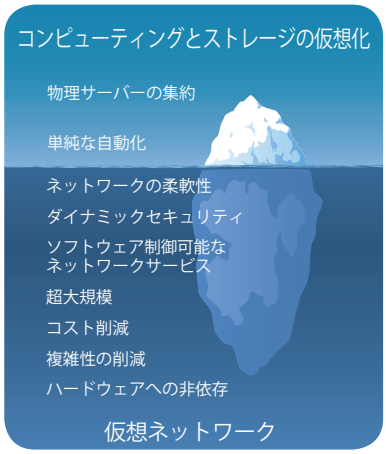
ネットワークは仮想化の時代へ

クラウドデータセンター向けネットワーク仮想化



変革

この10年間に開発されたコンピューティングおよびストレージの仮想化技術によって、ホスティングプロバイダーや企業、政府関係機関は、効率性と柔軟性を大幅に改善することができました。しかし、今日の仮想化技術は氷山の一角にすぎません。

クラウドデータセンターでは、オペレーターが仮想化の利点をフル活用すべく奮闘していますが、それも限界にきています。本来ダイナミックなものであるクラウドサービスには、より優れた柔軟性や拡張性、プログラマビリティが必要です。今日のデータセンターネットワークでは、その要求条件に応えることが出来ません。物理ネットワークはパケット転送には優れていますが、柔軟性に欠け、複雑かつコストもかかることが、クラウドサービスに必要とされる敏捷性を実現するための障壁となっています。
その結果、企業や政府関係機関が、大切なアプリケーションやデータをクラウドに移行することを妨げています。まさに、ネットワークこそがコンピューティングとストレージ仮想化への道を閉ざしてしまっているのです。

ネットワーキングは、この変革の波に乗り遅れています。それどころか、デバイスごとに手動でプロビジョニングするように設計された20年前の運用モデルのなかで、身動きがとれなくなっています。ネットワークは、何百もの個々のデバイスからなる、過剰に複雑で脆弱なシステムです。それらデバイスをつなぎ合わせるインターフェースは複雑でしばしばベンダー独自のものであり、ネットワーク全体をコントロールするAPIもありません。

障壁

ネットワークはクラウドコンピューティングの可能性を実現するための障壁となっています。ネットワークサービスは、物理ネットワークのハードウェアとトポロジーに縛られています。そのために、拡張性が限定されると同時に、ますます複雑性が増すため、膨大なコストがかかってしまうのです。有効な解決策がないまま、多くのデータセンターではカスタムCLIスクリプトを開発してハードウェアのプロビジョニングと設定の自動化を図っています。このようなアプローチは一時しのぎのもので、根本的な問題の解決にはならないばかりか、多くの場合、高額なハードウェアのアップグレードが必要になったり、ネットワークの運用がますます特定のベンダーに縛られることになってしまいます。

解決策

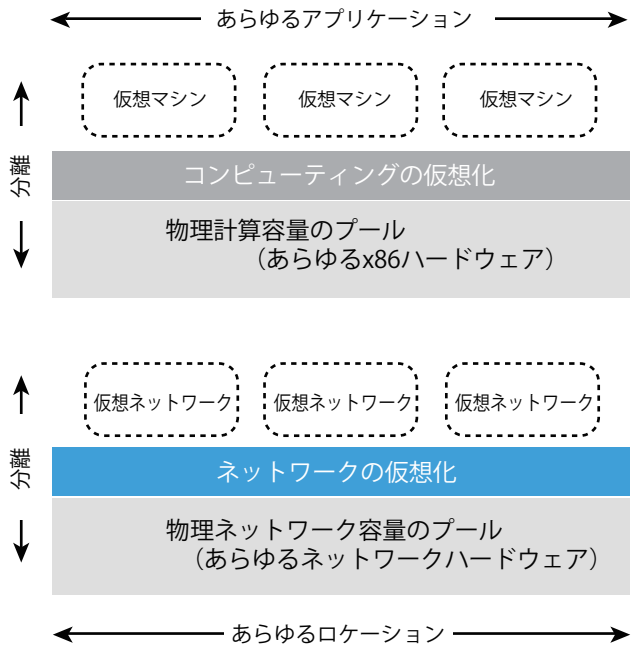
ネットワークを仮想化することです。サーバー仮想化が、基盤となるハードウェアからワークロードを分離・独立するように、ネットワーク仮想化は、ネットワークサービスを物理ネットワークのハードウェアから切り離すことができます。これにより、クラウドのニーズを満たすことのできる敏捷な仮想ネットワークを、初めてプログラマチックに生みだすことが可能になります。

nicira

分離

Niciraは、ネットワークをクラウド対応させる初のネットワーク仮想化プラットフォームを提供します。NiciraのNetwork Virtualization Platform（NVP）は、既存のIPネットワークのエッジに展開するソフトウェアです。仮想空間内でネットワーキング環境を忠実に再現します。サーバーハイパーバイザーが物理サーバーを計算容量プールに変換するのと同じように、NVPが物理ネットワークをネットワーク容量の汎用プールに変換します。物理ハードウェアから仮想ネットワークを切り離すことで、その物理ハードウェア上で動いている仮想ネットワークに影響を与えることなく、ネットワーク容量の拡張を可能にします。

これにより、役割を単純なIP接続の提供のみとされた物理ネットワークに対する要求はごく限定的なものとなり、専門特化したハードウェア機能は不要となってしまいました。物理インフラから切り離して運用される仮想ネットワークに影響を与えることなく、ハードウェアに依存しない能力の追加が可能です。



VLANの終焉

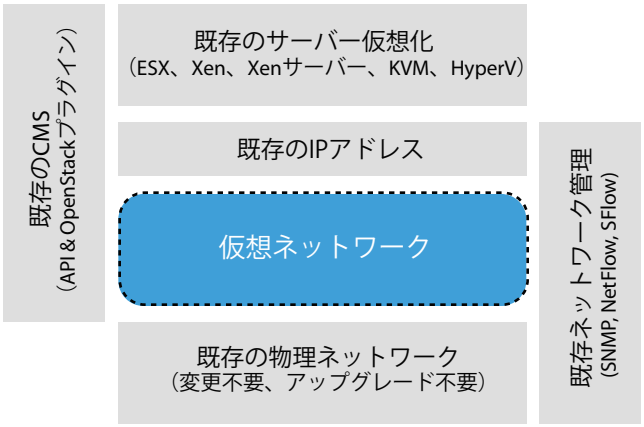
現在、複雑なL2ネットワークを作成・管理するには、ハードウェアを再設定して、VLANをデータセンターの別の場所まで延長することが必要です。VLANの限界は悩みの種ではないですか？　L2接続を顧客のデータセンターまで拡張したいとお考えですか？物理的マシンと仮想マシンを同じL2ネットワークに接続したいですか？　これらの質問に一つでも該当するものがあれば、ネットワークを仮想化する必要があります。

Niciraの仮想ネットワークは、ネットワークハードウェアから完全に分離し、お互いに独立した、何万もの仮想ネットワーク（最大のVLAN設定が提供する独立したドメインとは桁違いに多い）を動的にプロビジョニング可能です。仮想ネットワークは、既存の物理VLANに接続できますが、仮想ネットワークのアーキテクチャはVLANを必要としていません。

それぞれの仮想ネットワークは、企業ネットワークサービスに期待される全ての機能を持ったハードウェアベースのEthernetスイッチと全く同等のものです。違うのは、仮想ネットワークのポートはプログラム的にプロビジョニングされており、仮想マシンと共に、データセンター内あるいは複数のデータセンター間のどこにでも必要に応じて設置したり移動したりできることです。

独立性

ネットワークを仮想化すると、クラウドサービスのプロバイダーはベンダーによる囲い込みや、ネットワークハードウェアの更新などの悩みからも解放されます。新たなネットワーク機能を実現するのに、費用のかかるハードウェアのアップグレードが必要、という時代は終わりました。もしもすでにIP接続できるハードウェアを所有しているのであれば、物理ネットワークに必要なものはそろっていると言えます。Niciraは、ハードウェアのアップグレードを求めません。それにかわって、既存の物理ネットワークをIPバックプレーンに変換するコントロールクラスタが管理するインテリジェントネットワークエッジを、NVPが生成します。それにより、何万もの敏捷な仮想ネットワークをプログラマチックに構築することが可能になり、クラウド上のどこにでも作業負荷を分散することができます。NVPによって可能となる活用事例は以下の通りです。



既存の物理ネットワークへの投資

既存のネットワークが、従来のネットワークハードウェアまたは、名の知れたスーパースイッチの最新総合システムにて構築されたものであっても、IPトラフィックを転送できるのであれば、仮想化してクラウドをサポートすることが可能です。

既存サーバーの仮想化ソリューション

Niciraのソフトウェアは、ESX、Xen、Xenサーバー、KVM、HyperVなど、計算処理およびストレージ向けの多種多様な仮想化ソリューションとの高い親和性を実現し、分断されることなく、シームレスなITの運用を可能にします。さらに、複数のハイパーバイザーが混在している環境間において、作業負荷の移動に対応します。

既存のクラウド管理システム

Niciraは、既存のクラウド管理システム（CMS）または、それに取って代わりつつあるOpenStackなどと統合されることで、テナントごとに独立した仮想ネットワークの構築を自動化します。

既存の管理ツール

仮想ネットワークは、これまで物理ネットワーク（SNMP、NetFlow、sFlow）で使い慣れたモニター機能を提供します。

既存のIPアドレス

お客様のものも含め、IPアドレスを変更する必要はありません。そのため、クラウドへの作業負荷の移行を迅速化できます。

コントロール

ネットワークを仮想化すれば、ハードウェアの限界も物理的な境界もなくなり、クラウドは、新たなネットワークコンピューティングの時代へと入っていきます。しかし、クラウドコンピューティングの要となるのが、データおよびアプリケーションのコントロールとセキュリティであることに変わりはありません。ネットワーク仮想化はこのどちらもサポートします。

作業負荷をどこにでも分散配置

クラウドサービスのプロバイダーは、顧客が物理的な容量制限を超えるシステム運用をするたびに、ネットワークをクラウドで運用することの限界に突き当たります。データセンターには柔軟な計算能力がありますが、物理的に分離されており、ネットワークを拡張して顧客のニーズに応えるには、複雑でコストのかかる手動によるネットワークハードウェアの再設定が必要です。

Niciraのネットワーク仮想化ソリューションは、完全に独立した、マルチテナントクラウド環境をサポートします。つまり、クラウドデータセンターネットワークが、ダイナミックで拡張性の高い、マルチテナント環境になるということです。そこでは、何万という仮想レイヤー2ネットワークがたがいに独立しています。さらに、基盤となる物理的ファブリックに依存することなく、プログラマチックに作業負荷を分散配置することができるのです。物理的負荷も仮想負荷も、物理的なIPサブネットをまたいでデータセンター同士で、さらには顧客のデータセンターともつながって、1つの仮想ネットワーク上でダイナミックに結合・連動させることができます。

Niciraは、CMSと統合してテナントごとに分離された仮想ネットワークを自動的に構築します。仮想ネットワークは、テナント側からはL2スイッチのように見えます。しかし、それぞれの仮想ポートはL2～L7のサービスをサポートするので、L2接続から始めて、テナントの要求に応じて、追加サービスをダイナミックに積み重ねていくことができます。仮想ポートは、プログラムで生成し、要望に応じてデータセンターのどこにでも、物理負荷にも仮想負荷にも結合できます。仮想ネットワークは物理的なIPサブネットにまたがって、展開されるため、物理ネットワークをテナントの分離とは別に、分割・運用することができます。

クラウドのためのダイナミックセキュリティ

物理ネットワークでは、多くの場合、セキュリティは「チョークポイント」モデルを利用して構築されています。ネットワークセキュリティポリシーは、ネットワークを往来するトラフィックとして位置づけられ、アクセスの可否を手動で設定したルールやアクセスコントロールリストを備えたルーター、あるいはファイアウォールなどのインラインデバイスを通過します。「チョークポイント」モデルは、クラウドでは機能しません。クラウドはダイナミックに設計されていて、仮想マシン（VM）が行き来して移動し、ネットワークはつねに変化しつづけるものだからです。

Niciraは、ネットワークセキュリティの難題を解決します。仮想化ネットワークでは、セキュリティポリシーはプログラマチックに設定して、中央一元管理できるため、ネットワークのエッジに留めることができます。悪意のあるトラフィックは、ソースエッジにて瞬時に遮断されます。このモデルのもう一つの利点は、VMが移動したり、新しいハイパーバイザーが追加されたり、あるいは物理ネットワークデバイスが更新・交換された場合に、セキュリティポリシーもつねに更新されるということです。

仮想ネットワーク同士、および仮想ネットワークと物理コントロールネットワークのあいだには、完全なアドレス空間の分離があります。VMから送信されるパケットには一切の解釈が加えられず、その結果、システムは、なりすましや侵害されたVMなどの影響を受けないだけでなく、悪用される恐れのあるダイナミックトランキングやマルチキャスト、ディスカバリといったコントロールプロトコルもありません。

企業をクラウドへ移行

多くの企業がクラウドコンピューティングの利点を活用しようとしていますが、それには現行の業務を中断することなく、アプリケーションをクラウドへシームレスに移行させるソリューションが必要です。

Niciraは、仮想ネットワークをデータセンター全体に、そしてデータセンター同士に、さらには顧客の領域にまで拡張することを可能にします。仮想ネットワークはたがいに独立しながら、重なり合うMACおよびIPアドレスをサポートします。1つのサーバーハイパーバイザーにかかる作業負荷はさまざまなテナントに割り当てられ、独立性を保ちます。

サービスプロバイダーは、新しい企業顧客を難なく取りこむことができ、企業は既存のIP設定をそのまま維持できます。企業は、自社領域でもクラウドデータセンターでも、すべて同じL2ブロードキャストドメインで作業負荷をホストできます。

既存のハードウェアを拡縮

Niciraは、クラウド運営者が既存のネットワークハードウェアをさらに大きなスケールに拡張することを支援します。

すべてのネットワークハードウェアには限界があります。クラウドプロバイダーにとっては、VLAN限界とMACテーブル限界の2つが主なものです。仮想環境では、何万もの独立した仮想ネットワークが構築され、基盤となるハードウェアに依存することなく運用されます。したがって、VLANの限界に影響されることはありません。それに加えて、仮想ネットワークのアーキテクチャが物理スイッチに知らせるのは、物理ネットワークインターフェースカードのMACアドレスだけです。VMのMACアドレスは物理スイッチから取りだされるために物理スイッチには見えず、大幅な拡張が可能になります。

適切な運用モデル

クラウドでのダイナミックなサービスをコスト効率よく提供するため、サービスプロバイダーは、運営を自動化および最適化しなくてはなりません。Niciraは「ハンズオフ」でのサービス提供を可能にします。VMのほかに、仮想ネットワークや仮想ポート、ネットワークサービスおよびポリシーをプロビジョニングおよびプロビジョニングプロビジョニングの解除を実行するため、アプリケーションは、プログラムから随時にCMSと連動することができます。また、リソースを最適化するためにVMを移行する際、ネットワークサービス、ポリシーおよびVMと連動するテナント使用カウンターは、人の手を介さず、VMをデータセンター内のどこにでも移動することができます。

正確な従量課金

微細なポートレベルでのモニタリング機能が、ポートごと、サービスごと、時間ごとに使用量を正確に測定するため、コストと収益をきっちりとあわせたり、使用量に応じて正確に課金したりできます。

既存のIPv4インフラをしのぐIPv6

Niciraは、既存のIPv4物理インフラ上の仮想ネットワークで、IPv6エンドホストがシームレスに通信できるようにします。

地域によって、すでにIPv4アドレスが不足しているところがあります。飛躍的な成長を期待していながら、まだIPv6をサポートするようにネットワークインフラを最適化していないクラウドサービスのプロバイダーにとっては、これは深刻な問題です。Niciraは、魅力的なソリューションを提供します。仮想化ネットワークアーキテクチャの産物として、既存のIPv4物理インフラにある仮想ネットワーク上でIPv6エンドホストがシームレスに通信できるようにします。さらに、仮想ネットワークが独立しているという性質を活かして、仮想データセンターはIPv4仮想ネットワークもIPv6仮想ネットワークも、同じIPv4インフラ上でサポートできます。

ネットワーク仮想化チェックリスト

多くの製品がネットワークの仮想化を提供するとしていますが、そのほとんどはネットワーク仮想化とは呼べないものです。次の7つの重要な機能を提供していなければ、ネットワーク仮想化とは呼べません。

- ☐ 仮想ネットワークを、基盤となるネットワークハードウェアから完全に分離
- ☐ 論理空間に物理ネットワークサービスを忠実に再現
- ☐ 全てのサーバーハイパーバイザープラットフォームをサポートし、すべての仮想または物理マシン上で動作する、すべてのアプリケーションをサポート
- ☐ 複数の仮想ネットワーク間、および、と物理ネットワークやコントロールプレーンとの間で、セキュア なアドレス空間分離を提供
- ☐ プログラム的なプロビジョニングおよび仮想ネットワークコントロールが可能
- ☐ クラウドに必要なスケールへの拡張が可能（1万個以上の仮想ネットワーク）
- ☐ 物理ネットワーク容量を最大限に活用

サービス

クラウドサービスのプロバイダーが仮想化コンピューティングサービスを追加することは、いまや一般的な運営手法となっています。弾力的なコンピューティングおよびストレージ容量をダイナミックにプロビジョニングすることで、今日のクラウドのあり方が明確になります。しかし、セキュリティアクセスコントロールおよびサービスの質（QoS）保証などの、ポートレベルでのネットワークサービスを必要に応じてプロビジョニングすることは、サービスプロバイダーには手の届かないものでした。手動操作には、ダイナミックな環境でのそれらサービスのプロビジョニングやモニター、説明などが要求されるためです。

Niciraは、一般商品のネットワーク接続レベルから、企業のネットワークサービスレベルまで、すべてを同じ物理インフラでプロビジョニングした、ダイナミックな階層を形成するネットワークサービスモデルを可能にします。さらに、ネットワークサービスをポートごと、時間ごとに、プログラマチックにプロビジョニングし説明することができます。そうすることで、ネットワークサービスは随時ダイナミックにプロビジョニングされ、従量制の課金が可能になります。

業界初：APIをネットワークに

従来のネットワーキングモデルがサポートするのは、複雑なCLIスクリプトや融通のきかないプロセスに基づいて限定的に自動化されたハードウェアレイヤーの管理、または編成のみです。物理ネットワークを仮想ネットワークサービスから切り離すことで、NVPはビジネスとサービスを加速する独自の機能を提供します。ネットワークへのAPIの提供です。

図が示す通り、Niciraは、クラウドサービスを差別化する基礎的要素となる、レイヤー4～7のサービスを提供します。Niciraは、仮想クラウド環境独自のネットワークサービスを構築・提供しています。APIは、クラウドサービスのプロバイダー自身によってプラットフォームに書き込まれたファイアウォールまたは差別化したネットワークサービスのような、サードパーティのサービスと統合します。

それと同時に、プログラムによるこのようなアプローチは、物理ハードウェアに縛られているために発生する運用コストを削減し、ダイナミックなプロビジョニングサービスを手の届くものにします。これまでは、クラウドサービスのプロバイダーは、完全な企業ネットワークサービスモデルの提供か、仮想化の運用モデルか、どちらかを選ばなくてはなりませんでした。Niciraの仮想ネットワークなら、両方の最良のもの――ダイナミックネットワークセキュリティ、QoS、可視性、柔軟な拡張性、自動化したプロビジョニング、必要に応じたネットワークサービス、従量課金制――など、仮想化による運用効率のすべてを選択できます。

NVPー初のネットワーク仮想化プラットフォーム

Niciraは、分散型システムによって管理された既存のネットワークの周辺にインテリジェントネットワークエッジを構築し、物理ネットワークをIPバックプレーンに変換することで、クラウド内の作業負荷にアクセスする何万もの敏捷な仮想ネットワークの構築をプログラマチックに実行します。

インテリジェントエッジ

Open　vSwitch（OVS）は、インテリジェントエッジの中心となるコンポーネントです。OVSは遠隔操作のために設計されたスイッチソフトウェアです。OVSは現在、Niciraの仮想ネットワークにて、2通りの方法で展開しています（下図参照）。

1つめは、最も広く展開しているサーバーハイパーバイザーのOVSで、既存のESX、Xen、Xenサーバー、KVM、およびHyperVで動作する、包括的なソフトウェアソリューションです。

2つめは、仮想または物理的アプライアンスのOVSと一緒になった「ゲートウェイ」アプローチです。ゲートウェイはもともと、時代遅れの物理ネットワークに統合して展開されるもので、例としてVLAN全体を同じ仮想ネットワーク上のクラウドデータセンターに接続したり、仮想ネットワークをインターネットに接続したりするものがあります。

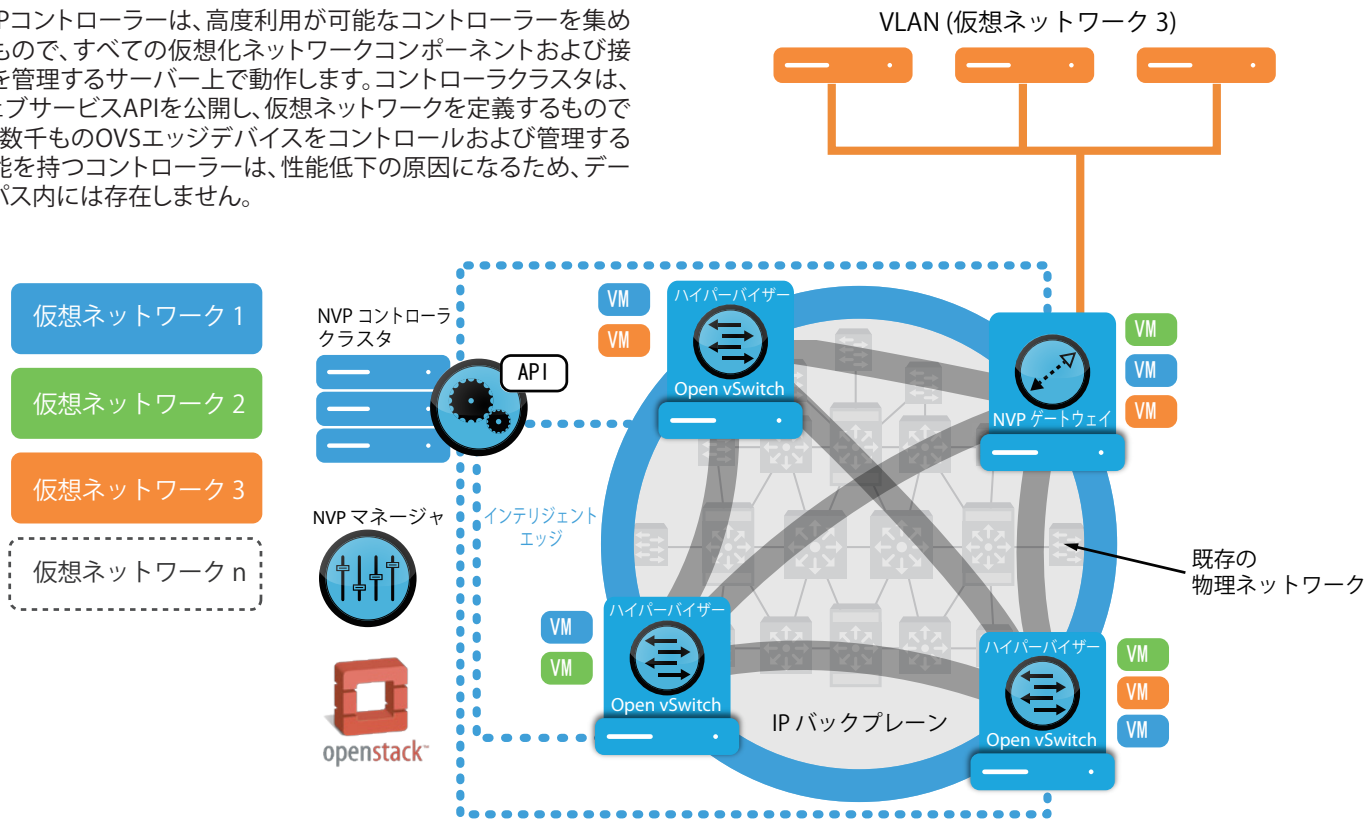
コントローラクラスタ

NVPコントローラーは、高度利用が可能なコントローラーを集めたもので、すべての仮想化ネットワークコンポーネントおよび接続を管理するサーバー上で動作します。コントローラクラスタは、ウェブサービスAPIを公開し、仮想ネットワークを定義するものです。数千ものOVSエッジデバイスをコントロールおよび管理する機能を持つコントローラーは、性能低下の原因になるため、データパス内には存在しません。

ネットワーク全体の仮想化は、クラウドコンピューティングの将来性に出資するためには大切なステップです。きちんとした将来的ネットワーク運用モデルは、必要に応じて独立した確かなネットワークの構築、削除、拡大、縮小、移行を可能にします。また、物理サーバーが仮想負荷の計算容量用汎用プールとして使われるのと同様にして、既存の物理ネットワークをネットワーク容量の汎用プールとして活用します。

仮想化ネットワークは、仮想化コンピューティングがサーバーの展開モデルを変えたように、物理ネットワークのハードウェア展開モデルを変えます。新たな展開モデルでは、すべての物理デバイスをいったんラックに乗せてケーブルをつないでしまえば、必要に応じてプログラムからプロビジョニングおよび再目的化することができます。仮想化ネットワークは、ベンダーによる囲い込みを排除し、最適価格の性能ソリューションを使って、物理IPファブリックを構築させることができます。

Niciraは、従来の物理ネットワーキングの標準的な特性を、クラウドの運用上の要件と組み合わせることで、ネットワークに仮想化という柔軟性を提供します。



Niciraについて

Niciraは、ネットワークを仮想化する企業です。Network Virtualisation Platform（NVP）は、仮想化ネットワークインフラのダイナミックな構築を可能にし、物理ネットワークのハードウェアから完全に分離・独立したサービスを実現します。AT&T、eBay、Fidelity Investments、NTT、Rackspaceなどの革新的企業が、NiciraのNVPを使ってサービスの提供を週単位から分単位へと加速すると同時に、複雑性とコストを大幅に削減しています。詳しくはウェブサイトwww.nicira.comをご覧ください。

Nicira 3460 West Bayshore Road Palo Alto, CA 94303 U.S.A.
Tel +1.650.473.9777 Fax +1.650.739.0997 info@nicira.com www.nicira.com