SDN in the Campus LAN
Offers Immediate Benefits

December 23, 2013
Mike Fratto, Principal Analyst, Enterprise Networking and Data Center Technology

Key Takeaways

• SDN in the campus LAN offers a wealth of opportunities for network equipment vendors to differentiate their product and service offerings.
• Many networking vendors are building out their SDN technologies to the campus LAN making for a competitive landscape over the next several years.
• Enterprise IT has been promised great advances only to be met with mediocre delivery. Expect resistance that can be overcome with demonstrated success.
• Focus on the optimizations SDN offers in operations, security, traffic engineering, monitoring, and application delivery.

Summary

Campus SDN is quietly poised to take off as networking vendors implement SDN technologies in LAN and WLAN equipment, and seek to differentiate their network offerings from competitors. Enterprise IT is ready for SDN in the campus since they are likely already using automation and programmatic control such as network access control and supporting unified communications at a hardware and software level. Extending that automation to an SDN is a natural progression; however, network suppliers will meet resistance to campus SDN from enterprise IT because unfulfilled promises in similar technologies have left a bad taste with administrators. Network vendors can overcome those initial objections by focusing on how campus SDN benefits organizations by providing a more robust framework for network security, isolation, and application delivery without additional management overhead than is available using existing methods.

Perspective

Networking vendors, the technical press, analysts, and bloggers have focused quite a bit of attention on SDN in the data center network because that is where there is an opportunity for enterprises to solve rather difficult and visible problems in building robust virtual environments. While that work will continue, there is also a great deal of benefit in pursuing SDN in the campus LAN such as improving isolation strategies, applying quality of service to application traffic, rapid and automated provisioning, and improved resiliency. In fact, enterprises are primed for SDN in the campus because they are already using automation during daily operations. VoIP phones are automatically discovered when they attach to the network, PoE is applied depending on the existing power budget and the priority of the phone, the appropriate VLAN is assigned to the port, IP addresses are handed out, and QoS is applied ensuring adequate quality of experience for VoIP calls. Many enterprises are using network access control in somewhat limited ways but they are using automated actions based on user or device authentication to provide access control and network provisioning. Some advanced IT shops are using event programming techniques on switches and routers to react intelligently to localized events like congestion or hardware failure.

On the other hand, enterprise IT has also been led down the primrose path of automatic networking before and left with a bad experience they’d rather not repeat. The reliance on the CLI for network configuration
is a direct result of continued gaps between what network management system (NMS) vendors have promised and what is actually delivered. Most NMSs support only a subset of the functionality needed to truly manage even a moderately sized network, which leads the administrator back to the CLI. NMSs are also expensive when software licenses for the NMS and the OS are added to the cost for the hardware, supporting software like a RDBMS, and the operational costs managing the NMS.

Commercial open source NMSs are used for monitoring while configuration and management happens through the CLI or point tools that are particularly well suited for a limited set of tasks such as initial provisioning, mapping, and data gathering for capacity planning or troubleshooting. Few IT staff or their management want to spend their time pecking away at a keyboard. They’d prefer to spend their time increasing the reliability of the network, ensuring good network performance regardless of utilization, and support other IT initiatives. When taken together, that points right at the goals of a software defined network that can respond intelligently to changes in the network, provides timely performance data that can be acted upon automatically or via manual intervention, and can help deliver the applications and services that IT and the organization demand.

Use Cases

There are a number of use cases that can help organizations improve their campus LAN today without adding more management overhead and they are significant enough to get IT to take notice. Network access control (NAC) was all the rage several years ago but inflated claims about the efficacy of the various technologies—over seven different access control methodologies at one point—combined with products that were poorly integrated with existing and newly acquired IT products doomed the NAC market to failure. Meanwhile, organizations realized few benefits from NAC and were largely successful only in separating employees from guests. However, enterprises want better control over client traffic for traffic engineering purposes which includes isolation as well as application performance than they are getting with existing VLAN and QoS methods.

Network isolation along with improved packet and flow processing based on a user identity is possible at the network level with improved 802.1X handling on wired ports and protocols like OpenFlow and Shortest Path Bridging (SPB) that provide more granular isolation on a per user or application level. Already Alcatel-Lucent, Avaya, and HP have demonstrated interoperable SPB implementations and the first two have live deployments. One of the design goals of SPB was reduced management overhead, which has been achieved. New additions to the protocol such as 802.1Qca - Path Control and Reservation, promise to provide better management control over SPB paths so that non-shortest paths can be implemented programmatically. The big benefit of SPB is that it is already available and interoperable on switches from a variety of vendors.

Along with network isolation, supporting mobile clients in the wired and wireless LAN is becoming increasing important as employees move about the enterprise. On the wired side, increased use of virtual desktop infrastructure (VDI) and VoIP is driving the need to tie a user identity to a network location and provide network and voice related services such location, call delivery, and E-911 regardless of where the user appears. On the WLAN, changes in wireless architectures such as moving from a pure controller or controller-less architecture to a hybrid approach that offers centralized controller based management and enforcement but off-loads traffic processing to the wireless AP or directly attached switch lends itself to a SDN model where control extends to the LAN/WLAN edge or even to the WLAN itself. SDN technologies will make network provisioning more user or node specific as well as dynamic as wireless devices roam from AP to AP. The benefits will be twofold, namely ensuring a user or node’s network policy moves based on roaming events and secondly allows WLAN traffic encapsulated in CAPWAP can be processed according to a policy to and from the controller.

Network traffic demands are increasing not only in terms of required capacity but also in terms of low and consistent latency that is required for unified communications and collaboration (UC&CC), live streamed media, and VDI. As uplinks become congested, all traffic suffers some loss of quality with high
priority suffering less and lower priority traffic suffering more, but all traffic suffers degradation because the traffic has to traverse the same limited number of links. Hop-by-hop queuing techniques used today are ultimately best effort and don’t have end-to-end control. The end-to-end nature of SDN provides an overall context for traffic management in a controller-based network and there’s a natural integration point for application servers to tell the network how to treat various traffic flows. For example, Microsoft is integrating Lync with other vendors’ networking gear so that encrypted traffic can be identified by Lync, which in turn tells the network--devices or a controller--what kind of prioritization is needed. Several vendors including Aruba Networks, Brocade, Dell, HP, and Juniper have Lync integration, and that is an example of inter-vendor integration and operation between an application and networking. Citrix has been working with several networking vendors to integrate its XenApp and XenDesktop platforms to provision the network proactively.

Active integration is superior to passive application classification because encrypted traffic can’t be properly classified, however, passive application detection such as Cisco’s NBAR and Alcatel-Lucent’s Application Fluency can be used to identify traffic on the network and apply access and quality controls based on a pre-defined policy. We expect to see intelligence at the network edge feed into a SDN controller in future products.

SDN provides improved traffic engineering by being able to create multiple paths through the network dynamically and intelligently. In the data center where there is a high concentration of servers and storage, multi-path Ethernet is highly desirable and achievable. In the campus LAN where clients, servers, printers, and other elements are distributed over a much larger area and traffic naturally lends itself to flows north/south between network tiers versus east/west in the data center, multi-path Ethernet has uses as an alternative to switch stacking and link aggregation strategies. In addition, building and campus wiring lends itself to tree topologies radiating from a central location; however, multi-path Ethernet in the wiring closet, within a building, or where there are divergent physical paths between buildings let organizations take advantage of all available network bandwidth with path diversity which naturally increases resiliency in the event of network failure.

Strategies

Without moving into new protocols like OpenFlow and SPB, SDN can be used with existing technologies like QoS marking, VLAN assignment, and ACL assignment using port profiles on existing networking equipment, but the granularity is relatively coarse when compared to what could be achieved with protocols like OpenFlow and SPB. In fact, it’s important to remember that OpenFlow was originally designed to provide researchers with the ability to create isolated networks running alongside production networks on existing campus equipment.

OpenFlow has a number of benefits such as a centralized controller that can take into context the entire network topology and capacity in making path decisions. Policies can be applied granularly such as down to the port, flow, user level or combination selectors. After the policy is applied, it is distributed across the network once. New versions of the OpenFlow specification give vendors better instrumentation to collect data from the network and extend the protocol as needed. OpenFlow has a number of drawbacks as well (e.g., being a new protocol and technology), which means network administrators need to take the time to understand how it works, how their chosen vendor has implemented it, and what it will take to deploy OpenFlow in their environment such as any necessary equipment upgrades, new purchases, and employee training. Much of the OpenFlow development activity has been in data center networking so vendors should develop OpenFlow applications relevant to the campus LAN. HP is heavily invested in OpenFlow with development from the technologies inception and support on over 50 of their networking products and other vendors are adding OpenFlow support with new product launches.

SPB, while not typically considered an SDN technology, provides many of the same features and benefits of OpenFlow without needing a controller and for the early backers of SPB such as Alcatel-
Lucent and Avaya there are already demonstrable interoperable products in the campus LAN market. In SPB, the action happens at the edge with traffic assigned to a virtual network on ingress which requires intelligent access devices that can properly identify and classify network traffic. Access switches from Alcatel-Lucent, for example, are integrated with their UC&C platform to assign traffic as it enters the network. In addition, classification engines can classify other traffic based on regular expressions matching which is better than basic port identification but lacking full classification engines such as Cisco’s NBAR. Expect traffic classification either at the network edge or via a controller will improve over time, providing more accurate data to use in making policy decisions.

### Near Term Drivers

- SDN technologies will continue to be developed for the campus LAN to provide better policy control and isolation on the LAN as well as extend applications management from the data center to the end user. Increasing use of BYOD WLAN clients is driving the need to have a more proactive network.

- Networking vendors are offering campus SDN and automation technologies for improved operations and end to end application and user control. The increased use of SDN will be a differentiator in competitive bids for network installations and upgrades.

- Converged wired and wireless networking is bringing together management strategies forcing uniform policy management and implementation across all networking. The increasing BYOD phenomenon is forcing enterprises to support more devices and provide access to company resources with the same policies in place.

- Campus LAN IT has been using automation more and is comfortable with defining automated actions. That prepared them for increasing the use of automation throughout the campus LAN which frees up IT to work on other tasks.

- IT hiring is still low but enterprise demands are increasing forcing IT to do more with less. Increasing demand for more agile networks that support the mobility of users is putting pressure on IT to automate many IT functions that are manual today.

### Competitor Response & Recommendations

- Alcatel-Lucent and Avaya should continue to promote the use and benefits of SPB in the campus LAN focusing on increasing the robustness of the network without impacting IT operations, the end-to-end nature of SPB and the benefits to application performance and security, and highlighting proven interoperability.

- Dell and HP should promote the use of OpenFlow in the campus LAN highlighting the benefits of OpenFlow over traditional networking and SPB. Demonstrating how OpenFlow controlled networks can address campus needs like isolation, security, application performance, and telemetry are key. Finally, showing how OpenFlow can be phased in gradually over time will ease enterprise IT hesitation.

- Cisco should continue to promote existing automated and integrated network features such as Trust-Sec and EnergyWise that leverage the value of the network and Cisco’s integration partners. In addition, continuing to educate the market on OnePK and keep the roadmap running is critical.

- All vendors should continue to show improved network security through per node or use isolation and better capabilities to quarantine devices and users; however, they should not refer to it as NAC, which has the perception of failure.

- All vendors should highlight interoperability among competitors that shows enterprise IT new equip-
Report:

SDN in the Campus LAN Offers Immediate Benefits

- All vendors should provide case studies in the form of white papers, webinars, and other media showing enterprise customers successfully deploying SDN in the campus. The case studies should include warts and all so that potential customers understand the potential hurdles and how they are overcome.

- Understand that campus SDN is unlike data center SDN and there is a great deal of automation that can be accomplished with software APIs that vendors are creating for their networking gear. You may not need a hardware refresh to gain the benefits of campus SDN, so be sure to explore the options with your VAR or vendor.

- Acquiring products supporting technologies like OpenFlow or SPB can narrow the choices you have in the future for integration of new products. Be sure that you fully understand your vendor’s partner ecosystem and understand the integration capabilities that are available.

- Evaluate your VAR’s capability and expertise with their vendors SDN products since you will be relying on them to help deploy and troubleshoot SDN in your network. SDN is still new technology and VARs are getting up to speed on their suppliers’ product lines and capabilities.