

Innovations in Campus Network Design and Service Delivery through Network Virtualization

Dennis O'Reilly
Network Architect
The University of British Columbia
dennis.oreilly@ubc.ca

QUESTnet
July 2010



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

- About UBC
 - UBCNET Network Architectural Overview
 - Business Challenges
 - Network Virtualization
 - Innovations in Service Delivery
 - Status to Date
 - Business Results
 - Business Case
 - Technical FAQs
- 10 min
- 15 min
- 10 min



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

The University of British Columbia (UBC)

- Located in Vancouver, British Columbia, on the west coast of Canada.
- Vancouver was the site of the 2010 Winter Olympics
- Ranked in top 40 universities in the world for the last five years.



The University of British Columbia (UBC)

- The Vancouver campus is located 20 minutes from downtown Vancouver.
- 402 hectares (4 square kilometers).
- Surrounded by beaches and forested park land.
- Several hundred major buildings.



The University of British Columbia Facts:

50,000 students
13,600 faculty and staff
19 faculties

<http://www.publicaffairs.ubc.ca/services-for-media/ubc-facts-figures>

This photo was taken from the top of a local mountain
looking down on Vancouver on a foggy winter day

Part 1

UBCNET Network Architectural Overview

Network Architecture, 10Gig Core, Internet Edge



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

Campus Deployment

- UBC has several hundred major buildings spread over the Vancouver campus.
- To aid scalability, UBC has adopted a standard campus network architecture.
- A typical large building is shown here.

Typical Large Building



UBC Life Sciences Building



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

7

Building Access Layer

- A typical building uses multiple access switch stacks, one or more per floor.
- All access layer stacks are Layer 2 only.
- All VLANs within a building are available on all L2 switch stacks in that building.
- VLANs are not bridged between buildings.
- The average number of VLAN per building is 20
- VLANs are used to segregate functions with a building. E.g.,
Departments, Faculty, Staff, Students, Labs, Servers, VoIP, Wireless, Building Mgmt Systems, Security Systems, etc.

Typical Large Building

Cisco and Nortel
Switch Stacks in
Comm Rooms



Layer
2

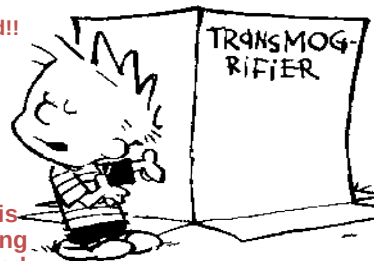


Access
Layer

UBC Has 2,887 Ethernet
Switches Installed

3,899 VLANs allocated!!

VLAN provisioning is
automated using using
an in-house developed
tool called the
Transmogrifier



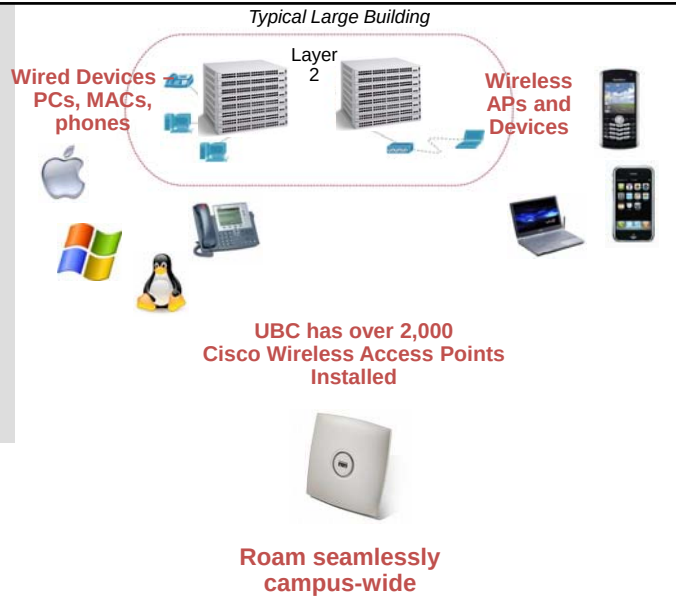
a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

8

Users – Wired and Wireless

- UBC users utilize many diverse devices and operating systems.
- All new access switches are 10/100/1000 and POE.
- ~60,000 network ports.
- UBC deploys over 2,000 APs, providing wireless coverage within all buildings on campuses.
- An wireless mesh deployment underway for outdoor plazas, bus loops, fields, and farm areas.
- 17,000+ concurrent wireless users.



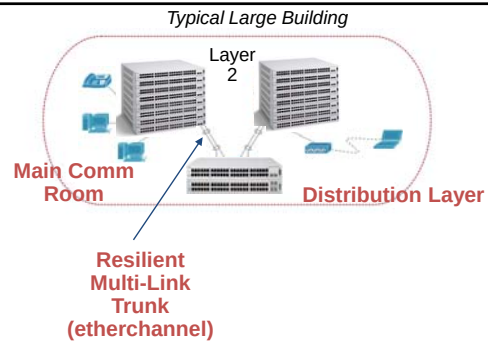
a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

9

Building Distribution Layer

- Within a building, access switch stacks attach to a distribution switch stack in the main comm room.
- The distribution layer is also Layer 2 for the most part.
- Resiliency provided by multi-link trunks to access switch stacks.



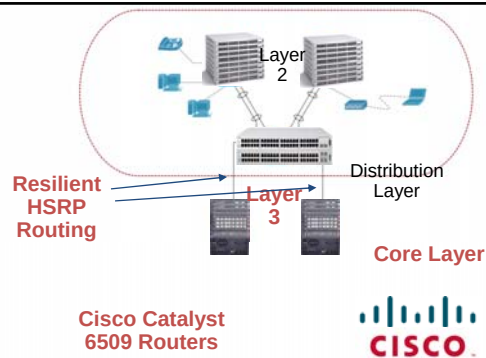
a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

10

Core Layer

- Buildings have Gig backbone connections to two core routers.
- Core routers are Cisco Catalyst 6509s.
- Core provides Layer 3 termination (routing).
- Resiliency provided by HSRP and OSPF.
- OSPF convergence is sub second



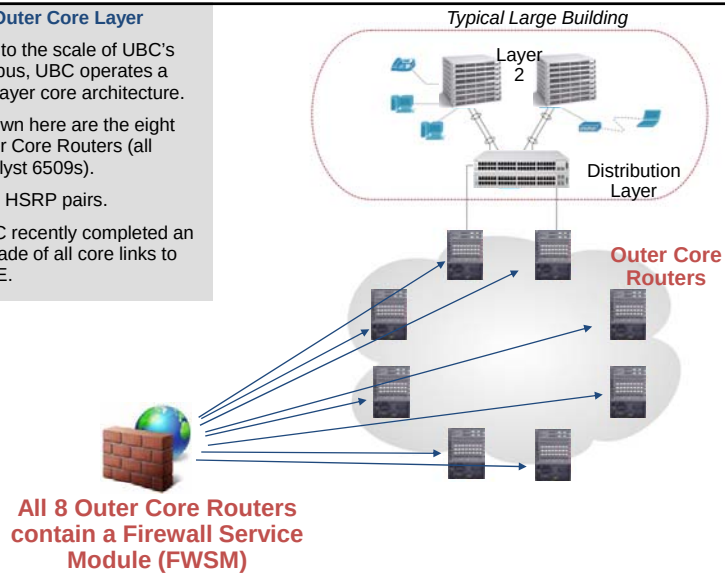
a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

11

Outer Core Layer

- Due to the scale of UBC's campus, UBC operates a two-layer core architecture.
- Shown here are the eight Outer Core Routers (all Catalyst 6509s).
- Four HSRP pairs.
- UBC recently completed an upgrade of all core links to 10GE.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

12

Inner Core Layer

- Due to the scale of UBC's campus, UBC operates a two-layer core architecture.
- Shown here are the two Inner Core Routers (also Catalyst 6509s).
- UBC's core network is completely L3 routed (OSPF)
- OSPF convergence is sub second.
- no bridging through the core (802.1Q is not used).

Typical Large Building

Inner Core Routers

Outer Core Routers

Distribution Layer

Layer 2

All Interfaces in the Core are 10GIGABIT

No bridging through the core

Jumbo Frame Enabled

Fully resilient core based on OSPF routing

a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

13

Buildings Across UBC

- UBC's Vancouver campus connects several hundred buildings of all sizes across the extensive UBC site.

Typical Large Building

Inner Core Routers

Outer Core Routers

Distribution Layer

Layer 2

All Interfaces in the Core are 10GIGABIT

No bridging through the core

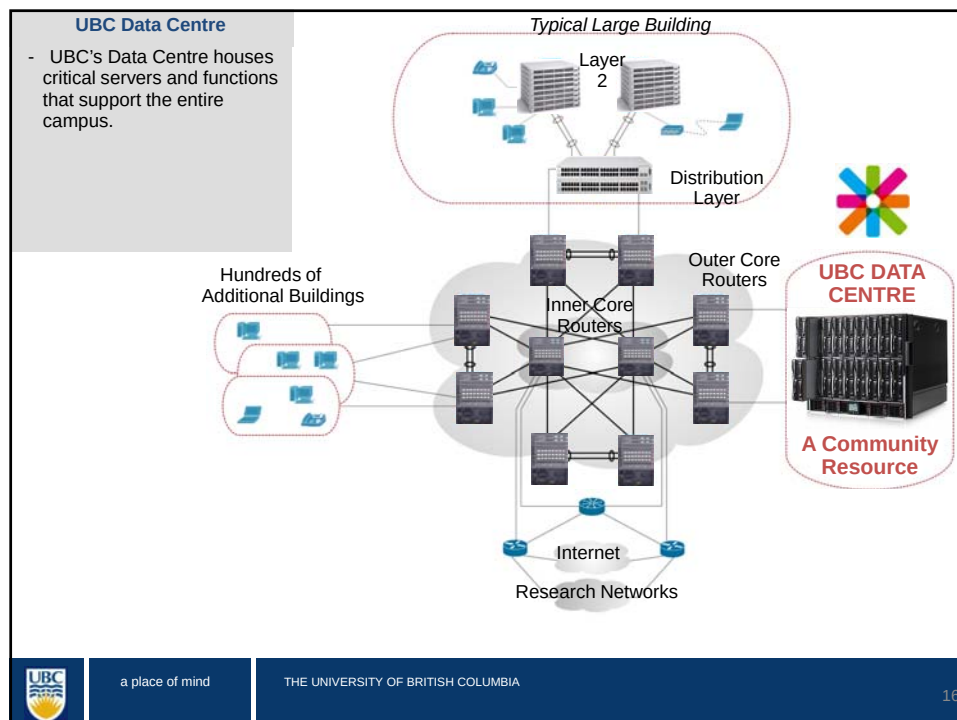
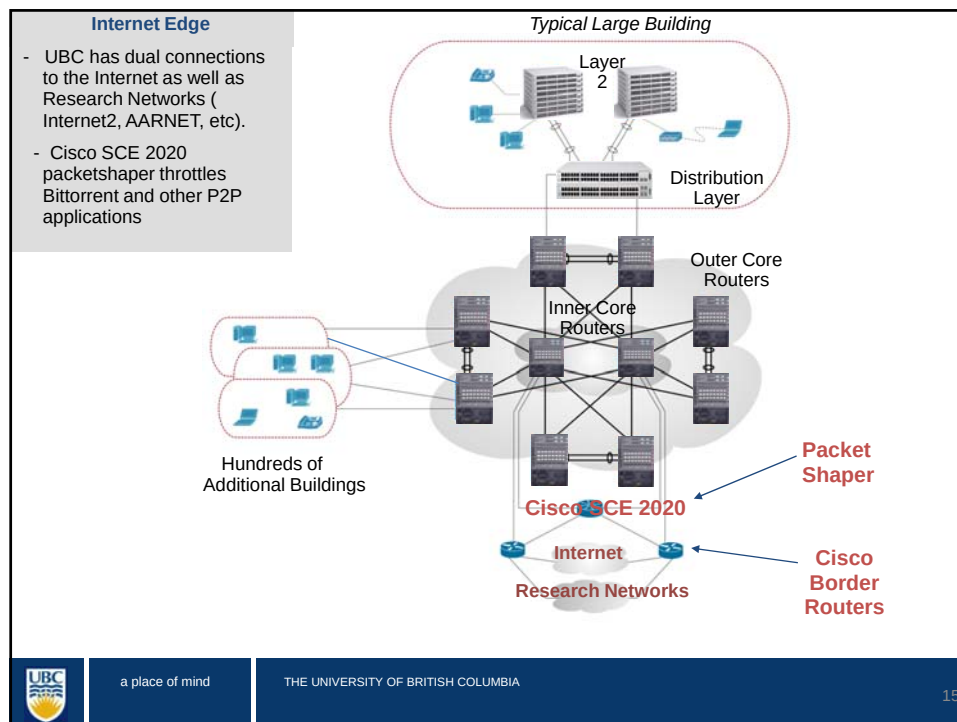
Jumbo Frame Enabled

Fully resilient core based on OSPF routing

a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

14



Interesting UBCNET Metrics ...

- Number of Ethernet switches installed = **2,887**
- Number of Wired Ports = ~ **60,000**
- Number of VLANs Allocated = **3,899**
- Number of Wireless Access Points = ~ **2,000**
- Maximum Simultaneously Connected Wireless Users = **17,000+**
- Total Commercial Internet Bandwidth = **1,750Mbps**



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

17

Part 2 Business Challenges



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

18

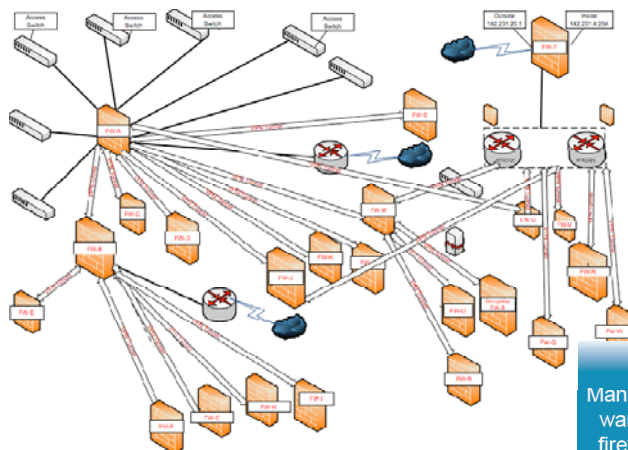
Business Challenges – Network

- Hundreds of buildings. 19 Faculties. Over 200 departments. Several thousand subnets.
- Faculties and departments have space in many buildings. Example, Faculty of Arts has space in 31 buildings.
- Proliferating low-end department-level firewalls across campus slowed performance and hampered troubleshooting.
- Faculties and departments want a single central fully redundant firewall to control access to all of their subnets and VLANs campus-wide?

How to accommodate this?



Business Challenges – Network



UBC Faculty of Medicine Network
Pre-Virtualization

Proliferation of different firewall types

Performance
issues as
campus scales
to 10GE

Difficult to support and troubleshoot

Many UBC faculties / departments want a **single, fully redundant** firewall system for their subnets and VLANs, Campus-wide.

How to accommodate this?



UBC – Business Challenges – Data Centre

- The University wants to virtualize all servers and storage in the data centre to achieve economies of scale, to save energy, and to provide off site backup of all data.
- Faculties and departments don't trust the central IT department. In many cases they operate their own servers, leading to increased costs for equipment, increased energy usage, and increased staff requirements.
- Firewalls protecting the data centre are performance bottlenecks, especially for virtual storage.

How to make departments trust the IT department, and understand that the data centre is a community resource?



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

21

Part 3 Network Virtualization



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

22

Network Virtualization – Concept #1 - VLANs

- Network Virtualization isn't new. VLANs are a form of network virtualization (at Layer 2).
- VLANs provide privacy, security, reliability within buildings.
- Many departments have asked UBC IT to bridge VLANs campus-wide.
- A nice idea, but it doesn't scale.
- So we have always said **NO**.



Question of the day:

- How is network virtualization extended campus-wide without using VLANs ???



a place of mind

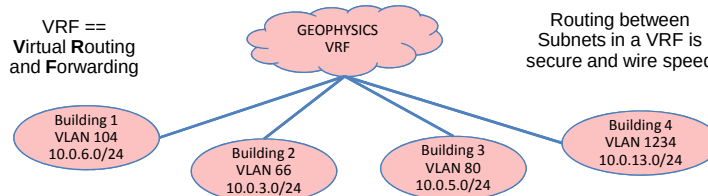
THE UNIVERSITY OF BRITISH COLUMBIA

23

Network Virtualization – Concept #2 – VRFs (1 of 3)

Introducing “VRFs”

- To extend network virtualization campus-wide, we virtualize the routers in the core network, effectively giving each department their own private campus-wide networks called VRFs.



- Just as VLANs work by having separate layer 2 forwarding tables (MAC address tables) in the switches, so VRFs work by having separate layer 3 forwarding tables (route tables) in the routers.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

24

Network Virtualization – Concept #2 – VRFs (2 of 3)

What is a VRF?

- A VRF is a completely private campus-wide network.

Routes
learned
via BGP

```
ROUTER#show ip route vrf ARTS-SOCIALWK
Routing Table: ARTS-SOCIALWK
B       10.82.73.24 [200/0] via 10.103.206.200, 2w4d
        10.103.0.0/24 is subnetted, 1 subnets
C       10.103.112.0 is directly connected, Vlan868
B*     0.0.0.0/0 [200/0] via 10.103.206.200, 2w4d
ROUTER#
```

- Any Subnets in any building campus-wide can be assigned to a particular VRF.
- A Subnet can be in only one VRF.
- A Subnet does not have to be in a VRF. In that case it is in the global routing table.
(The global routing table is the default VRF.)



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

25

Network Virtualization – Concept #2 – VRFs (3 of 3)

VRFs and Security

- A VRF allows different Subnets in different buildings anywhere on the campus to communicate directly, in a completely secure way, at wire speed.
- A department can have as many VRFs as they require to implement their security policies.
- To connect to a Subnet outside of a VRF, you must go through a firewall. Usually this is a Virtual Firewall.

Jumbo
Frames
enabled

Subnet
assigned
to VRF

```
ROUTER#show run interface vlan868
interface Vlan868
  description SOWK01-GENERAL=ARTS-SOCIALWK
  mtu 8500
  ip vrf forwarding ARTS-SOCIALWK
  ip address 10.103.112.254 255.255.255.0
  ip helper-address 10.82.1.1
  ip helper-address 10.103.1.1
End
ROUTER#
```



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

26

Network Virtualization – Concept #3 – Virtual Networks

Introducing “Virtual Networks”

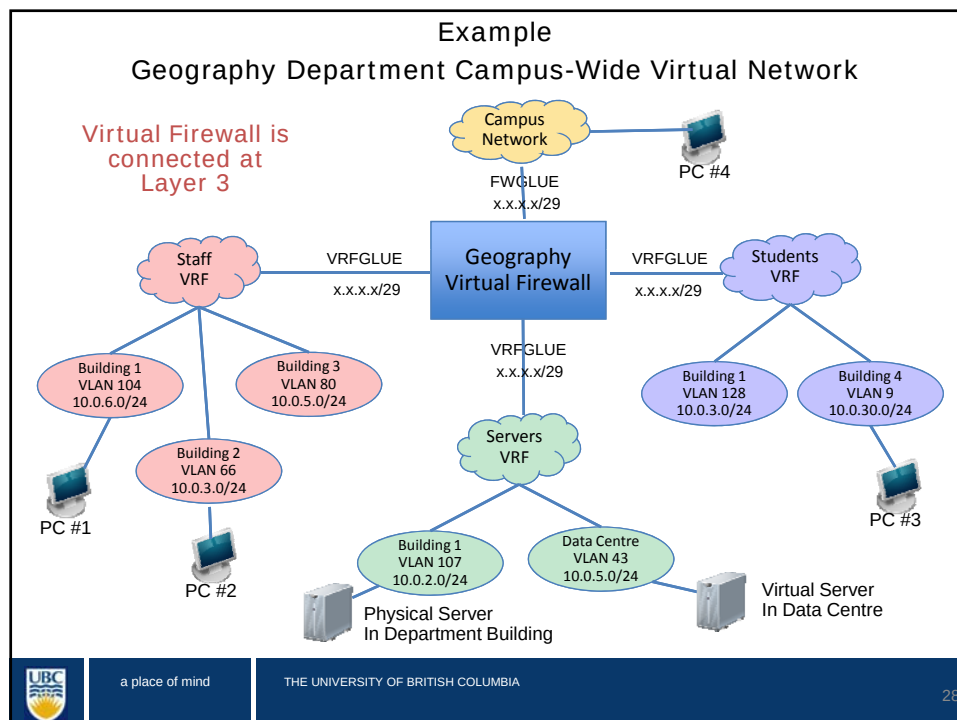
- Previously departments could construct private networks within buildings using VLANs. Now departments can construct private networks across campus using combinations of VLANs and VRFs.
- A Virtual Network is the set of all VLANs, Subnets, and VRFs belonging to a particular faculty or department, including the Virtual Firewall that ties all of the VRFs together.
- Virtual Networks are named after organizational units (e.g., ARTS01 or MATH01 or CPSC01).



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

27

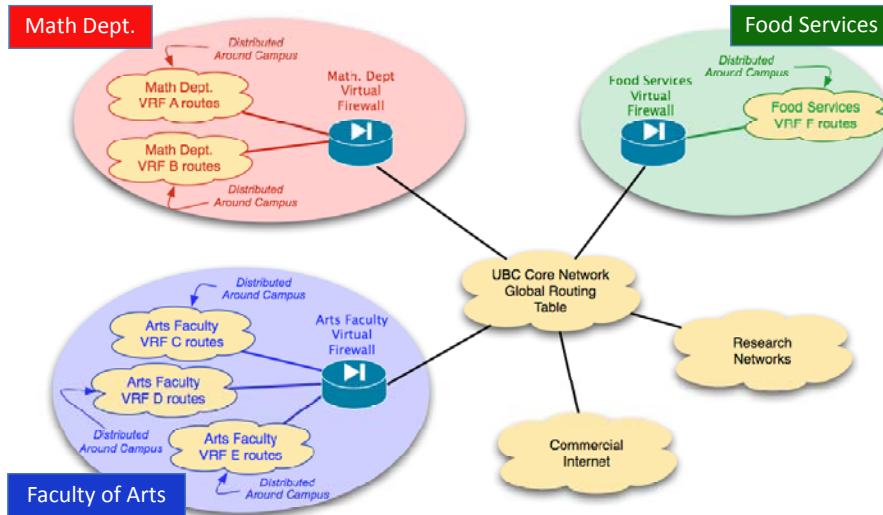


a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

28

Traffic Flow Between Departmental Virtual Networks



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

29

Part 4 Innovations in Service Delivery



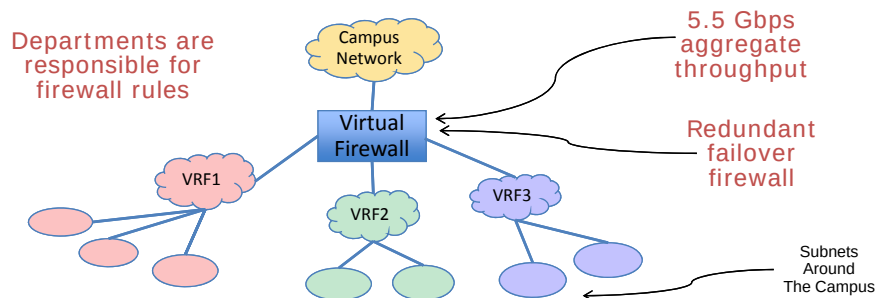
a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

30

Innovations – A Single Central Firewall

- Departments can have offices in any buildings campus-wide, and can have a single firewall controlling access.
- Departments can centralize security policies.
- For the first time, network security is an integral part of network provisioning.



a place of mind

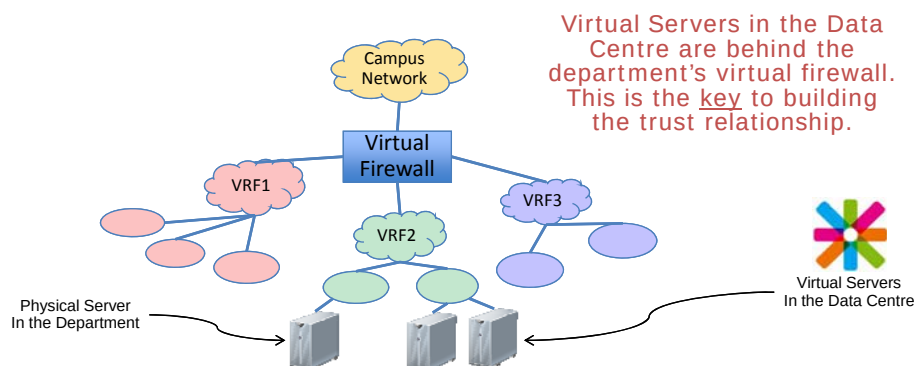
THE UNIVERSITY OF BRITISH COLUMBIA

31

Innovations – Virtual Servers



- Access VMware-based Virtual Servers across the core at gigabit speeds in a completely secure way without requiring a firewall in the path.
- Red Hat Linux, Windows Server, or Solaris.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

32

Innovations – Virtual Storage

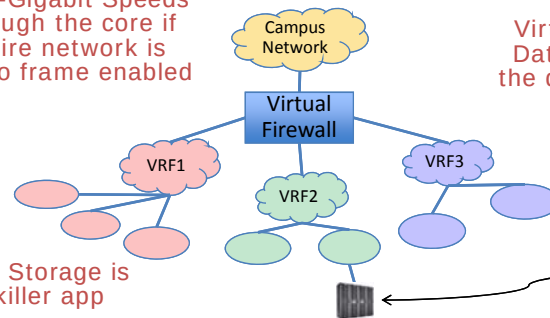


- Access SAN-based Virtual Storage using NFS, CIFS, or iSCSI) across the core at multi-gigabit speeds in a completely secure way without requiring a firewall in the path.

Multi-Gigabit Speeds through the core if entire network is jumbo frame enabled

Virtual Storage in the Data Centre is behind the department's virtual firewall !!!

Virtual Storage is the killer app



Virtual Storage
In the Data Centre
(automatically backed up off site)



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

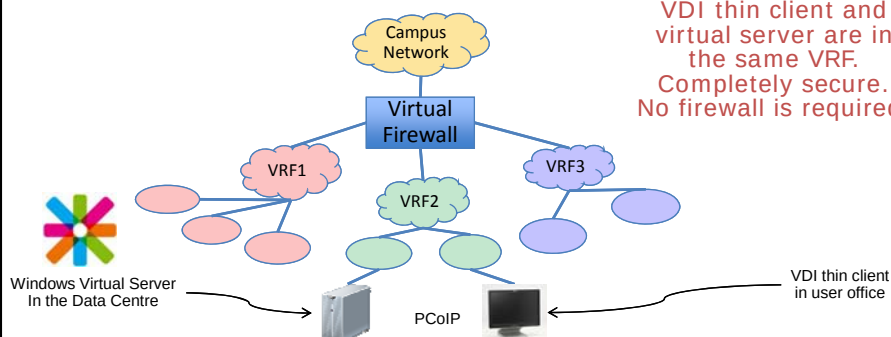
33

Innovations – Virtual Desktop



- Access a virtual desktop in the data centre from your thin PCoIP client in a completely secure way without requiring a firewall in the path.
- This is enterprise class virtual desktop.

VDI thin client and virtual server are in the same VRF. Completely secure. No firewall is required.



Windows Virtual Server
In the Data Centre

PCoIP

VDI thin client
in user office

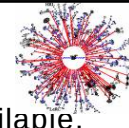


a place of mind

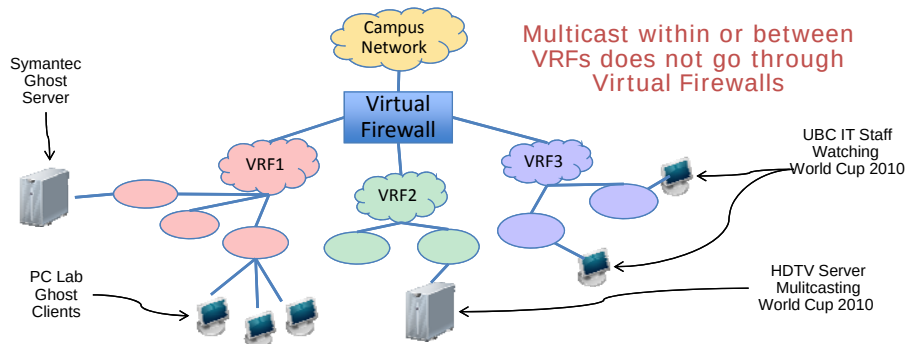
THE UNIVERSITY OF BRITISH COLUMBIA

34

Innovations – Campus-Wide Multicast



- For the first time campus-wide multicast is available, but only in the context of Virtual Networks.
- Image PCs (mVPN). Originate or receive HDTV broadcasts (extranet mVPN). Receive multicast broadcasts from external research network sites.



a place of mind

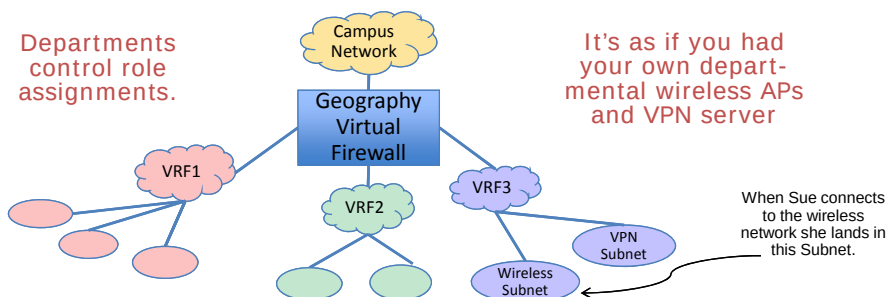
THE UNIVERSITY OF BRITISH COLUMBIA

35

Innovations – Identity-Based Wireless and VPN



- Login to the wireless service or SSL VPN service and be placed in a Subnet in a VRF behind your department's firewall.
- Based on role. For example, enter credentials "[sue.geog](#)" to get connected to a Subnet in a VRF in the Geography department virtual network.



a place of mind

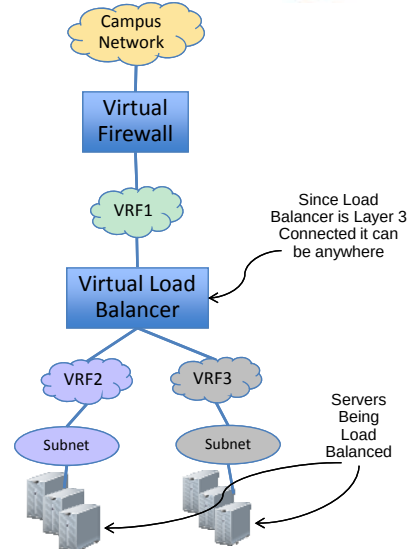
THE UNIVERSITY OF BRITISH COLUMBIA

36

Innovations – Layer 3 Virtual Load Balancers



- Like virtual firewalls, departments can have virtual load balancers.
- Based on Cisco ACE modules in the Catalyst 6500's.
- Suitable for high demand applications like library, student systems, financial systems, email, online course management, etc.
- Virtual load balancer is on the department's virtual network, behind the department's virtual firewall.
- Departments are responsible for load balancer rules.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

37

Innovations – Summary



A new layer of security, integral to network provisioning.
A single high performance virtual firewall controlling campus-wide access.
Departments can centralize security policies.

Access to the virtual data centre is wire speed and completely secure without requiring a firewall in the path.



Virtual Devices and Storage
Virtual Desktops
Campus-Wide Multicast
Identity-Based VPN
Identity-Based Wireless
Virtual Load Balancers



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

38

Part 5

Status to Date



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

39

Status to Date

Production Project began January 1, 2009

- Proof of Concept completed fall 2008
- Virtual networks have been created for 60 departments, each with it's own virtual firewall context.↑
- A total allocated 375 VRFs.←

Average 6 VRFs
Per Department

Uptake and buy in from the faculties
and departments has been overwhelming.

Project to complete in 2011

- Virtualization will be extended to all UBC campuses.
- Expect to max out at 600 VRFs with each router having no more than 250 VRFs.

Network tools upgraded to support Virtual Networks

- Router configurations are automated.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

40

Part 6

Business Results



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

41

Business Results

1. A more secure and higher performance network. Simplified design, deployment, and troubleshooting
2. New services are possible such as virtual storage and campus-wide HDTV broadcasts. Access is wire speed and secure without the need for a firewall in the path.
3. Responsiveness to service requests has improved dramatically because of virtualization. Service requests that took months, now take days or hours.
4. More flexible use of space. Departments can easily re-assign labs and offices, and even change buildings.
5. Simplified disaster recovery. Centralized VMs and virtual storage are automatically backed up.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

42

Business Results

6. Cost and energy savings. The university is positioned to reap the benefits of economies of scale. To date 150 departmental firewalls have been decommissioned. Hardware savings of \$2.75M on centrally provisioned VMs.
7. The trust between departments and the central IT department has strengthened. Departments are willing and eager to use centrally provisioned services.
8. Empowerment of the UBC educational system.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

43

Part 7 Business Case



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

44

Business Case

Network Upgrades and Virtualization

In 2008 our core network consisted of half old Nortel Passport routers, and half Cisco Catalyst 6500 routers. The old routers were failing frequently, and the core network 1Gbps links were nearing saturation. We had no choice but to upgrade to a 10Gbps core, and we decided to go all Cisco.

When we started the 10Gbps core network upgrade in early 2008, the virtualization project was not on the horizon.

With our existing Cisco infrastructure, the overlay of network virtualization did not cost us anything. It is just a different way of configuring the same equipment.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

45

Business Case

Data Centre Virtualization

We initiated the project to virtualize the network in 2008. At the same time a project was initiated to virtualize servers and storage in the data centre. We didn't recognize initially that there were tremendous synergies between the network virtualization projects and data centre virtualization projects.

The business case for data centre virtualization hinged around reducing data centre space, reducing server and disk storage procurement costs, reducing energy costs, and simplifying disaster recovery.

The goal is to provide 80% of the server and storage requirements on campus through the virtualized data centre.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

46

Part 8

Technical FAQs



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

47

Network Virtualization – FAQs

Is Virtual Networking mandatory?

No, it's not mandatory. In fact, it's completely optional. If a department doesn't want to take advantage of virtual networking then they don't have to. It will be business as usual. All of their subnets will continue to be in the global routing table.

If a department decides to use Virtual Networking, does it impact their existing VLANs and Subnets?

The only impact is that the department has to let the UBC IT know what VRF each subnet should be assigned to. Other than that, it's business as usual. No VLANs or IP addresses change.

How many VRFs can a department have?

A department can have as many VRFs as they want. One for every subnet if necessary. Although in practice most departments will only need a small number (~6) to implement their security policies.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

48

Network Virtualization – FAQs

Where is the virtual firewall located?

All eight outer core 6509 routers contain Firewall Service Modules (FWSM) modules. The virtual firewall could be located in any pair of these. However, in practice the virtual firewall will be located in the pair of 6509 routers providing service to the main building for the faculty or department.

If the department doesn't want to use a virtual firewall, can they use their own firewall?

Yes, but we strongly advise using virtual firewalls. Virtual firewalls are very high performance. All current Virtual Networks use virtual firewalls. Virtual firewalls are free to all UBC faculties and departments.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

49

Network Virtualization – FAQs

What technology are VRFs based upon?

VRFs are an industry standard technology supported by many vendors including Cisco Systems. The underlying technology leverages MPLS and BGP protocols. The defining document is RFC2547 - BGP/MPLS VPNs.

Does using VRFs impact network performance?

No, it doesn't. The router hardware always goes through the decision making process to decide what routing table to use even if you don't use VRFs.

How many VRFs can a Cisco router support?

Up to 512 VRFs per router without any performance hit. Up to 1024 with a minor performance hit.

Is all traffic MPLS encapsulated?

No. Only traffic in VRFs is MPLS-encapsulated. Traffic in the global routing table is not MPLS-encapsulated. So you can implement BGP MPLS as an overlay on the existing campus network.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

50

Network Virtualization – FAQs

Is implementing BGP MPLS easy?

- Yes, surprisingly easy. Really the only difference is that you use BGP rather than OSPF as the IGP. It's no more complicated than implementing a traditional OSPF-based core network.

Do VRFs complicate network troubleshooting?

- No. Surprisingly VRFs simplify network troubleshooting since the number of routes in a VRF is very small.

What Cisco documents describe how to do this?

The key documents are:

- “Network Virtualization – Path Isolation Design Guide”
- “Enterprise Network Virtualization – Path Isolation System Assurance Guide”



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

51

Network Virtualization – FAQs

Are there any special hardware or software requirements?

- Yes.
- Cisco 6500 routers must be up to Supervisor 720 Policy Feature Card PFC3B or PFC3C.
- Advanced IP Services image to get the BGP and MPLS support.
- Depending on the size of your core, a pair of BGP Route Reflectors may be necessary. Any low end Cisco router will do.

Is supporting MPLS difficult?

No, for campus networks supporting MPLS is trivial. It's essentially a one time configuration effort. Just a few statements of IOS commands per router.



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

52

That's All

Questions, Discussion



a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA

53