SDN, a New Definition of Next-Generation Campus Network

HUAWEI

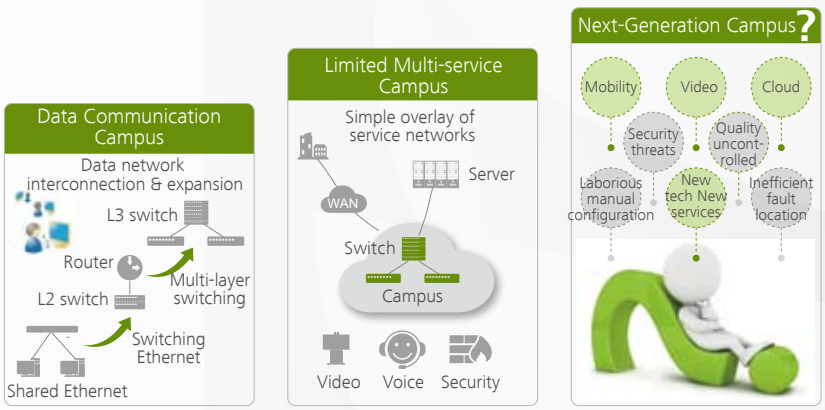
Contents

SDN, a New Definition of Next-Generation Campus Network

Campus Evolution and Development Trends

A campus network is the internal network of an enterprise or institution, where all routes are managed by the enterprise or institution itself. It connects to the WAN and the enterprise's data center, providing network access, data switching, and security isolation for employees, partners, and customers. Essentially, campus network is a networking and security solution.

Campus network development has experienced two stages. The first stage (before 2004) features in the connection-oriented campus networks that meet basic data communications requirements. The second stage (2004 to 2013) features in multi-service campus networks. In this stage, the capacity of campus network has expanded to 10 Gbit/s, and efficient service provisioning and quality management for video services have become core of campus networks.



Now, the third stage, smart campus network, is coming.

Three Changes to Drive the Campus Network Development

Fundamental Changes in User Behaviors

Bring Your Own Device (BYOD) diversifies user access modes in a campus and provides new ways for users to obtain and exchange information, bringing campus networks into the ubiquitous terminal era. Employees work style has changed from fixed (fixed time, fixed location, and fixed device) to mobile (anytime, anywhere, and any device). According to IDC, 35% of enterprise staff will use the mobile work style by 2013, and 1.2 billion users will enjoy the convenience of mobile working. Mobile working has the following requirements for network access:

Flexible: Users can use any of WiFi, 3G/LTE remote access over VPN, and traditional wired network to connect to a campus network.

Uniform authentication and management to improve user experience: A user-centered campus network must be built.

Easy-to-manage campus network without bottlenecks: Enterprises' IT departments want to build a simple network where security policies can be managed and applied based on user identities. Security policy control for WiFi access, remote VPN access, and wired network access should be performed on the same access-layer gateway device, so that wired and wireless access users can be managed in a uniform manner. (Switch and AC are integrated to uniformly manage wired and wireless users end apply security policies. Wired and wireless packets are forwarded on the same forwarding plane. SSIDs and VLAN IDs are used in the same management system.

Scenario awareness, open program invocation: Traditional wired networks can sense only access interfaces and IP addresses of users. In mobile working and multimedia applications, a network must be able to sense users' identities, locations, access time, as well as the access devices and modes they use. To deliver better user experience in these applications, the network must provide diversified user information. For example, an enterprise portal needs to deliver suitable web pages to users based on the device types used by the users, to ensure good user experience. As consumer IT technologies are widely used in enterprises, many consumer products supporting DLNA and Airplay need to be invoked by user terminals. For example, users in a meeting room can share a projector supporting Airplay using their own mobile terminals, and users outside the meeting room can see contents on the projector over the network. To support such applications, the network must have a uniform control center to implement access control and routing policies based on user management. In addition, the network needs to deploy next-generation smart campus core devices–programmable switches, to realize visualization awareness and policy control on network resources.

Fundamental Changes in Services Transmitted on Campus Networks

Nowadays, what users need is not a connection-oriented unaware network, but an application and service oriented network that is able change on demand.

Traditional campus networks are physical networks adopting the best-effort forwarding architecture. Due to bandwidth oversubscription, the bandwidth efficiency on such campus networks is low. On the one hand, the bandwidth oversubscription and best-effort forwarding model cannot provide high bandwidth and high reliability for video services (requiring strict latency and jitter) and non-linear editing multimedia services. When congestion, packet loss, or latency occurs, the network cannot ensure availability, user experience, and quality of these services. On the other hand, to provide as high quality and bandwidth as possible for concurrent services, access networks are upgraded from 100M to 1000M, but the actual average bandwidth utilization is less than 20%. IT departments of enterprises are in a dilemma: They want to improve the network efficiency while providing good network quality and bandwidth guarantee. This brings a badly need for a next-generation virtualized campus network that can adapt to user requirements and provide high-quality services. This network should provide pooling, service-oriented, network as a service (NaaS), like computing and storage networks.

Although traditional campus networks keep improving on reliability and service isolation, the improvements are made on the physical network, for example, MSTP on tree or ring topologies, virtualization through stacking or clustering, and complicated QoS configuration. Additionally, traditional reliability technologies cannot realize service-level reliability in the case of network congestion. It is difficult to improve quality of services sensitive to packet loss and jitter through improvements on the physical network. Temporary faults cannot be located even if these faults occur frequently. Network product and solution vendors are seeking a solution to these problems, but have not found an ideal solution due to limitations on chip and product capabilities. Some vendors have considered using RSVP-TE to isolate important services. However, RSVP-TE tunnels consume many CPU usages, and a network supports at most several hundred RSVP-TE tunnels. MPLS TE configurations are also complicated for IT maintenance personnel. Openflow is also a solution proposed by some vendors. However, as Openflow is implemented using commercial ASIC chips and supports only small entry sizes, it does not support programming based on service characteristics. Enterprise IT departments are concerned that deploying Openflow on the entire network will lose the advantages of traditional routing and forwarding and brings tremendous workloads on configuration and maintenance. For these reasons, Openflow is still an academic concept. A next-generation smart campus network must solve the problem of efficient network quality detection and high-quality service provisioning by changing the network architecture.

In a traditional campus network, the network is separated from services and

adopts static deployment. Therefore, the network cannot quickly adapt to changes in services, such as virtual machine migrations and frequent policy changes for BYOD services. Different services or departments are isolated using VLANs, VRFs, or ACLs, but these isolation technologies only have limited resources. Each device supports only 4K VLANs. The situations for VRFs and ACLs are similar. In addition, configuration and maintenance of these technologies are complicated. Once services or network topologies change, a large number of rules need to be reconfigured. This low-efficient service deployment significantly increases workloads of IT maintenance personnel. How to make a network flexibly adapt to service changes becomes an urgent need.

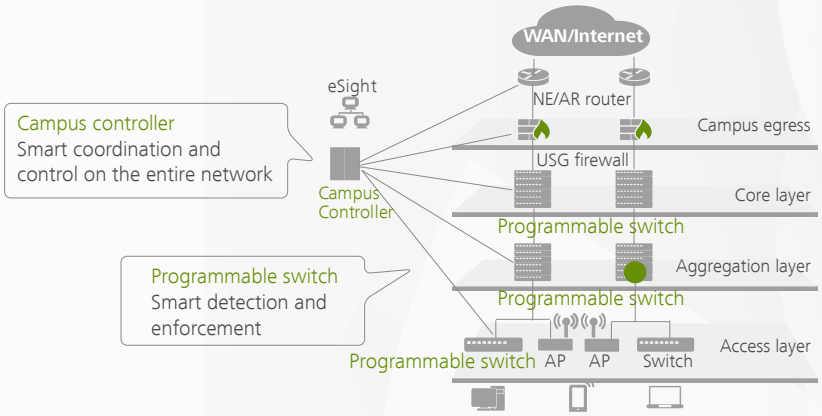
Fundamental Changes in the Traffic Model

The trend toward mobile working, ubiquitous terminals, and cloud computing has significant effect on the traffic model. The new traffic model features in traffic uncertainty, traffic bursts, and high bandwidth requirements. For example, the video service traffic volume is 128 times the voice traffic volume and 68 times the data traffic volume. Burst traffic rate is 3 to 5 times the average traffic rate. The packet loss ratio must be smaller than 10-6 for packet-loss-sensitive services and smaller than 10-2 for voice services.

As data-intensive, storage cloud, and cloud computing applications are deployed, data is concentrated in a data center. Sharing and interaction between users require communication between clients and servers. The use of desktop cloud application poses higher requirement for network latency and jitter. Since all data sent from data center servers, user experience is more sensitive to latency in data transmission. Sometimes, the predefined network deployment may be unable to handle burst traffic. Therefore, a network must have elastic scheduling mechanism and large buffer capacity to cope with uncertainty and flexibility of the traffic model.

Next Generation Campus Network Architecture and Model

The next generation campus network uses SDN-based smart campus network architecture and model.



Uniform Architecture, Global Coordination

1. Wired and wireless integration and implementation of uniform access and policy enforcement

The physical and logical architectures of the wireless AC and switch are integrated. The switch supports vertical stacking (that is, One Switch) and implements the wireless AC function; it can be deployed at the access or aggregation layer. APs and lower-layer access switches are managed by One Switch. The wired and wireless integration switch manages SSIDs and VLANs in a uniform manner; this fully employs mature VLAN configuration and management, facilitates operation and maintenance, and provides flexible access.

Security policies are not separately delivered to the AC and switch but to the switch supporting vertical stacking (One Switch). On a traditional wired network, access or aggregation switches are possible policy control points. Operation and maintenance personnel need to spend much time on device configuration including creating user group policies and setting authentication parameters. After a wireless network is deployed, an AC functions as a policy control point for wireless users. This also increases the configuration burden.

Huawei implements wired and wireless integration on an aggregation switch. This simplifies policy management and configuration because security policies are not enforced on distributed control points. The aggregation switch manages lower-layer access switches and APs, meeting security requirements and reducing network construction costs.

As WLAN technologies develop from 802.11 a/b to 802.11n and 802.11AC, wireless access bandwidth increases from dozens of Mbit/s to 1 Gbit/s; in traditional centralized forwarding mode, an AC will become the bottleneck on a wireless network. In light of these developments, Huawei uses the next-generation programmable switch and programming at the forwarding plane, wired and wireless integration to combine wireless AC forwarding and CAPWAP tunnel termination based on traditional wired forwarding. This implementation enables wired and wireless services to be transmitted on the same path and eliminates the bottleneck.

2. Global coordination based on the uniform campus controller (one controller)

Traditionally, when users access the campus network, the controller required only the identification and access level of the user; however, as BYOD develops, time and point of access as well as terminal type become important also. Security policies such as access control of users and network resources, and access management need to be intelligently enforced. Policies also need to be flexibly defined. For example, different access levels are granted to the same user who can connect to the network using different devices in wired or wireless mode. Visitors to the network must be authenticated and access time limitations established. The controller of the next-generation smart campus network automatically detects these attributes. After users connect to the network, the controller delivers versatile security control policies, which is implemented by One Switch. The campus controller can associate with an edge access switch. In addition, it implements requirements to monitor the load and optimize the path. The uniform policy center manages, controls, and distributes policies, thus providing open interfaces for upper-layer applications to obtain programmable resource capabilities so that the applications can define software.

3. Global coordination ensures network security

Global coordination implements a secure network based on global user detection and network behavior detection, and achieves uniform deployment, on-demand monitoring, and flow-based detection.

Open Resources, Software Defining Capability

The next-generation smart campus network must meet on-demand requirements of the high-quality virtual network and requirements for flexible adaptation in maintenance and scalability.

1. The next-generation smart campus network implements resource openness and programming. The hybrid SDN solution can forward packets using many routes, allows hundreds of or thousands of virtual and isolated networks to be built, and creates many backup paths on virtual networks for load balancing and high reliability. Application examples:

High-quality campus virtual network for Telepresence and video services

Telepresence and video services are core services of enterprises. On a campus network, problems such as slow convergence, node congestion, and insufficient device capability cause packet loss and poor user experience. Huawei IT builds a separate physical network, and Telepresence terminals connect through access switches, without crossing the office network.

The hybrid SDN solution based on the programmable switch can select campus network links with high bandwidth and reliability according to requirements of Telepresence and video services and relegate low-priority services to other paths, building a reliable video virtual network. Because all paths are known and the hybrid SDN solution provides hardware-based NQA fault detection, paths are immediately adjusted according to the detection result, ultimately optimizing user experiences.

Virtual campus network adapting to organization change

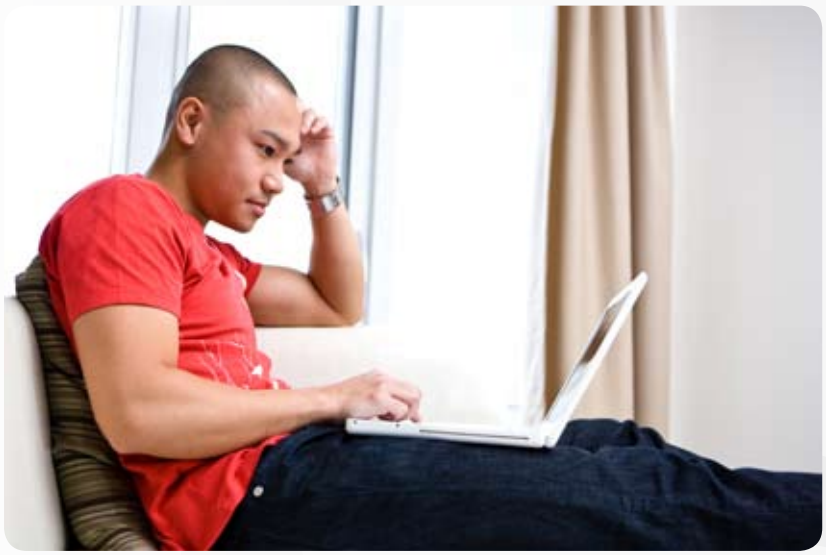
To ensure security, an enterprise divides departments into isolated sections. On a large-scale campus network, service re-isolation and network adjustment involve changes to numerous other configuration policies, making maintenance onerous and error-prone. For example, customers often require that isolation areas be divided project-wise; however, problems also arise where a team belongs to many projects. As a result, network configurations such as VLANs and ACLs frequently change, and the maintenance becomes burdensome. With the programmable hybrid SDN solution, campus controller, and programmable switch, the next-generation smart campus network provides large-scale virtual network capability, and flexibly adds, deletes, and modifies virtual networks in a batch. This greatly improves operation and maintenance efficiency, and meets deployment requirements of flexible service isolation.

2. Campus Controller-based scenario awareness capability, open interface of centralized policy engine, and forwarding-plane programming capability of the programmable switches.

Enterprise applications use these capabilities and interfaces to capture user access status parameters and demands and monitor network resource status, including locations, time, and connection topology. Resource opening capability enriches enterprise services and improves user experience. For example, an international school decides to implement E-learning. The learning share APP invokes the resource opening interface to obtain the Apple TV resource supporting Airplay, and makes the application available to students. Students share their access locations, terminal types, requirements, and courses through the resource opening interface.

3. Programmable Protocol Oblivious Forwarding (POF) for new services deployment and protection of long-term investments

The next generation of smart campus networks use Huawei’ s POF technology. Network behaviors are first defined by the control plane. Enterprises can then customize flexible policies to identify new service packets, which are deployed without affecting the existing physical network, thus protecting network investments.



Scenario Awareness, Quality Assurance

The next-generation smart campus network provides comprehensive network quality awareness and assurance.

The next-generation smart campus network supports the programmable flow-based fault detection mode for service flows and provides the comprehensive network fault detection and location capabilities. Using the switch's programmable capabilities, the fault detection flag can be inserted into service flows on the network to detect and locate any errors.

In the IP network era, the enterprise campus network needs to transmit a variety of services including video, voice, data, and VPN services. As customer requirements and real-time services increase, fault detection requirements on network packet loss ratio, latency, and jitter become higher. Traditional detection methods, such as Y.1731, insert test packets to simulate services, disrupting existing services and failing to report on real-time performance, making them entirely unsuitable for enterprise networks. The next-generation smart campus network uses the programmable network architecture and promotes real-time performance measurement. The network can directly measure real-time service packets, insert detection flags into different service flows, deploy measurement points on different devices, and summarize measurement results on one device for performance measurement.

In essence, the next-generation smart campus network uses the SDN framework and next-generation programmable switches to improve adaptability between campus network resources and services. Additionally, the network architecture is unified and complete, and network quality is measurable and manageable. These advantages contribute to the transition to SDN networks.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The product, service, or feature that you purchase should be restricted by the Huawei commercial contract and the clauses in the contract. All or a part of products, services, or features described in this document may not be purchased or used. Every effort has been made in the preparation of this document to ensure the accuracy of the contents, but the statements, information, and recommendations in this document do not constitute a warranty of any kind, expressed or implied.
The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure the accuracy of the contents, but the statements, information, and recommendations in this document do not constitute a warranty of any kind, expressed or implied.

Huawei Technologies Co., Ltd.
Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518219
People's Republic of China

Website: http://www.huawei.com
Email: support@huawei.com