OPEN NETWORKING
FOUNDATION

SDN in the Campus Environment

ONF Solution Brief
September 30, 2013

Table of Contents

2 Executive Summary
3 SDN Overview
4 Introduction
4 Attributes and Challenges of Today's Campus Networks
6 SDN in the Campus
7 Traffic Isolation Use Case
8 The Role of SDN and OpenFlow
10 Key Benefits
10 Conclusion
11 Contributors

Executive Summary

Today's campus networks are facing major challenges. Mobile clients, BYOD, video, and the ever-growing number of connected devices and applications are rapidly changing the network landscape, no matter whether the campus is corporate or educational. These dramatic changes tax the ability of current solutions to deliver agility, performance, and seamless user experience. One of the primary reasons for these challenges is that network technology evolution is simply not keeping pace with evolving demands. Software Defined Networking (SDN) can alleviate these challenges, offering flexibility and the ability to develop new capabilities quickly and cost-effectively.

This solution brief explores the key challenges faced by campus network administrators, examines some of the limitations of current solutions, and then illustrates how SDN overcomes the limitations of today's networks. Use cases will also be presented, followed by a discussion of the benefits of OpenFlow™-based SDN in the campus network.

SDN Overview

Software Defined Networking is a new architecture that has been designed to enable more agile and cost-effective networks. The Open Networking Foundation (ONF) is taking the lead in SDN standardization, and has defined an SDN architecture model as depicted in Figure 1.

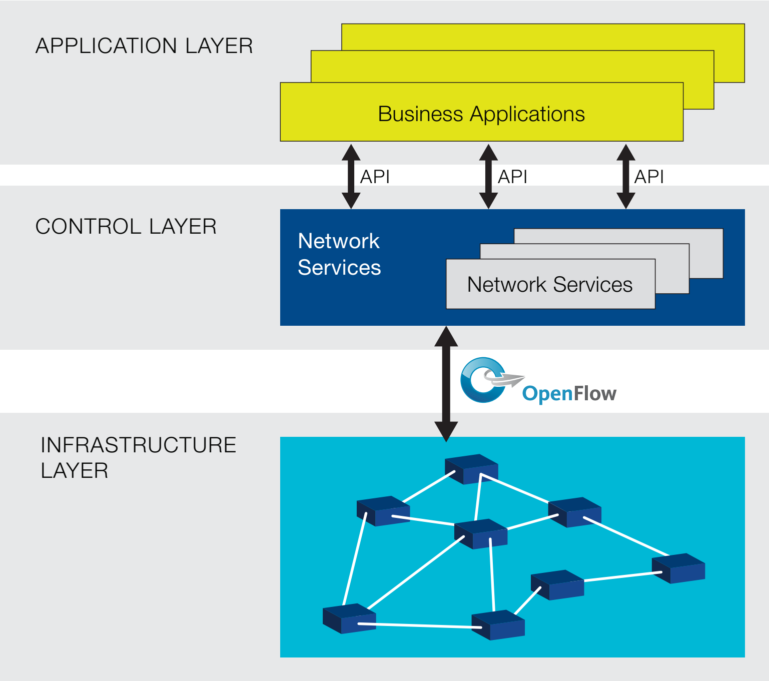

FIGURE 1
ONF/SDN architecture

The ONF/SDN architecture consists of three distinct layers that are accessible through open APIs:

- **The Application Layer** consists of the end-user business applications that consume the SDN communications services. The boundary between the Application Layer and the Control Layer is traversed by the northbound API.
- **The Control Layer** provides the consolidated control functionality that supervises the network forwarding behavior through an open interface.
- **The Infrastructure Layer** consists of the network elements (NE) and devices that provide packet switching and forwarding.

According to this model, an SDN architecture is characterized by three key attributes:

- **Logically centralized intelligence.** In an SDN architecture, network control is distributed from forwarding using a standardized southbound interface: OpenFlow. By centralizing network intelligence, decision-making is facilitated based on a global (or domain) view of the network, as opposed to today's networks, which are built on an autonomous system view where nodes are unaware of the overall state of the network.

- **Programmability.** SDN networks are inherently controlled by software functionality, which may be provided by vendors or the network operators themselves. Such programmability enables the management paradigm to be replaced by automation, influenced by rapid adoption of the cloud. By providing open APIs for applications to interact with the network, SDN networks can achieve unprecedented innovation and differentiation.
- **Abstraction.** In an SDN network, the business applications that consume SDN services are abstracted from the underlying network technologies. Network devices are also abstracted from the SDN Control Layer to ensure portability and future-proofing of investments in network services, the network software resident in the Control Layer.

Introduction

Over the past few years, IT organizations at enterprises and educational institutions have come under increasing pressure from end users to provide access to applications and data from anywhere and at any time. As mobile devices such as smartphones and tablets proliferate in campus environments, users increasingly access and store sensitive data on these devices—which are often owned by the user, not the organization. Not only must campus networks be secure, scalable, and manageable, they must also maintain isolation among an ever-increasing diversity of users, applications, services, devices, and access technologies. Consequently, networks that serve campuses must evolve to address these changing requirements.

Attributes and Challenges of Today's Campus Networks

Today's tech-dependent campuses require IT groups to support diverse sets of:

- **Users**: employees, customers, visitors, students, faculty, etc.
- **Devices**: smartphones, tables, laptops, desktops, cameras, IP phones, etc. — which could be owned by the users themselves (BYOD) rather than by the organization
- **Applications**: business-critical and financial, collaboration, physical security, sensors, Internet, and casual gaming applications
- **Connectivity options**: wired, wireless, branch access via WAN, remote VPN, and 3G/LTE

Mobility, BYOD, and compliance with ever-changing regulations present several challenges to existing campus networks. A campus-wide technology infrastructure must be able to:

- Deliver existing services in a rapidly-evolving environment
- Accelerate the deployment of new applications, upgrades, and network configuration changes
- Provide differentiated policies and services based on user context (user, device, application, location, and time)
- Converge and simplify management across wired and wireless LANs
- Apply and enforce application-specific performance
- Deliver new services to meet real-time demands
- Comply with ever-evolving regulatory requirements (PCI, HIPAA, SOX, etc.)

Typical campus network architectures are structured into three layers—core, aggregation/distribution, and access—that connect diverse endpoints, as shown in Figure 2. Typically, Layer 2 is used for the access layer, and Layer 3 is used for the core layer. The traditional three-tier architecture imposes operational constraints such as loop avoidance, limitations on multi-path connections, etc., which impact performance. Wireless is yet another layer and typically deployed as an overlay. This not only increases management costs and complexity (because wired and wireless networks are separate), it also precludes a seamless user experience (because the two networks provide different capabilities and feature sets).

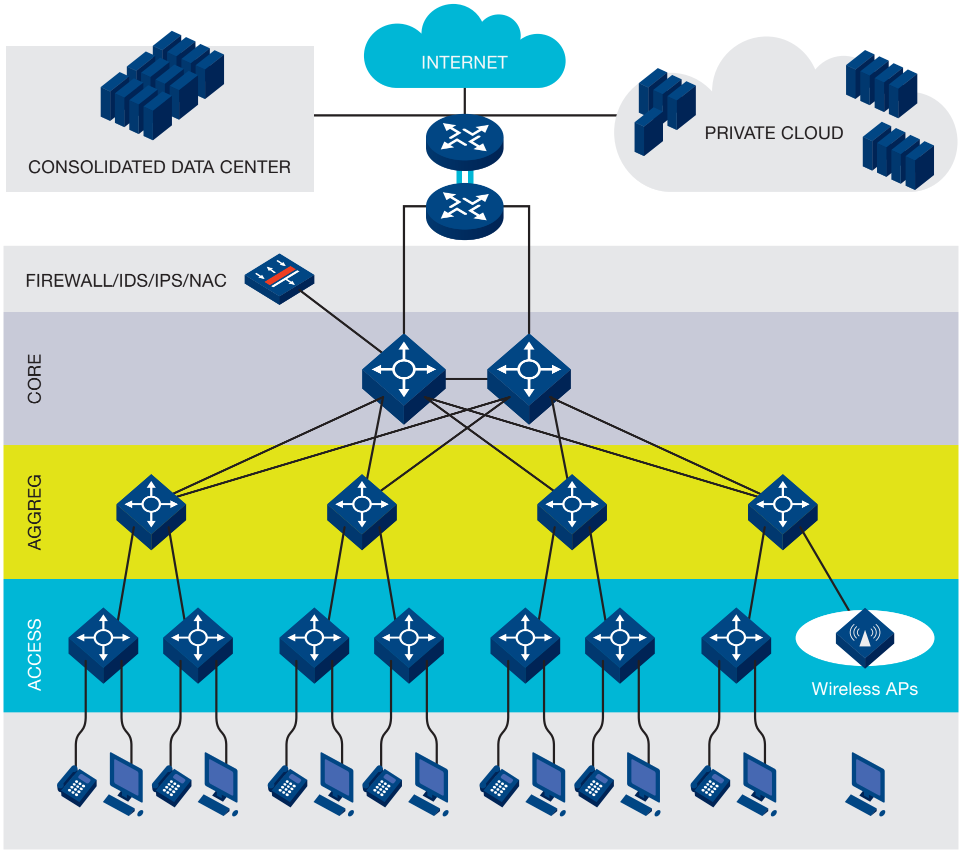

FIGURE 2
Architecture of a typical campus network

Because campus networks are by nature heterogeneous, they are often difficult to manage, leading to excess costs along with scalability and reliability problems. Network configuration changes are subject to lengthy provisioning times and configuration errors because network devices must be configured individually, typically through the CLI or proprietary element management systems.

Organizations are presently addressing these challenges in a fragmented fashion with wireless LAN controllers and Wi-Fi access points, VLANs for Layer 2 isolation, and Virtual Routing and Forwarding (VRF) for Layer 3 traffic isolation. These strategies might be efficient for specific circumstances, but often at the cost of scalability and flexibility.

An OpenFlow™-enabled Software Defined Network offers a much simpler approach to traffic isolation and unified management. By separating the control, management, and service layers from the data-plane layer, OpenFlow eliminates the limitations and operational overhead of VLANs and VRFs.

SDN in the Campus

An OpenFlow-based SDN network architecture simplifies the campus network while offering significantly greater flexibility.

- **Rapid service deployment and tear down** without impacting other logical networks, thanks to network virtualization.
- **Improved service availability** because alternate paths can be pre-computed, which also improves responsiveness compared with traditional network convergence upon topology changes.
- **Traffic isolation of logical networks** at both Layer 2 and Layer 3.
- **Optimal resource utilization**, because management, services, and applications are virtualized to maximize utilization while minimizing space and power consumption.

OpenFlow-based SDN introduces the multi-layer flow paradigm, which provides a higher level of control. By virtualizing the campus network in slices, granular policies can be applied to individual and/or groups of flows at the centralized controller, decoupling policy from hardware. For instance, access policies can be enforced for different departments, different types of access (wireless vs. wired), or even remote versus local users. Such policies are much simpler to enforce, especially for the increasingly mobile workforce.

Traffic Isolation Use Case

A sample use case will more clearly illustrate how OpenFlow-based SDN simplifies the management of a campus network. In this example, the campus is that of an educational institution.

A typical university network serves diverse tenants, including faculty, students, medical facilities, libraries, a police department, restaurants, and bookstores. These individual tenants may need private addressing schemes that may overlap. Some tenants are required to comply with regulations such as PCI and SOX. This requires the university network to isolate traffic among multiple tenants and operate logical networks over a single physical network.

SDN enables policies to be enforced per application, which in turn allows access only to specific network resources (or a specific share of network resources). Figure 3 depicts a typical university network where a single physical network is shared by many diverse entities in a single location.

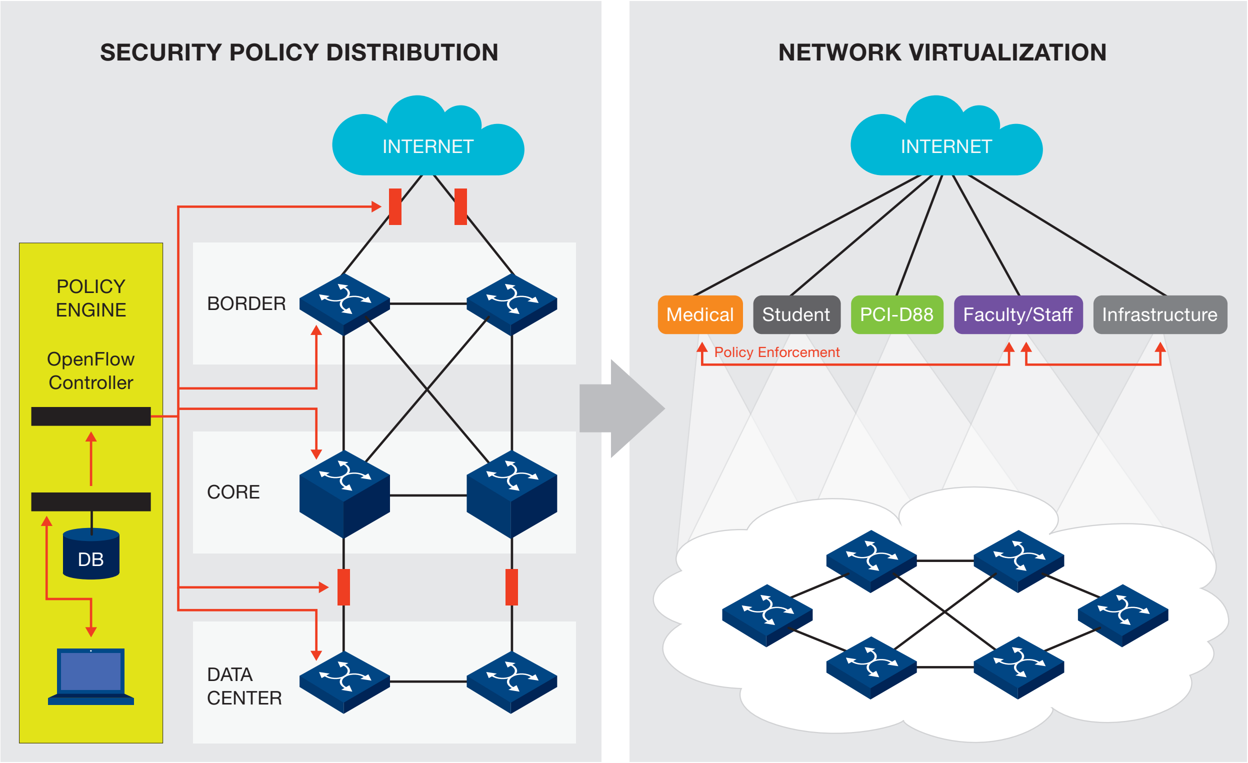

FIGURE 3. LEFT: A typical university network today. RIGHT: An SDN-based architecture.

Campus networks require logically partitioned networks, each with its own policy. Currently, solutions such as MPLS or VRF-Lite are used to create logical network slices over a single physical network. Deploying and managing these technologies is static, time-consuming, and very cumbersome. SDN/OpenFlow-enabled switches enable these logical networks to be created on demand in a matter of minutes instead of weeks. These switches can also enforce flexible policies to control and limit interaction among the logical networks.

The Role of SDN and OpenFlow

OpenFlow-based SDN can overcome the limitations with existing campus networks. Typically, a logical network is created by associating a physical port of a switch or VLAN to a specific logical network ID, with its own routing protocol instance and forwarding table. Whenever a packet needs to be forwarded, it will be associated with the logical network based on the port it arrived on or the VLAN ID. This approach has several limitations. A port or a VLAN can belong to only one logical network and therefore cannot support multiple flows that terminate on different logical networks. In addition, these methods are proprietary and cannot interoperate with each other.

With SDN, the controller can determine the logical network for every flow, then tunnel the traffic to the end of the logical network. It becomes easier to define logical networks as needed, avoiding the need to create a routing protocol instance in every router for each logical network. This approach is scalable and much more flexible than VLAN/VRF approaches. In addition, SDN-based logical networks can easily be created, updated, and terminated based on dynamic requirements. By programming the traffic forwarding rules across the data forwarding devices, it becomes easy to reorder service execution and implement service chaining.

Another advantage is that with SDN, one can easily deploy policies across logical networks to enable traffic across these networks.

Figure 4 summarizes additional use cases in the campus environment, and the benefits realized by SDNs.

FIGURE 4. Use cases for SDN in a campus network.

Use Cases	Network Challenge	Traditional Solution	SDN Solution
Network Virtualization (Slicing / Traffic Isolation)	Regulations and corporate policies require certain traffic to be segregated from other traffic in the network.	Use VRF/VRF-Lite/MPLS/Virtual LANs (VLANs) to create multiple virtual networks.	Isolate the traffic by segregating into different logical flows corresponding to logical networks.
Improving Security and Policy enforcement	Static security policies do not take into account the real-time context of the user or the network. Increasing number of internal and external threats, difficult to secure the edge.	ACLs, IDS/IPS, 802.1X, MAC Authentication. Many different tools to achieve security policies.	Improve security with more granular match rules based on user's context to dynamically apply security policies. Also enable policies to be decoupled from the physical perimeter, which is especially important for mobile users.
Seamless Mobility & BYOD	Difficult to provide seamless experience across wired and wireless networks, and provide context aware policies.	Limited integration of controllers into switches, QoS, IEEE 802.1X access control, VLANs.	Use OF-enabled switches and APs to recognize users and devices and provide same access policies and performance independence of the access network. More granular control over traffic.
Application Aware Networks	Applications and services can require on-demand capabilities from the network at any given time.	Static QoS policies, building network to handle predicted traffic patterns.	Allow applications to interact directly with network through SDN controller and set up QoS and policies, etc.
Management Simplification	Many devices with individual interfaces and static configurations are difficult to maintain.	CLI, scripting, SNMP & management tools to provide limited visibility and configurability of fragmented network devices.	Controller with management tool to set policies and provide a more dynamic view of the entire network, no touch device-level configuration. Automation significantly accelerates provisioning times, improving time to new features, services, and applications.
Video Streaming / Collaboration	Video streaming to large number of receivers is identical whether the receiver is over wireless or wired. Also, it is independent of device (smart phone/tablet/laptop).	Multicast is deployed – but it is not available. When multicast is not always available, a server would receive multicast stream and transmit unicast streams to receivers.	SDN controller constructs the network topology, sources and listeners of a multicast stream. SDN can build an optimal multicast tree without complex protocols and optimize streams based on types of end devices.

Key Benefits

OpenFlow-based SDN networks offer a number of tangible benefits in the campus environment, including:

- Traffic isolation through granular policy management applied to flows, facilitating compliance, security, and multi-tenancy.
- Bandwidth optimization through network virtualization and centralized control over the virtual and physical infrastructure. This improves the utilization of individual network devices as well as the overall network.
- Streamlined operations and management by simplifying the network configuration and supplanting manual and craft-sensitive management with automation.
- Improved reliability by leveraging centralized path selection and failover control to improve service and application availability.
- Improved agility through SDN programmability and abstraction.
- Openness from an architecture facilitated by OpenFlow, which promotes multi-vendor interoperability and affords customers control over the features roadmap. Adoption of open source software is also encouraged in the open SDN environment.

Conclusion

Campus networks face many diverse and challenging requirements, including technology integration, provisioning, and security policy enforcement. SDN/OpenFlow is particularly well suited to bring order to the chaos of campus networking, which typically includes layered switch fabrics, virtualized compute nodes, wired and wireless connectivity, and complex regulatory environments.

Centrally programmable OpenFlow controllers can substantially optimize campus network operations by reducing management overhead, boosting scalability, and reducing interoperability issues. Where massive growth in VMs overwhelms security policy enforcement in conventional physical switches, SDN can help streamline policy enforcement across wired, wireless, and virtual networks, and enable highly scalable private cloud computing environments.

Campus networks are inherently multi-tenant and must be virtualized to ensure distinct policy enforcement for the various users. OpenFlow-based SDN provides network virtualization and granular policy enforcement in a manner much simpler than conventional methods based on MPLS and VRF-Lite protocols.

As SDN evolves, the campus will benefit from a highly programmable, intelligent, and abstracted network architecture that will also be able to address future challenges.

Contributors

Suresh Katukam, Project Leader

Marc LeClerc, Editor

Marc Cohn

Pravin Kantak

Shaji Nathan

Komer Poodari

Tina Tsou

Open Networking Foundation / www.opennetworking.org

The Open Networking Foundation is a nonprofit organization founded in 2011, whose goal is to accelerate the adoption of open SDN.
ONF emphasizes the interests of end-users throughout the Data Center, Enterprise, and Carrier network environments.