University of British Columbia

- **UBCNET Network Overview (15 min.)**
  - Network Architecture, 10GIG Core Upgrade, Internet Edge
- **Network Virtualization (45 min.)**
  - New Concepts, New Functionality, Discussion

April, 2009

Dennis O'Reilly
UBC IT – Network Architect
University of BC

Part 1

- **UBCNET Network Overview**
  - **Network Architecture, 10GIG Core Upgrade, Internet Edge**

Typical Large Building

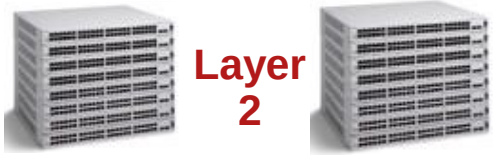
Campus Deployment –

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

UBC Life Sciences Centre

Typical Large Building

Cisco and Nortel Switch Stacks in Comm Rooms



Layer 2

Access Layer

NORTEL

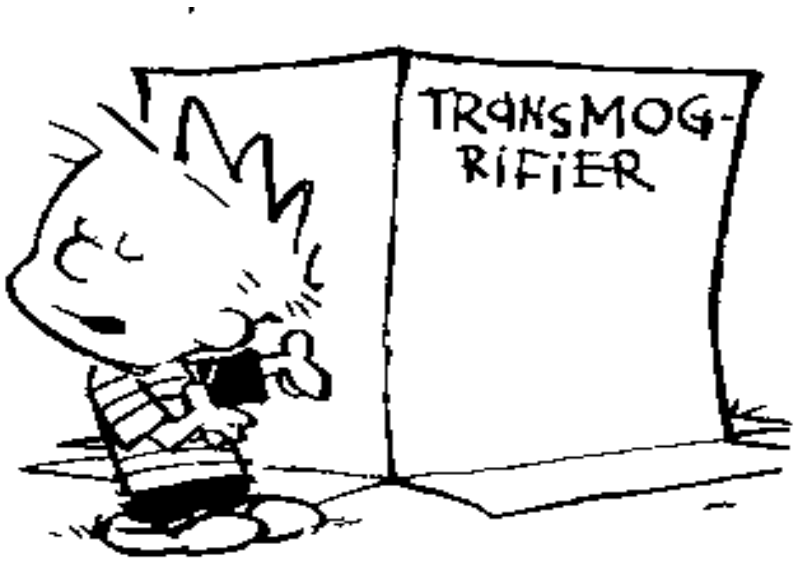
CISCO

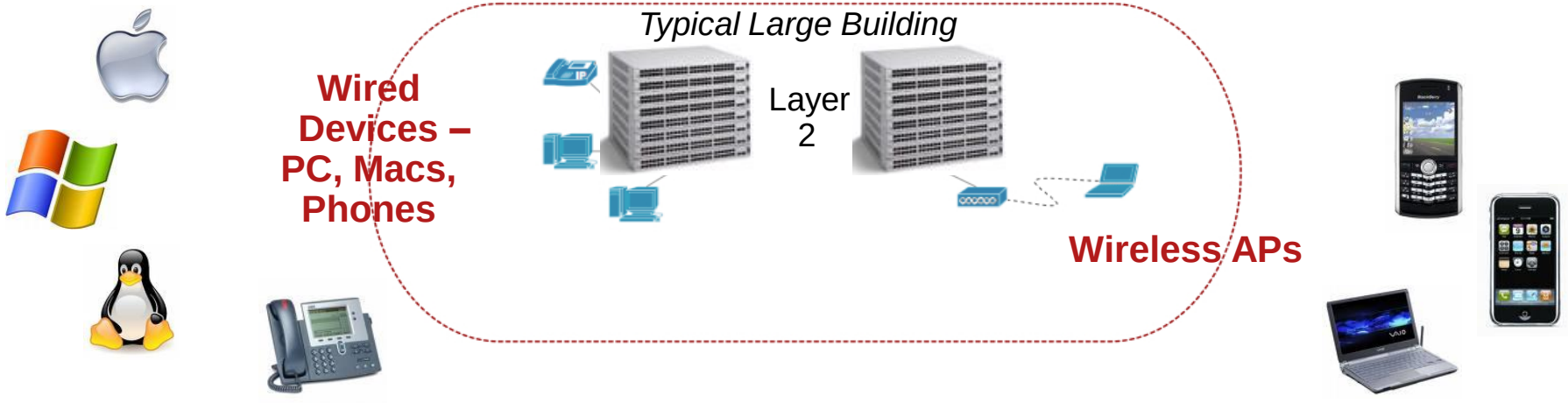
Building Access Layer –

- A typical building will use 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.
- VLAN assignment is controlled through the Transmogrifier.
- VLANs are not bridged between buildings.

UBC Has 2,709 Ethernet Switches Installed

And over 2,500 VLANs !!

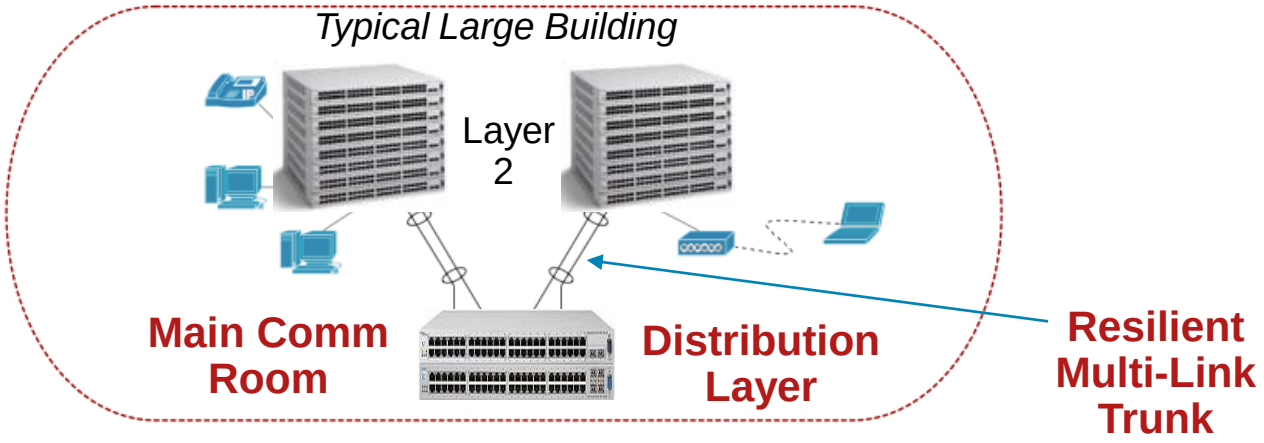




Users … Wired and Wireless –

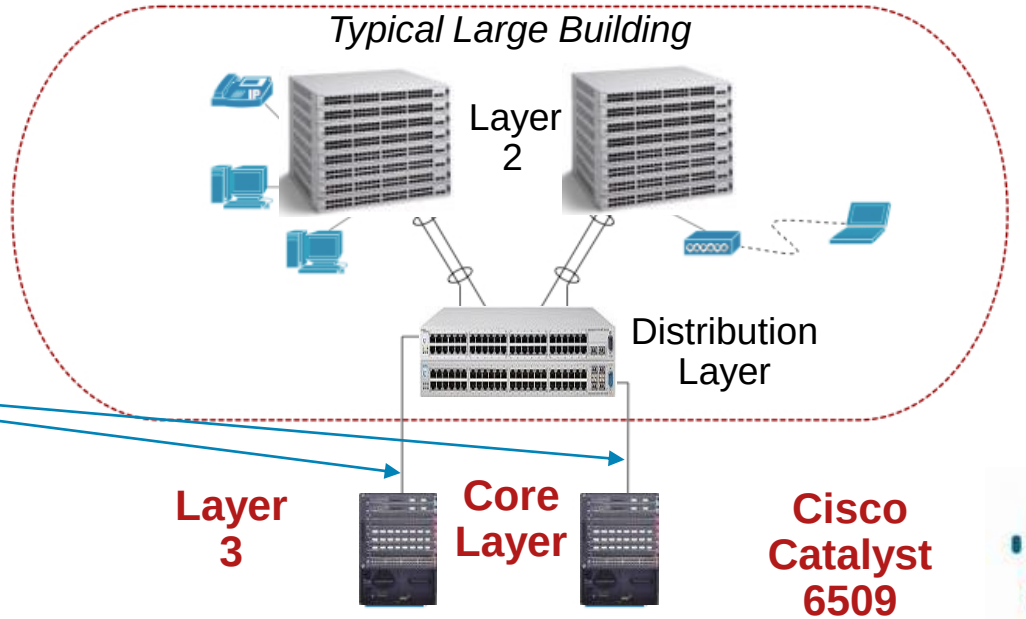
- UBC users utilize many diverse devices and operating systems.
- All new access switches are 10/100/1000 and POE..
- UBC deploys close to 2,000 APs, providing wireless coverage within all buildings on campus.
- An outdoor wireless mesh deployment is underway.

UBC Has Almost 2,000 Cisco Wireless Access Points Installed



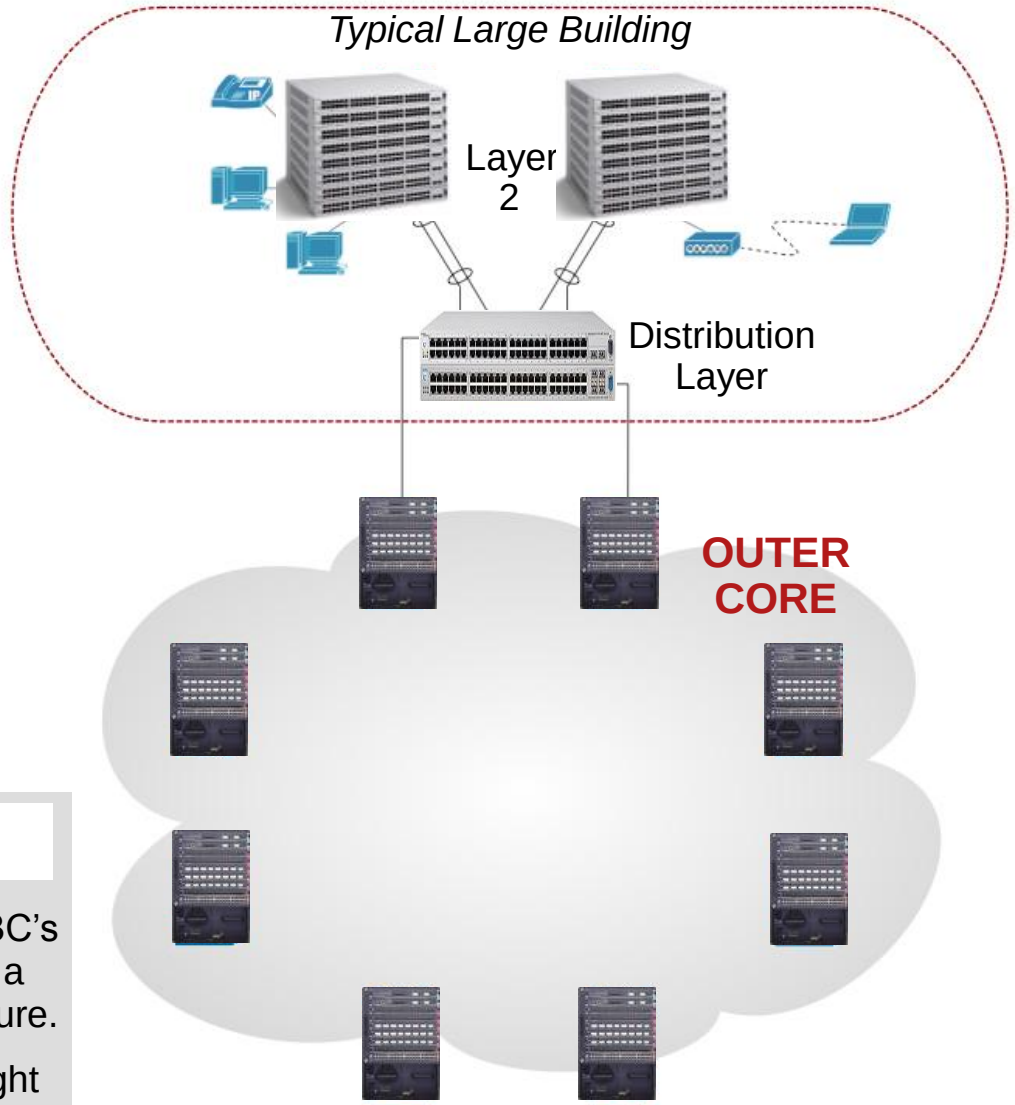
Building Distribution Layer –

- 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.



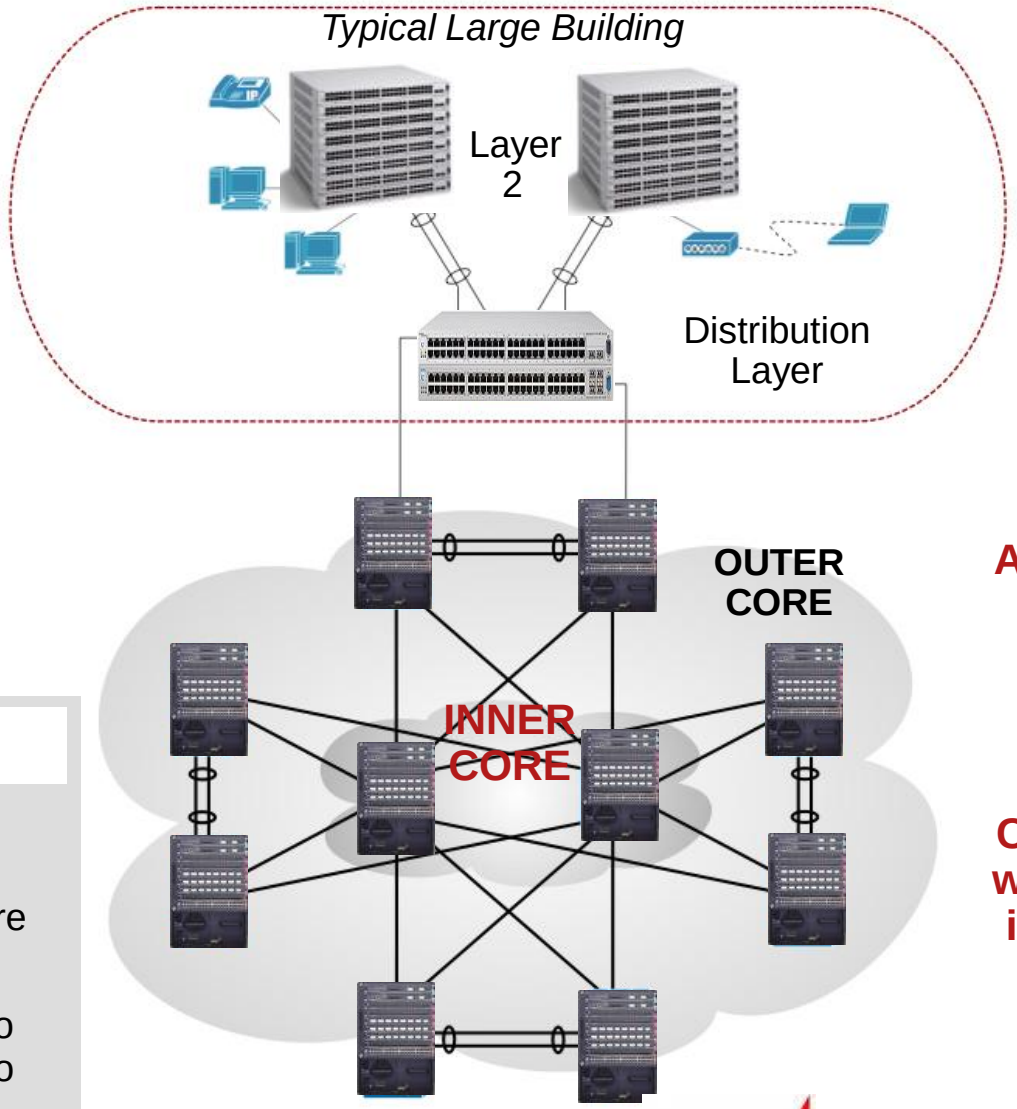
Core Layer –

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



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).
- UBC recently completed an upgrade of all core links to 10GE.



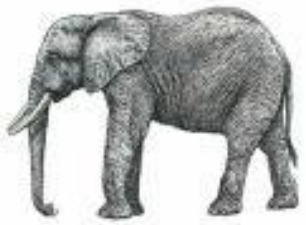
Inner Core Layer –

- 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) – no campus-wide VLANs
- OSPF convergence is sub second.

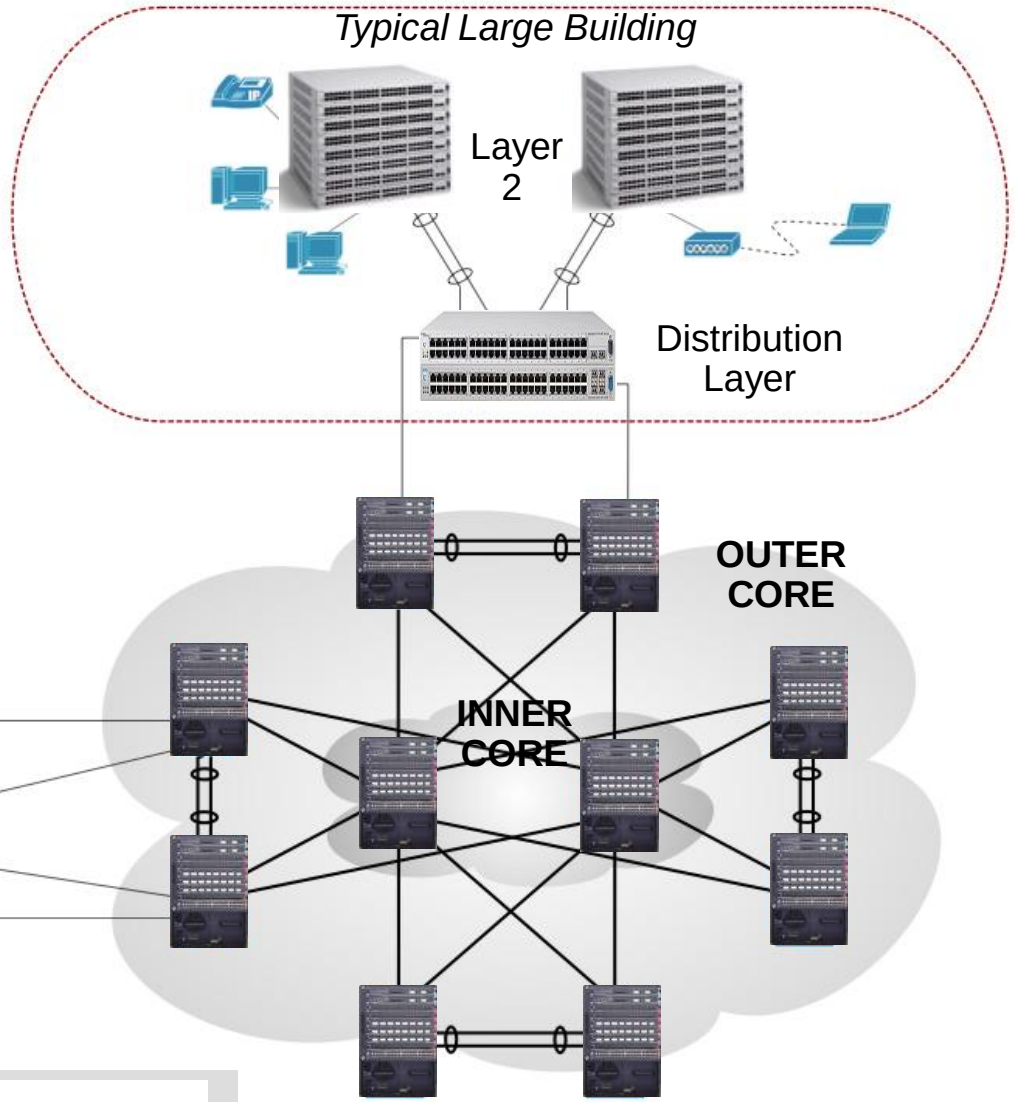
All Interfaces in the Core are 10GIGABIT

Core Network was upgraded in the last 12 months

100% Routed

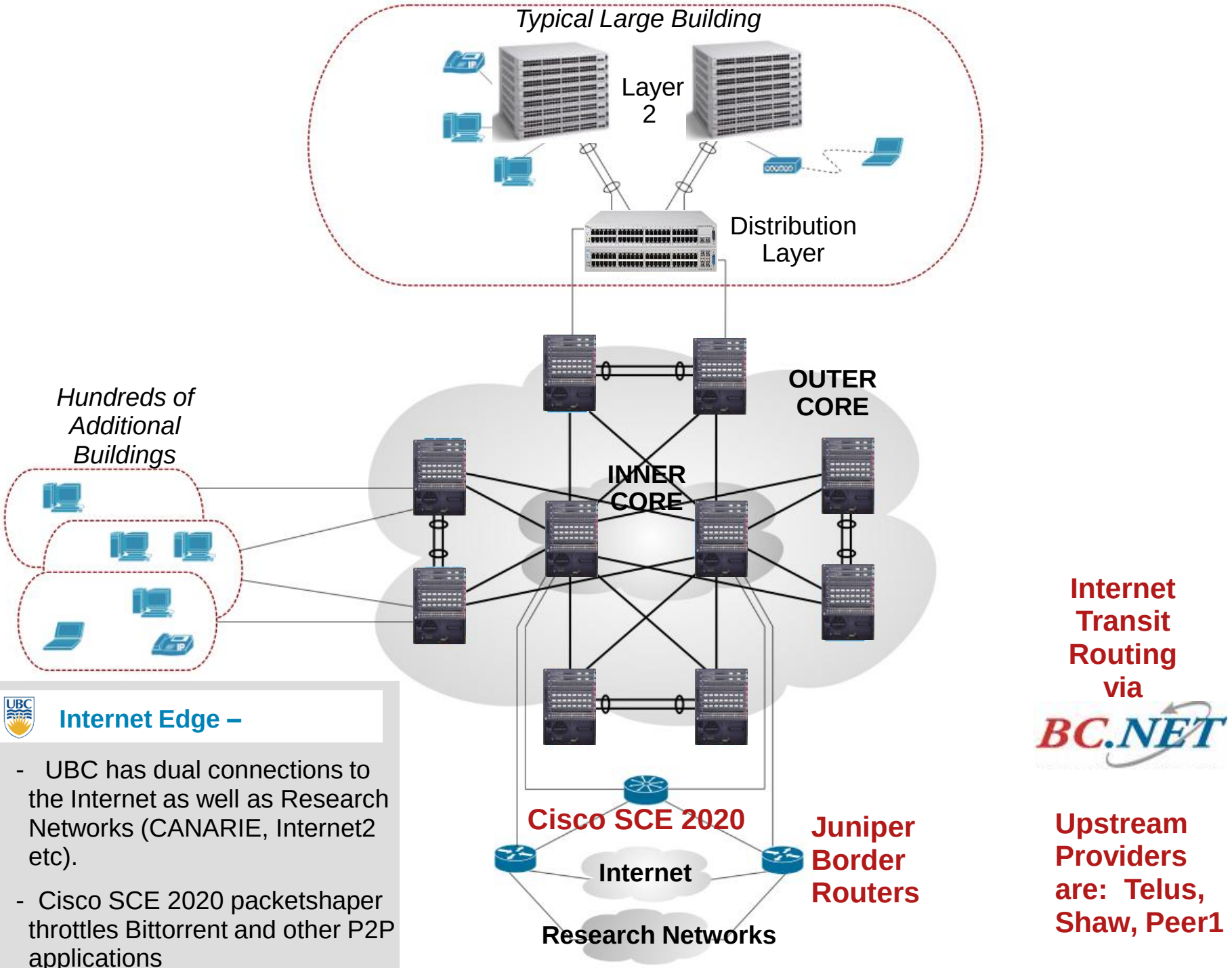


Jumbo Frame Enabled



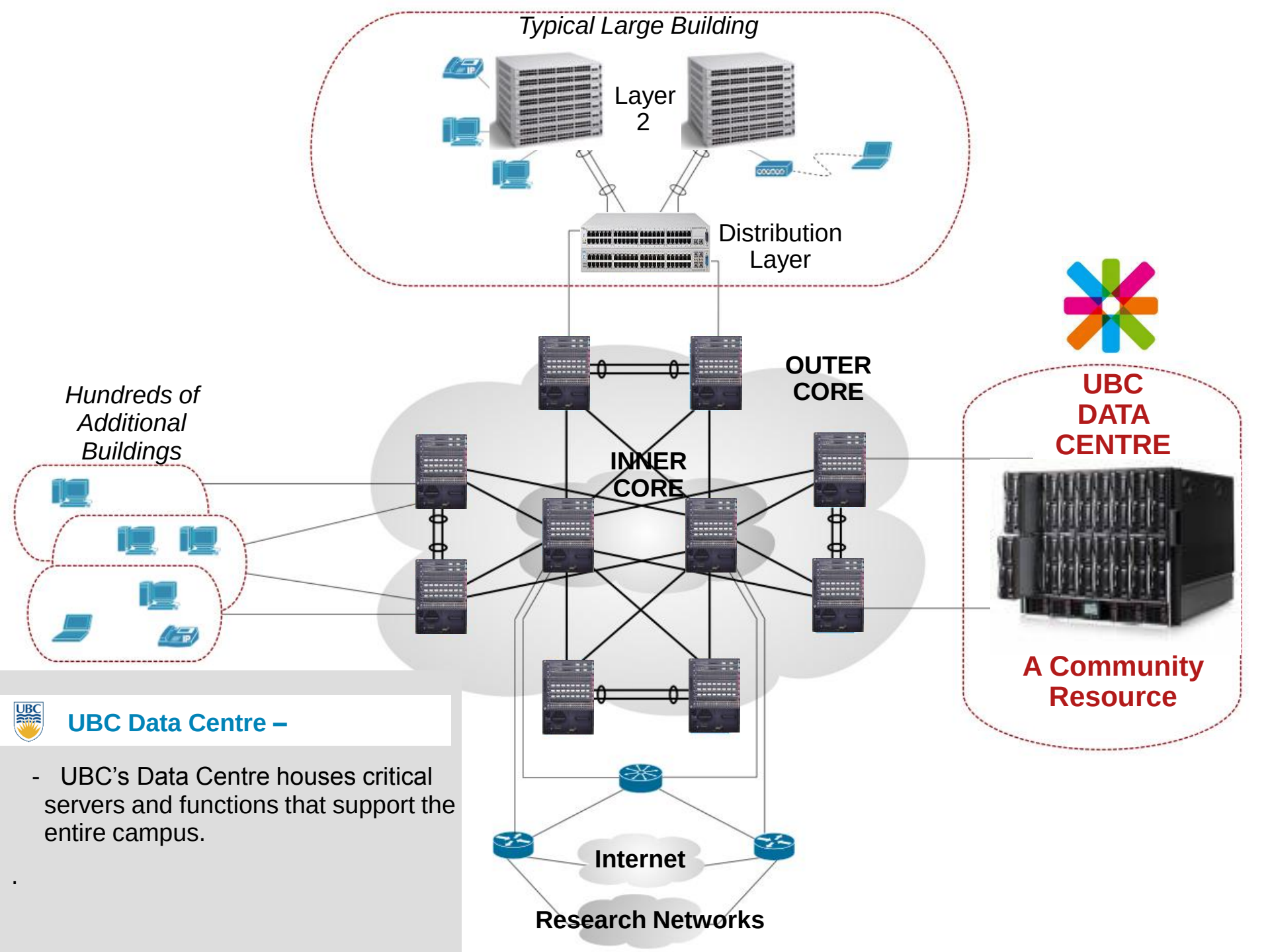
Buildings Across UBC –

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



Internet Edge –

- UBC has dual connections to the Internet as well as Research Networks (CANARIE, Internet2 etc).
- Cisco SCE 2020 packetshaper throttles Bittorrent and other P2P applications



UBC Data Centre –

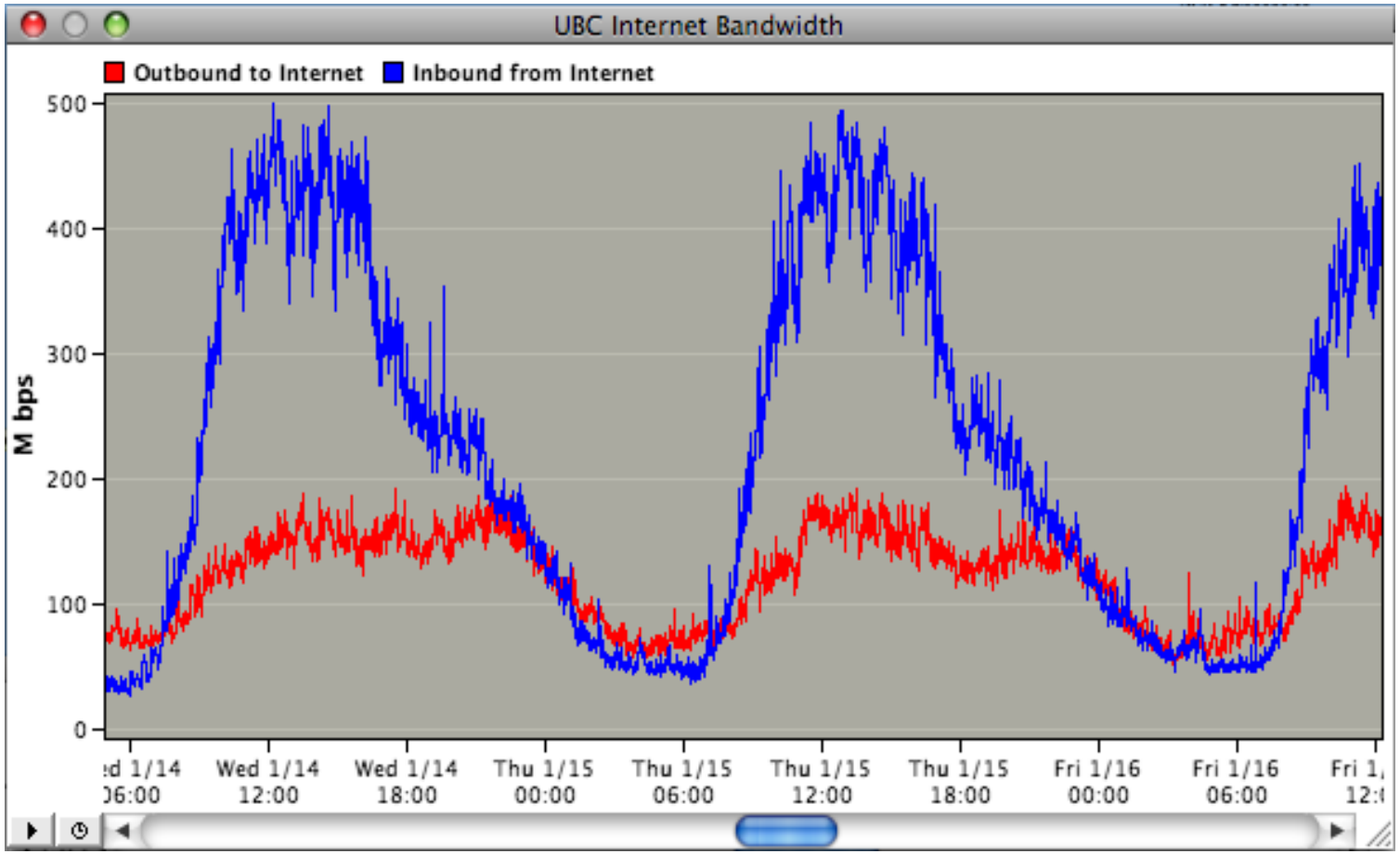
- UBC's Data Centre houses critical servers and functions that support the entire campus.

.

Interesting UBCNET Metrics

- Number of VLANs Allocated = 2,688
- Number of Subnets Allocated = 2,138
- Total Networks in the Transmogrifier = 479
- Number of Wired Ports Used in the Last Year = 38,287
- Maximum Simultaneously Connected Wireless Users = 10,000+
- Number of Wireless Access Points = ~ 2,000
- Number of Resnet Ports = 8,500
- Internet Bandwidth for Main UBC Network = 500 Mbps
- Internet Bandwidth for ResNet = 750 Mbps

Commodity Internet Typical Day…



Part 2

- **Network Virtualization**
  - **New Concepts, New Functionality, Discussion**

UBC –
Network Virtualization - Concept - VLANs

- **VLANs – Virtualization at Layer 2**

  Network Virtualization isn't new. VLANs are a type of network virtualization. Everyone is familiar with VLANs. We have deployed over 2,500 unique VLANs at UBC.

- **VLANs provide Privacy, Security, Reliability**

  Some buildings have over a 100 VLANs.

  Departments use VLANs to segregate servers, students, faculty & staff, and admin office computers.

  If a large building has multiple departments, each department can have their own VLANs.

  Ports are assigned to VLANs using the Transmogrifier.

UBC –
Network Virtualization - Concept - VLANs

- **VLANs – Virtualization Within Buildings**

  VLANs span buildings or building complexes.

  Any port in a building can be on any VLAN.

- **VLANs - Connecting to the Outside World**

  A VLAN has a Subnet associated with it.

  To connect to the other VLANs/Subnets or to the campus network you must go through a firewall or a router.

  Many departments have implemented departmental firewalls for this purpose.

  Commonly used firewalls are Cisco PIX, Sonicwall, Linux netfilter/iptables.

UBC –
Network Virtualization Concept - VLANs

- **VLANs – A Complete Virtualization Solution?**

  NO. The problem is VLANs can not be spanned to other buildings or across campus.

  So departments with offices in multiple buildings have multiple VLANs/Subnets in multiple buildings…

  …and multiple firewalls.

  This introduces complexity, inefficiency, and is the cause of countless network problems.

  What is the point of installing a state-of-the-art gigabit speed network, when departments everywhere are installing low end firewalls?

UBC –
Network Virtualization - Concept - Campus-Wide Virtualization

- **Demand For Campus-Wide Network Virtualization**

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.

- **Campus-Wide Network Virtualization**

  VLANs work by virtualizing the ethernet switches in the buildings, effectively giving each department their own ethernet switches.

- **Question of the day:**

  But how do we extend network virtualization campus-wide ???

UBC –
Network Virtualization - New Concept - VRFs

- **Campus-Wide Network Virtualization**

  To extend network virtualization campus-wide we have virtualized the routers in the core network, effectively giving each department their own private campus-wide network.

- **Introducing "VRFs" (pronounced verfs)**

  Virtual private campus-wide networks are called VRFs (Virtual Router Forwarding instances).

  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.

  Just as VLANs can extend through all switches in a building, so VRFs can extend through all routers campus-wide.

  Just as VLANs are named, so VRFs are named.

  Just as now everyone is comfortable with the term VLAN, so in two years will everyone be comfortable with the term VRF.

UBC –
Network Virtualization - New Concept - VRFs

- **What is a VRF?**

  A VRF is completely private campus-wide network. It is as if you had your own private routers.

  A VRF has a name, like ARTS-SERVERS or MATH-LABS. VRFs are named after UBC organizational units.

  Any Subnets in any buildings 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.

  A department can have as many VRFs as they require to implement their security policies.

  Routing between Subnets within a VRF is direct. No firewall is involved. It is wire speed (1Gbps).

  To connect to a Subnet outside of a VRF you have to go through a firewall. Usually this is a virtual firewall.

  VRFs are visible in the Transmogrifier.

UBC –
Network Virtualization - New Concept - VRFs

- **What a VRF Isn't**

  A VRF is not a campus-wide bridged VLAN.

  A VRF allows different Subnets in different buildings anywhere on the campus to communicate directly, in a completely secure way.

  But there are different Subnets in each building.

UBC –
Network Virtualization - New Concept - 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.

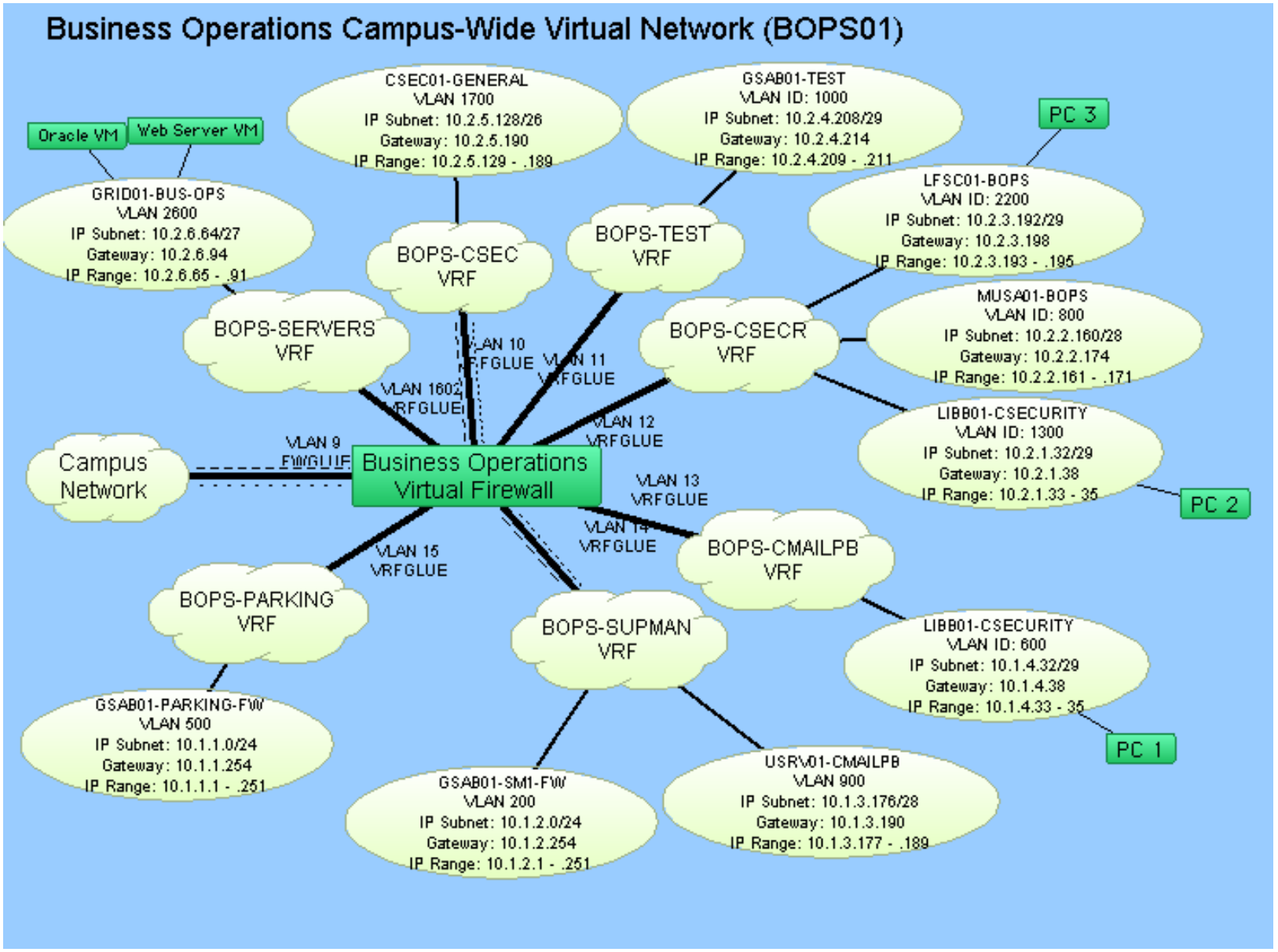
  A Virtual Network is the set of all VLANs, Subnets, and VRFs belonging to a particular faculty or department, including the virtual firewall that ties all of the VRFs together.

  Virtual Networks are named after organizational units (e.g., ARTS01 or ARCH01).

  Virtual Networks are visible in the Transmogrifier.

- **Real Life Example**

  Business Operations Virtual network. A picture is worth 1000 words.


Business Operations Campus-Wide Virtual Network (BOPS01)
CSEC01-GENERAL
VLAN 1700
IP Subnet: 10.2.5.128/26
Gateway: 10.2.5.190
IP Range: 10.2.5.129 - .189
GSAB01-TEST
VLAN ID: 1000
IP Subnet: 10.2.4.208/29
Gateway: 10.2.4.214
IP Range: 10.2.4.209 - .211
PC 3
Oracle VM
Web Server VM
GRID01-BUS-OPS
VLAN 2600
IP Subnet: 10.2.6.64/27
Gateway: 10.2.6.94
IP Range: 10.2.6.65 - .91
BOPS-CSEC
VRF
BOPS-TEST
VRF
LFSC01-BOPS
VLAN ID: 2200
IP Subnet: 10.2.3.192/29
Gateway: 10.2.3.198
IP Range: 10.2.3.193 - .195
BOPS-SERVERS
VRF
BOPS-CSECR
VRF
MUSA01-BOPS
VLAN ID: 800
IP Subnet: 10.2.2.160/28
Gateway: 10.2.2.174
IP Range: 10.2.2.161 - .171
VLAN 10
VRFGLUE
VLAN 11
VRFGLUE
VLAN 1602
VRFGLUE
VLAN 12
VRFGLUE
LIBB01-CSECURITY
VLAN ID: 1300
IP Subnet: 10.2.1.32/29
Gateway: 10.2.1.38
IP Range: 10.2.1.33 - 35
PC 2
VLAN 9
FWGLUE
Campus
Network
Business Operations
Virtual Firewall
VLAN 13
VRFGLUE
VLAN 14
VRFGLUE
BOPS-CMAILPB
VRF
VLAN 15
VRFGLUE
BOPS-PARKING
VRF
BOPS-SUPMAN
VRF
LIBB01-CSECURITY
VLAN ID: 600
IP Subnet: 10.1.4.32/29
Gateway: 10.1.4.38
IP Range: 10.1.4.33 - 35
PC 1
GSAB01-PARKING-FW
VLAN 500
IP Subnet: 10.1.1.0/24
Gateway: 10.1.1.254
IP Range: 10.1.1.1 - .251
GSAB01-SM1-FW
VLAN 200
IP Subnet: 10.1.2.0/24
Gateway: 10.1.2.254
IP Range: 10.1.2.1 - .251
USRV01-CMAILPB
VLAN 900
IP Subnet: 10.1.3.176/28
Gateway: 10.1.3.190
IP Range: 10.1.3.177 - .189

UBC –
Network Virtualization - Advantages

- **Advantages of Virtual Networks**

  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.

- **Virtual Networks are a new layer of security**

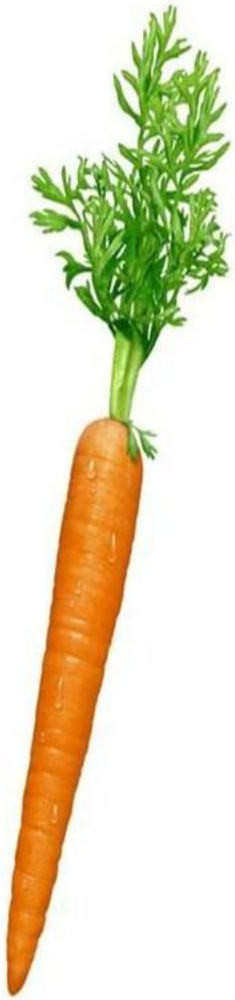
UBC –
Network Virtualization - Advantages

- **Virtual Networking is Completely Optional**

  However, if you want to take advantage of any of the following new features, then you will have to convert to using Virtual Networking.

  Like the Transmogrifier, the idea was to create a service so good that everyone would want to use it.

UBC –
Network Virtualization - New Functionality



Virtual Firewalls

Starting now, the only way to get a virtual firewall context from UBC IT is in conjunction with Virtual Networking.

All 8 UBC Outer Core Cisco 6509 Routers contain Firewall Service Modules.

5 Gigabit per second aggregate throughput.

Redundant failover firewall.

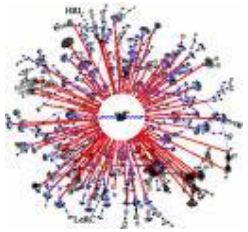
Looks and feels like a real hardware Cisco PIX firewall.

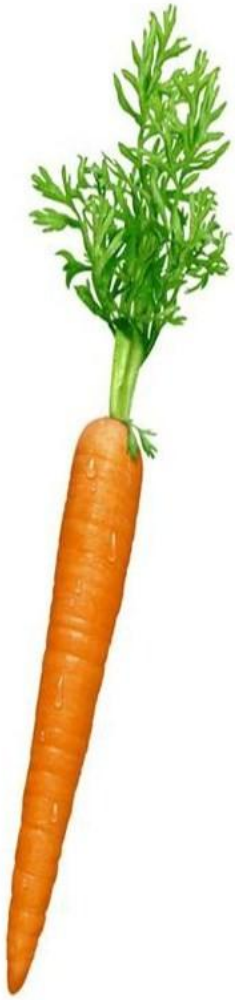
Departments are responsible for firewall rules.

Help from UBC IT in configuring your security policies and troubleshooting your firewall if and when you need it.

Firewall context appears in Transmogrifier.

UBC –
Network Virtualization - New Functionality





Campus-Wide Multicast

For the first time campus-wide multicast is available, but only in the context of Virtual Networks.

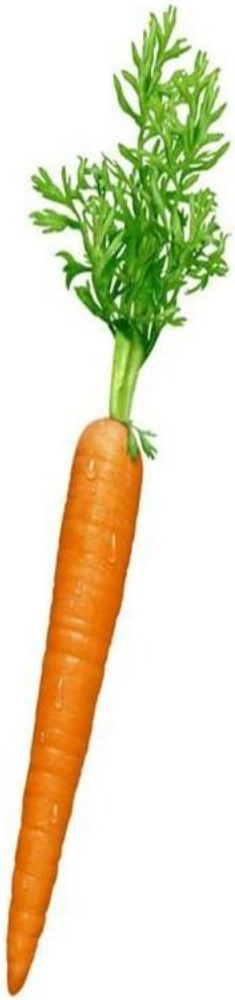
Multicast within all subnets in a VRF.
E.g., Ghostcast computer images campus-wide.

Multicast between VRFs, without going through a firewall.
E.g., Create high definition TV applications and broadcast them campus-wide.

Subscribe to UBC campus-wide multicast channels.

Receive multicast broadcasts from external research network sites.

UBC –
Network Virtualization - New Functionality



Identity-Based Wireless

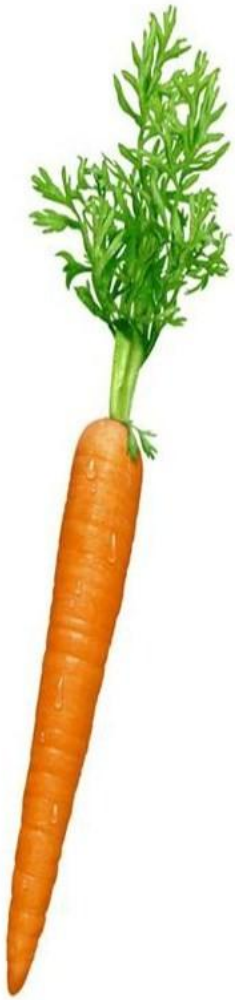
Connect to the UBC wireless network and be placed on a Subnet in a VRF behind your department's firewall.

It's as if you had your own departmental wireless network.

Based on CWL role. For example, enter credentials joseph@math.ubc.ca to get connected to a Subnet in a VRF in the Math network.

Departments are in control of delegation of CWL roles to their faculty, staff, and students.

UBC –
Network Virtualization - New Functionality



Identity-Based VPN

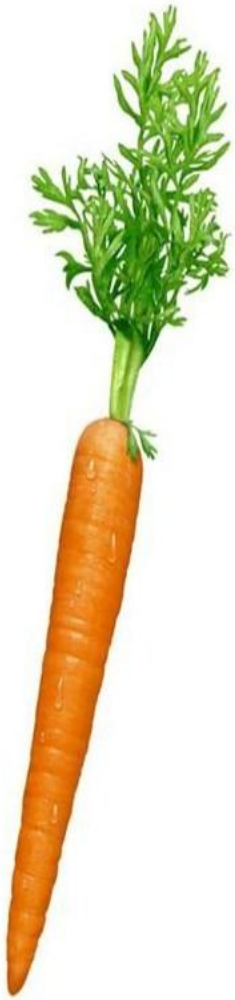
Connect to the new UBC SSL VPN server and be placed on a Subnet in a VRF behind your department's firewall.

It's as if you had your own departmental VPN Server.

Based on CWL role.

Departments are in control of delegation of CWL roles to their faculty, staff, and students.

UBC –
Network Virtualization - New Functionality



Virtual Devices

Subscribe to UBC IT's new VMware-based Virtual Devices service.

Red Hat Linux, Windows Server, or Solaris.

Virtual Devices are on your department's network, behind your departmental firewall, on the VRF of your choice.

Underlying SAN data storage is automatically replicated to multiple sites (for disaster recovery (DR)).

Very fast provisioning. Goal is on demand provisioning through web-page.

Virtual Devices appear in the Transmogrifier in your department's Virtual Network.

UBC –
Network Virtualization – Empowering

- **Empowering Faculties and Departments**

  Just as the Transmogrifier empowered departments, so Virtual Networks empower departments.

  Departments have full configuration authority over virtual firewall configuration.

  Departments have their own virtual wireless network and virtual SSL VPN server.

  Departments control which individuals have which identity-based networking roles.

  Linux, Windows, Solaris virtual devices provisioned on the department's virtual network behind the department's virtual firewall.

  UBC IT is in the background providing expert assistance if and when you need it.

  Virtual networks, VRFs, virtual firewalls, virtual devices are all visible in the Transmogrifier.

UBC –
Network Virtualization FAQs

- **Is Virtual Networking mandatory?**

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

- **If I decide to use Virtual Networking, does it impact my existing VLANs and Subnets?**

  The only impact is that you have to let the NMC know what VRF each subnet should be assigned to. Other than that, it's business as usual. No VLANs or IP addresses change. The Transmogrifier works as normal.

- **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.

UBC –
Network Virtualization FAQs

- **When is Virtual Networking available?**

  It's available now. Campus-wide for the Point Grey campus. Multicast and Virtual Devices are available now. Identity-based wireless and VPN will be available in 2Q09.

- **Is Virtual Networking available to UBC Okanagan and beyond?**

  Virtual networking will be extended to UBC Okanagan and the UBC Teaching Hospitals by March 2010.

- **How much does it cost?**

  Since it's just simple routing changes, it's free. Except for the virtual firewall.

- **How do I sign up?**

  Contact the UBC Network Management Centre.
  Email nmc@ubc.ca

UBC –
Network Virtualization FAQs

- **Is it difficult to convert to Virtual Networking?**

  Like any complex network conversion, it's complicated, especially if there is an existing firewall involved. The NMC will work with you to prepare a plan to transition your department's VLANs and Subnets to a Virtual Network.

  If you aren't familiar with Cisco firewalls then the NMC will create a test Virtual Network for you, including a virtual firewall and test VRFs, VLANs, and subnets so that you can get familiar with the technology. Then once you are comfortable with the technology you can work with the NMC to transition your VLANs and subnets.

  Most of the work for the department involves defining a centralized security policy and defining firewall rules that implement that security policy.

  A conversion can take anywhere from 1 month to 3 months.

- **Is troubleshooting Virtual Networks more difficult?**

  No, it's exactly the same as troubleshooting any network that contains a firewall. Common tools like ping and traceroute work as normal within the subnets in a VRF.

UBC –
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.

- **Where is my virtual firewall located?**

  All eight outer core 6509 routers contain firewall modules. Your virtual firewall could be located in any pair of these. However, in practice your virtual firewall will be located in the pair of 6509 routers providing service to the main building for your faculty or department.

- **If I don't want to use a virtual firewall, can I use my own firewall?**

  Yes you can, but we strongly advise using virtual firewalls. Virtual firewalls are very high performance.

UBC –
Network Virtualization - Summary

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 it all together.

Highlights

A new layer of security, integral to network provisioning.

A single high performance virtual firewall controlling campus-wide access.

Departments can centralize security policies.

Visible in the Transmogrifier.

New Functionality

Campus-Wide Multicast

Identity-Based Wireless

Identity-Based VPN

Virtual Devices

Virtual Desktops

Virtual Load Balancers

That's All.

- **Questions,** Discussion