Princeton’s Next Generation Network

Cyberinfrastructure for Research Data Management

Chris Tengi, Sr. Architect, Network Services - May 23, 2023
The Problem to be Solved

Legacy Network

• 20+ year old design
• Single border router, no firewall
• Single core router
• Layer 2 VLANs shared between buildings
• Mostly 1 Gb/s building connections, with a few 10 Gb/s
• No redundancy
• Manual port configuration
• Automation-hostile
The Solution

Next Generation Network

• New (to Princeton) design
• Dual border routers, and firewalls
• Dual core routers
• Layer 3 to the buildings
• Layer 2 VLANs within each building
• Mostly 2x10 Gb/s building connections, with some 2x40 Gb/s and some 2x100 Gb/s
• Dual/redundant “everything” (except APs)
• Colorless ports
• Enhanced security
• Automation-friendly
The Legacy Network (after the border upgrade)

Single core router (core-lewis)
Dual border connections
(Mostly) low-speed building uplinks
Connections to 2 data centers
The Next Gen Border

2, 10 Gb/s Commodity Internet (Edge)
2, 100 Gb/s Internet2 (Edge)
2 Border Routers
2 Border Firewalls
2 “auxcore” switch-routers for AL2S and Legacy L2 over NGN
The Next Gen Core

Dual NGN core routers

“auxcores” connect to core-lewis for L2

“auxcores” connect to NGN for VXLAN

All connections redundant
Redundancy in the Buildings

Legacy

- 1 uplink
- 1 aggregation switch
- 1 access switch
- 1 AP link

NGN

- 2 uplinks
- 2 aggregations switches
- 2 access switches
- 2 links per AP
NGN Bandwidth and Security

All buildings get 2 uplinks to the NGN core routers, for redundancy
Guaranteed bandwidth of 10 Gb/s, 40 Gb/s or 100 Gb/s
Upgrading “100 gig” buildings to ”200 gig” buildings is easy

Colorless ports use Aruba ClearPass to determine correct network for each device
Devices profiled/fingerprinted by MAC address and operating system
“Unverified” devices can be placed on a network without access to sensitive data and infrastructure
Questions?