Cisco Open Network Environment: Network Programmability and Virtual Network Overlays

Summary
Software defined networking (SDN) is an evolutionary approach to network design and functionality based on the ability to programmatically modify the behavior of network devices. Although still in its infancy, there is a great deal of optimism that SDN will make networks more flexible, dynamic, and cost-efficient, while greatly simplifying operational complexity. Cisco has recently begun unveiling its open network environment, a broad vision around extending network capabilities and extracting greater intelligence from network traffic through programmatic interfaces. SDN is a component of this open network environment.

This white paper focuses on a closely related aspect of SDN, the concept of Virtual Network Overlays, based on Cisco Nexus® 1000V, a virtual switch for multihypervisor environments. Through programmatic interfaces to the Cisco Nexus 1000V virtual supervisor module (VSM), Cisco will be enabling automation-centric provisioning of cloud infrastructures. The result is a dynamic and scalable way of building multitenant or hybrid cloud networks and massively scalable data centers that are optimized and operationally efficient.

The Cisco Approach to Programmable Network Infrastructures
The Cisco Open Network Environment is a customizable framework to harness the entire value of the intelligent network, offering openness, programmability, and abstraction at multiple layers in an evolutionary manner. The Cisco Open Network Environment offers a choice of protocols, industry standards, use-case-based deployment models, and integration experiences, while laying the foundation for a dynamic feedback loop of user, session, or application analytics through policy programming.

The Cisco Open Network Environment is delivered through a variety of mechanisms, including APIs, agents, and controllers. Benefits include increased infrastructure agility, simplified operations, and greater application visibility and awareness. These offer flexible deployment options with consistency across both physical and virtual environments. The Cisco approach complements traditional approaches to software defined networking (approaches that primarily focus on decoupling the control and data planes), while also encompassing the entire solution stack from transport to automation and orchestration.

SDN is a loosely defined term in the industry, generally referring to the concept of programming network behavior and network devices through separation of control and data planes to optimize the performance of certain traffic patterns and use cases. More broadly, many in the networking industry are optimistic about the possibility of deep programmability of network infrastructures for quickly modifying network behavior and providing more sophisticated policy controls through rich applications. In addition, organizations are looking to build better analytical and debugging tools to reduce network management and maintenance costs. Ultimately, this should accelerate the migration to highly efficient and scalable cloud environments and more manageable data center environments.
But Cisco’s Open Network Environment vision is differentiated from the common SDN definition in a couple of ways, as highlighted in Figure 1:

- First, network programmability and many of the use cases that benefit from it require APIs or interfaces at multiple layers of the network (not just at the control and forwarding planes). There are deeper internals in our operating systems, and even hardware and ASICs, that can be accessed to extend and enhance the network. Similarly, further up this network stack are higher level services, such as the management and orchestration APIs, for example, our Network Services Manager (NSM) API that supports orchestration and cloud portal applications such as Cisco® Intelligent Automation for Cloud (CIAC). In the Cisco environment, we imagine an application development environment that can access APIs at all levels of this stack.

- Second, many of the use cases for which organizations are looking not only require programming the network to the desired or optimal behavior, but also are seeking to extract the enormous amount of information and intelligence contained in the network infrastructure. Deeper and more insightful network intelligence can be pulled into a new class of analytical applications that can promote more sophisticated network policies and support business logic that impels the network. This ultimately makes the network more valuable and can support more innovative and revenue-generating services.

Implementation of SDN today is typically based on the OpenFlow standard, an open and industrywide initiative that defines communication mechanism between the control and data planes through a software “controller” that can modify network behavior by updating flow tables on network devices. Although this is an interesting capability for researchers, the scope of programmability is relatively narrow compared with broadly defined network functionality.

The concept of separating the control plane and the data plane was part of the architecture of the Cisco Nexus 1000V virtual switch. The forwarding or switching functionality is delivered by the Cisco Nexus 1000V virtual Ethernet module (VEM) running in a network hypervisor, while the management/control capability is implemented in the virtual supervisor module (VSM) running in a separate virtual machine or dedicated network services appliance (the Cisco Nexus 1010). The Cisco Nexus 1000V began shipping in May 2009 and had over 5,000 customers as of March 2012.

The Cisco Nexus 1000V and related portfolio are the foundation for the virtual network overlays, a complementary and alternative approach to SDN for network programmability. Virtual network overlays partition a physical network infrastructure into multiple logically isolated networks that can be individually programmed and managed to deliver optimal network requirements. Virtual network overlays are the approach taken frequently by multitenant environments such as cloud service providers and multitenant data centers.

In Figure 1, the diagram highlights one fundamental attribute of SDN, the separation of the network control plane from the forwarding plane. Through programmatic extensions or APIs represented at all levels of the diagram, we can develop control programs that extend or customize the network policies and behavior as needed.
Virtual Network Overlay Requirements

As mentioned earlier, the Cisco Nexus 1000V virtual switch is ideally suited to deliver virtual network overlays onto physical infrastructures. The Cisco Nexus 1000V forms the network edge (access layer) to virtual machines, providing the infrastructure to segment virtual applications into logically isolated networks that share both physical application servers and the physical network. A primary requirement is to deliver the virtual network infrastructure in such a way that it is consistent with the physical infrastructure. Management consistency should apply across physical and virtual devices and scale to cloud proportions.

The logical network still consists of server nodes (frequently virtual machines rather than physical servers), network nodes, and network services. A primary requirement is that even though the network overlay is running on a shared network infrastructure, there must be a way to logically isolate network traffic and partition needed resources, which can be done with virtual local area network (VLAN) assignments, or in today’s modern scalable multitenant data centers a more scalable version, VXLAN. VXLAN scales to over 16 million virtual networks in a single Layer 2 network domain while helping to extend application mobility across the data center.

Other methods to make sure of logical traffic isolation could include firewalls or virtual private networks (VPNs). However, the dynamic nature of network overlays and the frequent requirement to make them independent of the physical network and able to migrate to other physical infrastructures require that these security services be virtual in nature, rather than relying on any physical security services in the underlying network infrastructure. The virtual services include firewall and other security services, load balancing and application controllers, WAN optimization, and network analyzers.

The network overlay infrastructure is tightly integrated into the server virtualization infrastructure. The market requires a multihypervisor approach to avoid vendor lock-in, especially to address the service provider market and the increasing adoption of open source hypervisors.
Just as virtual machines are independent of the underlying application server and can easily move between servers, the virtual network overlay relies on completely virtualized network infrastructure and services to abstract the underlying physical network, which allows the overlay to be mobile to other physical networks. This is an important requirement for cloud computing, where applications and associated network services are migrated to cloud service providers and remote data centers on the fly as resource demands dictate.

Customers are looking for these virtual network overlays to be programmable to allow business logic and applications to drive and optimized network behavior and performance for individual virtual networks. In the case of the Cisco Nexus 1000V, this would mean programmatic APIs built on top of the virtual supervisor module or the control plane component of the network. REST-compliant APIs are required for application development, although the OpenStack Quantum API is emerging as an open model for orchestration applications.

Within the overlay network, there are requirements for primary networking protocols and functionality to support scalable deployments and increasing the resource pools across which virtual machines can be migrated. Cloud-ready scalability requires mobility across geographically remote data centers and across Layer 3 network boundaries with the support of various network protocols. Cisco FabricPath (based on the TRILL standard) provides data center scale and network redundancy for the overlay network, while Cisco Overlay Transport Virtualization (OTV) provides cross-data center mobility over Layer 3 networks. The Location ID Separator (LISP) protocol also improves application mobility scale by providing routing efficiencies.

Connecting traditional physical networks and campus LANs outside the data center or the service provider requires the ability to connect the scalable VXLAN virtual networks to traditional VLAN segments. This effectively requires a VXLAN-VLAN gateway with the associated network identifier address translations and other services.

Cisco’s Strategy for Virtual Network Overlays

The foundation of Cisco’s virtual network overlay is the Cisco Nexus 1000V virtual switch, which consists of two software components that run in a virtual machine hypervisor. The Cisco Nexus 1000V virtual switch forms the network edge to virtual applications, but because it is a virtual application itself, it provides the ability to meet all the requirements of overlay network and perform independently of the physical network.

The two major components of the Cisco Nexus 1000V are the Virtual Ethernet Module (VEM), which runs inside the application server, and the external Virtual Supervisor Module (VSM), which manages the VEMs (Figure 2) and can run in either a dedicated virtual appliance, the Cisco Nexus 1010 or in a shared application server.
Virtual Ethernet Module
The Cisco Nexus 1000V Series VEM runs in the network hypervisor and acts as the access layer switch to virtual machines while running inside the application server. Just as several line cards compose a single modular switch, many VEMs running across many application servers can act like a large single virtual switch. The VEM takes configuration information from the VSM and performs Layer 2 switching and advanced networking functions:

- PortChannels
- Quality of service (QoS)
- Security: private VLAN, access control lists (ACLs), and port security
- Monitoring: NetFlow, Switch Port Analyzer (SPAN), and Encapsulated Remote SPAN (ERSPAN)

In the event of loss of communication with the VSM, the VEM has Nonstop Forwarding (NSF) capability to continue to switch traffic based on the last known configuration. Thus, the VEM provides advanced switching with data center reliability for the server virtualization environment.

Virtual Supervisor Module
The Cisco Nexus 1000V Series VSM controls multiple VEMs as one logical modular switch. Instead of physical line-card modules, the VSM supports multiple VEMs running in software inside the physical servers. Configuration is performed through the VSM and is automatically propagated to the VEMs. Instead of configuring soft switches inside the hypervisor on a host-by-host basis, administrators can define configurations for immediate use on all VEMs being managed by the VSM from a single interface.
By using the capabilities of Cisco NX-OS, the Cisco Nexus 1000V Series provides:

- **Flexibility and scalability**: Port Profiles, a new Cisco NX-OS feature, provide configuration of ports by category, enabling the solution to scale to a large number of ports. Common software can run all areas of the data center network, including the LAN and SAN.
- **High availability**: Synchronized, redundant VSMs enable rapid, stateful failover and help ensure an always-available virtual machine network.
- **Manageability**: The Cisco Nexus 1000V Series can be accessed through the Cisco command-line interface (CLI), Simple Network Management Protocol (SNMP), XML API, and CiscoWorks LAN Management Solution (LMS).

The VSM is also integrated with VMware vCenter Server so that the virtualization administrator can take advantage of the network configuration in the Cisco Nexus 1000V Series.

**Mobility of Security and Network Policies Within the Virtual Network Overlay**

Network and security policies defined in the Port Profile follow the virtual machine throughout its lifecycle, whether it is being migrated from one server to another (Figure 3), suspended, hibernated, or restarted. In addition to migrating the policy, the VSM also moves the virtual machine’s network state, such as the port counters and flow statistics. Virtual machines participating in traffic monitoring activities, such as Cisco NetFlow or ERSPAN, can continue these activities uninterrupted by VMware vMotion operations. When a specific Port Profile is updated, the Cisco Nexus 1000V Series automatically provides live updates to all of the virtual ports using that same Port Profile. With the ability to migrate network and security policies through VMware vMotion, regulatory compliance is much easier to enforce with the Cisco Nexus 1000V Series, because the security policy is defined in the same way as physical servers and constantly enforced by the switch.

**Figure 3.** Mobility of Network and Security Properties
Virtualized Network Services with Cisco vPath

In addition to virtual machine switching, the Cisco Nexus 1000V Series supports Cisco vPath to provide a single architecture supporting multiple Layer 4 through 7 network services. In the Cisco vPath architecture, Virtual Service Nodes can provide a variety of network services, such as virtual firewall, load balancing, and WAN acceleration. Specifically, the Cisco vPath architecture provides:

- Intelligent traffic steering:
  - Redirect traffic from server requesting network service to the virtual service node (VSN)
  - Extend Port Profile to include network service profile
- Flexible deployment:
  - Each VSN can serve multiple physical servers
  - VSN can be hosted on a separate or dedicated server
- Network service acceleration:
  - Network Service Decision Caching: Cisco Nexus 1000V Series remembers network service policy from prior traffic, reducing traffic steering
  - Performance of virtual network services can be accelerated through enforcement in the hypervisor kernel

Other Enhancements to the Cisco Nexus 1000V for Virtual Network Overlays

The Cisco Nexus 1000V has evolved quickly and will be extended in the future to address the diverse set of requirements for both data centers and service providers, for multitenant environments, cloud readiness, and greater scalability:

- The Cisco Nexus 1000V is taking a strategy of supporting multiple hypervisors to address as many markets as possible, including all major commercial hypervisors and open source hypervisors.
- The Cisco Nexus 1000V and its companion virtual services appliance, the Cisco Nexus 1010, have introduced features to scale the number of virtual ports that can be supported across a single virtual switch or a single Layer 2 domain. That number currently scales to over 10,000 virtual ports on over 10,000 virtual segments.
- Support for OpenStack and REST APIs for automated, policy-based provisioning applications.
- Inclusion of the VXLAN-VLAN gateway for integration of virtual networks to physical networks.

Figure 4 shows these features deployed in a mixed multitenant environment, including separation of the VEM data plane and VSM control plane, support for orchestration APIs on the VSM, support for multiple hypervisors, and integration of the virtual and physical networks through the VXLAN-VLAN gateway.
Network Orchestration, Management, and Automation

Virtual network overlays are frequently found in highly scalable cloud or service provider environments, as well as in highly scalable multitenant data centers. For this reason, the definition, setup, and provisioning of virtual network overlays on the physical infrastructure, in the right location, with the right set of services can be greatly facilitated with an automated orchestration engine. For Cisco virtual network overlays, the Cisco Network Services Manager (NSM) meets the requirements for automating the provisioning of virtual networks and virtual services, as well as configuring physical network devices to create the overlay networks.

The Network Services Manager network abstraction layer helps you provision and deploy numerous individual network components as sophisticated network “containers.” You can create these containers:

- Across single and multipod cloud computing deployments
- Much more easily and quickly than with template- and script-based systems

In addition, Cisco Network Services Manager:

- Dramatically reduces network operational costs and potential misconfiguration
- Optimizes capacity use and accelerates service delivery

Cisco Network Services Manager offers a flexible, policy-directed approach to managing and controlling cloud computing network services. Through a configuration user interface, Network Services Manager helps administrators dynamically define and control an array of behaviors in their cloud computing environment, including:

- Creating different levels of service capability or “service tiers” for tenant use
- Defining the capabilities and resources available in each tier
- Structuring a system of “containment” customized to tenant application and deployment model needs

NSM interfaces to other workflow automation and cloud portals through an API. Cisco’s own orchestration system and its Cisco Intelligent Automation for Cloud are built on top of this NSM API to enable programmatic provisioning of the virtual network overlay network containers. NSM thus serves as an ideal example of network programmability at the management and orchestration layer and Cisco’s programmable network infrastructure.
Conclusion

Virtual overlay networks are modular, flexible network abstractions that meet business demands for application agility, more efficient use of resources, and greater scalability. They are an important complement to the concept of network programmability overall and can allow for segmented network slices for a variety of network needs over a shared physical infrastructure.

Virtual network overlays can accelerate cloud readiness for application networks and can provide all the virtual security and application performance services typical of dedicated data center environments. Cisco provides the complete network virtualization stack to achieve highly scalable and mobile virtual network overlays based on the Cisco Nexus 1000V virtual switch, a series of virtual service nodes that include the ASA 1000V cloud firewall and virtual Wide Area Application Services (vWAAS), as well as automated network provisioning and orchestration capabilities in NSM.

While virtual network overlays share some of the same architectural approaches and functional requirements of SDN, the Cisco virtual network overlay and the Cisco Nexus 1000V portfolio address the requirements differently than the traditional SDN approach. As a result, Cisco can provide much greater production-ready capabilities and services than pure SDN products allow. For instance, the OpenStack API, VXLAN, VXLAN-VLAN gateways, the range of virtual services on Cisco virtual networks, and multihypervisor support are not typically discussed as part of an SDN solution.