼロ・タッチ ファブリック" 機能では、既存のドメインに新しい Fabric Connect ノードを自動的に追加できるため、分散アーキテクチャとクラウド アーキテクチャでのスケール・アウトが飛躍的に簡略化されます。

機能の仕組み：Fabric Connect ドメインが既に導入されていて、このドメインが "シード スイッチ" のようなシンプルなものである場合、"ファブリック エリア ネットワーク" を自動生成することで、確立された Fabric Connect ノードと候補の Fabric Connect ノード間の管理上の通信が容易になります。ゼロ・タッチのファブリックでは、新しいノードが IS-IS エリアを自動的に検出して、ドメイン固有のニックネームを要求します（概念的には、DHCP に近い）。次に、デフォルトの B-VID 値を使用して双方向の IS-IS 通信を確立し、システム ID と管理 IP アドレスを自動的に構成します。

IPv6 IP ルーティング仮想化（フェーズ 1）。このリリースでは、既存の IPv6 ルーティング機能が仮想化によってさらに強化されています。つまり IPv6 は、グローバル ルーティング テーブル内で 1 つのインスタンスに限定されなくなりました。現在このスイッチは、128 個の IPv6 ルーティング インスタンスをサポートし、ECMP、代替ルート、ルート再配布、VSN 間ルーティング、DHCP リレー、ICMP Ping と Traceroute、および IPv6 の VRRPv3 などの機能をサポートします。また VRF インスタンスは、IPv4 と IPv6 の両方の統合、L3 仮想サービス ネットワークをサポートします。

Extreme Management Center

ネットワークはビジネスに必須の活力源です。画期的なアプリケーションを駆動し、人材というビジネスにとって最も重要な資産を強化します。有線と無線のインフラストラクチャを統合することで、継続性とモビリティがもたらされます。信頼性の高いネットワークは、組織が成功するうえで不可欠です。Extreme Management Center は、実践的な情報と細分化した可視性を提供し、ユーザ、デバイス、アプリケーションを自動制御します。

Extreme Management Center は、真の一元管理プラットフォームならではの迅速な操作により、すべての関係者に質の高いエクスペリエンスを提供します。有線、無線を問わず、アクセスエッジからプライベート クラウドまでインフラストラクチャ全体で機能するため、ユーザはネットワーク、デバイス、アプリケーション、ユーザをあらゆる角度から把握できます。Extreme Management Center は、ビジネスを次のレベルへと進化させる統合ツールセットです。

このパワフルなアプライアンス・ベースのソリューションは、次の機能を提供します。

- **一元的な管理運用**：互いに連携して機能する完全に統合された一連のツールによって、ネットワークの総合的情報がまとめて表示され、ワークフローの効率化と運用コストの削減につながります。
- **検出と可視化**：ネットワークとデバイスの充実した検出・可視化機能を備えています。これにより、ネットワーク・アタッチ デバイス（サーバ、ストレージサーバ、スイッチ、ルータ、電話機、仮想マシンとそのホストなど）に加え、Extreme Aura アプリケーションを検出できます。
- **障害と診断**：ネットワークから収集した情報を利用して、ネットワーク中断の最も可能性の高い原因を特定するとともに、イベントの相関性を分析して、影響を受けるデバイスとサービスを判断します。

- **構成とオーケストレーション**：直感的に操作できるシンプルなウィザードと使いやすいテンプレートが用意されており、複雑なネットワーク構成でも簡単に設定できます。構成テンプレートは一度作成して保存すれば、便利に適用してサービス開始までの所要時間を短縮し、人的ミスリスクを抑えることができます。
- **仮想化の管理**：並列 VM の移行に必要なコンパニオン ネットワーキング サービスの自動プロビジョニングを含め、仮想マシンの全ライフサイクル（アクティブ化、移行、廃止）にわたる情報を提供します。
- **パフォーマンス管理**：アプリケーションの動作と帯域幅の利用動向を監視、分析、報告するツールが組み込まれています。収集されたデータは、トラフィック パターン、アプリケーションの動作、トップ トーカー（トラフィック量の大きいデバイス）について貴重な情報をもたらします。パフォーマンス管理ツールは、キャパシティ プランニングや変更監視に使用できます。
- **統合 SDN 機能**：Fabric Orchestrator は、まさに将来を明確に見据えて開発された製品です。このプラットフォームは、Open Daylight ベースの SDN コントローラ プラグイン、ノース・バウンド REST インターフェイス経由でアクセスできるサードパーティ ツールとコントローラ、およびストレージやコンピューティング リソースと連動したネットワークオーケストレーションを実現する OpenStack ML2 ドライバのための統合ポイントを提供します。

ライフタイム保証

エクストリームの Fabric Connect エッジ デバイスをはじめとする一連のスタック可能スイッチには、包括的な保証サービスが含まれています。製品のライフタイム全期間にわたり、世界全域で故障ユニットの交換品が翌営業日に無料で発送されます。また故障部品の交換品も翌営業日に発送されます。さらに以下の基本的な技術サポートを提供しています。

レベル 1 の製品ライフサイクルのサポートからレベル 3 の購入後 90 日間サポートまで。これには、付属ソフトウェア バージョンのサポートが含まれ、オプションで、ソフトウェア リリース サービスをご利用いただけます。

ハードウェアに関する業界慣行に従い、"ライフタイム" の定義を、生産ライフサイクル フェーズに生産中止後の 5 年間を加えた期間とします。保証規定を超えた保護をご希望のお客様は、エクストリームの一連のサポート サービスをご利用いただけます。

まとめ

VSP 4000 は、他の Extreme Fabric Connect ソリューションとともに配備することで、収益性と利益性の向上、ビジネス運営の効率化、コスト削減、ビジネスの競争力強化を実現します。エクストリームは、あらゆる L2/3 サービス配備のためのシンプルで洗練されたアプローチを提供し、ファブリック対応ネットワークキングをリードしています。

VSP 4450GSX-PWR+	
スイッチの詳細	<ul style="list-style-type: none"> • 12 x 10/100/1000 ギガビット イーサネット RJ45 ポート (PoE+ 対応) • 36 x 100/1000 Mbps SFP ポート • 2 x 1/10 ギガビット SFP+ ポート • システム CPU 動作速度 : 1.2GHz • スイッチには 2 GB の 800 DDR3 DRAM を搭載 • RJ-45 コンソール ポートおよび USB 2.0 ポート • 1 x 19 インチ (44 mm) ラック マウント ブラケット セットが付属
寸法	1 ユニット : 高さ 4.4cm、幅 44cm (19 インチ ラック マウント対応)、奥行 43.6cm
重量	7.80 kg (17.2 ポンド) (1 個の PSU 装着時)。PSU の重量は 1 個 1.40 kg (3.1 ポンド)
電源と発熱量	<ul style="list-style-type: none"> • 1 x 1000 W AC のフィールド交換可能な電源ユニットが付属 • 冗長構成用に、フィールド交換可能な追加の第 2 AC 電源をサポート • PoE を含まない消費電力は通常 95 W、最大 140 W、発熱量は通常 324 BTU/時、最大 477.70 BTU/時

VSP 4450GSX-DC	
スイッチの詳細	<ul style="list-style-type: none"> • 12 x 10/100/1000 ギガビット イーサネット RJ45 ポート • 36 x 100/1000 Mbps SFP ポート • 2 x 1/10 ギガビット SFP+ ポート • システム CPU 動作速度 : 1.2GHz • スイッチには 2 GB の DRAM を搭載 • RJ-45 コンソール ポートおよび USB 2.0 ポート • 1 x 19 インチ (44 mm) ラック マウント ブラケット セットが付属
寸法	1 ユニット : 高さ 4.4cm、幅 44cm (19 インチ ラック マウント対応)、奥行 43.6cm
重量	7.80 kg (17.2 ポンド) (1 個の PSU 装着時)。PSU の重量は 1 個 1.40 kg (3.1 ポンド)
電源と発熱量	<ul style="list-style-type: none"> • 1 x 300 W のフィールド交換可能な DC 電源ユニットが付属 • 冗長構成用に、フィールド交換可能な追加の第 2 DC 電源をサポート • 熱定格 : 323 BTU/時

VSP 4850GTS	
スイッチの詳細	<ul style="list-style-type: none"> • 48 x 10/100/1000 ギガビット イーサネット RJ45 ポート • 2 x コンボ SFP ポート • および 2 x 1/10 ギガビット SFP+ ポート • システム CPU 動作速度 : 533 MHz • スイッチには 1 GB の RAM を搭載 • RJ-45 コンソール ポートは、業界標準のシリアル ポート接続が可能 • 1 x 19 インチ (44 mm) ラック マウント ブラケット セットが付属
寸法	高さ 4.4cm (1 RU)、幅 44.0cm、奥行 43.68cm
重量	11.48 Kg
電源と発熱量	<ul style="list-style-type: none"> • 1 x 300 W のフィールド交換可能な AC 電源ユニットが付属 • 冗長構成用に、フィールド交換可能な追加の第 2 AC 電源をサポート • 熱定格 : 323 BTU/時

VSP 4850GTS-PWR+	
スイッチの詳細	<ul style="list-style-type: none"> • 48 x 10/100/1000 ギガビット イーサネット RJ45 ポート • 48 x IEEE 802.3at PoE+ 対応ポート • 2 x コンボ SFP ポート • および 2 x 1/10 ギガビット SFP+ ポート • システム CPU 動作速度 : 533 MHz • スイッチには 1 GB の RAM を搭載 • RJ-45 コンソール ポートは、業界標準のシリアル ポート接続が可能 • 1 x 19 インチ (44 mm) ラック マウント ブラケット セットが付属
寸法	高さ 4.4cm (1 RU)、幅 44.0cm、奥行 43.68cm
重量	11.98 Kg
電源と発熱量	1 x 1000 W のフィールド交換可能な AC 電源ユニットが付属 冗長構成用または追加の PoE 用に、フィールド交換可能な追加の第 2 AC 電源をサポート 熱定格 : 383 BTU/時
最大 PoE+ 容量	<ul style="list-style-type: none"> • 1 台の 1000 W 電源での稼働時 : 855 W • 2 台の 1000 W 電源での稼働時 : 1855 W

VSP 4450GTX-HT-PWR+

スイッチの詳細	<ul style="list-style-type: none"> • 48 x 10/100/1000 ギガビット イーサネット PoE+ 対応 RJ45 ポート • 2 x 1 G SFP コンボ ポート • 2 x 1/10 ギガビット SFP+ ポート • システム CPU 動作速度: 1.2 GHz • スイッチには 2 GB の SDRAM を搭載 • RJ-45 コンソール ポートは、業界標準のシリアル ポート接続が可能 • 1 x 19 インチ (44 mm) ラック マウント ブラケット セットが付属 • 動作時温度範囲: 0 ~ 70 °C
寸法	高さ 8.8 cm (2 RU)、幅 44.0 cm、奥行 36.8 cm
重量	1 PSU 装着時: 合計 1.48 kg (23.1 ポンド)、PSU の重量: 1.4 kg (3.1 ポンド)
電源と発熱量	<ul style="list-style-type: none"> • 1 x 1000 W のフィールド交換可能な AC 電源ユニットが付属 • 冗長構成用に、フィールド交換可能な追加の第 2 AC 電源をサポート • 熱定格: PoE を含まない消費電力は通常 100 W、最大 145 W、発熱量は通常 321.2 BTU/時、最大 494.8 BTU/時

VSP 4850GTS-DC

スイッチの詳細	<ul style="list-style-type: none"> • 48 x 10/100/1000 ギガビット イーサネット RJ45 ポート • 2 x コンボ SFP ポート • および 2 x 1/10 ギガビット SFP+ ポート • システム CPU 動作速度: 533 MHz • スイッチには 1 GB の RAM を搭載 • RJ-45 コンソール ポートは、業界標準のシリアル ポート接続が可能 • 1 x 19 インチ (44 mm) ラック マウント ブラケット セットが付属
寸法	高さ 4.4cm (1 RU)、幅 44.0cm、奥行 43.68cm
重量	11.48 Kg
電源と発熱量	<ul style="list-style-type: none"> • 1 x 300 W のフィールド交換可能な DC 電源ユニットが付属 • 冗長構成用に、フィールド交換可能な追加の第 2 DC 電源をサポート • 熱定格: 323 BTU/時

仕様

全般

- ・ フレーム長: 64 ~ 1,518 バイト (802.1Q タグなし)、64 ~ 1,522 バイト (802.1Q タグ付き)
- ・ ジャンボ フレームのサポート: 最大 9.6 K バイト
- ・ スイッチ ファブリックの容量: 184 Gbps
- ・ パケット転送スループット (64 バイト パケット): 102 Mpps
- ・ レイテンシ (64 バイトのパケット): 9 マイクロ秒
- ・ RSTP、MSTP
- ・ VRRP バックアップ マスター
- ・ IPv4/IPv6 ルーティング
- ・ ポリシー ベース ルーティング
- ・ 入力および出力ポート ACL
- ・ 入力 VLAN ACL
- ・ エンタープライズ デバイス マネージャ GUI、オン・ボックス / オフ・ボックス
- ・ 構成およびオーケストレーション マネージャ
- ・ 仮想化パフォーマンスと Fault Manager
- ・ 仮想化プロビジョニング サービス
- ・ システム ロギング
- ・ ミラーリング: 1:1 / 1:M / M:1 / M:M
- ・ 主要状態インジケータ
- ・ フライト レコーダ
- ・ 自動 MDIX
- ・ MACsec (VSP 4450GSX-PWR+ のみ)
- ・ TACACS+
- ・ SLAMon エージェント

レイヤー 2

- ・ MAC アドレス: 32,000
- ・ ポート・ベース VLAN: 4,059
- ・ プライベート VLAN/E-Tree: 1,000
- ・ MSTP インスタンス: 12
- ・ MLT/LACP Groups: 50
- ・ 1 グループあたりの MLT リンク: 8
- ・ 1 グループあたりの LACP リンク: 8 アクティブ
- ・ Extreme VLACP インスタンス: 50
- ・ Extreme SLPP インスタンス: 128

レイヤー 3 IPv4 ルーティング サービス

- ・ ARP エントリ: 6,000
- ・ スタティック ARP エントリ: VRF/スイッチ1つあたり 2000
- ・ IP インターフェイス: 256
- ・ CLIP インターフェイス: 64
- ・ IP ルート: 最大 15,744
- ・ IP スタティック ルート: VRF 1 つあたり 1,000、スイッチ 1 台につき 1,000
- ・ RIP インターフェイス: 24
- ・ RIP ルート: 最大 15,744
- ・ OSPF インターフェイス: 100
- ・ OSPF ルート: 最大 15,744
- ・ OSPF エリア: VRF 1 つあたり 12、スイッチ 1 台につき 64
- ・ BGP ピア: 12
- ・ BGP ルート: 最大 15,744
- ・ ECMP グループ数: 500
- ・ 1 グループあたりの ECMP パス: 4
- ・ VRRP インターフェイス: 64 または 24 (高速タイマー使用時)
- ・ RSMLT インターフェイス: 252
- ・ IPv4 UDP 転送エントリ: 128
- ・ IPv4 DHCP リレー転送エントリ: 128
- ・ IP ルート ポリシー: VRF あたり 500、システム全体で 5,000
- ・ VRF インスタンス: 最大 128

レイヤー 3 IPv6 ルーティング サービス

- ・ ネイバー: 4,000
- ・ 静的ネイバー: 128
- ・ IP インターフェイス: 256
- ・ CLIP インターフェイス: 64
- ・ IP 構成済みトンネル: 254
- ・ IP ルート: 最大 7,488
- ・ IP スタティック ルート: 1,000
- ・ RIPng インターフェイス: 24
- ・ RIPng ルート: 最大 7,488
- ・ OSPFv3 インターフェイス: 最大 100
- ・ OSPFv3 ルート: 最大 7,488
- ・ OSPFv3 エリア: スイッチ 1 台につき 64
- ・ BGPv6 ピア: 12
- ・ ECMP グループ数: 500
- ・ 1 グループあたりの ECMP パス: 4
- ・ VRRP インターフェイス: 64 または 24 (高速タイマー使用時)
- ・ RSMLT インターフェイス: 252
- ・ VRF インスタンス: 最大 128

マルチキャスト

- IGMP インターフェイス : 4,059
- PIM アクティブ インターフェイス : 128
- PIM-SSM スタティック チャネル : 512
- IP マルチキャスト ストリーム : 1,000
- リージョンあたりのファブリック接続 PIM ゲートウェイ コントローラ : 5
- リージョンあたりのファブリック接続 PIM ゲートウェイ ノード : 64
- BEB ノードあたりのファブリック接続 PIM ゲートウェイ インターフェイス : 64
- ファブリック接続 PIM ゲートウェイ ソース通知 : 6,000

Fabric Connect

- 802.1aq/RFC 6329 最短パス ブリッジングおよびエクストリームによる拡張機能
- MAC アドレス : 16,000
- NNI インターフェイス / 隣接 : 最大 255
- リージョンあたりの BCB/BEB ノード : 2,000
- VSN あたりの BEB ノード : 2,000
- L2 仮想サービス ネットワーク : 1,000
- L3 仮想サービス ネットワーク : 最大 128
- IP ショートカット ルート : IPv4 で最大 15,744、IPv6 で最大 7,488
- L2 マルチキャスト仮想サービス ネットワーク : 最大 1,000
- L3 マルチキャスト仮想サービス ネットワーク : 最大 128

QoS およびフィルタリング

- IPv4 ACE: 入力 1530、出力 254
- IPv6 ACE: 入力 256
- QoS 優先順位付きキュー数 : 8

運用と管理

- ミラー ポート : 49
- sFlow: 1 秒あたり最大 100 サンプル
- Fabric RSPAN: 1,000 VLAN ID

環境仕様条件

- 動作時温度 : 0 ~ 50 °C (32 ~ 122 °F)
- 保管時温度 : -40 ~ 85 °C (-13 ~ 158 °F)
- 運用時湿度 : 相対湿度 0 ~ 95%、結露しないこと
- 保管時湿度 : 相対湿度 10 ~ 90%、結露しないこと 動作時高度 : 0 ~ 最大 3,048 m (0 ~ 10,000 フィート)
- 保管時高度 : 最高 0 ~ 12,192m (0 ~ 40,000 フィート)
- 騒音 :

- 35 °C で 50 dbA 未満

- 50 °C で 57 dbA 未満

- VSP 4000 の安全認証
- 世界基準 : 現行版の IEC 60950 (すべての CB 加盟国の個別要求事項を含む)
- CB 証明書 (加盟国の個別要求事項を含む)
- EN60950 欧州安全認証 (CE)
- UL60950 米国安全認証
- CSA22.2、#60950 カナダ安全認証
- NOM メキシコ安全認証
- S マーク アルゼンチン安全認証
- Anatel ブラジル安全認証
- 電磁ミッションおよびイミュニティ
- CISPR22 国際 EMC エミッション規格
- CIRPR24 国際 EMC イミュニティ規格
- EN55022:2006 欧州 EMC エミッション規格 (CE)
- EN55024 欧州 EMC イミュニティ規格 (CE)
- EN61000
- 欧州 EMC 追加規格 (CE)
- FCC Part 15 米国 EMC エミッション
- ICES-003 カナダ EMC エミッション
- VCCI 日本 EMC エミッション
- AN/NZS 3548 オーストラリア / ニュージーランド EMC エミッション規格
- CNS13438 台湾 EMC エミッション
- MIC 韓国 EMC 認証
- Anatel ブラジル EMC 認証

MTBF 値

- 214,542 ~ 311,104 時間 (24.49 ~ 35.31 年)

製品保証

- ライフタイム期間中、翌営業日に先出しハードウェア交換
- ライフタイム期間中の基本的な技術サポート
- 90 日間の高度な技術サポート
- オプションでソフトウェア リリース サービスも購入可能 : GW5300ASG / GW6300ASG

生産国

- 中華人民共和国

準拠規格

802.1 Bridging (Networking) and Network Management

- 802.1D MAC Bridges (別名 : Spanning Tree Protocol)
- 802.1p Traffic Class Expediting and Dynamic Multicast Filtering
- 802.1t 802.1D Maintenance
- 802.1w Rapid Reconfiguration of Spanning Tree (RSTP)
- 802.1Q Virtual Local Area Networking (VLAN)
- 802.1Qbp Equal-Cost Multi-Path (Shortest Path Bridging)
- 802.1Qcj Automatic Attachment to Provider Backbone Bridging (PBB) Services (一部のみサポート)
- 802.1s Multiple Spanning Trees (MSTP)
- 802.1v VLAN Classification by Protocol & Port
- 802.1ag Connectivity Fault Management
- 802.1ah Provider Backbone Bridges
- 802.1aq Shortest Path Bridging (SPB) MAC-in-MAC
- 802.1X Port-based Network Access Control
- 802.1AB-2005 Station & Media Access Control Connectivity Discovery (別名 : LLDP、 一部のみサポート)
- 802.1AE Media Access Control Security
- 802.1AX Link Aggregation

802.3 Ethernet

- 802.3-1983 CSMA/CD Ethernet (ISO/IEC 8802-3)
- 802.3i-1990 10Mb/s Operation, 10BASE-T Copper
- 802.3u-1995 100 Mb/s Operation, 100BASE-T Copper, with Auto-Negotiation
- 802.3x-1997 Full Duplex Operation, including Flow Control
- 802.3z-1998 1000Mb/s Operation, implemented as 1000BASE-X
- 802.3ab-1999 1000Mb/s Operation, 1000BASE-T Copper
- 802.3ae-2002 10Gb/s Operation, implemented as 10GBASE-SFP+
- 802.3an-2006 10Gb/s Operation, 10GBASE-T Copper
- 802.3ba-2010 40Gb/s and 100Gb/s Operation
- 802.3bm-2015 40Gb/s and 100Gb/s Operation, implemented as 40GBASE-QSFP+ & 100GBASE-QSFP28

IETF

- 768 UDP
- 783 TFTP
- 791 IP
- 792 ICMP

- 793 TCP
- 826 ARP
- 854 Telnet
- 894 Transmission of IP Datagrams over Ethernet Networks
- 896 Congestion Control in IP/TCP internetworks
- 906 Bootstrap Loading using TFTP
- 950 Internet Standard Subnetting Procedure
- 951 BOOTP: Relay Agent-only
- 959 FTP
- 1027 Using ARP to Implement Transparent Subnet Gateways
- 1058 RIP
- 1112 Host Extensions for IP Multicasting
- 1122 Requirements for Internet Hosts - Communication Layers
- 1155 Structure and Identification of Management Information for TCP/IP-based Internets
- 1156 MIB for Network Management of TCP/IP
- 1157 SNMP
- 1212 Concise MIB Definitions
- 1213 MIB for Network Management of TCP/ IP-based Internets: MIB-II
- 1215 Convention for Defining Traps for use with the SNMP
- 1256 ICMP Router Discovery
- 1258 BSD Rlogin
- 1271 Remote Network Monitoring MIB
- 1305 NTPv3
- 1321 MD5 Message-Digest Algorithm
- 1340 Assigned Numbers
- 1350 TFTPv2
- 1398 Ethernet MIB
- 1442 SMIv2 of SNMPv2
- 1450 SNMPv2 MIB
- 1519 CIDR
- 1541 DHCP
- 1542 Clarifications & Extensions for BOOTP
- 1573 Evolution of the Interfaces Group of MIB-II
- 1587 OSPF NSSA Option
- 1591 DNS Client
- 1650 Definitions of Managed Objects for the Ethernet-like Interface Types

IETF (続き)

- 1657 Definitions of Managed Objects for BGP-4 using SMIPv2
- 1723 RIPv2 Carrying Additional Information
- 1812 Router Requirements
- 1850 OSPFv2 MIB
- 1866 HTMLv2
- 1907 SNMPv2 MIB
- 1930 Guidelines for creation, selection, and registration of an AS
- 1981 Path MTU Discovery for IPv6
- 2021 Remote Network Monitoring MIBv2 using SMIPv2
- 2068 HTTP
- 2080 RIPv2 for IPv6
- 2131 DHCP
- 2138 RADIUS Authentication
- 2139 RADIUS Accounting
- 2236 IGMPv2 Snooping
- 2284 PPP Extensible Authentication Protocol
- 2328 OSPFv2
- 2362 PIM-SM
- 2404 HMAC-SHA-1-96 within ESP and AH1
- 2407 Internet IP Security Domain of Interpretation for ISAKMP1
- 2408 Internet Security Association and Key Management Protocol
- 2428 FTP Extensions for IPv6 and NAT
- 2452 TCP IPv6 MIB
- 2453 RIPv2
- 2454 UDP IPv6 MIB
- 2460 IPv6 Basic Specification
- 2463 ICMPv6
- 2464 Transmission of IPv6 Packets over Ethernet Networks
- 2466 MIB for IPv6: ICMPv6 Group
- 2474 Differentiated Services Field Definitions in IPv4 & IPv6 Headers
- 2475 Architecture for Differentiated Service
- 2541 DNS Security Operational Considerations
- 2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- 2548 Microsoft Vendor-specific RADIUS Attributes
- 2572 Message Processing and Dispatching for SNMP
- 2573 SNMP Applications
- 2574 User-based Security Model for SNMPv3
- 2575 View-based Access Control Model for SNMP
- 2576 Coexistence between v1/v2/v3 of the Internet-standard Network Management Framework
- 2578 SMIPv2
- 2579 Textual Conventions for SMIPv2
- 2580 Conformance Statements for SMIPv2
- 2597 Assured Forwarding PHB Group
- 2598 Expedited Forwarding PHB OA&M RFCs
- 2616 HTTPv1.1
- 2710 MLD for IPv6
- 2716 PPP EAP TLS Authentication Protocol
- 2787 Definitions of Managed Objects for VRRP
- 2818 HTTP over TLS
- 2819 Remote Network Monitoring MIB
- 2863 Interfaces Group MIB
- 2865 RADIUS
- 2869 RADIUS Extensions (一部のみサポート)
- 2874 DNS Extensions for IPv6
- 2925 Definitions of Managed Objects for Remote Ping, Traceroute, & Lookup Operations
- 2933 GMP MIB
- 2934 PIM MIB for IPv4
- 2992 ECMP Algorithm
- 3046 DHCP Relay Agent Information
- Option 82
- 3162 RADIUS and IPv6
- 3246 Expedited Forwarding PHB
- 3315 DHCPv6
- 3339 Date & Time on The Internet: Timestamps
- 3376 IGMPv3
- 3411 Architecture for Describing SNMP Management Frameworks
- 3412 Message Processing and Dispatching for SNMP
- 3413 SNMP Applications
- 3414 USM for SNMPv3
- 3415 VACM for SNMP
- 3416 Protocol Operations v2 for SNMP
- 3417 Transport Mappings for SNMP

IETF (続き)

- 3418 MIB for SNMP
- 3484 Default Address Selection for IPv6
- 3513 IPv6 Addressing Architecture
- 3569 Overview of SSM
- 3579 RADIUS Support for EAP
- 3587 IPv6 Global Unicast Address Format
- 3596 DNS Extensions to support IPv6
- 3748 Extensible Authentication Protocol
- 3768 VRRP; plus draft-ietf-vrrp-ipv6-spec-08
- 3810 MLDv2 for IPv6: Host Mode-only
- 3879 Deprecating Site Local Addresses
- 4007 IPv6 Scoped Address Architecture
- 4022 TCP MIB
- 4087 IP Tunnel MIB
- 4113 UDP MIB
- 4133 Entity MIB Version 3 (一部のみサポート)
- 4193 Unique Local IPv6 Unicast Addresses
- 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
- 4250 SSH Assigned Numbers
- 4251 SSH Protocol Architecture
- 4252 SSH Authentication Protocol
- 4253 SSH Transport Layer Protocol
- 4254 SSH Connection Protocol
- 4255 DNS to Securely Publish SSH Key Fingerprints
- 4256 Generic Message Exchange Authentication for SSH
- 4291 IPv6 Addressing Architecture
- 4292 IP Forwarding Table MIB
- 4293 IP MIB
- 4301 Security Architecture for IP1
- 4302 IP Authentication Header1
- 4303 IP Encapsulating Security Payload1
- 4308 Cryptographic Suites for IPsec
- 4363 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions (一部のみサポート)
- 4443 ICMP for IPv6
- 4429 Optimistic DAD for IPv6 (一部のみサポート)
- 4541 Considerations for IGMP & MLD Snooping Switches
- 4552 Authentication/Confidentiality for OSPFv3
- 4601 PIM-SM: Revised Protocol Specification
- 4607 Source-Specific Multicast for IP
- 4675 RADIUS Attributes for Virtual LAN and Priority Support (一部のみサポート)
- 4835 Cryptographic Algorithm Implementation Requirements for ESP & AH1
- 4861 Neighbor Discovery for IPv6
- 4862 IPv6 Stateless Address Auto- Configuration
- 5095 Deprecation of Type 0 Routing Headers in IPv6
- 5176 Dynamic Authorization Extensions to RADIUS
- 5187 OSPFv3 Graceful Restart (ヘルパー・モード)
- 5308 Routing IPv6 with IS-IS
- 5340 OSPF for IPv6
- 5424 The Syslog Protocol
- 5798 VRRPv3 for IPv4 & IPv6
- 5905 NTPv4: Protocol and Algorithms Specification
- 5997 Use of Status-Server Packets in RADIUS
- 6105 IPv6 Router Advertisement Guard
- 6329 IS-IS Extensions supporting Shortest Path Bridging
- 6933 Entity MIBv4 (一部のみサポート)
- 7358 VXLAN: A Framework for Overlaying Virtualized L2 Networks over L3 Networks (一部のみサポート)
- 7610 DHCPv6 Shield: Protecting against Rogue DHCPv6 Servers
- Internet-Draft IP/IPVPN services with IEEE 802.1aq SPB networks (draft-unbehagen-spb-ip-ipvpn-00)
- Internet-Draft SPB Deployment Considerations (draft-lapuh-spb-deployment-03)

MTBF

(単一の電源を装備したベース ユニット)

- VSP 4450GSX-PWR+: 最大 293,000 時間 (33.44 年)
- VSP 4450GSX-DC: 最大 308,000 時間 (35.15 年)
- VSP 4450GTX-HT-PWR+: 最大 224,500 時間 (25.62 年)
- VSP 4850GTS: 最大 311,104 時間 (35.51 年)
- VSP 4850GTS-PWR+: 最大 214,542 時間 (24.49 年)
- VSP 4850GTS-DC: 最大 311,104 時間 (35.51 年)

1 制御プレーン トラフィックに IPsec 機能を提供する目的でのみ実装されています。

発注情報

部品番号*	説明
EC4400A05-E6	VSP 4450GSX-PWR+ 50 ポート イーサネット スイッチ。36 x 1000BASE-SFP ポート、12 x 10/100/1000BASE-T ポート (PoE+ 対応)、2 x 10GBASE-SFP+ アップリンク ポートをサポート。単一の 1000 W AC 電源、基本ソフトウェア ライセンスが付属。
EC4400004-E6	VSP 4450GSX-DC 50 ポート イーサネット スイッチ。36 x 1000BASE-SFP ポート、12 x 10/100/1000BASE-T ポート、2 x 10GBASE-SFP+ アップリンク ポートをサポート。単一の 300 W DC 電源、DC コネクタ、基本ソフトウェア ライセンスが付属。
EC4400A03-E6	VSP 4450GTX-HT-PWR+ 50 ポート高温対応イーサネット スイッチ。48 x 10/100/1000BASE-T ポート (PoE+ 対応、2 x 1000BASE-SFP コンボ ポートを含む)、2 x 10GBASE-SFP+ アップリンク ポートをサポート。単一の 1000 W AC 電源、基本ソフトウェア ライセンスが付属。
EC4800A78-E6	VSP 4850GTS 50 ポート イーサネット スイッチ。48 x 10/100/1000BASE-T ポート (2 x 1000BASE-SFP コンボ ポートを含む)、2 x 10GBASE-SFP+ アップリンク ポートをサポート。単一の 300 W AC 電源、基本ソフトウェア ライセンスが付属。
EC4800A88-E6	VSP 4850GTS-PWR+50 ポート イーサネット スイッチ。48 x 10/100/1000BASE-T ポート (PoE+ 対応、2 x 1000BASE-SFP コンボ ポートを含む)、2 x 10GBASE-SFP+ アップリンク ポートをサポート。単一の 1000 W AC 電源、基本ソフトウェア ライセンスが付属。
EC4800078-E6	VSP 4850GTS-DC 50 ポート イーサネット スイッチ。48 x 10/100/1000BASE-T ポート (2 x 1000BASE-SFP コンボ ポートを含む)、2 x 10GBASE-SFP+ アップリンク ポートをサポート。単一の 300 W DC 電源、DC コネクタ、基本ソフトウェア ライセンスが付属。

冗長電源

部品番号*	説明
AL1905A08-E5	VSP 4850GTS 用 300 W AC 電源。電源コードは別途注文が必要。
AL1905A21-E6	VSP 4450GSX-PWR+ および VSP 4850GTS-PWR+ 用 1,000 W AC 電源。電源コードは別途注文が必要。
EC4005A03-E6HT	VSP 4450GTX-HT-PWR+ 用 1,000 W AC 電源 (色はミディアム グレー)。電源コードは別途注文が必要。
AL1905005-E5	VSP 4450GSX-DC および VSP 4850GTS-DC 用 300 W DC 電源 ² 。DC コネクタ付属。

注: スイッチと電源装置には電源コードが含まれていないため、別途注文が必要です。提供されている電源コードのリストについては、<http://bit.ly/2q1YBgo> で VSP 電源コード モデルに関するライフサイクル通知を参照してください。

² この PSU は、PoE をサポートしておらず、非 PWR+ VSP 4000 モデルのみを対象としています。

ライセンス

ほとんどの機能は、ハードウェアの購入時に付帯する基本ソフトウェア ライセンスによって利用できます。ただし、プレミアムソフトウェア ライセンスによって有効となることが特に記載されている場合はこの限りではありません。

オプションのアクセサリであるプレミアム ソフトウェア ライセンスを適用すると、レイヤー 3 仮想サービス ネットワーク、分散仮想ルーティング、24 を超える仮想ルーティングと転送のインスタンスの各機能のほか、現地の法規制が許す場合は、MACsec を利用できるようになります。

部品番号	説明
338835	VSP 4000 シリーズ プレミアソフトウェア ライセンス: L3 VSN、DvR リーフ、24 超の VRF、MACsec を有効化。
338836	VSP 4000 シリーズ プレミアソフトウェア ライセンス: L3 VSN、DvR リーフ、24 超の VRF を有効化。



エクストリーム ネットワークス株式会社 / Email extremejapan@extremenetworks.com

©2018 Extreme Networks, Inc. All rights reserved. Extreme Networks および Extreme Networks のロゴは、米国およびその他の国における Extreme Networks, Inc. の商標または登録商標です。その他のすべての名称は、該当する所有者の資産です。Extreme Networks の商標の詳細については、<http://www.extremenetworks.com/company/legal/trademarks> をご覧ください。製品の仕様や提供状況は予告なく変更される場合があります。16913-0618-01 UC7264-13