White Paper

Software-Defined Networking: Why We Like It and How We Are Building On It

What You Will Learn

According to the Open Networking Foundation (ONF), software-defined networking (SDN) is a network architecture that decouples the control and data planes, moving the control plane (network intelligence and policy making) to an application called a controller. Cisco advocates a broader view of SDN that incorporates multiple models for network programmability, in addition to the controller/agent model defined by the ONF for OpenFlow.

This white paper presents the Cisco perspective on SDN:

- Programming network behavior is a valuable capability for public sector organizations, especially as they prepare for big data, surging video traffic, Bring-Your-Own-Device (BYOD) environments, and cloud computing.
- Academia and the scientific research community have successfully applied network programmability to facilitate data sharing across institutions, and to deploy new types of distributed computing applications. In several instances, the OpenFlow protocol has replaced more traditional ways of supporting these deployments.
- Several Cisco® products have OpenFlow-capable images available, and there is a well-defined roadmap to expand OpenFlow support.
- To broaden the possibilities for network programming, and to address a wider range of use cases, a more expansive view of network programmability is needed. Cisco has developed the Cisco Open Network Environment (ONE) architecture as a multifaceted approach to network programmability delivered across three pillars:
  - A rich set of application programming interfaces (APIs) exposed directly on switches and routers to augment existing OpenFlow specifications
  - A production-ready OpenFlow controller and OpenFlow agents
  - A suite of products to deliver virtual overlays, virtual services, and resource orchestration capabilities in the data center

OpenFlow: Where It Is Strong and Where It Is Limited

Cisco is positive about OpenFlow. Cisco has developed a full-featured, production-ready OpenFlow Controller called the Cisco Extensible Network Controller. Several Cisco switches have OpenFlow agents available, and our roadmap calls for fully supported agents on the majority of Cisco routing and switching products.

OpenFlow is designed to support policy-based flow management within a network. OpenFlow is particularly well suited to use cases satisfied by pushing predefined policies to implement network segmentation. In addition to simple flow-matching and forwarding capabilities, later releases of the OpenFlow specification have introduced ways to implement simple quality of service (QoS) and flow metering.

In spite of these capabilities, there are several areas of network programmability that are outside the current scope of OpenFlow:

- **Facilities for element device management and monitoring:** Operating system image management, hardware management, zero-touch deployment, event triggering, element location information, and more
- **Capability to directly influence forwarding behavior of a network element:** Routing Information Base/ Forwarding Information Base (RIB/FIB) manipulation, route status, routing protocol advertisements, add/delete routes, and broad-spanning tree support
- **Data packet payload manipulation:** On-box encryption and VPN, customized encryption algorithms, deep packet inspection, application awareness requiring payload inspection, ability to inject packets into a network stream
- **Service deployment:** OpenFlow has no ability to instantiate a service directly on a network element. Service examples include firewall, Wide Area Application Services (WAAS), intrusion protection system (IPS) software, SDN Enabled broadband network gate (BNG), video monitoring, etc.
- **Distributed control plane and APIs:** OpenFlow's reliance on a centralized control plane limits application run time options

Flexible Deployment Models

OpenFlow requires a controller deployed on a server. The controller uses the OpenFlow protocol to communicate over the network with agents on switches and routers. Applications use APIs on the OpenFlow controller to implement network policy. Cisco believes it is advantageous to support multiple application deployment models in addition to the OpenFlow controller/application approach.

Centralized control planes offer the advantages of easy operations and management. A centralized model also introduces scalability concerns and limits options for application deployment. Direct access to decentralized device APIs opens a broad range of application possibilities that are not available in an OpenFlow centralized model. A hybrid approach, combining direct API access on a device to augment API access via a controller, may well be the optimal balance between centralized and decentralized control planes.

The ability to instantiate a service anywhere in the network based on dynamic demands has significant value. Flexible application deployment models are critical to delivering that capability. The Cisco approach supports multiple application deployment options:

- Applications running within software containers on routers and switches
- Applications executing directly on x86 hardware deployed on routers and switches
- Applications running on standalone or virtualized servers

Flexible deployment models provide several advantages:

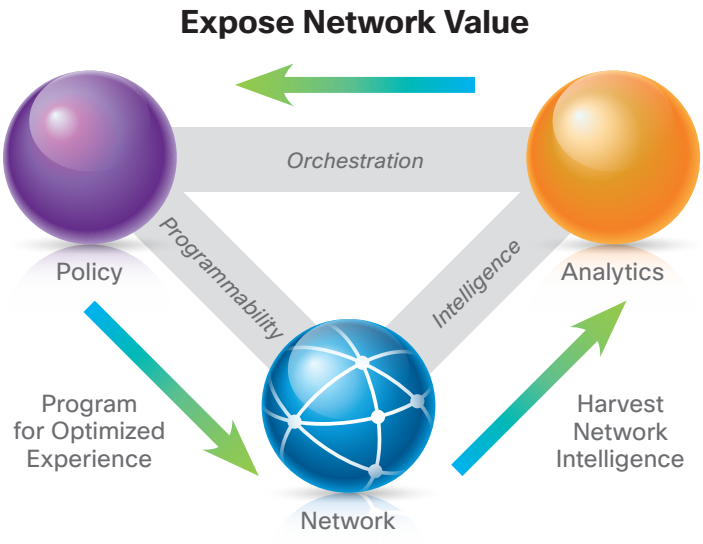
- Applications can be deployed on any network node in any location that needs services without requiring reachability between the node and a central controller.
- Distributed application deployment facilitates scalability and minimizes control-plane latency. The scalability of centralized controllers is as yet untested in large-scale production environments. Without appropriate controller scalability, large-scale events could overwhelm centralized controllers by the workload generated when processing large volumes of messages while simultaneously sending updated policies to hundreds of devices. Clustered controllers are entering the market at the time of this writing, which could mitigate these effects.
- Network devices can more swiftly adjust service policies in response to fluctuating flow demands when distributed device control planes are closely coupled with applications. OpenFlow scales best in a proactive control model where flows are statically defined and policies pushed to network elements. Controller scalability becomes a concern when there is a need to dynamically modify policy in reaction to dynamic network conditions, such as device hardware errors or other events impacting link or service availability.

A Broader Vision for Network Programmability

The Cisco vision for SDN is to provide true network programmability, enabling developers to write applications that extract real-time intelligence from the network, and apply analytics and intelligence to determine the appropriate policy. Policy is then pushed to the network elements via OpenFlow, onePK, or other means *(Figure 1)*.

This closed-loop model provides a tight coupling of the network-to-business applications, giving the applications the ability to coordinate network resources. This enables a scenario in which the network devices themselves provide analytics to detect traffic changes that indicate a surge in a specific application's traffic. The orchestration application can then automatically modify policy to reconfigure the network to simultaneously optimize both user experience and application performance.

Figure 1 *Cisco Vision for Network Programmability: Expose Network Value by Harvesting Network Intelligence to Dynamically Direct Policy*



What Does This Mean for the Public Sector?

The public sector has led the way in the adoption of SDN technologies, including OpenFlow. The scientific research community has growing expertise in using OpenFlow and other network programmability methods to solve the problems presented by moving, securing, and analyzing large data sets.

SDN Use Cases

The public sector also has unique challenges involving data encryption and secure network transport. These use cases are particularly suited to SDN solutions. Here are some examples:

- Improving network performance and right-sizing expensive service appliances by dynamically sensing trusted flows at the network edge to direct them around stateful services such as firewalls, IPS sensors, or network address translation (NAT) devices. This is a valuable capability when multiple research institutions share data.
- Automated provisioning of network bandwidth to accommodate scheduled data transfers. SDN is used to interface data management applications with the network to set up and tear down required transport paths to support large data set migrations. Distributed, high-throughput compute applications like HTCondor benefit by having a programmatic way to provision network paths for job distribution and workload management. These are frequently occurring use cases among scientific researchers.
- Isolation of network slices to segment the network by proactively pushing policy via a centralized controller to cordon off research traffic.
- Many large institutions, university systems, and state governments are adopting converged data center architectures to optimize application availability while reducing costs. SDN enables organizations to simplify the transition from multiple data centers to a single, multitenant architecture through the use of programmatic control of virtualized Layer 2 topologies and service orchestration.

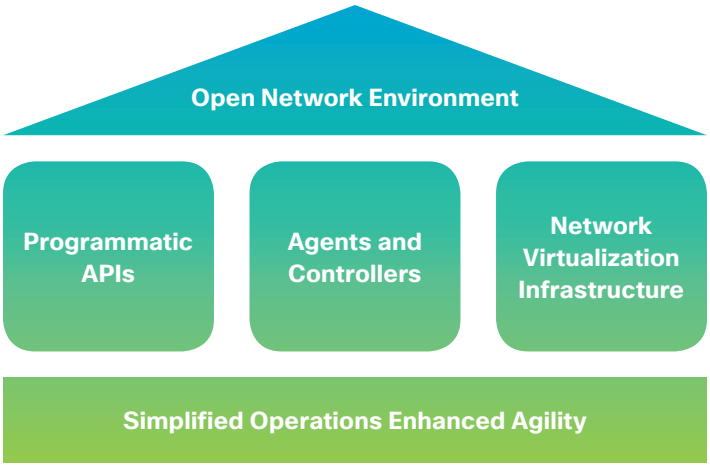
Use Cases Based on OpenFlow with Cisco onePK APIs

- Direct access to device APIs to implement zero-touch initial configuration as well as to automate configuration changes. The Cisco onePK has the ability to use protocols such as Puppet to instruct a newly deployed device to pull its configuration from the appropriate server. Programmatic delivery of network device configurations is desirable to minimize human error and to ease large-scale changes. Current methods are cumbersome and difficult to maintain across products and releases. Cisco onePK introduces a common set of APIs across operating systems and product sets to allow a single application to manage a heterogeneous installed base.
- Minimize the risk of new cyber-security threats that emerge from the need to support BYOD. A student-owned tablet introduces a known piece of malware onto the network. A network device could use a Cisco onePK application with packet payload inspection abilities to detect the malware and automatically mitigate the threat by quarantining the device or updating routing advertisements to black hole the offending traffic.
- Selectively protect sensitive information by dynamically encrypting flows using custom algorithms running on a network device. This capability has value for many federal IT organizations, and it is a critical capability in multitenant cloud architectures. As state government IT data centers centralize, they have a common need to encrypt particular application traffic from specific tenants. Cisco onePK has the ability to implement very granular policies, limiting encryption to only those flows requiring it, in addition to dynamically instantiating encryption services on relevant network nodes.
- In higher education residence halls, an application deployed on a router checks a database to determine a student's subscribed Internet service tier. The application then modifies the packet QoS markings accordingly to reflect the appropriate traffic class for that user. This can be accomplished on a single router deployed at a remote campus or a dorm hall edge without the need for a campus-wide OpenFlow deployment.
- An application deployed on a router connects to the reservation database for Cisco TelePresence® System. Seeing that a multipoint Cisco TelePresence session is scheduled for specific time, the application instructs the network to reserve the needed bandwidth for the appropriate time period. Cisco TelePresence does not have unique ports specific to the Cisco TelePresence application. Cisco onePK would use packet payload inspection to identify relevant flows. When the session concludes, the reserved bandwidth is released. Cisco onePK extends the traffic steering use cases described earlier by allowing flow identification based on payload analysis to augment tuple matching.
- Improving network economics by extending routing protocols to consider business parameters (such as dollar cost) in addition to technical parameters (such as speed) when selecting a network path.

Cisco Direction: Building on OpenFlow with Cisco onePK

To expand the possibilities of network programmability, Cisco has developed the Cisco ONE architecture *(Figure 2)*. Cisco ONE builds on OpenFlow, adding new capabilities to address challenges of WANs and data centers, as well as campus networks.

Figure 2 Cisco ONE Architecture



Cisco believes that the problem domains of the WAN, campus, and data center differ enough that no single technology will be an optimum fit for all realms. In addition, different customer segments have very different problems to address.

Cisco ONE reflects that belief and lays out an approach to network programmability incorporating a variety of technologies. Public sector organizations can use any or all of its components:

- The rich programmatic interface of Cisco onePK. The Cisco onePK APIs give Cisco and third-party controllers direct programmatic access to Cisco IOS® Software. They support hundreds of programmatic actions, including device discovery, device management, and policy and routing control. In addition, Cisco onePK Data Path APIs allow programmatic access to extract, modify, and reinsert packets in an active flow. The roadmap for Cisco onePK includes support for Cisco IOS, IOS-XE, IOS-XR, and NX-OS operating systems across nearly all Cisco Catalyst® and Cisco Nexus® Series Switches.
- OpenFlow support on the Cisco production-ready controllers: Unlike other OpenFlow controllers, the Cisco controller provides role-based access control, troubleshooting support, topology-independent forwarding, the ability to inject synthesized traffic, and trace routing. The controller has been in field trials since the beginning of 2012.
- Virtual overlays: Cisco virtual overlay technologies provide multitenant support and service orchestration using the Virtual Extensible LAN (VXLAN), and vPath features of Cisco Nexus 1000V Series Switches. Virtual overlays use familiar SDN models of centralized control, but transport is accomplished by encapsulating frames over a fixed, Layer 3 topology.

Conclusion and Recommendations

SDN is a compelling development for the public sector. It helps to simplify operations by automating and centralizing network management tasks. It makes the network more responsive to dynamic business and institutional needs by coupling applications with network control. Finally, SDN gives IT teams more agility, because they can quickly customize network behavior for emergent business needs. The increasing velocity of application development will continue to drive IT organizations to deploy technologies that allow them to scale and respond to rapidly changing demands.

We recommend that public sector organizations:

- Develop a strategy to adopt network programmability with the goal of reducing operational expense while providing a high-quality user experience when many traffic types compete for bandwidth.
- Take a phased approach to validate value and retire risk prior to large-scale deployment. Cisco is introducing SDN support across most of its switching and routing portfolio. This means you can conduct small-scale, proof-of-concept pilots without investing in new hardware. In many cases, you can deploy validated applications in production on existing hardware, with only a code upgrade.
- If you use OpenFlow, consider the Cisco ONE Controller. This controller has many unique capabilities that are necessary for production deployment, including troubleshooting features, role-based access control, and topology-independent forwarding.

For More Information

To learn more about the Cisco Open Network Environment (ONE), visit: www.cisco.com/go/one.

To learn more about Cisco onePK, visit: www.cisco.com/en/US/prod/iosswrel/onepk.html.

To learn more about Cisco Nexus 1000V Series Switches, visit: www.cisco.com/go/nexus1000v.