LightReading
www.lightleading.com

レポート
2015 年 3 月

テスト
パートナー: EANTC

参加企業名: CISCO

シスコのサービス プロバイダー仮想化およびクラウド ポートフォリオの検証

目次

概要

現在、すべてのコミュニケーション サービス プロバイダー（CSP）が直面する大きな課題は次のようなものです。高度な自動化機能を持ち、新しいサービスを迅速に設定してアクティブ化することができる、また、新しいクラウド機能を最大限に活用して、カスタマーのニーズを満たしながら利益をもたらす、プログラム可能で、インテリジェントで、反応が良く、効率的で、柔軟で、セキュアかつオープンなネットワークを構築し、実行するにはどうすればよいのか。

イギリスのサッカー界では、これは「大望」だと言われています。

そうです、大きな課題ですが、乗り越えられないものではありません。グローバルの通信およびネットワーク テクノロジー 業界には、この課題を探求し、日々ソリューションを考案しているスマートで革新的な企業がたくさんあります。CSP が知りたいことは、これらの先端的な、次世代 New IP 技術が、現在の、そして将来のニーズを満たすことができるかどうか、ということです。グローバル通信技術コミュニティの中心において、信頼できる独立メディアの Light Reading は、これらの非常に重要な質問に答えるのに最適な企業です。

その役割の一環として、Light Reading は別の独立した信頼できる組織である European Advanced Networking Test Center（EANTC）に、カリフォルニア州サンノゼにあるシスコを訪問し、そこでシスコが過去数年に渡り開発してきた数多くのシスコ クラウド、ソフトウェア定義型ネットワーキング、および仮想化プラットフォームに対して、CSP の立場にたって一連の検証および確認試験を実施するよう依頼しました。

EANTC チームはシスコの施設で 2 週間かけていくつものテストを実行し、多くの重要な質問を投げかけ、実施した内容やその理由、それに実施結果を記録しました。

このレポートはその 2 週間の結果です。次のページには、ネットワーク オペレータ チームと同じ方法で、EANTC チームがシスコの技術をどのように分析、検証、使用したか、およびその結果が詳細に記述されています。

EANTC チームは、今回使用したクラウド環境に適した方法で作業を進めました。EANTC は、ネットワーク テクノロジーの属性、制限、およびマルチベンダー導入の適合性のテストでよく知られています。シスコとの今回の取り組みにおいて同様の技術が多く使用されましたが、EANTC は、ハードウェアのパフォーマンス評価ではなく、さらに一体となったサービス対応のアーキテクチャや環境の機能および性能を評価すべきであることに気づきました。

EANTC は、サービス プロバイダー ネットワークの多くの複雑なプロビジョニングおよび障害管理の自動化や、オンデマンドでのプログラミングが可能で、従来の設定やアクティブ化ツールよりも速く簡単にサービスを展開できるということに気づきました。

次のページには、EANTC チームのプロセスと成果が詳しく説明されています。このレポートが皆さんの役に立つものとなることを願っています。

– Light Reading チームおよび Jambi I. Ganbar（シニア テクニカル マーケティング マネージャ）、Carsten Rossenhövel（最高業務責任者）、European Advanced Network Test Center AG（EANTC、ベルリンの独立したテスト ラボ、http://www.eantc.de/）EANTC は、メーカー、サービス プロバイダー、およびその他の企業に対してベンダー中立なネットワーク テスト設備を提供しています。

EANTC がサンノゼへ

Light Reading から連絡があったとき EANTC は、シスコを訪問してそのクラウドおよび仮想化サービス プロバイダー ソリューションを調査するという依頼に喜んで応じました。シスコは、次の 2 つの重要な質問に関して、私たちのチームがサンノゼの施設で調査するための包括的なストーリーを用意してきました。

- コミュニケーション サービス プロバイダー（CSP）は、どうすれば仮想化およびソフトウェア定義型ネットワークという新しい分野がもたらす無数の可能性について理解できるか。
- CSP は、Google、Amazon、Netflix などの Web サービス/OTT 企業と同様の速度と柔軟性を持つ新しいサービスを、どのように開発し、提供できるのか。

検証プロセス中、私たちはシスコが、緊急性や俊敏性、導入までの時間について、かつて聞いたことがないほど言及するのを耳にしました。これらは通常ソフトウェア開発チームが口にすることです。

シスコは、サービス プロバイダーのカスタマーが、ネットワーク機能仮想化（NFV）、ソフトウェア定義型ネットワーキング、およびクラウドベースのアプリケーション製品の評価、導入、および活用において異なるステージにあると言います。

そのためシスコは、EANTC が、顧客にビジネス VPN サービスを提供する CSP としての役割を実質的に果たせるように、各種のツール、ラボのリソース、およびその他の機能にアクセスできるようにしました。

シスコの目標は、ビジネス VPN サービスを開発および導入している多くの CSP カスタマーが体験する、3 つのステージからなる行程を私たちに体験させることでした。

ステップ 1：
CSP の評価とコンセプト実証ステージ

CSP は、Web ポータルの実験や、柔軟な仮想環境のプログラミングの可能性を理解しやすい「cloud in a box」というツールの使用から開始します。

ステップ 2：
導入ステージ：シスコ サービス プロバイダー SDN 導入ツール

このような実験が終了し、CSP が実現性を理解できたら、シスコは、CSP が最も適したクラウド ソリューションを作成できるようになる開発ツールや、ネットワーク容量やサービスの導入をサポートする製品を提供することができます。

ステップ 3：
クラウド サービスの作成および導入ステージ

シスコは、クラウド対応データ センターを使用して、ネットワーク サービスやアプリケーションを実行、管理する機能を提供します。ネットワーキングおよびデータ センターに関するシスコの専門知識に基づくこのクラウド サービスは、長期にわたって培われたものです。このサービスによって提供される可能性にスポットを当てるため、シスコは、CSP がクラウド プラットフォームに対する投資から収益を生み出す方法を示すアプリケーションを準備しました。

最初にステップ 1 から説明します。

ステップ 1：CSP の評価とコンセプト実証ステージ

主要な電気通信事業者の中核グループによって運営される ETSI の NFV Industry Specifications Group と EANTC との連携から、世界の大規模 CSP は、仮想ネットワーク機能の採用を加速し、クラウドサービスの開発や Web スケールでの運用に積極的に取り組んでいることが分かっています。

もちろん他にも多くのネットワーク事業者が存在し、（全部とは言わないまでも）その多くが、ネットワークや運用をより効率的で柔軟にする方法に関してサポートを必要としています。では、リソースに関わらず、すべてのタイプの CSP は、どのようにシスコを活用し、クラウド対応や仮想化においてベンダーが何を提供すべきかを見極めることができるのでしょうか。

1 つのエントリレベルのリソースは dCloud（http://dcloud.cisco.com/）と呼ばれる Web ベースのプラットフォームです。誰でも自由にアクセスして使用できるオンライン リソースで、これは実質的に New IP の世界で何が実現できるかを示すものです。このツールを検証するため、EANTC エンジニアはアカウントを作成し、自らシナリオを実行しました。一度アカウントが作成されると、ユーザには事前定義されたセットアップが提供され、シスコの新製品やコラボレーション（OpenDayLight 仕様に基づく SDN コントローラを含む）製品を実際に検証できます。合計で 40 の異なるシナリオが実施されました。3 つの異なる dCloud シナリオを実行しました。各シナリオは、2 週間の検証プロセスの後半でテストした実際のアプリケーションのプレビューです。

シナリオは次のとおりです。
- Cisco WAN Automation Engine 6.0 with 8-Nodes v1
- Cisco CloudVPN Technology Preview v2
- Cisco Network Control Systems 3.3 MPLS VPN v1

この検証フェーズで dCloud は、後で実施するシナリオのプレビューに使用されました。プロセスの一部として、独立した検証のために、dCloud のシナリオの 1 つ（サンドボックスと呼ばれる）を私たちのラップトップに接続するよう依頼しました。接続は簡単にでき、シスコのサンドボックスから私たちのラップトップへ接続する外部接続を経由してシナリオを実行できました。

シスコの dCloud はシスコ セールス エンジニアおよびアカウント チーム、そしてカスタマーの 2 つのタイプのユーザを対象に設計されたイネーブラです。これは、CSP 自身のネットワーク インフラストラクチャだけでなく Amazon Web Services（AWS）などのパブリック クラウドにも接続できます。

CSP がシステムやデータのセキュリティを懸念して評価プロセスでパブリック クラウドを使用したくない場合、シスコは /dev/innovate と呼ばれる革新的な開発ポッドのソリューションを提供しています。

この革新的なポッドとは、シスコが CSP に対して年単位でリースする自己完結型データ センター ラックです。ポッドには、クラウド サービス構築のために CSP が使用できる一連のシスコ製品が含まれます。
- Cisco UCS 5108 ブレード サーバ シャーシ
- UCS 2208XP ブレード シャーシ エクステンダ X 2
- UCS B200 M3 コンピューティング ノード X 6
- UCS 6248 ファブリック インターコネクト X 2
- Cisco ASR9001 ルータ X 1
- Nexus 5672 データ センター スイッチ X 1

ポッドには追加のコンポーネントをホストするラック スペースもあるため、CSP は、シスコ、または他のベンダーのものであっても追加のシステムを統合することができます。

ポッドの目的は、CSP の研究開発チームがその CSP の運用グループと直接やりとりし、拡張性、セキュリティ、ハイ アベイラビリティなどに関する質問に対応できるようにすることです。その他の利点としては、コンセプトからサービスの開発や作成に至る時間が短縮され、CSP が「Web スピード」で開発できるようになることです。

これらはすべて、CSP が仮想化戦略を検討する際に、その意思決定および開発プロセスを速めるシスコの努力の一環です。

評価ステージに続く次の論理的なステップは、CSP の導入プロセスへの移行です。

ステップ 2：導入ステージ：シスコ サービス プロバイダー SDN 導入ツール

SDN 対応サービス プロバイダー クラウドの導入のために、シスコは Evolved Services Platform（ESP）を開発しました。シスコによると ESP は、予測可能な設計、キャパシティ プランニング、およびマルチベンダー プロビジョニングなどの、自動化され、信頼できるアジャイルな運用環境を提供するために設計されています。

シスコがテスト用に提供した ESP の重要な要素は次の 2 つです。
- 2012 年後半の Cariden 買収後に開発された Cisco WAN Automation Engine（WAE）。
- Tail-f ベースの Cisco Network Service Orchestrator。これは名前が示すように、2014 年の Tail-f 買収によって得た技術に基づいて開発されました。

シスコの WAN Automation Engine は、CSP に多くの役立つ機能を提供します。ツールはネットワーク使用履歴データを収集し、過去と現在の経験則に基づいて将来の動作を予測することができます。基本的にソフトウェアは、CSP のバックボーン ネットワークのトラフィックを管理するために使用されます。バックボーン トラフィックの管理は通常、輻輳および輻輳に関連するイベントの把握に関する問題で、SDN の基礎と密接した重要な概念です。

WAE は、ネットワーク トポロジおよびネットワーク要素内のインストール状態を知るために、BGP-LS や Path Computation Element Protocol（PCEP）を使用します。その機能を示すために、シスコは ASR9006、CRS-4/S および Cisco 12000 製品ファミリーのモデルを始めとした 35 のルータから構成される大規模なデモンストレーション用ネットワークをセットアップしました。ネットワーク オペレータが単一のサプライヤでインフラストラクチャを導入することはほとんどないため、シスコは、サード パーティ ベンダーの IP インフラストラクチャも統合しました。

EANTC マルチベンダー相互運用性テストからすると、これは非常に積極的で意味のある決定だったと言えます。ちなみに EANTC マルチベンダー相互運用性テストは、パリの MPLS World Congress で年に一度行われ、12 年の歴史を持っています。

検証プロセスで使用されるものの詳細を携えて、私たちはラボに向かいました。

私たちの最初のタスクは、2 つのデバイス間のリンクを切断して結果を確認し、私たちが見たものが実際のネットワーク設定通りであることを確認することでした。

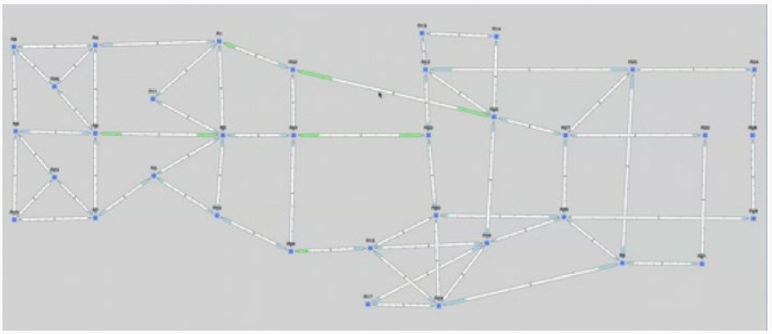

図 1：Cisco MATE Live ネットワークの概要（Cisco WAE の一部）

WAE で私たちが実行したテストは、その機能を検証し、Web ベースのアプリケーションを WAE 上にインストールできることを示すために設計されました。そのため、検証プロセスは 2 つのセクションに分割されました。1 つは CSP のオフライン アクティビティで、もう 1 つはライブ ネットワーク運用アクティビティです。

WAN Automation Engine：メンテナンス計画

可用性およびパフォーマンスに対するデバイス メンテナンスの影響をネットワーク オペレータに知らせるシステムがあれば便利だと思います。この機能テストでは、ルータのインターフェイスのメンテナンス作業を用意しました。

特定の時間にインターフェイス（この場合、RP2 と呼ばれるノード上）をオフラインにする予定があることを示すために、WAE ツール スイートの 1 つである MATE Live を使用しました。このプロセスの一環として、RP2 のメンテナンス中にネットワーク障害が発生する可能性を考慮し、アプリケーションがこの点をレポートに含めるようリクエストを作成しました。

これらのリクエストが送信されると、システムはメンテナンスとノード障害の結果を詳細にレポートしました。MATE Live は、緑の太字で「パス：輻輳要件の違反はありませんでした（PASS – no congestion requirements violated）」とレポートしました。

代替デバイスへの接続の詳細リストを受け取りました。その中でソフトウェアは、次のルートのリンク使用率は最大 98.7% だが、100% を超えることはないと予測していました。

これらの詳細を基に、ネットワークと MATE Live ソフトウェアの予測機能をテストすることにしました。シスコ チームは、手順が始まると、MATE Live の予測が正確かを示す「ペーパー トレール（証跡文書）」が生成されると説明しました。

そのため、テスト トラフィックがネットワーク内で実行されている間に私たちはラボに入り、特定された RP2 インターフェイスをダウンさせてネットワークのトポロジに障害を発生させました。その後、MATE Live によって予測された帯域幅を実際の帯域幅と比較し、両者がほぼ一致することを確認しました（予測値 591.06 Mbit/s に対し EANTIC によって記録されたのは 590.02 Mbit/s で、アプリケーションの誤差はわずか 1.04 Mbit/s でした）。

Cisco WAN Automation Engine：分離トンネル作成

一部のミッションクリティカルなアプリケーションでは、パケット損失への特別対策として、同じトラフィック ストリームを 2 つにコピーして送信するよう CSP ネットワークが設定されていることがあります。シスコ チームが示したとおり、コンテンツが動画の場合や、コンテンツ プロバイダーが障害発生時にパケットを一切ロストしたくない場合には特に重要です。

それでは、リンクが 1 つしかない、もしくはノードに障害が発生してもコンテンツ プロバイダーがパケットをロストしないようにするには、CSP は 2 つのトランスポート パスをどのように変えればよいのでしょうか。

基本的に WAE ソフトウェア機能は明確でした。2 つの MPLS トランスポート トンネルが、異なるロケーションでネットワークに入っても同じロケーションでネットワークから出て、パス内でリンクまたはノードを共有しない、ということを検証するのです。

この機能が動作していることを検証するために、MATE ツールを使用して R30 ノードと R35 ノード間（後者はシスコ デバイスではなくサードパーティ ルータ）で LSP（ラベルスイッチド パス）トンネルのペアを構築しました。テスト トラフィックを生成し、トラフィックが 2 つのトンネルを通過していることをデバイスの CLI（コマンド ライン インターフェイス）で検証しました。

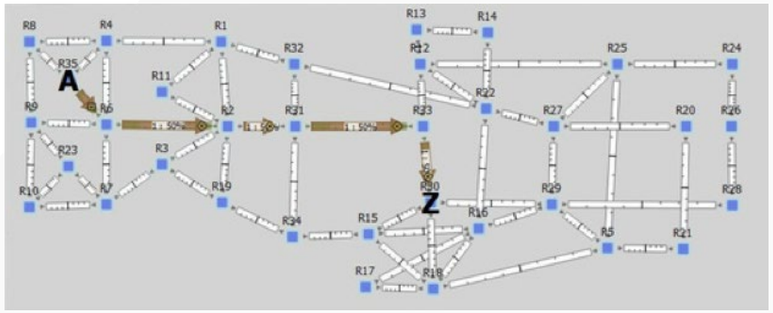

図 2：Cisco MATE Live を使用したデュアル トンネル セットアップ

次に、トンネル分離操作をして、構築したばかりのラベルスイッチド パス（LSP）を分割しました。

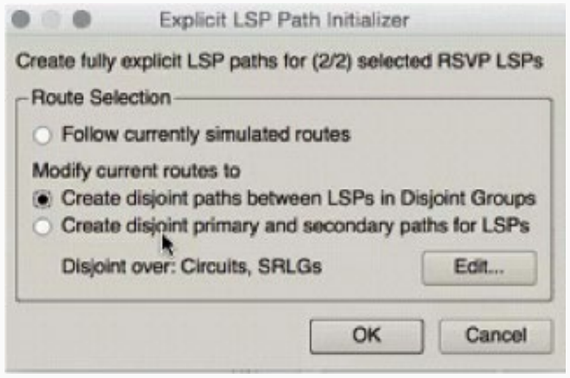

図 3：Cisco MATE Live を使用した LSP 分離操作

トンネルの分離コマンドが実行されたら、ルータへ再度ログインして、以前 LSP の作成に使用された 1 行だけのものとはまったく異なる設定を確認しました。

5 分待ってから、私たちがネットワーク上に設定した Ixia N2X テスター トラフィック ストリームに基づいてリンクが使用されていることを検証しました。設定がシスコおよびサードパーティ ルータの両方にインストールされていることを確認しました。この時点で、テスト トラフィックのレートを増加させ、線の色が使用率に基づいて変わったことをモニタしました（ツールは、リンク使用率を色で表しており、時間の経過にあわせて視覚的に確認できます）。

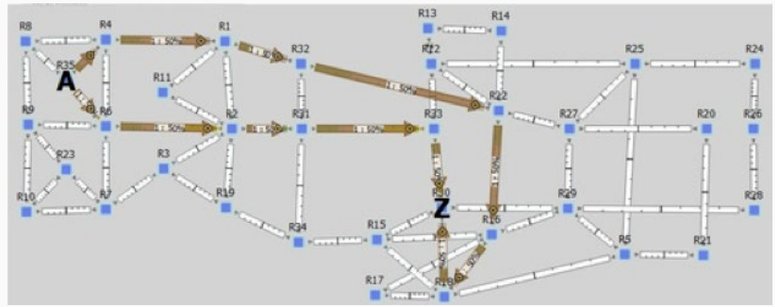

図 4：Cisco MATE Live に表示された LSP の分離結果

私たちはその仕組みに興味があったので、MATE Live が実際に設定をどのようにルータ上に作成したのかを尋ねました。シスコは、各種の標準規格に準拠した API を使用して、システムが Tail-f ベースの Cisco Network Service Orchestrator と相互に作用すると説明してくれました。MATE Live は、モデル処理ツールを使用します。このツールは、Network Service Orchestrator（NSO）に命令を送信し、NSO はデバイスに接続します。

MATE Live が提供する機能は、「what if（仮定）」機能と同等です。変更が必要であることを CSP が認識し、MATE Live GUI を使用して確定したら、NSO が作動し、ルータに設定変更を送信します。

設定前後のデータを比較すると、トンネル分離後操作は非常に複雑だったことに気づきました。設定の観点からすると、システムにとってはパスを設定する方がダウンさせるより簡単です。ただし、CSP（この場合は私たちの EANTC テスト エンジニア）は、実際にはデバイス設定の作成に時間をかける必要はありませんでした。

NSO の詳細に入る前に、WAE のその他の機能を検証する必要がありました。

Cisco WAN Automation Engine：オンデマンド帯域幅

次の検証プロセスには、WAE で実行する一連の Web ベース アプリケーションが含まれていました。

Web ブラウザ アプリケーションと WAE ソフトウェアはどのような関係でしょうか。シスコの DevNet で説明されているとおり、WAE は、開発者（この場合はシスコの開発者）が Web ブラウザで実行可能なアプリケーションを開発できるようにする、REST（Representational State Transfer）アプリケーション プログラミング インターフェイス（API）を公開しています。

私たちは Web ブラウザの開発者ビューを使用してブラウザとアプリケーション間のインタラクションをキャプチャし、REST と WAE の通信が確立されていることを確認しました。

最初にテストしたアプリケーションは、オンデマンド帯域幅でした。このツールを使用して CSP は、シスコが説明するとおり、短期間のためだけであっても、ネットワーク ノード間でサービス キャパシティを動的に追加できます。

私たちは、数週間続いた EANTC での相互運用性に関する一般公開イベントの間、ベンダー エンジニアの大きなグループのホストを務めることもあるため、この機能がエンドユーザへもたらすメリットにすぐに気付きました。イベントの間に私たちのネットワーク接続は輻輳し、その結果大幅な遅延が発生します。Web ツールを使用して、これらの期間中だけ帯域幅を追加することができたら、私たちが招いたエンジニアは、ダウンロード時間を短縮し、遠隔地にいることが多い開発者の同僚と簡単にコラボレーションできます。

この機能をテストするため、2 つのノード間（R35 および R30）でサービス（この場合、MPLS Label Switch Path）を作成し、トラフィックを 762 Mbit/s で送信しました。ラボのリンク キャパシティが、（全部ではありませんが）ほとんどのパスで 1 Gbit/s だったため、GUI で、GigE リンクの使用率は黄色、10GigE リンクは緑で表示されました。

色はネットワーク使用率の特定のレベルを表し、輻輳の可能性について CSP に警告するために使用されます。CSP は、特定のレベルより下の使用率を緑で、上の使用率を黄色で示すよう、しきい値を設定することができます。システムは、リンクを赤で表示することもでき、それは、しきい値をさらに高く超えたことを示します。

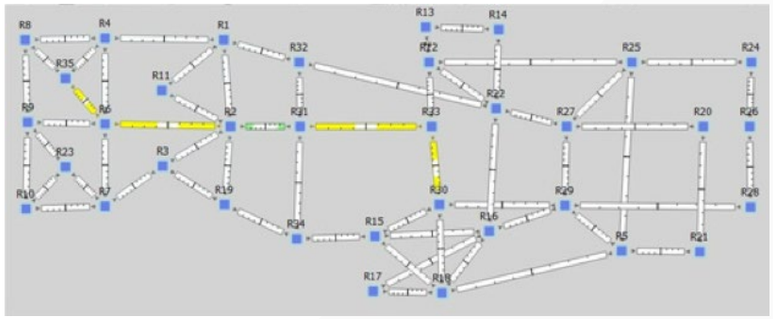

図 5：ネットワーク内のサービス パス使用率

次に、オンデマンド帯域幅ツールを使用してさらに 400 Mbit/s をサービスにリクエストしました。アプリケーションは次のスクリーンショットのようなレポートを作成しました。お分かりのように、システムはパスの最初のホップで輻輳をレポートしました（CSP ネットワークではよくあるように、ネットワーク内では他のトラフィックが実行されていました）。

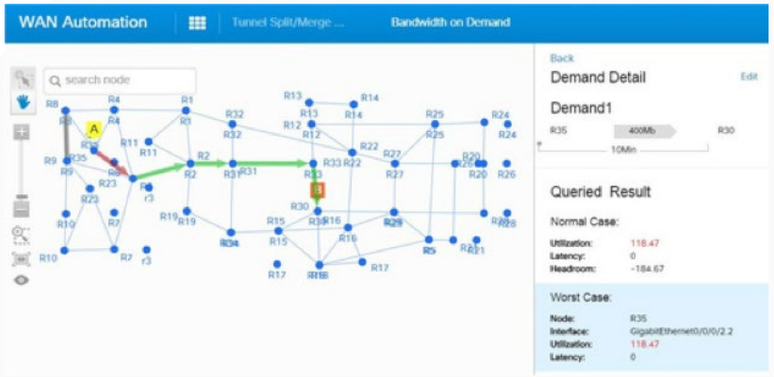

図 6：オンデマンド帯域幅の使用率レポート

私たちにはまた、「最適化」を促すオプションが提示されました。このオプションを選択すると、システムは新しいパスを推奨しました（図 7 参照）。

ホップ制限または特定の遅延を指定しなかったため、私たちは、アプリケーションがサービスに対して追加のキャパシティをどのようにプロビジョニングするかを知りたいと思いました。ツールは、茶色の矢印の「what if」ルートをソリューションとして提示しました。そのルートは、人間のエンジニアが選択することはほとんどないと思われるネットワーク ルートです。

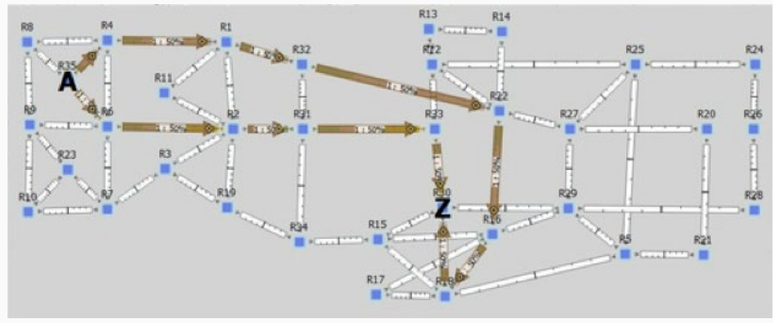

図 7：オンデマンド帯域幅推奨パス

図 7 が示すように、システムは、A からエンド ポイント（トポロジ上の Z マーク）までのかなり長いルートを通るまったく新しいパスを作成しました。そのパスは、予測しなかった方向からエンド ポイントに到達するものでした（私たちには「後方」から到達するように見えました）。

パス内のノードの数は 5 から 7 へと変わりましたが、このパスを使用することで、色が示すように両方の LSP が使用率を 50% 未満と予測しました。設定に同意したら、今回は累積レート（762 Mbit/s プラス 400 Mbit/s）でトラフィックを再生成し、トポロジ上のリンクの色が、輻輳するリンクがないことを示す薄い緑色に変わったことを確認しました。また、予想通り、損失したトラフィックはありませんでした。

プロセスに参加したシスコのマネージャの 1 人は、「これは飛行機のオートパイロットのようなものです。オートパイロットであっても、飛行機を操作するために何をすべきか把握しているパイロットが必要です」と言いました。

これは、ネットワーク エンジニアリングの実に新しいアプローチです。システムが問題のソリューションの開発を担当し、ネットワーク オペレータは単にシステムを監視するだけでよいのです。

Cisco WAN Automation Engine：帯域幅予約機能

アプリケーションが、過去および現在のネットワーク状態（リンク使用率、遅延、およびデバイス レイアウトなど）に関する大規模なデータベースを持っていれば、アプリケーションはネットワークの将来の使用率を計算（または「予測」）できる可能性があります。

シスコが次に示すアプリケーションは帯域幅予約機能と呼ばれます。このアプリケーションを使用して、サービス プロバイダーの顧客は、将来の一定の期間、帯域幅を予約することができます。

EANTC はこのプロセスで、顧客企業の代わりに Web インターフェイスを使用して帯域幅をさらに追加するよう依頼しました。このような機能は、オフサイトのバックアップやデータベースの同期など、頻繁に発生するわけではないが、短期間に大量の帯域幅を必要とする、企業の IT アクティビティを迅速に実現する素晴らしい方法です。

実際にシステムが想定通りに動作していることを確認するため、私たちはサービス全体に 100 Mbit/s のテスト ストリームを流し始めました。最初のサービス パラメータでは 10 Mbit/s しかなかったので、90 Mbit/s のトラフィック ロスを記録しました。次に、帯域幅予約の Web GUI を使用して、キャパシティを 10 分間だけ 100 Mbit/s に増やしました。

[実行(go)] ボタンをクリックすると、ほぼ瞬間的にトラフィック ジェネレータのトラフィック ロスのレポートが停止しました。

ネットワークのこの迅速な反応は顧客企業がすぐに使用できるもので、サービス プロバイダーにとっては、サービスを改善し、収益源を増やす素晴らしい手段です。

このツールには注目に値するもう 1 つの要素があります。Web インターフェイスでは、このアプリケーションが、閉ざされたテスト ラボではなく、国際電気通信ネットワークでどのように実行されるかを示しています。それを見て、ノードが地図上で地理的に分散していること、また、遅延が、帯域幅予約リクエストを作成する際に設定できる要素の 1 つであることに気づきました。

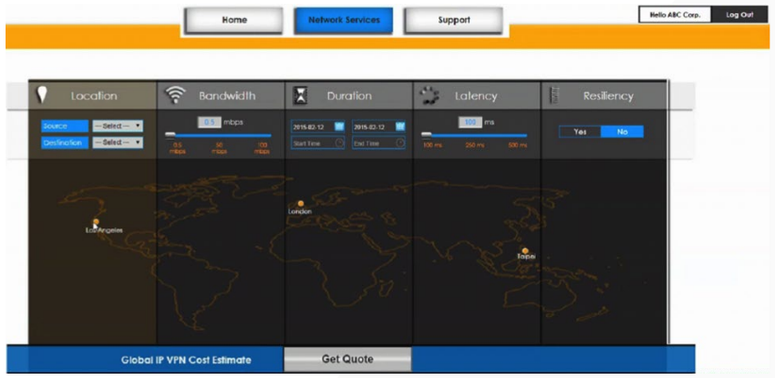

図 8:シスコの WAN Automation Engine 帯域幅予約アプリケーション インターフェイス

シスコは、遅延は、緯度および経度パラメータを基に地理的ロケーションから取得でき、また、Cisco Prime ネットワーク管理ツール(本テスト対象外)を使用してネットワークを監視したり、WAE データベースに実際に測定データを追加したりすることが可能だと説明しました。

異なるリンク遅延をシミュレーションできる障害ジェネレータがラボにはなかったため、遅延制限が機能するかどうかは検証できませんでしたが、この評価はフォローアップ テストの一部にすることを予定しています。

Cisco WAN Automation Engine:トンネル分割/結合マネージャ

私たちが検証した WAE 上で実行される最後の Web アプリケーションは、トンネル分割/結合と呼ばれる最適化ツールです。

主な使用例は、ブラウンフィールド展開で、そこでは多くのラベル スイッチド パス(LSP)がネットワーク内にすでに存在します。WAE をネットワークに導入したら、サービス プロバイダーは LSP を再度最適化して不要なものを削除し、残ったものを最適化するというのがそのコンセプトです。

もう 1 つの使用例は、ネットワークで自動帯域幅 LSP が使用される場合です。この場合シスコは、LSP 上の帯域幅設定が大きくなって障害が発生した場合に、ネットワークがバックアップ リンクに対してシグナルを送れない、という問題に対応しようとします。

いずれの使用例においても、ネットワークを最適化し、無駄なネットワーク リソースを取り戻すことができれば、帯域幅制限のあるネットワークで役立ちます。

ツールが正常に機能していることを検証するため、テスト ネットワーク内のすべての LSP に対して、最大および最小の帯域幅しきい値を指定しました。Cisco WAE は、ネットワークのどの LSP を分割、また結合するかの推奨事項のリストを出しました。[すべて選択(Select all)] をクリック後、[最適化(Optimize)] ボタンをクリックしました。

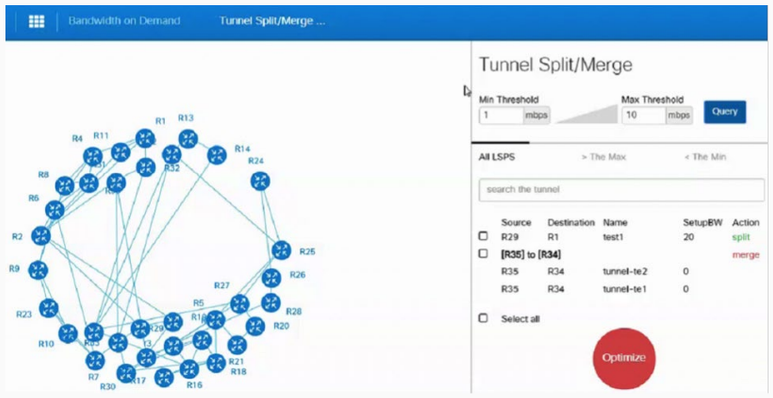

図 9:シスコの WAN Automation Engine トンネル分割/結合アプリケーション インターフェイス

optimize コマンドを実行すると、分割対象のトンネルが実際に分割され、結合対象のトンネルが結合されたことを確認するレポートを受信しました。ルータ設定を確認し、変更が適用されたことを検証しました。

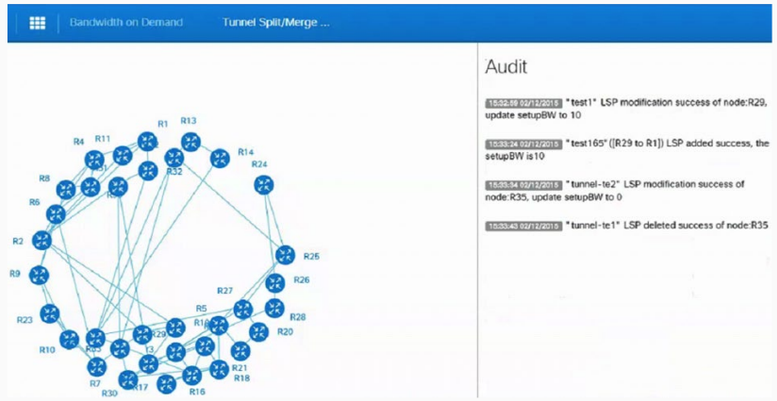

図 10:シスコの WAN Automation Engine トンネル分割/結合結果

WAN Automation Engine の概要

シスコの WAN Automation Engine のテストを通して、シスコがサポートしていると説明している機能が実際にサポートされていることを確認しました。

私たちは、保守ツールおよびオンデマンド帯域幅ツールによる正確なリンク使用率レポートを記録しました。また、WAN Automation Engine が、シスコおよびサードパーティ デバイスのいずれも設定できることを確認しました。ほとんどすべてのネットワークがマルチベンダーであるため、これは CSP にとって重要な要素です。

これまで見てきたように、WAE によってエンジニアは、ネットワークの LSP 機能を高いレベルで抽象化して監視できます。

また、独立したテスト ラボ、およびネットワークのサブスクライバという両方の立場から見て、帯域幅予約とオンデマンド帯域幅ツールの操作性は非常に素晴らしく、大きな進歩と言えるものでした。

WAN Automation Engine などのソフトウェア ツールや、PCEP および REST などの定義された標準プロトコルを使用すると、ネットワークの自動化や動的プログラミング、または要求に応じたプログラミングが可能になります。

次に、Network Service Orchestrator について見て行きましょう。

Tail-f ベースの Cisco Network Service Orchestrator

シスコが EANTC に提供した、管理およびオーケストレーション ポートフォリオのもう 1 つの重要な要素は、前述の Tail-f ベースの Cisco Network Service Orchestrator です。

EANTC は Network Service Orchestrator（NSO）を熟知しています。私たちがシスコのサンノゼのラボでその機能を検証していたとき、NSO チームのメンバーが、私たちのベルリンのラボでマルチベンダーの相互運用性をテストしていました。EANTC が異なる 2 つのラボで製品を同時にテストするのは珍しいことです。

NSO とはどういうものなでしょう。シスコは、NSO とは 2 階層のトランスレータ ソフトウェア ツールボックスのようなものだと表現しています。

1 つ目の層は、CLI、JSON-RPC、REST などの各種サービス ツールに対するプログラム可能なインターフェイスです。この層は、ネットワーク オペレータまたは他のアプリケーションに対応しています。私たちの初期のプロセスで、WAE は、ネットワーク内で MPLS ラベル スイッチド パス（LSP）をプログラムするのに NSO を使用していました。

2 つ目の層はネットワークに対してサウスバウンドで、Network Elements Drivers（NED）と呼ばれています。この層は、各種の標準規格に準拠したインターフェイス（IETF NETCONF または SNMP など）を使用し、CLI インターフェイスで拡張されます。

しかし、驚くべきことが起きるのは、NSO がネットワーク サービス プログラマビリティを提供する 2 つの層の間です。インターフェイス間には、サービス マネージャおよびデバイス マネージャと呼ばれる 2 つのソフトウェア モジュールがあります。これらの 2 つのソフトウェアを使用して、NSO はサービス モデルおよびそれらをデバイスに実装するために何が必要かを理解することができます。サービス モデルは Yang（IETF RFC 6020）で定義されています。これは、IETF RFC 6020 に記載されているように、「Network Configuration Protocol（NETCONF）、NETCONF リモート プロシージャ コール、および NETCONF 通知によって操作される設定および状態データのモデリングに使用されるデータ モデリング言語」です。

サービス モデルは、サービスを作成する方法における重要な変化を意味します。サービス モデルによって、設定を定義することからサービスを定義することへフォーカスは移ります。NSO は関連するネットワーク デバイス上でサービスを設定します。

それでは、NSO は何ができるのでしょうか。

Cisco Network Service Orchestrator：サービス プロビジョニング

私たちは、この検証プロセスを、サービスが何も設定されていない要素の検証から開始しました。NSO インターフェイスには、5 つのカスタマー エッジ（CE）ルータが表示され、それらは、シスコからの 2 つのプロバイダー エッジ ルータと別の主要なベンダーからの 2 つのプロバイダー エッジ ルータに接続されていました。ラボ ネットワークの中心に IP ルータがありました。私たちの目標は、このマルチベンダー、マルチオペレーティング システム ネットワーク上に IP/MPLS レイヤ 3 バーチャル プライベート ネットワーク（L3VPN）サービスを設定することでした。（シスコのプロバイダー エッジ ルータも、1 つは Cisco IOS、もう 1 つは Cisco IOS-XR という、少し違うオペレーティング システムで実行していたため、複数のオペレーティング システムを管理する機能は重要な特徴と言えます）。

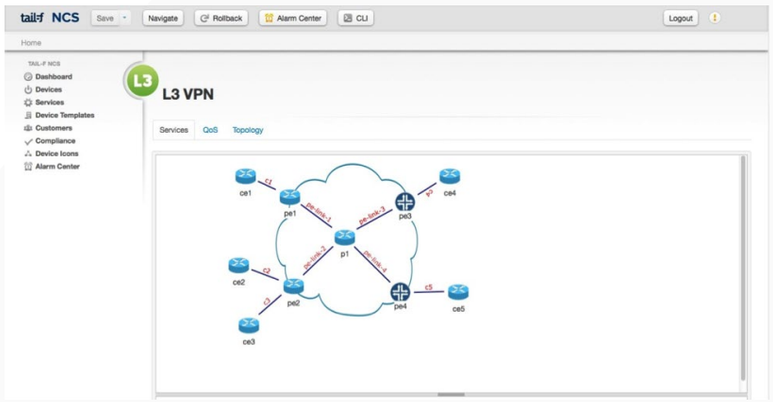

図 11：シスコの NSO によって検出されたネットワーク トポロジ

このようなテストでは最初は何も特別なことは起こりません。私たちは、ルータ上でソフトウェアのアクセスを手動で有効にする必要がありました。その後、NSO 設定データベース（CDB）とデバイスを同期させました。私たちは、シスコがデバイスに対して 2 つの異なるインターフェイスを使用していることに気づきました。シスコ デバイスは CLI モジュールを使用し、NSO は NETCONF を使用してサードパーティ ルータに接続していました。なぜ 2 通りのアプローチがあるのでしょう。

シスコ チームは、CSP が現在の実際のネットワークで使用するのと同じ方法で、CLI および NETCONF の両方を使用する実用的なアプローチを示したかったのだと説明してくれました。また、NETCONF は、シスコ製品に接続するのに使用しやすく、CLI は、サードパーティ ルータに接続するのに使用しやすいからだと話しました。

私たちは最初に、CE1 から PE1 への接続、および CE2 から PE2 への接続が必要な「Volvo」というサービスを設定しました。作業は、ルータの設定と良く似ていましたが、ルータの CLI 上ではなく、NSO コマンド プロンプト上で設定したという点が大きく異なっていました。次に、「commit dry-run」という NSO コマンドを使用して、デバイスに送信する設定をデバイス上の既存の設定と比較しました。障害が発生しないことを確認してから、設定を適用しました。

驚くべきことが起こったのはこの時でした。大した労力もかけずに NSO へほんの少し情報を与えただけで、ルータに何百行ものコードを入力することなく、新しいサービスを作り出すことができたのです。NSO は、高級言語でサービスを作成できるため、エンジニアはネットワーク要素の設定ではなくサービスについて考えることに集中できます。検証プロセスでこのことを数値によって示すことができました。

NSO 設定データに 15 行追加すると、シスコの設定は 318 行になることがわかりました。次に、CE ルータに接続されたテスターを使用して CE1 と CE2 の間にトラフィックを送信することができました。サービス モデルには 600 Mbit/s のシェーパーが含まれていたため、シスコ チームに、トラフィック レートを 700 Mbit/s に増やすよう依頼して、ドロップされたパケットを探しました。実際 1 方向につき 100 Mbit/s のトラフィックがロストしており、サービス モデルの帯域幅リミッタが機能していることが証明されました。

この時点でトポロジには、2 つの CE ルータおよび 2 つの PE ルータ（いずれもシスコ）があったので、さらに 2 つのサードパーティ ルータを追加しました。今回は、新規サービス（CE から PE への接続 1 つ）用に NSO CLI インターフェイスで 6 行の設定が必要でした。その結果、デバイス設定およびサービス機能の設定は191 行になりました。シスコ チームは、単に CE ルータを PE ルータの上にドラッグするだけで、デバイスはすでに「検出」されていると説明しました。テスト トラフィックを再度送信して、新しいデバイスが実際にサービスに追加されているか確認しました。

この初期テストの結果はいくつかの理由で素晴らしいものでした。まず、私たちが使用していた NSO CLI は、シスコ CLI に似ており、使い慣れていて、快適でした。これは NSO がベンダー CLI を再現できるためです。ネットワーク エンジニアが他のベンダーの CLI を使用する方が快適なら、NSO CLI はそのベンダーの CLI と同じように動作し、より使いやすくなります。その結果、マルチベンダー ネットワークでも、（一旦サービスおよびデバイス モデルが適用されたら）1 つの CLI で操作できるようになります。

このような複雑なサービス（接続だけでなく QoS 設定も含む）の作成がほんの数行の設定で済んだということからも、このソフトウェア ツールのメリットが実際に明らかになりました。すぐ次に浮かぶ疑問は、サービスを変更する場合はどうか、ということです。

Cisco Network Service Orchestrator：サービス変更

正しく機能し、テストも済んだ IP/MPLS L3VPN サービスがテスト ネットワークで実行されている状態で、一部の設定をネットワーク上で修正することにしました。

GUI インターフェイスを使用して、CE ルータ（CE2）の 1 つで AS 番号を変更し、設定がデバイス自体に適用されたことを確認しました。トラフィックが実際にすべてのエンド ポイント間を流れているため、この特定の CE 上のサービスが 6 秒間中断し、その後フル稼働に戻ることを計算できました。

今度は、GUI を使用して、ある CE の接続先を別の PE に変更しました。私たちが行なったのは、エンドポイント パネルに移動し、変更したい CE に適用する別の PE インターフェイスを選択して、変更を適用するだけでした。今回も、適用の結果、生成される設定を承認前に検証でき、それからコミットしました。

関心を持ったのは、単にデバイスの設定が変更されただけではなく、NSO が最初の PE ルータ上で不要になった設定をクリーンアップしたということでした（テスト環境全体が 1 つのスイッチ上にあったため、接続を変更してもケーブルの再配線は必要ありませんでした）。

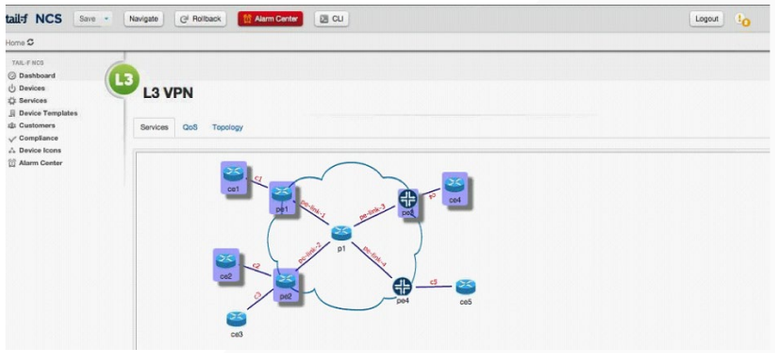

図 12：初期サービス設定、サービスに参加するすべてのルータ（NSO によって紫でハイライト）

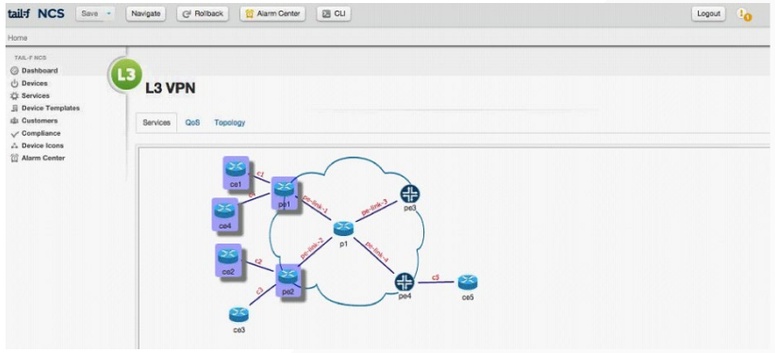

図 13：IP/MPLS L3VPN サービスの結果（NSO によって CE4 が戻っている）

Cisco Network Service Orchestrator：サービスの復元

ここでネットワーク運用チームがまだ納得せず、一部のネットワーク エンジニアがまだルータ設定を変更していて、シスコの NSO を使用していないと仮定しましょう。このような問題を識別し、できれば労せず解決するためのメカニズムが NSO 内に存在する必要があります。

NSO が実際にこのようなシナリオにスマートな方法で対応できるかどうかを確認するために、シスコのエンジニアの 1 人に、CE ルータの 1 つにログインし、BGP 設定を削除するように依頼しました。エンジニアが「no router BGP」と入力したら、この CE ルータのすべてのテスト トラフィックがロストを示したのにすぐ気付きました。

このような状況がネットワークで発生すると、その根本となる原因を識別し、問題を解決する必要があります。これは人間の本性です。

私たちは NSO CLI を使用して、CE ルータの問題の前後のネットワーク内の設定を比較しました。NSO のレポートには、設定の一部が失われたとありました。私たちは「re-deploy」というコマンドを使用して、CE ルータ上の設定をオーバーライドしました。シスコ チームが説明したとおり、NSO はデバイス上にあるべきサービス モデルを現在の設定と比較し、無くなった最低限の設定だけを適用します。

私たちは、サービスが通常の動作に戻ったことを確認し、次のテスト シナリオに進みました。

```
admin% request vpn l3vpn volvo re-deploy dry-run
cli {
    device {
        name ce4
        data  config {
                  ios:router {
                +       bgp 65103 {
                +           neighbor 192.168.1.18 {
                +               remote-as 100;
                +               activate;
                +           }
                +           address-family {
                +               ipv4 unicast {
                +                   neighbor 192.168.1.18 {
                +                       activate;
                +                   }
                +                   network 10.8.8.0 {
                +                       mask 255.255.255.0;
                +                   }
                +               }
                +           }
                +       }
                +   }
    }
}
[ok][2015-02-13 11:34:53]

[edit]
admin% request vpn l3vpn volvo re-deploy
[ok][2015-02-13 11:37:57]
```

図 14：再導入時の NSO コマンド ライン インターフェイス

Cisco Network Service Orchestrator：ノード障害によるサービスの復元

次の検証は、設定を適用する準備ができたが、サービスに含めなければならないデバイスに障害が発生したという状況です。今回は、シェーパー帯域幅の割り当てを 600 Mbit/s から 1 Gbit/s に変更しました。dry-run コマンドを再度使用すると、設定に適用される変更をハイライトしたレポートが生成されました。次の図を参照してください。

図 15：変更予定部分がハイライトされたドライランの結果を NSO でコミット

設定を適用する前に、サービスに含まれているルータの 1 つをシャットダウンしました。ここで、NSO がサービス内のデバイスの 1 つに接続できなかったため、commit コマンドが拒否されました。

サービス復元テストはいずれも、シスコの NSO ソフトウェアがネットワーク内の変更に反応し、オペレータのミスを回避できることを証明するものでした。ソフトウェアはまた、ソフトウェアの実行対象のアクティビティをオペレータが簡単に制御できるようにするメカニズムも示しました。

Cisco Network Service Orchestrator：デバイス管理

CSP が大規模なネットワークを持つ場合、すべての設定コマンドを手動で入力することは面倒で時間がかかり、エラーの可能性が高くなることは明らかです。シスコ チームは、NSO はサービスとデバイスの両方を理解しているため、オペレータが設定変更に対するテンプレートを作成するだけですべてのデバイスに適用できる、と説明しました。

この機能の検証は比較的単純なテストと判断し、シスコ チームに 3 つのデバイス タイプ（Cisco IOS デバイス 2 つ、サードパーティ デバイス 1 つ）のすべてで SNMP をアクティブにするよう依頼しました。シスコは、合計 10 行のコマンドを含む設定を作成しました（サードパーティ設定に 4 行、2 つの Cisco IOS 設定はそれぞれ 3 行必要でした）。SNMP コンフィギュレーション コマンドにはそれぞれ、ドル記号で示される変数と SNMP コミュニティが含まれていました。コミュニティ ストリングを CLI で提供し、設定をデバイス グループに適用したところ、数秒で 9 つのルータすべてに SNMP 読み取り専用アクセスと正しいコミュニティ（パブリック）が設定されたことを確認しました。

これは興味深く、役立つ可能性のある概念です。私たちはシスコに、どの Element Management System（EMS）が検証ネットワーク内のデバイスを担当しているのか尋ねました。実際には、NSO がデバイス管理を統合しており、デバイスとの接続を常に維持しているため、デバイス内の変更に動的に対処することができます。

Cisco Network Service Orchestrator：サービス モデル変更

最後に（とはいえ大事なことですが）、設定に変更を加えた場合に何が起こるかを確認するために、テスト内で使用したサービス モデルへのアクセスを依頼しました。

実施した検証プロセスから、ソフトウェアにおいてサービス モデルは最も重要な要素の 1 つであることは明らかで、関心がありました。そこで QoS モデルを変更し、bronze、silver および gold の 3 つのクラスを追加してパッケージをリロードしました。

ここで、サービスに QoS 設定を適用するために NSO CLI を使用しようとすると、すべてのデバイス（CE、PE およびサードパーティ デバイス）上でサービスに追加したばかりの 3 つのオプションが表示されました。設定がデバイスに適用されたかどうかを検証しましたが、すべてのデバイスに QoS 設定の変更が正しく適用されているのを見ても、もう驚くことはありませんでした。

Cisco Network Service Orchestrator（NSO）：テストの要約

NSO に焦点を当てたテストでは、サービス作成から変更、再導入、およびデバイス管理に至るまでのフル サービス ライフ サイクルを調査しました。最低限の NSO 設定コマンドでさまざまなデバイス設定を作成できることが明らかになり、業務の効率化を確認することができました。

もちろん、サービスおよびデバイス モデルの作成に関する労力についてはわかっていませんが、これはフォローアップ検証プロセスの格好のトピックとなるでしょう。

また、NSO は、シスコ以外のデバイスを含む複数のデバイスをプロビジョニングできる、というシスコの主張が正しいことも確認しました。マルチベンダーで複数の世代のオペレーティング システムを設定することは、ブラウンフィールド展開に対応する新しい方法で、SDN へ向かうトレンドとも見合うものです。実際、テンプレートを使用したサービスの作成は、ネットワークの設定というよりもネットワークのプログラミングのように思えました。

ステップ 3：クラウド サービスの作成および導入ステージ

シスコの WAN Automation Engine および Network Service Orchestrator はいずれも、CSP のために設計されたソフトウェア ツールです。CSP が、ネットワーク デバイスの運用や、新しいサービスの展開を自動化して迅速に実施できるように設計されています。

シスコが説明したとおり、いずれのツールも新規サービスの導入を完全に自動化するために使用できます。次の検証プロセスでアプリケーションに焦点を当てたのは、シスコによると CSP は、中小企業（SMB）の市場に効果的にアプローチできていない、ということが背景にあります。SMB の市場セグメントで顧客を獲得し、サービスを展開するのに費用がかかりすぎるからです。

ただし、制御と柔軟性の向上により、特にセルフプロビジョニング ツールを使用すれば、マーケットのダイナミクスが変わる可能性があります。独立したテスト ラボである EANTC が、マーケットのダイナミクスについて意見を述べることはできません。しかし、私たちにできるのは、エンド カスタマーがサービスをプロビジョニングし、CSP のコール センターとやりとりしたり、サービス プロバイダーの運用部門を煩わせることなくサービスを使用できるかをテストすることです。そのためには、注文からサービス導入、サービス管理および品質保証に至るまでのサービス ライフ サイクル プロセス全体が完全に自動化されている必要があります。

仮想マネージド サービス向け Cisco Cloud Managed VPN ソリューション

シスコは、ある Tier 1 CSP カスタマー向けに作成したシステムを提示しました。サービスは前述の CSP のロゴとその他の企業イメージで完全にブランド化されていました。このため、このセクションで表示する図は dCloud から取得したものです。同じサービスが評価シナリオとして存在し、dCloud 検証の一部となっていました。

私たちが構築しようとしたシナリオは、VPN が必要なロケーションを 2 つ持つ小規模な企業です。私たちはこのビジネスを（愛情をこめて）「Lakshmi's Café」と呼ぶことにしました。このプロセスでは、CSP からカフェのオーナーであるエンドユーザに視点が移りました。オーナーに扮した私たちの目的は 2 つです。1 つは、VPN を使用して両方のロケーションに接続すること、もう 1 つは、想像上のカフェで提供する予定の無料 WiFi が確実に保護されるようにすることです。

サービスの注文プロセス全体は、Web インターフェイス経由で進められました。まず、カフェに新しいカスタマー アカウントを作成することから始めました。次の図に示されているように、メニューには複数のオプションがありました。[Cloud VPN フル（Cloud VPN Full）] サービスを選択しました。ファイアウォール、URL フィルタリング、リモート アクセス、およびインターネット アクセスの Cloud VPN が含まれていたからです。

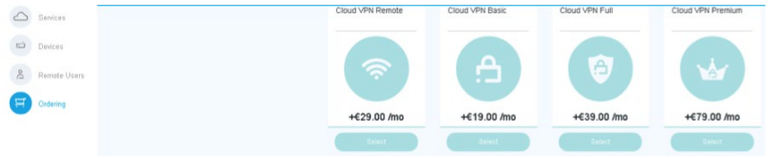

図 16：Cisco Cloud VPN サービス タイプ メニュー

クリックして次のページに進んだら、接続するサイト数、および各サイトでのユーザ数を入力する必要がありました。スタッフの増員が予測されることも示すことができました。シスコ チームによると、これは帯域幅計算に使用するためのものです。

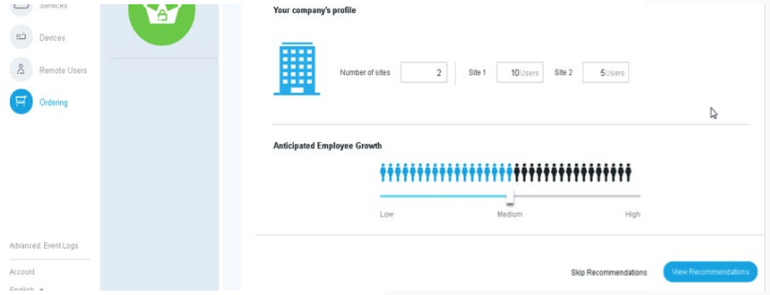

図 17：Cisco Cloud VPN 企業プロファイル設定

この手順が完了したら、いくつかの質問の意図が理解できました。基本サービスの価格は最初のページに表示されます。企業プロファイルに応じて、追加の帯域幅を有償でサービスに追加することができます。シスコは、企業プロファイル データを使用してカスタマーの規模に適したものを推奨します。私たちは、推奨されたものをそのまま受け入れることにして次のページに進みました（ここでは私たちはネットワーク エンジニアではなくカフェのオーナーです）。

この時点でシスコは、速度がライセンスの一部であることを説明しました。つまり、サービスに関連付けられる仮想ルータには、それに関する特別なライセンスがあるということです。

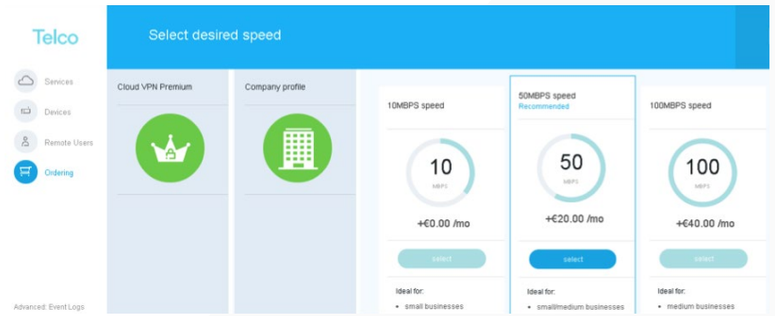

図 18：[Cisco Cloud VPN スピード選択（Cisco Cloud VPN Speed Selection）] パネル

次のパネルでは SSL ライセンスのタイプを選択できました。ここは、中小企業がつまづく可能性がある場所です。SSL VPN とは何で、なぜ必要なのでしょうか。これが頭に浮かぶ最初の疑問です。今回の例では、SSL VPN が何であるか知らなかったため、「何か分からないものにはお金を払わない」という理屈に基づき最も基本的な推奨項目を適用しました。

シスコは、SSL VPN 接続とは、クラウドへ安全に接続するためのもので、カスタマーがサービスに安全にアクセスするには必要なものだと説明しました。

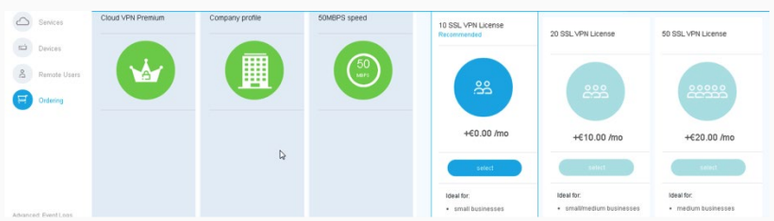

図 19：[Cisco Cloud VPN SSL ライセンス（Cisco Cloud VPN SSL License）] パネル

ここはサービスが形作られる場所で、仮想化が力を発揮するところです。次のパネルでは、URL フィルタリング オプションを選択できました。カフェのオーナーとして、お店を訪れる人が悪意のある違法な Web サイトを訪問できないようにする、というアイデアは気に入りました。また私たちのカフェでは成人向けのサイトへのアクセスも禁止したいと考えました。中度のレベルの URL フィルタリング サービスを選択し、シスコに質問しました。

ベンダーへの質問は単純です。「これはどのように機能するのですか」というものでした。シスコは、一度サービスが注文されたら Web セキュリティ仮想アプライアンス（WSAv）が CSP クラウドでインスタンス化され、URL フィルタリング機能を実行するのだ、と説明してくれました。これを念頭に置いた上で、私たちは発注プロセスに進みました。また、発注が完了したらバックグラウンドで実行されるプロセスをすべて記録したいとシスコに伝えました。

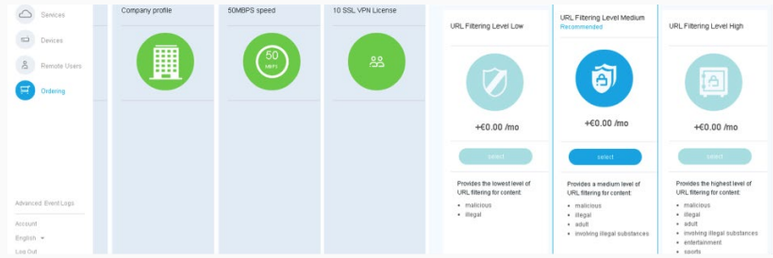

図 20：[Cisco Cloud VPN URL フィルタリング レベル（Cisco Cloud VPN URL Filtering Level）] パネル

すぐに作業は完了しました。次のパネルに移動すると、かなり高額の 2 つのデバイスのリストが表示されました。私たちには 2 つのサイトがあり、デバイスには WiFi アクセス ポイント機能も含まれていたため、十分メリットは得られると考え、次のパネルへ進みました。もう 1 つは、Amazon のような出荷先住所システムで、ルータをカフェのそれぞれのサイトへ送信できました。「ご購入いただきありがとうございます（thank you for your purchase）」というパネルが表示され、これで、Lakshmi's Café の Cloud VPN サービス購入は完了しました。

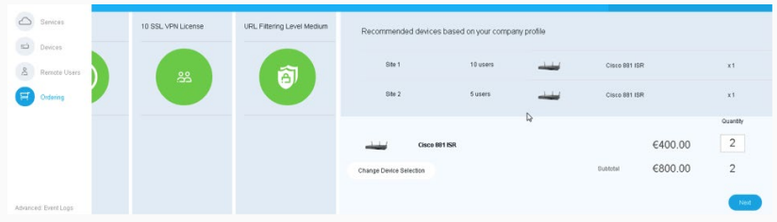

図 21：[Cisco Cloud VPN デバイス（Cisco Cloud VPN Device）] パネル

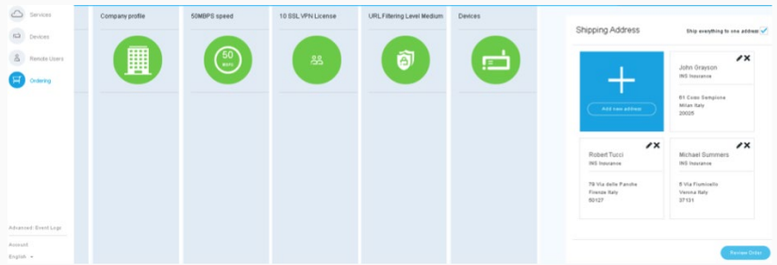

図 22：[Cisco Cloud VPN URL フィルタリング、出荷先住所（Cisco Cloud VPN URL Filtering Shipping Address）] パネル

Cisco Cloud VPN：舞台裏

サービスを追加したら、次のステップは、ルータが届くのを待つことでした。私たちはもちろんこのステップは省略し、サービスが開始するステップへ進みました。

シスコが説明したように、Lakshmi's Café が小型ルータを受け取ったら、ルータのシリアル番号を同じ Web インターフェイス パネルに手動で入力します。これによりサービスのインスタンス化プロセスが開始します。Web インターフェイスにシリアル番号を入力し、プロセスをモニタするためにコマンド ライン インターフェイスに切り替えました。

システムがサービスの準備ができたことを通知するまで、ログはおよそ 20 分間スクロールしました。その中には、Cisco CSR1000v や Web セキュリティ仮想アプライアンス（WSAv）、Cisco ASA 1000V クラウド ファイアウォールの準備も含まれていました。シスコが言うように、仮想機能はすべて Kernel Based Virtual Machines（KVM）でインスタンス化されました。

その後、シスコの Network Services Orchestrator（NSO）を使用して、仮想デバイスやその他のデバイスを確認し、注文したものがすべてインスタンス化され、管理可能であることを検証しました。最後に、2 つのルータの CLI を使用して 2 つの IPsec トンネルが確立されたことを検証しました。シスコは、IPsec トンネルの 1 つが管理（NSO に接続）用に使用され、もう 1 つがユーザ データ用に使用されることを説明しました。シスコは、すべてが OTT（オーバーザトップ）であることを前提にしている、ということです。つまり、NSO やその他の管理用アクセスはインターネット経由（管理 IPSec トンネル）で行う必要があることを意味しています。

最後に、さらに 2 つのアクションを実施しました。2 つ目のカフェをサービスに追加し、最終的にサイトの 1 つをサービスから削除しました。いずれの作業も Web インターフェイスから実行し、シスコの NSO を使用して両方を検証しました。

Cisco Cloud VPN ソリューションのライフ サイクルのまとめ

シスコが説明したとおり、サービスを完全に自動化できるバックエンド システムの全体は、ETSI の NFV ISG アーキテクチャのインスタンスです。このテストで検証した要素をマッピングしようとした場合、次の要素を NFV アーキテクチャにうまくマッピングできることがわかります。

表 1：ETSI NFV ISG アーキテクチャへのマッピング

ETSI NFV ISG アーキテクチャの要素 [1]	Cisco Cloud VPN 要素
NFV Infrastructure（NFVI）：仮想コンピューティング、ストレージ、およびネットワーク リソースが利用可能な、一連の物理コンピューティング、ネットワークおよびストレージ リソース	KVM ハイパーバイザをホストする Cisco UCS
Virtualized Network Functions（VNF）：物理的機能と類似または同等の機能を持つソフトウェア インスタンス	仮想ルータ：Cisco CSR1000v、仮想 Web セキュリティ アプライアンス：Cisco WSAV、仮想ファイアウォール：Cisco ASA 1000V クラウド ファイアウォール
Virtualized Infrastructure Manager（VIM）	OpenStack および OpenDayLight
VNF マネージャ	Cisco Elastic Service Controller（ESC）
オーケストレータ	Tail-F ベースの Cisco Network Services Orchestrator

注 1：ETSI の GS NFV 002 文書に基づく。

今回は Lakshmi's Café のオーナーと言うエンド カスタマーの観点から、素晴らしい体験をしました。サポートや発注部門に問い合わせることなく、Web インターフェイスのみを使用して、接続や複数のサービスも含むサービスを作成したのです。同じくカスタマーの視点から測定すると、すべての追加機能（ファイアウォールなど）を含むサービス全体が、立ち上がって開始されるまでの時間は 20 分でした。

サービス プロバイダーの視点からすると、カスタマーは、運用チームを介さずにかなり複雑なサービスを作成したと言えます。クラウドや、私たちがすでにテスト済みの各種自動化ツール、それにオープンソース ソフトウェア（OpenStack）を使用し、出荷部門以外は人間を介することなくサービスが展開されました。

発見したもう 1 つの点は、サイトがさらに多くても同じ時間でサービスを追加できるということです。仮想サービスのインスタンス化は一定であるため、かかる時間は同じだからです。違うのは最初のライセンスだけです。これは、フォローアップ テストで検証すべき優れた点です。

実稼動環境のアプリケーション デモ：Project Squared および Mobility IQ

パズルの最後のピースは、テストや検証ではなく、シスコがカスタマー用に開発した 2 つの Software as a Service（SaaS）アプリケーションのハンズオン デモンストレーションです。シスコが説明したとおり、ソフトウェア ツールはいずれも稼働中の実稼動環境で実行されているため、「ハンズオン」では使用できませんでした。

シスコの Intercloud（「クラウドのクラウド」）の運用アーキテクトである Reinhardt Quelle は、シスコはオープンなクラウド環境の構築に長年取り組んできた、と説明しました。また、彼はこの説明を裏付けるために、シスコがどのように OpenStack を使用しているかを OpenStack Web サーバ上のブログに投稿しました。Reinhardt が説明したとおり、特筆すべき点、そしてこのようなアプリケーションのサービス プロバイダーへの価値提案は、アプリケーションが「すぐに稼働」するということです。サービス プロバイダーは、サービスを作成するためにコンポーネントに投資する必要はありません。

Reinhardt が、シスコ自身のデータ センターやパブリック クラウド アクセス、CSP クラウドを含む実稼働システム全体を一通り私たちに説明してくれたとき、Intercloud のサービス プロバイダーの 1 つでノードが表示されたのに気づきました。Light Reading が 2014 年中に何度かレポートしたとおり、シスコが、世界中のいくつかのサービス プロバイダーと Intercloud の契約を結んでいるのは周知の事実です。それにもかかわらず、システムについて検討している間にノードが表示されたのは嬉しい偶然でした。

2014 年 9 月にレポートしたとおり、Deutsche Telekom（DT）も Intercloud エコシステムに参画しています。EANTC もドイツの企業であるため（規模は Deutsche Telekom と比較になりませんが）、私たちはデータ ガバナンスに興味がありました。ドイツでは、プライバシー法が米国とは大きく異なります。たとえば、DT のようなサービス プロバイダーは、どんなサービスで使用されたデータであってもその制御を維持し、データがドイツ国内にとどまることを保証できる必要があります。Reinhardt は、暗号化やセキュリティだけでなくデータ ガバナンスも Intercloud の重要な側面であると説明してくれました。データをドイツから別の国に移動させたいと思いましたが、シスコによるとシステムが稼働中で、このようなテストは後日実行したほうがよいとのことでした。

そこで Intercloud の理論的な側面について説明する代わりに、Intercloud 上で実行されるアプリケーションについて説明するよう依頼しました。シスコは、私たちがすでに Intercloud 対応アプリケーション、dCloud を検討したことを指摘しました。また、これから検討するアプリケーションは、CSP が SaaS アプリケー

ションをカスタマーにさらに販売するためにシスコが作成したものだと説明しました。

Cisco WebEx Squared

Synergy Research は、シスコの WebEx が、51% の市場シェアを持つ、SaaS 型 Web 会議システムのグローバル リーダーだと位置づけています。コラボレーション ツールが（ファイル共有、検索および暗号化などの機能を追加しながら）年々進化すると共に、その消費するリソースも増加してきました。ネットワーク化された企業の大部分にとって、コラボレーション ツールはミッション クリティカルでもあるので、回復性と可用性が重要視されます。そのためにシスコは労力を費やして WebEx を進化させようとしたのです。新しいコラボレーション ツールは現在 Project Squared と呼ばれ、Web や iTunes ストア、Google Play から入手できます。

私たちは Squared をスマートフォンにインストールし、すべての会話は Web インターフェイス経由に変わりました。Squared は複数のクラウドで実行されるため、最近の Xen ハイパーバイザのバグ発生（RackSpace の再起動が必要）の際にも Squared サービスにはまったく影響がなかった、と Reinhardt は説明しました。

私たちは、Project Squared が本物であることを確信しています。ですから皆さんも、アプリケーションをダウンロードして使用するだけで、本物であることを確認できるでしょう。また私たちは、シスコが示した Web ベースの管理システムを基に、多くのクラウド（パブリック、CSP ベース、そしてシスコ自身）に及ぶ広範なインフラストラクチャを持つことも確認できました。テストの次の段階では、このインフラストラクチャの調査にさらに時間を費やすことができたらと思います。

Mobility IQ

シスコは Mobility IQ をリリースしたばかりです。この SaaS アプリケーションは、小さな携帯や WiFi アクセスに、優れた可視性を提供するように設計されています。アプリケーションは、このサービスを自身の顧客に提供する、CSP のカスタマーを対象としています。

このサービスは何をもたらすのでしょうか。シスコは、稼働中のカスタマーと、大きな都市部で主要なスポーツ競技場やコンサート ホールを運営する企業を慎重に抽出しました。ツールを使って、WiFi 接続レート、アクセス ポイントの稼働状況、帯域幅使用率、スペクトル使用率などの技術的な重要性能評価指標（KPI）に関する統計が得られました。これらのネットワーク セントリック KPI に基づき Mobility IQ は、「どの階が混雑しているか」とか「どの洗面所が混んでいるか」といったコンシューマの質問に対する回答を提示します。後者の指標を利用した理論では、WiFi エリア内のサービスのオペレータは、エンド ユーザに割引の通知を送ることで、カスタマーを誘導することができます。

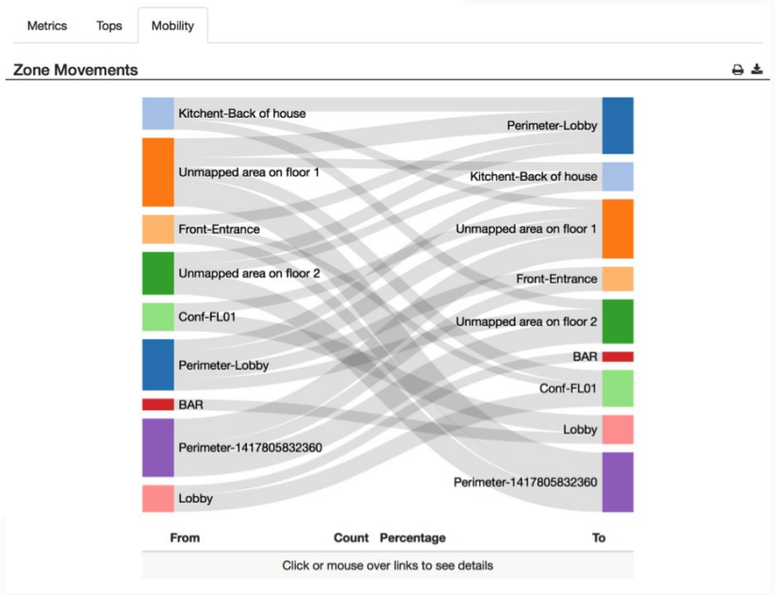

図 23：Mobility IQ Zone Movement の例

シスコは、洗練されたさまざまな Web インターフェイスを実際に見せてくれました。そのインターフェイスでは、さまざまな KPI の概要が表示され、CSP はビューをさらに調整し、組織レベルへのアクセスを提供できるようになります。その機能の詳細の他に興味深かった点は、シスコが CSP に期待するサービスの使用方法でした。シスコがサービス プロバイダーに Mobility IQ を販売して全体を統合することで、サービス プロバイダーはサービスの再ブランド化「だけ」すればよい、というものでした。

今回もシステムが稼働中だったので、統計収集などの要素にアクセスしたり、WiFi アクセス ポイントの障害をシミュレーションすることはできませんでした。システムは実際のもので、稼動可能なことは確認できます。Project Squared とあわせて、将来のテストで稼働中のシステムを検証できることを期待しています。

結論：有意義な開発

EANTC は、2013 年 7 月の 3 回目の会議から、ETSI Network Functions Virtualization Industry Specification Group（NFV ISG）の補助メンバーとなっています。ISG はその設立時に、ビジョン、原動力、進捗状況、および結果の概要を示す 3 つのホワイト ペーパーをリリースしました。NFV の概念がまとまり始めた際、ISG の CSP メンバーは「標準化の取り組みが長期化するのを避けることで推進力を維持する」ことを確認しあいました。

このレポートでは、シスコの仮想化ソリューションが本物であることを確認できました。レポートで示したように、シスコの Cloud VPN は NFV のアーキテクチャを忠実に守っているように思われます。私たちは、シスコのソリューションは、少なくとも 1 つのサード パーティ デバイスで機能し、サービスを統合および管理するために、フリー ソフトウェアや IETF で定義された標準インターフェイスを使用していることも検証しました。

このレポートは、既存の標準およびコードに基づく実際の具体的な推進力を示すものです。ちょうどそれは、IP セクターの巨人からもたらされることになりました。帽子を脱いで敬意を表します。

— Jambi I. Ganbar（シニア テクニカル マーケティング マネージャ）、Carsten Rossenhövel（最高業務責任者）、European Advanced Network Test Center AG（EANTC、ベルリンの独立したテスト ラボ、http://www.eantc.de/）

EANTC は、メーカー、サービス プロバイダー、およびその他の企業に対してベンダー中立なネットワーク テスト設備を提供しています。