

Cisco Catalyst 9000

新時代のインテントベース
ネットワーキングを実現する
スイッチ



Cisco Catalyst 9000

新時代のネットワーキングを実現するスイッチ

このマニュアルについて	7
作成者	8
謝辞	9
本書の構成	10
対象読者	11
執筆の方法論	12
はじめに	13
要旨	14
業界トレンド	17
ビジネス事例	19
Catalyst 9000 ファミリ	23
概要	24
Catalyst 9300	26
Catalyst 9400	30
Catalyst 9500	39
25 G と 100 G - 企業での高速接続を実現	45
パッケージング、ライセンス、サポート	47

ASIC - プログラマブル回路の力	51
ASIC とは	52
プログラマブル ASIC を使用する理由	55
UADP - プログラマブル ASIC チップ	59
UADP ファミリ	66
Cisco IOS XE	70
IOS の進化	71
Cisco IOS XE のアーキテクチャ	74
Cisco IOS XE の利点	77
高可用性	79
概要	80
Catalyst 9300 の高可用性	82
Catalyst 9400 の高可用性	88
StackWise Virtual	95
グレースフル挿抜	101
Cisco IOS XE へのパッチの適用	104

セキュリティと ID 106

概要	107
暗号化トラフィック分析	108
信頼できるシステム	112
MACsec	115

QoS およびキューイング 120

概要	121
バッファとキュー	123
UADP ASIC における QoS およびキューイング	128
階層型 QoS	133
Stackwise Virtual の QoS	137
オーバーレイ テクノロジーの QoS	138

アプリケーションの可視性およびコントロール 143

概要	144
アプリケーションの認識	145
アプリケーション制御	148

IoT	149
概要	150
Power over Ethernet のイノベーション	151
AVB - オーディオ ビデオ ブリッジング	154
Bonjour 向け Cisco DNA サービス	156
ユーザ中心の プラットフォーム設計	158
概要	159
RFID	160
ブルー ビーコン	161
Bluetooth コンソール	162
WebUI	163
フレキシブル テンプレート	164
プログラマビリティおよび自動化	167
概要	168
デバイス プロビジョニング	170
オープンなプログラマブル デバイス API	172
データ モデル	174
デバイス API プロトコル	177
モデル駆動型テレメトリ	182
スクリプティング	184
設定管理ツール	186
Cisco DevNet	188

アプリケーション ホスティング	189
アプリケーション ホスティングの運用	190
ハードウェア リソース	192

キャンパス ネットワーク設計	193
概要	194
物理インフラストラクチャ	197
マルチレイヤ キャンパス	202
コラプスト コア	205
ルーテッド アクセス	207
キャンパス MPLS	209
キャンパス ワイヤレス	212
SD-Access	216

付録	220
参考資料	221
略語	223

このマニュアルについて

作成者

本書は、カリフォルニア州サンノゼにあるシスコ本社で 1 週間にわたって実施された集中セッションにおいてテクニカル マーケティング、製品管理、エンジニアリング、セールスの諸チームが取り組んだコラボレーションの成果物です。

- Bob Sayle - セールス
- Dave Zacks - テクニカル マーケティング
- Dimitar Hristov - テクニカル マーケティング
- Fabrizio Maccioni - テクニカル マーケティング
- Ivor Diedricks - 製品管理
- Jay Yoo - エンジニアリング
- Kenny Lei - テクニカル マーケティング
- Mahesh Nagireddy - テクニカル マーケティング
- Minhaj Uddin - テクニカル マーケティング
- Muhammad Imam - テクニカル マーケティング
- Sai Zeya - テクニカル マーケティング
- Shawn Wargo - テクニカル マーケティング

謝辞

本書の実現を支えてくれたシスコのエンタープライズ ネットワーク ビジネス製品管理、エンジニアリング、セールスの各チームに感謝します。この取り組みをサポートしてくれた Carl Solder と Muninder Sambi に感謝します。また、リソースの調整に優れた手腕を発揮して終始サポートしてくれた Cynthia Resendez と、計画立案やロジスティクスの面で協力してくれた Sehjung Hah にも感謝します。

あわせて、Book Sprints (www.booksprints.net) チームにも心より感謝申し上げます。

- Adam Hyde (創立者)
- Barbara Rühling (CEO 兼ファシリテータ)
- Henrik van Leeuwen (イラストレータ)
- Juan Carlos Gutiérrez Barquero (テクニカル サポート)
- Agathe Baëz (書籍プロデューサ)
- Raewyn Whyte、Susan Tearne (校正)
- Barbara の率いるチームが環境を整えてくれたおかげで、私たちは、拡大する需要に応えるべく、コラボレーションと技術的スキルを駆使してこの技術書を作り上げることができました。

本書の構成

本書は最初から順に読むことをお勧めします。ただし、読者の役割や関心に応じて、いくつかの章を順番にとらわれずに参照することも可能です。本書は複数のセクションで構成されており、各セクションは複数の章に分かれています。

本書では、Catalyst 9000 ファミリを紹介し、企業のビジネス ドライバを検証して、企業の IT が直面している課題に Catalyst 9000 で対応する方法について説明します。さらに、Catalyst 9000 プラットフォームのアーキテクチャ基盤について、シスコの革新的な Unified Access Data Plane (UADP; ユニファイド アクセス データ プレーン) ASIC を搭載したハードウェアの観点と、Cisco IOS XE ソフトウェアによって提供される最新機能の観点の、両側面から掘り下げていきます。この両要素は、今日のエンタープライズ ネットワークに対するさまざまな要求に Catalyst 9000 ファミリが対処するための基盤となっています。

これらの要求に Catalyst 9000 プラットフォームで対応する方法については、次のセクションに概要をまとめています。そのセクションでは、高可用性、セキュリティ、QoS、Application Visibility and Control、IoT、ユーザ中心のプラットフォーム設計について取り上げています。Cisco IOS XE ソフトウェアでは、ネットワーク管理インターフェイスに対して、標準に準拠したオープンなモデルベース アプローチが採用されています。これらの機能についてはプログラマビリティおよび自動化のセクションで扱います。その後、Catalyst 9000 でのアプリケーション ホスティングについて考察します。最後に、ネットワーク設計の現状および今後の発展や、エンタープライズ ネットワーク アーキテクチャの継続的な変革に向けて Catalyst 9000 が果たす主導的役割について考察します。

対象読者

ネットワーク管理者、エンジニア、アーキテクトは、組織のビジネス ニーズに応えるプレッシャーに常にさらされています。本書では、シスコの革新的な Catalyst 9000 ファミリー スイッチに焦点を置き、ネットワークの専門家が現在直面している多くの課題の解決にどのように役立つのか説明します。Catalyst 9000 は、柔軟性に優れたオープンで強力なハードウェアとソフトウェアによって、最新のテクノロジーを提供しています。ネットワークの専門家は、本書を活用することにより、Catalyst 9000 ファミリーを理解し、そのアーキテクチャを深く把握して、次世代ネットワークの強力な基盤となるツールであることを理解できるでしょう。

本書は、Catalyst 9000 による新時代のインテントベース ネットワーキングを理解し導入するためのガイドとして、ネットワーク専門家、IT マネージャ、エグゼクティブ、および最新の優れたネットワーク テクノロジーに関心があるすべての人に、ご活用いただけます。

執筆の方法論

完成を目指して集中すれば、ほぼすべてのものがそこに向かって急速に前進する

- W.E. Channing

Catalyst 9000 ファミリを設計する上で最も重視されているテーマは、シンプルさ、一貫性、パフォーマンスです。本書の目的は、エンタープライズ ネットワークにおける現在の課題を読者に示し、Catalyst 9000 プラットフォームによるその解決方法を検証することにあります。Catalyst 9000 は、最先端のハードウェアおよびソフトウェアの機能を提供しており、シンプルさを損なわずに将来のプロトコルとネットワーク アーキテクチャに容易に適応できます。本書では、新時代のネットワークの基礎となるこの強力な新しいネットワーク プラットフォームを、掘り下げて説明していきます。

エンタープライズ ネットワークのパラダイムを変えるプラットフォームについて書籍を執筆するという挑戦を引き受けたのは、多様なバックグラウンドを持つ 12 名のシスコのエンジニアです。執筆の初日を終えたとき、Catalyst 9000 によってネットワークにもたらされる機能の幅広さを思うと、改めてこの作業の難しさが感じられました。しかしチームは作業を続け、長時間にわたる精力的な執筆ののちに本書は誕生しました。Book Sprints (www.booksprints.net) の方法論によって、私たちならではの強みがそれぞれ盛り込まれ、チーム指向の環境が育まれて完成までの期間が短縮されました。

#NetworkIntuitive

#NewEraOfNetworking

はじめに

要旨

IoT の進化に対する需要、ユビキタス モビリティ、クラウド化、急激に拡大するセキュリティ脅威によって、世界は急速に変化しています。世界中のあらゆる規模の企業が、レガシー システムをデジタル テクノロジーに置き換え、競争優位性の確保、生産性の向上、運用コストの削減を目指しています。この変化に対応しようとする企業の増加に応じて、ネットワークも適応する必要があります。企業のネットワークの構築を、これまでの 30 年間と同じ方法で行うことはできません。組織は、継続的に学習、適応、保護、および進化できる動的なネットワークを構築する必要があります。

The Network. Intuitive. (ネットワークに直感を)

Cisco Digital Network Architecture (Cisco DNA) と Software-Defined Access (SD-Access) は、組織における機会創出、セキュリティ強化、俊敏性の向上、運用効率の改善を支援します。直感性を企図して設計されたネットワークが、インテント（目的）を理解し、セグメンテーションと暗号化によって脅威を軽減しながら、継続的な学習と変化を実現します。シスコの Catalyst 9000 スイッチは、エンタープライズ LAN アクセス/ディストリビューション/コア スイッチから成る名高い Catalyst ファミリの次世代製品であり、Cisco DNA と SD-Access を活用するために設計された最初の専用プラットフォームです。

新しい Cisco Catalyst 9000 ファミリ スイッチは、まったく新しいネットワーキング時代「The Network. Intuitive.」の基盤として設計されています。本書では、Catalyst 9000 ファミリ スイッチについて掘り下げていき、刻々と変化するエンタープライズ ネットワークのニーズに対し、このプラットフォームが現在から将来までどのように対応していくのか考察します。

業界で初めて固定型、スタックابل、およびモジュラ型のスイッチを 1 つのファミリ内に揃えたことにより、キャンパスおよびブランチ ネットワーク内のすべてのプラットフォームで、共通の ASIC により単一のソフトウェア イメージを実行することが可能になりました。設計の際にはネットワーク内各所の拡張性要件を考慮するだけで済むようになり、エンタープライズ ネットワークの総所有コスト (TCO) が大幅に削減されます。

Catalyst 9000 シリーズは、次の 2 つの基盤をベースに構築されています。

- **共通ハードウェア**：柔軟性に優れたプログラム可能な ASIC および CPU アーキテクチャを採用。
- **共通ソフトウェア**：オープンな Linux ベースのモジュラ型オペレーティング システムとシンプルな機能ライセンスを採用。



x86 マルチコア
CPU

セキュアなコンテナ アプリ
ケーション ホスティング



UADP
ASIC

プログラマブル パイプ
ライン 柔軟なテーブル



オープンで拡張可能な
Cisco IOS XE

モデル駆動型 API
ストリーミング テレメトリ

Catalyst 9000 ファミリは、**Unified Access Data Plane (UADP) ASIC** 搭載の共通 ASIC アーキテクチャをベースに構築されています。この ASIC は、プログラム可能で柔軟かつ革新的な、プラットフォームに特化したチップとして機能します。ネットワーク インフラストラクチャは、UADP によって、新しいテクノロジー、トレンド、ビジネス ニーズに継続的に適応することが可能になります。また、Catalyst 9000 のプラットフォームは、標準のマルチコア 64 ビット **x86 CPU** アーキテクチャをベースに構築されています。共通の CPU アーキテクチャによって、予測可能なソフトウェア処理とコントロール プレーンの管理が可能になります。それにより、次世代ネットワーク アーキテクチャに対応する処理能力を確保するとともに、アプリケーション ホスティングのプラットフォームを提供して問題の診断と解決を容易にします。

Catalyst 9000 プラットフォームはいずれも、オープンなモジュラ型**インターネット オペレーティング システム Cisco IOS XE** 上で稼働します。このため、シスコのエンタープライズ プラットフォーム（Catalyst スイッチ、ISR/ASR ルータ、ワイヤレス LAN コントローラを含む）全体でのポータビリティが向上します。それにより機能開発のスピードが増して、高可用性が向上し、キャンパス ネットワーク全体で一貫した機能を容易に導入できるようになります。Cisco IOS XE では、明確に定義された一連の API が用意されているため、管理性が向上し、自動化とプログラミングのシンプル化が実現します。

結論

Catalyst 9000 は、シスコの革新的な UADP ASIC、x86 CPU、Cisco IOS XE ソフトウェアを備えた共通のハードウェア/ソフトウェアをベースに構築されており、新時代のネットワークの基盤になります。

業界トレンド

現在、業界で一般的に見られるトレンドは、主に IoT、モビリティ、クラウド、セキュリティの4つのカテゴリに分類されます。

IoT のトレンドと考察

ビジネス プロセス/運用のデジタル変革の一貫として、生産性の向上、リスクの低減、セキュリティの強化を実現すべく、新しいデバイス、センサー、マシンが接続されています。今後数年の間に、何十億台ものマシン同士が接続され、分析とビジネス ポリシーに基づく機械学習インテリジェンスが必要になっていくでしょう。エンタープライズ キャンパス ネットワークには、このように増え続けるマシン間接続をサポートすることが求められます。

シスコの調査「Internet of Things: Workloads and Key Projects 2017 (Internet of Things : ワークロードとキー プロジェクト 2017) 」によると、組織における IoT データの集約、フィルタリング、分析は、ネットワーク エッジにおいて実施されるだろうと予測されています。ネットワーク エッジでの IoT データ処理を推進する主な要因は、セキュリティの強化およびデータ分析の高速化です。ネットワークは、IoT の現在および将来の要求に応えられるよう進化する必要があります。

モビリティのトレンドと考察

ワイヤレスおよびモビリティは、エンタープライズ ネットワーク インフラストラクチャ市場を活性化しています。BYOD およびモバイル アプリケーションを活用することで、従業員がスマートフォン、タブレット、個人のラップトップから企業データにアクセスすることが可能になりました。それにより、バックエンドの IT インフラストラクチャに新たな課題が発生するとともに、従業員の間でエンタープライズ モビリティへの需要が高まっています。モビリティは今や戦略的資産です。従業員やゲストが社内ネットワークとインターネットにアクセスするための主要な手段になっています。モビリティは、間違いなく今後のエンタープライズ ネットワークに欠かせない要素となるでしょう。

クラウドのトレンドと考察

企業は、プライベート クラウド（オンプレミスまたはコロケーション）やパブリック クラウドのクラウド サービスによって、社内 IT を強化しようとしています。クラウド インフラストラクチャでは、仮想と物理の要素が混在し、ワークロードはオンプレミスとオフプレミスのリソース間を移動します。キャンパス ネットワークは、オフプレミスおよびパブリック クラウドとインターフェイスを取るだけでなく、オンプレミス稼動時に匹敵するアプリケーション パフォーマンス、セキュリティ、ポリシー準拠を、ワークロードに対して確保する必要があります。

セキュリティのトレンドと考察

これらの新しい接続によって、セキュリティの意義がますます大きくなっています。新しい接続はすべて、攻撃ベクトルとなる可能性があります。攻撃の巧妙化はいっそう進み、さらに困ったことに、多くの場合、暗号化によって検出が難しくなっています。キャンパス ネットワークには、広範囲でリアルタイムに異常を検出し、悪意の可能性のあるふるまいやパターンを認識することで、これら新しい接続のセキュリティを確保することが必要になります。

ビジネス事例

Catalyst 9000 スイッチは、IoT、モビリティ、クラウド、セキュリティにおける画期的なイノベーションによって、ネットワーキング分野でのシスコのリーダーシップを拡大します。

IoT 事例での活用

ネットワークには、センサー、アラーム システム、HVAC システム、バッジ リーダーなど、従来は接続されなかったデバイスや、独自のプロトコルが使用されていたデバイスが、新たに多数接続されています。Catalyst 9000 プラットフォームは Cisco Identity Services Engine (ISE) と連携してこれらのデバイスを自動的にプロファイリングして、セキュリティとセグメント化を提供し、ポリシーを適用することができます。

デバイスは、Bonjour (mDNS) プロトコルを使用して、サービスのアドバタイズを始めます。Bonjour 向け Cisco DNA Service は、ネットワークの場所やセグメント全体でこれらのサービスを可視化し、サービスに基づいてポリシーを適用します。また、Cisco DNA Center によってすべてのサービスを一元的にオーケストレーションします。

たとえば LED 照明などの一部の IoT デバイスは、常時電力を必要とします。Catalyst 9000 では、無停止型 PoE および高速 PoE がサポートされ、スイッチがリロードされる間も照明が維持されます。

プロフェッショナル メディアや音声アプリケーションに対応するために、Catalyst 9000 は Audio Video Bridging (AVB) と IEEE 1588 時刻同期をサポートしています。

結論

Catalyst 9000 は、Internet of Things (IoT) の接続に最適なプラットフォームです。

モビリティ事例での活用

有線ネットワークとワイヤレス ネットワークは、これまで別々のチームで構築・運用されてきました。Catalyst 9000 と SD-Access によって一元的なオーケストレーションが可能になり、有線とワイヤレスを統合した 1 つのネットワークが確保されます。これにより、ワイヤレス クライアントがネットワークにさらに追加されても、ボトルネックを発生させずにネットワークをシームレスに拡張できます。AP は Catalyst 9000 スイッチに直接接続し、ハードウェアでのデータ プレーンによる直接転送が可能になります。

このネットワーク アーキテクチャでは、有線とワイヤレスに同じポリシーが適用されます。有線とワイヤレスのトラフィック間でネットワーク セグメンテーションとグループベースのポリシーが一貫しているため、運用がシンプルになります。

SD-Access アーキテクチャによって、ネットワーク中の全デバイスで、シンプルかつシームレスなローミングが実現します。

Catalyst 9000 では、業界トップクラスの mGig および PoE 性能が提供されているため、802.11ac Wave 2 や将来のワイヤレス イノベーションを活用した高密度のワイヤレス環境の構築が可能です。

結論

Catalyst 9000 は、有線とワイヤレスのアクセスを統合するための最適な基盤を提供します。

クラウド事例での活用

ネットワークの導入と運用をより迅速にするために、シスコは、プログラマティック フレームワークとツールを追加して、YANG モデルを使用した gNMI API、RESTCONF、NETCONF による自動化の活用を推進しています。

ストーリーミング テレメトリによって、ほぼリアルタイムでの運用データの可視化が促進されます。

Catalyst 9000 は、ローカル ストレージでのアプリケーション ホスティングをサポートし、フォグ コンピューティングやネットワーク機能仮想化を実現しています。これにより、ネットワークに注入される分散型インテリジェント エージェントをサポートして、分析、アシュアランス、セキュリティ、クラウドベース アプリケーションに活用しています。Catalyst 9000 プラットフォームはサードパーティ製アプリケーションをホストすることができ、業界トップクラスの柔軟性を提供します。

結論

Catalyst 9000 は、クラウドへの移行を実現する、完全プログラム可能なオープン プラットフォームです。

セキュリティ事例での活用

エンタープライズ ネットワークに接続するデバイスは多様であり、数も拡大しています。許可された通信だけが可能になるようデバイスやユーザを制限するために、ネットワークのセグメント化を使用することができます。Catalyst 9000 プラットフォームは、ハードウェアで SD-Access、MPLS、VRF-Lite、TrustSec に対応し、マクロレベル（ネットワーク セグメント）およびミクロ レベル（ユーザまたはデバイス グループ）でのさまざまなセグメント化機能を備えています。

暗号化されるネットワーク トラフィックの増加に伴い、ネットワークとの接続点でこれらの脅威を検出して軽減することが重要になっています。Catalyst 9000 は、Encrypted Traffic Analytics (ETA; 暗号化トラフィック分析) 機能を使用して、暗号化されたトラフィックに潜むマルウェアを検出してその脅威を軽減します。ETA のさらなる利点として、暗号化されたトラフィックを復号せずに、その中の異常を検出することが可能です。

Catalyst 9000 は、フル Flexible Netflow を使用して、ネットワークを通過するすべてのフローについてのメタデータをハードウェアで収集します。これを Cisco Stealthwatch などのシスコのセキュリティ ソリューションと組み合わせることで、サービス妨害攻撃やその他の悪意あるアクティビティを検出できます。

Catalyst 9000 では、ライン レートで動作しながら、最大 256 ビットの AES MACsec を使用してスイッチ間リンクを暗号化することができます。この暗号化機能は、スイッチとエンドポイント間の接続にも使用できます。

最後に、Cisco Trustworthy Systems セキュリティ ソリューションによって、ネットワーク スイッチ自体も保護されます。デバイス、ネットワーク通信、ホストされたアプリケーションを保護することで、ハードウェアとソフトウェアの整合性を、統合アプローチによって包括的に検証することが可能です。

結論

Catalyst 9000 は、ネットワーク業界でトップクラスの安全性を誇るスイッチング環境を提供します。

Catalyst 9000 ファミリ

概要

新しい Cisco Catalyst 9000 スイッチ プラットフォームは、エンタープライズ LAN アクセス/ディストリビューション/コア スイッチから成る Cisco Catalyst ファミリの次世代製品であり、Cisco DNA と SD-Access を活用するために設計された最初の専用プラットフォームです。この新しいスイッチング システムは、モビリティ、IoT、クラウド、セキュリティにおける画期的なイノベーションによって、ネットワーキング分野でのシスコのリーダーシップを拡大します。Cisco Catalyst 9000 プラットフォームは、UADP ASIC を活用して、はるかに高いパフォーマンスを実現するとともに、新しい機能や特長を数多く追加しています。

図 Catalyst 9000 スイッチ



Catalyst 9000 スイッチング プラットフォームは、強力な共通のハードウェアとソフトウェアを基盤として構築されています。この共通性と一貫性により、ネットワーク エンジニアや管理者にとって運用がシンプルかつ容易になるため、総運用コストが削減され、操作性が向上します。

共通ハードウェア

ハードウェアには、内部的にも外部的にも共通の設計が採用されています。ハードウェア内部では、共通の ASIC である Unified Access Data Plane (UADP) ASIC が使用され、パケットを柔軟に処理できるようになっています。ハードウェアには、共通コンポーネントがもう 1 つあります。スイッチ CPU です。Catalyst スイッチとしては初めて x86 ベース CPU をオンボードに搭載したことで、ネットワーク スイッチで通常可能なアプリケーション以外のアプリケーションも追加してホストすることが可能になっています。

ハードウェア外部は、世界最高のデザイナーの 1 人である Pininfarina 氏によって設計されました。Pininfarina 氏は、有名なフェラーリのデザイナーです。このような優れたインダストリアル デザインが、Catalyst 9000 ファミリのユーザ エクスペリエンスを向上させ、人間工学に基づいたデザインと属性の共通化によって、デバイスの運用がシンプルになっています。詳細については、第 11 章「ユーザ中心のプラットフォーム設計」を参照してください。

共通ソフトウェア

Catalyst 9000 ファミリ スイッチでは、**まったく同じ Cisco IOS XE バイナリ イメージ**が実行されます。Cisco IOS XE は、オープンでプログラム可能な、強化された OS です。30 年に及ぶ歴史と多くの機能を持つ Cisco IOS XE は、機能の充実度の点でネットワーク業界トップクラスと言っても過言ではないでしょう。Catalyst 9000 プラットフォーム全体で 1 つのバイナリ イメージを共有することで、機能がエンドツーエンドでサポートされ、ネットワーク内のどこにおいても同等の機能が可能になります。また、ソフトウェアリリースの際、キャンパス ネットワーク全体で 1 つのイメージをテストするだけで済むので、対象の絞り込みにも役立ちます。

Catalyst 9000 は、強力なハードウェアおよびソフトウェア基盤によって、現在のエンタープライズ ネットワークが抱える課題に対応することができます。同時に、お客様にとっての一貫性とシンプルさをもたらします。Catalyst 9000 ファミリは、Catalyst 9300 (スタックブル)、Catalyst 9400 (モジュラ型シャーシ)、Catalyst 9500 (固定構成コア) の 3 つのメンバーで構成されています。各プラットフォームについては、後続の章で詳しく説明します。

Catalyst 9300

Cisco Catalyst 9300 シリーズは、シスコのスタックابل エンタープライズ固定スイッチング プラットフォームの主要製品です。スタッキング帯域幅が 480 Gbps、1 スタックあたりの最大デバイス数が 8 台の Catalyst 9300 は、業界トップクラスの密度を誇る帯域幅スタッキング ソリューションです。

 Catalyst 9300



プラットフォーム概要

Catalyst 9300 はどのモデルも、高さが 1 RU で、デュアル電源装置と冗長ファンを備えています。接続性と拡張性は各モデルによって異なります。これらのモデルは、以下の 4 つのサブファミリに分類されます。どのサブファミリにも、24 ポートおよび 48 ポートの銅線モデルが含まれています。

- 1 データ専用モデル：デスクトップやプリンタなど、10 Mbps ~ 1 Gbps のデータ接続しか必要としないデバイス用に最適化されたモデル。
- 2 PoE/PoE+ モデル：データ モデルと同じ機能に加え、30 W の Power over Ethernet (PoE+) 機能をサポートしたモデル。すべてのポートが PoE/PoE+ をサポートしており、すべてのポートで同時に PoE+ をアクティブにすることができます。

- 3 UPoE モデル : PoE+ モデルと同じ機能に加え、60 W の PoE 機能をサポートしたモデル。任意のポートに UPoE を設定できますが、スイッチ 1 台あたりで使用可能な PoE 電力は合計 1,800 W です。
- 4 mGig モデル : mGig ポートにおいて最大 10 Gbps の複数のスピードでの接続が可能なモデル。mGig 接続を必要とするデバイスとして最も一般的なのは 802.11 ac Wave 2 をサポートするワイヤレス アクセス ポイントですが、デスクトップへの有線接続に使用しても利点があります。このモデルではすべてのポートで UPoE をサポートしていますが、スイッチ 1 台あたりで使用可能な PoE は合計 1,800 W です。このサブファミリには、以下の 2 つのモデルがあります。
 - 24 ポート mGig : 24 ポートすべてで、100 Mbps、1 Gbps、2.5 Gbps、5 Gbps、10 Gbps をサポートします。
 - 48 ポート混在 mGig : 最初の 36 ポートが 100 Mbps、1 Gbps、2.5 Gbps をサポートし、残りの 12 ポートは全帯域の mGig 速度をサポートします。

ネットワーク モジュール

Catalyst 9300 のすべてのスイッチに、オプションとして、アップリンク ネットワーク モジュール用のスロットが 1 つ用意されています。アップリンク モジュールには 4 つの種類があります。また、これらのモジュール上のポートはアップリンク接続のみに制限されているのではなく、ホストへの接続にも使用できます。

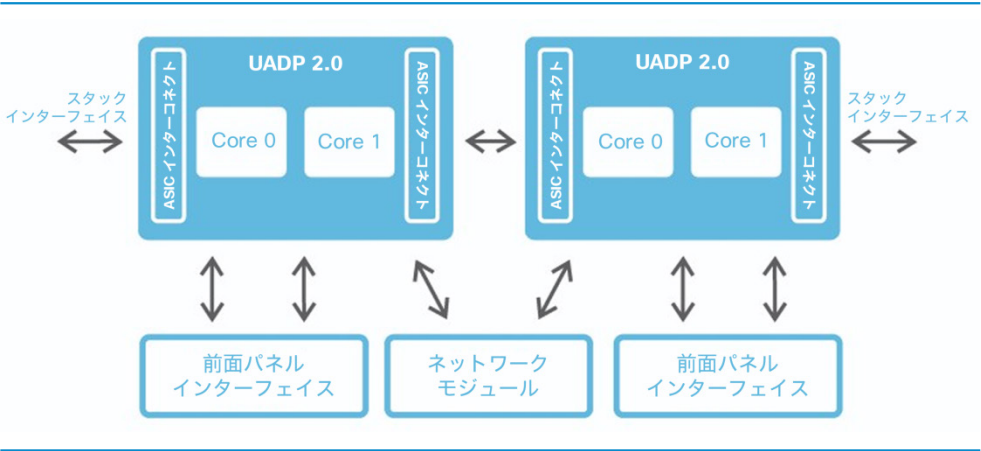
- 1 1 G RJ-45 ポート X 4 (10 Mbps、100 Mbps、1 Gbps サポート)
- 2 mGig ポート X 4 (PoE なし)
- 3 10 G SFP+/SFP ポート X 8
- 4 40 G QSFP+ ポート X 2
- 5 25 G SFP28 ポート X 2

Catalyst 9300 スイッチは、Catalyst 3850 アップリンク モジュールと互換性があります。ただし、Catalyst 9300 アップリンク モジュールには、Catalyst 3850 との互換性はありません。

アーキテクチャ

Catalyst 9300 の非 mGig モデルには、UADP 2.0 ASIC が 1 つ搭載されています。mGig モデルには 2 つの UADP 2.0 ASIC が搭載されています。Catalyst 9300 では、パケット サイズを問わず、すべてのポートがライン レートで動作します。

図 Catalyst 9300 のアーキテクチャ



StackWise-480

Catalyst 9300 では、最大 8 台のスイッチをスタックして統合し、1 台の論理スイッチとして動作させることが可能です。これにより、ネットワーク エンジニアがスイッチのスタックを 1 つのスイッチとして管理、設定、トラブルシューティングすることが可能になります。StackWise-480 の動作については、第 6 章「高可用性」で詳しく説明します。

電源装置およびファン

Catalyst 9300 スイッチは、デュアル冗長電源装置をサポートしています。この電源装置は、350 W AC、715 W AC、1,100 W AC、および 715 W DC オプションで利用可能です。電源装置は、たとえば AC と DC など、どのような組み合わせでも使用できます。

Catalyst 9300 スイッチには、現場交換可能な 3 つのファンが搭載されています。これらのファンは、N+1 冗長モードで稼働します。

StackPower

Catalyst 9300 には、専用の StackPower ケーブルを使用して共有の電力プールを作成する機能があります。電源装置の障害が発生した場合や、PoE 電力消費が増えた場合、スイッチは、共有プールの電力を利用して追加の負荷に対応できます。StackPower は、電力共有モードまたは冗長モードの 2 つのモードで導入できます。詳細については、第 6 章「高可用性」を参照してください。

Catalyst 9400

Cisco Catalyst 9400 シリーズは、シスコのモジュラ エンタープライズ スイッチング アクセス プラットフォームの主要製品です。最大 9 Tbps のシステム帯域幅をサポートするシャーシ アーキテクチャにより、将来にわたって、類のない投資保護を提供します。また、高密度 PoE 導入向けの電力供給性能に優れ、エンドポイントに対して 60 W の Power over Ethernet を提供します。9400 シリーズは、デュアル スーパーバイザや N+1/N+N 電源冗長性などの機能により、最新の高可用性を実現しています。このプラットフォームは、革新的なデュアル サービス対応ファントレイ設計と横方向のエアフローによってエンタープライズ向けに最適化され、クローゼットに収納しやすい約 16 インチ以内の奥行きとなっています。1つのシステムで最大 384 アクセスポートまで拡張できます。

🖼 Catalyst 9400 ファミリ



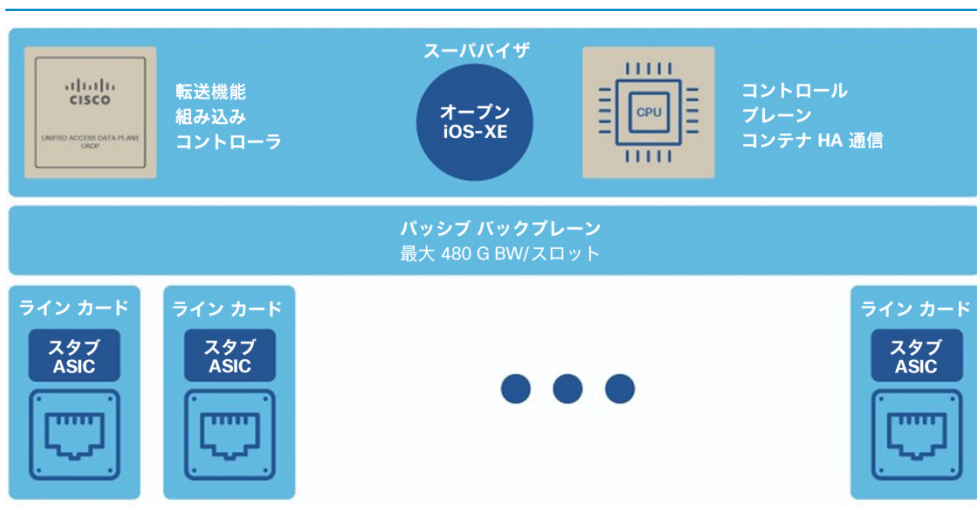
プラットフォーム概要

Catalyst 9400 スイッチは、スロット 1 つあたり最大 480 G の帯域幅を提供します。さまざまなサイズ要件に対応するために、密度の異なる 3 種類のシャーシ モデル（4、7、10 スロット）を用意しています。3 つのシャーシ オプションすべてが、デュアル スーパーバイザ スロットを備えて高い可用性を実現しています。シャーシは、2 つのスーパーバイザ スロット間で 720 G 以上の帯域幅をサポートする設計になっており、将来のスーパーバイザでは複数の 100 G ポートをサポートできるようになります。Power over Ethernet へのニーズの高まりに対応するために、スロット 1 つあたり 4,800 W 以上の PoE 電力を供給できる性能を備えています。

アーキテクチャ

Catalyst 9400 には、一元化アーキテクチャが採用されています。つまり、転送、サービス、キューイングはすべてスーパーバイザで実施され、その一方で、ライン カードは、スタブ ASIC と PHY のみを備えた透過的なものとみなされます。この一元化されたシンプルな設計によって、既存のライン カードは残したままスーパーバイザだけをアップグレードすることで、機能のアップグレードが簡単にできるようになります。そのため、投資が大幅に保護されます。

図 Catalyst 9400 のアーキテクチャ



スーパーバイザ

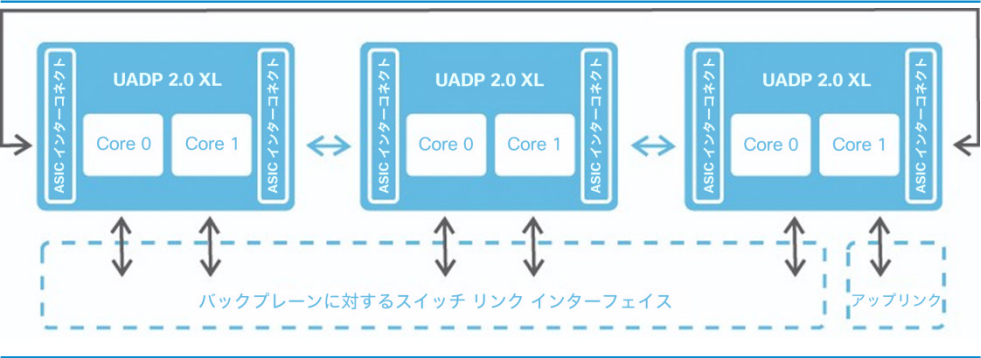
現在 Catalyst 9400 では、Sup-1 と Sup-1XL の 2 つのバージョンのスーパーバイザを利用できます。どちらのスーパーバイザにも 3 つの UADP 2.0 XL ASIC が使用されています。3 つの ASIC は 720 G ASIC インターコネクトで相互に接続され、各 ASIC 間でパケットが転送されます。

Sup-1 は、すべてのシャーシ モデルにおいてスロット 1 つあたり 80 Gbps の帯域幅を提供し、アクセス環境に最適化されています。

Sup-1XL は、10 スロット シャーシでは 80 Gbps/スロット、7 スロット シャーシでは 120 Gbps/スロット、4 スロット シャーシでは 240 Gbps/スロットの帯域幅をそれぞれ提供します。また、Sup-1XL は、各種テンプレートも柔軟にサポートして、アクセス、ディストリビューション、コア、SD-Access、NAT などのさまざまな導入モデルに対応しています。

UADP には、バックプレーンを介してライン カードのスタブ デバイスを接続する Switch Link Interface (SLI) があります。Sup-1/Sup-1XL では各 SLI は 10 G レートで動作し、前面パネルの一連のポートを集約します。これを SLI ポート グループと呼んでいます。将来のスーパーバイザでは SLI はさらに高速で動作し、既存のライン カードに対して、より多くの帯域幅を提供できるようになります。そのため、既存のライン カードへの投資がさらに保護されます。

図 Catalyst 9400 Sup-1XL のアーキテクチャ



スーパーバイザ アップリンク

Sup-1 と Sup-1XL はどちらも、8 つの SFP/SFP+ ポートと 2 つの QSPF+ ポートを前面に備えています。Sup-1 と Sup-1XL のアーキテクチャは、トータルで 80 G のアップリンク帯域幅を提供し、1 G/10 G/40 G インターフェイスをサポートしています。インターフェイス 1 ~ 8 は 1 G/10 G SFP/SFP+ をサポートし、インターフェイス 9 および 10 は 40 G QSFP をサポートします。

ライン カード

Catalyst 9400 スイッチは、mGig、Cisco UPoE、データ転送、10 G ライン カードを提供して、さまざまな接続要件に対応しています。

- 銅線 RJ-45 モジュール：

- 1 48 ポート データ ライン カード：このモジュールの 48 ポートすべてで 10 Mbps、100 Mbps、1 Gbps がサポートされています。
- 2 48 ポート PoE+/PoE ライン カード：データ ライン カードでサポートされるすべての機能に加え、PoE+ (30 W) および PoE (15.4 W) をサポートしています。
- 3 48 ポート UPoE ライン カード：PoE+/PoE ライン カードでサポートされるすべての機能に加え、UPoE (60 W) もサポートしています。スロット内の 48 ポートすべてで UPoE を同時に提供できます。
- 4 48 ポート mGig ライン カード：最初の 24 ポートは従来の 10/100/1000 銅線 RJ-45 ポートで、残りの 24 ポートは 100 Mbps、1 Gbps、2.5 Gbps、5 Gbps、10 Gbps をサポートする mGig ポートです。このモジュールの 48 ポートすべてで UPoE (60 W)、PoE+ (30 W)、PoE (15 W) がサポートされています。スロット内の 48 ポートすべてで UPoE を同時に提供できます。

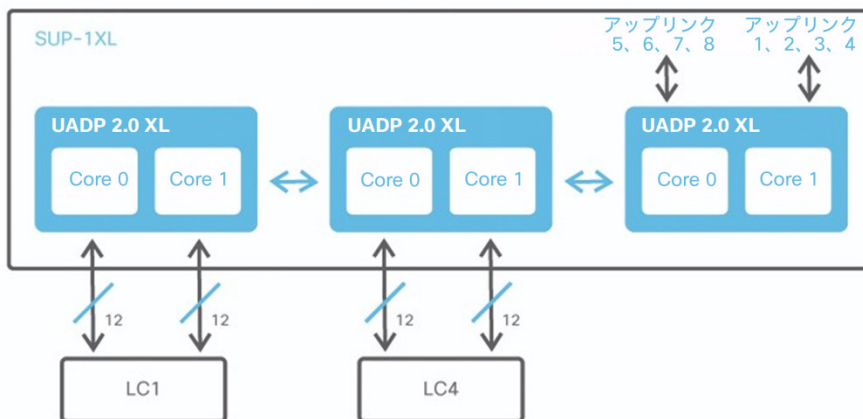
- 光ファイバ SFP/SFP+ モジュール：

- 1 24 ポート SFP ライン カード：100 Mbps および 1 Gbps の速度をサポートしています。
- 2 48 ポート SFP ライン カード：24 ポート SFP ライン カードの 2 倍の密度に対応しています。
- 3 24 ポート SFP+/SFP ライン カード：100 Mbps、1 Gbps、10 Gbps をサポートしています。これらのポートは、アップリンク デバイスだけでなく 10 G ホストへの接続にも使用できます。

ライン カード スロットの帯域幅

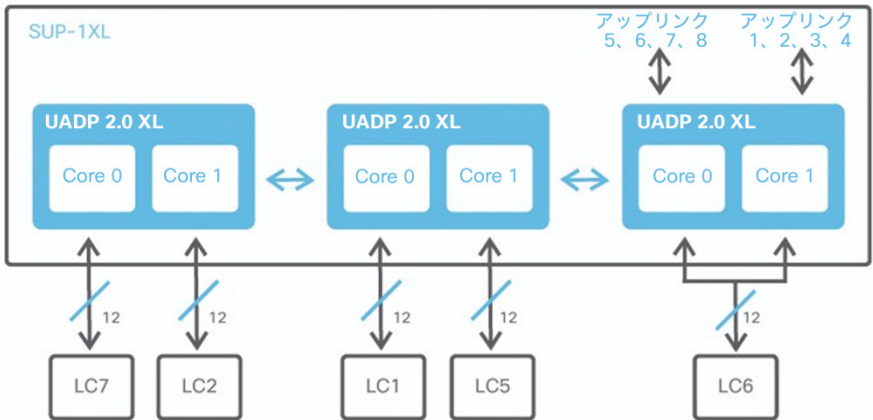
次の 3 つの図は、4 スロット、7 スロット、10 スロットのシャーシで Sup-1XL 帯域幅がライン カードのサポートに使用される様子を示しています。また、各ライン カードへの SLI 数の配分も示しています。

図 4 スロット シャーシ



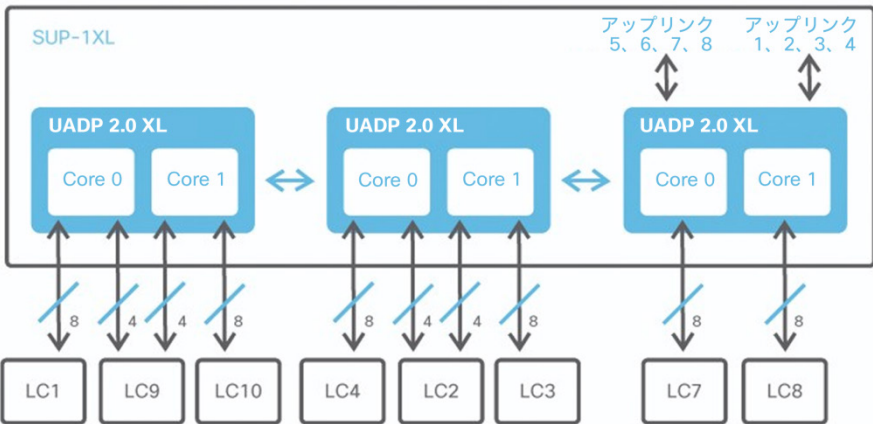
4 スロット シャーシ：各ライン カード スロットに対して 24 の SLI がアクティブ。各 UADP が 1 つのライン カードに対応。

図 7 スロット シャーシ



7 スロット シャーシ : 各ライン カード スロットに対して 12 の SLI がアクティブ。各 UADP が 2 つのライン カードに対応。

図 10 スロット シャーシ



10 スロット シャーシ : 各ライン カード スロットに対して 8 つの SLI がアクティブ。各 UADP が 3 つのライン カードに対応。

ライン カードのオーバーサブスクリプション

1 G ライン カードは、どのバリエーションにおいても、すべてのパケット サイズに対してライン レートで動作します。10 G 光ファイバ ライン カードと mGig ライン カードは、Sup-1 と Sup-1XL によりオーバーサブスクリプションになります。また、ライン カードは、より高速で動作する SLI の数を増やすことで、将来のスーパバイザにおけるスロット帯域幅の拡大を活用できるよう設計されており、その点に留意することも大切です。

ライン カードのパフォーマンス モード

オーバーサブスクライブされた 10 G モジュールで 10 G ライン レートのパフォーマンスが必要な場合、24 ポート SFP/SFP+ と mGig ライン カードの両方を有効にしてパフォーマンスを最大化することができます。パフォーマンス モードを有効にすると、システムは各 SLI ポート グループにつき 10 G ポートを 1 つだけ使用します。

7 スロット シャーシと 10 スロット シャーシでの 10 G 光ファイバ ライン カードへの SLI ポート グループのマッピングを、次の図に示します。

図 7 スロットと 10 スロットの SLI ポート グループ

7 スロット シャーシ : 12 ポートグループ



10 スロット シャーシ : 8 ポートグループ



ステートフル スイッチオーバー (SSO)

Catalyst 9400 は、SSO による冗長スーパーバイザをサポートしています。SSO モードでは、冗長スーパーバイザ エンジンが、アクティブ スーパーバイザの設定と完全に同期します。冗長スーパーバイザ エンジンがそれ以降、さまざまなプロトコルの状態を維持し、スーパーバイザの障害またはスイッチオーバーの際のスイッチ使用不能時間を最小限に抑えます。詳細については、第 6 章「高可用性」を参照してください。

インサービス ソフトウェア アップグレード (ISSU)

ISSU は、Catalyst 9400 で利用可能なアップグレード プロセスであり、トラフィックの転送を続けながらスーパーバイザ ソフトウェアをアップグレードすることができます。このプロセスは、ステートフル スイッチオーバーをベースに構築されています。ISSU により、ネットワークの可用性が高まり、計画されたソフトウェア アップグレードにより生じるダウンタイムが短縮されます。詳細については、第 6 章「高可用性」を参照してください。

電源装置

Catalyst 9400 用の電源装置は、小型フォーム ファクタでありながら、大容量と効率的な出力を実現しています。7 スロットと 10 スロット シャーシは 8 つの電源装置ベイを備え、4 スロット シャーシは 4 つの電源装置ベイを備えています。Catalyst 9400 には、N+1 と N+N の冗長電源オプションがあります。詳細については、第 6 章「高可用性」を参照してください。

ファントレイ

Catalyst 9400 のファントレイには、N+1 冗長モードで動作する複数の独立ファンが含まれています。各ファンは、システムの温度と高度に基づいて速度を変えながら動作します。そのため、電力が効率的に使用され、ノイズレベルも低減します。Catalyst 9400 のファントレイは、シャーシの前面からも背面からも交換できます。一般的なワイヤリングクローゼットでの配線ケーブル管理では、ファントレイの保守の際にシャーシ前面からケーブルを外すのが面倒な場合がありましたが、Catalyst 9400 では、この構造によって作業がかなりやりやすくなり、ダウンタイムが削減されます。

 Catalyst 9400 のファントレイ



Catalyst 9500

Catalyst 9500 シリーズ スイッチは、業界初の固定 1 RU コア/ディストリビューション レイヤ専用スイッチです。9500 シリーズ スイッチは、優れたテーブル スケール (MAC/ルート/ACL) およびバッファリング機能を備えています。このプラットフォームは、最大 3.2 テラビット/秒のスイッチング容量と最大 20 億パケット/秒の転送パフォーマンスを実現しています。きめ細かいポート密度によって、ノンブロッキング 100 ギガビット イーサネット (QSFP28)、40 ギガビット イーサネット (QSFP+)、25 ギガビット イーサネット (SFP28)、10 ギガビット イーサネット (SFP+) スイッチを提供します。

図 Catalyst 9500



プラットフォーム概要

Cisco Catalyst 9500 プラットフォームは、Cisco Unified Access Data Plane (UADP) ASIC アーキテクチャをベースにした固定構成スイッチから成っています。モデル駆動型プログラムビリティをサポートしている Cisco IOS XE オペレーティング システム上で稼働するこのプラットフォームは、コンテナをホストする性能を備え、サードパーティ製アプリケーションやスクリプトをスイッチ内でネイティブに実行します。また、デュアル冗長電源や可変速高効率冗長ファンなどの基本的な高可用性機能にもすべて対応しています。

100 ギガビット イーサネット スイッチ

- C9500-32C : 100 GE ポート X 32 および UADP 3.0 ASIC X 2 を備えた、Cisco Catalyst 9500 シリーズの高性能スイッチ。
- C9500-32QC : 40 GE ポート X 32 または 100 GE ポート X 16 および UADP 3.0 ASIC X 1 を備えた、Cisco Catalyst 9500 シリーズの高性能スイッチ。

40 ギガビット イーサネット スイッチ

- C9500-24Q : 40 GE ポート X 24 および UADP 2.0 ASIC X 4 を備えた、Cisco Catalyst 9500 シリーズのスイッチ。
- C9500-12Q : 40 GE ポート X 12 および UADP 2.0 ASIC X 2 を備えた、Cisco Catalyst 9500 シリーズのスイッチ。

25 ギガビット イーサネット スイッチ

- C9500-48Y4C : 25 GE ポート X 48 + 100/40 GE ポート X 4 および UADP 3.0 ASIC X 1 を備えた、Cisco Catalyst 9500 シリーズの高性能スイッチ。
- C9500-24Y4C : 25 GE ポート X 24 + 100/40 GE ポート X 4 および UADP 3.0 ASIC X 1 を備えた、Cisco Catalyst 9500 シリーズの高性能スイッチ。

10 ギガビット イーサネット スイッチ

- C9500-40X : 1/10 GE ポート X 40 および UADP 2.0 ASIC X 2 を備えた、Cisco Catalyst 9500 シリーズのスイッチ。
- C9500-16X : 1/10 GE ポート X 16 および UADP 2.0 ASIC X 1 を備えた、Cisco Catalyst 9500 シリーズのスイッチ。

アーキテクチャ

Catalyst 9500 スイッチはライン レートで動作します。また、特定の機能を最適にサポートできるようにシステム リソースを設定することが可能です。スイッチ アーキテクチャは、主に、次の 3 つのコンポーネントで構成されています。

- UADP ASIC
- x86 CPU コンプレックス
- ASIC インターコネクト

UADP ASIC

Catalyst 9500 ファミリ スイッチは、UADP 2.0 と 3.0 の 2 つのバージョンの UADP ASIC をベースに構築されています。両 ASIC は、アーキテクチャは類似していますが、スイッチング容量、ポート密度、ポート速度、バッファ機能、転送拡張性が異なります。

UADP 2.0 ASIC は、28 ナノメートル テクノロジーを使用して 2 つのコアで構築されており、コア 1 つあたり最大 120 Gbps、合計で 240 Gbps の帯域幅をサポートし、1 秒間で最大 3 億 7,500 万パケットを転送できます。UADP 2.0 ASIC を搭載したスイッチは、合計で最大 22 万 4 千件の IPv4/11 万 2 千件の IPv6 ハードウェア テーブル、最大 5 万 4 千件のセキュリティ ACL TCAM、2 X 16 MB の共有バッファをサポートします。

UADP 3.0 ASIC は、16 ナノメートル テクノロジーをベースに 2 つのコアを使用して構築されており、コア 1 つあたり最大 800 Gbps、合計で 1.6 Tbps の帯域幅をサポートし、1 秒間で最大 10 億パケットを転送できます。UADP 3.0 ASIC を搭載したスイッチは、合計で最大 41 万 6 千件の IPv4/IPv6 ハードウェア テーブル、最大 5 万 4 千件のセキュリティ ACL TCAM、36 MB の統合バッファをサポートします。

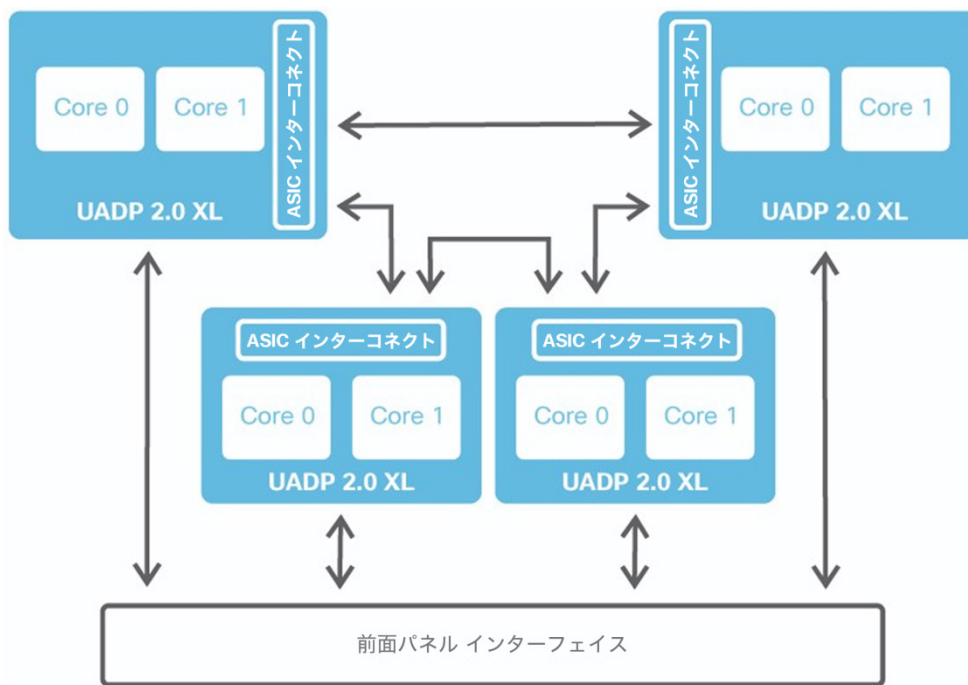
x86 CPU コンプレックス

Catalyst 9500 シリーズのスイッチには、すべて同じ CPU、システム メモリ、フラッシュ ストレージが採用されています。CPU は 2.4 Ghz x86 クワッド コア、メモリは 16 GB DDR4 RAM、ストレージは 16 GB 内蔵フラッシュ ストレージを搭載しています。アプリケーション ホスティングや汎用ストレージ向けに USB 3.0 SSD ストレージをサポートしています。また、UADP 3.0 搭載モデルは最大 960 GB の M2 SATA SSD ストレージ オプションをサポートしています。

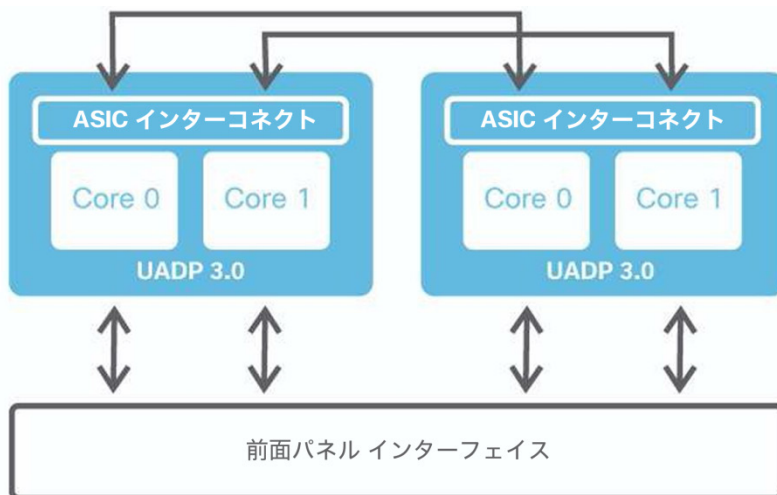
ASIC インターコネクト

Catalyst 9500 スイッチは、ASIC 間の通信に高速 ASIC インターコネクト リンクを使用しています。2 つの ASIC 間のインターコネクト帯域幅は、UADP 2.0 で最大 720 Gbps、UADP 3.0 では最大 800 Gbps となります。ASIC 内のローカル ポート宛ての packets は、ASIC インターコネクト リンクを使用しません。

Cisco Catalyst 9500 スイッチ ブロック図 - UADP 2.0



Cisco Catalyst 9500 高性能スイッチ ブロック図 - UADP 3.0



ネットワーク モジュール

Cisco Catalyst 9500 シリーズの C9500-40X および C9500-16X スイッチ モデルでは、オプションとしてアップリンク ポート用にネットワーク モジュールをサポートしています。デフォルトのスイッチ構成には、ネットワーク モジュールは含まれていません。ネットワーク モジュールのポートはいずれもライン レートで動作し、スイッチのダウンリンク ポートでサポートされるソフトウェア機能はすべてネットワーク モジュール ポートでもサポートされます。これらのスイッチは、ネットワーク モジュールの活性挿抜 (OIR) をサポートしています。

 Catalyst 9500 のネットワーク モジュール

電源装置

Catalyst 9500 スイッチは、最大 2 つの AC または DC 小型フォーム ファクタ プラチナ定格電源装置をサポートし、システム合計で最大 650 W、950 W、1600 W までの容量に対応しています。AC 2 台、DC 2 台、または AC 1 台と DC 1 台のいずれかの組み合わせで電源装置を搭載できます。電源装置は冗長ロードシェアリング モードで連携して動作し、各電源装置がそれぞれの容量の約 50 % で稼働します。1 台の電源装置が故障した場合は、もう一方の電源装置がシステム全体の電力を供給できます。Catalyst 9500 スイッチは、電源装置の OIR をサポートしています。

ファンおよびファントレイ

Cisco Catalyst 9500 スイッチは、合計 5 つの独立ファンまたはデュアル ファン トレイ (SKU によって異なる) を搭載しています。それぞれの独立ファンの動作スピードは可変です。9500 スイッチのハードウェアは、1 つまでのファンまたはファントレイの障害に対応できます。残りのファンが自動的にそれぞれの RPM を増やして補い、十分な冷却性能を維持します。9500 スイッチは、最大 120 秒間、ファン/ファントレイの OIR をサポートします。

25 G と 100 G - 企業での高速接続を実現

シスコは、新しいイーサネット テクノロジーを市場に投入するいくつかの取り組みにおいて、先駆的な役割を果たしてきました。たとえば、100GBASE Quad Small Form Factor Pluggable (QSFP28) と 25GBASE Small Form Factor Pluggable (SFP28) などです。25GBASE オプションには、エンタープライズ キャンパスの距離をサポートするデュアル レートの光ファイバ (25 G および 10 G) が含まれ、次世代ネットワークのスピードとアーキテクチャの変革を促進しています。これらのイノベーションによって、柔軟なオプションと下位互換性が実現し、コストと物的財産の変更を最小限に抑えながら現在の 10 G/40 G を超えるネットワーク速度が推進されます。

Cisco Catalyst 9500 の 25 G および 100 G スイッチのポートフォリオ

Catalyst 9500 スイッチは、次世代の 25 G/100 G 対応高速エンタープライズ キャンパス ネットワークを実現するための基盤となります。これらの新たな速度をコアおよびディストリビューションでサポートするために、シスコでは、業界をリードするポート密度と柔軟性を備えたスイッチ オプションを豊富に取り揃えています。

Cisco 25 G Optics ポートフォリオ

Cisco 25GBASE SFP28 ポートフォリオは、さまざまな高密度/低電力 25 ギガビット イーサネット接続オプションを提供し、進化するキャンパス ネットワークをサポートしています。

Cisco 25 G Optics の特長と利点

- エンタープライズ ネットワークにおいてデュアル レート光ファイバをサポートし、優れた**投資保護**を実現
- 必要に応じて他の IEEE 準拠 25 G インターフェイスと**相互運用可能**
- 優れたパフォーマンス、品質、信頼性を**認定および検証済み**
- IEEE 802.3by **準拠**の高速電気インターフェイス

詳細については、『[Cisco 25GBASE SFP28 optics and copper modules](#)』を参照してください。

Cisco 100 G Optics ポートフォリオ

Cisco 100GBASE QSFP28 ポートフォリオは、さまざまな高密度/低電力 100 ギガビットイーサネット接続オプションを提供し、エンタープライズ コア/ディストリビューションレイヤをサポートしています。3 層キャンパス ネットワークでは、ディストリビューションレイヤが 25 G または 40 G に移行していることに伴い、100 G 対応のコアレイヤが望まれています。40 G と 100 G の光ファイバのフォーム ファクタには互換性がある点に留意することも大切です。

Cisco QSFP28 Optics の特長と利点

- 100 G ギガビット イーサネット Cisco QSFP ポートに接続する、**ホットスワップ可能な入出力デバイス**
- 必要に応じて他の IEEE 準拠 100GBASE インターフェイスと**相互運用可能**
- 優れたパフォーマンス、品質、信頼性を**認定および検証済み**
- IEEE 802.3bm 準拠の高速電気インターフェイス

詳細については、『[Cisco 100GBASE QSFP optics and copper modules](#)』を参照してください。

パッケージング、ライセンス、サポート

Catalyst 9000 には、新しいシンプルなライセンス モデルが採用されています。前世代のスイッチにはさまざまなライセンス タイプがあり（LAN Base、IP Base、IP Services、Enterprise Services）、複数の Catalyst スイッチ ファミリ間でライセンス タイプが異なることによって、状況がいっそう複雑になっていました。Catalyst 9000 ファミリは、すべてのプラットフォームに同じソフトウェア パッケージング/ライセンス モデルを採用しています。

この新しいモデルには、次のような利点があります。

- 機能のパッケージングがシンプルになる。
- よりコスト効率の高いソリューションで機能を利用できる。
- 機能とサポートを追加できるので、先行コストを抑えられる。

ソフトウェア パッケージングとライセンス

Catalyst 9000 には、次の 2 つのソフトウェア パッケージが用意されています。

- **Essentials** : ネットワーク運用に使用する基本的なネットワーク機能を提供します。
- **Advantage** : Essentials パッケージのすべての機能に加え、高度なセキュリティ、可用性、自動化、アシュアランスなどの高度な機能を提供します。

各ソフトウェア パッケージに、永久ライセンスとサブスクリプション ライセンスの 2 つのライセンスが付属しています。永久ライセンスは、ハードウェア デバイスの耐用期間を通して有効性を維持し、サブスクリプション ライセンスは、期間ごとに更新可能です。ソフトウェア ライセンスには次の 2 つのタイプがあります。

- **Network** : ネットワーク機能の基本セットを永続的に使用できます。
- **Cisco DNA** : 独自のプラットフォーム/ソリューション機能セットを 3、5、または 7 年間使用できます。

1つのパッケージに、機能レベルが統一された2つのライセンスが組み合わせられています。

- **Essentials パッケージ** = Network Essentials ライセンス X1 + Cisco DNA Essentials ライセンス X1
- **Advantage パッケージ** = Network Advantage ライセンス X1 + Cisco DNA Advantage ライセンス X1

Catalyst 9000 スイッチを購入する際には、これら2つのソフトウェアパッケージのいずれか1つを選択する必要があります。前述のように、パッケージと2つのライセンスは密接に結びついています。ライセンスを個別に購入することはできません。

各パッケージにおける機能グループの概要を次の図に示します。

図 Advantage および Essentials パッケージ

Advantage パッケージ		Essentials パッケージ	
Cisco DNA Advantage (Cisco DNA Essentials を含む)		Cisco DNA Essentials	
期間 : 3、5、7 年		期間 : 3、5、7 年	
Cisco DNA ライセンス	高度な自動機能 ・ SD-Access ・ アプリケーション ポリシー ・ 暗号化されたトラフィックの分析 ・ Bonjour 向け Cisco DNA サービス ・ サードパーティ製アプリケーションホスティング	Cisco DNA ライセンス	基本的な自動機能 ・ PnP アプリケーション ・ LAN 自動化 ・ Embedded Event Manager
	アシュアランスと分析 ・ グローバル インサイト、トレンド ・ コンプライアンス、カスタム レポート ・ Switch 360 & Wired Client 360 ・ SD-Access とスイッチ インサイト ・ アプリケーションの稼働状況、Application 360、パフォーマンス (損失、遅延、ジッター)		基本的なアシュアランス ・ 稼働状況ダッシュボード - ネットワーク、クライアント、アプリケーション ・ 基本的なスイッチと有線クライアントの稼働状況の監視
ネットワーク機能	エレメント管理 ・ パッチ ライフサイクル管理	ネットワーク機能	エレメント管理 ・ ソフトウェア イメージ管理 ・ 検出、インベントリ、トポロジ
	テレメトリと可視性 ・ ERSPAN ・ AVC (NBAR2) ・ Wireshark		テレメトリ ・ フル Flexible NetFlow
Network Advantage (Network Essentials を含む)		Network Essentials	
永久ライセンス		永久ライセンス	
ネットワーク機能	セキュリティ管理の強化 ・ MACSEC-256	ネットワーク機能	必須のスイッチ機能 ・ レイヤ 2、ルーテッド アクセス (RIP、EIGRP Stub、OSPF (1000 ルート))、PBR、PIM Stub マルチキャスト (1000 ルート) PVLAN、VRRP、PBR、CDP、QoS、FHS、802.1x、Macsec-128、CoPP、SXP、IP SLA Responder SSO
	IoT とモビリティ ・ CoAP、AVB、PTP		DevOps の統合 ・ Netconf、Restconf、gRPC ・ YANG データ モデル ・ GuestShell (On-Box Python) ・ PnP エージェント、ZTP
	完全なルーティング機能 ・ BGP、HSRP、OSPF、ISIS、GLBP		テレメトリと可視性 ・ モデル駆動型テレメトリ ・ サンプル NetFlow ・ SPAN、RSPAN
柔軟なネットワーク セグメンテーション ・ VRF、VXLAN、LISP、MPLS		高可用性と復元力 ・ NSF、GiR、Stackwise Virtual*、ISSU/FSU、パッチ適用 (CLI)	
マルチキャストによる帯域幅利用の最適化 ・ MSDP、mVPN、AutoRP、PIM-BIDIR			

注 プラットフォームによっては利用できない機能もあります。

各パッケージの機能の全一覧を確認するには、[Cisco Feature Navigator](#) を使用してください。

テクニカル サポート

Catalyst 9000 ファミリのテクニカル サポートは、ハードウェアも前述の機能パッケージもカバーしています。ハードウェアの問題のトラブルシューティングや、部品またはシャーシの交換に関するテクニカル サポートには、次のような一般オプションを提供しています。

- 拡張版制限付きライフタイム保証（カバーする内容は次のとおり）
 - Cisco Technical Assistance Center (TAC) により（最初の購入日から）90 日間提供されるテクニカル サポート
 - ハードウェアのトラブルシューティングおよび交換（スイッチの耐用期間中を通して有効）

利用規約については、www.cisco.com の『[Enhanced Limited-Lifetime Warranty](#)（拡張版制限付きライフタイム保証）』を参照してください。

- シスコまたはシスコ パートナーを通じて利用できるプレミアム サービスには、テクニカル サポートとハードウェア交換の両方が含まれます。
 - 利用可能なサービスについては、シスコまたはパートナー セールス チームにお問い合わせください。

ソフトウェア サポートは、次の形態で提供されます。

- ネットワーク ライセンスによって有効となるスイッチの基本機能は、デバイスの耐用期間を通して有効です。ネットワーク ライセンスが付与されたコンポーネントにはソフトウェア アップデートを無期限に利用できます。
- スwitchの基本機能に関するテクニカル サポートを、Cisco Technical Assistance Center (TAC) により（最初の購入日から）90 日間提供します。

利用規約については、www.cisco.com の『[Enhanced Limited-Lifetime Warranty](#)（拡張版制限付きライフタイム保証）』を参照してください。

- スイッチの Cisco DNA Essentials または Cisco DNA Advantage ライセンスによって有効となる機能向けのソフトウェア サポートは、サブスクリプション期間を通して有効です。サブスクリプションの有効期限が切れると、これらの機能に対するサポートも終了します。

Cisco DNA ライセンス サブスクリプションは期間ベースですが、期限切れになっても、ライセンスによって利用可能になった機能は引き続き動作しますので、注意してください。ただし、ライセンスの有効期間の期限が切れると、期限切れの Cisco DNA ライセンスでサポートされる機能へのテクニカル サポートは、すべて終了します。

ASIC - プログラマブル 回路の力

ASIC とは

特定用途向け集積回路（ASIC）とは、CPU などのように汎用処理に使用されるのではなく、特定のタスク（パケットのブリッジやルーティングなど）向けに設計された、シリコンベースのマイクロチップです。イーサネットスイッチが機能するためには ASIC が欠かせません。

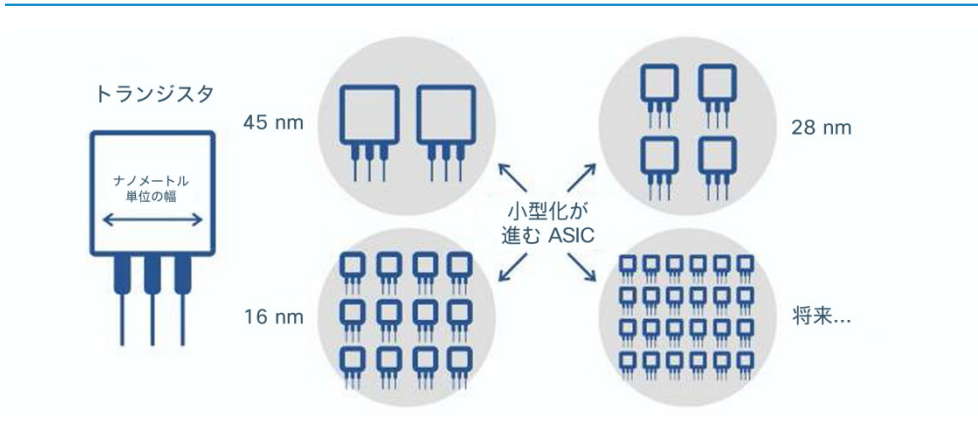
製品の一部を成す ASIC はその製品向けに、また、ソリューションをサポートする ASIC はそのソリューション向けに、それぞれカスタム設計されます。ネットワークスイッチの ASIC は、パケットの認識、操作、L2/L3 転送を非常に高速（現在は数十～数百ギガビット/秒、将来的にはテラビット/秒）で処理しながら、トラフィックに対して、優先付け（例：QoS）、アカウントリング（例：NetFlow）、セグメント化（例：VRF、SGT）、トラフィックフィルタリングおよび適用（例：ACL）、パス選択（例：PBR）などの豊富なサービスを提供します。

ASIC のマイクロチップは、ナノメートル（1 m の 10 億分の1）単位で計測されます。これは、トランジスタなど、ASIC を構成しているさまざまなコンポーネントのサイズです。ASIC を小型化する主な利点は、次の 3 点です。

- 速度の向上（電子が移動する距離が短い）
- 低電力消費および、熱として浪費されるエネルギーの少なさ
- 低コスト（シリコン素材の欠陥に遭遇する可能性が減ることで、チップの歩留まりが向上）

現行の ASIC は、一般的に 45 ～ 28 ナノメートルの範囲で製造されています。新しいモデルでは、16 ナノメートルにまで小型化されたものもあります。

図 マイクロチップ パッケージ

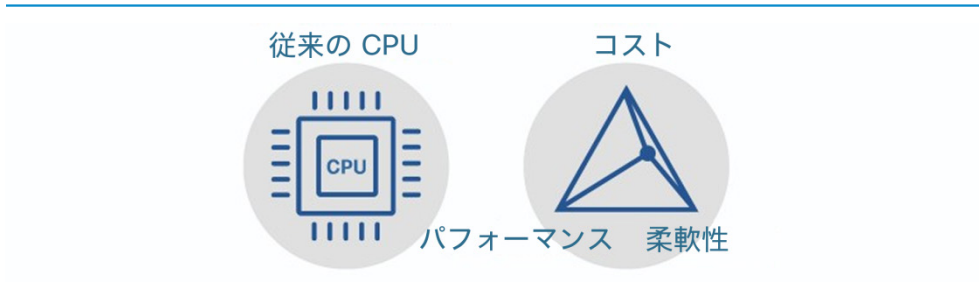


ASIC の必要性

スイッチ内でトラフィックを転送するためには、汎用 CPU では遅すぎます。汎用 CPU は、ラップトップやサーバでランダム アクセス アプリケーションを実行するには高速かもしれませんが、ネットワーク トラフィックの操作や転送となると、話が異なります。トラフィックを処理するには、大容量メモリ テーブル（MAC アドレス用の L2 テーブル、IP ルート用の L3 テーブル、セキュリティや QoS 用の L4 ACL など）を常にルックアップする必要があります。

汎用 CPU では、これらのテーブルはすべてオフチップ メモリ（CPU 自体の中にはないメモリ）に保持されるため、頻繁なメモリ アクセスによってパフォーマンスが大幅に低下します。また、着信パケットを処理する際のデータ パスとバッファも限られます（なにしろ着信パケットの数は 1 秒間に数百万、さらには数十億にもなるのです）。パケットが受信されてキューに格納されると、CPU は、実際の処理機能を実行して、宛先検索のためのルックアップや、パケット形式の書き換えなどを実施する必要があります。このような理由から、CPU はトラフィック処理には適していません。

図 従来の CPU - 柔軟性：高、パフォーマンス：低、コスト：中



結論

CPU は、柔軟性には優れていますが低速です。エンタープライズ ネットワークの要件を満たすためには ASIC が不可欠です。

後続の章では、従来のタイプのネットワーク ASIC と最新のプログラマブル ASIC の両方について考察します。管理者がこれらの章を読めば、ASIC がスイッチの動作において中心的な役割を果たす理由や、最新の ASIC が現在および将来のエンタープライズ ネットワークの基盤を構築する仕組みを理解できるでしょう。

プログラマブル ASIC を使用する理由

従来の ASIC

シスコのスイッチやルータには、長年にわたって、多くの ASIC が使用されてきました。これらの各 ASIC は、キャンパス ネットワークにおけるさまざま役割に必要な、特定の機能や規模に対応して設計/開発されたものです。それぞれが、ネットワーク内での役割に応じて異なる機能、速度、拡張性を備えています。

ただし、すべての ASIC に共通することがあります。それは、このクラスのネットワーキング ASIC が固定 ASIC と呼ばれていることです。これらの ASIC の特徴（動作、スピード、スケールなど）は、すべて製造工程の中で「焼き付け」られており、まったく新しいバージョンの ASIC を作らない限り変更することはできません。

固定 ASIC と呼ばれるもう 1 つの理由は、処理動作にあります。名前が示すとおり、すべての着信パケットが、処理パイプラインと呼ばれる、固定された一連のステップを通過します。一般的な固定 ASIC 処理パイプラインのステージは、ほぼ次のようになっています。

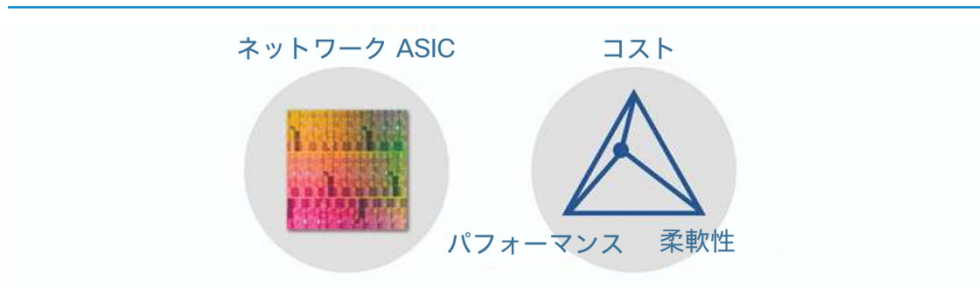
- 1 着信パケットの解析（ヘッダーを調べる）
- 2 レイヤ 2 処理（MAC ルックアップなど）
- 3 レイヤ 3 処理（IP ルックアップなど）
- 4 ポリシー処理（ACL ルックアップなど）
- 5 パケットの書き換え、トラフィック数計測
- 6 キュー スケジューリングおよび転送

図 従来の ASIC - 処理パイプライン



もう1つ注目すべきこととして、固定 ASIC は、その設計/製造方法やネットワーク スイッチへの統合に要する時間のため、最終製品を提供するまでに何年もかかることも珍しくありません。固定 ASIC は、非常に費用対効果が高く効率的ですが、柔軟性や適応性には欠けています。固定 ASIC では、チップをハード的に固定して処理を行うタイプのパケットにしか対応できません。

図 従来の ASIC - パフォーマンス：高、柔軟性：低、コスト：中



ネットワークおよびプロトコルの進化

なぜ ASIC を変える必要があるのでしょうか。たとえば、Catalyst 3750 の ASIC は、ハードウェアで IPv4 と IPv6 のパケットしか転送できません。この ASIC は、VXLAN の開発より前に設計されたため、ハードウェアで VXLAN を処理することができません。また、固定 ASIC であるため、処理パイプラインを変更して VXLAN などの新しいプロトコルを処理できるようにすることもできません。処理するためには、まったく新しい ASIC を作成する必要があります。

このように柔軟性に欠けていても、ネットワークおよび関連プロトコルが大きく変わらなかった時代には問題はなかったかもしれません。しかし、新時代のネットワークにおいては、すべてが「ソフトウェアによって定義」され、プロトコルや拡張性要件が常に変わっていきます。そのため、VXLAN-GPO、GPE、NSH などの新しいパケット形式やカプセル化への対応が、ASIC に求められているのです。

結論

従来の固定 ASIC アーキテクチャでは（ひいてはネットワークそのものにおいて）、シスコの新しいソフトウェア定義型の環境で求められる高度で革新的な機能を導入するためには、ハードウェアの交換が必要です。

プログラマブル ASIC

両方の長所を活かすにはどうすればよいのでしょうか。マルチギガビットまたはマルチテラビットのネットワーク デバイスに必要なスピードと、新しいネットワーク イノベーションに適応するための柔軟性を両立できる方法はあるのでしょうか。これらの疑問から導き出されたのが、プログラマブル ASIC というコンセプトです。これは、ニーズの出現に合わせて新しい機能を導入できるよう設計された柔軟なネットワーク マイクロチップと、ネットワークに必要なパフォーマンスを兼ね備えたものです。

初期の試みとして、Field Programmable Gate Array (FPGA; フィールド プログラマブル ゲート アレイ) が開発されました。FPGA は、基本的には、再プログラム可能な論理ゲートを備えたシンプルな ASIC であり、製造後でも当初の動作を変更することができます。FPGA は、ある程度の柔軟性を備えていますが、開発とサポートに多額の費用がかかります。特定のタスク専用構築されておらず、オンボード メモリをほとんど（またはまったく）搭載していないため、メモリ アクセスには他のチップが必要になります。

このような制約のため、ほとんどのネットワーク デバイスにおいて、FPGA の使用はたいてい特殊な役割に限定されています。FPGA は、固定 ASIC のパケット転送機能を補うものとして、固定チップにはない「1 つの特殊な機能」を提供するために使用することができます。たとえば、Catalyst 4500 Supervisor-8 では、FPGA を使用して、スイッチ ASIC でサポートされていない VXLAN カプセル化を実現しています。FPGA は一般に、スイッチのメイン転送エンジンとして使用するにはコストがかかりすぎます（設計および製造コスト、ボードのスペース、熱、電源）。柔軟性を確保するために FPGA と ASIC を組み合わせた設計にすると、最終的にスイッチ全体のコストが高くなります。

図 FPGA - コスト：高、柔軟性：中、パフォーマンス：中



まとめると、CPU は柔軟性に優れていますが、高速転送に対する拡張性には欠けています。固定 ASIC はスピードと拡張性には優れていますが、柔軟性に欠けています。FPGA は柔軟性と拡張性に優れているものの、非常にコストがかかります。結局どうすればよいのでしょうか。

シスコは、このニーズを数年前から認識し、その見通しに基づいて、プログラム可能で柔軟性に優れた **Unified Access Data Plane (UADP) ASIC** を開発しました。

UADP ASIC は、新しく登場するネットワーク プロトコルやカプセル化に対応するために必要な柔軟性に加え、固定 ASIC のスピードと、キャンパス ネットワークのさまざまなエリア（コア、ディストリビューション、アクセス）に対応するための適切なコストおよび拡張性を兼ね備えています。シスコは UADP によって、まったく新しい時代のネットワーキングを、まさに切り開きました。

後続の章では、Catalyst 9000 ファミリ スイッチの中核を成す Unified Access Data Plane ASIC について説明します。

UADP - プログラマブル ASIC チップ

UADP - 柔軟性に優れたシスコのスイッチ用プログラマブル ASIC

Unified Access Data Plane (UADP) ASIC は、Catalyst 9000 ファミリ スイッチの中核を成すものです。具体的に言うと、Catalyst 9000 スイッチは、Catalyst 3850/3650 で使用されていた前世代の ASIC から進化した最新世代の UADP ASIC をベースに構築されています。

UADP を世界で最も高度なスイッチの土台として理想的なものにするためには、柔軟性が重要になります。この柔軟性により、Catalyst 9000 ファミリは以下のことを実現しています。

- 新しいフレーム カプセル化を取り扱うことができ、新しい機能やプロトコルが可能になる。
- メモリ テーブルを再プログラミングし、スイッチをニーズの変化に適応させることができる。
- 複数のインターフェイス タイプやシャーシ構成をサポートし、進化するネットワーク設計に対応できる。
- 一貫して高性能を維持し、アプリケーションの多様性の拡大に対応できる。
- 柔軟なトラフィック処理/アカウンティングを統合した、豊富な一連のサービスを提供できる。

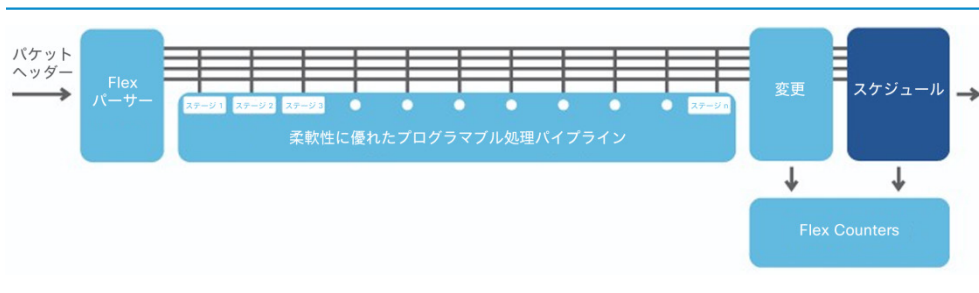
あらゆる段階での柔軟性

UADP の設計においては、当初から、あらゆる側面に柔軟性が組み込まれてきました。UADP では、固定構成型チップに存在するほぼすべての処理段階が、柔軟なチップによって置き換えられています。

パーサー ステージでは、パケット タイプとヘッダーを認識し、ASIC パイプラインでさらに処理を行うためにそれらを分析する仕事を実施されます。従来の ASIC では、パーサー ステージが固定されているため、固定 ASIC をアップグレードして新しいパケット タイプやヘッダーをハードウェアで認識あるいは処理させることはできません。UADP には、さまざまなタイプのヘッダーのパケットを解析できる、再プログラム可能な FlexParser が含まれています。

従来の固定処理型のパイプラインとは異なり、UADP の柔軟な多段階パイプライン (L2/L3 転送、ポリシー適用、書き換え、キューイングなど) は、(ファームウェアのマикроコードを利用した) 全面的な再プログラミングも可能です。ほとんどの固定 ASIC にはない、入力パイプラインと出力パイプラインがあります。

図 プログラマブル UADP - 処理パイプライン

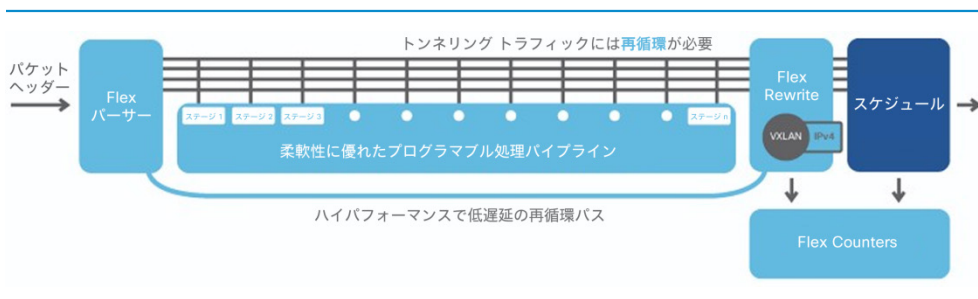


パケット再循環

トラフィック トンネリングは、現代のネットワークでは一般的な設計です。GRE、MPLS、VXLAN は、送信時にパケットの外側部分に別のヘッダーを追加 (つまりカプセル化) し、パケット受信時にヘッダーを削除 (つまりカプセル化解除) するため、トンネルと見なされています。ASIC では、パケットのトンネリングが必要な場合は常に、元のパケットに対して、別のヘッダーを追加するための複数回の処理 (つまり再循環) を行う必要があります。

トンネリングの最中の動作を少し考えてみると、その理由がわかります。パケットが到着し、そのパケットをトンネル（VXLAN など）経由で送信する必要があることを ASIC が（スイッチの設定に基づいて）判断した場合には、元のパケットの前部に、トンネルのローカル側の送信元 IP とリモート側の宛先 IP が設定された新しいトンネル ヘッダーを追加する必要があります。宛先 IP アドレスはトンネルのリモート側の IP アドレスに変更されているため、トンネルに適用される可能性のあるすべてのポリシーとともに、パケットを処理パイプライン内で再循環させ、この新しい宛先に転送する必要があります。

図 プログラマブル UADP - パケット再循環



UADP では、約 500 ナノ秒（0.5 マイクロ秒）でパケットを再循環させることができます。トンネリングが必要な場合でも、転送パフォーマンスへの影響は最小限で済みます。1つのパケットを最大 16 回まで再循環できますが、通常必要なのは 2、3 回です。再循環に利用する帯域幅には融通性があります。つまり、その時点で前面パネルのスイッチ ポートに使用されていない予備の帯域幅も使用できます。

必要であればパケットを複数回再循環できるこの機能により、UADP の柔軟なパイプライン アーキテクチャを通じてさらに複雑な使用例に対応することが可能になります。トラフィック トンネリングが一般的なものになった今、UADP がトンネリングのために構築され最適化されたのは必然的なことです。

統合マイクロエンジン

UADP によって実行される高度な機能の中には、非常に大量の処理を必要とするものがあります。フラグメンテーションや暗号化などのいくつかのタスクは一般的な固定アルゴリズムに基づいており、UADP パイプライン内のサイクルを無駄に使用するのとは非合理的と言えます。このような場合は、オンチップのマイクロエンジンを使用して一般的な機能を並行して処理することで、貴重な UADP パイプラインのパフォーマンスを他の機能のためにとっておくことができます。

UADP に組み込まれているマイクロエンジンの機能の例を以下に示します。

暗号化と復号：セキュリティとデータの機密性は、現代のネットワークにおける最重要課題です。すべての UADP に、2 つのレベルのハードウェア暗号化機能が組み込まれています。1 つは、すべての UADP ポートにおいてライン レートで動作するポート レベルの MACsec (802.1AE) です。MACsec は、リンクレベルの暗号化を実現してデータの機密性を保証します。つまり、パケットは MACsec 対応リンクに送信される際に暗号化され、MACsec 対応リンクから受信される際に復号されます。

UADP は、CAPWAP や VXLAN などのパケット形式に基づいてトラフィックを暗号化できる Datagram Transport Layer Security (DTLS) マイクロエンジンも備えています。DTLS は、トンネル オーバーレイ トラフィックの暗号化のベースとして機能します。UADP ハードウェアでは、必要に応じて、中継時にこれら 2 つの機能 (MACsec と DTLS) を組み合わせることができます。どちらも、Galois Counter Mode (AES-256-GCM) による、256 ビットまでの鍵を使用した AES 暗号化アルゴリズムを採用しています。

フラグメンテーション：ネットワークにおいてリンクの最大伝送ユニット (MTU) サイズを超過した場合、元のパケットをフラグメント化してから、もう一方の側で再構築する必要があります。たとえば、トラフィックをトンネリングする際に出力インターフェイスの MTU が小さすぎて元のパケットにトンネル ヘッダーを加えることができない場合などに該当します。UADP は、その他の多くの ASIC とは異なり、ハードウェアでフラグメンテーションを実施できます。エンドツーエンドでの MTU の調整を簡単には実施できず、加えてトラフィックトンネリングの使用が増加しているような環境では、この機能が重要になります。

NetFlow の統合：ネットワークを通過するすべてのトラフィックのアカウンティングは、さまざまな使用例において重要とされます。最も端的な例は、ネットワークのベースライン化とキャパシティ プランニングです。NetFlow を使用すれば、エンドツーエンドのセッション（TCP または UDP）の全体的状態をスイッチで追跡し、パケット フロー全体の重要な情報を抽出して分析することができます。UADP では、Flexible NetFlow（FNF）のすべての収集機能がハードウェアに実装されています。Catalyst 9000 シリーズは、スイッチを通過するすべてのパケットについての NetFlow 統計情報収集を、全体的なパケット処理の本質的な一部として実施することができます。

Cisco Encrypted Traffic Analytics（ETA）は、NetFlow の機能を活用してフローを検査し、初期データ パケット（IDP）交換などの重要なフロー情報や、暗号化されたトランザクションのパケット長とパケット時間のシーケンス（SPLT）に関する情報を抽出します。Cognitive Threat Analytics を使用したクラウドベースの機械学習機能や Cisco Stealthwatch をこれと統合することで、高精度のネットワーク「フィンガープリント」分析の実施が可能になり、暗号化フローが「通常」のインターネット トラフィックを意味するものなのか、あるいは暗号化マルウェアによる脅威を意味する可能性があるのか、判断できるようになります。

ポリシーと ACL：チップに搭載されている統合 TCAM（Ternary Content Addressable Memory）ブロックを使用してパフォーマンスを最大化する UADP ASIC には、トラフィック分類やポリシー適用を実施するためのさまざまなオプションが備えられています。TCAM マッチングによって、IPv4 または IPv6 アドレスや、仮想ネットワーク（VN）などの特別なタグ、拡張可能グループ タグ（SGT）、QoS、CoS、DSCP 値などのパケット マーキングを使用して、トラフィック フローをマッチングすることができます。UADP は、ネットワーク管理者によって設定された適合ポリシーを適用することができます。たとえば、許可/拒否、QoS の再マーキング、パス選択、パケット コピーなどのアクションがあります。UADP の柔軟なパイプラインでは、パフォーマンスを低下させることなく、複数の並列アクションに関して最大 2 つのパケット マッチングを参照することができます。

パケット複製：ある種のアプリケーション トラフィックでは、パケットの複製（複数のコピーの作成）が必要になる場合があります。たとえば、入力マルチキャスト ストリームでは、スイッチ上の複数の受信者に対して複製が必要になることがあります。UADP アーキテクチャは、複製に最適化されています。処理中は各パケットを中央のバッファ メモリに保持し、その後、すべての受信者に対して 1 つまたは複数のコピーを送信することができます。これは非常に効率的な複製アプローチであり、遅延や、容量消費の多いメモリ間パケット コピーを、最小限に抑えられます。

統合スタッキング機能

UADP は、柔軟性に優れた非常に強力な ASIC です。多くの場合、ポートのタイプと密度に基づいて、単一の UADP ASIC で 1 つのスイッチ全体を構築できます。

しかし、複数の UADP ASIC を接続して統合システムを構築することが必要になる場合もあります。UADP では、次の ASIC 間接続オプションをサポートしています。

- 外部ケーブルを使って複数のスイッチをスタックし、単一の統合スタックを構築する。
- 固定スイッチのベースボード上で複数の ASIC をリンクする。
- モジュラ型スイッチのスーパーバイザ モジュール上で複数の ASIC をリンクする。

UADP では、前面パネルのスイッチ ポートに加え、専用的高速 ASIC インターコネクト インターフェイスを備えた設計になっているため、このような柔軟な設計オプションが可能になっています。

マイクロコードによる UADP プログラミング

Cisco IOS XE では、複数のソフトウェア レイヤが使用されます。その中には、より密接にハードウェアと関連付けられているソフトウェア レイヤがあります。たとえば、ユーザとの連携を伴う機能（CLI を利用する場合など）は通常、上位レイヤにあり、ハードウェアにはあまり依存していません。ハードウェア ドライバなど、ソフトウェアのインフラストラクチャ部分（マイクロコードと呼ばれるもの）は、ハードウェアと直接連携します。この、ソフトウェアのマイクロコード レイヤで、実際に ASIC がプログラミングされます。Cisco IOS XE のアーキテクチャの詳細については、第 5 章「Cisco IOS XE」を参照してください。

UADP ファミリ

UADP ASIC の歴史は、シスコが Catalyst 3850 スイッチを発表した 2013 年に始まりました。前述のように、ASIC の設計と製造プロセスは非常に複雑で、個々のコンポーネントや製品が完成するまでに何年もかかる場合があります。数年に及ぶ革新的な取り組みを経て、UADP が開発されました。

UADP 1.0 では、多くのコンポーネントがまったく新しいものであり、柔軟性を持たせるように設計したために、当時のほとんどの固定 ASIC よりも長い期間が設計に費やされました。UADP 1.0 は、共通アーキテクチャがすべてで共有される UADP ASIC ファミリの最初のバージョンでした。UADP 1.0 は 65 ナノメートル (nm) プロセスをベースに構築されました。一方、最新の UADP 3.0 は 16 nm で構築されています。UADP は、ASIC テクノロジーの面で大幅に進歩し、世代を重ねることに、組み込むトランジスタの数が増えています。トランジスタが増えることで、ASIC に組み込むことのできる性能、拡張性、特性、機能が向上しています。

UADP 1.0/1.1

UADP 1.0 は、トランジスタを 13 億個搭載したシングル コア ASIC で、利用可能な総帯域幅は 56 Gbps になります。前のセクションで説明したプログラム可能な機能の多くを初めて備えた ASIC でした。UADP 1.0 は、その柔軟性から、さまざまなフレキシブル タイプの packets カプセル化に対応できる初めての ASIC の 1 つとなりました。第 1 世代の Catalyst 3850/3650 は UADP 1.0 を使用していました。

2015 年までに、同じ ASIC 設計の新バージョン (バージョン 1.1) が発表されました。ASIC の中核となる要素とアーキテクチャは基本的に同じですが、いくつかの重要な機能が新たに追加されました。UADP 1.0 と 1.1 の主な違いは、ASIC 内部へのデュアルコア アーキテクチャの採用です。

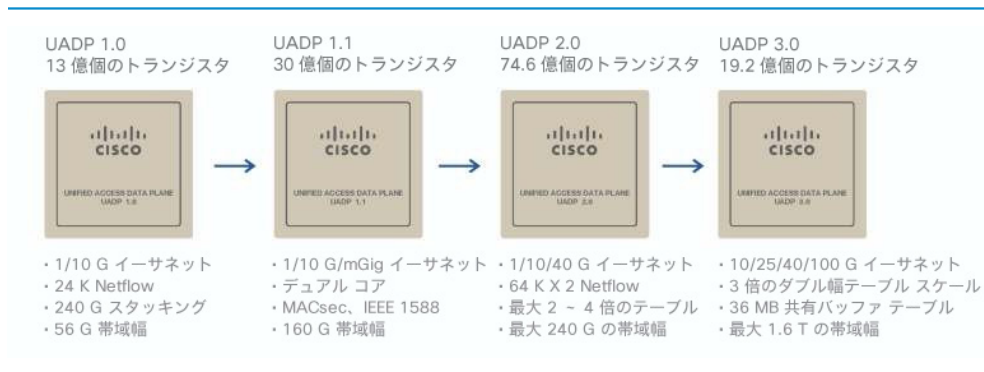
UADP 1.0 とは異なり、UADP 1.1 では、30 億個のトランジスタを搭載した 2 つの ASIC コアが使用されています。1 つの ASIC パッケージで UADP 1.0 チップを 2 つ使用する場合とほぼ同じ結果が得られます。また、UADP 1.1 では、総帯域幅とパフォーマンスが最大 160 Gbps (コア 1 つにつき 80 Gbps) に向上したほか、アップデートされた新しいマイクロエンジンもいくつか追加されています。たとえば IEEE 1588 タイムスタンプや MACsec 256 ビット暗号化 (AES 256 GCM) などの機能が、UADP 1.1 で新たにサポートされています。第 2 世代のマルチギガビットおよび SFP+ バージョンの Catalyst 3850/3650 は UADP 1.1 を使用しています。

UADP 2.0

Catalyst 9000 シリーズは、次世代の UADP、つまり UADP 2.0/3.0 ASIC をベースに構築されています。

UADP 2.0 は、トランジスタを 74 億 6,000 万個搭載したデュアルコア ASIC (UADP 1.1 と同様) で、総帯域幅がさらに向上して最大 240 Gbps となっています。UADP 2.0 は、容量と柔軟性を増した再プログラム可能なメモリ テーブルも備え、複数のネットワーク エリアに同じデバイスを導入できるオプションを提供しています (これについて第 14 章「キャンパス ネットワーク設計」で説明しています)。

図 UADP 1.0、1.1、2.0、3.0 の比較



UADP 2.0 ASIC には、UADP 2.0 と UADP 2.0 XL の 2 つのバリエーションがあります。アーキテクチャはどちらも同じですが、UADP 2.0 では、総帯域幅、テーブル サイズ、全体的性能が、アクセス レイヤ デバイス向けに最適化されています。Catalyst 9300 プラットフォームは、UADP 2.0 を使用しています。

UADP 2.0 XL は、モジュラ アクセスやディストリビューション レイヤ スイッチ向けに最適化されています。その役割に適したポート速度と密度に対応するために、メモリ テーブルのサイズが大きく (XL という名称はそれに由来しています)、総帯域幅と全体的性能が高くなっています。UADP 2.0 XL は、720 Gbps の ASIC 間接続のデータ パスがデュアル構成になっているため、複数の ASIC が必要なプラットフォームへの適合性がさらに向上しています。最初の Catalyst 9500 プラットフォームおよび Catalyst 9400 Supervisor-1/Supervisor-1XL は、UADP 2.0 XL を使用しています。

表 UADP 2.0 と 2.0 XL の比較

	UADP 2.0	UADP 2.0 XL
合計帯域幅	最大 160 G	最大 240 G
テーブル サイズ	標準	XL テーブル
TCAM エントリ数	20,000	54,000
バッファ	16 MB	32 MB
スタック帯域幅	240 G	720 G
スタック リング	1	2

UADP 3.0

ワイヤレス スピードの進化、接続デバイス (IoT) の増加、高画質ビデオ会議に拍車をかけられて、ネットワーク スピードには終わりのない要望が寄せられています。新しいテクノロジーが日々登場し、ネットワークのパフォーマンスおよび拡張性に対する新たな要求が生じています。

UADP 3.0 は、トランジスタを 192 億個搭載したデュアルコア ASIC で、最大 1.6 Tbps の総帯域幅を実現しています。UADP 3.0 は、新しいインターフェイス スピード (25 G や 100 G など) や新たなネットワーク設計/ソリューションによって生じる課題に対応できるように設計された、最新バージョンの UADP です。1 つの UADP 3.0 ASIC で、100 G ライン レートのポート 16 個に対応できます。

帯域幅の増加に加えて、UADP 3.0 にはいくつかの新たな改善点が組み込まれ、キャンパス コアおよびディストリビューション向けの理想的な ASIC となっています。また、共有パケット バッファ (36 MB) が拡大して、インターフェイス速度の向上に対応しています。さらに、メモリ テーブル サイズがダブル幅に拡大しており、IPv4 アドレス (32 ビット) と IPv6 アドレス (128 ビット) の両方を 1 つのエントリに保持することができます。他の多くの ASIC や前世代の UADP では、シングル幅のテーブルしかサポートしておらず、IPv6 をサポートするためにはルックアップ サイクルを増やす必要があります。新たな UADP 3.0 ASIC が搭載される最初の製品となるのは、新しい 10/25/40/100 G Catalyst 9500 プラットフォームです。

Cisco IOS XE

IOS の進化

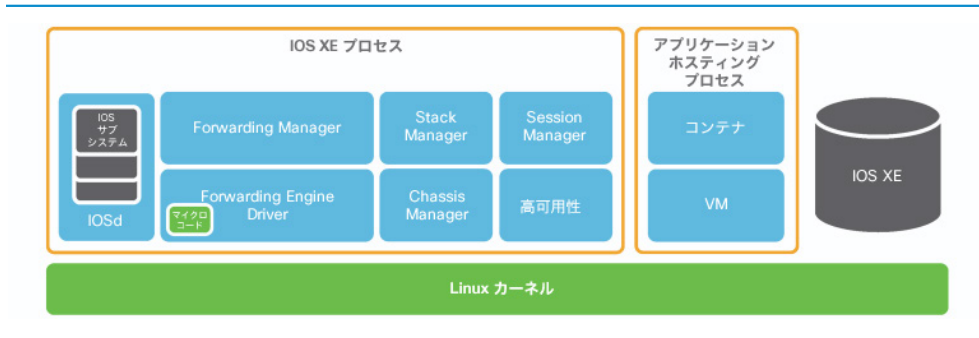
Internetwork Operating System (IOS) の起源は、1986 年に発表されたシスコの最初の製品、AGS マルチプロトコル ルータにさかのぼります。当時の IOS は、かなり初歩的なモノリシック オペレーティング システム (OS) でしたが、業界初のネットワーク オペレーティング システムの 1 つでした。それ以来、何千もの機能が追加され、この 30 年間、業界がさまざまな変遷をたどるのにつれ、IOS は、より機能が充実した OS へと進化してきました。

IOS はさまざまな製品に対応して徐々に多くのバージョンへの分岐も遂げて、幅広いバリエーションが誕生しました。同時に、シスコの製品ポートフォリオも、さまざまな種類のスイッチやルータに拡大してきました。データ センターやサービス プロバイダーなどの専用ネットワーク エリアが発展し、そのエリア向けに NX OS や IOS XR などの新たなオペレーティング システムが導入されました。

数年前、シスコは IOS XE を導入しました。これは、IOS のモノリシック コードを再構築して、モジュラ化の進んだ最新のソフトウェア アーキテクチャを構成するよう設計された製品です。Cisco IOS XE では、OS を複数のコンポーネントに分割して、機能のモジュラ化とポータビリティを実現しました。下位レベルの Linux カーネルを導入して、CPU のロードバランシング、メモリ管理、拡張ハードウェア リソース管理機能を提供しました。現在 IOS は、Linux カーネル上でモジュラ型プロセスとして実行されています (IOSd と呼ばれています)。このアプローチにより、Wireshark やワイヤレス LAN コントローラ (WLC) などの他のモジュラ機能の導入が可能になっています。今後 Cisco IOS XE には、同様のアプローチによって、さらに多くのアプリケーションが組み込まれていく予定です。

Cisco IOS XE は常に進化しています。新しいアプリケーションの継続的な登場に伴い、CLI や SNMP などの定評ある設定/モニタリング向けモデルが、設定/モニタリング データ モデル向けに標準化された API に置き換わり始めています。

図 従来の IOS と IOS XE の比較



最新の Cisco IOS XE ソフトウェアは、以下のような、主要な顧客ニーズに対応できます。

- エンタープライズ ネットワーク向け共通 OS の提供
- 新しい機能やテクノロジーの迅速な導入
- ネットワークを保護するセキュアな OS
- モジュラ性および高可用性
- プログラマビリティおよび自動化

これらの要件を考慮して、プログラマブル UADP 1.0 ASIC を使用する Catalyst 3850/3650 スイッチに、Cisco IOS XE 16.1 が導入されました。それ以来、他のエンタープライズ ネットワーク プラットフォームも、顧客ニーズへの対応に必要なソフトウェアの柔軟性と拡張性を備えた Cisco IOS XE を採用するようになりました。この統合 OS ソフトウェアリリースには、以下のようなさまざまな利点があります。

- 管理対象ソフトウェア イメージの削減
- ソフトウェア機能認証時間の短縮
- 複数のプラットフォーム間で統一された一貫性のある操作性
- 場所を問わずにすべての機能を実行できる機能

さらに、統合されたコード リリースを使用しているため、コア レイヤ プラットフォームの機能をアクセス レイヤ プラットフォームに移す必要が生じた場合も、はるかに簡単に実現できます。ほとんどの場合、プラットフォームに依存するコードを変更するだけで、異なるプラットフォーム間で機能をインポートできます。

Catalyst 9000 スイッチでは、これをさらに 1 歩推し進めています。Catalyst 9000 製品ファミリ全体で同じソフトウェア リリース バージョンを実行しているだけでなく、バイナリ ソフトウェア イメージも同じものを使用しています。異なるプラットフォーム（Catalyst 9300、9400、9500 など）ごとに複数のバイナリ ファイルを管理する必要がなく、Catalyst 9000 シリーズのいずれかのバイナリ ファイルを 1 つダウンロードすれば、それをすべてのプラットフォームで実行できます。これは、ソフトウェア イメージの選択、導入、使用を大幅にシンプルにする付加価値となります。

Cisco IOS XE のアーキテクチャ

Cisco IOS XE は、Linux OS 上に構築されています。Cisco IOS XE の各種コンポーネントは、個別のサブプロセスとして実行されますが、すべての機能の動作状態を同じ形式で保存する共通の情報データベースを共有しています。このモジュラ型 OS アーキテクチャは、プロセスの再起動やパッチ適用などの主要機能を備えているだけでなく、Linux コンテナまたは仮想マシン (VM) を使用してシスコおよびサードパーティ製アプリケーションをホストすることもできます。

Cisco IOS XE アーキテクチャでは、次の 3 つの機能が大きく強化されています。

- IOS のモジュラ化
- Cisco IOS XE データベース
- VM およびコンテナ

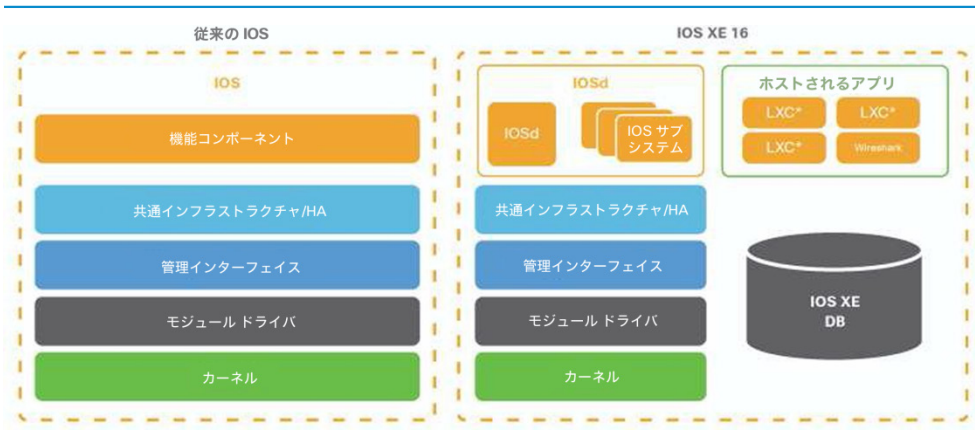
モジュラ型 OS

Cisco IOS XE では、従来の IOS コードが複数のモジュールに分割されています。ベースの IOS コードの大部分は、従来の IOS 機能やスイッチングおよびルーティング プロトコルなどのコンポーネントから構成されるデーモン (IOSd) としてホストされています。

IOSd はさらに複数の IOS サブシステムに分割されており、そのうち 1 つのサブシステムに対する処理を、当該部以外の IOSd コードに影響せずに実施することができます。IOSd では、各サブシステムが当該部以外の IOS コードからは完全に分離しているため、個々のサブシステムに障害が発生した場合の復元力も備えています。

OS がこのようにモジュラ化されているため、ソフトウェア パッチの適用による IOS のアップデート (ソフトウェア メンテナンス アップグレード、略して SMU と呼ばれています) を、稼働中のシステムに影響を与えずに実施することができます。

図 Cisco IOS XE



Cisco IOS XE データベース

これまでの IOS は、すべてのスイッチング/ルーティング プロトコルの状態と、関連する転送情報を、分散して保持していました。プロセスの状態に関する情報がメモリのさまざまな場所に異なる形式で保存されていたため、スイッチの外部で利用できず、不便でした。

Cisco IOS XE アーキテクチャでは、コードとデータが分離されます。OS の新機能として、システムの動作状態と設定を保存する IOS XE データベースが追加されています。データは標準の形式で保存されます。状態の情報を一元化データベースに格納することにより、IOS XE のさまざまなコンポーネント間で簡単に情報を共有できるなど、大きな利点が得られます。

この標準 IOS XE データベースによって、システム データをデータ モデルとして表現することが容易になります。IOS XE には、データベースを YANG などの一般的なデータ モデルに変換するためのインターフェイスが備えられており、モデル駆動型テレメトリ (MDT) を使用した効率的なエクスポートが可能になっています。MDT については、第 12 章「プログラマビリティおよび自動化」で詳しく説明します。

コンテナと VM

Cisco IOS XE は、Catalyst 9000 で LXC コンテナと VM ホスティング機能をサポートしています。第 13 章「アプリケーション ホスティング」を参照してください。

Cisco IOS XE の利点

現代のソフトウェア定義型環境は絶え間なく変化しており、Catalyst 9000 には、オープンで使いやすく柔軟かつ安全な OS ソフトウェア基盤が不可欠になっています。Cisco IOS XE は、複数のエンタープライズ ネットワーク製品に共通しているオープンなモジュラ型オペレーティング システムで、お客様に多くのメリットをもたらします。Cisco IOS XE のモジュラ性、標準データベース、オブジェクトベース モデル、コンテナによって、ネットワーク管理者およびエンジニアの運用業務に役立つ重要な機能が提供され、運用コストの削減が実現します。

また、Catalyst 9000 スイッチ全体で 1 つのソフトウェア イメージが使用されることで、ネットワーク管理がシンプルになり、ソフトウェア ライフサイクル管理が改善されるというメリットもあります。これにより、一貫した形式や操作性が実現し、すべてのデバイスを同じインターフェイスでプロビジョニングすることができます。「場所を問わずにあらゆる機能を実行可能」というアプローチは、機能を他のプラットフォームに非常に短時間で移行できることを意味しています。たとえば最近では、短時間で Catalyst プラットフォームにソフトウェアをインポートした例として、MPLS、NAT、NBAR2 などがありました。

他にも、Cisco IOS XE インストール モード、新たな Web UI、Cisco Trustworthy Systems などが、主な利点として挙げられます。

Cisco IOS XE インストール モードでは、パッケージがすでに .bin ファイルから抽出されているため、メモリの消費量が少なくなります。バンドル モードと比べると、インストールモードのほうが Catalyst 9000 スイッチで IOS を速く起動できます。ISSU、パッチ適用、FSU などの先進的な高可用性機能はインストール モードでのみサポートされているため、インストール モードが推奨されます。

Cisco IOS XE Web UI の導入により、標準的な Web ブラウザでデバイスを操作できるようになりました。簡単な設定、トラブルシューティング、CPU やメモリの高使用率のモニタリングを Web UI で実施できます。また、さまざまなアプリケーションを監視する AVC などの、高度な機能を設定することもできます。

シスコは、ネットワーク攻撃の防御を支援する信頼できるスイッチとして Catalyst 9000 ファミリ スイッチを構築しました。Catalyst 9000 ファミリは、信頼できるシステムとして、プラットフォームの信頼性の検証、悪意あるコードの実行の防止、ランタイム防御の確立、通信の保護を実現します。詳細については、第 7.3 章「信頼できるシステム」を参照してください。

高可用性

概要

ビジネスの継続性を確保するためには、高可用性（HA）を備えたネットワークとネットワーク機器を構築することが不可欠です。Catalyst 9000 スイッチには、HA を実現する従来からのさまざまな技術に加え、さらに新しい技術も導入されています。このセクションでは、以下の手法について解説します。

- Catalyst 9300 の高可用性：スタッキング、電源、Fast Software Upgrade
- Catalyst 9400 の高可用性：シャーシ、スーパーバイザ、電源、ISSU
- Catalyst 9500 の高可用性：Stackwise Virtual、ISSU
- グレースフル挿抜
- Cisco IOS XE のパッチ適用

Catalyst 9000 スイッチは、2 つの HA 技術を活用しています。

ステートフル スイッチオーバー

ステートフル スイッチオーバー（SSO）によって、冗長デバイス構成を実現するレイヤ 2 セッションの中断が最小限になります。SSO は、アクティブ コンポーネントとスタンバイ コンポーネント間で、転送テーブルと、実行中設定と起動時設定の両方を複製します。アクティブ デバイスに障害が発生した場合、システムは即座にスタンバイ デバイスに制御を切り替えます。

ノンストップ フォワーディング (NSF)

通常、ネットワーキング デバイスが再起動すると、デバイスが一度ダウンした後に再び起動したことを、そのデバイスのすべてのルーティング ピアが検知します。このような移行によって、いわゆるルーティング フラップが発生します。ルーティング フラップは、複数のルーティング ドメインに広がる場合があります。再起動によって発生したルーティング フラップによって、ルーティングが不安定になります。これはネットワーク全体のパフォーマンスに悪影響を及ぼします。ノンストップ フォワーディング (NSF) は、SSO 対応デバイスでのルーティング フラップを抑制します。NSF では、スイッチオーバー後にルーティング プロトコル情報が復元されている間に、既知のルートでデータ パケットの転送を継続できます。NSF を使用すると、ピア ネットワーキング デバイスでルーティング フラップは発生しません。

この章のサブセクションでは、各スイッチのファミリが SSO および NSF を少し異なる方法で活用して高可用性を実現していることを説明します。

Catalyst 9300 の高可用性

Catalyst 9300 では、Stackwise-480、StackPower、Fast Software Upgrades (FSU) などの機能によってアクセス レイヤの冗長性を実現しています。

Catalyst 9300 スイッチ スタック

固定構成の Cisco Catalyst 9300 シリーズ スイッチには、ポート密度とスイッチング性能を拡張し、ワイヤリング クローゼットにおける冗長性を実現するための、スタッキング機能が備えられています。さらに、スタッキングにより複数のスイッチを統合して 1 つの論理スイッチを形成することで、運用がシンプルになります。

Catalyst 9300 上の Cisco IOS XE では、最大 8 メンバーまで、任意の Catalyst 9300 モデルを混在させてスタックすることが可能です。各メンバーは、各スイッチ背面のスタッキング ポートに接続された特殊なスタッキング ケーブルを使用して、物理的にリング状に接続されています。

Catalyst 9300 スタックは、最大 448 ポートに対応する確定的なノンブロッキング スイッチング性能を提供します。このスイッチング性能によって、以下のようなハードウェア アクセラレーション型の統合ネットワーク サービスを実現できます。

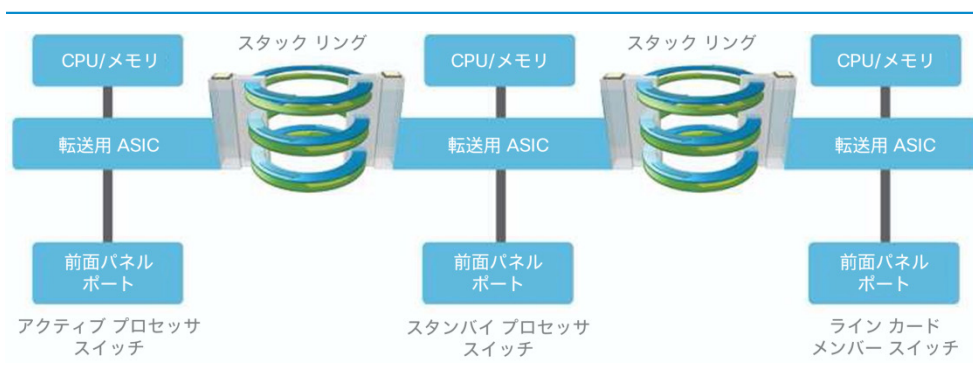
- PoE (最大 15.4 W)
- PoE+ (最大 30 W)
- Universal PoE (最大 60 W)
- Quality of Service (QoS)
- アクセス コントロール リスト
- Flexible NetFlow

注 スタック内のすべてのスイッチが、同じバージョンの Cisco IOS XE およびライセンスを実行する必要があります。

Stackwise-480 アーキテクチャ

Catalyst 9300 スイッチは、Stackwise-480 と呼ばれるスタックリング ファブリックを使用して、スタック構成を実現します。Stackwise-480 という名称は、対応可能な総スタック容量が 480 Gbps であることに由来しています。ファブリックは、6 つの反転リング（40 Gbps/リング）で構成され、システムのスループットは、これらのリングのスループットの合計（240 Gbps）に応じた値になります。スタック リングに空間的再利用を導入すると、スループットが 2 倍になります。空間的再利用は、宛先パケットストリッピングによって可能になります。通常、リング アーキテクチャでは、リングからのパケット ストリッピングはパケット送信元のスイッチで行われ、リング メンバーがパケットを処理している間は、リングには他のデータは転送されません。しかし、空間的再利用の場合は、複数のフローを共存させることができます。空間的再利用では、宛先スイッチに送信されるパケットを宛先スイッチ自身がストリッピング（除去）することでリングの使用可能帯域幅が解放され、そのリングに他のスタック メンバーが追加パケットを挿入できるようになります。

図 Stackwise-480 のアーキテクチャ



Stackwise-480 は、スタック内の 1 つのスイッチをアクティブ スイッチとして選択し、もう 1 つ別のスイッチをホットスタンバイとして選択することで、統合された制御/管理プレーンを生成します。残りのスイッチはスタック メンバーになります。アクティブ スイッチは、レイヤ 2 およびレイヤ 3 ネットワークの制御処理すべてと、全ステータス情報をホットスタンバイ スイッチと同期させる処理を受け持ちます。アクティブ スイッチは、スタック全体の管理を一元化します。管理者は、すべての設定およびモニタリングをアクティブ スイッチ経由で実施します。

転送アーキテクチャは、スタック内のすべてのメンバー スイッチで分散型スイッチングを実現できるように設計されています。スタック内の各スイッチは、それぞれのローカルハードウェア リソースを活用することで、データ プレーンのパフォーマンスを最適化します。たとえば、転送タスクおよび QoS や ACL などのネットワーク サービスが含まれます。スタック処理を分散することで、ワイヤスピードのパフォーマンスが実現し、全体的なシステム リソース容量が増加します。また、アクティブ スイッチ プロセッサの過負荷を回避し、スタックリングの帯域幅容量を最適化します。

Stackwise-480 での SSO/NSF のサポート

Catalyst 9300 スイッチは、ネットワーク通信を途切れなく提供するために、レイヤ 2 およびレイヤ 3 のステートフル機能を幅広くサポートしています。スタック内のアクティブ スイッチは、プロトコル ステート マシン、ソフトウェア転送テーブル、システム設定をスタック内のスタンバイ スイッチと同期させます。サポートされるプロトコルを次の表に示します。

表 Stackwise-480 でのステートフル プロトコルのサポート

レイヤ	HA 対応プロトコル
レイヤ 2	STP、VLAN、VTP、DTP、CDP、UDLD、SPAN/RSPAN、802.1x、PAGP/LACP、IGMP Snooping
レイヤ 3 - IPv4	ARP、EIGRP、OSPF、IS-IS、BGP、MPLS LDP
レイヤ 3 - IPv6	EIGRPv6、OSPFv3、IS-ISv3、BGPv6、ICMPv6
サービス	QoS、ACL、PBR、NetFlow、ポート セキュリティ

StackPower

Cisco StackPower は、スイッチ スタック内で利用できるすべての電力を 1 つの共通電力プールに集約し、スタック メンバー間で電力を共有させます。1 つの電力スタックに最大 4 つのスイッチを設定できます。そのためには、Cisco StackPower ケーブルを使用して、各スイッチの背面にある特別なポートに接続する必要があります。StackPower を使用するには、まず Stackwise-480 を有効にしておく必要があります。したがって、メンバーが 8 つのデータ スタックの場合には、2 つの電力スタックに 4 スイッチずつ設定することで、8 メンバーのスタックをすべて使用できます。

Cisco StackPower を利用すると、スイッチ スタック 1 つあたりに必要な電源装置の数と、ワイヤリング クローゼットに必要な電源プラグの数が少なくなります。低負荷での非効率的な電源装置運用によるエネルギーの無駄を最小限に抑え、ワイヤリング クローゼット内の冷却を削減することで、コストをよりいっそう節約できます。このテクノロジーでは、外部電源シェルフも必要なくなるので、ワイヤリング クローゼット内のスペースや電源プラグがさらに開放されます。

StackPower の動作モード

Cisco StackPower には、共有モードと冗長モードの 2 つの動作モードがあります。

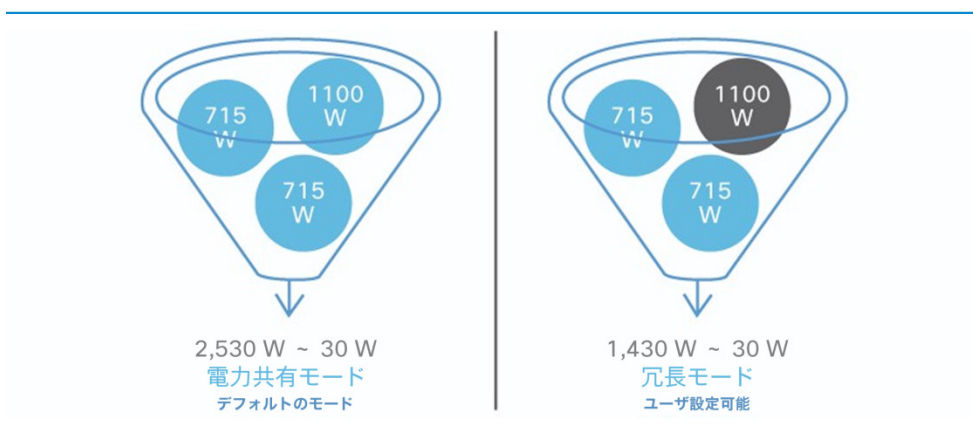
共有モード（デフォルト）では、すべての入力電力がスタック内のあらゆる箇所で使用可能になります。使用可能な総電力量によって、電力バジェットが決まります。電源装置に障害が発生した場合は、電力バジェットに残っている使用可能電力が利用されるため、システム コンポーネントにも PoE デバイスにも影響は及びません。電力バジェットに十分な電力がない場合は、優先順位に基づいて、PoE デバイスがシャット ダウンし、その後でスイッチがシャット ダウンする可能性があります。デフォルトでは、以下の順に電力が制限されます。

- 1 低プライオリティ ポート
- 2 高プライオリティ ポート
- 3 スイッチ

電力使用の優先順位は設定で変えることができます。デフォルトでは、システム内のポートはすべて、優先順位が低くなっています。

冗長モードでは、最大の電源から供給される電力が電力バジェットから差し引かれます。それにより、使用可能総電力は少なくなりますが、電源障害発生時に利用できるバックアップ電源が確保されます。

図 StackPower の共有モードと冗長モードの比較



また、StackPower は、新しいスイッチがスタックに追加された場合に備えて、30 W 分の引き当ても用意しておきます。

さらに、Cisco StackPower では、Cisco Expandable Power System (XPS 2200) を使用することで、より大規模な電力プールの導入も可能になります。このシステムでは、最大 8 台のスイッチと電力を共有します。

Fast Software Upgrade (FSU; 高速ソフトウェア アップグレード)

Catalyst 9300 スタンドアロン スイッチまたはスタック構成スイッチで通常のソフトウェア アップグレードを実施すると、その間、新しいイメージが完全にロードされるまで、ユーザ トラフィックが中断されます。これは、ソフトウェアのアップグレード中にコントロール プレーンとデータ プレーンが同時にリセットされるためです。

Fast Software Upgrade (FSU) 機能では、コントロール プレーン機能とデータ プレーン機能の更新が分離され、そのためシステム アップグレードへの影響が少なくなります。このプロセスを利用すると、スイッチがコントロール プレーンを更新する間も、トラフィックは中断されず、引き続き転送されます。FSU プロセスで転送に影響が出るのは、データプレーンがアップグレードされるときだけです。FSU では、通常のアップグレード プロセスと比べて、アップグレードによるダウンタイムが約半分になります。

FSU 機能は、スタッキング システムとスタンドアロン システムの両方でサポートされます。また、ソフトウェアのアップグレードだけでなく、スイッチのリロードの管理に使用することもできます。

Catalyst 9400 の高可用性

Cisco Catalyst 9400 シリーズでは、停止を最小限に抑えるために、次のような機能が提供されています。

- デュアル スーパーバイザ ステートフル スイッチオーバーとノンストップ フォワーディング
- スーパーバイザ エンジン アップリンクの冗長性
- インサービス ソフトウェア アップグレード (ISSU)
- 電源の冗長性
- 電力使用の優先順位設定

デュアル スーパーバイザ ステートフル スイッチオーバーとノンストップ フォワーディング

2 つめのスーパーバイザ モジュールがシャーシに挿入されると、デフォルトで、スーパーバイザ エンジンの冗長性が有効になります。冗長スーパーバイザ エンジンは、アクティブ スーパーバイザの実行中設定および起動時設定と自動的に同期します。スイッチの現在の転送状態も冗長スーパーバイザに複製され、継続的に更新されます。アクティブ スーパーバイザ エンジンに障害が発生した場合は、ステートフル スイッチオーバー (SSO) がトリガーされます。SSO とノンストップ フォワーディング (NSF) が両方設定されている場合は、スイッチオーバー時にルーティングに対する影響は生じません。それ以外の場合、影響を受けないのはレイヤ 2 スイッチングのみとなります。

スーパーバイザ エンジン アップリンクの冗長性

図 スーパーバイザ アップリンク ポート グループ



- ポートグループ1: 10 Gイーサネット 1 ~ 4、40 Gイーサネット 9
- ポートグループ2: 10 Gイーサネット 5 ~ 8、40 Gイーサネット 10

上の図では、各スーパーバイザに 10 GE インターフェイス X 8 と 40 GE インターフェイス X 8 があります。インターフェイス 1 ~ 8 が 10 GE インターフェイスで、ポート 9、10 が 40 GE インターフェイスです。スーパーバイザはさらにこれらのインターフェイスを 2 つのポートグループにまとめます。インターフェイス 1 ~ 4 と 9 が最初のポートグループに属し、インターフェイス 5 ~ 8 と 10 が 2 つめのポートグループに属します。

各ポートグループが、最大 40 Gbps のトラフィックをサポートします。スーパーバイザは、この 40 Gbps を、10 GE インターフェイス X 4 または 40 GE インターフェイス X 1 のどちらかで柔軟に使用できます。

スーパーバイザは、異なるインターフェイス タイプの混在に対応しています。一方のポートグループに 4 つの 10 GE インターフェイスを接続して他方のポートグループには 40 GE インターフェイスを接続することも選択可能です。

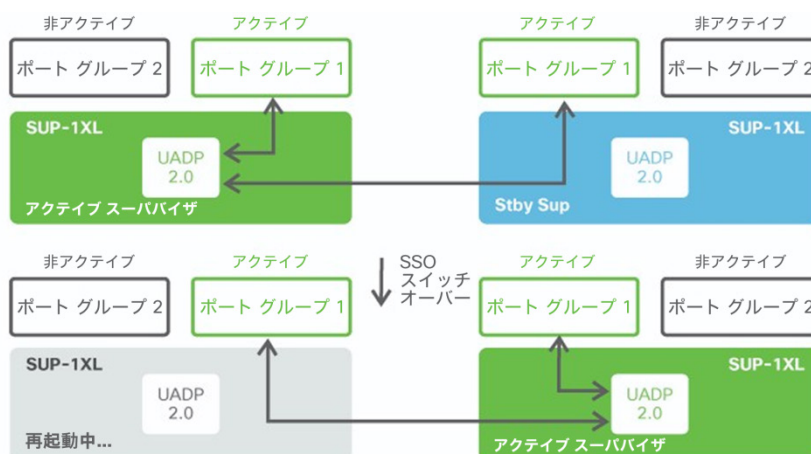
図 デュアル スーパーバイザ アップリンク構成



- ポートグループ1: 10 Gイーサネット 1 ~ 4、40 Gイーサネット 9
- ポートグループ2: 非アクティブ。10 Gイーサネット 5 ~ 8、40 Gイーサネット 10

Catalyst 9400 にデュアルスーパーバイザがインストールされている場合、同スイッチは両方のスーパーバイザ上の 2 番目のポート グループを自動的に無効にします。スーパーバイザのスイッチオーバーが発生したときには、再起動中のスーパーバイザのアクティブなアップリンクポートが、中断することなくトラフィックの転送を続けます。

図 ステートフル スイッチオーバー時にもアップリンクはアクティブ状態を維持



インサースビス ソフトウェア アップグレード

インサースビス ソフトウェア アップグレード (ISSU) を利用すると、ソフトウェアのフル機能アップグレードによる計画停止をなくすることができます。つまり、システムを停止させることなく Cisco IOS XE ソフトウェアのアップグレード、ダウングレード、ロールバックを行うことが可能です。ISSU テクノロジーは、補助機能として、SSO と NSF を使用します。

ISSU は、特定の順番で発行された exec レベルの CLI コマンド セットを使用して実装される管理プロセスです。

ISSU の前提条件

Cisco Catalyst 9400 スイッチで ISSU を実行する前に、次のことを確認する必要があります。

- スイッチが、同じモデルの冗長スーパーバイザ エンジンを使用している。
- アクティブ スーパーバイザが新しい Cisco IOS XE イメージにアクセスできる。または、Cisco IOS XE イメージが事前にフラッシュにロードされている。
- スイッチがルーティング プロトコルを実行している場合は、（必須ではないが）NSF が推奨される。
- システムが、インストール モードで実行されている。

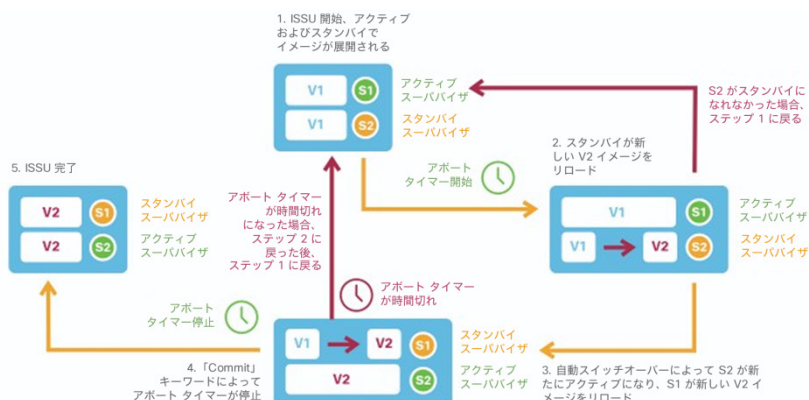
ISSU プロセス

ISSU プロセスには 5 つのステップがあります。

- 1 管理者が ISSU を開始します。新しいイメージがアクティブとスタンバイの両方のスーパーバイザで展開されます。
- 2 スタンバイ スーパーバイザ エンジンに新しいイメージがリロードされます。
- 3 スイッチがスタンバイ スーパーバイザへの自動スイッチオーバーを実施し、それがアクティブ スーパーバイザとなります。もう一方のスーパーバイザに新しいイメージがリロードされ、スタンバイ ロールに変わります。
- 4 ISSU プロセスが正常に完了すると、アップグレードがコミットされます。正常に完了しなかった場合は、ISSU プロセスによって前のイメージに自動的にロールバックされます。
- 5 これで、ISSU は完了です。

ISSU プロセスの仕組みの詳細を、次の図に示します。

図 ISSU プロセスの詳細



注 スーパーバイザのスイッチオーバー中に、1 秒未満でトラフィックの再コンバージェンスが行われます。

電源冗長モード

Cisco Catalyst 9400 シリーズの 4 スロット シャーシには 4 つの電源ベイがあり、7 スロットおよび 10 スロット モデルには 8 つのベイがあります。電源は、連結モードまたは冗長モードで動作させることができます。

デフォルトは連結モードです。連結モードでは、すべての電源がアクティブで、システムの負荷を共有します。1 つの電源に障害が発生した場合、残りの電源が負荷を引き受けます。

冗長モードは、N+1 と N+N の 2 種類の構成をサポートしています。N+1 では、いずれか 1 つの電源に障害が発生した場合に対応できます。N+N では、複数の電源に障害が発生した場合に加え、電源入力回路に障害が発生した場合にも対応できます。

N+1 冗長電源モード

このモードはユーザ設定モードであり、ユーザがいずれか 1 つの電源をバックアップとして指定することができます。バックアップとして指定された電源は、スタンバイ モードを維持します。アクティブな電源のいずれかに障害が発生した場合、バックアップ電源がアクティブになります。

図 N+1 冗長電源モード



N+N 冗長電源モード

このモードもユーザ設定モードです。このモードでは、オペレータが電源をアクティブとバックアップの 2 つのグループに分割します。アクティブ グループの電源がシステムの負荷を共有し、バックアップ電源はスタンバイ モードを維持します。2 つのグループは、同じ入力回路にも別々の入力回路にも接続できます。プライマリの入力源に障害が発生するか、アクティブな電源のいずれかに障害が発生した場合、すべてのバックアップ電源がアクティブになります。

図 N+N 冗長電源モード



電力使用優先順位

Catalyst 9400 シリーズでは、ライン カード スロットの電力使用優先順位を設定できます。PoE の追加消費や突然の障害によって、システムの使用可能電力を超える電力が必要になる場合、システムは、電力制限を開始します。スーパーバイザとファン トレイは常に最優先され、順位の変更はできません。デフォルトでは、まず一番下のスロットのライン カードから電源がオフになり、その後、順番に上のスロットまで進んでいきます。ただし、各ライン カードの電力使用優先順位を個別に設定することもできます。

StackWise Virtual

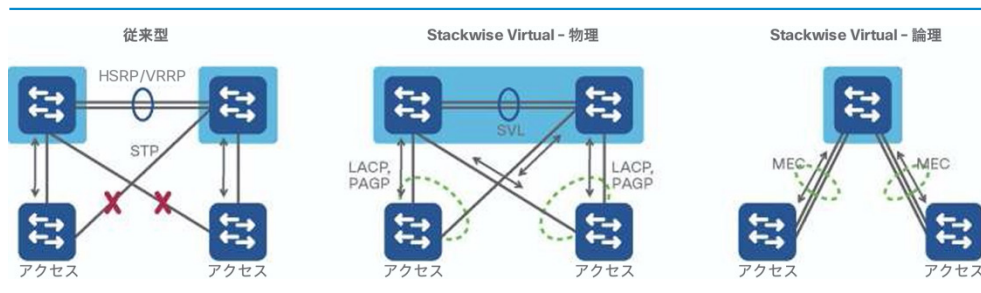
Cisco Catalyst 9500 シリーズの Stackwise Virtual 機能では、2 つの物理スイッチを 1 つの論理スイッチに統合することができます。2 つのスイッチは 1 つのスイッチとして動作し、同じ設定と転送状態を共有します。これは、前世代の Catalyst スイッチ ラインにおける仮想スイッチ システム (VSS) 機能と類似しています。

注 Stackwise Virtual を機能させるには、両方の Catalyst 9500 スイッチが同一のハードウェア、ソフトウェア、ライセンス レベルを使用する必要があります。

Stackwise Virtual によってキャンパス ネットワークの設計が大幅にシンプルになります。2 つのスイッチが 1 つのスイッチとして動作するためループの起こらないトポロジを作成できます。したがって、スパンニング ツリー ドメインは、Stackwise Virtual ペアを 2 つのブリッジ ノードではなく 1 つのブリッジ ノードとして扱います。

また、Stackwise Virtual は、ステートフル スイッチオーバー、ノンストップ フォワーディング、インサービス ソフトウェア アップグレードなどの高可用性機能も備えており、それによってデバイスレベルでの冗長性が実現し、HSRP や VRRP などのレイヤ 3 冗長プロトコルが不要になります。MultiChassis EtherChannel (MEC) もサポートし、リンク冗長性と帯域幅増加の両方を実現しています。

図 従来のアーキテクチャから Stackwise Virtual への移行がもたらす利点

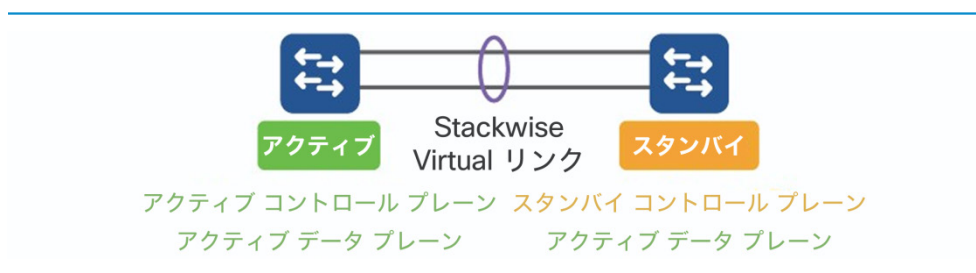


Stackwise Virtual のアーキテクチャ

Stackwise Virtual ペア内では、1つのデバイスがアクティブな仮想スイッチとして指定され、もう 1 つはスタンバイ仮想スイッチとなります。アクティブな仮想スイッチは、すべてのコントロールプレーン機能を管理し、システムの現在の状態をスタンバイピアに配布します。

- 管理（実行中設定、起動時設定、SNMP、Telnet、SSH など）
- レイヤ 2 プロトコル（BPDU、LACP など）
- レイヤ 3 プロトコル（EIGRP、OSPF、BGP、LDP など）

図 Stackwise Virtual ドメイン



データプレーンとトラフィック転送の観点からすると、Stackwise Virtual ペア内の両スイッチは、どちらもトラフィックをアクティブに転送します。各スイッチは、転送の判断をそれぞれローカルで行い、必要な場合には L2/L3 MEC またはレイヤ 3 Equal Cost Multipath (ECMP; 等コスト マルチパス) を利用して隣接するスイッチにトラフィックを転送します。

Stackwise Virtual のコンポーネント

Stackwise Virtual は、次のコンポーネントを使用して構成されます。

- 1 Stackwise Virtual リンク
- 2 デュアルアクティブ検出リンク
- 3 MultiChassis EtherChannel

Stackwise Virtual リンク

Stackwise Virtual リンク (SVL) は、Stackwise Virtual ドメインを構成する重要なコンポーネントです。2 つのスイッチのコントロール プレーンの同期に使用されるシグナリング パスを提供します。これは、2 つのスイッチ間で転送する必要があるすべてのユーザ データ トラフィックのデータ パスとして機能します。SVL は、任意の 10/40 G インターフェイスを使用して設定できる EtherChannel です。Stackwise Virtual は、SVL を構成するためのインターフェイスを最大 8 つまでサポートしています。シスコでは、2 つのスイッチ間で冗長性を確保するとともに、一方のピアのアップリンクまたはダウンリンクに障害が発生した場合のスイッチ間共通帯域幅を増やすために、1 つの SVL に複数のリンクを使用することを推奨しています。

デュアルアクティブ検出

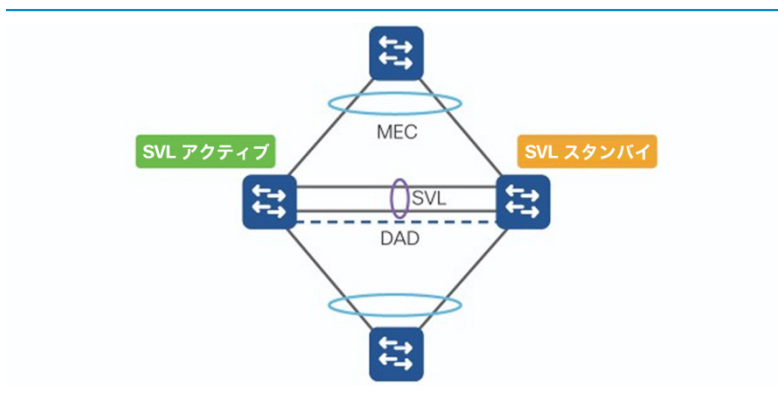
何らかの理由で SVL リンクに障害が発生した場合、Stackwise Virtual ペア間の通信は切断されます。こうなると、両方のスイッチがアクティブ ロールを担うデュアルアクティブ状態となり、転送とネットワーク トポロジの両方に悪影響が及ぶ可能性があります。シスコは、デュアルアクティブ状態を回避するために、デュアルアクティブ検出 (DAD) を設定することを推奨しています。DAD は、デュアルアクティブ状態を検出すると、1 つのスイッチのポートを無効にしてトラフィックのブラックホール化を防ぎます。無効化されたこのスイッチが再起動されて、デュアルアクティブ状態が解消します。デュアルアクティブ検出は、任意の 1/10/40 G インターフェイスの専用リンクを使用して導入することもできますし、ePAgP を使用して設定することもできます。DAD リンクには、最大 4 つのインターフェイスを使用できます。冗長性を確保するために複数のリンクを使用することが推奨されます。

注 管理インターフェイスを DAD に使用することはできません。

MultiChassis EtherChannel

MultiChassis EtherChannel (MEC) では、デュアルホーム接続を個別リンクではなく EtherChannel リンクとして設定できるため、Stackwise Virtual スイッチと隣接スイッチ間の接続がシンプルになります。MEC では、レイヤ 2 またはレイヤ 3 のいずれかのマルチパス設定が可能であり、それによって帯域幅が増加し、物理リンクの冗長性が確保されます。Stackwise Virtual は、128 MEC をサポートしており、「オン」、LACP、PAgP のいずれかのモードを使用して設定できます。

図 Stackwise Virtual のコンポーネント



Stackwise Virtual の高可用性

アクティブな Stackwise Virtual スイッチで障害が発生した場合、スタンバイ スイッチが即座にアクティブになり、トラフィックの転送を続けます。Stackwise Virtual は、NSF および SSO を活用して 1 秒未満でスイッチオーバーを実現します。

注 NSF をルーティング プロトコルに対して明示的に有効にしておく必要があります。

Stackwise Virtual のインサービス ソフトウェア アップグレード

Stackwise Virtual は、インサービス ソフトウェア アップグレードをサポートしています。ISSU を活用することで、ネットワークを停止させずに Stackwise Virtual ペアで Cisco IOS XE ソフトウェアをアップグレードすることができます。ISSU は、アップグレード、ダウン グレード、ロールバックをサポートします。

ISSU の前提条件

Catalyst 9500 Stackwise Virtual スイッチで ISSU を実行する前に、次のことを確認する必要があります。

- アクティブ スイッチが新しい Cisco IOS XE イメージにアクセスできる。または、Cisco IOS XE イメージが事前にフラッシュにロードされている。
- スイッチが、インストール モードで実行されている。
- NSF が有効になっている。

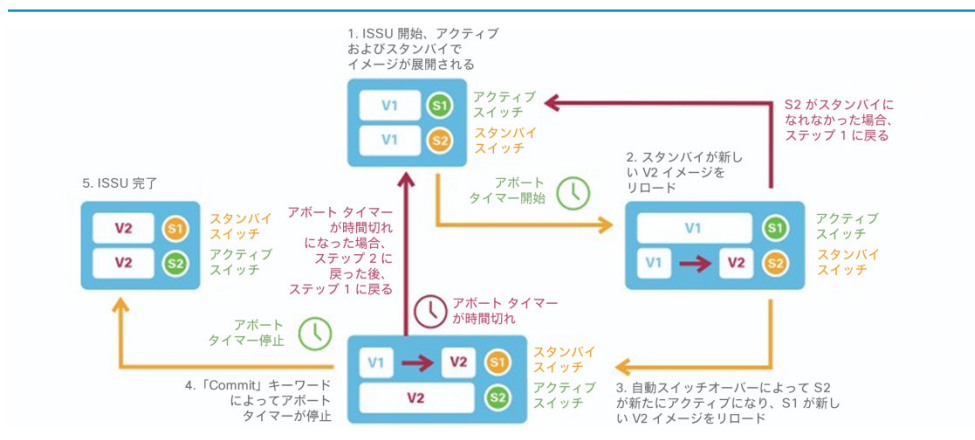
ISSU プロセス

ISSU プロセスには 5 つのステップがあります。

- 1 管理者が ISSU を開始します。新しいイメージがアクティブとスタンバイの両方のスイッチで展開されます。
- 2 新しいイメージがスタンバイ スイッチにリロードされます。
- 3 自動スイッチオーバーによって、スタンバイ スイッチが新たなアクティブ スイッチになります。もう一方のスイッチに新しいイメージがロードされ、スタンバイ ロールに変わります。
- 4 ISSU プロセスが正常に完了すると、アップグレードがコミットされます。正常に完了しなかった場合は、ISSU プロセスによって前のイメージに自動的にロールバックされます。
- 5 これで、ISSU は完了です。

ISSU プロセスの仕組みの詳細を、次の図に示します。

ISSU プロセス



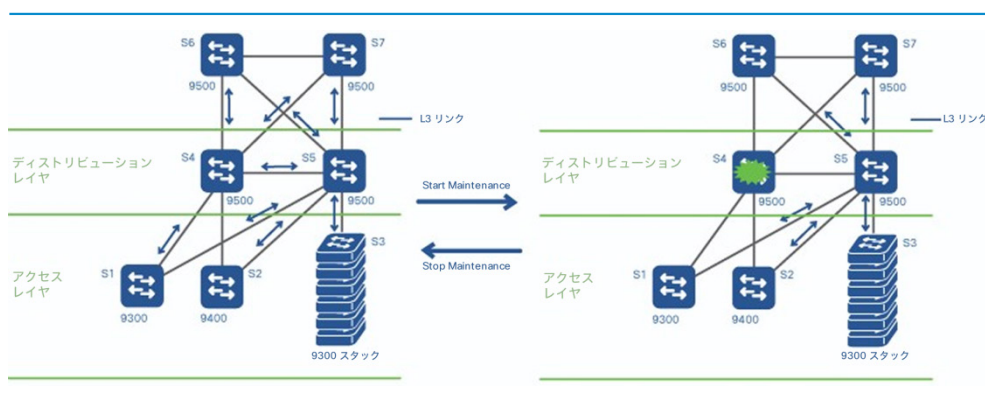
注 スイッチオーバー中に、1 秒未満でトラフィックのコンバージェンスが行われます。

グレースフル挿抜

いったんスイッチがトラフィックの転送を始めると、アクティブ フローに影響を与えずにそのスイッチをネットワークから簡単に取り外す方法はありません。ハードウェアの交換、ソフトウェアのアップグレード、トラブルシューティングなどのメンテナンスを実行する必要がある管理者にとっては、それでは問題があります。この問題はグレースフル挿抜（GIR）によって解決できます。GIR では、冗長パスと既存のルーティング プロトコルを活用して、アクティブ フローに影響を与えずにデバイスをグレースフル（円滑）に分離することができます。その逆に、作業が完了した際にデバイスを再び挿入して再稼働させることも、円滑に実施できます。

基本的に GIR では、これからメンテナンスしようとするネットワーク デバイスのルーティングやファーストホップ ゲートウェイのメトリックをネットワーク管理者が操作して、そのパスを通らないようにすることが、容易に可能です。これは、メトリックの数値を実際より大きくするか、このデバイスがトラフィックの転送に最適なパスではないことを示すメッセージをピアに送信することによって、実現されます。トラフィックがデバイスを通らなくなれば、メンテナンス アクションを始めることができます。メンテナンスが完了すると、変更したメトリックを元の値に戻すことで、通常のトラフィック フローが円滑に回復します。以下の図は、ルーテッド アクセス トポロジのサンプルです。S4 がメンテナンス モードになり、すべてのトラフィックが冗長パスに円滑に転送される様子を示しています。

図 グレースフル挿抜の実行



注 GIR は、コアおよびディストリビューション レイヤで使用されることを想定しています。

GIR は、2 ステップ コマンド構造になっています。GIR がなければ、同じ結果を実現するのにも、リスクを伴う多段階の手動プロセスが必要になるはずです。GIR のコマンド構造はシンプルです。start maintenance コマンドでスイッチを運用から除外し、stop maintenance コマンドで稼動状態に戻します。

GIR では、スイッチの抜き取りと挿入の管理に、それぞれ maintenance-mode プロファイルと normal-mode プロファイルの 2 つのプロファイルが使用されます。maintenance-mode プロファイルには、スイッチをメンテナンス モードに移行するためのすべてのコマンドが含まれています。一方、normal-mode プロファイルには、スイッチをネットワークに再挿入するためのすべての CLI コマンドが含まれています。

現在 IPv4 と IPv6 の両方に対して GIR でサポートされているプロトコルは、以下のとおりです。

表 GIR プロトコルと挿抜方法

プロトコル	グレースフルな抜き取り	グレースフルな挿入
ISIS	Overload ビットを 1 にして LSP を更新	Overload ビットを 0 にして LSP を更新
OSPF	メトリックを最大にして LSA を送信	メトリックを元に戻して LSA を更新
HSRP	終了メッセージをアドバタイズ	Hello メッセージをアドバタイズ
VRRP	優先順位 0 をアドバタイズ	元の優先順位に戻す

Catalyst 9000 スイッチでは、サイト固有の挿抜方法を実行するためのカスタムのメンテナンス プロファイルを柔軟に定義できます。たとえば、デバイスに HSRP または VRRP が設定されている場合、デフォルトでは、アクティブ/スタンバイ ロールを変えながら、アクセス レイヤに接続しているレイヤ 2 ポートが GIR メンテナンスによってシャット ダウンされます。しかし、カスタマイズしたテンプレートを利用すれば、HSRP/VRRP だけの分離を定義して、レイヤ 2 ポートはシャット ダウンしないようにすることができます。

Catalyst 9000 シリーズ スイッチは、メンテナンス前後のスイッチの状態を記録する、システム生成のスナップショットも提供します。スナップショットは、スイッチが稼動状態に戻ったときに正常に動作しているか確認するのに役立ちます。

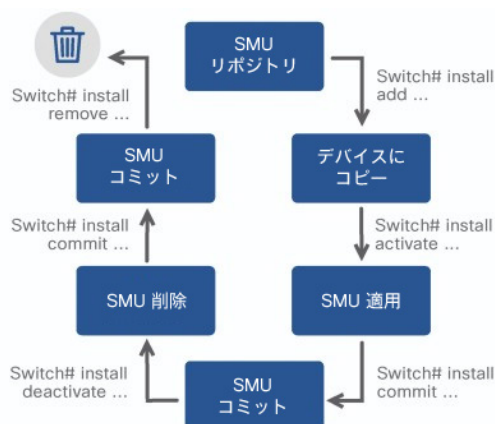
Cisco IOS XE へのパッチの適用

ソフトウェアには不具合が発生するものです。愉快的なことではありませんが、それが現実です。スイッチのオペレーティング システムに障害が発生した場合、ネットワークの動作、ひいては事業運営にまで影響が及びます。障害を発見すると面倒な気分になりますが、障害を修正するのも、同じくらい厄介な作業になる可能性があります。多くの場合、既存のコードの適格性を再確認して、問題が本当に解決されたことを確認するとともに、新しいコードによって新たな問題が発生しないことを検証する必要があります。さらに、ネットワーク インフラストラクチャ全体に新しいソフトウェアを展開して適用する際には、一般に、システムのダウンタイムを調整する必要があります。

Cisco IOS XE では、この問題を解決する方法としてパッチ適用を導入しています。モジュラ型オペレーティング システムである Cisco IOS XE では、イメージ全体をアップグレードすることなく、ソフトウェア内のピンポイント修正を行うことが可能です。つまり、バグやセキュリティ脆弱性を解決するのに、まったく新しいイメージの適格性を再確認する必要がなく、場合によっては、スイッチをリセットしてダウンタイムを招く必要すらありません。

パッチ適用は、ソフトウェア メンテナンス アップグレード (SMU) とも呼ばれています。そのワークフローを、下の図に示しています。SMU を適用するとき、管理者はまず、スイッチにパッチをアップロードします。次に、新しいパッチが利用可能であることをスイッチに認識させるために、パッチを有効にします。有効になると、そのパッチが適用されます。この時点でパッチは有効になります。ただし、必要であれば、管理者がそのパッチを無効にして削除し、ローカル ストレージから SMU を削除することで、ロールバックすることもできます。しかし、修正に問題がなければ、管理者がパッチをコミットすることで、パッチはシステムのリロード後も永続的に有効となります。

図 ソフトウェア メンテナンス アップグレードのワークフロー



パッチ適用には、コールド パッチとホット パッチという 2 つの種類があります。コールド パッチを適用する場合、問題を修正するためにはスイッチのリロードが必要です。一方、ホット パッチではシステム リロードの必要はありません。代わりに、パッチが適用されたプロセスのみをスイッチによって再起動させる必要があります。

SMU パッチを導入するには、いくつかの方法があります。管理者がスイッチごとにスイッチのコマンド ライン インターフェイスを利用することができます。大規模なインフラストラクチャ全体にパッチを配布する場合、シスコでは、Catalyst 9000 API または Cisco DNA Center を活用するスクリプトの使用を推奨しています。これには、ソフトウェア イメージ管理ユーティリティが含まれています。

セキュリティと ID

概要

このセクションでは、Catalyst 9000 プラットフォームに固有の新しいセキュリティ機能に焦点を当てます。以前の Catalyst スイッチ ファミリのセキュリティ機能は、Catalyst 9000 プラットフォームにも引き継がれています。

暗号化トラフィック分析

暗号化トラフィックの急増により脅威状況が変化しています。たとえば、2015 年から 2016 年の間に、暗号化されたトラフィックは、21 % から 40 % へと、約 2 倍に増加しています。ガートナーは、2019 年までに、全 Web トラフィックの 80 % が暗号化されると予測しています。攻撃者もこれを認識しており、暗号化を使用して検出を回避したり悪意のあるアクティビティを隠蔽したりすることで、この状況を自分たちに都合よく利用しています。

Catalyst 9000 シリーズが登場する前は、暗号化されたセッションの中に隠蔽された攻撃を検出するためには、面倒でコストのかかる対策が必要でした。簡単に言うと、暗号化フローの途中に、復号するためのハードウェアをインストールする必要があったのです。このようなシステムは、不要な遅延を招くため、ユーザ エクスペリエンスを損なうことになりかねません。また、企業にとっては、この手法を導入することで、新たな法的義務やプライバシーの問題が生じます。

シスコは、Catalyst 9000 スイッチに暗号化トラフィック分析 (ETA) 機能を備えることでこの問題を解決します。ETA は、パッシブ モニタリングによって、暗号化されたトラフィックに潜むマルウェア通信を特定します。追加の機器は不要で、非標準的なトラフィック リダイレクションを実行する必要もありません。ETA は、関連データ要素を抽出し、クラウドベースのグローバル セキュリティ データを含む機械学習手法を採用することで、マルウェア通信を特定します。

ETA は、実証済みのモニタリング技術である Flexible NetFlow (FNF) を起点として始まります。FNF は、Catalyst 9000 スイッチのローカルで動作し、Catalyst 9000 スイッチを通過するすべての会話（つまりフロー）をトラッキングします。これらのやり取りに関するさまざまな情報がフロー レコードに収集されます。レコードの一般的な値としては、送信元アドレスと宛先アドレス、ポート、バイト数などがあります。

ETA は、新しいフロー メタデータを導入することで、暗号化フロー内に潜む悪意あるアクティビティの識別を支援します。新しいメタデータとは、初期データ パケット (IDP) および、パケット長と時間のシーケンス (SPLT) です。

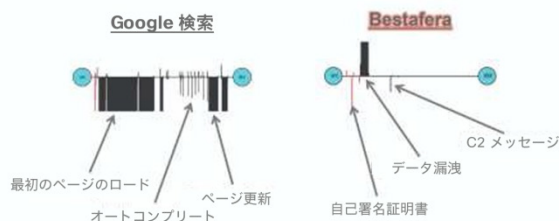
初期データ パケット (IDP)

初期データ パケット (IDP) は、2 つのホスト間で最初に交換されるパケットです。ETA の場合、IDP は、セキュア セッションを確立するためのハンドシェイク中に発生します。セッションが暗号化されていても、2 つのエンドポイント間で最初に交換される Transport Layer Security (TLS) は、平文で渡されます。ETA プロセスは TLS ハンドシェイクを確認して、使用されている TLS のバージョンや、暗号化セッションを伝送しているアプリケーションなどを学習し、その内容をレポートすることができます。これは、セキュリティ監査を実施する際に非常に役立つ情報となり得ます。

パケット長と時間のシーケンス (SPLT)

パケット長と時間のシーケンス (SPLT) とは、フロー内のパケットの長さとパケットの到着間隔を示すものです。長さはバイト単位、到着間隔はミリ秒単位で測定されます。SPLT によって、ETA は、暗号化されたフローについて初期パケット以外の情報も得られるようになります。ETA は、各フローの SPLT 測定値を、既知の悪意あるふるまいと比較して、攻撃を特定します。たとえば、次の図を例にして考えてみましょう。

図 通常のふるまいと悪意のあるふるまいの SPLT の比較



示されている 2 つのグラフは、一般的なブラウザでの Google 検索と Bestafera 攻撃の SPLT 測定値を比較したものです。Bestafera は、Windows マシンでトロイの木馬として動作するマルウェアです。どちらの例でも、送信元 (src) は、ユーザの PC です。宛先 (dst) は、Google 検索の例では Google 検索エンジンの 1 つであり、右側の例では、悪意のある攻撃者のマシンです。それぞれの送信元と宛先の間の線は、時間を表しています。タイムラインより上に伸びている縦線は、ユーザから Google またはハッカーに送信されたデータ量を示し、タイムラインより下の線は、ユーザの PC にダウンロードされたデータの量を示しています。

Google ページ検索での SPLT をトレースすることで、ユーザがサイトを参照した流れがわかります。ユーザが検索条件に入力すると、Google のオートコンプリート機能がトリガーされます。目的の検索文字列を選択すると、ページに検索結果がリロードされます。これに対して Bestafera のグラフでは、大きく異なっている点がいくつかあります。Bestafera のプログラムは、ユーザのマシンで実行されている間に、自身のコマンド & コントロールサーバに到達し、デジタル証明書をダウンロードします。マルウェアは、取得した証明書を使用して、暗号化されたチャネルをオープンし、被害者のセンシティブ データを抽出します。その後アイドル状態になり、定期的にコマンド & コントロール (C2) チャネルを使用してチェックインし、次の命令を確認します。

Cisco Cognitive Analytics

ETA は、Cisco Stealthwatch および、クラウドベースのサービスである Cisco Cognitive Analytics と連携し、ETA のメタデータに対して機械学習インテリジェンスを適用します。Cognitive は、IDP と SPLT のフロー データを前述のように処理し、結果をシスコの脅威インテリジェンス マップと比較します。脅威インテリジェンス マップは、シスコのセキュリティ調査部門である Cisco Talos によって世界中から収集されたセキュリティ データを Cognitive Analytics エンジンに提供します。Cognitive はデータを使用して、インターネット上の 1 億 5,000 万台におよぶ既知のエンドポイントまたはリスクのあるエンドポイント全体から 20 種類の特徴をモデル化します。最終的な結果として、特定のフローの悪意の有無に関し、より正確な評価が下されます。

暗号化コンプライアンス

ETA は、あらゆるネットワーク通信で使用される暗号化機能も特定します。また、TLS のバージョン、鍵交換手法、認証アルゴリズムなど、使用されているさまざまな暗号化パラメータについてレポートします。これによって、ネットワークで使用されている暗号化アルゴリズムとパラメータを明確に把握し、組織の暗号化ポリシーを検証することができます。

Catalyst 9000 スイッチでの ETA

Flexible NetFlow 情報をすべて収集できる Catalyst 9000 スイッチは、ETA をサポートするプラットフォームとして理想的です。データ収集は直接 UADP ASIC を使用してハードウェアで実施されるため、ネットワークのパフォーマンスは一切低下しません。さらに、Catalyst 9000 スイッチは、オンボードの x86 マルチコア CPU を活用して、IDP データと SPLT データを収集するために必要なオーバーヘッドの増加に対処します。

信頼できるシステム

ネットワーク インフラストラクチャはさまざまな攻撃を受けています。実行中のオペレーティング システムの欠陥がエクスプロイトされたり、不正なソフトウェアがインストールされたりすることで、ネットワーキング機器がハイジャックされる可能性があります。さらには、ハッカーが簡単に侵入できるように構築された偽造デバイスを、管理者がひそかに導入している可能性もあります。このような事態になると、そのネットワーク ノードは、個人の通信傍受、センシティブ データの漏洩、ホスト/サーバ/ネットワーク自体に対するその他の攻撃を犯罪者が行うための、起点にされてしまう可能性があります。シスコは、ネットワーク攻撃の防御を支援するために、信頼できるスイッチとして Catalyst 9000 シリーズを構築しました。

Cisco Trust Anchor

すべての Catalyst 9000 スイッチで、Cisco Trust Anchor (CTA) がローカルに導入されています。CTA は、特別に設計された改ざん防止チップで、デバイスに組み込まれている保護機能を強化するために使用されます。このチップが除去されると、スイッチは動作しません。CTA は、組み込みのセキュリティを強化するいくつかのテクノロジーを提供しています。

乱数ジェネレータ

乱数ジェネレータ (RNG) は暗号化に不可欠な機能です。CTA では、NIST 準拠 (NIST SP 800-90A および B 認定相当) の乱数ジェネレータを使用し、チップ自体の中にある完全にランダムなソースからエントロピーを抽出します。

セキュアな固有デバイス識別子

Catalyst 9000 スイッチには、セキュアな固有デバイス識別子 (SUDI) である X.509v3 証明書が設定されています。SUDI は製造時に生成されてインストールされ、公的に識別可能なルート証明書機関とつながっています。SUDI のフィールドには、スイッチの製品識別子とシリアル番号が含まれています。この 2 つのフィールドを含んでいることで、SUDI とスイッチが一意にバインドされるため、スイッチがシスコ純正のハードウェアであることを確認できます。

CTA は、SUDI 証明書と、関連する鍵ペア、証明書チェーン全体を保持します。さらに、各 SUDI の公開キー/秘密キーのペアが暗号化されて特定の CTA チップにバインドされます。その秘密キーは絶対にエクスポートされません。

セキュアなストレージ

上記に加え、Catalyst 9000 の CTA には、安全性の高いストレージ エリアが組み込まれています。暗号化鍵、パスワード、LSC、LDevID などの共通項目がここに置かれています。

Cisco Trust Anchor テクノロジー

Catalyst 9000 シリーズは、CTA のコア コンポーネントを基盤とすることで、ハードウェア認証、OS の整合性、セキュア ブート プロセスを実現しています。

純正ハードウェア チェック

ネットワーク モジュールまたはスーパーバイザはすべて、独自の CTA を持つことで、純正ハードウェアであることを証明します。モジュールが装着されると、特殊なライブラリを使用して、モジュールのローカル CTA が読み込まれ、純正であることが確認されます。このライブラリを使用すると、偽造モジュールをスイッチに導入することが不可能になります。

イメージの整合性

イメージの整合性の確保とは、ユーザが実行しようとしているコードが改ざんされたものではないとユーザに保証することを意味します。これは、ソフトウェア実行ファイルの信頼性を確立する上で重要なステップです。整合性確保プロセスには、ハッシュ アルゴリズムを利用して一意のデジタル署名を実行ファイルに生成することが含まれています。整合性チェックが正常に完了した場合、そのコードは有効で信頼できるものと保証されます。

セキュア ブート

Catalyst 9000 スイッチは、セキュア ブート プロセスを実行します。まず、セキュアな開始点である信頼源の確立から始まります。CTA が信頼源となり、有効なソフトウェアの信頼チェーンをブート サイクル中に確立するための基盤として使用されます。

ランタイム防御

信頼できるオペレーティング システムがロードされた後は、実行中のファームウェアを保護することが、スイッチの信頼性を確保するための最後のステップになります。Cisco IOS XE のランタイム防御は、さまざまな方法で拡張されています。

さまざまなコードやデータが読み込まれるメモリ内の空間をランダムに配置するために、アドレス空間配置のランダム化 (ASLR) テクノロジーが追加されました。これによって、攻撃プログラムは、コードの注入や秘密情報の窃取を行うためのジャンプ先を特定することができなくなります。

シスコは、Cisco IOS XE コードの構築に際して Safe C ライブラリを使用しました。シスコのソフトウェア エンジニアは、libc の代替となる Safe C ライブラリの中から、以下のようないくつかの機能を活用しました。

- 境界チェック メモリおよび文字列関数、オブジェクト サイズ チェック。
- 開発者がセキュリティ リスクを注入するのを防ぐための、コンパイル タイム超過警告。
- バッファ オーバーフローや整数オーバーフローを検出するランタイム チェックの挿入。
- 高度なカーネル保護手法。

MACsec

MACsec が開発された理由

ネットワークを害する意図を持った人物によって、直接接続された 2 台のネットワーク デバイス間に、TAP デバイスやレイヤ 1/2 デバイスを追加されてしまうことがあります。その場合にネットワーク管理者が、リンクの切断/再接続は認識しても、デバイスが追加されたことには気づかない可能性もあります。こうなると侵入者は、リンク経由で送信されるすべてのデータをリッスンし、そのデータを有害な目的に使用できるようになります。リンクへの一切の侵入を防ぐために、Media Access Control Security (MACsec) が開発されました。MACsec には、以下を防御できる利点があります。

- DoS 攻撃
- 中間者攻撃
- パッシブ通信傍受
- 反射攻撃
- マスカレード

図 回線上のデータを窃取する侵入者



Catalyst 9000 スイッチに実装された MACsec は、IEEE 802.1AE および 802.1X-2010 標準規格に完全に準拠し、OSI スタックのレイヤ 2 で動作します。レイヤ 2 導入は、ネットワーク パフォーマンスに影響を与えずに、リンクで転送されるほぼすべてのパケットを含むため、使用されました。

直接接続された 2 つのレイヤ 2 ピア間に MACsec セッションを確立するには、鍵のネゴシエーションが必要です。セッションを確立できる Session Key Exchange Protocol には、MACsec Key Agreement (MKA; MACsec 鍵合意) と Security Association Protocol (SAP; セキュリティ アソシエーション プロトコル) の 2 種類があります。

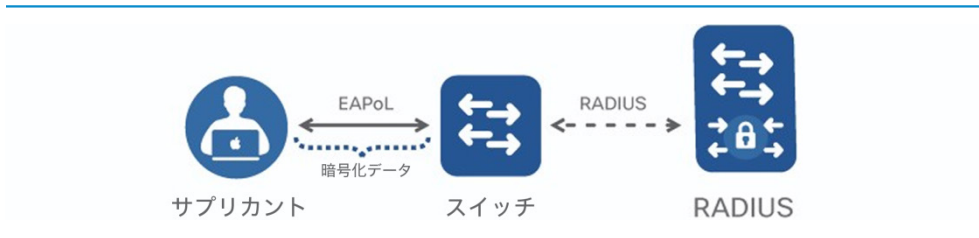
現在 MACsec は、スイッチ-スイッチ間、ユーザ/サーバ ホスト - スイッチ間、ルーター-スイッチ間で有効化され、データ保護を実現しています。

トポロジ

ホスト - スイッチ間：通常は前面パネル ポートを使用

ホストは、Cisco Anyconnect Client を実行し、ホスト上でソフトウェア暗号化/復号を行う必要があります。最新の Anyconnect は、AES 128 ビットまでの暗号化をサポートしています。

図 ホスト - スイッチ間の MACsec

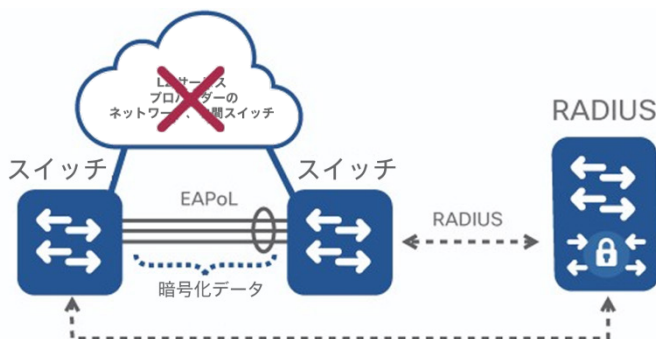


ホスト - スイッチ間のトポロジ

- 手動鍵交換には非対応。
- dot1X 鍵交換をサポート (ACS/ISE が必要。大規模向け)。
- ユーザ単位の認証/暗号化をサポート。

スイッチ - スイッチ間：通常は、ネットワーク モジュールのアップリンク ポートまたは Catalyst 9400 シャーシのスーパーバイザ アップリンクを使用

図 スイッチ - スイッチ間の MACsec



スイッチ - スイッチ間のトポロジ

- 手動鍵交換設定をサポート。
- RADIUS 経由での dot1X 鍵交換には非対応。
- dot1x サプリカントがすべてのスイッチで有効になっており、x.509 証明書が共有鍵の代わりに使用されている場合、MKA 向けに EAP-TLS をサポート。

対応プラットフォーム

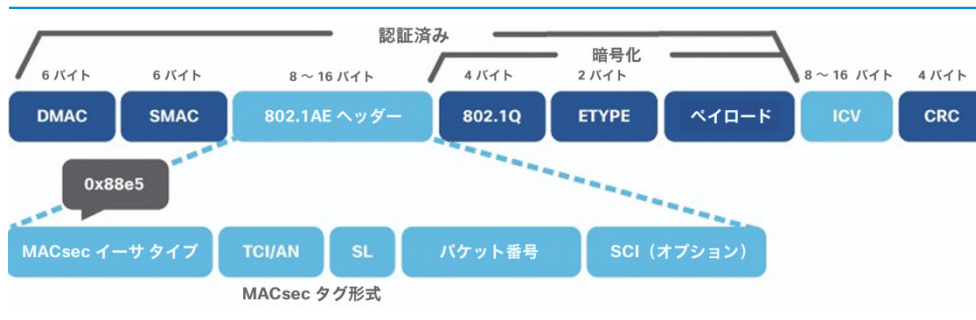
MACsec では、ライン レートでの暗号化/復号を実施するために、スイッチでのハードウェア サポートが必要となります。Catalyst 9000 ファミリは、UADP ASIC に統合ブロックを備えており、任意のスピードでライン レートの MACsec 暗号化/復号を実施できます。

表 各プラットフォームでの MACsec サポート

	MACSec	Cat 9300	Cat 9400	Cat 9500
スイッチ - スイッチ間	128 ビット SAP	ライン レート	HW 対応	ライン レート
	128 ビット MKA	ライン レート	HW 対応	ライン レート
	256 ビット MKA	ライン レート	HW 対応	ライン レート
ホスト - スイッチ間	128 ビット MKA	ライン レート	HW 対応	ライン レート
	256 ビット MKA	HW 対応	HW 対応	HW 対応

MACsec に対応するためにハードウェア サポートが必要とされる理由は、MACsec セッションの確立に使用される新しいパケット フレーム形式にあります。MACsec は、新しい形式のパケットを区別するために、新たな Ethertype (0x88e5) を使用します。

図 MACsec フレーム形式



- 認証：AE ヘッダーの 16 バイトのみを使用。
- 暗号化：AE ヘッダーの 16 バイトと ICV の 16 バイトを使用。
- IP MTU/フラグメンテーションには影響なし。
- 宛先および送信元 MAC の後のすべてのフィールドを暗号化（MPLS または dot1Q タグを含む）。

- dot1Q Cos や MPLS EXP マーキングには影響なし（復号後または暗号化前に使用されるため）。
- ライン レートの計算の際、追加されたパケット用オーバーヘッド ヘッダー フィールドを除外する必要がある。ポートのビット レートは変わらない（パケット サイズに依存しないため）。
- 「inner shim ヘッダー」は 20 バイトで、常に変わらない。
- 1 ポートあたりのライン レート = (パケット サイズ + inner shim ヘッダー) / (パケット サイズ + inner shim ヘッダー + **オーバーヘッド**) 。
- 認証および 1500 バイトのパケットの場合のライン レート : (1500 + 20) バイト / (1500 + 20 + 16) バイト = 帯域幅の 99 %。
- 暗号化および 1500 バイトのパケットの場合のライン レート : (1500 + 20) バイト / (1500 + 20 + 32) バイト = 帯域幅の 98 %。

QoS およびキューイング

概要

輻輳とは

輻輳とは、宛先ポートがパケットを転送することができず、その結果、送信されるいくつかのパケットにドロップまたは想定以上の遅延が発生する状況のことを言います。

輻輳に対応すべき理由

輻輳が発生すると、後続の着信パケットをハードウェア バッファで処理できない場合に、パケットがドロップされる可能性があります。パケットがドロップされた場合、クライアント アプリケーションによって再送を行う必要があります。多くのアプリケーションが再送を行うと、再送にも輻輳が発生して、輻輳解消までプロセスが続くため、ネットワークのパフォーマンスが実際に低下する可能性があります。

ハードウェア バッファを追加するだけでは、必ずしも輻輳の問題を軽減することはできません。遅延による影響が大きいトラフィックは、できるだけ早く宛先に転送する必要があるからです。

Catalyst 9000 での QoS および輻輳の管理

Catalyst 9000 スイッチでは、Modular QoS CLI (MQC) モデルを使用して、ポリサー、シェーパー、トラフィック再マーキングを設定します。

Modular QoS モデル

Catalyst 9000 スイッチでは、次の利点から、MQC モデルを採用しています。

- 一貫性のある QoS 設定モデルが実現する。
- ポリシー、クラス、タイプに基づいている。
- 2 レベルの階層型ポリシーをサポートしている。
- クラス、キュー、ポートまたは VLAN ごとにトラフィックを分類できる。
- クラスベースのポリシングとシェーピングをサポートしている。

Catalyst 9000 の Cisco [MQC](#) の詳細については、Cisco.com を参照してください。

QoS マーキング

QoS マーキングには、プロトコルの種類に応じて次の 3 つの標準タイプがあります。

- L2 COS/ユーザ優先度 - 3 ビット (0 ~ 7)
- MPLS EXP - 3 ビット (0 ~ 7)
- L3 DSCP、IPv4 用 ToS (IPv6 用トラフィック クラス) - 6 ビット (0 ~ 63)

[QoS マーキング](#)の詳細については、Cisco.com を参照してください。

バッファとキュー

UADP ASIC は、PBC 共有バッファ メモリを備えています。UADP 2.0 コアはそれぞれ、個別のバッファ メモリまたは分割されたバッファ メモリと内部のデータ パスを使用して、コア間でパケットを転送しています。UADP 3.0 では、2 コア間で新たな統合パケットバッファがサポートされています。ASIC のすべてのポートで単一のパケット バッファを利用できるため、メモリ アクセスが高速化し、バーストの吸収力が高まります。

表 バッファの大きさの情報

	UADP 2.0	UADP 2.0 XL	UADP 3.0
コアあたりのバッファ サイズ (MB)	8	16	36
ASIC あたりのバッファ サイズ (MB)	16	32	36

ハードウェア バッファの割り当て

従来、ハードウェア バッファは各キューに静的に割り当てられていました。しかしそれでは、バーストが発生した場合に、すべてのキューのバッファとしては不足する可能性があります。この問題を解決するため、Catalyst 9000 プラットフォームでは Dynamic Threshold Scaling (DTS; 動的なしきい値拡張) を採用しています。

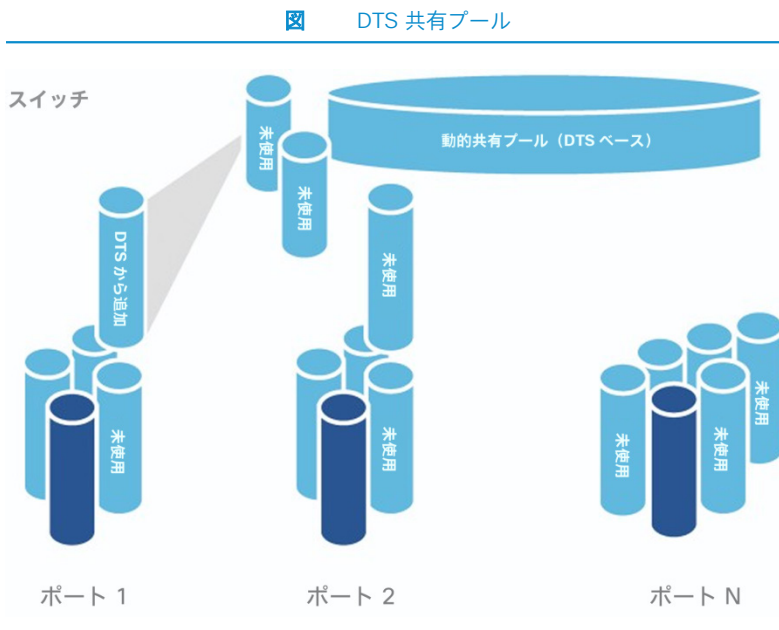
ハードウェア バッファは、下記の複数のセグメントに分割されます。

- 入力バッファ (11 %) : スタックおよび ASIC インターフェイスへの転送が予定されているバッファに使用されます。
- 出力スタック バッファ (25 %) : スタック ポートからトラフィックを受信する際に使用されます。
- バッファ サイズは、最大 8 スタック メンバーに対応できるように設定されています。

- 出力ポート バッファ（64 %）：最も大きいバッファで、ポート キュー構造に使用されます。
 - これらのバッファは、DTS を使用してさまざまなキューやポート間で共有できます。

DTS 共有プール

DTS では、未使用バッファから成る動的共有プールが作成されます。共有プールのバッファは、バーストや輻輳のためバッファ領域を増やす必要のあるポートに、動的に割り当てられます。



DTS には以下のような機能があります。

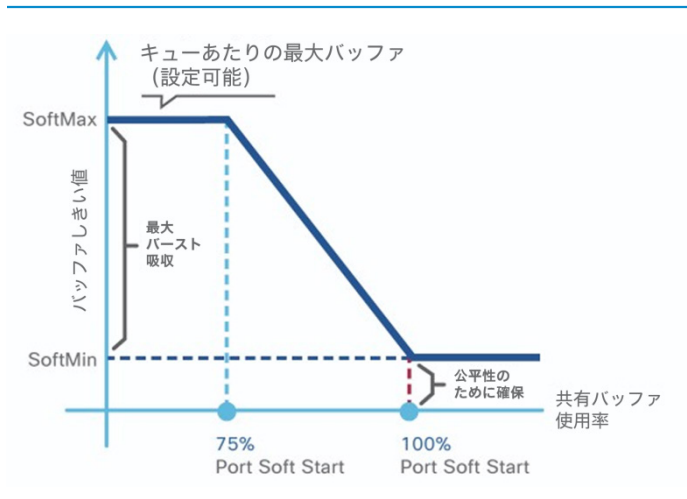
- バッファは、ポートごとに、専用（ハード）カテゴリと共有（ソフト）カテゴリに分割されます。
 - 共有バッファは、パケット バーストの吸収に適しています。
 - 専用バッファは、安定したパフォーマンスの実現に貢献します。
- 専用バッファが最初に使用され、次に共有バッファが使用されます。
 - 共有バッファの管理には Dynamic Threshold Algorithm (DTA; 動的しきい値変更アルゴリズム) が使用されます。
- バッファ サイズの割り当ては、（専用バッファと共有バッファ間で）柔軟に変更可能です。
 - 専用バッファのしきい値は、ポート/キューごとに設定可能です。
 - 共有バッファのしきい値は、グローバルな最大値として設定可能です。
 - 共有プールは、DTS アルゴリズムによって自動的に調整されます。

DTS パラメータ

DTS の調整には次のパラメータを使用します。

- SoftMin : ポートごとに割り当てられる共有バッファ領域の最小値
- SoftMax : ポートが共有プールから利用できる共有バッファの最大値
- Port Soft Start : SoftMax が減少し始めるタイミング
- Port Soft End : SoftMin と SoftMax が一致するタイミング

図 DTS パラメータの仕組み



DTS バッファ設定の詳細については、Cisco.com を参照してください。

ハードウェア キュー

Catalyst 9000 シリーズは、デフォルトで 2 キュー構造を実装しています。この 2 キュー構造は、DSCP 16、24、32、48、56 に対応する絶対プライオリティキューと、すべての DSCP 値に対応する通常キューから成っています。

ユーザは、ハードウェアのキューイングを、最大 8 つまで再設定できます。また、キューごとに 3 つのしきい値を設定可能です。2 つのキューを使用してキューイングの優先順位を差別化することができます。Catalyst 9000 のポートごとに独自の出力キューイング ポリシーを設定可能です。Catalyst 9000 スイッチは、Weighted Round Robin (WRR; 加重ラウンドロビン) を使用して、送信キューからトラフィックを出力するスケジュールを決定します。

輻輳管理

Catalyst 9000 シリーズでは、キューイング プロセスに Weighted Random Early Discard (WRED; 加重ランダム早期廃棄) アルゴリズムが追加されています。WRED は、輻輳時における高優先度トラフィックのドロップによる影響を最小限に抑えるのに役立ちます。どのポートでも、最大 4 つのキューで WRED を使用できます。

注 WRED はプライオリティ キューでは使用できません。

UADP ASIC における QoS およびキューイング

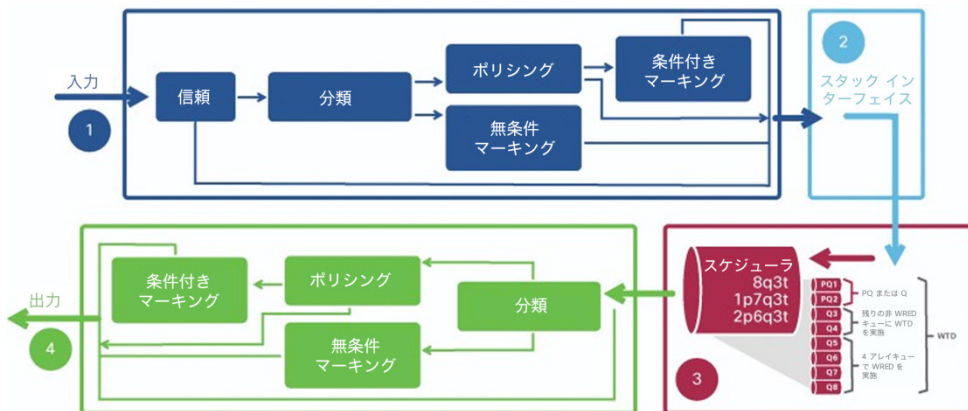
このセクションでは、パケットが UADP を通過する際に、さまざまな QoS およびキューイングのプロセスがパケットに適用される仕組みについて説明します。

QoS のパケット フローには、大きく分けて以下の 4 つのパートがあります。

- 1 入力分類、ポリシング、マーキング
- 2 スタック インターフェイスに対するキューイング
- 3 出力キューイングおよびスケジューリング
- 4 出力分類、ポリシング、マーキング

次の図は、これら 4 つのパートを表したものです。このセクションでは、この図に続けて、各ステップの詳細を説明します。

図 UADP ASIC における QoS およびキューイングのパケット フロー



入力分類、ポリシング、マーキング

このサブセクションでは、上記 QoS およびパケット キューイングのパケット フロー図の最初の処理ブロックについて説明します。

QoS 処理は、ポートがパケットを受信してそのマーキングをチェックするところから始まります。入力パケットのマーカは、デフォルトで信頼されます。デフォルトで信頼することが望ましくない場合は、UADP でパケットを分類してライン レートでポリシーまたは再マーキングを適用することができます。

デフォルトの信頼動作およびキューイング動作を次の表にまとめます。

表 デフォルトの信頼動作およびキューイング動作

着信 パケット	発信 パケット	信頼動作	キューイング動作
レイヤ 3	レイヤ 3	DSCP/優先度を保持	DSCP に基づく
レイヤ 2	レイヤ 2	対象外	CoS に基づく
タグ付き	タグ付き	DSCP および CoS を保持	DSCP に基づく (信頼 DSCP が優先)
レイヤ 3	タグ付き	DSCP を保持、CoS は 0 に設定	DSCP に基づく

Catalyst 9000 ファミリ スイッチは、次のタイプに基づいてトラフィックを分類します。その際、論理コンストラクト (AND または OR) を使用して複数の分類パラメータを設定することができます。

- ACL
- DSCP
- IP 優先順位
- COS
- EXP
- TCP/UDP ポート

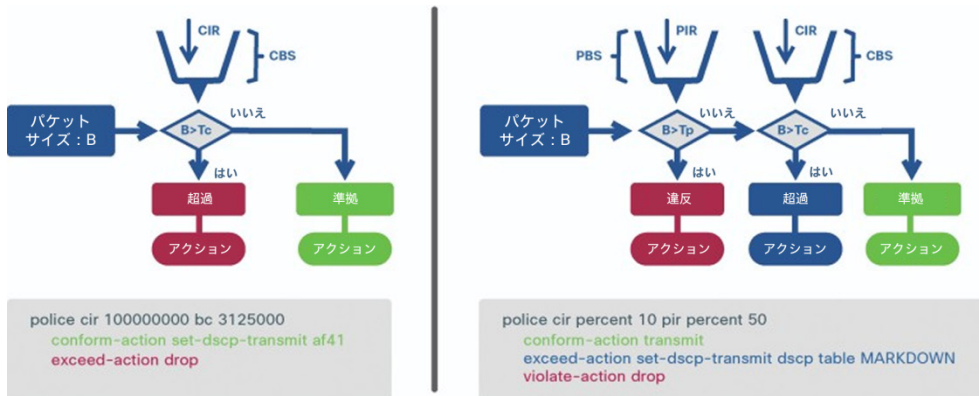
- NBAR プロトコル
- VLAN 単位

ポリサーとバースト レート

Rate と Burst は、ポリシング設定において暗黙的に使用される、重要な 2 つのパラメータです。1 レート 2 カラーのポリサーでは、レート（別称「設定情報レート（CIR）」）は、所定の間隔で転送できる最大データ量として定義されます。バーストは、CIR に対する超過可能性を表します。2 レート 3 カラーのポリサーでは、最大情報レート（PIR）も指定できます。PIR とは、CIR を超えても許可される上限レートです。最大バーストは、超過可能な PIR 量を表します。

Catalyst 9000 シリーズでは、1R2C と 2R3C の両方のポリサーをサポートしています。

図 Catalyst 9000 ポリサー タイプ



UADP ASIC インターコネクト キューイング

このサブセクションでは、上記 QoS およびパケット キューイングのパケット フロー図の 2 番目の処理ブロックについて説明します。

UADP ASIC インターコネクトは、複数の UADP ASIC 間のポイントツーポイント接続です。同じスイッチ上で接続される場合と、別のスイッチにつながるスタック ケーブルと接続される場合があります。入力キューイング スケジューラ (IQS) は、輻輳を管理し、他の UADP ASIC 宛てのパケットのスケジューリングおよびキューイングを実施します。優先ラベルを付与されたパケットが、最初に ASIC インターコネクトでキューイングされます。

出力キューイングおよびスケジューリング

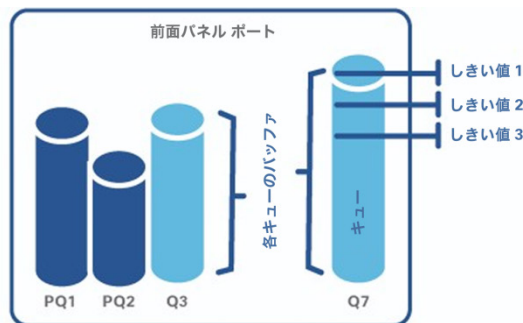
このサブセクションでは、上記 QoS およびパケット キューイングのパケット フロー図の 3 番目の処理ブロックについて説明します。

前述のように、スケジューラは EQS ブロックの一機能であり、複数のポート キュー、キューに割り当てられるしきい値、およびバッファを提供します。

ポート キュー

Catalyst 9000 スイッチの各ポートは、最大 8 つの出力キューに対応しており、その内 2 つをプライオリティ キューとして設定できます。Weighted Round Robin (WRR; 加重ラウンドロビン) 技術を使用して、割り当てられた重み付けに応じて送信キューを空にします。Catalyst 9000 は、前のセクションで説明したように、DTS および WRED をそれぞれ使用して、バッファと輻輳を管理します。

図 ポート キューイング パラメータ



キュー バッファ

各キューは、送信データを保管するために一定量のバッファ（メモリ）スペースを使用する必要があります。キューの深度が大きいほど保持できるトラフィックも多くなります。バッファを使用すると、送信されるパケットがキューイングされるため、遅延が発生します。

キューのしきい値

しきい値とは、スイッチ ポートによって設定される任意の内部レベルであり、輻輳管理アルゴリズムによるデータのドロップの開始ポイントになるキュー使用率を定義するものです。しきい値到達時にドロップ対象となるべきデータは、パケットの優先度に応じて決まります。各しきい値にトラフィックを割り当てるには、DSCP または COS が使用されます。このようにして輻輳管理アルゴリズムは、しきい値超過時に、どの優先度を持つどのパケットがドロップ対象になるのかを即座に認識します。Catalyst 9000 ポートの各キューには、3 つのしきい値を設定できます。

シェーパー

シェーパーは通常、送信元のデータ レートが想定より高い場合に、バッファまたはキューイング メカニズムを使用して過剰なトラフィックを遅延させることで、パケットを保持してフローをシェーピングします。一方ポリサーは、シェーパーがまずトラフィックをバッファしようとするのとは対照的に、トラフィックをすぐにドロップします。シェーパーは、Catalyst 9000 のハードウェア キューで適用されます。

出力分類、ポリシング、マーキング

このサブセクションでは、上記 QoS およびパケット キューイングのパケット フロー図の 4 番目の処理ブロックについて説明します。

出力分類、ポリシング、マーキングは、1 つの重要な違いを除いて、大部分が入力処理とまったく同じです。その違いとは、ヘッダーの QoS マーカーが入力バスによって変更されていない場合に限って元のヘッダーを使用でき、変更されている場合は入力マーキングが使用されるという点です。

階層型 QoS

階層型 QoS (HQoS) では 2 つのポリシー レベルを設定することができます。これにより、さらに細かいポリシー設定が可能になります。階層型ポリシーは、上位レベルの親ポリシーと下位レベルの子ポリシーから成る構造とみなすことができます。管理者は、HQoS を使用して以下のことを実行できます。

- 子ポリシーの複数のキューを親クラスによってシェーピングする。
- 集約トラフィックに特定のポリシー マップ アクションを適用する。
- クラス固有のポリシー マップ アクションを適用する。

Catalyst 9000 スイッチの主な利点の 1 つに、ハードウェアでの HQoS のサポートがあります。

Catalyst 9000 では、以下の 4 つの HQoS を組み合わせることができます。

- 1 ポート シェーパー
- 2 集約ポリサー
- 3 ポート単位/VLAN 単位のポリシー
- 4 シェーパーを使用する親ポリシー

ポート シェーパー

HQoS ポート シェーパーは、class-default クラスを使用して、すべての出力トラフィックにシェーパーを適用します。シェーピングされたこの帯域幅内で子ポリシーを追加することが可能です。

次の CLI は、HQoS ポートシェーパの設定例を示しています。

```
policy-map PARENT
  class class-default
    shape average percent 10
    service-policy CHILD

policy-map CHILD
  class VOICE
    priority level 1
    police rate percent 20
  class C1
    bandwidth remaining percent 10
  class C2
    bandwidth remaining percent 20
  class C3
    bandwidth remaining percent 70
```

HQoS ポートシェーパに関する注意

- 親ポリシーで使用できるのは「class-default」クラスのみ。
- 子ポリシーに設定できるプライオリティキューは2つまで。
- 子ポリシー内のクラスごとに帯域幅を変えることが可能。

集約ポリサー

HQoS 集約ポリサーは、class-default クラスを使用して、すべての出力トラフィックにポリシーを適用します。ポリシングされたこの帯域幅内で子ポリシーを追加することが可能です。

次の CLI は、HQoS 集約ポリサーの設定例を示しています。

```
policy-map PARENT
  class class-default
    police cir percent 30
    service-policy CHILD
```

```

policy-map CHILD
  class C1
    set dscp 10
  class C2
    set dscp 20
  class C3
    set dscp 30

```

HQoS 集約ポリサーに関する注意

子ポリシーでのアクション セットとして table-map を使用できます。

ポート単位/VLAN 単位のポリシー

複数の親 HQoS ポリサーが適用され、それぞれのポリサーは、分類基準としての VLAN に一致します。個別にポリシングされた各 VLAN の帯域幅内で子ポリシーを追加することが可能です。

次の CLI は、HQoS のポート単位/VLAN 単位の設定例を示しています。

```

policy-map PARENT
  class vlan10
    police rate percent 10
    service-policy CHILD
  class vlan20
    police rate percent 20
    service-policy CHILD
  class vlan30
    police rate percent 30
    service-policy CHILD

policy-map CHILD
  class C1
    set dscp 10

```

HQoS ポート単位/VLAN 単位ポリシーに関する注意

- 子ポリシーでのアクション セットとして table-map を使用できます。
- 親ポリシーの下に複数のクラスを設定できます。
- VLAN 単位の分類の代わりにシェーピングを使用できます。

親ポリシーでのシェーパの使用

親ポリシーの下で複数の HQoS シェーパが適用され、それぞれのシェーパはトラフィック クラスに一致します。個別にシェーピングされた帯域幅内で子ポリシーを追加することが可能です。

次の CLI は、HQoS 親ポリシーでのシェーパ使用の設定例を示しています。

```
policy-map PARENT
  class C1
    shape average percent 10
    service-policy CHILD
  class C3
    shape average percent 20
    service-policy CHILD
  class class-default
    shape average percent 30
    service-policy CHILD

policy-map CHILD
  class C1
    police rate percent 10
    set dscp 10
```

HQoS 親ポリシーでのシェーパ使用に関する注意

子ポリシーでのアクション セットとして table-map を使用できます。

Stackwise Virtual の QoS

Stackwise Virtual を実行する Catalyst 9000 シリーズ スイッチは、スタンドアロン スイッチと同じルールに準拠しています。ただし、Stackwise Virtual Link (SVL) を形成するために使用する特別なポートは例外です。SVL は、内部システム リンクとして扱われます。そのため、SVL の設定、運用モード、復元力、Quality of Service (QoS)、ロードシェアリングは、すべて特別なルール セットに従います。SVL ポートの QoS およびキューイングメカニズムは、ハードコードされています。SVL ポートでは、カスタムの QoS またはキューイング ポリシーは適用されません。

SVL に適用されるデフォルト ポリシーを次の図に示します。

Stackwise Virtual Link の QoS



[Stackwise Virtual の QoS](#) の詳細については、Cisco.com を参照してください。

オーバーレイ テクノロジーの QoS

最新のスイッチング ネットワークは、仮想ネットワーク オーバーレイを使用して、大規模なモビリティ、セグメンテーション、プログラマビリティに対応しています。オーバーレイは、SD-Access を実現する重要な要素です。

GRE および VXLAN の QoS

GRE および VXLAN は、元の IP パケット/フレームの外側に IP パケット ヘッダーを付けてカプセル化するオーバーレイ テクノロジーです。その際、元のペイロードは変更されません。

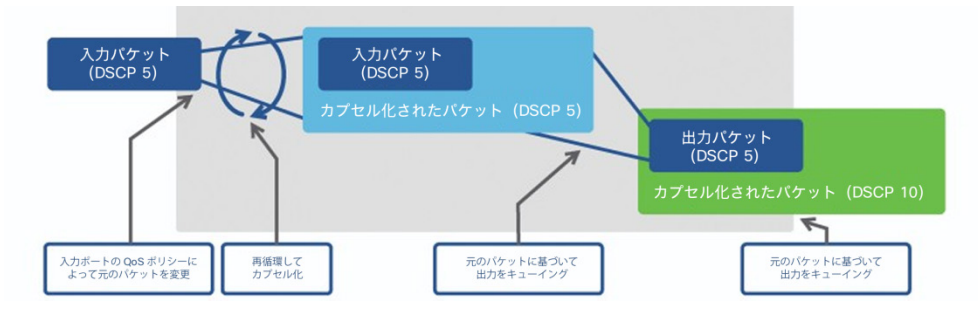
UADP ASIC での GRE および VXLAN カプセル化

GRE によるカプセル化では、元の IP パケットに新しい IP アドレスおよび GRE ヘッダーが付けられてカプセル化され、内側の IP ヘッダーの ToS バイト値が外側の IP ヘッダーにコピーされます。GRE インターフェイスでは、入力トラフィックに対する QoS ポリシーはサポートされていません。

VXLAN によるカプセル化では、元の L2 フレームに新しい IP アドレスおよび VXLAN ヘッダーが付けられてカプセル化され、元の L2 フレームの一部である内側の IP ヘッダーの ToS バイト値が、外側の IP ヘッダーにコピーされます。

出力キューイングは、（コピーされた）元のヘッダーの値に基づいて実施されます。

図 GRE/VXLAN オーバーレイ カプセル化の QoS マーキング



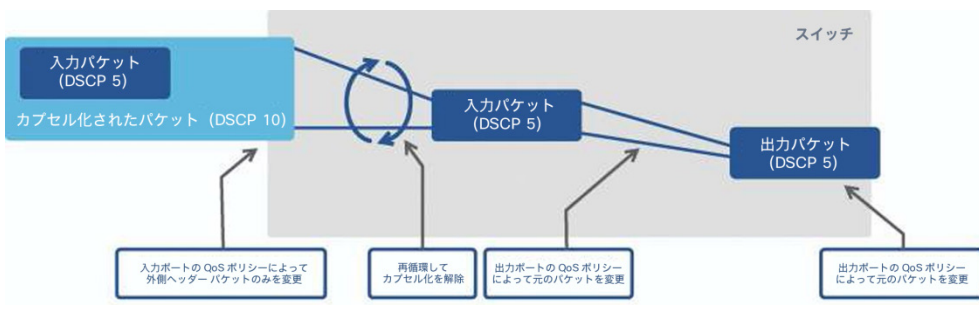
注 キューイングアクションは、出力ポリシングアクション/マーキングアクションに先立って適用されます。UADP における出力 QoS 動作の詳細については、前のセクションを参照してください。

UADP ASIC での GRE および VXLAN カプセル化の解除

どちらのケースでも、（カプセル化されたパケットを受信した）入力インターフェイスに QoS ポリシーが適用される際には、外側のヘッダーのみが分類に使用され、QoS は外側のヘッダーにのみ適用されます。内側のパケットは変更されず、元のマーキングがそのまま残ります。実際の GRE/VXLAN トンネル インターフェイスでは、出力トラフィックに対する QoS ポリシーはサポートされていません。

（カプセル化を解除された元のパケットを送り出す）出力インターフェイスに QoS ポリシーが適用される際には、元のパケットに QoS ポリシーが適用されます。

図 GRE/VXLAN オーバーレイ カプセル化解除の QoS マーキング



GRE オーバーレイでの QoS (RFC 2784) の詳細については、cisco.com を参照してください。

VXLAN オーバーレイでの QoS (RFC 7348) の詳細については、cisco.com を参照してください。

MPLS QoS

MPLS オーバーレイでは、QoS 処理用に、MPLS ヘッダー内の MPLS Experimental ビット (EXP) フィールドが使用されます。IP ネットワークにおいては、DSCP (6 ビット フィールド) によってクラスとドロップの優先度が定義されます。EXP ビットは、IP DSCP でエンコードされた情報の一部を伝達するためにも、ドロップの優先度をエンコードするためにも使用できます。

デフォルトでは、Cisco IOS XE によって、DSCP の最上位 3 ビット、または IP パケットの ToS フィールドが、MPLS ヘッダーの EXP フィールドにコピーされます。ただし、DSCP または ToS と EXP ビット間のマッピングを定義することで EXP フィールドを設定することもできます。

DSCP または ToS を EXP にマッピングするために使用できるモードは 3 つあります。

- Uniform モード（デフォルト）：QoS は 1 階層のみ。エンドツーエンド。

入力 PE ルータによって、着信 IP パケットの DSCP が、インポーズされたラベルの MPLS EXP ビットにコピーされます。EXP ビットは、コアを通過する際に、中間の P ルータで変更される場合と変更されない場合があります。変更される場合、新しい EXP 値が IP パケットの DSCP ビットにコピーされます。

- Full Pipe モード：2 階層の QoS を使用。1 階層目はデータに対する基盤的な QoS で、ASIC コアを通過しても変わりません。2 階層目はホップごとの QoS で、外側のヘッダーに適用され、基盤的 IP パケットとは分離しています。

IP パケットが MPLS ネットワークのエッジに到達すると、削除された MPLS ラベルの EXP ビットに基づいて、出力 PE ルータが、アウトバウンド キューイング用の新規公開 IP パケットを分類します。内側の IP パケットの DSCP ビットは変更されません。

MPLS QoS の各モードの概要を以下に示します。

表 MPLS QoS のモード

トンネリング モード	IP からラベルへ	ラベルから ラベルへ	ラベルから IP へ
Uniform	ToS/DSCP を MPLS EXP にコ ピーする (SP に よって変更される 場合もあり)		MPLS EXP が IP ToS/DSCP にコピーさ れる
Pipe		MPLS EXP が SP QoS ポリシーに よって変更される 場合あり	元の ToS/DSCP が保持 される (出力キューイングは MPLS EXP に基づく)
Short-Pipe (注 : Catalyst 9000 では サポートされていま せん)	MPLS EXP が SP QoS ポリシーに よって設定される		元の ToS/DSCP が保持 される (出力キューイングは ToS/DSCP に基づく)

[MPLS QoS \(RFC 5462\)](#) の詳細については、[cisco.com](#) を参照してください。

アプリケーションの可視 性およびコントロール

概要

ネットワーク エンジニアは、エンドツーエンドでビジネスに対応するポリシーを適用して、目標とするパフォーマンスを達成することを求められています。それに加えて、アプリケーション パフォーマンスの問題を迅速に切り分けて解決することも要求されます。ネットワークで実行されているさまざまなタイプのアプリケーションを詳細に監視し、ビジネス関連トラフィックのパフォーマンスを最適化することが、ネットワーク エンジニアには必要です。

Cisco Catalyst 9000 スイッチは、Application Visibility and Control (AVC) ソリューションをサポートしています。AVC は、エンタープライズ ネットワークにおけるビジネスクリティカルなアプリケーションに対して、真に革新的で強力なアプリケーション認識機能を提供するツールです。Cisco AVC ソリューションは、さまざまな技術を活用して、1,400 を超えるアプリケーションの認識、分析、制御を実現します。対象となるアプリケーションには、音声およびビデオ、電子メール、ファイル共有、ゲーム、ピアツーピア (P2P)、クラウドベース アプリケーションなどがあります。

Cisco AVC には、主に次の 3 つの機能があります。

- レイヤ 4 を超えるネットワークにおいてアプリケーションをきめ細かく検出するための認識機能
- ビジネスとの関連性に応じてトラフィックに優先順位付けする機能
- 特にビジネス関連のトラフィックに関して、アプリケーション帯域幅に優先順位を設定することにより制御を行う機能

アプリケーションの認識

AVC では、次世代の Network-Based Application Recognition 2 (NBAR2) を使用してアプリケーションを識別します。

NBAR2

NBAR2 は、ネイティブのステートフル ディープ パケット インスペクション (DPI) 機能を備えており、アプリケーション認識エンジンを強化して、1,400 を超えるアプリケーション (140 の暗号化アプリケーションを含む) に対応します。

NBAR2 には、以下のような強力な機能が備わっています。

- アプリケーション分類機能 (カテゴリ、サブカテゴリ、アプリケーション グループ など)
- HTTP URL、SIP ドメイン、メール サーバなどのデータのフィールド抽出機能
- ポート、ペイロード値、HTTP URL/ホストに基づいてアプリケーションの定義をカスタマイズする機能
- プロトコルごとに属性をカスタマイズできる機能

AVC は、スタンドアロンとスタック構成の両方のスイッチの有線アクセス ポートに設定できます。Catalyst 9000 スイッチでは、パフォーマンスを重視して最適化された NBAR2 が使用されています。アプリケーション識別に必要なパケットが少なくすむため、スイッチの CPU に対する影響が軽減されています。Catalyst 9300 スタックでは、NBAR2 検出が各スタック メンバーで実行され、メンバーを追加することにソリューションが拡張します。

NBAR2 は、プロトコル検出を有効にすることで、インターフェイスでのアプリケーション可視性に対して明示的にアクティブになります。また、一致プロトコル分類基準を含む QoS ポリシーを付与することで、アプリケーション ポリシーに対してアクティブになります。

アプリケーションのモニタリング

CLI または WebUI を使用してアプリケーションをモニタリングすることができます。

- 1 CLI では、長期間の累積統計情報が得られます。
 - CLI コマンド : `show ip nbar protocol-discovery top-n`
- 2 Catalyst 9000 スイッチの WebUI では、最大で直近 48 時間における 5 分ごとの統計情報が得られます。

 Catalyst 9000 の WebUI



- 3 Flexible Netflow を利用した AVC モニタリング。

Flexible NetFlow (FNF) をインターフェイスに設定することで、インターフェイスに関するアプリケーション統計情報を取得できます。AVC ソリューションは、NetFlow v9 および IPFIX と互換性があります。FNF では、特定の要件に応じてトラフィック分析のパラメータをカスタマイズできます。

Catalyst 9000 スイッチでの FNF データ収集は、UADP ASIC を搭載したハードウェアで実行されます。Catalyst 9300 スタック スイッチでの FNF データ収集は、スタックの各メンバーで実行され、メンバーを追加することにソリューションが拡張します。

アプリケーション制御

シスコの Quality of Service (QoS) には、AVC 内の制御部分で使用されるトラフィックのレート制限、優先順位付け、シェーピングの機能があります。

QoS では、指定されたアプリケーションを特定の QoS クラス/キューに配置することができます。それによって、次のことが可能になります。

- 遅延の影響が大きく優先度の高いトラフィックを、プライオリティ キューに配置する。
- QoS トラフィック クラス内の単体アプリケーションまたはアプリケーション グループに対して最低限の帯域幅を保証する。

QoS は、ネットワーク トラフィックを管理する際に、NBAR2 から得られるアプリケーション情報を使用できます。QoS の class-map ステートメントによって、NBAR2 対応アプリケーションや L7 アプリケーション フィールド (HTTP URL、ホストなど)、および NBAR2 属性へのマッチングが可能になります。Class-map ステートメントは、IP、サブネット、DSCP など、その他すべての一般的な QoS マッチ属性と併用することができます。

Catalyst 9000 スイッチでの QoS 適用は、UADP ASIC を搭載したハードウェアで実行されます。

IoT

概要

Internet of Things (IoT) は、業界で最も急速に拡大しているトレンドの 1 つです。IoT によって、Power over Ethernet (PoE) などの既存のテクノロジーにおける重要な革新や、Audio Video Bridging (AVB) 、Bonjour 向け Cisco DNA サービス、アプリケーション ホスティングなどの新たな技術やソリューションが推進されています。アプリケーション ホスティングについては、別途、専用のセクションで説明します。

IoT の詳細については、www.cisco.com/go/iot を参照してください。

Power over Ethernet のイノベーション

現在、Power over Ethernet (PoE) は、ネットワーク導入環境のいたるところで使用されています。PoE は、多くの最新ネットワーク環境において基盤技術の役割を果たし、IP フォン、アクセス ポイント、IP カメラなどのデバイスの利用を可能にしています。PoE は、イーサネット接続ケーブルを通してデータを送信するだけでなく、デバイスを稼働させる電力も供給します。PoE 対応デバイスに電力供給する屋内コンセントを個別に設ける必要はなく、電源ケーブルや配線のための追加コストが不要になります。

シスコが初めて独自のインライン パワー (ILP) を実装したときの PoE の最大電力は 7 W が限度でしたが、現在では、PoE は、IEEE 802.3af (一般に「PoE」と呼ばれ、最大 15.4 W をサポート) および IEEE 802.3at (「PoE+」と呼ばれ、最大 30 W をサポート) として標準化されています。利用できる総 PoE 電力の増加および PoE アプローチの標準化によって、PoE 受電デバイスを利用した大規模で活発なエコシステムが急増しています。

今日、PoE 電力は、規模の大小を問わず、あらゆるエンタープライズ ネットワーク環境で一般的に使用されています。PoE によって、デバイスの接続や利用が便利になるとともに、受電デバイス インフラストラクチャの復元力が増えています。たとえば、中央のワイヤリング クローゼットにある 1 台の UPS バックアップ電源によって、すべてのダウンストリーム受電デバイスの中断を抑止できるようになりました。

Catalyst 9300/9400 スイッチは、PoE と PoE+ のいずれもサポートしています。使用中の電源の容量と密度に応じて、すべてのポートまたは一部のポートで PoE/PoE+ 電力を使用できます。Catalyst 9300 プラットフォームにおける StackPower でのシスコのイノベーションによって、複数のスタッカブル スイッチで PoE 電力を共有することも可能になります。これは、ネットワーク上の受電デバイス数および高可用性の面で大きなメリットとなります。

PoE の現在の発展形 - UPoE

シスコは創業以来、PoE のパイオニアとして、標準規格の進歩を促進し、PoE イノベーションを次の段階に進めるための土台作りに取り組んできました。受電デバイスに必要とされる電力が、802.3at で定義された最大値 30 W を超えてきたことに合わせ、シスコでは、UPoE (Universal PoE) の定義と導入を主導的に進めています。UPoE は最大 60 W の PoE 電力を供給します。UPoE はシスコ独自のソリューションですが、PoE 電力をより多く必要とする受電デバイス (仮想デスクトップ端末、IP タレット、コンパクト スイッチ、ビル管理用ゲートウェイ、LED 照明、ワイヤレス アクセス ポイント、IP フォンなど) にとって、非常に有効なイノベーションです。

Catalyst 9300 スイッチおよび 9400 スイッチのライン カード モデルのどちらにも、UPoE 電源オプションのサポートが用意されています。シスコは、PoE、PoE+、UPoE 電源オプションを、1 G 銅線スイッチ ポートだけでなく mGig ポートでも提供し、高スループット/高レベル PoE 電力を必要とするデバイスの要求にえています。

PoE の詳細については、www.cisco.com/go/poe を参照してください。

注 Catalyst 9300 スイッチおよび Catalyst 9400 スイッチの PoE ハードウェアは、802.3bt に対応しています。

新たなイノベーション - Fast PoE と無停止型 PoE

PoE の利用が増えるのにつれて、使用例も多様化しています。より革新的な新しい PoE の利用方法の 1 つに、ビルの照明器具への電力供給があります。たとえば、商業用および工業用照明の単一の電源として PoE+ または UPoE ポートが使用されています。

照明器具の電源として、従来の方法に変えて PoE を利用する理由は何でしょうか。

- 電力消費の少ない照明器具は、60 W の UPoE 電力を使用するほうが、従来の照明システムの場合より効率よく機能する。
- PoE 電力は、従来の高価な電気配線よりもコストの低い Cat5e/6/6a ケーブルを使用して供給できる。
- PoE による DC 電力では、AC 電力に比べて、多くの新しい電気器具を、より効率的に使用できる。

これ以外の PoE 使用例として、ビル システム内の IoT デバイスへの電力供給などがあります。たとえば、ビル制御、サーモスタット、HVAC 制御システム、ドア ロック、バッジリーダーや、ビルのインフラストラクチャに欠かせないその他多くの同様の機器に、電力が供給されています。

シスコは、これらのビジネス クリティカルな導入をサポートするために、Fast PoE と無停止型 PoE という 2 つの新しい PoE 導入モードを生み出しました。

Fast PoE は、スイッチの起動プロセス中に PoE 電力を迅速に供給することを目的としています。Cisco IOS XE コントロール プレーンがすべてロードされるのを待たず、スイッチ電源投入から 30 秒以内に接続デバイスに PoE 電力を供給することを目指します。停電発生後、スイッチのリロードがすべて完了するまで数分待つのではなく、IoT などのデバイスをできるだけ早くオンラインにするためには、Fast PoE の機能が特に重要です。

無停止型 PoE の目的もこれと似ていますが、若干異なります。無停止型 PoE の目的は、Cisco IOS XE のコントロール プレーンがリロード中であっても、ダウンストリーム デバイスに対する PoE 電力の供給を続け、接続デバイスの電力を継続して確保することにあります。たとえば、（ソフトウェア アップグレード中など）スイッチのリロードが予定されている場合、リロード サイクル中に照明器具など重要な接続デバイスの電源がダウンするのは、望ましいことではありません。

AVB - オーディオ ビデオ ブリッジング

これまで、オーディオおよびビデオ（AV）の実装や導入は、アナログのポイントツーポイントのインフラストラクチャに依存してきました。AV がデジタル伝送に移行しても、これらのインフラストラクチャの性質がポイントツーポイントであるという点は、ほとんど変わっていません。従来、この導入モデルは非常に複雑でコストもかかり、運用上の大きな課題となっていました。これらのデジタル化問題に対して提案されたソリューションの多くは、標準化されておらず、高価で、運用上の負担も大きなものでした。

イーサネットは、デジタル AV データ交換のための柔軟かつ安価な共通媒体を実現できる AV 実装の新方法として、広く認識されていました。しかし、イーサネットの設計は、低遅延、安定性、無損失というデジタル AV の要件に対応したものではありませんでした。

そんな中、オーディオ ビデオ ブリッジング（AVB）標準規格セットが生まれました。AVB 標準規格は、主に次の領域から構成されています。

- **IEEE 802.1Qat** : Stream Reservation Protocol (SRP) /Multiple Stream Reservation Protocol (MSRP) 。AV ストリームの伝送に必要なエンドツーエンドのアドミッション コントロール システムを提供することで、帯域幅や遅延などのリソースの可用性を確保します。
- **IEEE 802.1Qav** : Forwarding and Queuing for Time-Sensitive Streams (FQTSS) 。AV トラフィックのスケジューリング メカニズムを提供します。
- **IEEE 802.1AS** : generalized Precision Time Protocol (gPTP) 。時間の影響を受けやすい L2 デバイス上アプリケーションに対して時刻同期を実行します。gPTP は、IEEE 1588 Precision Time Protocol (PTP) 標準規格に基づいています。
- **IEEE 802.1BA** : AVB デバイスの機能、オプション、設定、デフォルト、プロトコル、プロシージャに関するプロファイルを定義します。

AVB の詳細については、www.cisco.com/go/avb を参照してください。

AVB 標準規格は、Catalyst 9000 シリーズ スイッチおよび Catalyst 3850/3650 プラットフォームでサポートされています。AVB 対応のエンドポイントとスイッチを使用すると、アナログ AV 信号が AVB エンドポイントで集約され、Catalyst ベースのインフラストラクチャ上で送信されます。AVB は 1 つのシステムとして、AV インフラストラクチャを、信頼できるシンプルなイーサネット メディアに凝縮するための、コスト効率と柔軟性に優れたソリューションとなっています。

AVB は未来のデジタル メディア制作にとって重要な要素です。Catalyst 9000 シリーズは、この重要な標準規格セットをサポートしています。

Bonjour 向け Cisco DNA サービス

Apple 社の Bonjour プロトコルは、教育機関や小売業などのキャンパス環境で、デバイス検出や、ネットワーク サービス接続のシンプル化のために、広く利用されています。マルチキャスト DNS (mDNS) 標準規格に基づく Bonjour は、多くの Apple デバイスを始め、さまざまな種類のデバイスやサービスで幅広く使用され、デバイスの検出やデバイス接続を容易にしています。

Bonjour プロトコルは、家庭やスモール オフィス環境での「プラグ アンド プレイ」型の使用向けに最適化されており、エンタープライズ環境で使用するにはシンプルすぎます。mDNS プロトコルは、デバイスやサービスの検出にリンクレイヤ マルチキャストを使用しており、仕様上、ルーティングはできないため、ローカルの L2 ブロードキャスト ドメイン（つまり 1 ホップのみ）に限定されています。そのため、もともとルーテッド インフラストラクチャをベースとしている大規模なエンタープライズ ネットワークでの導入と使用は、当然ながら限られます。

Bonjour および mDNS の詳細については、www.cisco.com/go/mdns を参照してください。

シスコはこの課題に対処するために、Cisco IOS XE を搭載したさまざまなスイッチング プラットフォームやルーティング プラットフォームに、サービス検出ゲートウェイ（別称「Bonjour ゲートウェイ」）サービスを導入しました。これらのプラットフォームにおけるサービス検出ゲートウェイ機能の目的は、Bonjour クライアントや提供サービスが同一ネットワーク デバイス上の異なる L3 IP サブネットに配置されている場合でも、Bonjour アナウンスを ON にされたサービスに接続できるようにすることにあります。

Bonjour 向け Cisco DNA サービスでは、これをさらに発展させるため、Cisco DNA Center 上で稼働するネットワーク全体規模のアプリケーションにまで、この機能を拡張しています。また、重要なこととして、エンタープライズ ネットワーク全体で、Bonjour サービスに対するポリシーベースのアクセスを提供しています。対処が必要な大きな課題の 1 つに、数多くのさまざまなサービスやデバイスのアダプタイズメントをポリシーに基づいて制限するという問題があります。たとえば公立学校では、教師が Apple TV デバイスに接続して授業のコンテンツを表示できるようにする一方で、同じネットワークに接続している生徒にはこの機能を利用できないようにすることが望ましい場合があります。

注 Bonjour mDNS アドバタイズメントをポリシーベースでフィルタリングする機能は、ネイティブの Bonjour プロトコル自体ではサポートされていません。

ただし、シスコのサービス検出ゲートウェイと Bonjour 向け Cisco DNA サービス (Cisco DNA Center で稼働) を組み合わせることにより、強力な一連のポリシーベース アクセス制御を、Bonjour アナウンス ON のリソースに対して適用しながら、自社のエンタープライズ環境全体に Bonjour サービスを拡張することができます。

ユーザ中心の プラットフォーム設計

概要

Catalyst 9000 ファミリにおいて、プラットフォームの使いやすさは、設計上の重要ポイントとされています。ネットワークの運用コストは製品の初期購入コストよりもはるかに高いため、これは非常に重要なことです。Catalyst 9000 では、ハードウェア（RFID、ブルービーコン、Bluetooth コンソールなど）とソフトウェア（WebUI やフレキシブルテンプレートなど）の両面で、使いやすさが向上しています。

RFID

多数のスイッチのインベントリ管理には、時間がかかります。各スイッチにラベルやタグを付与したり、インベントリ データベースにすべての情報を手で入力したりすることで、デバイスのプロビジョニングが遅れます。

Catalyst 9000 では、ネットワーク デバイスやそのコンポーネントのトラッキングが、以前よりもはるかに簡単になっています。シスコは、前面の UHF 電波固体識別 (RFID) テクノロジーを備え、資産の管理、検出、トラッキングに最新の自動識別機能を適用しています。RFID タグは、スキャナから 1.8 m (6 フィート) 以内にあれば、見えていなくてもスキャナで読み取ることができます。

Catalyst 9000 ファミリは、Serialized Global Trade Item Number (SGTIN; 個別商品識別コード) -198 ビットでエンコードされたパッシブ RFID タグと連携しています。Catalyst 9400 では、スーパーバイザ エンジン、ライン カード、電源装置、ファントレイなどのすべてのコンポーネントに RFID タグが付いています。Catalyst 9000 RFID タグはパッシブ タグであるため、追加の電源は必要ありません。プロセスに必要な電力は RFID リーダーの信号から供給されます。また、同時に複数のタグを読み取ることができます。

RFID タグには、インベントリ管理に必要なデバイス情報 (シリアル番号、製品 ID、製造日など) が記録されています。シスコの RFID にはユーザ パーティションがあり、インベントリ管理者が、独自のカスタム データをパスワードで保護して格納することができます。Cisco IOS XE では RFID タグ内の情報を読み取ったり変更したりすることはできません。これを管理できるのは RFID システムのみです。

詳細については、Cisco.com で [RFID ホワイト ペーパー](#) を参照してください。

ブルー ビーコン

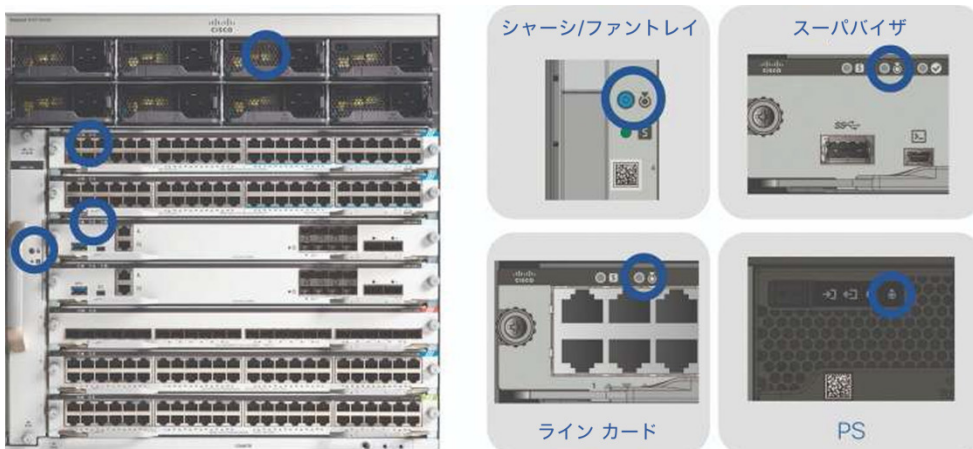
大規模な企業においては、機器のトラブルシューティング、設定、移行をする際に、特定のデバイスを見つけることが難しい場合があります。シスコでは、デバイスの識別を支援するため、Catalyst 9000 ファミリにブルー ビーコン LED を装備しています。このブルー ビーコンのオン/オフ設定は、コマンドライン インターフェイス (CLI) からでも、デバイスのボタンの手動操作によっても可能です。ブルー ビーコンをオン/オフするたびに、デバイスは、Syslog メッセージを生成します。

Catalyst 9300 シリーズのブルー ビーコン LED は、前面と背面の両方にあります。スタック構成の Catalyst 9300 スイッチの場合、各メンバーのブルー ビーコンは個別に管理できます。

Catalyst 9500 シリーズでは、ブルー ビーコン LED は、シャーシの前面に 1 つだけ備えられています。

Catalyst 9400 シリーズでは、ファントレイ、スーパーバイザ、ラインカードモジュール、電源装置それぞれに、操作可能なブルー ビーコンが装備されています。

図 Catalyst 9400 のブルー ビーコン



Bluetooth コンソール

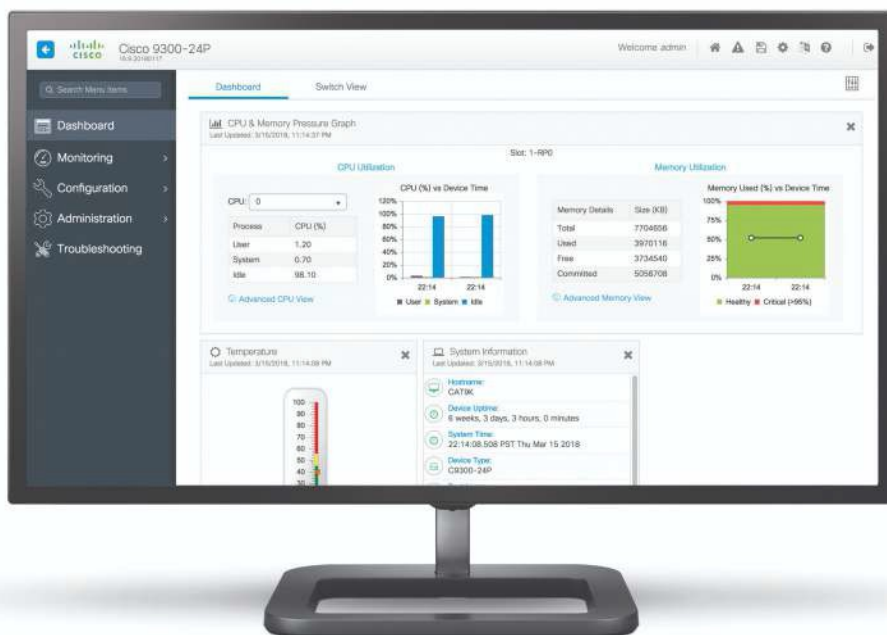
多くの場合、ネットワーク管理者は、コンソール ケーブルを使用してオンサイト構成を行っています。しかし、コンソール ケーブルには長さの制約があるため、使い勝手がよくありません。

Catalyst 9000 シリーズでは、コンソールへのワイヤレス アクセスを可能にする Bluetooth コンソール機能を、オプションとして用意しています。前面パネルの USB ポートに Bluetooth ドングルを接続して、有線のイーサネット管理インターフェイスと同じ機能を持つワイヤレス インターフェイスを有効にする必要があります。SSH または Telnet での CLI アクセス、WebUI での設定、イメージ ファイルや設定ファイルの転送に Bluetooth を使用できます。

WebUI

WebUI は、グラフィカル ユーザ インターフェイスのデバイス管理ツールで、デバイスの設定やモニタリングを実施することができます。WebUI ツールは、すべてのライセンス レベルでシステム イメージに組み込まれています。WebUI をデバイス上で有効にするには、HTTP/S サーバおよびローカルまたは外部サーバの認証を設定します。

Catalyst 9000 の WebUI



フレキシブル テンプレート

フレキシブル テンプレートを利用すると、Catalyst 9000 スイッチに、ネットワーク設計におけるさまざまな役割を設定することができます。UADP ASIC には、ネットワーク内の特定のロールに応じてハードウェア テーブルを最適化する機能があります。たとえば、セキュリティ ACL のエントリ数を減らして、その分を代わりに QoS ACL に設定することが可能です。Cisco IOS XE では、フレキシブル テンプレートは Switch Database Manager (SDM; スイッチング データベース マネージャ) テンプレートと表されます。

注 Catalyst 9300 でサポートされているのは、アクセス レイヤ向けに最適化されたデフォルト テンプレート 1 つだけです。

Sup-1XL 搭載 Catalyst 9400 および UADP 2.0 XL 搭載 Catalyst 9500 で使用できる SDM テンプレートを以下に示します。

表 各プラットフォームで使用可能な SDM テンプレート

	アクセス/ ディストリ ビューション	コア	SDA	NAT
目的	MAC および セキュリティ 用のシステム リソースを最 大化	ユニキャストおよびマ ルチキャスト ルー ティング用のシステム リソースを 最大化	ファブリッ ク導入をサ ポートする ためのシス テム リソー スを最大化	コラプスト コア WAN の導入をサ ポートするための レイヤ 3 および NAT 用システム リソースを最大化
最長プレフィックス照合 (v4/v6)	64,000/ 32,000	64,000/ 32,000	64,000/ 32,000	64,000/32,000
ホスト ルート数 (v4/v6)	最大 112,000/ 最大 56,000	最大 96,000/ 最大 48,000	最大 144,000/ 最大 72,000	最大 112,000/ 最大 56,000
マルチキャスト (v4/v6)	16,000/ 8,000	32,000/ 16,000	16,000/ 8,000	32,000/16,000
MAC アドレス	64,000	16,000	16,000	16,000
QoS ACL	18,000	18,000	18,000	3,000
PBR/NAT	2,000	2,000	2,000	16,000

UADP 3.0 搭載 Catalyst 9500 で使用できる SDM テンプレートを以下に示します。

表 各プラットフォームで使用可能な SDM テンプレート

	ディストリ ビューション	コア	SDA	NAT
目的	MAC および セキュリティ 用のシステム リソースを最 大化	ユニキャストおよびマ ルチキャスト ルーティ ング用のシ ステム リ ソースを最 大化	ファブリッ ク導入をサ ポートする ためのシス テム リソー スを最大化	コラプスト コア WAN の導入をサ ポートするためのレイ ヤ 3 および NAT 用システム リソー スを最大化
最長プレフィックス 照合/ホスト ルート数 (IPv4 および IPv6)	114,000	212,000	212,000	212,000
マルチキャスト (IPv4 および IPv6)	16,000	32,000	32,000	32,000
MAC アドレス	80,000	32,000	32,000	32,000
QoS ACL	16,000	16,000	16,000	8,000
セキュリティ ACL	27,000	27,000	27,000	20,000
PBR/NAT	3,000	3,000	2,000	15,500

プログラマビリティ および自動化

概要

設定および運用に関する意思決定には、次のような要因が影響を及ぼしています。

- デバイスやアプリケーションの数という点で、ネットワーク インフラストラクチャが急速に拡大している。
- イノベーションの迅速化が必要とされている。
- 運用コスト削減と生産性向上が求められている。
- 変更がうまくいくことを確信できない（通常、テストが不十分なことが原因）。
- 手作業のプロセスが多すぎる。

これらすべての要因によって、自動化へのニーズがますます高まっています。この傾向は、デバイスのプロビジョニングから、ネットワーク デバイスおよびネットワーク インフラストラクチャの設定/管理/モニタリング/トラブルシューティングの完全自動化に至るまで、あらゆる段階にあてはまります。

数年前にソフトウェア定義型ネットワーキング（SDN）が導入され、そのときから「プログラマビリティ」という用語が聞かれるようになりましたが、その定義は非常にあいまいです。本書では、「プログラマビリティ」（細かく言うと「ネットワーク デバイスのプログラマビリティ」）という用語を、「自動化を実現するためのネットワーク デバイス オペレーティング システムの一連の機能」と定義します。

シスコのソリューションと各社の独自開発（DIY）の比較

Cisco IOS XE のプログラミング機能は、非常に柔軟性に優れており、主に次の 3 つの領域で使用できます。

- **シスコのソリューション**：他の箇所でも触れたように、Cisco DNA Center と SD-Access は、有線およびワイヤレス デバイスで構成されたキャンパス ネットワーク全体を自動化して保証するターンキー ソリューションを実現します。Cisco DNA Center のプログラマビリティは、シスコの自社内で幅広く活用されています。

- **サードパーティ統合**：サードパーティ ソフトウェア ベンダーが、利用可能なオープン データ モデル、API、ツールを使用して、シスコと直接連携することなく独自のネットワーク管理ツールおよびシステムを構築することができます。
- **各社の独自開発 (DIY)**：お客様またはパートナーが、ネットワーク デバイスに直接アクセスして、デバイス ライフサイクルの全フェーズを自動化する独自のカスタム ソリューションを構築できます。

デバイス プロビジョニング

Cisco IOS XE では、正確で一貫した反復可能な自動プロビジョニング プロセスを実現するために、以下のオプションが用意されています。自動プロセスでは、従来の手動プロセスと比べて、運用コストも導入期間も削減されます。

- ブート前実行環境 (PXE)
- ゼロタッチ プロビジョニング (ZTP)
- シスコ ネットワーク プラグ アンド プレイ (PnP)

ブート前実行環境 (PXE)

ブート前実行環境 (PXE) は、システム管理者の間で非常に一般的に利用されているプロビジョニング プロセスです。BOOTP、DHCP、TFTP などの標準プロトコルに基づいたサーバ プロビジョニングに使用されています。デバイス起動の際、事前にロードされたイメージを使用する代わりに、DHCP リクエストが送信されて PXE サーバが検索されます。PXE サーバはデバイスにイメージを送信します。デバイスは、ダウンロードされたばかりのそのイメージを使用して起動します。

Cisco IOS XE は、iPXE をベースにして PXE を実現しています。iPXE とは、HTTP などのプロトコルを追加でサポートするために構築された、オープン ソース バージョンの PXE です。iPXE は、有線およびワイヤレスのいずれの接続でも実行できます。PXE プロセスは、「ネットワーク ブート」と呼ばれることがよくあります。

ゼロ タッチ プロビジョニング

初期インストール中または設定を消去して再起動した後では、デバイス起動時にスタートアップ設定が見つからない状態になります。ゼロ タッチ プロビジョニング (ZTP) をサポートしているデバイスは、このようなときに、ZTP モードに入ります。デバイスは、次の詳細情報を取得できる DHCP サーバを探します。

- IP アドレスおよびゲートウェイ
- DNS サーバ
- TFTP/HTTP サーバの IP アドレスまたは URL (DHCP オプション 150 を使用)
- Python スクリプト名 (DHCP オプション 67 を使用)

デバイスは、取得した IP アドレスを使用して起動し、Guestshell を有効にします。次に、TFTP/HTTP サーバから Python スクリプトをダウンロードし、デバイス設定を実行します。Guestshell により、Python スクリプトの実行環境が提供されます。

ダウンロードされた Python スクリプトに実装されているプロビジョニング ロジックは柔軟性が高く、デバイスの部分的な設定または全体の設定を、1 つまたは複数のフェーズで実施することができます。また、イメージのアップグレードやパッチ管理なども可能です。このオプションを使用すれば、フル カスタマイズ可能な何百台ものスイッチを、手動設定なしで導入することができます。

シスコ ネットワーク プラグ アンド プレイ

シスコ ネットワーク プラグ アンド プレイ (PnP) は、APIC-EM や Cisco DNA Center などの多くのシスコ製品/ソリューションと統合された、デバイス プロビジョニングのターンキー ソリューションです。

Cisco PnP により、エンタープライズ ネットワークを利用するお客様に、シンプルかつセキュアな統合ソリューションが提供されます。新しいブランチ/キャンパス デバイスのロールアウトや、既存ネットワークのシスコ ルータ/スイッチ/ワイヤレス デバイス更新のプロビジョニングが容易になります。

Cisco PnP アーキテクチャおよびブート シーケンスは ZTP に似ていますが、カスタマイズされた Python スクリプトをダウンロードするのではなく、APIC-EM や Cisco DNA Center の GUI を使用して、設定/イメージのアップグレード/パッチを管理します。プロセス全体が完全に自動化されています。

オープンなプログラマブル デバイス API

これまで長年にわたり、お客様はコマンド ライン インターフェイス (CLI) で Perl や TCL などの各種スクリプト言語を使用して、さまざまなレベルの自動化に取り組んでこられました。CLI スクリプトにはいくつか制約があります。たとえば、トランザクション管理機能が不十分、構造化されたエラー管理機能がない、コマンドの構造や構文が頻繁に変わるといった問題です。そのためスクリプトは安定性に欠け、維持するのにコストがかかります。これらはすべて、CLI の設計に起因する「副作用」のようなものです。CLI は、人間によって使用されることを想定して設計されており、プログラム可能なインターフェイスによる使用は考慮されていなかったのです。

CLI ベースの自動化の持つ欠点を克服するために、SNMP が設計されました。SNMP は、設定と運用の両方に使用されるよう意図されたものでしたが、実際には、ほとんどデバイスのモニタリングにしか使用されていません。その理由は、定義された検出プロセスがないため適切な MIB モジュールを見つけにくいことにあります。また、MIB に対する書き込み権限がない、仕様上 UDP プロトコルの使用に制約がある、セキュリティおよびコミットに関する有効な標準メカニズムがない、といった問題もその理由になっています。

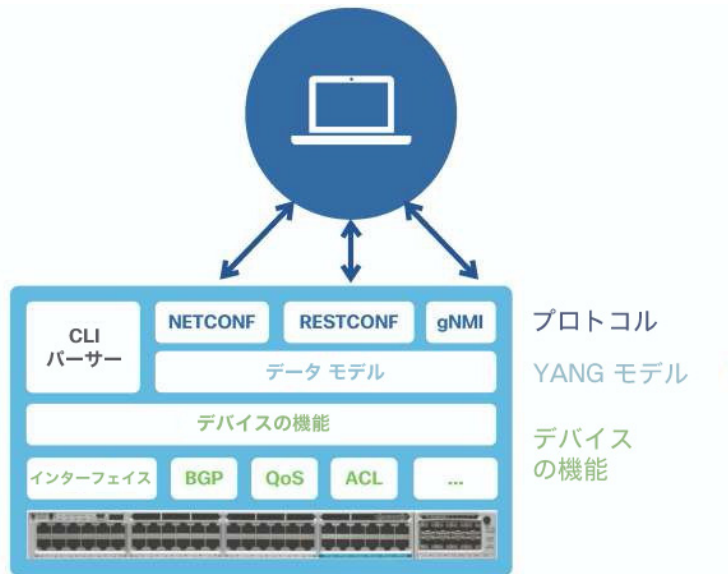
コンピュータ プログラミングにおけるアプリケーション プログラミング インターフェイス (API) とは、アプリケーション ソフトウェアを構築するためのサブルーチン定義、プロトコル、ツールをセットにしたものです。優れた API があれば、提供されたすべての構成要素をプログラマーが組み合わせることで、コンピュータ プログラムの開発が容易になります。ソフトウェア ベンダーやお客様は、構造化データ、エラー処理、各種 API 管理ツールなどの主要な機能を備えた API を求めています。

シスコのようなネットワーク ベンダーは、長年にわたってさまざまな API の導入に取り組んできました。たとえば、2006 年に NETCONF を初めて実装し、その後、WSMA、onePK、NX-API などが続きました。これらの API はお客様の間であまり普及していません。その理由は数多くありますが、主に、ベンダー独自のものであるということによります。

シスコが、Cisco IOS XE、Cisco NX-OS、Cisco IOS XR などすべての主要オペレーティングシステムで、NETCONF や YANG データ モデルなどのオープンな標準規格に基づく新たな API を構築しようと決めた理由は、そこにあります。

次の図は、デバイスレベルの機能の上に一般的な YANG データ モデル インフラストラクチャとオープン スタンダード API を構築して、デバイス設定と動作状態の両方を定義する様子を示しています。NETCONF、RESTCONF、gNMI などのさまざまなプロトコルを、外部の自動化ソフトウェア ツールチェーンとのインターフェイスとして使用することができます。

図 オープンなプログラマブル デバイス API



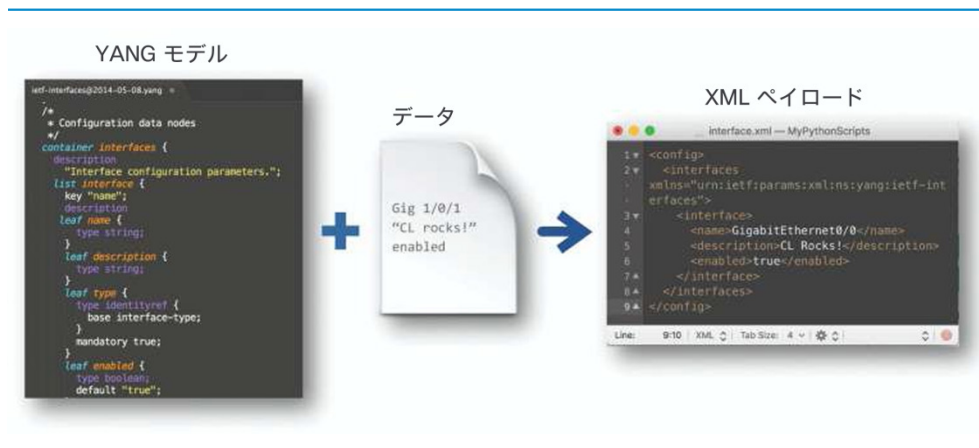
データ モデル

データ モデルは、オープンなプログラマブル API の最も重要なコンポーネントの 1 つです。データモデルは、特定の機能のデータ構造、構文、セマンティックを詳細に定義するものであり、CLI による非構造化データの問題を解決することを目的としています。

YANG

Yet Another Next-Generation (YANG) は、IETF が開発したデータ モデリング言語です。これによって、異なるネットワークベンダー製の機器間でデータモデルを再利用できるようになります。ネットワークデバイスの設定やモニタリングを自動化するために、ネットワーク事業者の間で広く使用されています。YANG は、[RFC 6020](#) で定義されています。

図 YANG モデルの例



上図のように、YANG データ モデルは、テンプレートと見なすことができます。デバイスの設定や状態を取得/変更するためには、YANG モデルに実際のデータを適用して、ネットワークデバイスと交換可能なオペレーションを構築する必要があります。

データ モデルの種類

注 IETF の標準規格では、コンフィギュレーション データ モデルとオペレーショナル データ モデルは区別されています。

コンフィギュレーション データ モデルは、システムを初期のデフォルト状態から現在の状態に変えるために必要とされる、書き込み可能データのセットです。基本的にコンフィギュレーション データ モデルは、特定のタスクを実施するようデバイスに指示するものであり、Cisco IOS XE デバイスの実行コンフィギュレーションに簡単にマッピングできます。

オペレーショナル データ モデルは、デバイスに関する、読み取り専用のデータ ステータス情報/統計情報のセットです。オペレーショナル データ モデルは、デバイスの実際の動作内容によって構成され、従来 show コマンドによって得られていた情報とマッピングされます。

コンフィギュレーション データ モデルとオペレーショナル データ モデルはいずれも、ネイティブ データ モデルまたはオープン データ モデルにさらに分類できます。

ネイティブ データ モデルは、シスコなどのネットワーク ベンダーによって定義された、オペレーティング システムに固有のモデルです。たとえば、Cisco IOS XE 用のネイティブ モデルや Cisco NX-OS 用のネイティブ モデルがあります。

オープン モデルは、IEEE や IETF などの標準化団体または OpenConfig などのワーキング グループによって定義されます。オープン モデルの大きな利点は、異なるオペレーティング システムやベンダー間で共通して使用できるという点にあります。これによって、すべてのデバイスを一貫した方法で管理できます。

オープン モデルは、ネイティブ モデルのサブセットになります。というのも、オープン モデルを定義するプロセスは、通常、ネイティブ モデルを定義するプロセスよりも時間がかかるためです。その主な理由は、ネイティブ モデルの場合はベンダーが自身の裁量で柔軟に定義できるのに対して、オープン モデルを定義するためには多くの関係者が内容やモデル構造に合意する必要があるからです。

Cisco IOS XE で採用されているアプローチでは、IOS XE ネイティブ データ モデルの包括的リストが提示され、オープン モデルも、利用可能になりしだい提供されます。Cisco IOS XE のオープン モデルは、対応する IOS XE ネイティブ モデルにマッピングされています。したがって、シスコのお客様は、特定の機能を管理するためにオープン モデルまたはネイティブ モデルのどちらを使用するか、自由に決めることができます。

現存するさまざまなオープン データ モデルの中で最近広く普及するようになったのが、OpenConfig データ モデルです。OpenConfig は、大規模なネットワーク事業者によるインフォーマルなワーキング グループです。Google 社の主導のもと、各社のネットワークの自動化という同じ目標が共有されています。

シスコは、広く知らている [GitHub リポジトリ](#) に YANG データ モデルを公開しており、新しいリリースが利用できるようになるたびに更新しています。

データ モデルは、GitHub リポジトリからダウンロードできるだけでなく、Catalyst 9000 の Cisco IOS XE ではデバイスから直接ダウンロードすることもできます。この機能は非常に便利です。特に、第 6 章「高可用性」に記載したパッチ プロセスを使用してデバイス上でデータ モデルが更新されている場合に役立ちます。

ツール、SDK、リソース

API オペレーションは手動で構築することも可能ですが、それではあまり実用的ではありません。データ モデルの検索/検証と API オペレーション構築のためのツールが数多く開発されているのは、そのためです。

現行のツールの中で最も一般的に使用されているいくつかのツールを下記に挙げます。

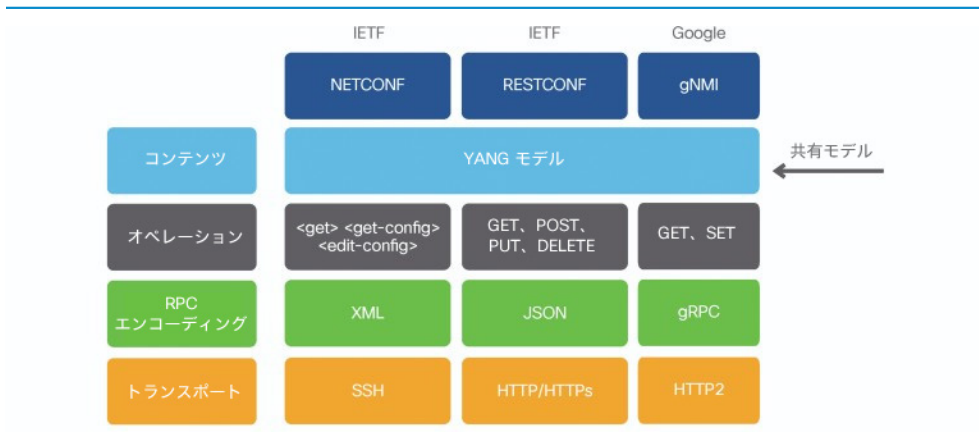
- **PYANG** : 検索/検証およびドキュメントの自動作成のための Python ライブラリ。
- **YangExplorer** : モデルの確認を簡単に開始し、小規模タスクを自動化するための、オープン ソースのツール。
- **YDK** (YANG 開発キット) : YANG でモデル化された API の抽象化レイヤを提供するソフトウェア開発キット。
- **Yang カタログ** : 業界で利用可能なすべての YANG モジュールのためのリファレンス。

デバイス API プロトコル

Catalyst 9000 デバイスの Cisco IOS XE でサポートされるさまざまなインターフェイス プロトコルでは、一般的なデータ モデルのインフラストラクチャが共有されています。純粋に技術的な観点から言うと、すべてのプロトコルを使用して同じ 1 つの YANG データ モデルを管理することも可能ですが、当然ながら、その方法では維持が容易ではありません。

次の図は、スタックの各レイヤにおける各 API プロトコルの主な違いをまとめたものです。トランスポート レイヤでの違い (SSH、HTTP、HTTP2) を始めとして、リモート プロシージャ コール (RPC) に使用されるエンコーディング形式およびオペレーション方法の違いを示しています。

図 デバイス API プロトコルの比較



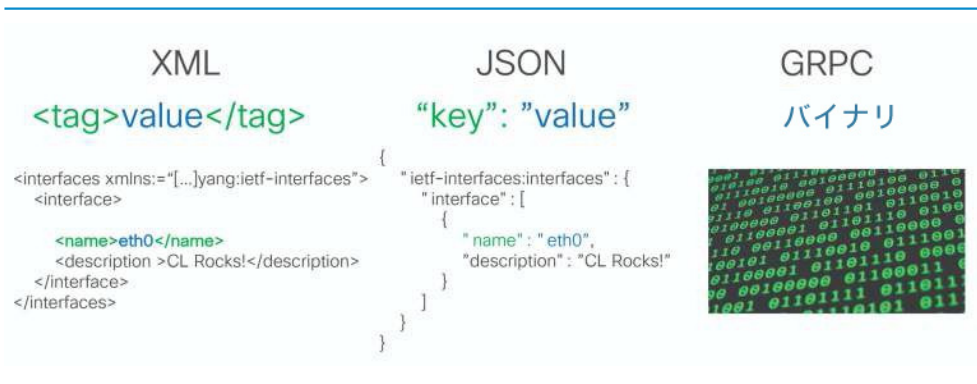
注 YANG データ モデル インフラストラクチャは、Cisco IOS XE のすべての API プロトコル間で共通しています。

エンコーディング形式

API プロトコルはどれも、通信にリモート プロシージャ コール (RPC) を使用します。外部サーバで実行されているクライアントがネットワーク デバイスに RPC メッセージを送信し、ネットワーク デバイスは RPC 応答メッセージを返信します。RPC と RPC 応答のデータ ペイロードはどちらも、プロトコルによって定義されている形式でエンコードされます。最も一般的なエンコーディング形式は、次のとおりです。

- **Extensible Markup Language (XML)** は、人間が理解できるテキスト ベースの形式で、交換される情報が、タグを使用して表されます。HTML とよく似ていますが、HTML が Web ページを構築するためのものであるのに対して、XML はデータを記述するためのものです。NETCONF は XML を使用しています。
- **JavaScript Object Notation (JSON; JavaScript オブジェクト表記)** は、XML に代わるものです。JSON も人間が理解できるテキストベースの形式ですが、タグの代わりに <キー:値> のペアが使用されており、データの解析がより容易になっています。一般的に JSON のほうが XML よりも好まれているのはそのためです。RESTCONF は、JSON と XML の両方をサポートしています。
- **Google リモート プロシージャ コール (gRPC)** は、Google 社が自社独自アプリケーション向けに定義したエンコーディング形式のオープン ソース バージョンです。非常に効率的で拡張性に優れていることが実証されています。バイナリ形式のため、人間が読んで理解することはできません。クライアント側でのエンコードおよびサーバ側でのデコードの実施に関しては、プロトコル バッファに依存しています。gNMI はさまざまなエンコーディング形式をサポートしていますが、推奨されている形式は gRPC で、それが最も多く使用されています。

図 RPC エンコーディング形式



NETCONF

NETCONF は、各ネットワーク事業者の自社ネットワーク管理を支援するために IETF が定義した、一般的なネットワーク設定プロトコルです。新しいプロトコルと思われることが多いのですが、実際にはかなり前からあり、シスコが IOS で NETCONF のサポートを始めたのは 10 年以上前のことになります。

その後 NETCONF は、新しい一連の IETF Request For Comments (RFC) の定義によって大きく進化してきました。[RFC-6241](#) は、NETCONF の基本を定義し、拡張機能オプションという概念を導入しました。NETCONF の拡張機能の例としては、YANG データ モデル言語 ([RFC-6020](#)) と通知機能 ([RFC-5277](#)) があります。

NETCONF スタックには SSH トランスポートと汎用 RPC 形式のメッセージが含まれ、XML 形式でエンコードされます。

主な NETCONF オペレーションは、次のとおりです。

- **<get>**：実行コンフィギュレーションおよびデバイスの状態情報を取得します。IOS XE の「show」コマンドに簡単にマッピングできます。
- **<get-config>**：指定した設定の全部または一部を取得します。IOS XE の「show run」コマンドと類似しています。

- **<edit-config>**：設定の全部または一部を変更します。Cisco IOS XE の config terminal モードを使用した場合と同じ動作をします。

RESTCONF

RESTCONF は、（NETCONF と同様に）IETF によって [RFC-8040](#) で定義された、ネットワーク設定プロトコルです。

RESTCONF スタックには、HTTP/HTTPS トランスポートと（NETCONF と同様に）汎用 RPC 形式のメッセージが含まれ、XML または JSON 形式のいずれかでエンコードされます。

RESTCONF オペレーションは REST フレームワークによって定義され、対応する NETCONF オペレーションに簡単にマッピングできます。

- **GET**：リソースを取得します。NETCONF の <get-config>、<get> と類似しています。
- **POST**：新しいリソースを作成します。<edit-config> に operation="create" オプションを付けて実行する場合と類似しています。
- **PUT**：リソースの作成または変更を行います。<edit-config> に operation="create/replace" オプションを付けて実行する場合と類似しています。
- **DELETE**：リソースを削除します。<edit-config> に operation="delete" オプションを付けて実行する場合と類似しています。

すべてのオペレーションにおいて、ターゲット リソースは、インターネット上の Web ページの参照に標準的に使われている URL を使用して定義されます。

gNMI

Google ネットワーク管理インターフェイス (gNMI) は、NETCONF や RESTCONF に代わる YANG モデル アクセス用のプロトコルです。

NETCONF と RESTCONF はどちらも IETF によって定義された標準ベースのプロトコルですが、それに対して gNMI は、Google 社が開発したオープン ソースのネットワーク管理プロトコルです。

gNMI オペレーションは、次のとおりです。

- **CAP** : 最初の接続でネットワーク デバイスに送信され、デバイスの機能を検出します。
- **GET** : デバイスの設定または状態を取得します。Prefix、Paths、Data Type (Oper、Config、All) などの属性を伴います。
- **SET** : デバイス設定を変更します。GET と同じ属性 (ただし Type (Update、Replace、Delete) は除く) を伴います。

モデル駆動型テレメトリ

ネットワーク モニタリングの課題

CLI および SNMP をベースにした自動化ソリューションは、時間とともに、不完全かつ非効率的で、拡張や維持が困難であることがわかってきました。スピード、拡張性、障害の切り分け、フォレンジック分析、ほぼリアルタイムでのデータ可用性という新たな要件が生じたことで、従来のモニタリング ソリューションは、ほとんどの組織にとって不十分なものとなっています。

新しいパラダイム

従来型モニタリング ソリューションが持つ上記の欠点や短所に対応するために、モデル駆動型テレメトリ (MDT) が設計されました。MDT は、第 12.3 章「オープンなプログラマブル デバイス API」で定義されている YANG データモデルと同じ形式の構造化データを、効率的かつ拡張可能な方法で提供しています。ネットワーク デバイスへの影響も少なくなっています。

MDT は、新たなネットワーク モニタリング アプローチを提供しています。そのアプローチでは、オペレーショナル データがネットワーク デバイスから外部コレクタに継続的にストリーミングされます。そして、ネットワーク モニタリングのためのリアルタイムでの統計情報アクセスを実現しています。データのストリーミングは、変更時もしくは定期的な間隔で実施できます。

プル方式である SNMP の get リクエストと違い、MDT はプッシュ方式を採用しています。

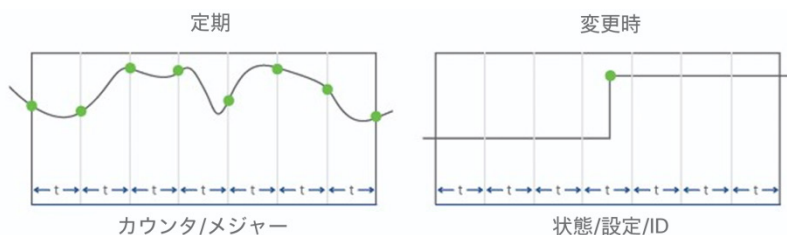
Catalyst 9000 での Cisco IOS XE MDT の実装は、標準の IETF PUB/SUB (パブリケーション/サブスクリプション) に基づいています。

デバイスからストリーミング データを取得するためには、YANG モデルのデータ セットへのサブスクリプションを外部コレクタで設定する必要があります。サブスクリプションは、RPC サブスクリプション メッセージを利用して作成できます。デバイスでサブスクリプションを有効にすると、そのサブスクリプションの全有効期間にわたって継続的にデータが送信されます。定期的通知または変更時通知を使用して宛先にデータをストリーミングすることで、パブリケーションが実現します。

定期的な通知の場合、データは、設定された間隔で宛先にストリーミングされます。更新間隔は 1/100 秒単位で表されます。概念的には SNMP の「get」リクエストに似ていますが、MDT プッシュベース モデルでは、レートがはるかに速いという利点があります。インターフェイス カウンタや CPU 使用率など、頻繁な変更が想定されるデータには、定期的なパブリケーションが推奨されます。

変更時通知の場合、データは、変更が発生した場合にのみパブリッシュされます。変更時パブリケーションは、頻繁な変更が想定されないデータへの使用や、変更発生時にそれをすぐ把握することが重要な場合での使用に最適です。

図 定期的なサブスクリプションと変更時サブスクリプション



Cisco DNA Center Assurance では、同様のアプローチを使用して、MDT 対応デバイスからストリーミング データを収集し、他のデータ ソースと関連付けています。

データ コレクタを自社で開発するのは複雑なタスクですが、独自のコレクタの構築を前向きに検討しているお客様には、TCollector、collectd、Elastic Stack（一般に「ELK Stack」と呼ばれています）などのオープン ソースのツールや、Apache Kafka、ActiveMQ、RabbitMQ などのメッセージング ブローカーを活用することをお奨めします。

スクリプティング

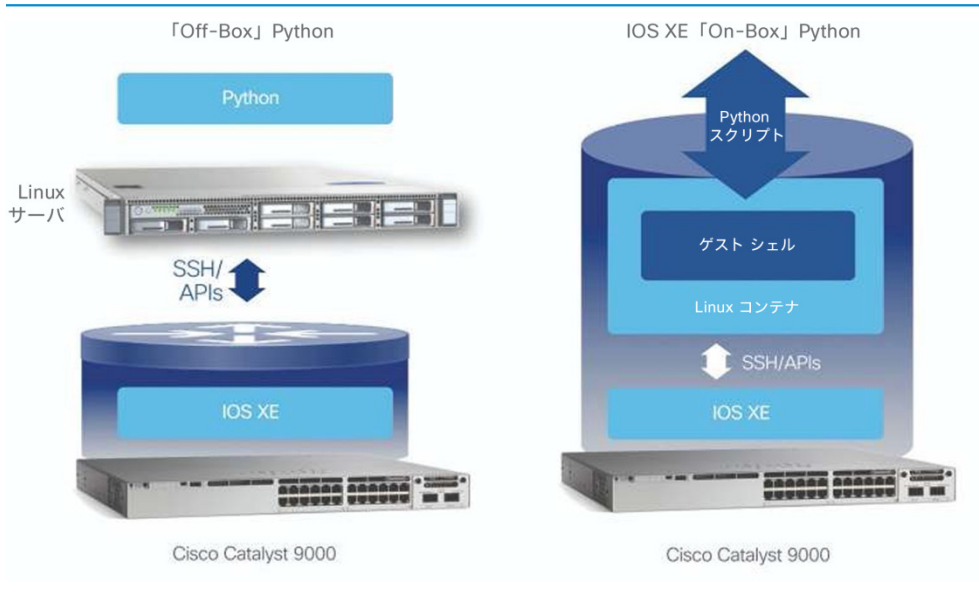
小さなタスクを迅速かつ簡単に自動化する際には、長年の間、スクリプトが使用されてきました。各種スクリプト言語のうち Perl、TCL、JavaScript などが、徐々に他の言語よりも一般的になってきました。最近では Python が最も人気のあるスクリプト言語になりました。Python の人気が拡大し続ける主な理由の 1 つは、その始めやすさです。インタラクティブなシェルが用意されており、スクリプトを 1 行ずつ簡単に実行できます。また、他の大半のスクリプト言語よりも、読んでわかりやすい形式になっています。

しかし、おそらく最も重要な理由は、ほとんどのオペレーティング システムで利用できる Python ライブラリが豊富に公開されていることと、Python パッケージ マネージャ (pip) を使用して簡単にライブラリのインストール/更新/アンインストールを実施できることにあります。また、アプリケーション ライブラリの依存関係の管理に役立つ Python 仮想環境という利点もあります。

Off-Box Python と On-Box Python

Cisco IOS XE が稼働している Catalyst 9000 を Python スクリプトで自動化するには、2 つの方法があります。それらの方法は一般的に、Off-box スクリプティングと On-box スクリプティングと呼ばれています。

図 Cisco IOS XE の Off-Box Python と On-Box Python



- **Off-Box** Python スクリプトは外部サーバで実行され、SSH で Cisco IOS XE デバイスに接続して、CLI ベースの自動化やオープン API を利用した自動化を実現します。
- **On-Box** Python スクリプトは、Catalyst 9000 内部において、Guestshell と呼ばれる組み込みの Linux コンテナで実行されます。Python スクリプトは、Off-Box Python スクリプトと同じメカニズムを使用して、基盤となる Cisco IOS XE に、Guestshell 環境からアクセスすることができます。

Catalyst 9000 は、Off-Box と On-Box の 2 つのオプションを用意していることで、集中型または分散型の別を問わず、Python ベースのアプリケーション アーキテクチャに最適なツールとなっています。

設定管理ツール

設定管理ツールを利用すれば、大規模な環境において、システムやアプリケーションを一貫性のある方法で自動化することができます。このようなツールは、10 年以上にわたってシステム管理者に使用されています。最近では、ネットワークの自動化にも設定管理ツールを使用（または使用を検討）しているお客様が増えています。設定管理ツールには、以下のようなさまざまな利点があります。

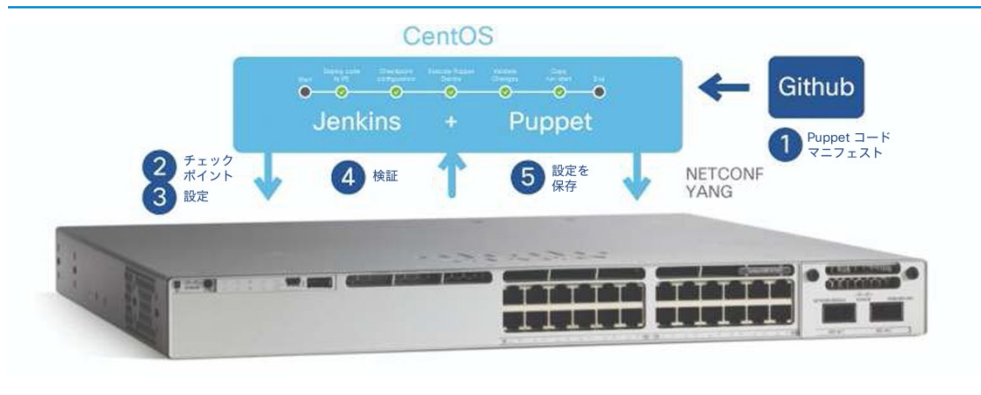
- さまざまなベンダーおよびオペレーティング システムに適用される一貫したアプローチ。
- バージョン管理システムと簡単に統合可能。
- ハードウェアおよびソフトウェアのデバイス情報を簡単に収集可能。
- インテントベースの設定アプローチを採用。
- システム、アプリケーション、またはデバイスがすでに望ましい状態である場合は、変更は行われない。

ネットワーキングの分野では、設定管理ツールは当初、データセンターのネットワークの自動化のみに使用されていましたが、現在では、エンタープライズ ネットワークにも使用され始めています。最も広く使用されているツールは Ansible と Puppet です。設定管理ツールは、アーキテクチャによってエージェントベースとエージェントレスの 2 つのグループに分類できます。エージェントベースのアーキテクチャでは、管理対象デバイスにソフトウェア エージェントをインストールする必要がありますが、エージェントレス アーキテクチャでは不要です。これは大きな違いです。特に、デバイスにサードパーティ製ソフトウェアをインストールすることに慎重になる傾向の強いエンタープライズ環境では、その違いは重要です。

Ansible は、エージェントレス アーキテクチャをベースにしており、そのことが成功の大きな要因になっています。Ansible では、Cisco IOS XE が稼働している Catalyst 9000 スイッチなどのシスコ デバイスがすでにサポートされており、インターフェイス、VLAN、VRF、ユーザなどを設定するためのインテントベースのモジュールや、CLI および NETCONF ベースの設定が提供されています。

Puppet は従来、管理対象デバイス上にエージェントを必要としていましたが（エージェントベースのアーキテクチャ）、現在 Puppet では、ネットワークデバイス専用のエージェントレスアーキテクチャが開発されています。また、NETCONF API をベースにして、Cisco IOS XE が稼働しているシスコデバイスもサポートされる予定です。

設定管理ツールは、DevOps/NetOps カルチャを推進する多くのお客様の間で台頭している新たなトレンド、つまり継続的統合と継続的導入（CI/CD）の、重要なコンポーネントになっています。

 Puppet による Cisco Catalyst 9000 での CI/CD


CI/CD は、実稼働環境に新たな変更を導入する際にかかる時間を短縮しながら、より確実に変更を成功させるために開発された、新たな設定管理プラクティスです。CI/CD では、障害発生時のロールバックを簡単に実現するためのソース管理システムとの統合と、テストプロセスの自動化によって、これを可能にしています。CI/CD フレームワークを実装している環境では、開発サイクルの短縮、イノベーションの促進、トータル IT コストの削減が実現しています。

Cisco DevNet

Cisco DevNet は、主要なシスコ オペレーティング システムで提供されている最新のプログラマビリティ技術の学習をお客様やパートナーが簡単に始められるように構築されたイニシアチブです。Cisco DevNet では、自己学習型ラボ、ビデオ コース、シミュレートされたデバイスや実際のハードウェア上でプログラマビリティ技術をテストするためのデバイス サンドボックスに加え、API ドキュメント、コミュニティ サポートなどが提供されています。

Cisco DevNet



Cisco [DevNet](https://developer.cisco.com) はすべて無料です。お客様とパートナーは、サイン アップするだけで学習を開始できます。

アプリケーション
ホスティング

アプリケーション ホスティングの運用

エンタープライズ ネットワークでは、ビジネス関連のさまざまな使用例でアプリケーションが使用されています。エンタープライズ アプリケーションの例として、パフォーマンス モニタやプロトコル アナライザなどの管理ツール、侵入検知サービスなどのセキュリティ ツールセットが挙げられます。従来そのようなアプリケーションは、外部の物理サーバまたは仮想サーバで運用されてきました。

シスコは、あらゆるネットワーク デバイスで実行されているコンテナ化アプリケーションを管理するために、Cisco Application Framework (CAF) を構築しました。CAF は、Cisco IOx と呼ばれています。元々は Internet of Things (IoT) アプリケーションをホストするために構築されたものでしたが、Catalyst 9000 では IOx をキャンパス環境内のエンタープライズ アプリケーションに活用しています。

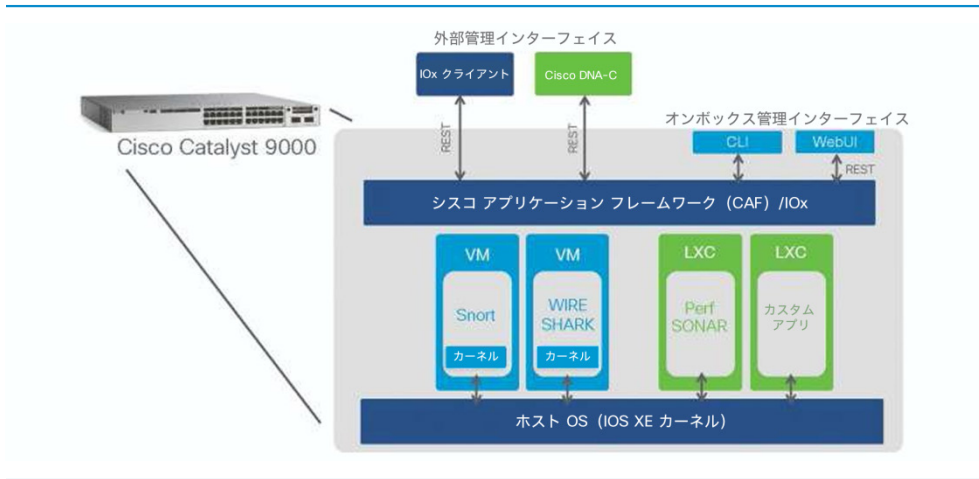
Catalyst 9000 の Cisco IOx は、LXC (Linux コンテナ) および KVM ベースの仮想マシンにコンテナ化されたアプリケーションをサポートしています。ネイティブの Docker コンテナはまだサポートされていませんが、Docker ツールを使用して簡単に LXC 形式で IOx アプリケーションを構築できます。Cisco IOx を利用することで、任意のコンテナ化アプリケーションをネットワーク デバイスに導入することが可能になります。

シスコは、アプリケーション ホスティング向けの特定のサービスを定期的に公開していますが、IOx フレームワークに適した KVM ベースの VM または Linux LXC の導入を奨励および支援しています。

Catalyst 9000 は、ホストされたアプリケーションを管理するためのオプションをいくつか用意しています。

- **Cisco DNA Center** : シスコの SDN コントローラ。すべての LAN、WAN、WLAN エンタープライズ デバイスを実行するために使用。
- **IOx クライアント** : Python ベースのツール。IOx アプリケーションの構築および管理が可能。
- **Web UI** : Cisco IOS XE の GUI。デバイスを設定およびモニタリングし、IOx アプリケーションもサポート。
- **コマンド ライン インターフェイス** : IOx および IOx アプリケーションを管理するための Cisco IOS XE コンソール コマンド セット。

図 Catalyst 9000 のアプリケーション ホスティング フレームワーク



IOx アプリケーションの構造

IOx アプリケーションは、アプリケーション記述子や 1 つ以上のディスク イメージを含んで、標準の Linux tar アーカイブ形式にパッケージされています。オプションで証明書ファイルやその他の補助ファイルが含まれることもあります。アプリケーション記述子は、YAML 形式で書かれたファイルで、以下のような情報を含んでいます。

- アプリケーション情報：名称、説明、バージョン、作成者
- アプリケーションの種類：LXC または VM
- 必要なハードウェアリソース：CPU、メモリ、ストレージ
- アプリケーションで使用する仮想ネットワーク インターフェ이스のリスト
- アプリケーション自体をロードするために使用されるディスク イメージ ファイル
- スタートアップ タスクまたは実行前スクリプト

IOx アプリケーションの構築方法に関するステップごとの説明については、Cisco DevNet Web サイトを参照してください。

ハードウェア リソース

Catalyst 9000 上で稼働する Cisco IOS XE は、アプリケーション ホスティング用に専用のメモリおよび CPU リソースを予約します。メモリおよび CPU のリソースを予約することで、スイッチではユーザ アプリケーション用に個別の実行空間が提供されます。これにより、スイッチの IOS XE ランタイム プロセスが保護され、その整合性とパフォーマンスの両方が確保されます。

アプリケーションは、Catalyst 9000 によって提供される外部 SSD ストレージ (USB または M2 SATA) オプションのいずれかに配置する必要があります。アプリケーションは、デバイス内蔵のフラッシュ ストレージにはアクセスできません。このストレージは、整合性を確保するために、IOS XE 用に予約されています。

注 外部 SSD ストレージは、ホストされたアプリケーションと Cisco IOS XE との間で共有されます (予約はされていません)。

表 Catalyst 9000 のアプリケーション ホスティング リソース

プラットフォーム	メモリ (GB)	CPU (コア)	USB ストレージ (GB)		M2 SATA ストレージ (GB)
			USB 2.0 前面	USB 3.0 背面	
Catalyst 9300	2	1.8GHz X 1	16	120	N/A
Catalyst 9400	8	2.4GHz X 1	16	N/A	960
Catalyst 9500 (UADP 2.0 搭載)	8	2.4GHz X 1	16	120	N/A
Catalyst 9500 (UADP 3.0 搭載)	8	2.4GHz X 1	N/A	N/A	960

キャンパス

ネットワーク設計

概要

ネットワークを最適化するには、個々のデバイスを密接に連携させる必要があるため、ネットワークの設計が重要になります。各プラットフォームはそれぞれ機能を持っており、類似した機能も数多くありますが、さまざまなプラットフォームを組み合わせると、結果的にネットワーク動作が最適化する場合もあれば、最適とは言えない場合もあります。そのため、具体的な目的に応じて最適なプラットフォームを選択することが重要です。シスコは、幅広いニーズに対応すべく、さまざまな Catalyst 9000 シリーズ モデルを提供しています。

キャンパス ネットワークでは主に、ユーザとそのデバイスの相互通信や、データ センター内サービス、プライベート/パブリック クラウド サービス、およびインターネットとの通信の方法に、重点が置かれています。また、キャンパス ネットワークは地理的に分散し、それぞれの要件が多様化する傾向にあります。ユーザやデバイスの種類や数、それに地理的な多様性が、最適なネットワーク設計を決める要因となります。

結論

「適材（適切なプラットフォーム）」を「適所（適切なジョブ）」に選択しましょう。

シスコには、30 年に及ぶキャンパス環境設計の実績があります。その間に、さまざまな設計を開発して厳しいテストを実施してきました。そこから、次の 5 種類のキャンパス設計モデルが生まれました。

- **マルチレイヤ**：コアとディストリビューションの間にルーティングを使用し、スイッチング アクセス機能を備えた、多層型設計。
- **コラスプト コア**：ルーテッド コアとスイッチド アクセス機能を備えた、小規模サイト向けの 2 層型設計。
- **ルーテッド アクセス**：すべてのレイヤでエンドツーエンドにルーティングを利用する多層型設計。
- **キャンパス MPLS**：ルーテッド ドメインの上で MPLS を使用して、セグメント化されたサービスを提供する、多層型設計。
- **Software-Defined Access (SD-Access)**：上記の設計をベースにした多層型ネットワーク ファブリック。コントローラーによって自動化および保証される。

各設計モデルは独自の要件セットに対応して進化してきましたが、全モデルに共通する一連の特性があります。キャンパス設計の共通特性には、次のようなものがあります。

- **階層**：定義されたロールを各レイヤに割り当てる、構造化された設計。構造化されたケーブル設備に対応。
- **冗長性**：物理的な冗長性（リンク、シャーシ、電源）、データ プレーンの冗長性、コントロール プレーンの冗長性が含まれている。
- **帯域幅**：各ネットワーク層に、集約システムの負荷をサポートできるだけの十分なキャパシティが備えられている。
- **ポート密度**：各ネットワーク層に、接続されたすべてのネイバーをサポートできるだけの十分なインターフェイスが備えられている。
- **拡張性**：すべての相互接続とネットワーク サービスをサポートできるだけの十分なハードウェア/ソフトウェア リソースが備えられている。
- **ワイヤレス LAN**：キャンパス全体のモビリティをサポートできるだけの十分な有線インフラストラクチャと機能が備えられている。

各 Catalyst 9000 プラットフォームは、1 つまたは複数の設計モデルに対応して設計されていますが、すべてのプラットフォームに共通する機能セットがあります。

- **Catalyst 9500 シリーズ**：1/10/25 G SFP および 40/100 G QSFP のオンボード ポートとモジュール ポートを備えた固定型フォーム ファクタ。
 - 中規模から大規模のキャンパス コアおよびディストリビューション設計に対応できるだけの十分な ASIC 帯域幅とテーブル規模を備えています。
- **Catalyst 9400 シリーズ**：10/100/1000/mGig RJ45、1/10 G SFP モジュールおよび 40 G QSFP スーパーバイザ ポートを備えたモジュラ型フォーム ファクタ。
 - 大規模なキャンパス アクセス設計または中規模のディストリビューション設計に対応できるだけの十分な ASIC 帯域幅とテーブル規模を備え、高密度のユーザ アクセス向けに設計されています。

- **Catalyst 9300 シリーズ** : 10/100/1000/mGig RJ45 および 1/10/25 G SFP または 40 G QSFP のモジュール ポートを備えた固定型のスタックابل フォーム ファクタ。
 - 大規模なキャンパス アクセス設計に対応できるだけの十分な ASIC 帯域幅と テーブル拡張性を備え、高密度のユーザ アクセス向けに設定されています。

結論

Catalyst 9000 スイッチは、新時代のネットワーキングに対応可能な、最大の柔軟性・最大の拡張性・復元力を備えたプラットフォーム。

本書では、ほとんどの部分が各 Catalyst 9000 プラットフォームの個々の詳細に焦点を当てていますが、以降の章では、Catalyst 9000 シリーズ全体に共通するソリューションに特化し、そのソリューションによってネットワーク設計全般をいかにシンプル化および最適化できるか説明していきます。

物理インフラストラクチャ

このセクションでは、最適なキャンパス ネットワークを実現できる十分な帯域幅とポート密度を備えるために、設計の際に考慮すべき、重要な物理インフラストラクチャ条件について説明します。

スピードへの要求

2016 ~ 2021 年の期間における IP トラフィック全体の年平均成長率 (CAGR) は、最大 24 % になると予測されています。前述のように、高速ワイヤレス テクノロジーの導入拡大や、IoT デバイス/センサーの急増、大量のデータを処理する強力な新しいエンドポイントの登場によって、ネットワーク エンジニアは、物理インフラストラクチャを再設計する必要に迫られています。クライアント アクセス速度は、毎秒 1 ギガビット (Gbps) から、2.5 Gbps、5 Gbps を経て、将来的には 10 Gbps にもなろうとしています。これらの新しいクライアント アクセス速度要件に対応するためには、10 G を超えるネットワークインフラストラクチャ速度が必要になります。

しかし、高速化によって、別の課題がもたらされる可能性があります。たとえば、既存の 10 G の Small Form-factor Pluggable (SFP) ポートから 40 G の Quad Small Form factor Pluggable (QSFP) に変更するには、トランシーバやケーブルに多額のコストがかかります。リンクアグリゲーションの代替手段を使用することも 1 つのアプローチですが、複数の 10 G リンクでの効果的なロード シェアリングの実現は、ハッシュ アルゴリズムやトラフィック パターンに依存します。

簡単に移行できるように後方互換性を確保することも、キャンパス ネットワークに新たな速度を適用する際に考慮すべき、もう 1 つの重要事項です。SFP や QSFP などの一般的なトランシーバ フォーム ファクタを使用するのが効果的です。最新の 10 G SFP+ と新しい 25 G SFP28 インターフェイスは、100 M および 1 G SFP との後方互換性をサポートしています。同様に、新しい 100 G QSFP28 インターフェイスは、40 G QSFP との後方互換性をサポートしています。

注 Cisco 25 G SFP28 トランシーバは、10 G または 25 G のいずれの速度でも動作するデュアルレート光ファイバをサポートしています。

たとえば、ディストリビューション レイヤ リンクへのアクセスを 10 G から 25 G にアップグレードする場合は、簡単に移行できます。10 G SFP+ トランシーバを取り外して、25 G SFP28 トランシーバを新しく導入するだけです（使用するケーブルは同じです）。リモート側がまだ 10 G SFP+ トランシーバを使用している場合、リンクは 10 G で動作します。対応する 25 G SFP28 トランシーバがリモート側に設置されると、リンクは 25 G で動作するようになります。

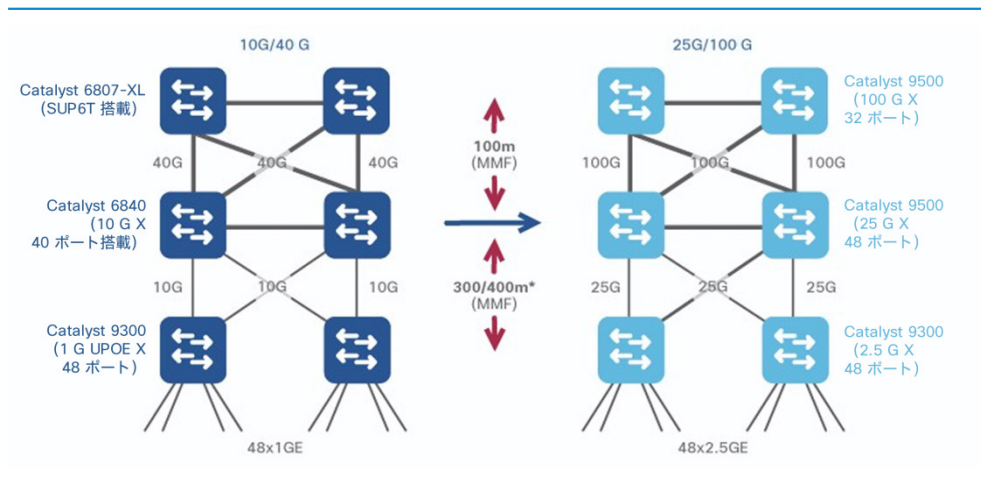
使用例 1：同じケーブル距離での速度移行

アクセス レイヤの帯域幅が 10/100/1000 M から 2.5 G に増大すると、キャンパス バックボーンは、10/40 G から 25/100 G に移行する必要があります。そのためには、既存の環境とほぼ同じケーブル距離をまかなえる新しい光ファイバが必要となります。

結論

革新的な Cisco SFP-10G/25G-CSR-S トランシーバを使用すると、従来のケーブル距離が 300/400 m までの場合、OM3/4 MMF ケーブル（光ファイバの品質によって異なる）で 25 G の速度を実現できます。

図 同じケーブル距離での速度移行



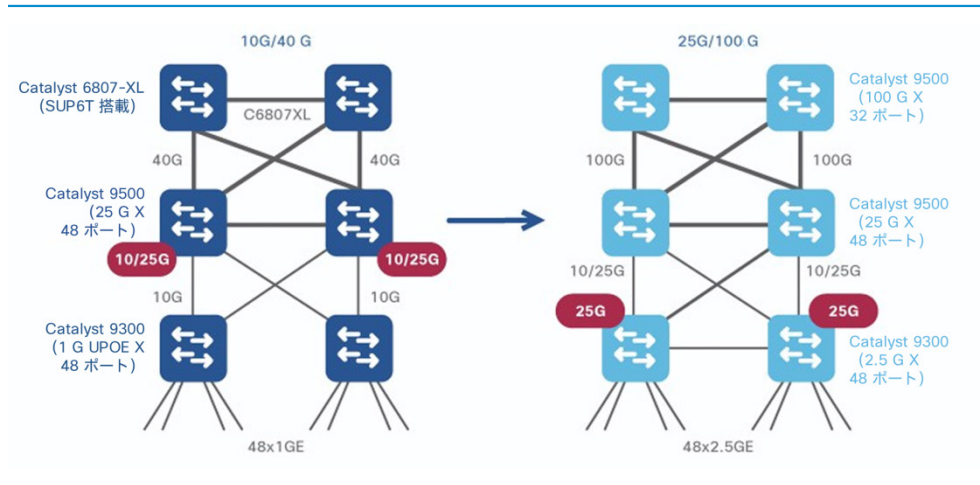
使用例 2 : デュアルレート光ファイバによる速度移行

Cisco 25 G ポートフォリオでは、デュアルレート光ファイバを備えたトランシーバによって 10 G との後方互換性を提供しています。Cisco デュアルレート光ファイバは、サポートされている最高速度に自動的にネゴシエートします。たとえば、リモート デバイスが 10 Gbps にしか対応していない場合、2 つのデバイスは 10 Gbps の速度で動作します。

結論

インフラストラクチャを 25 G にアップグレードする必要はありません。トランシーバは 10 G で動作でき、通常の更新サイクルの一貫でアップグレードすることが可能です。

図 デュアルレート光ファイバによる速度移行



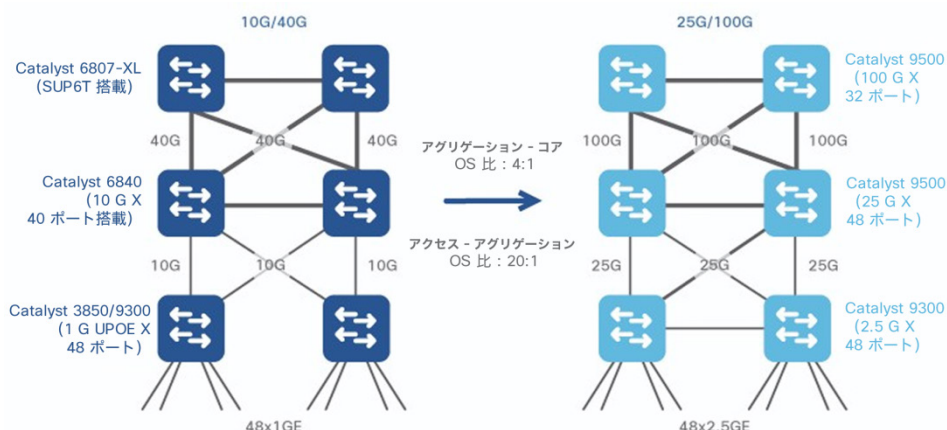
使用例 3 : 同じオーバーサブスクリプション率での速度移行

オーバーサブスクリプションに対するこれまでの推奨設計値の目安は、アクセス レイヤからディストリビューション レイヤでは ~ 20:1、ディストリビューション レイヤからコア レイヤでは ~ 4:1、コア レイヤでは ~ 2:1 または 1:1 でした。推奨されるオーバーサブスクリプション率を維持するためには、アクセス レイヤの帯域幅の増加 (例 : 2.5 G) に対応してスイッチ間の接続をアップグレードする必要があります。

結論

帯域幅が 2.5 倍以上増加しているのに、10/40 G から 25/100 G に移行するのは自然な流れです。

図 同じオーバーサブスクリプション率での速度移行



使用例 4 : 高速化対ロード シェアリング

速度のアップグレードのペースは、ケーブルの更新サイクルを上回っています。増大する帯域幅への要求に対応するには、基本的に次の 2 つのアプローチがあります。

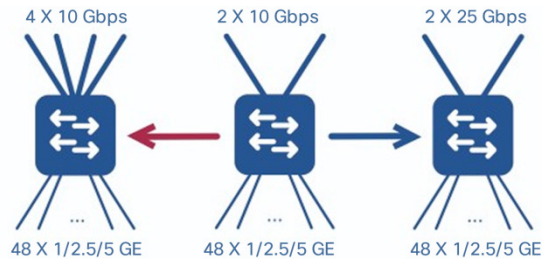
- アップリンクをさらに追加する (リンク アグリゲーションまたは ECMP を使用)
- より速いスピードに対応したケーブルとトランシーバに交換する

どちらのアプローチにも、大きな課題とコストへの影響があります。リンクを追加すると、効果的なロード シェアリングを実現する作業が複雑化し、QoS にも何らかの影響が出ます。高速リンク スピードにアップグレードする場合は、ロードシェアリングや QoS 上の課題はありませんが、トランシーバや配線の交換が必要になる可能性があります。

結論

Catalyst 9000 プラットフォームは、さまざまなポート速度で、一般的なポート タイプとトランシーバのセットをサポートしています。そのため、既存のインフラストラクチャを高速化することが非常に簡単です。

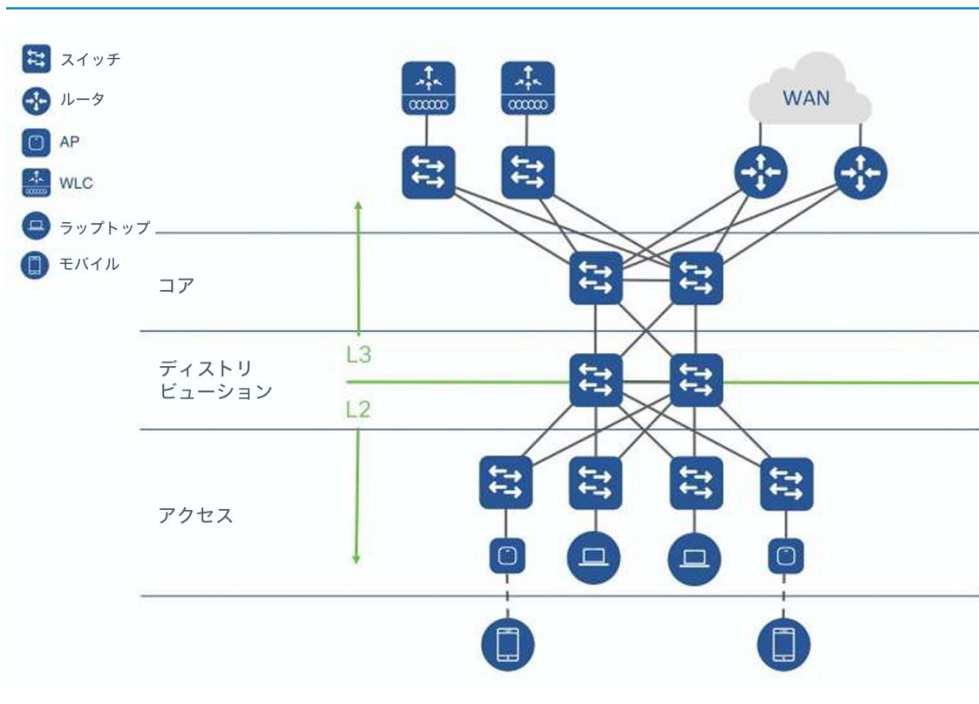
図 高速化対ロード シェアリング



マルチレイヤ キャンパス

マルチレイヤ LAN は、最も一般的に導入されている設計モデルです。コア、ディストリビューション、アクセスの3つのレイヤで構成されています。

図 マルチレイヤ キャンパス設計



マルチレイヤ キャンパス設計におけるコア レイヤは、他のネットワーク レイヤ（DC、WAN、ブランチなど）との高速相互接続ポイントとして、レイヤ 3 の IP ルーティングおよび機能をベースに設計されています。ディストリビューション レイヤは、コアに対する IP ルーティング アップストリームと、アクセス レイヤに対するレイヤ 2 スイッチング ダウンストリームで構成されています。ディストリビューション ブロックは、ネットワークの他の部分に転送されるクライアント トラフィックの集約ポイントとして機能し、スイッチングされたワイヤリング クローゼットをルーテッド コアに中継する役割を担います。アクセス レイヤの主な役割は、エンドポイントを接続し、そのトラフィックをネットワークの他の部分にスイッチングすることです。

この設計には、主に次のようないくつかの利点があります。

- 20 年間にわたって広く実装され、有効性を実証されている。
- 複数のレイヤから成る階層によって、各接続ブロックに特定の役割と責務が割り当てられる。
- 拡張性に優れたモジュラ型で、他のレイヤの設計に大きな影響を与えることなく、任意のレイヤでブロックを追加あるいは削除できる。
- アーキテクトが製品評価に使用する LAN スイッチの責務と、ネットワーク ポリシー構築に使用する LAN スイッチの責務が、分けて定義されている。
- 必要に応じて複数のアクセス ワイヤリング クローゼット間でスパニング VLAN（レイヤ 2 ドメイン）を形成することが可能であり、柔軟に設計できる。

ただし、この設計にもいくつか欠点があります。特に問題なのが、L2/L3 インターチェンジとしての役割を担うディストリビューション レイヤが、その役割のため複雑になってしまうことです。L2 ネットワークは、BUM トラフィック（Broadcast：ブロードキャスト、Unknown unicast：不明なユニキャスト、Multicast：マルチキャスト）用のフラッディング ドメインと見なされ、リンクに障害や再コンバージェンスが発生した際にループする可能性があります。L2 ネットワークが正しく調整されていない場合、BUM トラフィックが処理リソースを消費してしまったり、参加しているスイッチがパスの最適化を繰り返すことでネットワーク ループが生じてフローがブロックされたりすると、障害が発生します。

そのような状況に対応するためには、Rapid Per-VLAN Spanning Tree (RPVST)、スパニング ツリー プロトコル (STP) ループ ガード、IGMP スヌーピング、ストーム制御などのツールが使用されます。ただし、管理者がこれらの機能を有効化しモニタリングする必要があります。同様の状況は、アクセス レイヤ スイッチング境界を越えてルーテッド ネットワークにトラフィックを転送する際にも発生します。マルチレイヤ設計では、スパニング ツリーのスイッチングが IP ルーティングに適合しない (L2 と L3 のトポロジが一致しない) 場合、最適なパスが得られずフローが非対称となり、その結果、トラフィック フラッディングが発生する可能性があります。管理者は、First Hop Routing Protocol (FHRP) を使用して、スイッチに障害が発生した場合でも STP ルート スイッチが IP デフォルト ゲートウェイとしての機能も持つように、スイッチを設定する必要があります。

注 Catalyst 9000 シリーズ スイッチは、引き続きマルチ レイヤ ネットワークをサポートしていきます。また、その独自の機能は、リソース テンプレートによって各レイヤの役割に最適化されます。

Catalyst 9500 10/40 G モデルは、UADP 2.0 をベースにしており、ディストリビューション SDM テンプレートをデフォルトで使用して、ディストリビューション レイヤのロールに最適な ASIC テーブルを割り当てます。また、Catalyst 9500 10/25/40/100 G モデルは、UADP 3.0 をベースにしており、コア SDM テンプレートをデフォルトで使用して、コア スイッチに最適な ASIC テーブルを割り当てます。

結論

Catalyst 9500 シリーズ プラットフォームは、コアおよびディストリビューション レイヤに最適です。

Catalyst 9300/9400 シリーズ スイッチは、いずれも UADP 2.0 フォワーディング エンジンを採用し、アクセス SDM テンプレートを実装して、スイッチド アクセス ロールに最適な ASIC テーブルを割り当てます。スタックابلな固定フォーム ファクタの Catalyst 9300 は、スイッチレベルの冗長性を確保するために最適です。一方、モジュラ型スイッチの Catalyst 9400 は、スーパーバイザ、ラインカード、電源の冗長性を 1 つのシャーシに備えることで、最高レベルのネットワーク可用性を実現します。どちらのスイッチ製品ラインでも、小/中規模から大規模まで、さまざまな規模のワイヤリング クローゼットに対応できます。

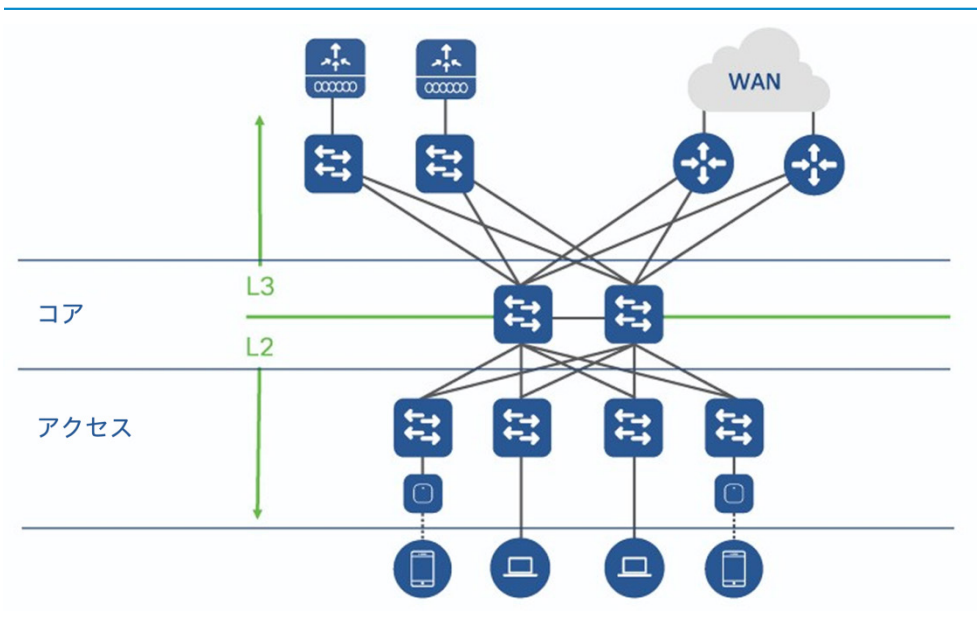
結論

Catalyst 9300/9400 シリーズ プラットフォームは、アクセス レイヤに最適です。

コラプスト コア

コラプスト コアは、小規模キャンパス ネットワーク向けのマルチレイヤ LAN と同じ原則に基づいて設計されており、コア レイヤとディストリビューション レイヤが相互にコラプス（統合）されています。

図 2 階層のコラプスト トポロジ



マルチレイヤ設計の利点は、コラプスト コアにもすべてあてはまります。必要なネットワーク インフラストラクチャが比較的少なく、コスト効率に優れた手頃なサイズの小規模サイト向けソリューションです。

欠点についても、マルチレイヤと同じことがこの設計にもあてはまります。つまり、ディストリビューション レイヤが複雑という前述の欠点が、コアにも該当します。

Catalyst 9500 シリーズ モデルでは、固定フォーム ファクタ設計の中に、プログラマブル UADP ASIC を採用しています。モデル間の違いはポート速度と密度の違いですが、すべてのモデルにおいて、ディストリビューション SDM テンプレートを使用することで、コラプスト コア スイッチとして使用する転送テーブルを最適化することができます。

結論

Catalyst 9500 シリーズ プラットフォームは、コラプスト コア レイヤに最適です。

この設計ではアクセス レイヤに関する変更点はなく、Catalyst 9300/9400 をアクセス レイヤに使用する際の推奨事項がそのままあてはまります。

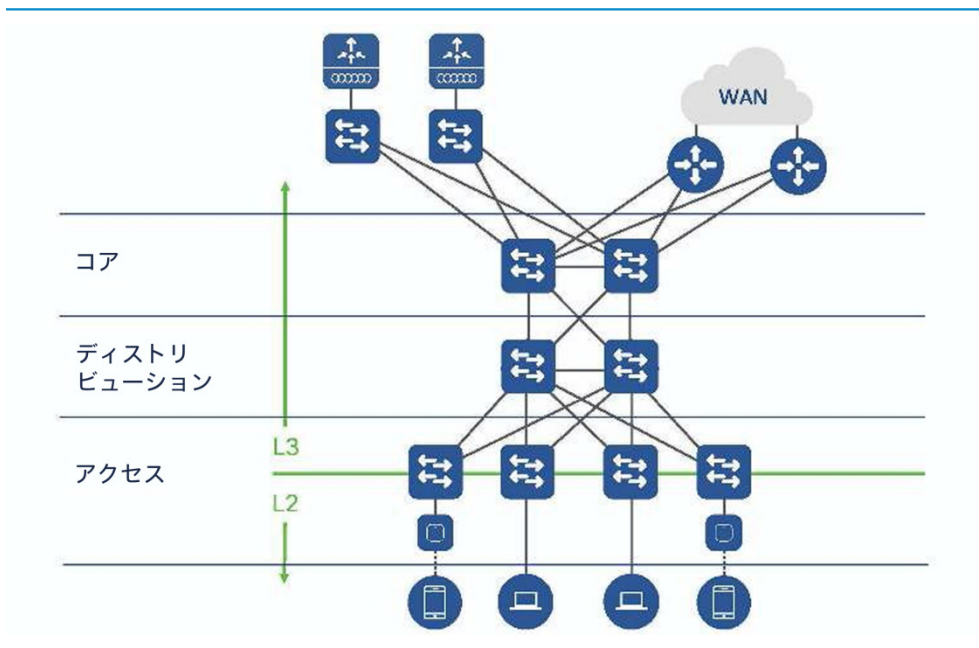
結論

Catalyst 9300/9400 シリーズ プラットフォームは、アクセス レイヤに最適です。

ルーテッド アクセス

ルーテッド アクセス設計では、従来のマルチレイヤ アーキテクチャと同じ物理ネットワーク トポロジが使用されます。これは、完全 3 層アーキテクチャが採用されている場合でも、コラプスト コア方式が採用されている場合でも同じです。両者の違いは、レイヤ 2 とレイヤ 3 の境界の位置にあります。名前が示すように、ルーテッド アクセス設計では、L3 境界がアクセス レイヤまで下がり、VLAN は各アクセス レイヤ スイッチ内のローカルに配置されます。これらのスイッチは、ルーテッド アップリンクを使用して、キャンパス ネットワークにアップストリーム方向に接続します。

図 ルーテッド アクセス設計



ルーテッド アクセス設計を使用することで、次のようなさまざまなメリットが得られます。

- すべてのネットワーク リンクが一貫した設定によるルーテッド接続であるため、導入と管理がシンプルになる。
- 802.1Q トランクを設定したり、レイヤ間でスパニング ツリー プロトコルと First Hop Routing Protocol を調整したりする必要がなくなる。
- 単一の制御プロトコルによってネットワークの動作を管理できるため、ネットワークの運用とトラブルシューティングがシンプルになる。
- L2 ドメインをアクセス レイヤに移行し、STP ドメインを各スイッチに分離することで、障害ドメインが大幅に減少する。
- 利用可能なすべてのネットワーク パスを、より効率的に利用できる。ルーテッド アクセス ネットワークは、STP ブロッキングを適用せず、代わりに Equal Cost Multipath (ECMP; 等コスト マルチパス) を使用して、フローをアクセス レイヤからアップストリーム方向にすべての接続間で自動的に分配する。

ルーテッド アクセス ネットワークにはいくつか欠点があります。ルーテッド アクセス設計モデルでは、キャンパス ネットワーク全体に VLAN を展開することはできません。大規模な L2 ドメインはネットワークの安定性を損なう恐れがあるため、キャンパス設計ではそれを除外することがベスト プラクティスとされますが、ときには、MAC レイヤのみで稼働しているシステムを相互に接続するためにそれが必要となる場合もあります。ルーテッド アクセス設計にはもう 1 つ欠点があります。ACL が実装されている場合、ACL を階層型設計のディストリビューション レイヤで一元的に管理するのではなく、アクセス レイヤに分散させる必要があるということです。

ルーテッド アクセス ネットワークでは、階層型と同じトポロジを利用します。そのため、Catalyst 9000 シリーズ プラットフォームの位置付けも同じです。Catalyst 9500 スイッチは、固定フォームのディストリビューションおよびコアとして最適で、Catalyst 9300/9400 は、アクセス レイヤ スイッチとして最適です。9300/9400 を L2 スイッチとして最適化する SDM テンプレートに加え、L3 アクセス用に最適化するためのプログラム変更を実施するテンプレートも用意されています。

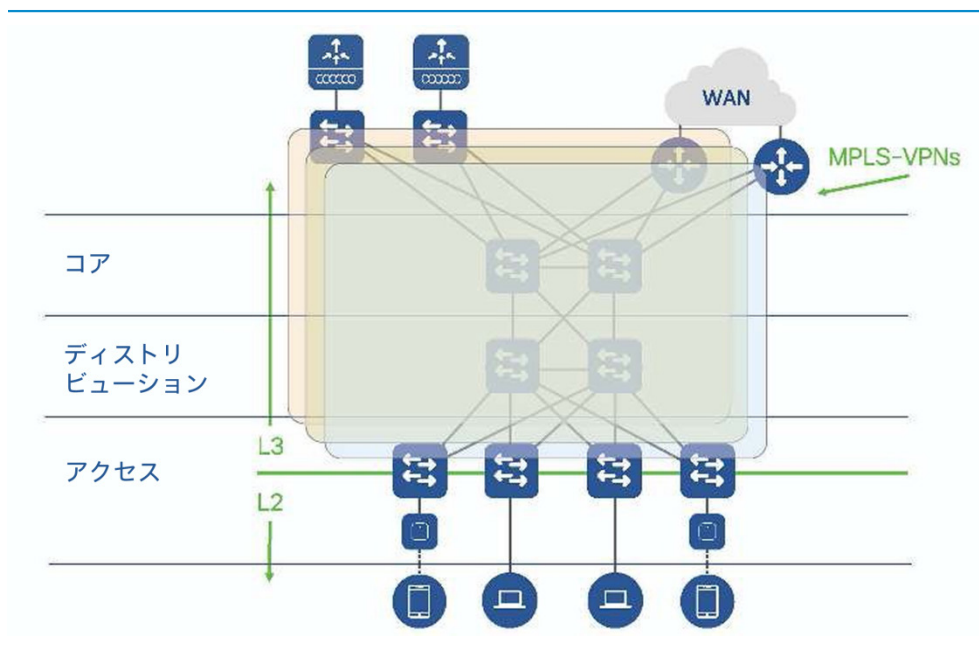
結論

Catalyst 9000 シリーズでは、すべてのスイッチがルーテッド アクセス ネットワーク向けに最適化されています。

キャンパス MPLS

キャンパス MPLS 設計は、以前のネットワーク設計をベースに構築され、ルーティング ドメインを仮想的に分離します。そのためには、ネットワーク内のすべてのルーテッド ポイントの上に MPLS-VPN 技術をオーバーレイする必要があります。マルチレイヤ キャンパスの場合、MPLS はディストリビューション ブロックからネットワーク コアを通して拡張し、ルーテッド アクセス設計では、MPLS は LAN 全体に展開します。

図 キャンパス MPLS



MPLS-VPN をキャンパス設計に導入する主な利点として、マクロレベルのネットワーク セグメンテーションがあります。MPLS-VPN は、Virtual Routing and Forwarding (VRF) インスタンスを使用して、ルーティング ドメインを分離します。たとえば、企業のプライベート セグメントへのアクセスをゲスト トラフィックに許可しないことなどが可能になります。キャンパス MPLS ネットワークにおいても、ネットワーク管理者が MPLS プロトコルを操作することで、たとえば、基本的なルーティングでのラベル スイッチングの効率を向上させたり、ネットワーク内でトラフィックを誘導してパスを最適化（いわゆる MPLS-TE またはトラフィック エンジニアリング）したりすることなどが可能です。

ただし、MPLS では、MPLS アーキテクチャのプロバイダー エッジ (PE) デバイス間で必要な VRF 情報を交換するために、（マルチプロトコル BGP に基づく）コントロール プレーンを追加する必要があるため、IP ネットワークが複雑になります。複数の仮想ルーティング ドメインを作成して管理するためには、アーキテクトによる適切な設計と、オペレータの管理知識が必要になります。設計段階では、LAN 用に選択した機器が L2、L3、さらには MPLS プロトコルにも対応できるか評価する必要があります。運用段階においては、ネットワーク管理者が、MPLS プロトコルやそのルールを理解して、複数のルーティング プレーンでトラブルが同時発生した場合にも対応できるようにしておく必要があります。

簡易な方法としては、VRF-Lite をエンドツーエンドで導入することで、MPLS タギングなしで VRF を使用してネットワークのセグメンテーションを実現することができます。VRF-Lite は、スイッチ間で 802.1Q トランクと VLAN ID を活用して、異なる VRF に存在するトラフィックを区別して転送します。VRF-Lite は小規模には適していますが、VRF が 8 ~ 10 を超えると急に、管理が過度に難しくなります。キャンパスまたは WAN 内をセグメント化することに加えて、この VRF 数を超える拡張が必要になった場合、従来は、さらに複雑な（ただし拡張性に優れている）MPLS-VPN ソリューションが選択されていました。

セグメンテーションに対する企業の要件は、より厳しいものになりつつあります。MPLS-VPN は、マクロセグメンテーションには対応しているものの、アクセス制御ポリシーを使用したマイクロセグメンテーションには対応していません。現在のセキュリティ チームでは、同じルーティング ドメインに属するホスト間でポリシーを適用することが必要になっています。（VRF を使用した）マクロセグメンテーションと（拡張可能グループ タグ (SGT) を使用した）マイクロセグメンテーションを組み合わせる機能については、第 14.8 章「SD-Access」で詳細に説明します。

Catalyst 9000 はシリーズ全体でキャンパス MPLS をサポートしています。ルーテッド アクセス ネットワークと同様の推奨事項があてはまり、その上に MPLS 機能のサポートが追加されています。Catalyst 9500 プラットフォームは、コアおよびディストリビューション レイヤ サービス向けに設計されており、Catalyst 9300/9400 スイッチ製品ラインは、アクセス デバイスとして最適です。

結論

Catalyst 9000 シリーズでは、すべてのスイッチがキャンパス MPLS ネットワーク向けに最適化されています。

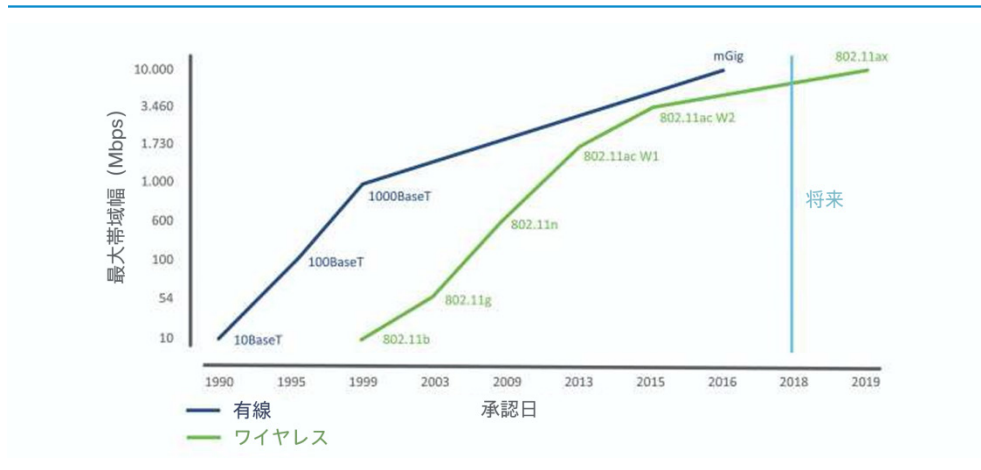
キャンパス ワイヤレス

Catalyst 9000 スイッチは、独自の機能やイノベーションを多彩に提供し、有線 LAN アクセスと最適なワイヤレス アクセスのいずれにも対応可能です。

802.11 ワイヤレス LAN (Wi-Fi) は、アクセス レイヤ技術の 1 つです。Wi-Fi は急速に、ユーザが自分のクライアント マシンを接続する際の標準的な選択肢になってきています。ユーザは、より迅速に作業を完了させるために、自分のコンピュータやスマホを持ち歩きたいと考えています。ユーザにとってモビリティは、生産性と効率性を向上させるための強力なツールです。

今や最新のワイヤレス環境によって、有線インフラストラクチャに匹敵する（もしくは凌駕する）リンク スピードが得られるようになっていました。現在、802.11ac Wave 2（将来的には 802.11ax）を使用したワイヤレス環境では、マルチギガビット ワイヤレス リンク スピードが実現されています。

図 有線およびワイヤレスの進化



企業は、このようなモビリティのトレンドを認識しており、モバイル ワーカーのニーズを満たすだけでなく、予算を最適化して固定エンドポイントとモバイル エンドポイントの適切なバランスを実現するためにも、ワイヤレスのみのオフィスへの移行を試んでいます。また、このワイヤレス アクセス志向のトレンドに対応するためにはより柔軟な有線インフラストラクチャが必要であるということも、認識する必要があります。

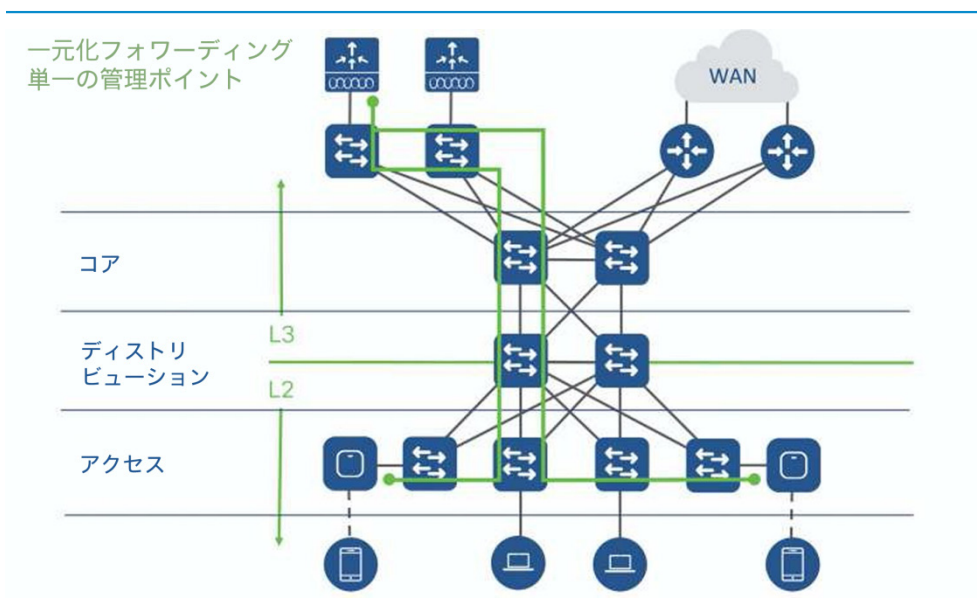
結論

802.11ac Wave 2 導入の増加に対応して、スイッチは、mGig や 25 G、100 G などのより高速な接続スピードをサポートする必要があります。

マルチレイヤ キャンパス設計では、一元化されたワイヤレス ネットワークにワイヤレス LAN コントローラ (WLC) が使用されます。WLC は通常、コア (またはリモート データセンターの場合もあり得る) に接続されているサービス ブロックにおいて、キャンパス ディストリビューション レイヤまたはコア レイヤのいずれかで接続します。ワイヤレス アクセス ポイント (AP) は、一般的に PoE および高速銅線イーサネットを使用してアクセス レイヤ スイッチに接続します。

この設計では、WLC が中央の管理ポイントになります。ワイヤレス AP の設定とモニタリングはすべて、WLC で行われます。AP は、受信したすべてのデータ トラフィックを WLC にトンネリングし、転送およびポリシーに関するすべての判断を行うよう要求します。つまり WLC は、L2 ワイヤレス アクセスの境界になり、ローカルの L3 ルーティングの境界と接続されます。この手法によって、ワイヤレス クライアントは、AP 間で L2 ローミングしながらも、ネットワークには同じ L3 サブネット内で接続されているように認識させることができます。

図 一元化 WLAN 設計



一元化ワイヤレス ネットワーク設計では、ネットワーク管理者が何百台もの AP を単一の管理ポイントから設定することができます。一元化設計は、802.11 ネットワークにおけるローミングの課題も解決します。ルーティング境界を超えてワイヤレス ネットワークを拡張する代わりに、WLC が、ネットワーク内の単一のポイントでワイヤレス ネットワークを統合します。

このアプローチには 1 つの課題があります。ワイヤレス LAN と他の有線ネットワークは、やはり別々に管理されるということです。可能であれば、すべてのエンドポイントに単一のポリシーを定義して、アクセス メディアに関係なくそのポリシーを同じ方法で適用できれば理想的です。ワイヤレスと有線が分離されていると、無駄な作業の重複が発生し、設定を間違える可能性があります。

もう 1 つの問題は、ネットワークの拡張性です。AP がすべてのデータを中央の WLC に転送する際、コントローラがトラフィックの全負荷を処理できる必要があります。WLC が 1 Gbps または 10 Gbps のリンクを複数使用して接続し、AP が限られた数のクライアントを 10 Mbps または 100 Mbps で接続している環境では、これは問題視されてきませんでした。802.11ac Wave 2 が導入されると、WLC は、1 Gbps を超えるスピードで接続できる何百台ものクライアントに対応するために、10 Gbps のリンクを複数サポートすることが必要になります。そのために、WLC に接続するスイッチには、より多くの帯域幅と、より高いポート密度が求められます。

結論

Catalyst 9000 シリーズでは、すべてのスイッチがキャンパス ワイヤレス ネットワーク向けに最適化されています。

SD-Access (Software-Defined Access) は、有線とワイヤレス双方の LAN 環境に対する革新的なアプローチを提案しています。SD-Access は、一元管理の利点をそのまま保持しながら、ポリシーの共通化と拡張性に対応しています。

SD-Access

シスコの SD-Access (Software-Defined Access) ソリューションは、ネットワークのエッジからアプリケーションまでソフトウェアベースのポリシーとセグメンテーションを提供する、プログラマブル ネットワーク アーキテクチャです。SD-Access は、Cisco DNA Center (Cisco Digital Network Architecture Center) を使って導入されます。この Cisco DNA Center は、ネットワーク要素の設計の設定、ポリシー定義、自動プロビジョニングを提供するとともに、インテリジェントな有線およびワイヤレス ネットワーク向けのアシュアランス分析を提供します。

図 SD-Access ソリューションの概要



SD-Access は、論理オーバーレイ ファブリック ネットワークを構築して、キャンパス上の場所に関係なく、ホスト モビリティ、セグメンテーション、グループベース ポリシーによるメリットを提供します。これは、Cisco DNA Center によって完全に自動化され保証されています。

Catalyst 9000 シリーズ プラットフォームは、Cisco SD-Access の物理レイヤとネットワーク レイヤに参加します。SD-Access ネットワーク レイヤ（ファブリック）は、主に次の 2 つのコンポーネントで構成されています。

- **ネットワーク アンダーレイ**：従来の階層型レイヤ 3 ルーテッド ネットワークに類似していますが、ファブリック オーバーレイを実現するためにネットワーク デバイス間でデータ パケットを伝送することに重点を絞っています。設計の観点からするとルーテッド アクセス設計と同じです。
- **ファブリック オーバーレイ**：基本的には論理（トンネル）ネットワーク。すべてのネットワーク デバイスを仮想で相互接続します（「ファブリック」を形成します）。ファブリック オーバーレイによって仮想環境が構築され、マクロレベル/マイクロレベルのセグメンテーション、グループ ベースのセキュリティおよびアプリケーション ポリシー、有線およびワイヤレス クライアントに対する動的ホスト モビリティ サービスが可能になります。

SD-Access ワイヤレス

SD-Access では、ワイヤレス データを有線データとまったく同じように扱います。このアプローチにより、両方のメディアでポリシーを共通化することができます。ワイヤレス ネットワークのコントロール プレーンは引き続き一元化されています。ただし、ワイヤレス データプレーンに関しては、SD-Access では転送処理がスイッチ インフラストラクチャを介してローカルの分散型転送モデルに移行されます。すべてのクライアント トラフィックをコントローラにトンネリングする代わりに、各アクセス ポイントが、接続するファブリック エッジスイッチに VXLAN トンネルを直接構築します。スイッチは、このトラフィックを終端し、その後ワイヤレス トラフィックに対して、有線ホストと同じような完全処理を実施します。処理には、VN や SGT を中心として構造化されたグループベースのポリシーなどが含まれます。

SD-Access ワイヤレスの主な利点には次のようなものがあります。

- **一元化されたコントロールプレーン**：AP 管理、RRM、クライアント オンボーディング、ローミングなどのワイヤレス インフラストラクチャの動作は、一元管理されたワイヤレス ネットワーク内で行われます。
- **分散型データプレーン**：ワイヤレス データトラフィックは、最適なパフォーマンスと拡張性を実現するために、ファブリック エッジ スイッチに分散されます。
- **シームレスな L2 ローミング**：クライアントは、元の IP アドレスとグループ ポリシーを維持しながら、キャンパス全体に展開された VN 内でシームレスにローミングできます。
- **シンプルなポリシー適用**：SD-Access では、ポリシーとネットワーク構成要素の間には依存関係がなく、有線およびワイヤレスのエンドポイント全体でそれがアプリケーションに対して抽象化されています。

Cisco SD-Access の詳細については、www.cisco.com/go/sdaccess を参照してください。

SD-Access によってオーバーレイが構築されると、ネットワーク デバイスは、LISP、VXLAN、SGT などの新しいカプセル化方式やプロトコルをサポートする必要があります。

Catalyst 9500 シリーズに SDA SDM テンプレートを使用させる設定を行うことができます。それにより、SD-Access ファブリック ボーダー ロールに ASIC テーブルが適切に割り当てられます。柔軟性に優れた UADP ASIC によって、VXLAN-GPO フレーム カプセル化や統合 SGT ベースの ACL 分類/適用のほか、新しい数多くの SD-Access 機能が実現します。

結論

Catalyst 9500 シリーズ プラットフォームは、SD-Access ファブリック ボーダー ロールに最適です。

Catalyst 9300/9400 シリーズに SDA SDM テンプレートを使用させる設定を行うことができます。それにより、SD-Access ファブリック エッジ ロールに ASIC テーブルが適切に割り当てられます。柔軟性に優れた UADP ASIC によって、SD-Access ワイヤレスへの直接 AP VXLAN トンネリングなどを含め、VXLAN-GPO フレーム カプセル化や統合 SGT ベースの ACL 分類/適用が実現します。

結論

Catalyst 9300/9400 シリーズ プラットフォームは、SD-Access ファブリック エッジ ロールに最適です。

付録

参考資料

Catalyst 9000 ファミリおよびその機能に関する詳細情報が提供されているその他の Web サイト :

Cisco Catalyst 9000 ファミリの概要 :

https://www.cisco.com/c/ja_jp/products/switches/catalyst-9000.html

Cisco Catalyst 9000 シリーズ スイッチの概要 :

https://www.cisco.com/c/ja_jp/products/switches/catalyst-9300-series-switches/index.html

https://www.cisco.com/c/ja_jp/products/switches/catalyst-9400-series-switches/index.html

https://www.cisco.com/c/ja_jp/products/switches/catalyst-9500-series-switches/index.html

Cisco Catalyst 9000 シリーズ スイッチ ホワイト ペーパー :

<https://www.cisco.com/c/en/us/products/switches/catalyst-9300-series-switches/white-paper-listing.html>

<https://www.cisco.com/c/en/us/products/switches/catalyst-9400-series-switches/white-paper-listing.html>

<https://www.cisco.com/c/en/us/products/switches/catalyst-9500-series-switches/white-paper-listing.html>

Cisco Live オンデマンド ライブラリ :

[https://www.ciscolive.com/global/on-demand-library/?#\[英語\]](https://www.ciscolive.com/global/on-demand-library/?#[英語])

以下のセッション ID を検索してください。

BRKARC-2035 : The Catalyst 9000 Switch Family – An Architectural View (Catalyst 9000 スイッチ ファミリ - アーキテクチャ ビュー)

BRKARC-3467 : Cisco Enterprise Silicon – Delivering Innovation for Advanced Routing and Switching (Cisco Enterprise Silicon - 高度なルーティングとスイッチングのためのイノベーション)

BRKARC-3863 : Catalyst 9300 Switching Architecture (Catalyst 9300 スイッチング アーキテクチャ)

BRKARC-3873 : Catalyst 9400 Switching Architecture (Catalyst 9400 スイッチング アーキテクチャ)

BRKCRS-3300 : IOS XE: Enabling the Cisco Digital Network Architecture (IOS XE : Cisco Digital Network Architecture の実現)

Catalyst 9000 ファミリのプログラマビリティおよび自動化に関する詳細情報が提供されているその他の Web サイト :

DevNet (Cisco Developer Network) :

<https://developer.cisco.com/>[英語]

<https://developer.cisco.com/site/ios-xe>[英語]

Cisco Live オンデマンド ライブラリ :

<https://www.ciscolive.com/global/on-demand-library/?#/>[英語]

以下のセッション ID を検索してください。

BRKCRS-1450 : Introduction to Catalyst Programmability (Catalyst プログラマビリティについて)

BRKCRS-2451 : Scripting Catalyst switches—tools and techniques beyond the basics (Catalyst スイッチのスクリプティング - 高度なツールおよび手法) BRKCRS-2004 : Application Hosting and Model-Driven Telemetry on Open IOS XE (オープン IOS XE におけるアプリケーション ホスティングおよびモデル駆動型テレメトリ)

略語

AAA : Authentication, Authorization and Accounting (認証、許可、アカウントティング)

ACK : Acknowledgement (確認応答)

ACL : Access Control List (アクセス コントロール リスト)

AES : Advanced Encryption Standard

AOC : Active Optical Cables (アクティブ 光ケーブル)

API : Application Programming Interface (アプリケーション プログラミング インターフェイス)

AQM : Active Queue Management (アクティブ キュー管理)

AR : Augmented Reality (拡張現実)

ARP : Address Resolution Protocol

ASIC : Application-Specific Integrated Circuit (特定用途集積回路)

AVB : Audio Video Bridging (オーディオ ビデオ ブリッジング)

AVC : Application Visibility and Control (アプリケーションの可視性と制御)

BGP : Border Gateway Protocol

BOOTP : Bootstrap Protocol (ブートストラップ プロトコル)

BPDU : Bridge Protocol Data Unit (ブリッジ プロトコル データ ユニット)

BUM : Broadcast Unknown unicast Multicast (ブロードキャスト、不明なユニキャスト、マルチキャスト)

BYOD : Bring Your Own Device (個人所有 デバイスの持ち込み)

CAF : Cisco Application Framework (シスコ アプリケーション フレームワーク)

CAPWAP : Control And Provisioning of Wireless Access Points

CDP : Cisco Discovery Protocol

CEF : Cisco Express Forwarding

CI/CD : Continuous Integration, Continuous Delivery (継続的統合、継続的導入)

CLI : Command Line Interface (コマンドライン インターフェイス)

CoS : Class of Service (サービス クラス)

CPU : Central Processing Unit (中央処理装置)

CSMA/CD : Carrier Sense Multiple Access with Collision Detection (キャリア検知多重アクセス/衝突検出)

CTA : Cisco Trust Anchor

CTA : Cognitive Threat Analytics

CoA : Change of Authorization (認可変更)

DAC : Direct Attach Copper (直接接続銅線)

DAD : Dual-Active Detection Link (デュアルアクティブ検出リンク)

DHCP : Dynamic Host Configuration Protocol

DIY : Do-It-Yourself (各社の独自開発)

DMZ : DeMilitarized Zone (緩衝地帯)

Cisco DNA : Cisco Digital Network Architecture

DNS : Domain Name System (ドメインネーム システム)

DNS-AS : DNS as Authoritative Source (信頼できるソースとしての DNS)

DPI : Deep Packet Inspection (ディープパケット インスペクション)

DSCP : Differentiated Services Code Point (DiffServ コード ポイント)

DTLS : Datagram Transport Layer Security

DTP : Dynamic Trunk Protocol (動的トラUNK プロトコル)

DTS : Dynamic Threshold Scheduler (動的しきい値スケジューラ)

EAP - ECC : Error-Correcting Code (エラー訂正コード)

EAPoL : Extensible Authentication Protocol over LAN (LAN 上で動作する拡張可能な認証プロトコル)

EARL : Encoded Address Recognition Logic (暗号化アドレス認識ロジック)

ECMP : Equal-Cost Multipathing (等コスト マルチパス)

ECN : Explicit Congestion Notification (明示的輻輳通知)

EFC : Egress Forwarding Controller (出力転送コントローラ)

EGR : Egress Global Resolution (出力グローバル解決)

EIGRP : Enhanced Interior Gateway Routing Protocol

ELLW : Enhanced Limited-Lifetime Warranty (拡張版制限付きライフタイム保証)

EQS : Egress Queuing Scheduler (出力キューイング スケジューラ)

ERSPAN : Encapsulated Remote

Switched Port Analyzer (カプセル化リモート スイッチド ポート アナライザ)

ETA : Encrypted Traffic Analytics (暗号化トラフィック分析)

FIB : Forwarding Information Base (転送情報ベース)

FIFO : First In First Out (先入れ先出し)

FNF : Flexible NetFlow

FPGA : Field Programmable Gate Array (フィールド プログラマブル ゲート アレイ)

FSU : Fast Software Upgrade

FTP : File Transfer Protocol

GIR : Graceful Insertion and Removal (グレースフル挿抜)

gNMI : google Network Management Interface (google ネットワーク管理インターフェイス)

GPE : Generic Protocol Extension (一般プロトコル拡張)

GPO : Group Policy Object (グループ ポリシー オブジェクト)

GRE : Generic Routing Encapsulation

gRPC : google Remote Procedure Call (google リモート プロシージャ コール)

Gbps : Gigabits per second (ギガビット/秒)

HA : High Availability (高可用性)

HQoS : Hierarchical QoS (階層型 QoS)

HSRP : Hot Standby Router Protocol

HTTP : Hypertext Transfer Protocol

HVAC : Heating Ventilation and Air Conditioning (冷暖房空調設備)

HW : Hardware (ハードウェア)

IBNS : Identity-Based Networking Services

IDP : Initial Data Packet (初期データパケット)

IEEE : Institute of Electrical and Electronics Engineers (電気電子学会)

IETF : Internet Engineering Task Force (インターネット技術特別調査委員会)

IFC : Ingress Forwarding Controller (入力転送コントローラ)

IGMP : Internet Group Management Protocol

IGR : Ingress Global Resolution (入力グローバル解決) IPsec : Internet Protocol security (インターネット プロトコル セキュリティ)

ILP : Inline Power (インライン パワー)

IPFIX : IP Flow Information Export (IP フロー情報エクスポート)

IPTV : Internet Protocol Television (インターネット プロトコル テレビジョン)	MACsec : Media Access Control security
IQS : Ingress Queuing Scheduler (入力キューイング スケジューラ)	MDT : Model Driven Telemetry (モデル駆動型テレメトリ)
IS-IS : Intermediate System-to-Intermediate System	MEC : Multi-Chassis EtherChannel (マルチシャーシ EtherChannel)
ISE : Identity Services Engine	MFIB : Multicast Forwarding Information Base (マルチキャスト 転送情報ベース)
ISSU : In-Service Software Upgrade (インサービス ソフトウェア アップグレード)	mGIG : multigigabit (マルチギガビット)
IoT : Internet of Things	MKA : MACsec Key Agreement (MACsec 鍵合意)
JSON : JavaScript Object Notation (JavaScript オブジェクト表記)	MLD : Multicast Listener Discovery (マルチキャスト リスナー検出)
KVM : Kernel-based Virtual Machine (カーネルベースの仮想マシン)	MMF : Multi-Mode Fiber (マルチモード ファイバ)
LACP : Link Aggregation Control Protocol	MPLS : Multiprotocol Label Switching (マルチプロトコル ラベル スイッチング)
LAN : Local Area Network (ローカル エリア ネットワーク)	MSB : Most Significant Bits (最上位ビット)
LDP : Label Distribution Protocol (ラベル配布プロトコル)	MTU : Maximum Transmission Unit (最大伝送ユニット)
LED : Light-Emitting Diode (発光ダイオード)	MBPS : Megabits Per Second (1 秒当たりのメガビット数)
LISP : Locator/ID Separation Protocol	NAT : Network Address Translation (ネットワーク アドレス変換)
LXC : Linux Container (Linux コンテナ)	NBAR : Network-Based Application Recognition
MAB : MAC Authentication Bypass (MAC 認証バイパス)	NSF : Non-Stop Forwarding (ノンストップフォワーディング)
MAC : Media Access Control	

NSH : Network Services Headers (ネットワーク サービス ヘッダー)	POE : Power Over Ethernet
NSO : Network Service Orchestrator	pps : packets per second (1 秒あたりのパケット数)
OIR : Online Insertion and Removal (活性挿抜)	PSU : Power Supply Unit (電源装置)
OM : Optical Multimode (光マルチモード)	PXE : Preboot Execution Environment (ブート前実行環境)
onePK : one Platform Kit	PnP : Network Plug and Play (ネットワーク プラグ アンド プレイ)
OS : Operating System (オペレーティングシステム)	QSA : QSFP to SFP Adapter (QSFP - SFP 変換アダプタ)
OSI : Open Systems Interconnection model (開放型システム間相互接続)	QSFP : Quad Small Form-factor Pluggable
OSPF : Open Shortest Path First	QoS : Quality of Service (サービス品質)
P2P : Peer-to-Peer (ピアツーピア)	RADIUS : Remote Authentication Dial-In User Service (リモート認証ダイヤルイン ユーザ サービス)
PAgP : Port Aggregation Protocol (ポート集約プロトコル)	RED : Random Early Discard (ランダム早期廃棄)
PBC : Packet Buffer Complex (パケットバッファ複合)	REST : REpresentational State Transfer
PBR : Policy-Based Routing (ポリシーベース ルーティング)	RFC : Request For Comments
PDU : Protocol Data Unit (プロトコルデータ ユニット)	RFID : Radio Frequency Identification (無線 IC タグ)
PE : Provider Edge router (プロバイダーエッジ ルータ)	RNG : Random Number Generators (乱数ジェネレータ)
PHY : PHYsical layer (物理層)	RPC : Remote Procedure Call (リモートプロシージャ コール)
PMK : Pair-wise Master Key (ペアワイズマスター キー)	RPM : RPM Package Manager (RPM パッケージ マネージャ)

rpm : revolutions per minute (1 分間当たりの回転数)

RSPAN : Remote Switched Port Analyzer (リモート スイッチド ポート アナライザ)

SAP : Security Association Protocol (セキュリティ アソシエーション プロトコル)

SATA : Serial AT Attachment (シリアル AT アタッチメント)

SD-Access : Software Defined Access

SDK : Software Development Kit (ソフトウェア開発キット)

SDM : Switch Database Manager (スイッチ データベース マネージャ)

SFP : Small Form-factor Pluggable

SGACL : Scalable Group Access Control List (拡張可能グループ アクセス コントロール リスト)

SGFW : Security Group Firewall (セキュリティ グループのファイアウォール)

SGT : Scalable Group Tag (拡張可能グループ タグ)

SGTIN : Serialized Global Trade Item Number (シリアル番号付きグローバル商品識別コード)

SIP : Session Initiation Protocol

SKU : Stock Keeping Unit (最小在庫管理単位)

SLI : Switch Link Interface (スイッチ リンク インターフェイス)

SMC : Stealthwatch Management Console (Stealthwatch 管理コンソール)

SMF : Single Mode Fiber (シングル モード ファイバ)

SMU : Software Maintenance Update (ソフトウェア メンテナンス更新)

SNMP : Simple Network Management Protocol

SPAN : Switched Port Analyzer (スイッチド ポート アナライザ)

SPLT : Sequence of Packet Lengths and Times (パケット長と時間のシーケンス)

SQS : Stack Queue Scheduler (スタック キュー スケジューラ)

SRAM : Static Random-Access Memory (静的ランダム アクセス メモリ)

SRP : Spatial Reuse Protocol (スペース再利用プロトコル)

SSD : Solid-State Drive (ソリッド ステート ドライブ)

SSH : Secure Shell (セキュア シェル)

SSO : Stateful Switchover (ステートフル スイッチオーバー)

ST : Service Template (サービス テンプレート)

STP : Spanning Tree Protocol (スパニング

ツリー プロトコル)

SUDI : Secure Unique Device Identifier
(セキュアな固有デバイス識別子)

SVL : Stackwise Virtual Link (Stackwise
Virtual リンク)

SW : Software (ソフトウェア)

SXP : SGT Exchange Protocol (SGT 交換
プロトコル)

TAC : Technical Assistance Center (テク
ニカル アシスタンス センター)

TCAM : Ternary Content Addressable
Memory

TCO : Total Cost of Ownership (総所有コ
スト)

TCP : Transmission Control Protocol (伝
送制御プロトコル)

TFTP : Trivial File Transfer Protocol (トリ
ビアル ファイル転送プロトコル)

TLS : Transport Layer Security

TTL : Time to Live (存続可能時間)

ToS : Type of Service (タイプ オブ
サービス)

UADP : Unified Access Data Plane (ユニ
ファイド アクセス データ プレーン)

UDLD : Unidirectional Link Detection
(単方向リンク検出)

UDP : User Datagram Protocol (ユーザ

データグラム プロトコル)

UHF : Ultra High Frequency (超高周波)

UI : User Interface (ユーザ インターフェ
イス)

UPoE : Universal Power over Ethernet

URL : Uniform Resource Locator

USB : Universal Serial Bus (ユニバーサル
シリアル バス)

VLAN : Virtual LAN (仮想 LAN)

VM : Virtual Machine (仮想マシン)

VN : Virtual Network (仮想ネットワーク)

VR : Virtual Reality (仮想現実)

VRF : Virtual Routing and Forwarding (仮
想ルーティングおよびフォワーディング)

VRRP : Virtual Router Redundancy
Protocol

VTP : VLAN Trunk Protocol (VLAN トラン
ク プロトコル)

VXLAN : Virtual eXtensible LAN (仮想拡張
LAN)

WAN : Wide Area Network (ワイドエリア
ネットワーク)

WLC : Wireless LAN Controller (ワイヤレ
ス LAN コントローラ)

WRED : Weighted Random Early Discard
(重み付けランダム早期廃棄)

WRR : Weighted Round Robin (加重ラウンド ロビン)

WSMA : Web Services Management Agent
(Web サービス管理エージェント)

WTD : Weighted Tail Drop (重み付けテール ドロップ)

XFP : 10 Gigabit Small Form Factor
Pluggable

XML : Extensible Markup Language (拡張
マークアップ言語)

YANG : Yet Another Next Generation

YDK : YANG Development Kit (YANG 開発
キット)

ZTP : Zero-Touch Provisioning (ゼロタッチ
プロビジョニング)

Bob Sayle
Dave Zacks
Dimitar Hristov
Fabrizio Maccioni
Ivor Diedricks
Jay Yoo
Kenny Lei
Mahesh Nagireddy
Minhaj Uddin
Muhammad Imam
Sai Zeya
Shawn Wargo