McGill

Network and Information Security Upgrade

Information Session for Lan Administrators

Info Session #1
October 20, 2017
09:30am to 11:00 am
Burnside Hall, Room 201

Info Session #2
October 24, 2017
09:30am to 11:00 am
Burnside Hall, Room 201

Info Session #3
November 3, 2017
09:30am to 11:00 am
Burnside Hall, Room 201

McGill | Information Technology Services

Connect. Learn. Innovate.

Objective for today

Introduce you to…

- The Network Upgrade & Information Security project
  - Upcoming changes
  - High Level Timeline

Allow the project team to…

- Explain how we can work together by:
  - Providing overview of next steps
  - Reviewing areas of support

Logistic Information

We have the time we need!

- **Presentation of 1 hour & then 30 mins for questions…**
- **Room is available after 90 mins**

Please ask your questions anytime throughout the presentation

Don't forget to fill in the attendance sheet

The presentation will be available on our new project website!

Bathroom location & keys

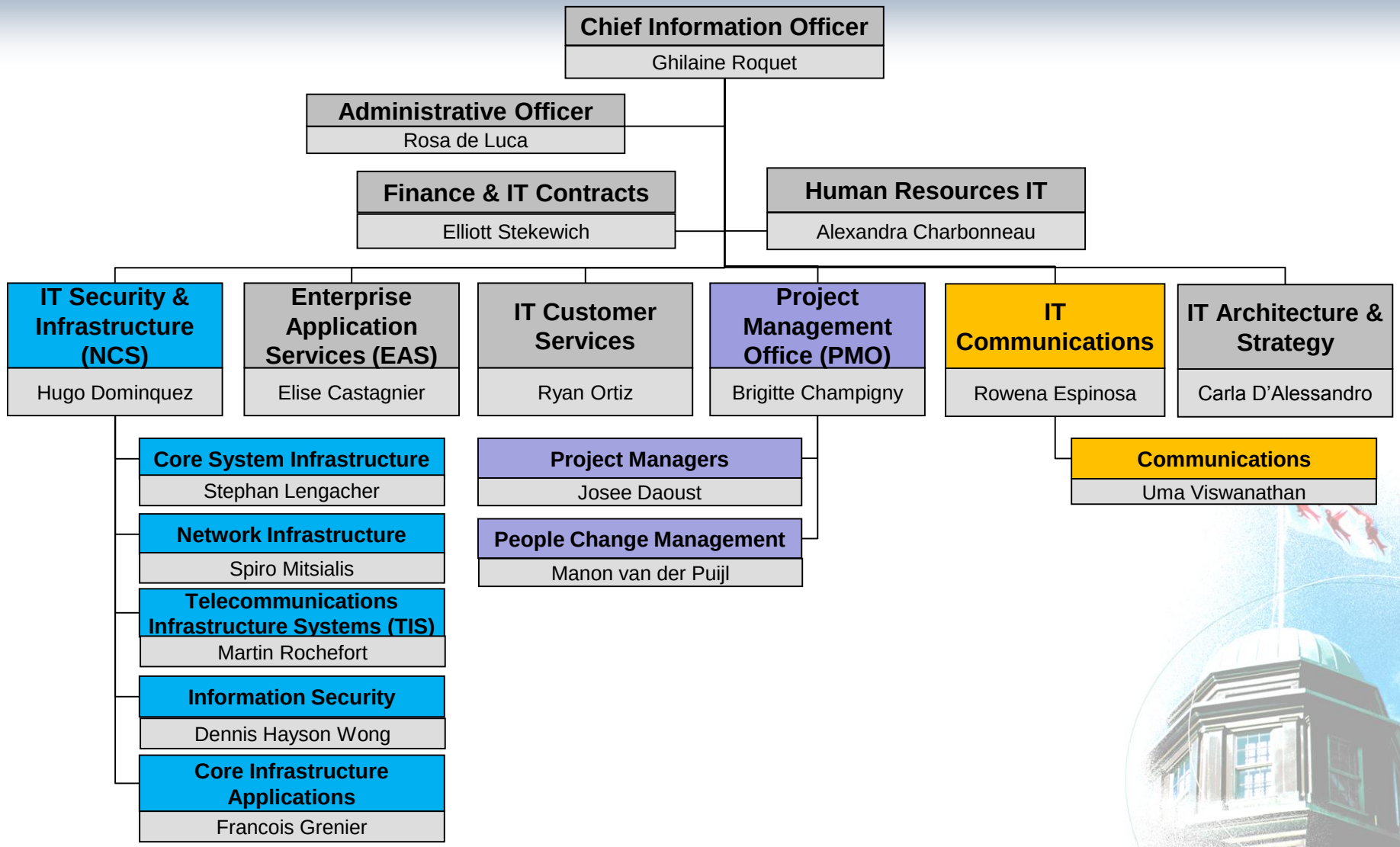
Agenda

Introduction	
• Project team	Josee Daoust
• Round Table introduction	All
Project Context	Spiro Mitsialis
Achievements & Timeline	Josee Daoust
Technical Overview of upcoming changes	
• Network Upgrade	Spiro Mitsialis
• Information Security Upgrade	Dennis Hayson Wong
Wired & Wireless - Key Steps	Josee Daoust
Support areas	Uma Viswanathan
Wrap Up	Josee Daoust

Network & Information Security Upgrade

WHO WE ARE…

The IT Services (ITS) Organization



The Project Team

NCS

Network Infrastructure

Telco Deployment Leads
- Paolo Maddalena
- Mary Paseli

Wireless Deployment Lead
- Norman Chu

NetInf Manager
- Spiro Mitsialis

Telecommunications Infrastructure Systems

Physical Infra Deployment Lead
- Maxime Marcil

Fiber Deployment
- Christian Charland

TIS Manager
- Martin Rochefort

Information Security

Architect
- Pascal Bourbonnais

Analyst
- Luis Latorre

InfoSec Manager
- Dennis Hayson Wong

PMO

Project Manager
- Josee Daoust

Change Management & Communications

Communications Lead
- Uma Viswanathan

Change Management Advisor
- Manon van der Puijl

>10 IT Project Members supporting all initiatives in scope!

Network & Information Security Upgrade

PROJECT CONTEXT

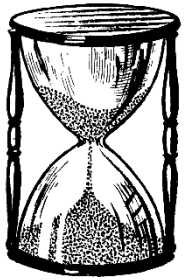
Why does the network need an upgrade?

Network equipment out of date

Vulnerability to IT security threats

Network equipment no longer supported

Wireless network too slow and inadequate coverage



No longer possible to sustain McGill's growth

Laying foundation for new communication features

Project Scope

Many different elements are part of the project scope:

Network Upgrade:

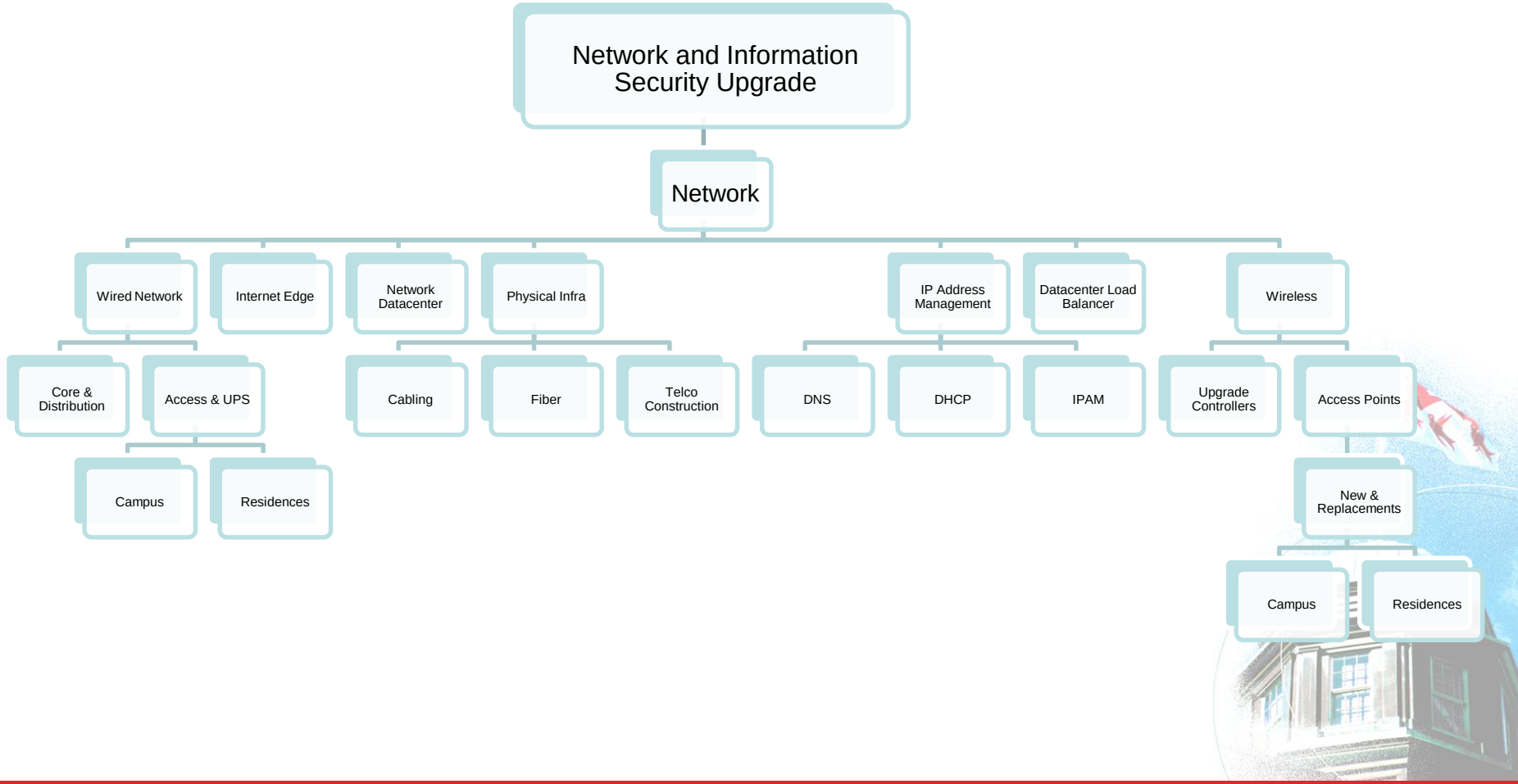
- Wired Network
- Wireless Network
- Internet edge
- Network Datacenter
- Physical Infrastructure (cabling, fiber)
- IP Address Management, DNS, DHCP (DDI)
- Datacenter Load Balancer Evergreening

Information Security:

- Security information and event management (SIEM)
- Next Generation FW (NGFW) & Intrusion Prevention System (IPS)
- Wired Authentication & Network Admission Control (NAC)
- Cisco AMP for End Points

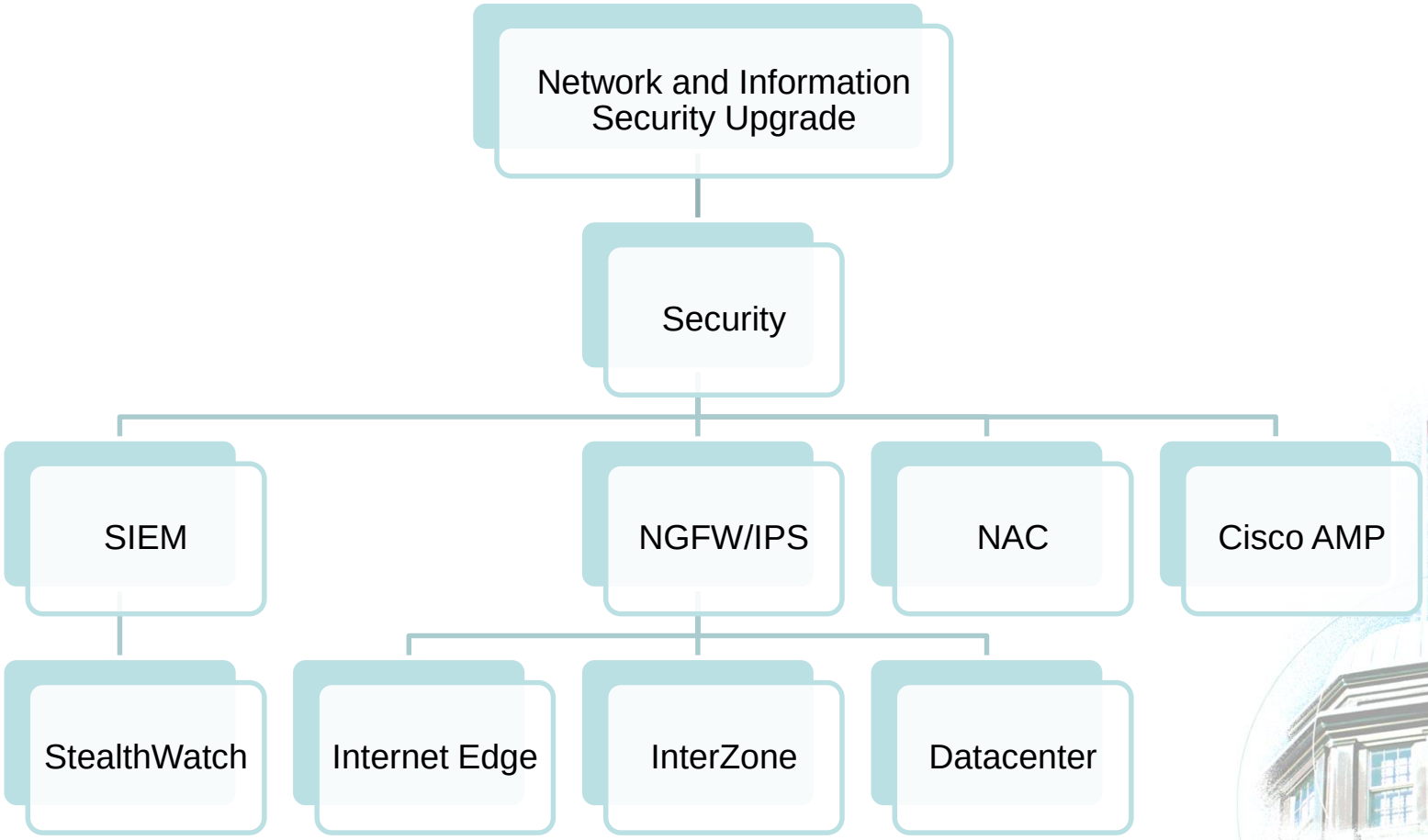
Project Scope - details

More detailed view of the project scope:



Project Scope - details

More detailed view of the project scope:



What are we improving?

- Upgrade structured cabling to structured cabling Gigabit capable
- Increase capacity (bandwidth and number concurrent of users)
- Increase resiliency and availability
- Control/optimize operational costs (within and outside of IT)
- Improve security configuration of the network
- Replace security vulnerable equipment
- Facilitate mobility of users & create Unified Network Experience: Wired/Wireless/VPN
- Build network to scale easily for fast-growing demand in research
- Support for upcoming initiatives including Unified Communications (VoIP)

Network & Information Security Upgrade

ACHIEVEMENTS & TIMELINE

Achievements so far

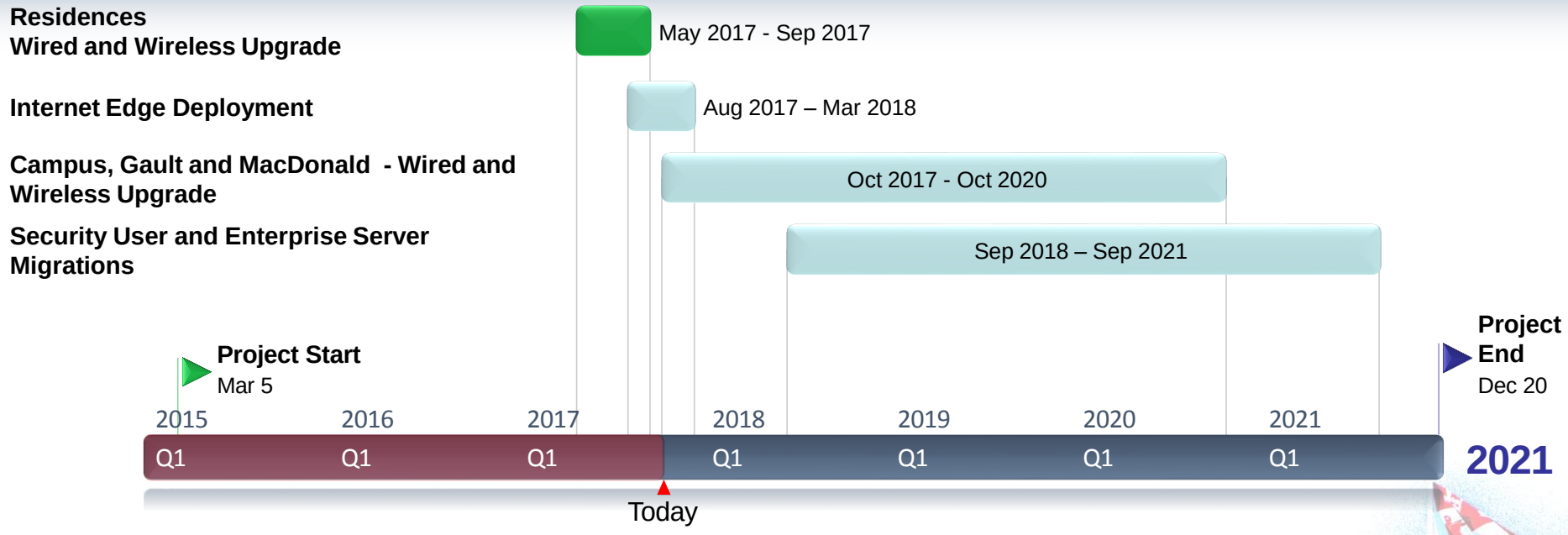
**CFT: Call for Tender = RFP*

Project Launch ($)	**March 2015**
Awarded CFT* DDI (IPAM/DHCP/DNS)	**November 2015**
Implemented DDI (IPAM/DHCP/DNS)	April 2016
Completed HL Architecture for Network	April 2016
Awarded SIEM CFT *	**August 2016**
Telecom Rooms (14) Construction completed	September 2016
Datacenter F5 Load Balancer refresh	September 2016
Awarded Network Upgrade CFT*	**March 2017**
Awarded UPS CFT*	**March 2017**
Awarded Wireless CFT*	**March 2017**
Awarded IPS/FW CFT*	**August 2017**
Residences Wired and Wireless Upgrade	September 2017
Awarded Fiber CFT*	**October 2017**
Designed LL architecture for Network & Security	October 2017

PLEASE NOTE!

7 Call for Tenders/RFPs, very time consuming!

High-level Timeline



PLEASE NOTE!

This is just the high level schedule for largest subprojects, much more work ongoing and involved…

Short-term Upgrade Activities

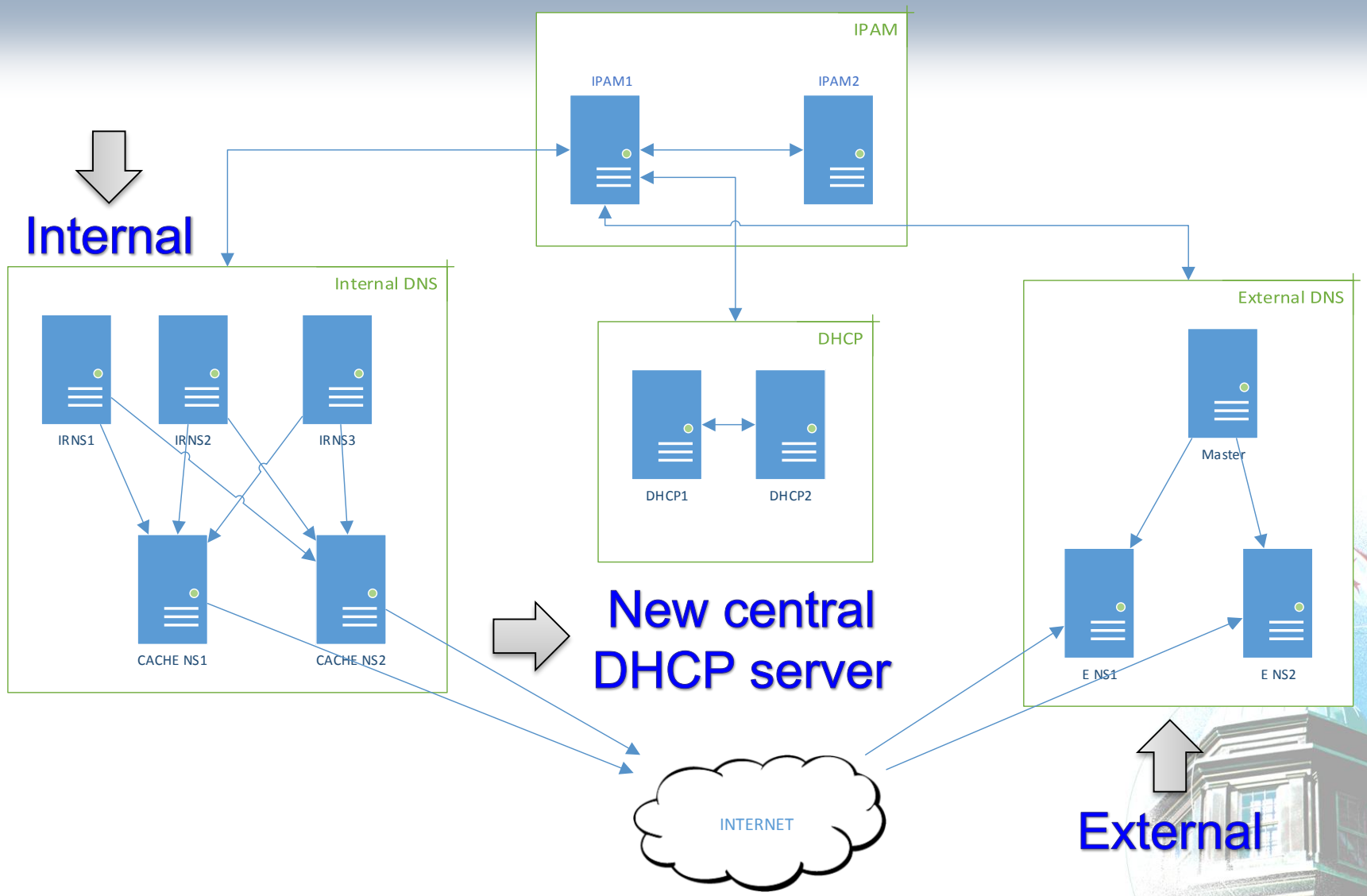
Before the end of 2017, we target:

- The following buildings are candidates to receive the wired/wireless upgrade (starting with NW District):
    1. Life sciences building (Medicine)
    2. Chancellor Day Hall (Law)
    3. Peel 3647 (Medicine)
    4. Peel 3674 (Law)
    5. Peel 3690 (Law)
- New Internet Edge with NGFWs will be deployed
- Cisco AMP End Point Protection deployment
- Last CFT to be awarded

Network Upgrade

TECHNICAL OVERVIEW

Main Changes to DDI (DNS, DHCP, IPAM)



Main Changes to DDI (DNS, DHCP, IPAM)

In 2015, "**Efficient IP**" was selected for DDI. Main changes:

IP Address Management (IPAM)

- Delegated Access to Subnets/VLANs
- NetChange Module – View switch port info and find IP addresses
- Manage DHCP and DNS from IPAM
- Helps identify/reconcile unused IP's
- No more spreadsheets
- IPv6 Support

New DNS infrastructure

- Internal & External DNS
- DNS RPZ reputation feed

New redundant DHCP servers

- With delegated access
- Managed via IPAM
- ***Note:*** *Want to move all connections to DHCP*

DO YOU NEED MORE INFORMATION?

Contact NetInf for Access and Training

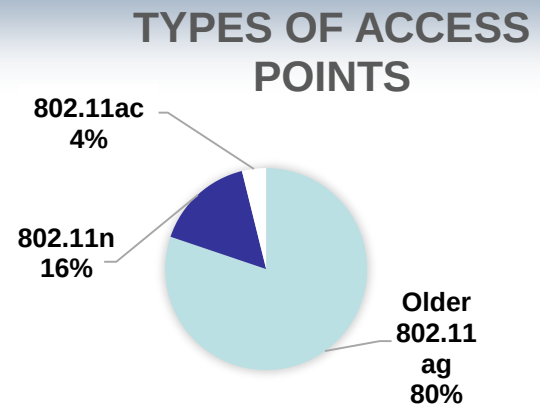
Participate in our next training Session! (November 17 & November 24)

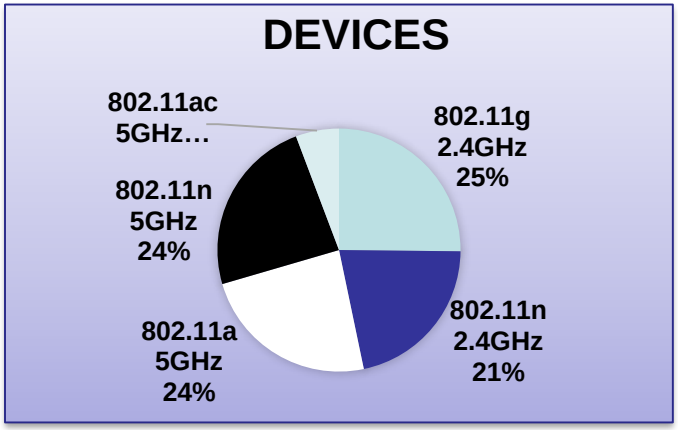
Wireless – Why is an upgrade needed?

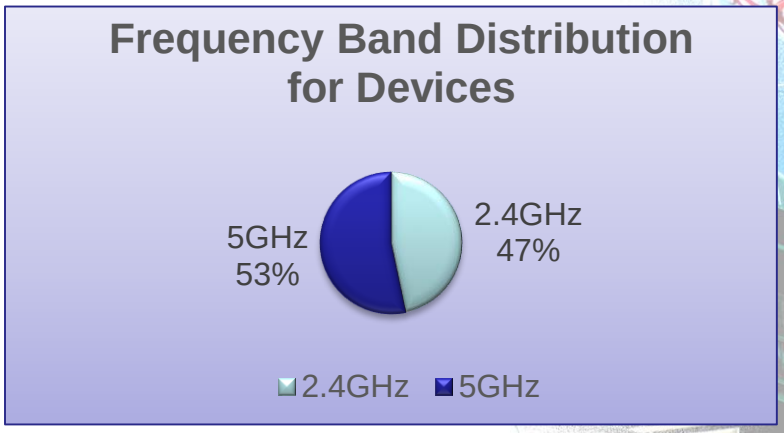
The current 4000+ Aruba AP's (campus and Rez) need an upgrade because:

- Need to fill coverage holes and upgrade high density area as needed
  - Most classrooms have been upgraded with high density AP's
- Current AP65 (a,g) are too slow

Note: *Some 11ac will not be replaced, but 11n will be replaced*







Wireless – What are we moving towards?

Technology: Aruba 802.11ac wave 2 AP's

Timeline: 3 years (in parallel to Wired switch replacement)

Improvement:

- 30%-50% APs will be added to fill 5GHz holes (Many high density AP's)

What was already done?

- Residences received the wireless upgrade during summer 2017
  - Bandwidth consumption for REZ has doubled going from 1.5Gbps to 3Gbps
- All new areas also done

Upcoming challenges:

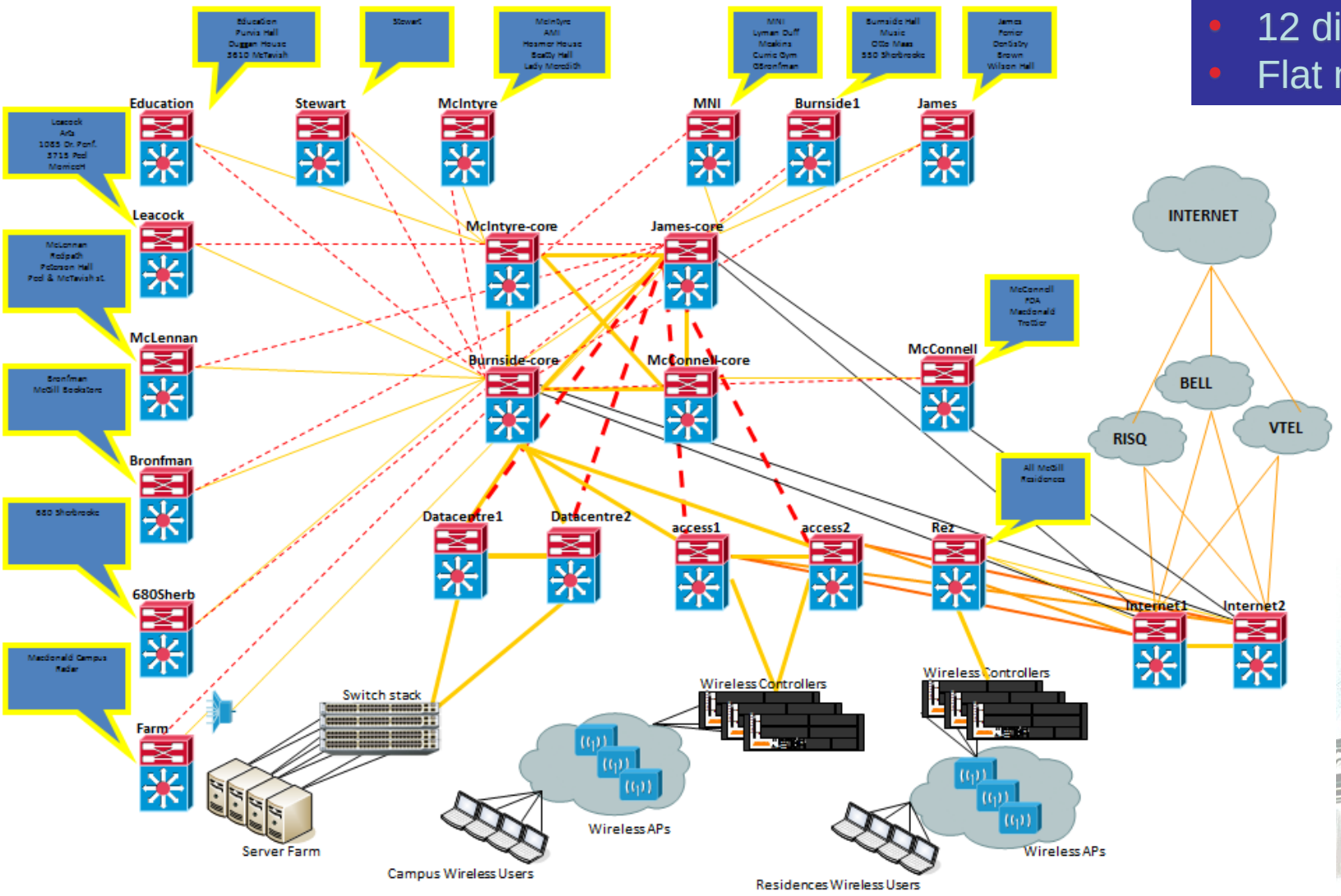
- Asbestos
- Scheduling
- Access to building/room to change AP's (access with security guards)

PLEASE REMEMBER!

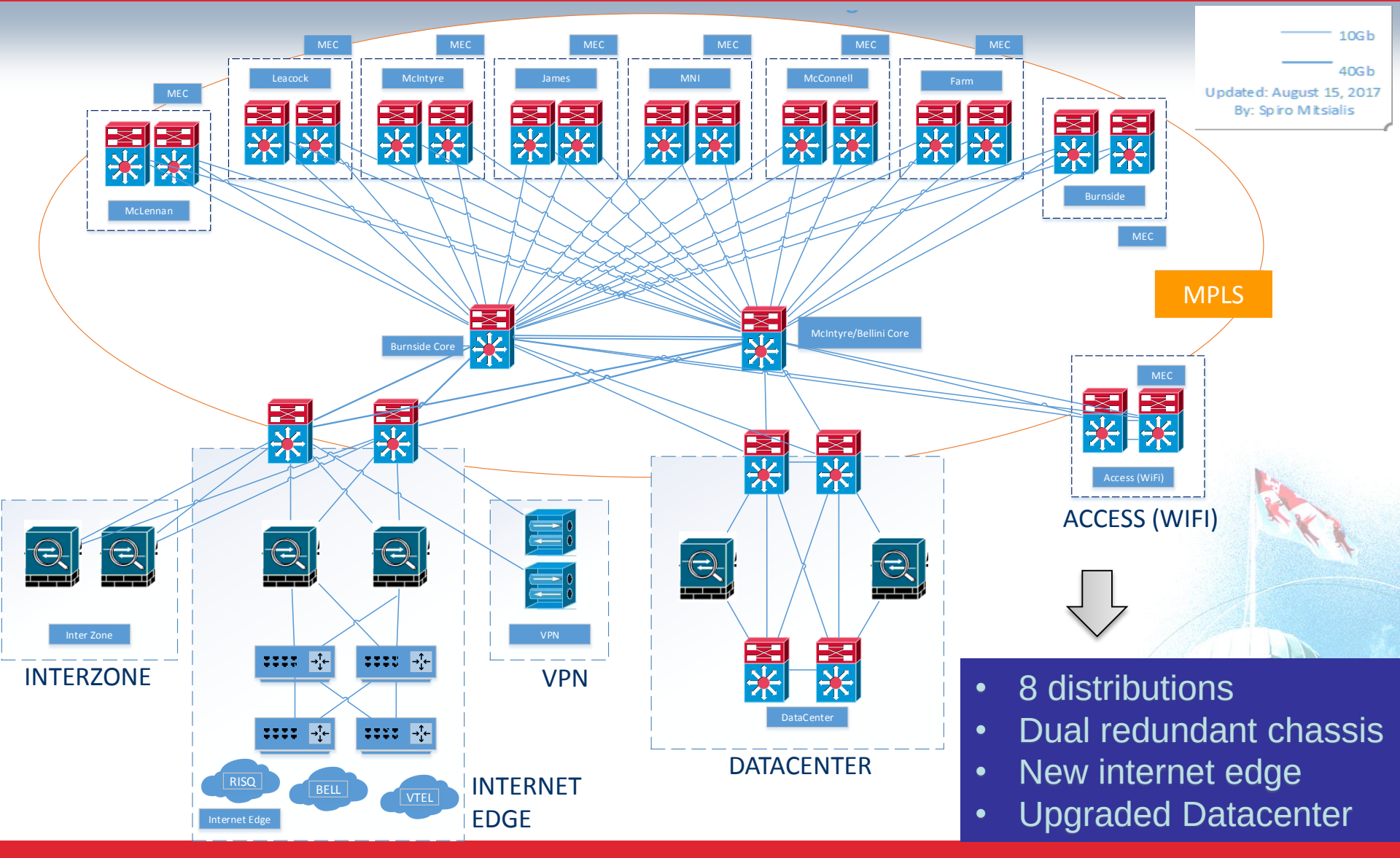
Buy devices that support 5GHz and 11ac

Current Network Architecture

- 12 distributions
- Flat network



Future MPLS Network Design



- 8 distributions
- Dual redundant chassis
- New internet edge
- Upgraded Datacenter

Main Changes to MPLS Network Design

New Core/Distribution

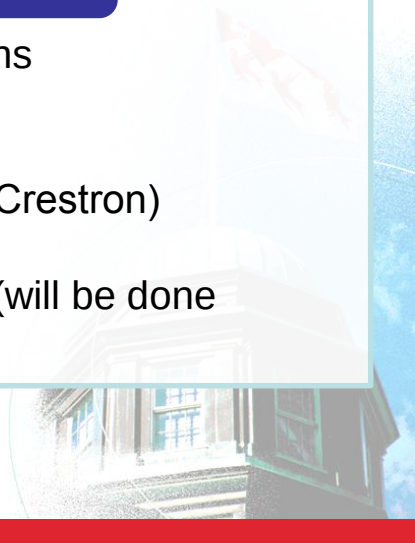
- Capable of 10-40-100Gbps

Dual Chassis Distribution for increased redundancy

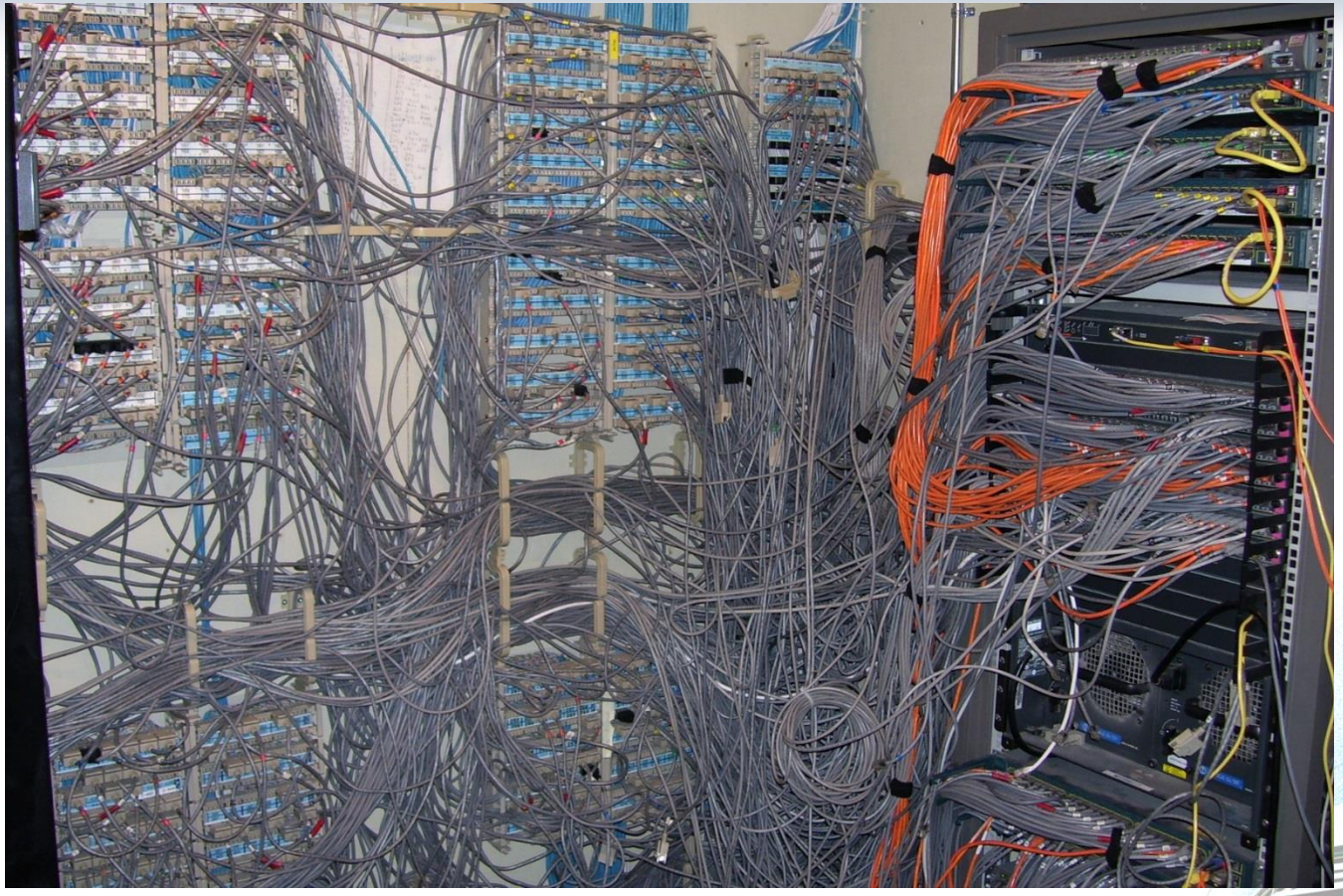
- 4 x 10Gbps Distributions, Wireless, Datacenter
- 4 x 40Gbps InterZone & Internet Edge

New Access Layer using virtual chassis

- Use of pigtails and New structured cabling to support 1 gig connections
- Switch stacked and managed via 1 IP address
- All gigabit ports PoE; 2 x 10G uplinks/stack
- PoE reserved for AP's, security cameras and classroom automation (Crestron)
  - VoIP Phones will use local Power
- DHCP Snooping and ARP Inspection (**all devices must use DHCP**) (will be done in a later phase)



Telco Room - Before



Telco Room - After

PLEASE REMEMBER!

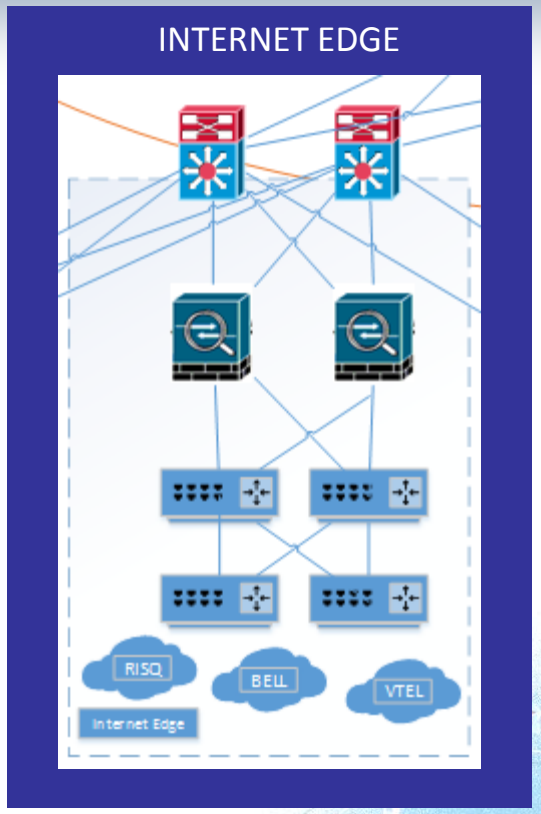
Keep telco rooms clean and neat

Keep webtools up to date (911)

Other Changes

Refresh of Internet Edge (Fall 2017)

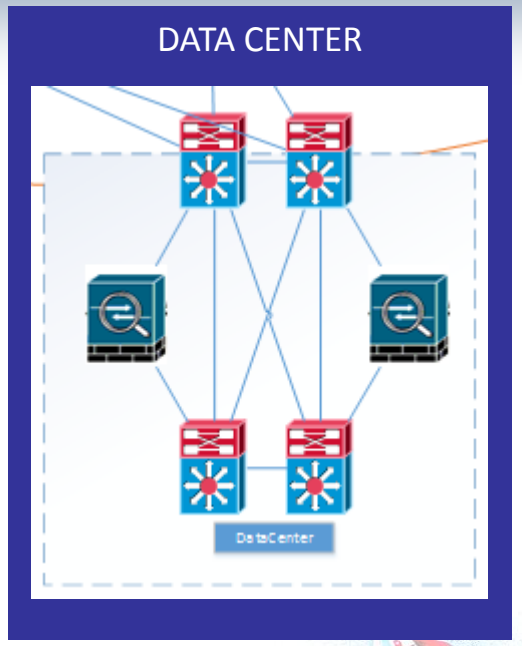
- New Routers
- Eliminate Packet Shaper
- Next Gen Firewalls/IPS
  - Use of private IP (10.0.0.0/8) with NAT
  - Use of state full firewalls instead of router ACL's



Other Changes

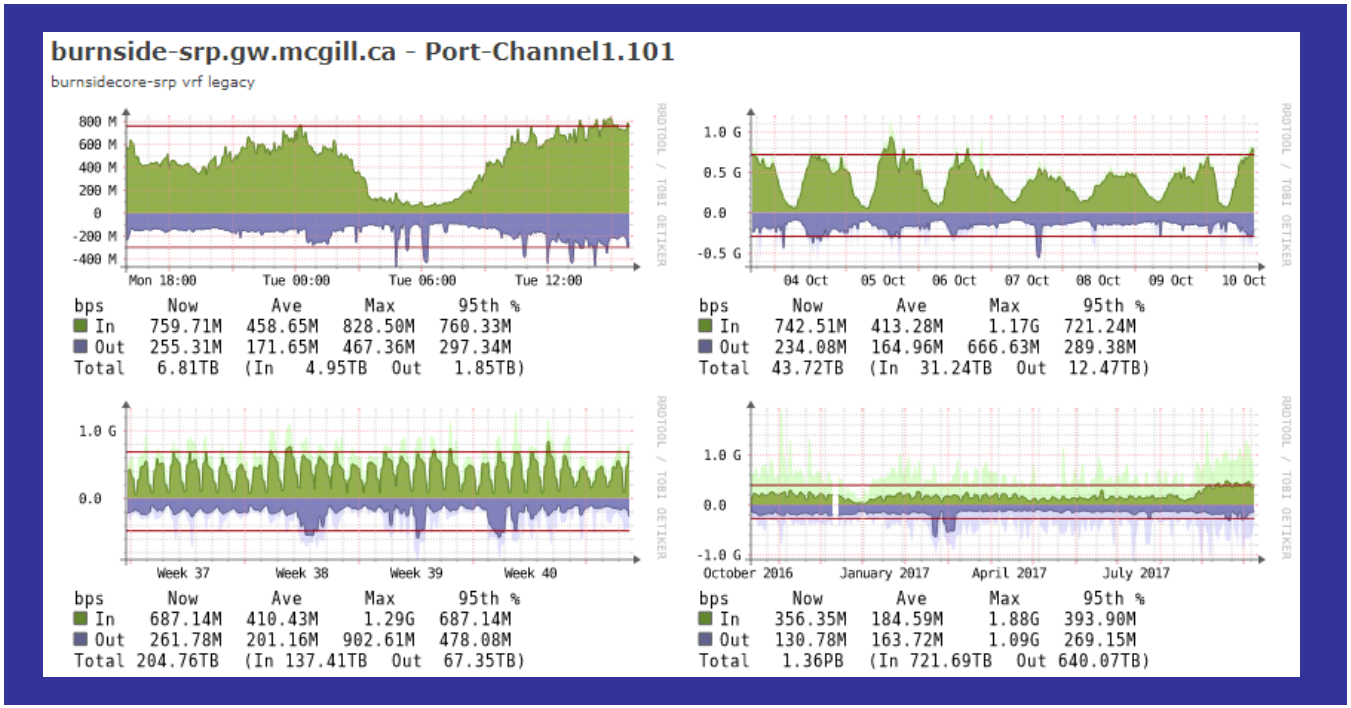
Refresh of Datacenter (2019)

- New Routers and Switches (Nexus line)
- Next Gen Firewalls/IPS
  - Three (3) zones within Datacenter:
    - DMZ – Internet Facing
    - Apps Tier – Internal to McGill
    - Server Farm – Restricted Access (User's and servers)
- Load balancers (done)



Other Changes

- New Monitoring and Management software
  - LibreNMS to replace MRTG/CACTI
  - Replace Webtools (in ~18 months)



Firmware Upgrades

- New features; bug fixes; security updates

- Anticipate 2-3 firmware upgrades per year
- Will be done off hours (early mornings)

- Core/Internet Edge is redundant therefore no outages

- Distribution dual chassis (virtual switch)
  - Upgrade one chassis at a time
  - Downtime: seconds

- Access Layer (Telco rooms)
  - Reboot of stack
  - Outage of 10-30min depending on microcode

- **Pre-Established Maintenance Windows**
  - Need to establish regular maintenance windows
  - Anticipate 8 weeks to upgrade all of Campus (2 windows/week)

When is a bad time for upgrades?
(September, Exams Periods, ??)

Information Security

TECHNICAL OVERVIEW

Next Generation Security

New and more advanced security features will be implemented:

Next Generation Firewalls (Cisco Firepower)	New Integration of Network & FWs into SIEM*	New End Point Protection
• Intrusion Prevention • Threat Intelligence • Advanced Malware Protection	• Behavior Analytics: • Flows, Events, Cisco StealthWatch	• Cisco AMP • Network Access Control (NAC) – Cisco ISE

Complementary Security Initiatives (Outside of Network & Information Security Upgrade)

- Other features available from the Cisco Security Enterprise License Agreement 5.0

Umbrella, Cognitive Threat Analytics, Mail Security, etc.

These initiatives will be ongoing over the next 2 years

*SIEM: Security Information and Event Management

Security Zones – What and Why

Security zones are logical groupings of entities

Why do we need Security zones?

- Access to follow the user: wired/wireless/vpn
- Consistent experience between users

Provide Unified User Experience

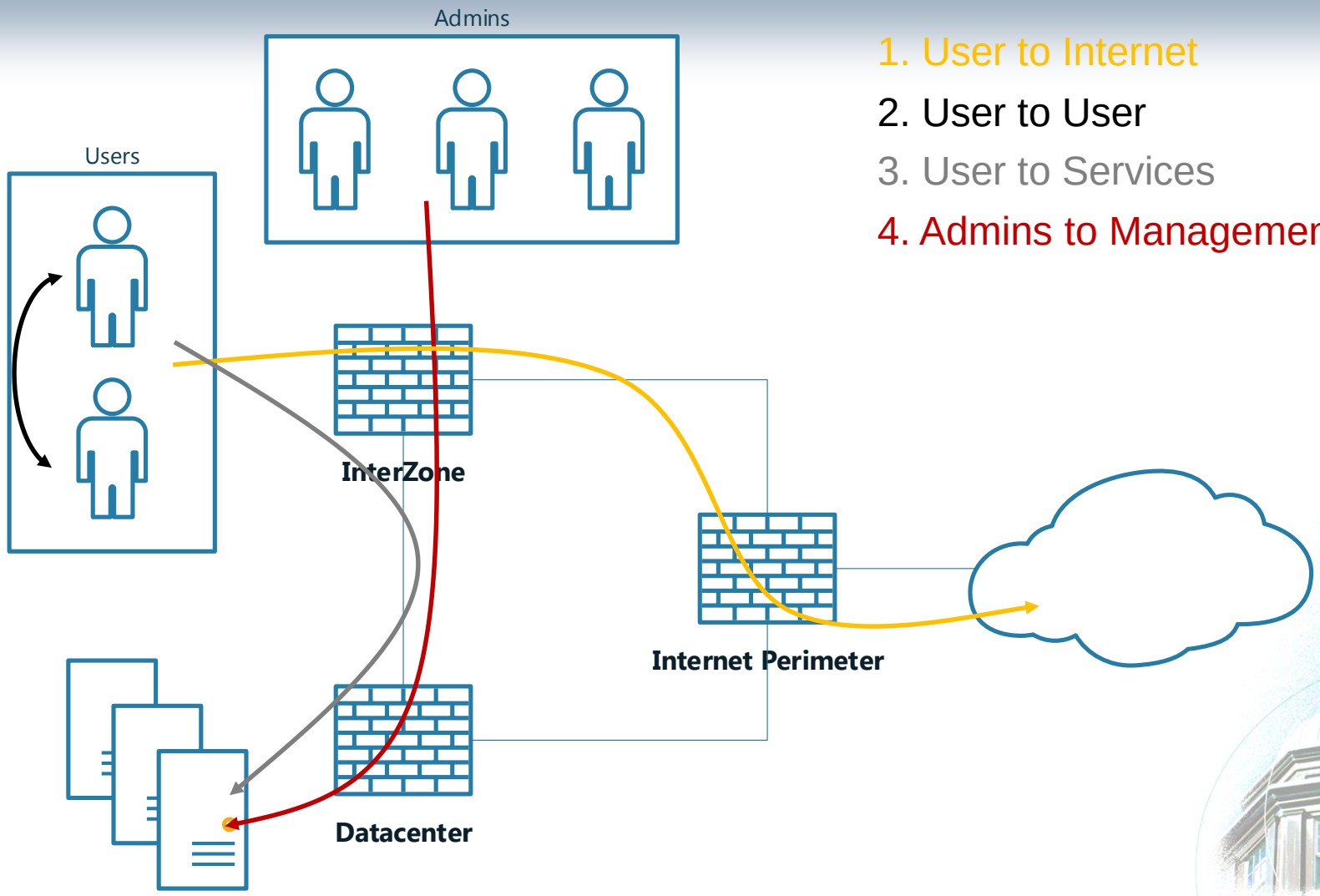
- Centralized inspection gates between zones
- Policies based on identities not IPs
- More standardized and logical (Fewer VLAN per group)
- Less VLAN and ACL sprawl.
- More efficient system deployment

Improved Management

- Layered security approach

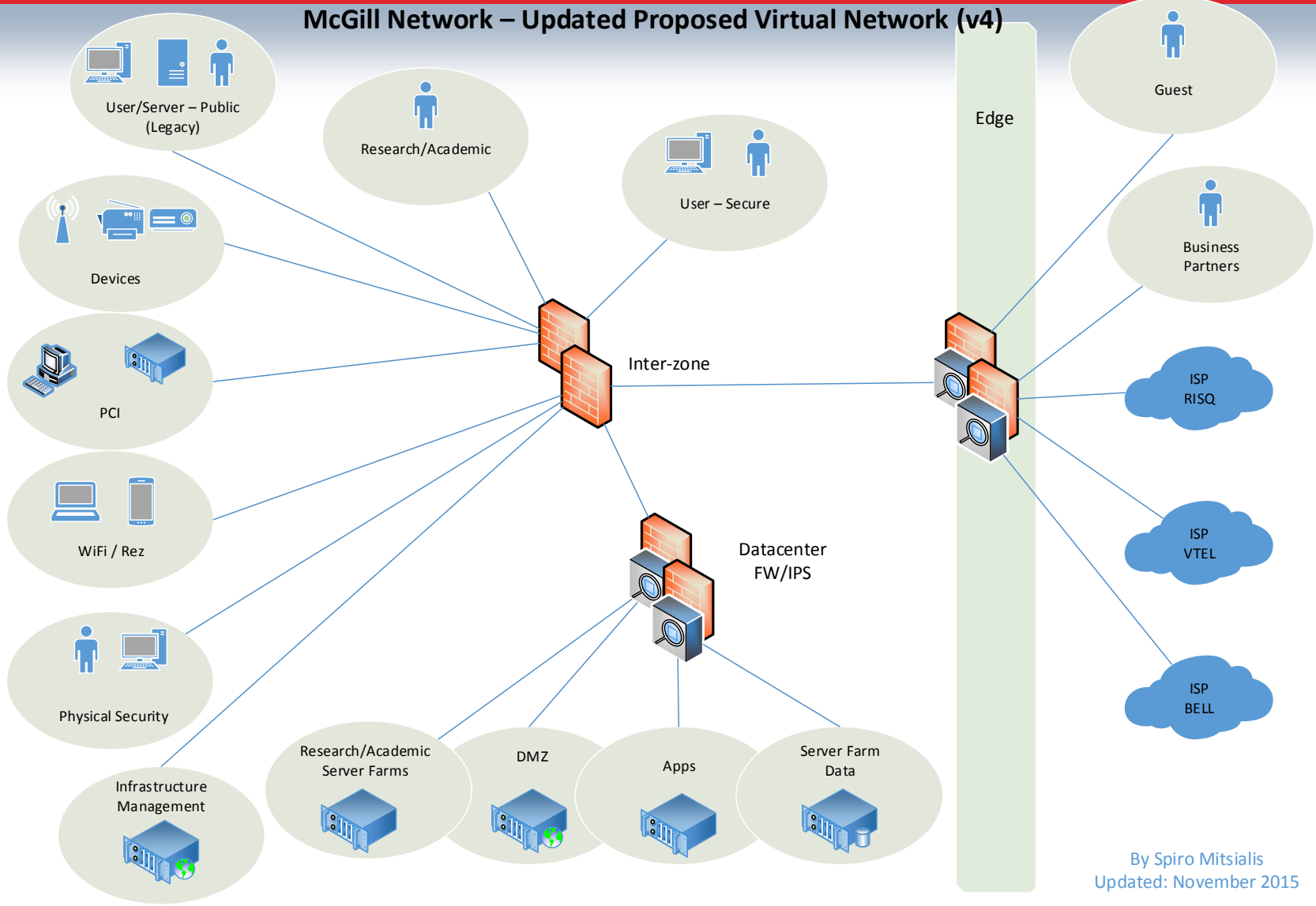
Security in Depth / more control for LAN admin

User Network Traffic Flows



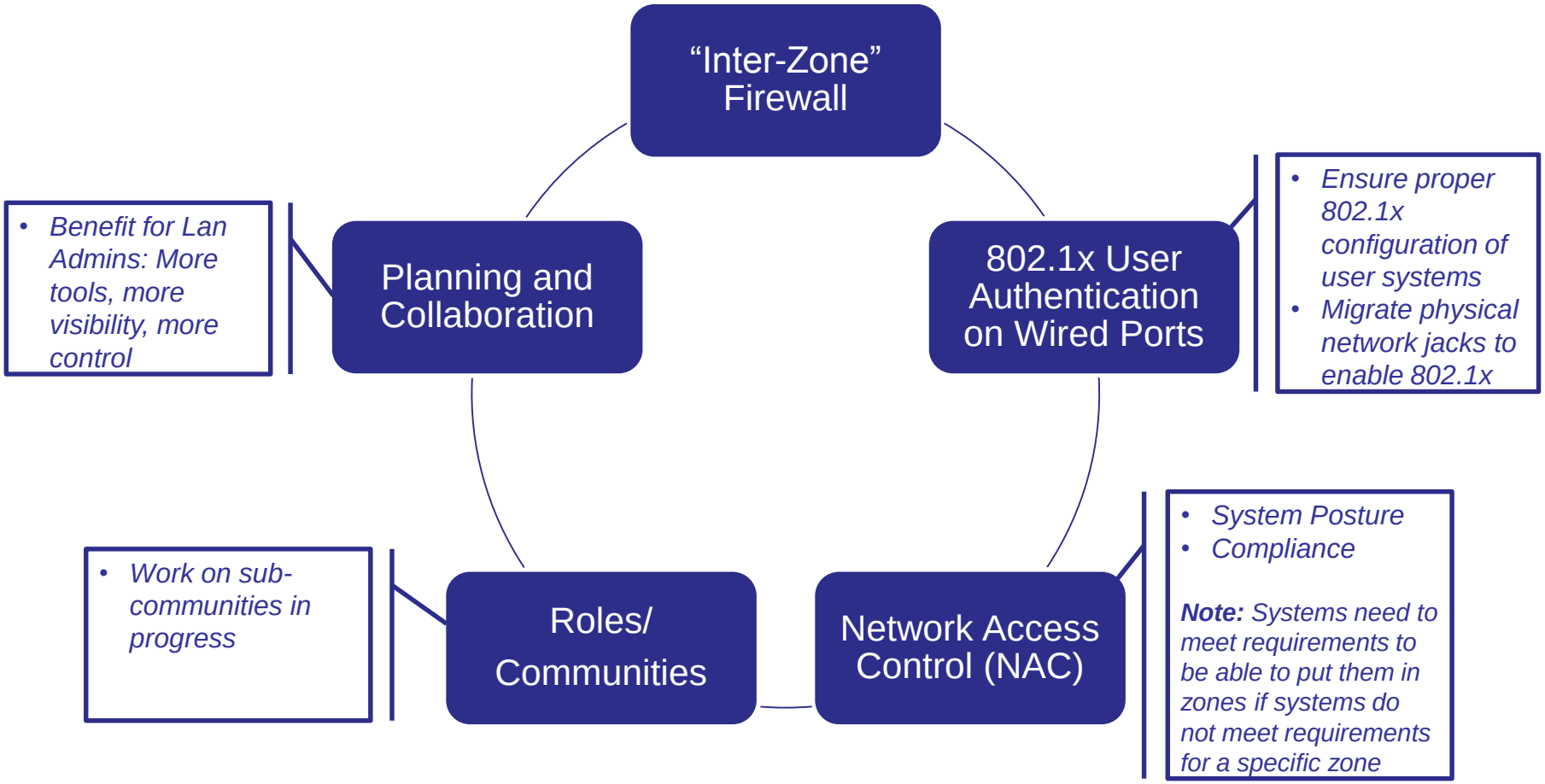
1. User to Internet
2. User to User
3. User to Services
4. Admins to Management

Security Zones – based on User Zones



By Spiro Mitsialis
Updated: November 2015

How do we get there?



Wired & Wireless Upgrade

KEY STEPS FOR EACH BUILDING

Wired - What needs to be done?

Wired - Migration

- Access switch replacement (new Cisco 3850 models)
- UPS replacement (new Eaton models)
- Physical Infrastructure updates (much of this is prior to migrations windows):
  - New racks, new wall brackets
  - New fiber runs
  - Replace CAT5 with new structured cabling to support gigabit connections

IMPORTANT

- As much non-network disruption preparatory work to occur prior to Migrations
- Migrations happen early AM before start of business, some WEs
- During Migration window, **no** wired or wireless access, network will come back gradually during the window

Wireless - What needs to be done?

Wireless - Upgrade

- Installation of Access Points (AP):
  - Replacements and Relocation of existing access points with new technology
  - Add new access points

IMPORTANT

- Sporadic interruptions of wireless service during AP swap/relocation (30-60 mins)
- Work to be done during work hours where possible

Key Steps for Each Building

1 TIMELINE

What: Discussion with with Building Directors & LAN Admin

Why: To provide information on timing & discuss building access needs

Action required for Building Director/LAN Admin
Collaborate in discussions with Project team

2 CONFIRM

What: Email to Building Director & LAN Admin & Poster

Why: To formally confirm date of building migration start & details specific to building

Action required for Building Director/LAN Admin:

- Communicate information to impacted building occupants
- Support hanging of posters

3 REMIND

What: Reminder email to Building Director/LAN Admin re. Building migration start

Why: To provide a 48 hour notice/reminder that building migration starts

Action required for Building Director/LAN Admin:
Send reminder to impacted users:

- Migration is happening
- Users to leave their computers and devices on

4 SUPPORT

What: Post-Migration information to LAN Admin

Why: To inform any oustanding issues/anomalies from the migration

Action required for Building Directors/LAN Admin:
Collaborate with project team to resolve issues after migration

Note: Project team support within 72 hrs post migration to the Lan Admin

NOTE: The different steps may require 2-12 wks, varies on the size & state of telco rooms

Network & Information Security Upgrade

WHAT DO WE NEED FROM YOU?

Why are you here?

- You are a subject matter expert in your area
- You have essential skills to support and communicate this upgrade
- You have an important role within your organization

With your help, we can make this project a succes!

What do we need from you?

Support

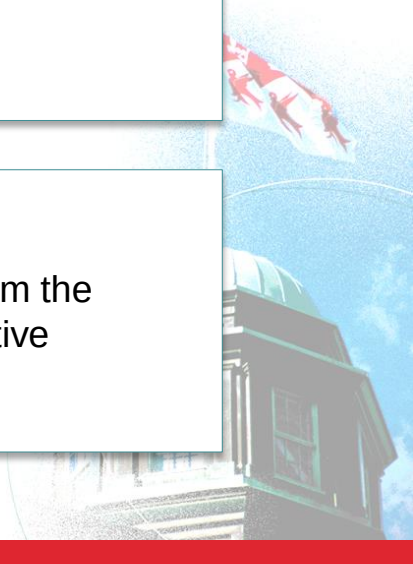
- Raise any technical issues to project team
- Support access to building according to project schedule
- Collaborate with project team to resolve issues after migration

Communicate

- Support communicating the timing of the migrations to impacted building occupants
- Support communicating through the appropriate communication channels (email, posters, etc)

Influence

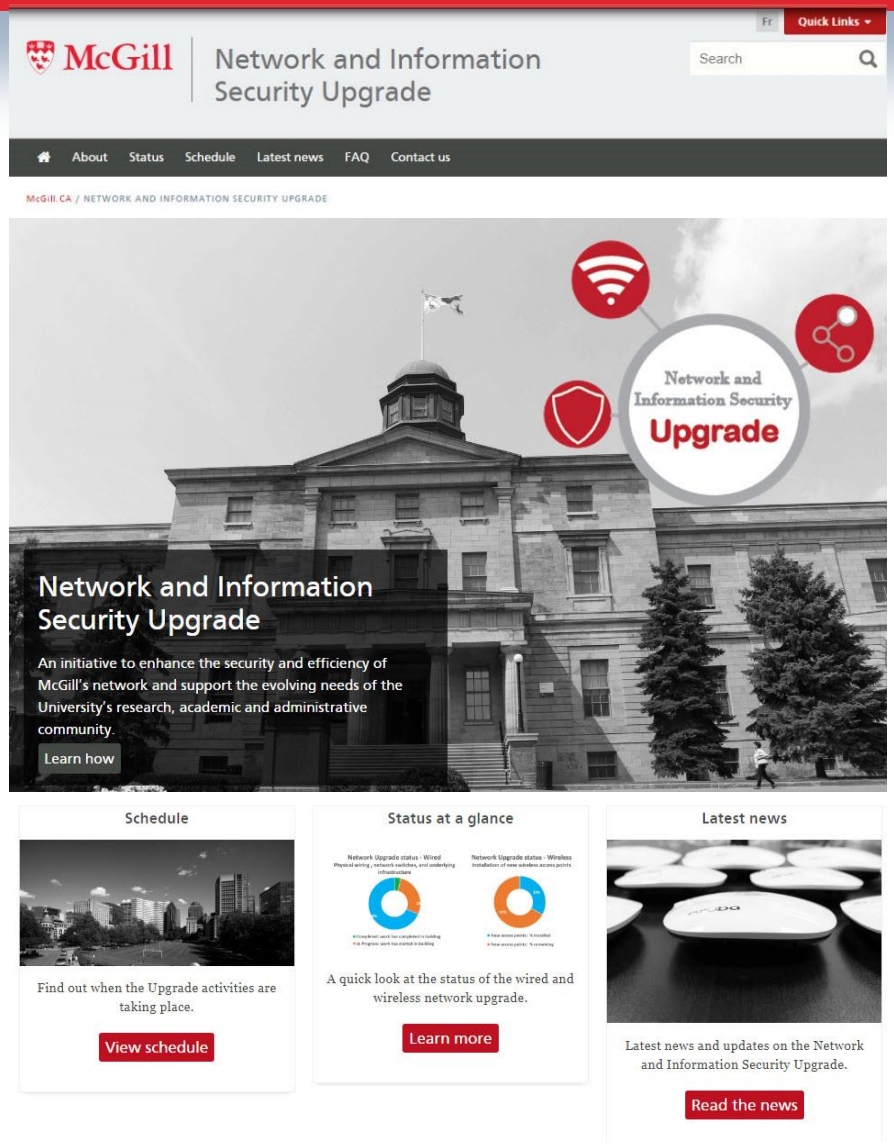
- Promote the changes and benefits resulting from the Network & Information Security Upgrade initiative



More concretely… how can you help?

Activity	By who?	When?	Input
Support the communication for dates of building migration start / services interruptions to building occupants (email, poster)	Lan Administrator/ Building Director	Target: 2 weeks before migration start	Information sent to you by IT project team
Send reminder to building occupants to leave their computers and devices on	Lan Administrator/ Building Director	2-3 days before migration	Information sent to you by IT project team
Sign up for DDI training Session (November 17 & 24) – *as required*	Lan Administrators		
Report issues and concerns to project team	Lan Administrators	During migration	
Buy devices that support 5GHz and 11ac	Lan Administrators	Ongoing	
Keep telco rooms clean and neat and ensure webtools remain up to date	Lan Administrators	Ongoing	
Ensure systems are updated (latest supported Operating Systems)	Lan Administrators	Ongoing	
Access switch Maintenance Windows	Lan Administrators	By Nov 10th/2017	

Project website: mcgill.ca/network-upgrade



- Upgrade schedule
- Project status
- Support: FAQs and webform

Project email communication

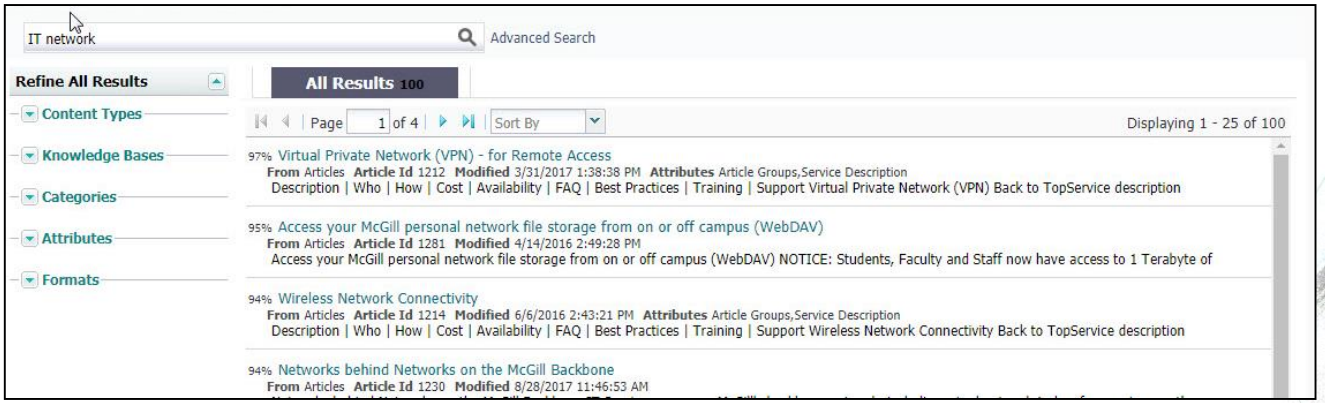
Network and Information Security Upgrade Project

network.project@mcgill.ca

Need more info? McGill IT Knowledge Base

- **Go to mcgill.ca/it**
- **Enter a search term (e.g. IT network, Wireless, etc)**

Search results: links to articles



Your Support

Together, we can make this project a success!

Thank you for being here today!