Wang Shihong

New network architectures are facilitating the convergence of data centers and campus networks. >>

SDN Enters Campus Life

| By *Wang Shihong, General Manager, Switch Domain, Enterprise Network Product Line, Huawei Technologies Co., Ltd.*

Software-Defined Networking (SDN) technologies first emerged and have been used most actively in the field of data centers. New concepts and solutions, such as overlay, policy orchestration, and open networks, continue to dominate research efforts, while major vendors compete to provide the market with the widest possible selection of equipment and solutions.

Expect Fast Change

Campus network conflicts are brewing between the forces of supply and demand. The movement towards all-wireless environments and the popularity of mobile offices have created numerous security challenges. Simultaneously, the global economy requires companies to always be ready to deploy additional network nodes and attend to the difficulty of maintaining network policies as those node numbers increase. In these matters and many others, SDN is bringing dramatic changes to campus networks.

As the construction of enterprise wireless networks gains momentum and remote access technologies, such as Virtual Private Network (VPN), grow in maturity, the borders of enterprise campus networks have disappeared, and the choice of office locations is more flexible than ever. For enterprises, enhanced mobility creates both higher productivity and more complicated network management and security schemes that require updates to the traditional management of access rights and Quality-of-Service (QoS) standards.

Control Plane Abstraction

Service orchestration is an important characteristic of SDN architectures that provides the ability to decouple service policies from IP addresses. SDN controllers abstract the details of the physical network and each individual appliance. The result allows network administrators to adopt IT-based management approaches that require less configuration time and greater opportunities for innovation.

In the area of policy orchestration, administrators can easily place users and resources into separate security based on 'Who, What, Where, When, Why, and How' conditions. This approach ensures a consistent experience for mobile office users from any location and from any device. For network managers, this dynamic technology reduces the workload for network configuration and maintenance, and deploys up to 80 percent more efficiently than traditional, IP address-based Virtual Local Area Networks (VLANs) and Access Control Lists (ACLs).

From Months to Days

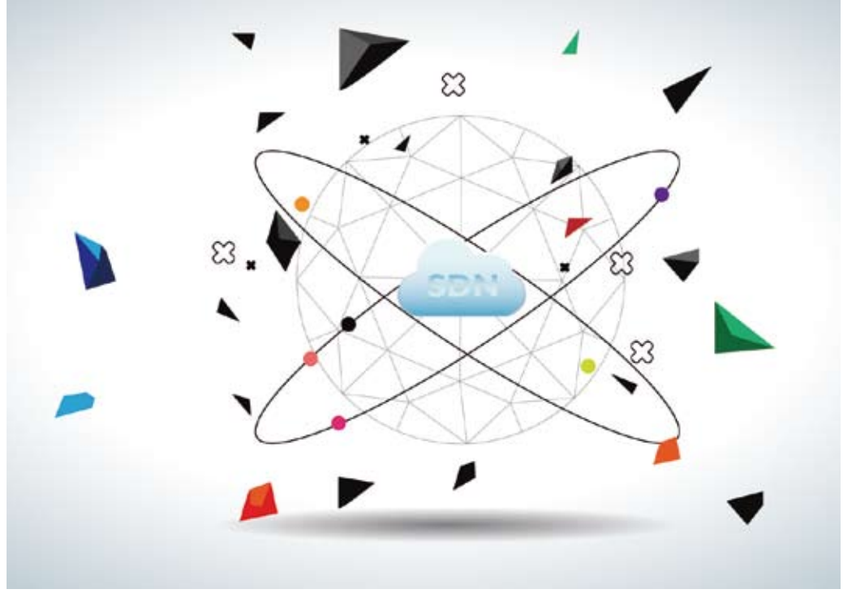
The disadvantages of traditional networks include slow service response, complex configurations, and high Operations & Maintenance (O&M) costs. The burden on organizations has been the need to build and maintain large teams of highly trained experts to address every configuration, provisioning, and operations detail, including emergency service calls. During the development and construction of traditional networks, qualified engineers are expected to complete the following without a flaw:

- **Network Designs** deliver requirements and specification documents, configuration templates, and service requirement parameters. Configuration templates generally consist of command line instructions that typically involve over 500 lines of software code for each core node.
- **Network Deployments** require command line configuration of individual network devices and large amounts of repetitive work that is prone to error.

Configuration orchestration, like policy orchestration, is based on the separation of service policies from networks. The traditional complexity of converting service requirements to network configurations is now handled by the SDN controller. The result for a 5,000-user campus network is a planning and deployment cycle that is reduced from months to days.

Visualized O&M

Routine O&M accounts for more than 50 percent of the workload measured by the Operating Expense (OPEX). A wide variety of normal tasks are interrupted by urgent situations that require expensive troubleshooting, and everyday situations may include complaints by WLAN users about disconnections, access failures, or QoS issues such as frame loss during video services. Preventive measures are necessary to ensure optimal network performance and user experience, such as optimizing devices before they are overloaded and adjusting resource configurations based on daily and weekly traffic flows.



Visualized O&M solutions based on SDN controller platforms supported by Big Data analytics are emerging to help users stay on top of their networks through automation.

- Application Visibility

Application visibility enables users to have a graphical understanding and comprehensive control of their networks. Troubleshooting efficiency is improved:

- Accurate fault location and real-time display of quality indicators, such as delay and packet loss
- Real-time display of CPU/memory/cache resources, with alarms and optimization suggestions
- Display of network paths, including loops and abnormal congestion, with automatic troubleshooting analysis

- User Visibility

User visibility helps in building Big Data platforms to support business analysis, including:

- Recording user service operations
- Tracing user service routes
- Recording user access, connections, and lifecycle characteristics of applications

Visibility into users helps operators obtain aggregated user information on which deep data analytics are performed to determine optimal resource configurations.

Third-party Systems and Complex Customization

In the current market for campus network components, customers have a choice of products from many vendors. At the solution level, however, interworking remains a major challenge as continuous service innovations and the demand for customization are putting pressure on vendors to offer open interfaces.

Two open source organizations are particularly relevant. Open Networking Foundation (ONF) promotes the OpenFlow protocol to decouple the control plane from the forwarding plane of network switching equipment; and OpenDayLight provides an SDN controller that extends the functions of conventional configuration management interfaces, such as the Network Configuration Protocol (NETCONF) and Simple Network Management Protocol (SNMP) for compatibility with legacy equipment on existing networks.

Customers are requiring open interfaces at each network layer, including:

- **Forwarding Layer** for customizing network encryption abilities and services
- **Management Layer** for interworking with third-party controllers, including OpenFlow, SNMP, and NETCONF interfaces
- **Control Layer** for interworking with third-party devices and upper-layer applications

SDN enables campus networks to address a number of critical pain points, including service deployment, O&M, interworking with third-party systems, and complex customization. SDN is an innovative architecture positioned to create a wave of transformations by offering customers the chance to unleash the full potential of their campus networks.▲

Focus

SDN enables campus networks to address a number of critical pain points, including service deployment, network O&M, interworking with third-party systems, and complex customization. >>