University Lowers Barriers, Fortifies Security with Virtualization

University of British Columbia network virtualization saves money and improves security for faculties and departments.

EXECUTIVE SUMMARY

University of British Columbia

- Education
- Vancouver, British Columbia
- 13,600 faculty and staff, 50,000 students

BUSINESS CHALLENGE

- Lack of campus network capacity constrained flexible use of resources by students and faculty
- Proliferating department-level firewalls slowed performance and hampered troubleshooting
- Capacity requirements in data center grew exponentially, adding to IT costs

NETWORK SOLUTION

- Cisco Catalyst 6509 Series Switches, equipped with 10 Gigabit Ethernet modules, support high-performance dual-layer campus core, and attachment to campus distribution and access layers, and to data center
- MPLS VPNs, combined with Firewall Services Modules (FWSMs) on the Catalyst 6500 switches, support fully virtualized campus network
- Cisco Nexus 5000 Series Switches extend virtualization across data center, to support secure access to centrally-stored resources

BUSINESS RESULTS

- Network virtualization provides improved security for departments and faculties, along with simplified design, deployment, and troubleshooting
- Over 150 physical firewalls eliminated to date, allowing better throughput across campus, from data center to end user
- Applications, virtual machines, and storage can be more flexibly used by faculties and departments, without being constrained by location of physical networks or physical firewalls

Business Challenge

In 2008, the University of British Columbia (UBC) celebrated its 100th anniversary. UBC founders established B.C.'s first university to help transform a frontier province into a prosperous contributor to the nation and the world. The school has certainly exceeded expectations, ranking among the top 40 institutes in the world for the last five years.

There are over 200 buildings spread over the 1.5 square mile UBC Vancouver campus. Nineteen faculties, including the schools of Medicine, Architecture, Law, and Engineering, and dozens of departments rely on the advanced technology provided by UBC's IT and network infrastructure team.

However, each faculty also has its own IT staff and budget, resulting in a dynamic balance between decentralized departmental control and University-wide IT policies and programs. One of the downsides of decentralized control was the growing proliferation of physical firewalls deployed by each faculty. Numerous firewalls caused issues with troubleshooting problems across the network, hampering support. In addition, budget constraints often resulted in the use of low-end firewalls by faculties and departments that slowed performance. Firewalls also created physical boundaries within which departments had to operate, greatly limiting flexibility in accessing resources across campus. For example, the Faculty of Arts has 24 departments operating in over 30 buildings, making deployment and configuration of distributed physical firewalls challenging.

Firewalls are required for implementation of each faculty or department’s security boundaries and policies, yet the method of firewall deployment and use across UBC was not keeping pace with the University’s needs.

Demands on the UBC data center were also increasing significantly. Storage needs were more than doubling every year, driving up capital and operating expenses.

In 2008, Marilyn Hay, Manager of Network Planning in the University's IT Infrastructure group, initiated a project to virtualize faculty and department networks and firewalls across campus. At the same time, Lois Cumming, Manager of Systems in the University's IT Infrastructure group, also initiated a server and storage virtualization project in the data center. “Over time, we recognized that there were tremendous synergies between the network virtualization and data center virtualization projects,” says Hay, “and the two programs worked together to achieve more than we ever anticipated.”

> “Faculty and departments maintain the control they are accustomed to, securing information better than before, while expanding their ability to use campus resources. The University can manage campus-wide resources more efficiently and cost-effectively."
> **— Marilyn Hay, Manager of Network Planning, University of British Columbia**

Network Solution

To support growth, UBC worked with Cisco to increase network core capacity to 10 Gigabit Ethernet. The University uses a four-layer network architecture, which consists of outer and inner core layers, with access and distribution layers servicing buildings across the campus. Ten Cisco Catalyst® 6509 Switches, equipped with 10 Gigabit Ethernet modules, form the UBC outer and inner campus core, with Cisco® Catalyst 4900M and 3750-E / 3750G Switches at the campus distribution and access layers.

The investment in the Catalyst 6509 switches demonstrated additional benefits when Hay's team decided to implement network virtualization using Multiprotocol Label Switching (MPLS) VPNs. Although service providers have made use of scalable MPLS technology for years, with the introduction of MPLS VPN support on the Cisco Catalyst 6500, the benefits of MPLS have now become affordable for campus environments like UBC.

MPLS VPNs can be configured to securely virtualize the network, transparently connecting users and resources at any location across the campus, without performance or network design compromises. Each department or faculty is provisioned with one or more VPNs, allowing secure separation of functional areas across campus in a simple, scalable fashion.

The modular Catalyst 6500 chassis supports Firewall Services Modules (FWSMs), which were virtualized by the University for the individual security needs of the faculties and departments. Each faculty and department continues to manage its own security policies, on its own virtual firewall. The virtual firewalls are located centrally, at the boundary of a department’s VPN, eliminating the need to distribute multiple physical firewalls over multiple buildings. Without the physical firewalls in the cross-campus data path, departments now have a high-performance, virtualized, and secure infrastructure all the way from the data center to the desktop user.

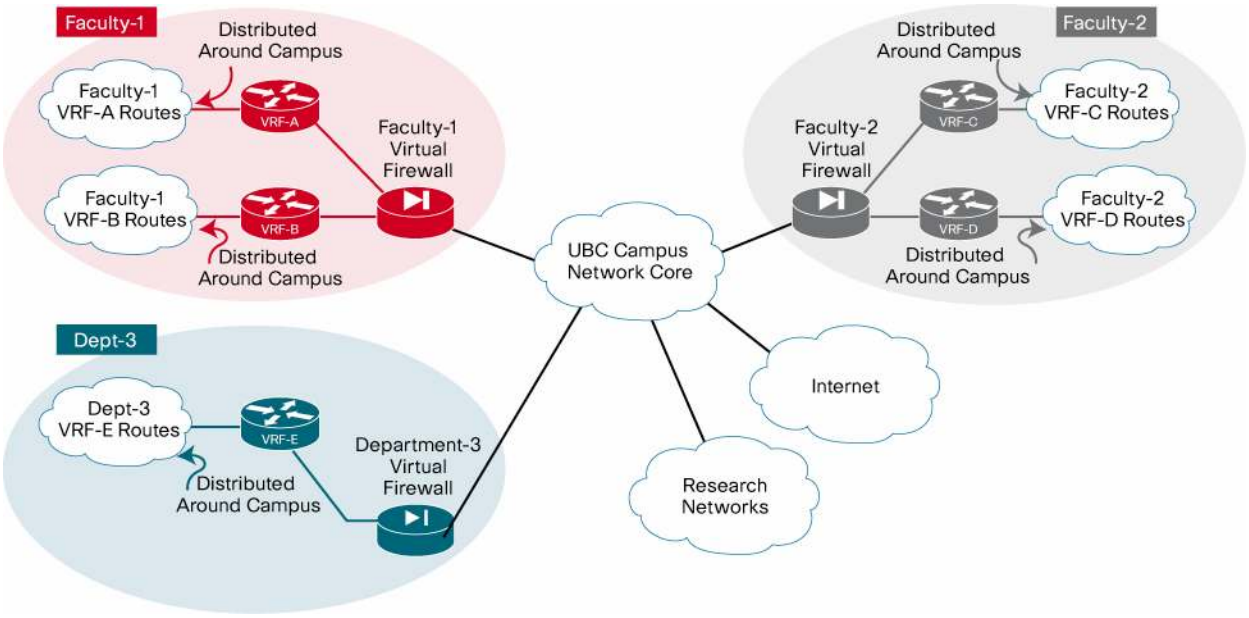
“We have essentially given faculties and departments their own private clouds with high performance access to virtual data center resources,” says Hay. “They maintain the control they are accustomed to, securing information better than before, while expanding their ability to use campus resources. At the same time, the University can manage campus-wide resources more efficiently and cost-effectively.”

Technical Implementation

To design the network and plan the deployment with confidence and speed, the UBC team took advantage of published Cisco design guides for campus-wide network virtualization. These guides provide multiple options for

architecture, design, and deployment, all using a modular approach including access control, path isolation, and services edge capabilities.

UBC provides each faculty or department with its own set of VPN routing and forwarding (VRF) instances. A VRF is essentially a separate IP routing table that allows a faculty or department's set of subnets, located anywhere on campus, to be partitioned from those of other faculties or departments. Each set of VRFs is deployed with an associated redundant virtual firewall pair, located on the Catalyst 6500 FWSMs in the UBC outer core layer. This arrangement allows secure access in and out of each VPN, for traffic flowing between functional areas within a department, between faculties and departments, or out to the Internet.



By using a virtualized network infrastructure, UBC is able to centralize its security policies, and force traffic to route through a central virtual firewall for each faculty and department, regardless of their location on campus.

Two Cisco 7200 Series Routers act as route reflectors for the UBC MPLS VPN deployment, greatly simplifying the deployment and making scalability easy. To maximize performance, UBC has also implemented a pair of Cisco Catalyst 6500s, for 10 Gigabit Ethernet throughput and scalability, at the Internet border.

In the data center, UBC deployed the Cisco Nexus® 5000 Series Switches to help consolidate physical and virtual servers and storage devices. The virtualized servers and IP-based storage are mapped to VLANs within the data center, which are mapped into the VRFs and virtual firewalls designated for each faculty or department. This mapping provides high-performance access and security all the way from the virtual machines in the data center to the applications on user desktops.

UBC also added Application Control Engine (ACE) modules to the Catalyst 6500 switches to provide virtualized load-balancing services for faculties and departments. When University users access resources at the data center over the virtualized campus and data center network, the ACE module load balances the sessions across the appropriate pool of virtual and physical servers, as required.

Because the ACE modules are providing virtual load balancing, like the virtual firewalls, each department and faculty can configure and manage its own load-balancing configuration and rulesets. This capability helps ensure that each department gets the services that it needs from the data center, while allowing UBC's IT department to scale and adapt resources based on changing requirements.

UBC also uses Network Analysis Modules (NAMs) in its Catalyst 6500s, for packet-level inspection and troubleshooting. Because the NAMs understand MPLS VPN tags, the network team continues to use these familiar tools in their virtualized environment.

UBC's Business Operations department participated in the network virtualization pilot program, which replaced five physical firewalls, located in five buildings, with a campus-wide virtualized network equipped with a single, fully redundant virtual firewall pair. The planning took two weeks, and the cutover was "100 percent trouble-free," says Dennis O'Reilly, senior network architect at UBC. "And after a year and a half of operation, we have not had a single technical issue."

Business Results

O'Reilly has been with UBC for four decades. Over that period of time, he can cite about seven technology changes that he would characterize as revolutionary in the life of UBC. O'Reilly sees the network and data center virtualization projects as having that level of impact on university life.

"Departments wanted control of their resources, and did not want to rely on centralized IT resources," says O'Reilly. "Now the buy-in has skyrocketed. Departments are saving money, because we can take advantage of volume purchases. The virtualization program has done more than eliminate equipment, it has empowered our whole educational system."

At UBC, faculties and departments participate in the network virtualization program on a strictly voluntary basis. Over 60 departments have signed up for virtualization so far, and over 150 physical firewalls have been decommissioned to date.

O'Reilly says that the trust between faculty IT staff and the central IT staff has continued to strengthen, because the responsiveness of Hay's team has improved thanks to virtualization. "We virtualized the Faculty of Medicine in a single day, and the cutover was completely nondisruptive," says O'Reilly. "We can accommodate user requests in much less time, sometimes from months to days."

"Breaking down physical firewalls has actually broken down other kinds of walls; now departments can more easily reassign classrooms and even change buildings," says O'Reilly. "And without the low-performance physical firewalls in the way, users are now experiencing much higher performance to the desktop."

Prior to virtualization, UBC limited the use of multicast due to security concerns. Within the virtualized network deployment, such security concerns are alleviated. The University can now provision multicast support, both within and between VRFs, in a secure and controllable fashion. Multicast services over UBC's virtualized network allow new types of applications to be deployed across the campus, including image distribution for labs, as well as video distribution for learning and interactive services.

Centralizing and virtualizing departmental services has had another benefit: a better backup and disaster recovery strategy. Previously, each department had to worry about its own disaster recovery planning. Now all faculties and departments that are participating in the virtualization program can be more confident, because their information is centrally stored, and automatically backed up, in the data center, while helping ensure that secure departmental separation is maintained, both within the data center, and across the University's campus network.

"When we did the network core upgrade, the virtualization project was not on the horizon," says Hay. "With our existing Cisco infrastructure, the overlay did not cost us anything, and the payback in terms of user satisfaction has been incalculable."

Next Steps

UBC is in the process of mapping its virtualized campus wired network into the University's large, campus-wide wireless network of over 2000 access points, using the Wireless Services Modules (WiSMs) in the Catalyst 6500 switches, allowing the extension of virtualized departmental services to both wired and wireless users.

In addition, UBC's virtualized network provides the foundation to deploy a virtualized desktop infrastructure, which UBC is currently evaluating.

It is a virtual certainty, as UBC's virtualized network and data center deployment continues to expand, that faculty and students will continue to give virtualization high marks.

PRODUCT LIST

Borderless Networks – Switching and Routing

- Catalyst 6500 Series Switches
- Catalyst 4900M Series Switches
- Catalyst 3750-E Series Switches
- Catalyst 3750G Series Switches
- Cisco 7200 Series Routers

Security

Firewall Services Modules (FWSMs)

Wireless

- Wireless Services Modules (WiSMs)
- Wireless Control System (WCS)
- Wireless Access Points (AP 1140)

Network Management

Network Analysis Modules (NAMs)

Data Center – Switching

- Nexus 5000 Series Switches
- Cisco MDS Series Switches

Data Center – Load Balancing

- Application Control Engine (ACE) Modules
- ACE 4710 Appliances

For More Information

For more information on Cisco's Network Virtualization design guides, go to http://www.cisco.com/go/networkvirtualization

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C36-9609342-00 06/10