Cisco Open Network Environment: Bring the Network Closer to Applications

White Paper

April 2014

Shashi Kiran, Senior Director, Marketing, Data Center and Cloud
Gary Kinghorn, Senior Marketing Manager, Data Center and Cloud

What You Will Learn

The Cisco® Open Network Environment (ONE) is the industry's broadest approach to make networks more open, programmable, and application-led. It is the key to network automation and more efficient operations.

Table 1: Basic Definitions
What Is Software-Defined Networking?
"…In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications…" **Source:** http://www.opennetworking.org.
What Is OpenFlow?
OpenFlow is an open protocol that specifies interactions between decoupled control and data planes.
What Is OpenStack?
OpenStack is open source software for building public and private clouds. It includes computing (Nova), networking (Quantum), and storage (Swift) services. **Source:** http://www.openstack.org.
What Are Virtual Network Overlays?
An overlay network is created on existing network infrastructure (physical or virtual) using a network protocol. Examples of overlay network protocols are generic routing encapsulation (GRE), Virtual Private LAN Service (VPLS), and Virtual Extensible LAN (VXLAN). Integrated Network Overlays bring tighter synergy between physical and virtual networks.

IT Trends and the Advent of Open Networking

Advances in IT, computing, and communications are forcing a rapid evolution of networking technology and making new demands on IT departments:

- Cloud: Cloud computing is causing the network to become more scalable, flexible, and application-aware. Applications must be predictable and independent of network considerations if they are to be flexibly located in various cloud locations.

- Video: Video and other integrated, high-bandwidth communications services are causing the network to become more flexible for all forms of network traffic, with greater dependency on quality of service (QoS).

- Mobility: Trends in client mobility, wireless computing, and bring-your-own-device (BYOD) initiatives are causing the network to adapt to deliver numerous new services with new performance and security considerations.

- Data deluge: The dramatic increase in real-time data collection and storage, particularly in video and voice applications, is challenging scalability and QoS requirements, even as the Internet of Everything brings more connected elements together.

Customers are looking to their IT infrastructure to solve these key challenges. The network in particular has a strategic position and should deliver:

- Simplicity: Organizations can no longer afford the complex, task-intensive approach to network management. The scalability and on-demand flexibility required of today's modern network applications require greater automation and programmatic orchestration, not manual operations.

- Agility: The network must be constantly optimized for rapidly changing business requirements and applications. To automate this repurposing of the network infrastructure and make the business more agile, programmatic orchestration of the network is needed.

- Flexibility: The network, which used to be viewed primarily as complex and rigid, is rapidly evolving into a strategic business enabler. Businesses are demanding the automation of critical processes and a network with the flexibility to rapidly deliver crucial enabling services and generate revenue.

To deliver these requirements, networks must be more open, programmable, and application-aware. Networks must evolve to meet these emerging trends without compromising the resilience, service richness, or security they have today.

Table 2: Market Requirements Vary by Use Case
Research and Academia • Researching with OpenFlow and SDN controllers in a standards-based approach; guided by federal grant money in this research area • Primary use case: Network slicing - logical partitioning of networks for individual tenants or organizations, with specific programmatic control for each slice **Massively Scalable Data Center Applications** • Large, single-application data centers seeking more customized debugging, optimization, and analytic applications to better tune networks • Primary use case: Optimal flow management, analysis, and debugging with deep programmatic access **Cloud Environments** • Seeking automated provisioning and programmable overlay networks • More interested in open source technologies such as OpenStack or orchestration application programming interfaces (APIs) and tools; multi-tenancy also a requirement **Service Providers** • Want to build policy-based control and analytics applications • Want to develop custom programs to monetize new services for customers and offer better service-level agreements (SLA) **Enterprises** • Seeking to accelerate virtualization and cloud-readiness; would like to automate more IT processes • Primary use cases: Focus on orchestration and automation and online implementation of QoS and security policies

Open Networking, Software-Defined Networking (SDN), and network programmability (see Table 1 for definitions) have emerged to address these trends by providing much greater automation and orchestration of the network fabric, and by allowing dynamic, application-led configuration of networks, services, and applications.

Market Requirements and Open Networking Deployment Models

Network programmability requirements vary by market, industry, and size of the organization. Universities and research institutions do not have the same requirements or use cases as cloud service providers or massively scalable single-tenant data centers. Table 2 shows the varying customer requirements and use cases that are guiding solutions in each area.

The important point is that network programmability is not a single technology or use case. There are multiple deployment models for network devices and fabrics. The use cases dictate multiple approaches.

There is a tendency in the industry to bring these use cases under the SDN umbrella, causing further confusion. Even the term "SDN" varies in meaning from organization to organization. For this reason, Cisco has aligned our definition of SDN with that of the Open Network Foundation (ONF) as covered in the "Basic Definitions" in Table 1.

Network Programming Models

It is also worthwhile to look at different approaches to network programmability. Traditional network devices have integrated control and data-forwarding capabilities (Figure 1, model 1). These devices can be exposed to applications through representational state transfer (REST) application programming interfaces (APIs), without necessarily de-coupling the control- and data-plane elements. This scenario has the advantages of taking better advantage of the benefits of hardware intelligence, deeper programmatic access, and better customization. Technically this approach of not de-coupling the control and data planes would not be considered as SDN, but can be instrumental in enabling SDN deployment models.

A common attribute of SDN systems (Figure 1, model 2A) is the concept of the separation of the control and data planes, although how they are separated and where the applications run vary in the different programming models discussed here. While this separation has its benefits, you have to forgo the features of the native operating system control plane and must re-create features and capabilities with the controller or in applications that sit atop the controller.

Figure 1.　　Deployment Models for Open Networking
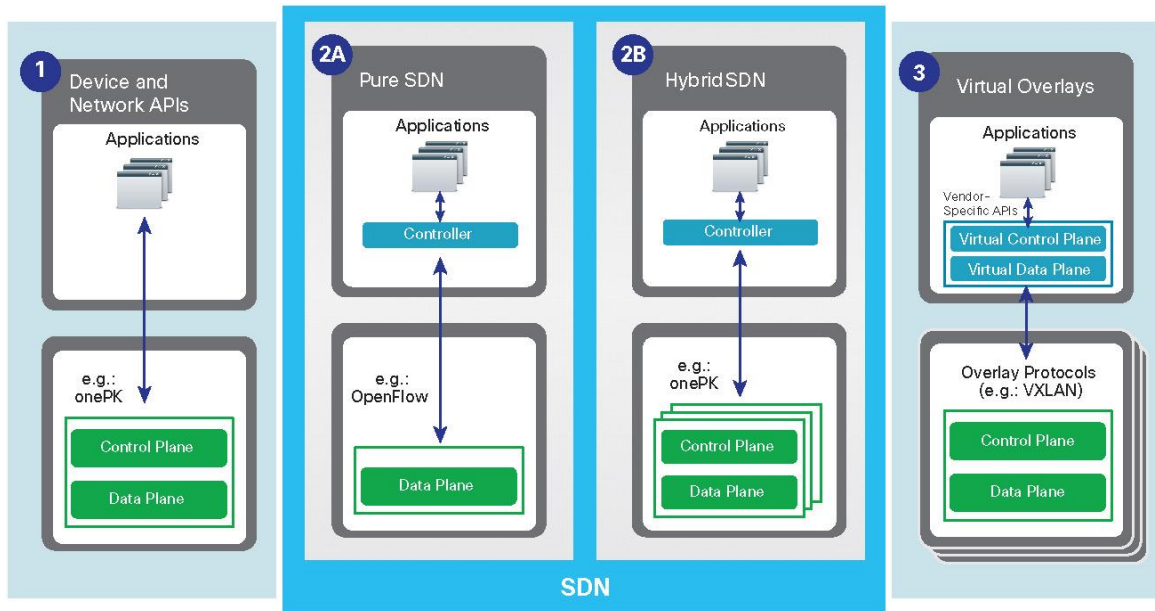
These architectural models are still being debated and discussed. Concerns such as security, availability, and scale need to be factored in. You also need a mechanism to adopt newer models without disrupting your environment. There are merits to centralizing a control plane, such as topological views and centralized management, but the subjects of scale, resiliency, security, and standardization still need to be addressed. Further, depending on the objective, there may be different methods of evolving the network, without necessarily de-coupling the control and data planes. A practical variation, also known as "Hybrid SDNs" (Figure 1, model 2B), is having a distributed control plane in addition to some form of centralized control. Hybrid SDN can provide a more evolutionary approach and retain existing network capabilities, while still delivering on the benefits of a centralized controller model.

Virtual network overlays are also becoming quite prominent in the industry focused on virtualized environments, with REST APIs now being available on top of a virtual control and data plane pair. OpenStack is rapidly becoming a viable alternative for building orchestration applications on top of virtual network overlays as well.

Cisco's primary differentiation in delivering open, programmable networks to customers is that it supports **all** of these deployment models, including device- and network-specific APIs (for example, onePK), and support for a controller-based SDN model (for example, the Cisco eXtensible Network Controller with support for OpenFlow). Likewise, Cisco also supports virtual overlay models (Figure 1, model 3) such has those enabled by the Cisco Nexus® 1000V Switch.

Customers can choose the best model based on their use case and alignment with their IT requirements. There could be multiple deployment models within the same organization. Cisco also believes in creating an environment that can take advantage of the intelligence within networked environments, including better linkages to analytics, policy engines, and service orchestration mechanisms that can provide more value to customers.

Introducing the Cisco Open Network Environment

The Cisco Open Network Environment (ONE) is a holistic approach to bring the network closer to applications. It is a customizable framework for harnessing the entire value of the intelligent network, offering openness, programmability, and abstraction at multiple layers, providing better linkages to analytics, policy engines, and orchestration tools.

It is delivered through a variety of mechanisms, advocating open APIs, open standards, and open-source technologies. Benefits include increased infrastructure agility, simplified operations, and greater application visibility and awareness.

Cisco ONE focuses on exploiting the synergies between hardware, software, and application-specific integrated circuit (ASIC), while continuing to bring consistency across physical, virtual, and cloud environments. It complements traditional approaches to SDN (that focus primarily on decoupling the control and data planes), while also securely supporting other deployment models. In short, Cisco ONE offers the broadest approach to open, programmable networks, including SDN controllers, open APIs, and virtual network infrastructures across a variety of deployment models (Figure 2).

Figure 2.   Cisco Open Network Environment
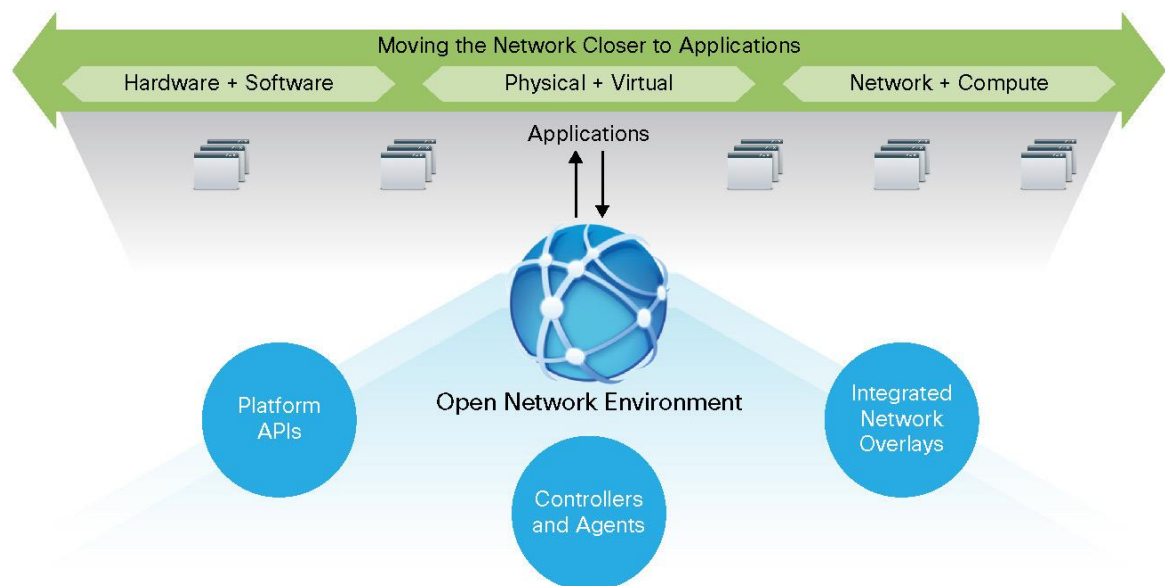
Cisco ONE: Innovations Across the Portfolio

Today, Cisco is delivering several approaches to realize this vision of open networking:

- Device and network APIs through a comprehensive SDK
- Cisco Controller
- Programmable, virtual network overlays

As requirements, standards, and technologies evolve, other APIs and products will likely emerge within this three-pronged vision.

Cisco onePK API and Software Developer Kit

The Cisco ONE Platform Kit (onePK) API is a software development kit for network programming specific to Cisco network devices and network operating systems that allows access and control of the full range of Cisco capabilities.

The main elements of the programming architecture, shown in Figure 3, include:

- Programs written in C, Java, Python, or possibly other languages in the future
- The programmatic interfaces or presentation layer; that is, the set of APIs that expose the network functions and libraries in various network devices and across all network operating systems (Cisco IOS® Software, Cisco IOS XR Software, and Cisco NX-OS Software) in a consistent manner
- The communications channel between the presentation layer and the infrastructure layer, which accesses the network devices; this element provides something like a client-server two-tier application implementation on a traditional server
- The infrastructure layer, or the abstraction layer, which provides the framework code for platform-specific implementations; this code helps ensure that the application programmer does not have to worry about the specifics of the different network operating systems being progammed
- The network OS-specific implementations of the Cisco onePK libraries on the various platforms (for example, Cisco IOS Software, Cisco NX-OS, and Cisco IOS-XR Software)

Figure 3.   Cisco onePK Software Architecture
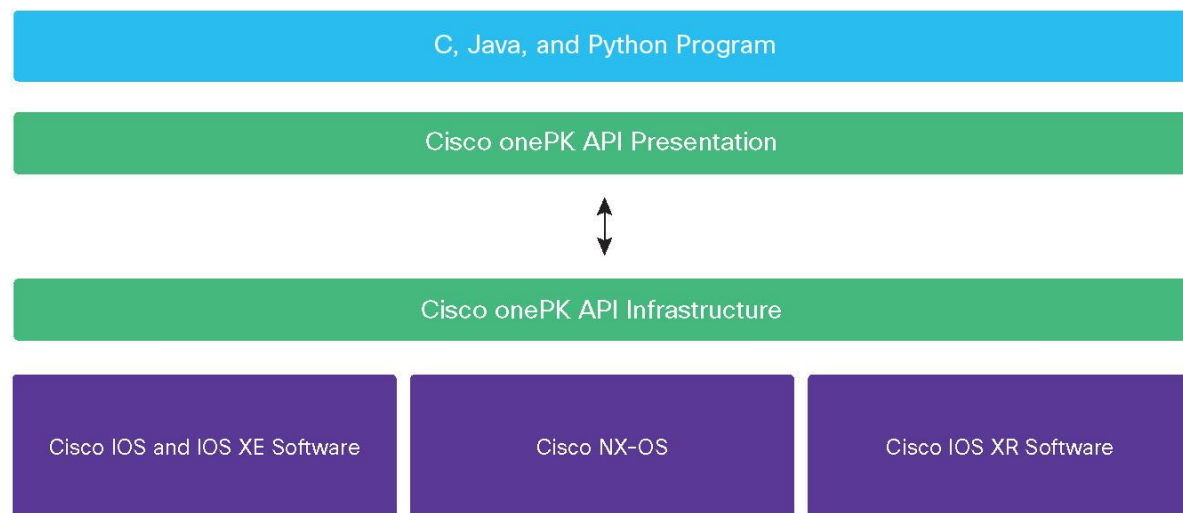
Developers can use the same APIs across the whole network, even when the devices in the network are running a different network OS. As the network and technology evolve, this API consistency will be maintained so that new devices and platforms, with different operating systems, can be included without the need to modify the SDN programs.

onePK allows you to get the benefits of application linkages across **all** the different programmability models described earlier. This benefit can be brought about as a software update onto existing switches and routers, providing you with an evolutionary path and strong investment protection to explore any model you choose to adopt. Further protocols such as OpenFlow can run as agents onto onePK, thereby allowing for hybrid environments and ease of transitioning into an SDN model.

Unlike the SDN controller model, Cisco onePK provides greater flexibility in the way that the network applications are deployed in the network. You can deploy them centrally on another device or locally on the device itself.

An example of how onePK provides greater insight and control of Cisco platforms than other SDN approaches was the announcement of the Cisco Unified Access Data Plane (UADP). Cisco UADP is a programmable ASIC that supports onePK APIs and is initially being deployed in the Cisco Catalyst® 3850 Unified Access Switch, as well as the Cisco 5750 Wireless LAN Controller. The UADP ASIC provides access to low-level device metrics for analysis, as well as enabling programmability from onePK applications across the range of supported devices. It also accelerates the time to roll out custom features to the UADP-enabled platforms.

Cisco eXtensible Network Controller (XNC)

The Cisco XNC conforms to the original SDN controller model described earlier. It supports the industry-standard OpenFlow protocol, which enables a more heterogenous, platform-independent approach to network programmability that includes both Cisco and third-party networking devices.

The Cisco XNC is based on a highly available, scalable, and extensible architecture that provides the following core features:

- The industry's first multiprotocol interface support, including support for both Cisco onePK and OpenFlow
- Functions to support network visibility and programmability, such as network topology discovery, network device management, and access to detailed network statistics
- A service abstraction layer (SAL) that enables modular device support through either OpenFlow or Cisco onePK, for investment protection after the controller is deployed in a production network
- Consistent management access to the controller through a GUI REST application or through northbound programmatic APIs for inclusion in other external programs
- Security features such as role-based access control (RBAC); integration with the enterprise authentication, authorization, and accounting (AAA) infrastructure; and secure control protocols

The Cisco XNC also provides advanced features such as:

- Monitor Manager, an SDN approach to the network tapping use case
- Topology-Independent Forwarding (TIF), which enables the administrator to customize the path of a data flow through the network
- Cisco network applications that include the logical partitioning of portions of the network using an approach called network slicing (the primary use case in universities, as discussed later in this document)
- Clustering based High-availability to provide scalability and fault tolerance

The Cisco XNC offers the developer community and independent software vendors (ISVs) multiple choices of northbound (or external) APIs to provide true network programmability from external applications.

The Cisco XNC centralized control plane coexists with the traditional control plane of networking devices to support the hybrid integrated mode described by the ONF. In this mode, the network devices continue to run well-known network control protocols, such as Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS), and the applications on the Cisco XNC complement those with, for example, OpenFlow control features.

The Cisco XNC has a built-in web based GUI and northbound APIs. You interact with the Cisco XNC through the GUI or using RESTful API. The GUI is built as an application, so it uses the same northbound API as any other controller-based application. This approach means that everything that is entered through the GUI is available to any external application (for example, another orchestration or management entity). Figure 4 shows an example of the GUI.

OpenFlow agents exist on network devices and respond to the OpenFlow requests from the controller. Agents are supported across many of the Cisco network families, including Cisco Nexus and Catalyst switches, allowing network programmability to be consistently supported across platforms and across data center and campus WAN networks.

Figure 4.   Cisco XNC GUI

The Cisco Controller's extensibility and modularity allows addition of support for emerging SDN protocols in addition to OpenFlow, such as the Interface to Routing Systems (I2RS) protocol for programmatic control of routers being developed by the IETF. I2RS focuses on functions specific to routers rather than flow-oriented forwarding like OpenFlow. This integrated support for multiple protocols and device types, as well as multiple vendor platforms, provide a centralized point of control for a greater portion of the network, as well as more flexibility for SDN application developers.

Cisco Nexus 1000V Virtual Network Overlay and OpenStack Quantum API

Cisco pioneered the concept of a virtual switch with the Cisco Nexus 1000V Virtual Switch in 2009. Virtual networks built on the Cisco Nexus 1000V now form virtual overlay networks, including comprehensive Layer 4 through Layer 7 services, as described earlier. To program the virtual network overlays, Cisco is also making available APIs on the Cisco Nexus 1000V - for instance, the OpenStack Quantum API - which enables implementation of portable cloud orchestration applications on top of the Cisco Virtual Network Infrastructure (VNI).

The concept of separating the control plane and the data plane was part of the original design of the Cisco Nexus 1000V Virtual Switch. OpenFlow defines a separate controller from the underlying network device; similarly, the Cisco Nexus 1000V has two separate components: the virtual supervisor module (VSM), which acts as the control plane, and the virtual Ethernet module (VEM), which acts as the virtual-switch forwarding plane. To make the virtual overlays programmable, the VSM is programmable through northbound interfaces, including OpenStack and REST APIs.

One advantage of the Cisco Nexus 1000V in building these virtual overlays is that it is consistent with the physical infrastructure from the management and policy perspectives. Management consistency applies across physical and virtual devices and scales to cloud proportions.

Because the network overlay is running on a shared network infrastructure, another requirement is a way to logically isolate network traffic and partition needed resources. This isolation can be achieved with VLAN assignments, or in today's modern scalable multitenant data centers, a more scalable version: Cisco Nexus Virtual Extensible LANs (VXLANs). VXLAN scales to more than 16 million virtual networks in a single Layer 2 network domain, so even the largest cloud environments will not run out of overlay partitions anytime soon.

Cisco continues to bring elements of Layer 4-7 services, service chaining aspects onto virtualized environments. It also supports a multi-hypervisor and multi-cloud environment. At the same time, the integration between the overlay virtual infrastructure and the physical continues to grow tighter, giving you a choice of integrated stacks that you can program in a consistent manner.

Cisco ONE Use Cases

A good way to understand the power of open networking, SDN, and network programmability is to explore some general use-case scenarios in which analytical, monitoring, and optimization software programs are inserted into the network. These use cases are diverse and they are targeted at different markets and customer types, but the common outcome is much greater real-time analysis and optimization of network resources, with greater control and flexibility for individual tenants in multitenant environments.

In considering these use cases, note that network programmability can take many forms and can apply to the network as a whole or to only specific devices. Although many use-case scenarios include some aspect of monitoring, analytics, and orchestration, not all do. There are likely thousands of business-justified use cases for SDN and Cisco ONE, and as the technology matures, many more will likely emerge.

We are taking a cross-architectural approach with the open network environment, and the use cases are reflective of this approach.

Service Provider Monetization and Tuning of Customized Services for Tenants

Service providers are repeatedly challenged to deploy new services and tools in a timely way. The flexibility to add these new services and tune them for specific clients can result in substantial additional revenue: for example, in the form of optimal capacity, dedicated resources, or additional infrastructure.

Currently, administrative tools require significant amounts of time to set up and change network configurations and apply business policies to meet new service-level agreements (SLAs). The use case in Figure 5 shows how Cisco ONE can improve this process.

In this example, Cisco ONE is used to optimize the network between an enterprise customer and a cloud service or content provider. The solution provides real-time multilayer monitoring of transport, IP and Multiprotocol Label Switching (MPLS), and services between the user and the service provider. This information allows the provider's SDN application to adapt to any network condition, look at congestion and packet-loss rates, and create new paths to meet the business SLAs for telepresence, financial trading applications, or other time- and bandwidth-sensitive scenarios.

Figure 5.   Cisco ONE Can Be Used to Build Applications That Optimize the Service Provider Network in Real Time
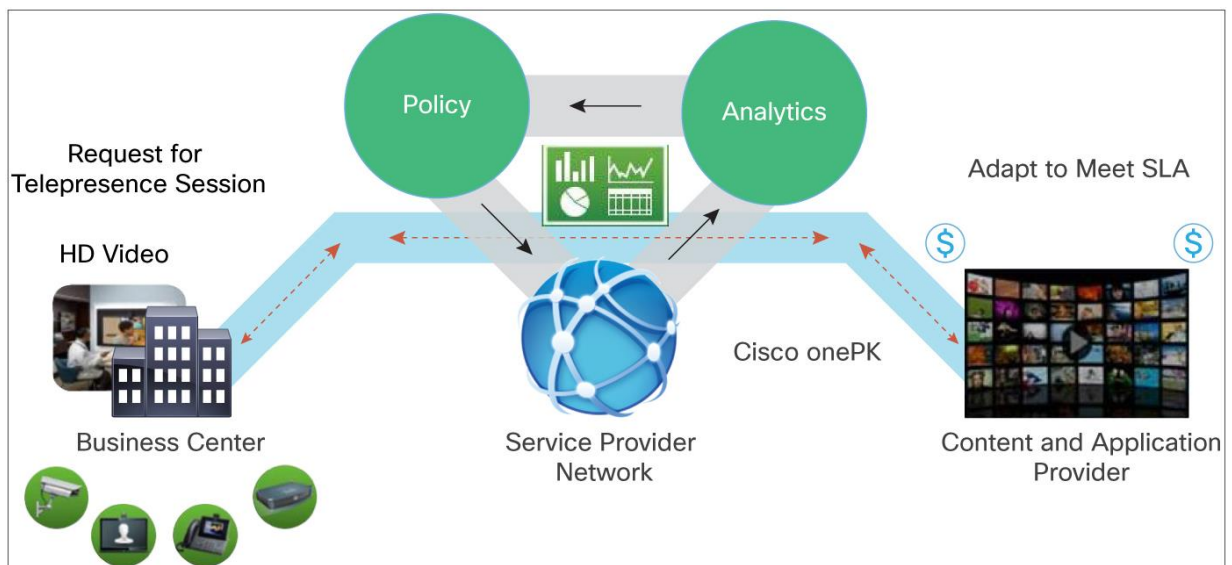
The solution notifies those applications that there is a network change that has not been seen at the application layer; the change is measured in real time, and the network adapts immediately to meet the SLA. This responsiveness can result in measurably better and more reliable service levels in real time, based on specific parameters and conditions built into the custom SDN application, and it enables the service provider to monetize the additional resource and service levels.

Cisco ONE thus can be used to build applications that optimize the service provider network in real time, allowing providers to better monetize value-added services for clients. The Cisco XNC and agents provide a bidirectional feedback loop with SDN policy and analytics engines.
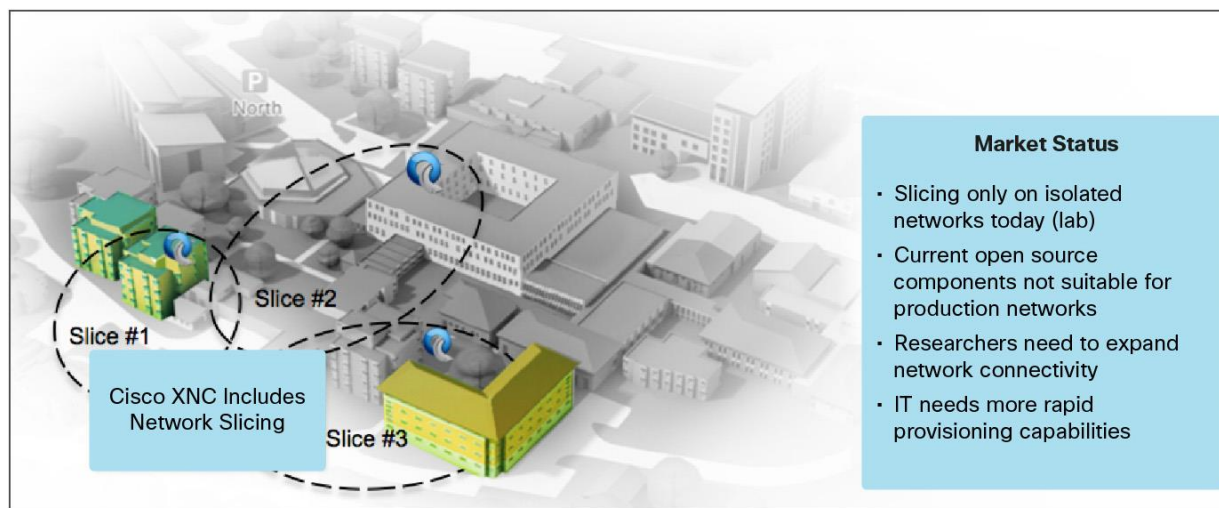
Campus Network Slicing

University campus networks offer an increasingly wide array of networking services to one of the broadest user bases of any organization. Some universities have medical or high-security facilities and must maintain regulatory compliance accordingly. Student networking services vary depending on whether they are on or off campus, and in almost all cases students and faculty bring their own devices. Administrative offices must also be able to manage the day-to-day activities of the university. Often event management must include the rapid provisioning of point-of-sale terminal support and back-end payment reconciliation. Faculty must have both data and video access on the university campus, across campuses, and to other universities.

As a result, the capability to partition networks, called slicing, based on SDN has increased in popularity. Although slicing is being performed today on isolated networks, the need to perform it on production networks is now becoming a priority. Much of the early research and collaboration between universities on OpenFlow and SDN has been based on National Science Foundation (NSF) funded projects such as GENI, an open, collaborative research environment to explore networking at scale. Network slicing is a primary use case for the controller model, particularly in universities, allowing tenants to control custom forwarding paths and network behavior for their own diverse needs.

The automation and flexibility of network programmability is well suited to increasing business agility through automation with relatively low operating expenses (OpEx) and low risk. The Cisco XNC is a natural fit for the types of requests that universities need to service (Figure 6).

Figure 6.   Campus Network Slicing Is a Primary Use Case for the Cisco XNC

Cisco adds value to the campus slicing use case in several ways:

- The Cisco XNC is designed for production networks. Connectivity to policy creation and security tools used to manage the conventional network is transparent. Additionally, Cisco has created TIF, which enables policy management to be enforced independently across each of the slices created by IT.
- The Cisco XNC offers Java- and REST-based northbound interfaces, helping ensure that a wide range of applications can integrate into the Cisco infrastructure. This integration is important for helping ensure that SDN operates with the major provisioning processes of the network on campus.

- The capability of the Cisco XNC to access the vast amount of intelligence present in Cisco network devices allows a more comprehensive set of analytical data to be presented to applications to improve the results of network tuning.

Universities now have the opportunity to add increased automation and dynamic reconfiguration to evolve their SDN use cases to include production network management and control for multitenant environments.

Data Center Use Case: Cabling Verification and Error Detection

An illustrative data center use case is a cabling validation and debugging program using onePK. One large data center customer estimated that 10 percent of new switches are cabled incorrectly when initially deployed. This incorrect cabling can lead to problems in auto-configuration, as well as inefficient network behavior (in the best case). Automating the tedious verification process of new switch hardware installation could save time and reduce headaches, and is a prime use case for network programmability.

Figure 7.   A onePK Application for Analyzing Network Topology and Comparing to Intended Wiring Diagrams for Error Detection and Failure Prevention
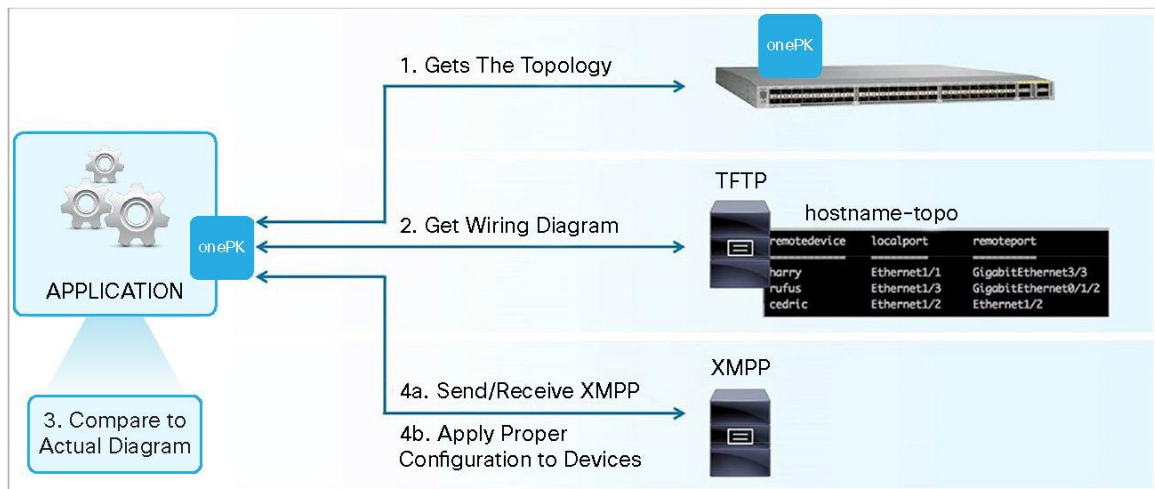
The onePK verification application can run on a centralized server or controller and monitor all connected devices throughout the data center running the onePK agent. The onePK agent runs on the Cisco Nexus 3000, representative of the many top-of-rack switches in our topology, and not only helps a network manager identify a cabling mismatch, but also prevents the port from getting auto-configuration details that would cause network problems because of the cabling error. In addition, the onePK program can generate a new wiring diagram as needed and apply proper configurations automatically to the affected devices.

The application oversees the process of each switch connecting to its nearest neighbors and compares the results to the wiring diagram file (perhaps a text file we retrieve from a TFTP server). If there is a discrepancy, an Extensible Messaging and Presence Protocol (XMPP) message can be sent to a network administrator to remediate the problem. With power-on auto-provisioning and onePK agents installed on many Cisco Nexus top-of-rack switches, this application can work with new devices out of the box as part of the power-on process.

Benefits of the Cisco Open Network Environment

Cisco ONE offers a comprehensive vision across all IT infrastructure, flexible deployment options (SDN and non-SDN progamming models), and investment protection through incremental adoption. It is the broadest structured approach to open networking in the industry today. In addition, professional services from Cisco and our partners, plus global support, help ensure long-term success:

- Extending the capabilities of existing, proven validated infrastructure significantly reduces risk and time to capability.
- Cisco ONE is designed to be deployed incrementally, preserving investments and avoiding turnover.
- Cisco ONE builds on Cisco innovation together with industry development of SDN technologies and standards. This approach maintains high flexibility and choice for customers.

The Cisco onePK model is consistent across a wide range of Cisco routers and switches. Organizations and service providers can write their applications once and deploy them anywhere, with investment protection for future platforms. Cisco Certified developer partners can be confident of a large market opportunity that targets a large installed base of network equipment.

The Cisco XNC offers the flexibility of conformance to an open standard and the capability to control third-party network devices, while supporting multiple API and SDN specifications. The industry-leading Cisco VNI forms the foundation for programmable network overlays that can simplify cloud deployments and integrate automation and orchestration tools.

We are in a unique position to help you evaluate these new technologies and determine how best to integrate them into your broader networking strategies. As the industry leader in networking, we have the expertise and experience to help your organization extract tangible value from Cisco ONE to support your strategic goals.

Why Cisco?

Customer Value and Choice; Flexible Deployment Options

- Industry leader: Cisco is the worldwide leader in networking with a deep commitment to open networking including open source, open standards, and open interfaces. We have been contributing to and leading several initiatives for open standards and open source, including at the Open Network Foundation, OpenStack consortium, OpenDaylight project, IETF, IEEE, and ETSI among others.
- Unparalleled innovation: Only Cisco brings together innovation across hardware, software, services, and ASICs to deliver tightly integrated solutions that offer lower total cost of ownership (TCO). We have traditionally offered strong investment protection with evolutionary approaches to revolutionary benefits.
- Cross-architectural solutions: Cisco offers holistic cross-architectural solutions that are secure and transcend branch-office, campus, data center, cloud, and service provider environments.
- Choice of deployment models: Cisco offers a use-case led deployment model to embrace emerging technologies such as network programmability and SDN in an evolutionary manner, offering investment protection and lower TCO.
- Technical and Advanced Services: Cisco has a mature partner ecosystem including training and developer partners, the Cisco Development Network (CDN), as well as a Professional and Technical Support Services organization to help foster customer success through all aspects of the customer's open networking and SDN experience. Working together, the Cisco ecosystem helps customers architect software-led programmability to enable simplification in the overall solution.

For More Information

For more information, please visit http://www.cisco.com/go/one.

Printed in USA

C11-728045-02   04/14