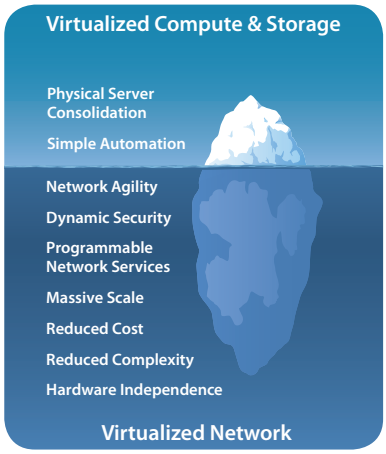
It's Time to Virtualize the Network.

Network Virtualization for Cloud Data Centers



TRANSFORMATION

Hosting providers, enterprises and government agencies have gained significant efficiency and flexibility as a direct result of the compute and storage virtualization technologies developed over the past decade. However, current virtualization technologies are only the tip of the iceberg.

In cloud data centers, operators strive to leverage the full benefits of virtualization, but have reached a barrier. The dynamic nature of cloud services requires a new level of flexibility, scalability and programmability. These requirements go beyond the capabilities of today's data center networks. The physical network – while excellent at forwarding packets – is an inflexible, complex and costly barrier to realizing the full agility required by cloud services. As a result, it hinders the ability of enterprises and government agencies to onboard critical applications and data to the cloud. Indeed, the network has gated the success of compute and storage virtualization.

Networking has not kept pace with this transformation and instead is bogged down in a 20-year-old operational model originally designed for manual provisioning on a device-by-device basis. Networks are overly complicated, fragile systems constructed from hundreds of individual devices tied together by complex and frequently vendor-specific interfaces with no programmatic interface for network-wide control.

THE BARRIER

The network is a barrier to achieving the promise of cloud computing. Network services are bound to physical network hardware and topology. This binding results in limited scalability, increased complexity and inflated costs for customers. In the absence of a viable solution, many data centers develop custom CLI scripts to automate hardware provisioning and configuration. A stopgap, this approach does not fix the underlying problem and, in most cases, requires expensive hardware upgrades and binds network operations even more tightly to a particular vendor.

THE SOLUTION

Virtualize the network. Just as server virtualization decouples and isolates the workload from the underlying hardware, network virtualization decouples network services from the underlying physical network hardware. This enables programmatic creation of agile, virtual networks that meet the needs of clouds for the first time.

nicira

DECOUPLE

Nicira delivers the first network virtualization platform that enables the network for cloud. Nicira's Network Virtualization Platform (NVP) is software that operates at the edge of any existing IP network and faithfully reproduces the entire networking environment in the virtual space. NVP transforms a physical network into a generalized pool of network capacity, like a server hypervisor transforms physical servers into a pool of compute capacity. Decoupling virtual networks from the physical hardware allows you to scale the pool of network capacity without affecting the virtual networks operating above it.

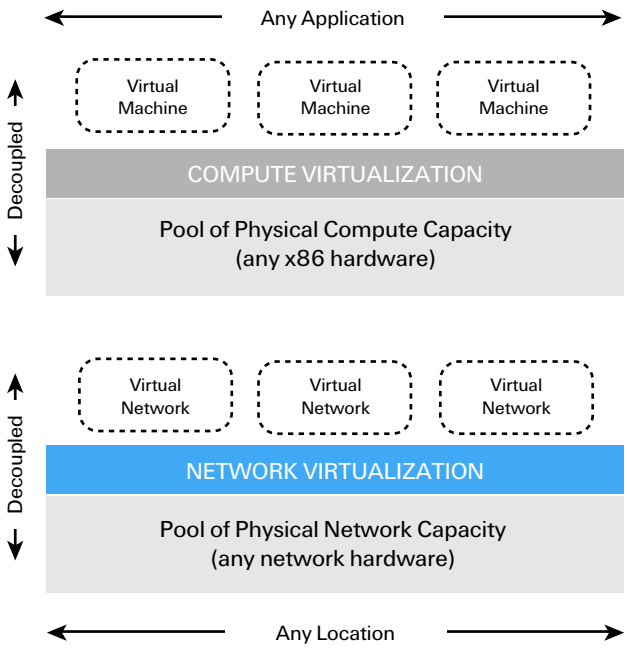
Now relegated to delivering simple IP connectivity, the demands on the physical network are greatly reduced and requirements for specialized hardware features are eliminated. Hardware independent capacity can be added as required without affecting the virtual networks operating decoupled from the physical infrastructure.

THE END OF THE VLAN

Today, creating and managing complex L2 networks usually requires reconfiguration of hardware to extend VLANs to another part of the data center. Are VLAN limits one of your concerns? Would you like to be able to extend L2 connectivity into your customer's data center? Do you want both physical and virtual workloads to be on the same L2 network? If you answered yes to any of these questions, you need to virtualize your network.

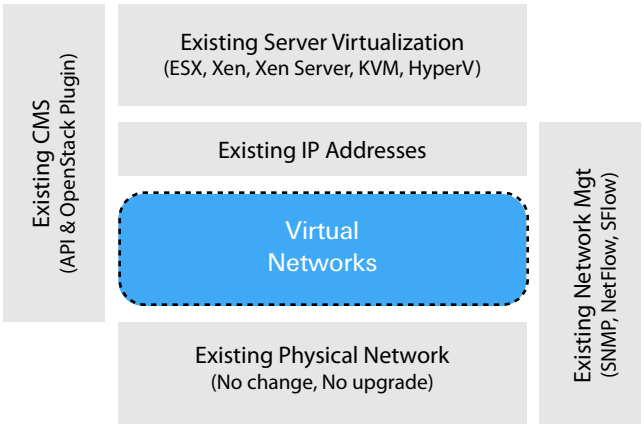
A Nicira virtualized network supports many tens of thousands of dynamically provisioned, fully isolated virtual networks, completely decoupled from the underlying network hardware (this is an order of magnitude larger than the isolation domains provided by the largest VLAN configurations). Virtual networks are able to connect into existing physical VLANs, but VLANs are not required by the architecture.

Each virtual network is equivalent to a hardware-based Ethernet switch, with all of the enterprise network services you expect. The difference is that virtual network ports are programmatically provisioned, attached to workloads and placed or moved on demand, anywhere in the data center or across multiple data centers.



INDEPENDENCE

Network virtualization frees cloud service providers from the tyranny of vendor lock-in, including slow network hardware upgrade cycles. The days of requiring costly hardware upgrades to realize new network capabilities are over. If your hardware provides IP connectivity, you already have what is needed for the physical network. Nicira requires no hardware upgrades. Instead, NVP creates an intelligent network edge managed by a control cluster that transforms your existing physical network into an IP backplane and enables the programmatic creation of 10s of thousands of agile virtual networks to connect workloads anywhere in your cloud. NVP lets you leverage your:



Existing physical network investment
Whether your existing network is built on traditional network hardware or the latest integrated system of brand name super switches, if it forwards IP traffic, it can be virtualized and can support your cloud.

Existing server virtualization solution
Deployed without disruption, Nicira software operates seamlessly with your compute and storage virtualization solution, whether it's ESX, Xen, Xen Server, KVM or HyperV. Moreover, it supports workload mobility in mixed hypervisor environments.

Existing Cloud Management System
Nicira programmatically integrates with your existing Cloud Management System (CMS) or emerging alternatives like OpenStack to automate the creation of isolated virtual networks for each tenant.

Existing management tools
Virtual networks deliver the visibility you are used to in physical networks (SNMP, NetFlow, sFlow). Virtual network traffic looks the same to your management tools.

Existing IP addresses
There is no need to change your IP addresses or force your customers to change theirs. This accelerates onboarding of workloads to the cloud.

CONTROL

Virtualize your network, and your cloud enters a new era of network computing where hardware limitations and physical boundaries vanish. However, the key requirements of cloud computing remain control of data, applications and security. Network virtualization supports both objectives.

Place any workload, anywhere

Cloud service providers are painfully reminded of the barrier the network is to their cloud operations each time a tenant grows beyond the compute capacity built into its physical pod. While flexible compute capacity exists in the data center, it is physically isolated and requires costly and complex manual reconfiguration of network hardware to extend the network and meet customer needs.

Nicira's network virtualization solution supports fully isolated, multi-tenant cloud environments. This means the cloud data center network becomes a dynamic, highly scalable, multi-tenant environment in which tens of thousands of virtual Layer 2 networks are fully isolated from each other. In addition, you can now programmatically place any workload anywhere, independent of the underlying physical fabric. Both physical and virtual workloads can be dynamically joined on the same virtual network that spans physical IP subnets, across and between data centers and even into customer data centers.

Nicira integrates with your CMS to automate the creation of isolated virtual networks for each tenant. A virtual network appears as an L2 switch to tenants. However, each virtual port supports L2-L7 services, so you can tier service offerings, beginning with L2 connectivity and dynamically adding additional services as required by a tenant. Virtual ports are programmatically created and attached to either physical or virtual workloads, anywhere in the data center, on demand. Virtual networks span physical IP subnets, allowing the physical network to be engineered and segmented independently from tenant isolation.

Dynamic security for clouds

In physical networks, security is often built using a "choke point" model. Network security policy is enforced as traffic traverses the network and passes through inline devices such as routers or firewalls with rules or access control lists, which are manually configured to allow or deny access. The "choke point" model simply does not work for clouds. Clouds are dynamic by design; VMs come up, go down, move and the network is expected to change continuously.

Nicira transforms the network security equation. In a virtualized network, security policies can be programmatically configured and centrally managed, then pushed to and enforced at the edge of the network. Malicious traffic is dropped immediately at the source edge. An added benefit of this model is that security policies are always up-to-date even when VMs move, new hypervisors are added or physical network devices are updated or replaced.

There is complete address space isolation between virtual networks, and between virtual networks and physical and control networks. There is no interpretation of any part of any packet sent by the VM, and as a result, the system is impervious to spoofing or compromised VMs and there are no control protocols, such as dynamic trunking, multicast or discovery, which could be exploited..

Migrate enterprise to cloud

Many companies are eager to take advantage of the benefits of cloud computing, but they need a solution that allows them to migrate applications seamlessly into the cloud, without disrupting current operations.

Nicira enables virtual networks to span throughout a data center, between data centers and even onto customer premises. Virtual networks are fully isolated from each other, supporting overlapping MAC and IP addresses. Workloads on the same server hypervisor can be assigned to different tenants and remain fully isolated.

Service providers are able to painlessly onboard new enterprise customers, allowing the enterprise to maintain existing IP configurations. Enterprises can host workloads both on premises and in the cloud data center, all on the same L2 broadcast domain.

Scaling your existing hardware

Nicira enables cloud operators to obtain greater scale from their existing network hardware.

All network hardware has limitations. Two key limitations for cloud providers are VLAN limits and MAC table limits. In a virtualized

environment, tens of thousands of isolated virtual networks can be created and operated independently from the underlying hardware and therefore are not affected by VLAN limitations. Additionally, the architecture of a virtualized network exposes only the MAC addresses of physical network interface cards to physical switches. The MAC addresses of the VMs are abstracted from and therefore invisible to physical switches, enabling far greater scale.

The right operational model

In order to cost effectively offer dynamic services in the cloud, service providers must be able to automate and optimize operations. Nicira enables "hands off" service delivery. Applications are able to programmatically interface with the CMS to provision and de-provision virtual networks, virtual ports, network services and policies along with VMs, on demand. Then, when VMs migrate to optimize resources, the network services, policies and tenant usage counters move with the VM, anywhere in the data center, with no human interaction.

Accurate, pay-as-you-go accounting

Fine grain port-level visibility accurately measures usage on a, per-port, per-service, per-hour basis, allowing you to tightly align costs with revenue and accurately bill based on usage.

IPv6 over existing IPv4 infrastructure

Nicira allows IPv6 end hosts to communicate seamlessly over virtual networks on an existing IPv4 physical infrastructure.

Some Regional Internet Registries have already run out of IPv4 address space. This is a serious concern for cloud service providers who are expecting significant growth, but have not upgraded their network infrastructure to support IPv6. Nicira offers an attractive solution. Simply as a product of the virtualized network architecture, Nicira allows IPv6 end hosts to communicate seamlessly over virtual networks on an existing IPv4 physical infrastructure. Additionally, leveraging the isolated nature of the virtual networks, the virtualized data center can support both IPv4 virtual networks and IPv6 virtual networks on the same IPv4 infrastructure.

Network Virtualization Checklist

Many products claim to provide network virtualization, but most do not. The following are the seven key features any network virtualization must deliver.

- ☐ Completely decouple virtual networks from the underlying network hardware
- ☐ Faithfully reproduce physical network services in the logical space
- ☐ Complement any server hypervisor platform, and any application on any virtual or physical machine
- ☐ Provide secure address space isolation between virtual networks, the physical network and the control plane
- ☐ Allow programmatic provisioning and virtual network control
- ☐ Enable cloud scale (>10K virtual networks)
- ☐ Take full advantage of physical network capacity

SERVICES

Adding virtualized compute services is now standard operating procedure for cloud service providers. Dynamic provisioning of elastic compute and storage capacity defines cloud as we know it today. However, on-demand provisioning of port level network services, such as security access control and quality of service (QoS) guarantees, have been out of reach for services providers because of the manual operations required to provision, monitor and account for such services in a dynamic environment.

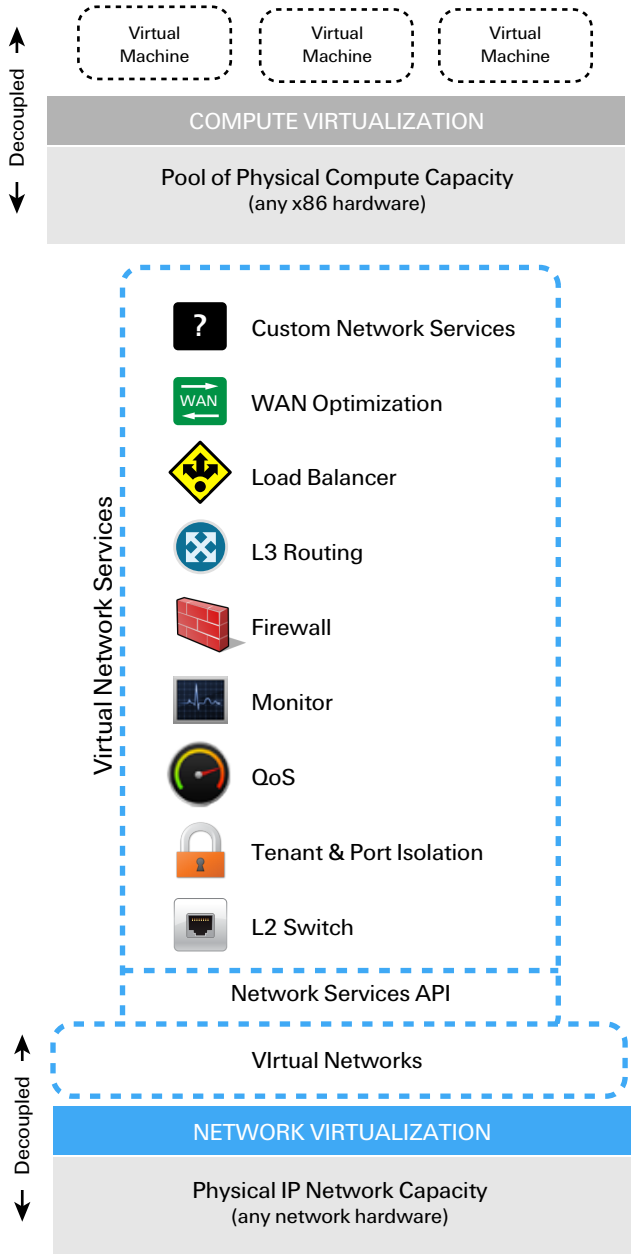
Nicira enables a dynamically tiered network service model, ranging from commodity level network connectivity to enterprise class network services, all provisioned on the same physical infrastructure. Moreover, Nicira enables network services to be programmatically provisioned and accounted for on a per-port, per-hour basis. This allows network services to be dynamically provisioned on demand, and charged for on a pay-as-you-go basis.

AN API INTO THE NETWORK: AN INDUSTRY FIRST

Traditional networking models only support management or orchestration of the hardware layer with limited automation based on complex CLI scripts and inflexible processes. By decoupling the physical network from virtual network services, NVP provides a unique capability that accelerates business and services velocity: it provides an API into the network.

As the diagram illustrates, this means that Nicira can provide Layer 4-7 services, which are the building blocks for differentiated cloud services. Moreover, Nicira is creating network services that are unique to virtualized cloud environments. The API integrates with third-party services such as firewalls or differentiated network services written to the platform by the cloud service provider itself.

And at the same time, this programmatic approach eliminates the operational costs which, when bound to physical hardware, put such dynamic provisioning services out of reach. In the past, cloud services providers had to choose between offering a complete enterprise network service model or an operational model of virtualization. A Nicira virtualized network enables the best of both worlds — dynamic network security, QoS, visibility, elastic scale, automated provisioning, on-demand network services and pay-as-you-go pricing — all with the operational efficiency of virtualization.



NVP - The First Network Virtualization Platform

Nicira creates an intelligent network edge around your existing network, managed by a distributed system, that transforms your physical network into an IP backplane and enables the programmatic creation of tens of thousands of agile virtual networks to connect workloads in your cloud.

An intelligent edge

Open vSwitch (OVS) is the core component on the intelligent edge. OVS is switch software designed for remote control. OVS is currently deployed in two ways at the edge of a Nicira virtualized network. (See diagram below).

First, and most widely deployed, is OVS in the server hypervisor, a complete software solution that works with your existing ESX, Xen, Xen Server, KVM and HyperV hypervisors.

Second is the "gateway" approach, with OVS deployed in a virtual or physical appliance. The gateway is primarily deployed to integrate with legacy physical networks, for example, to connect an entire VLAN into the cloud data center on the same virtual network or for connecting virtual networks to the Internet.

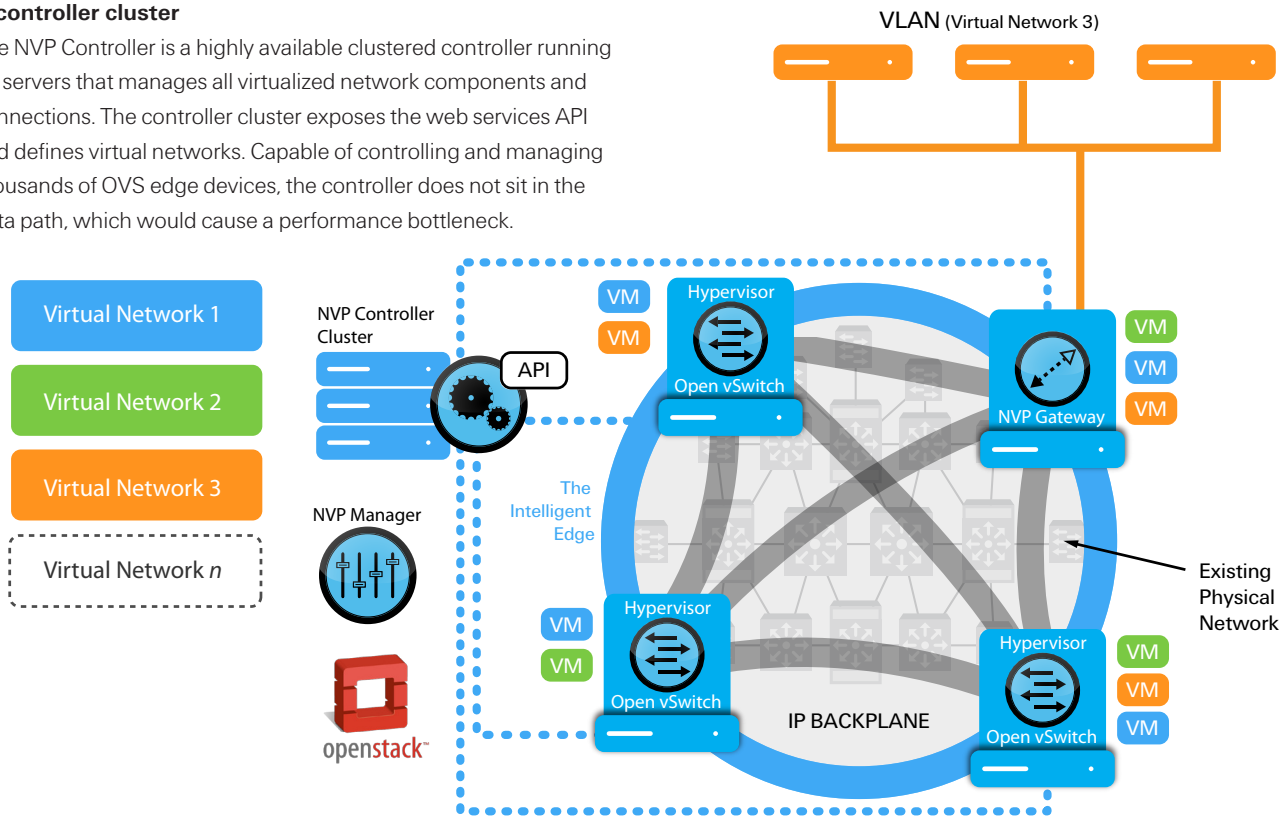
A controller cluster

The NVP Controller is a highly available clustered controller running on servers that manages all virtualized network components and connections. The controller cluster exposes the web services API and defines virtual networks. Capable of controlling and managing thousands of OVS edge devices, the controller does not sit in the data path, which would cause a performance bottleneck.

Full network virtualization is the essential next step for capitalizing on the promise of cloud computing. The right network operational model for the future enables isolated and distinct networks to be created, deleted, expanded, contracted and migrated on demand, leveraging the existing physical network as a generalized pool of network capacity just as physical servers are used as a generalized pool of compute capacity for virtual workloads.

Virtualized networks change the deployment model for physical network hardware, just as compute virtualization has changed the deployment model for servers. The new deployment model allows all physical devices to be racked and cabled once, and then programmatically provisioned and re-purposed on demand. Virtualized networks remove vendor lock-in from the equation, allowing the physical IP fabric to be built using the best price performance solution.

Nicira brings the flexibility of virtualization to the network, combining the standard attributes of traditional physical networking with the operational requirements of the cloud.



About Nicira

Nicira is the network virtualization company. Nicira's Network Virtualization Platform (NVP) enables the dynamic creation of virtual network infrastructure and services that are completely decoupled and independent from the physical network hardware. Innovative companies such as AT&T, eBay, Fidelity Investments, NTT and Rackspace are using Nicira NVP to accelerate service delivery from weeks to minutes and dramatically reduce complexity and cost. For more information, please visit www.nicira.com

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