ITS Information Technology Services

UNIVERSITY NETWORK REPORT

ACADEMIC YEAR 2016-2017

SEPTEMBER 21, 2017

Table of Contents

Table of Figures

1. Executive Summary

This report provides metrics and performance of the university's network along with recommendations and commentary. Questions may be sent to networking@its.utexas.edu

1.1. Points of Interest

- 11,500 pieces of equipment create the university's network, with a projected $14M annualized operating cost.
- Over 295,000 unique devices use the university's network (mostly wireless). Device growth has slowed to 2% annually.
- Bandwidth consumption increased 24% from the previous year.
- Building network grades increased to an average of 81 (B-) with $4M of deferred building network investment.
- Increasing complexity, growth, and expense call for new approaches including:
    - Saving over a million dollars annually by shifting more devices to wireless.
    - Using the new Wired General Network for scaling, security, compliance, and automation.

1.2. New Investments

Information Technology Services (ITS) made the following investments in the network since the last report:

- Core Wireless Lifecycle
- Backup Internet Service Provider

Planning is underway for:

- Replacement of the primary Network Operations Center (funded, under construction, completion fall 2017)
- Network Core Lifecycle
- Network Address Translation Lifecycle

1.3. New Requirements

There were no new requirements this period. IT Governance is examining central IT operations and funding, and may change operation and funding models.

2. Scope of The University of Texas at Austin

The University of Texas at Austin has an enrollment of approximately 51,000 students as well as 23,000 faculty and staff, with a FY1617 budget of $2.87 billion. It is ranked among the top 20 public universities and has been awarded over $1.1 billion in sponsored research awards over the past two years. There are 18 colleges and schools, as well as over 90 research units, seven museums and 17 libraries. See: http://www.utexas.edu/about/facts-and-figures

The university's network serves roughly 200 buildings and sites, comprising over 24 million gross square feet. (Figure 1)

The network is funded and operated in a federated model. Central staffing and operations are provided by Information Technology Services (ITS). Spending on all information technology by ITS for FY1617 was approximately $41.5 million. Total IT spending is not tracked but believed to be on the order of $150 million. University units provide distributed funding for equipment in buildings, operations, and staffing (mostly resource planning, moves, adds and changes). While support and funding is distributed, ITS Networking is ultimately responsible for all university networks, and co-manages 90% of the wired networks and all of the wireless networks.

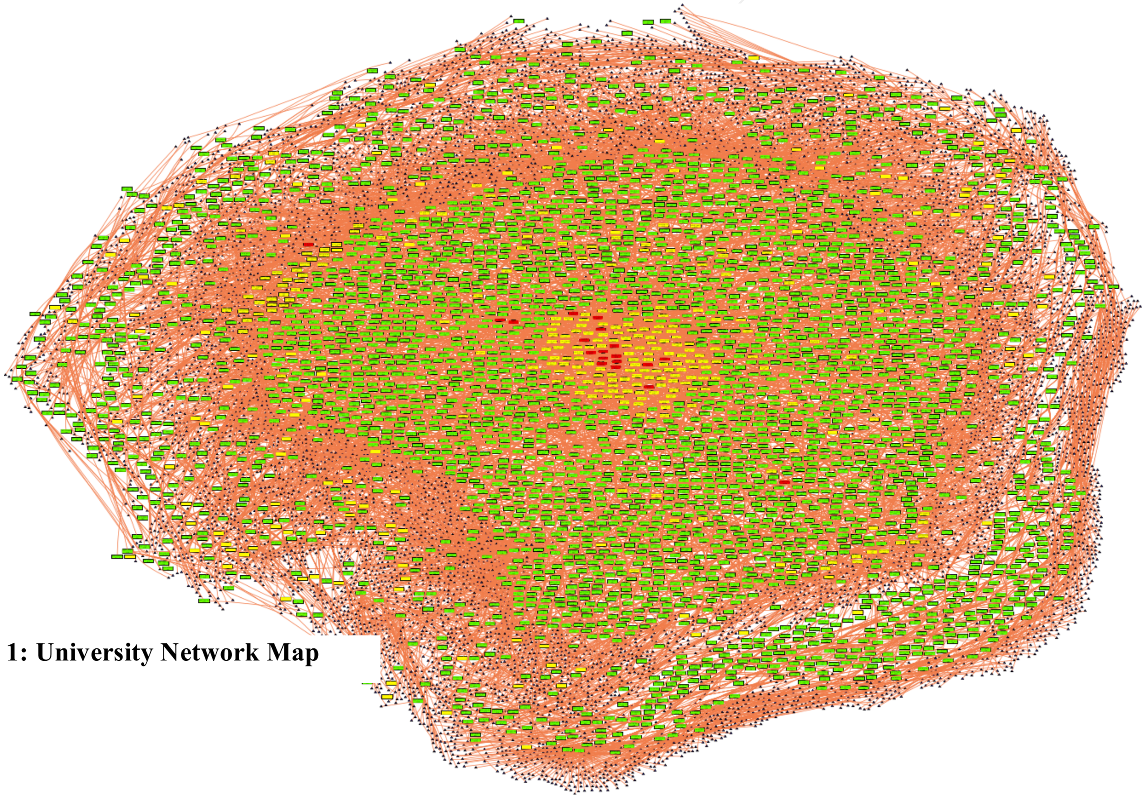


Figure 1: University Network Map

3. Service Levels

Key service level metrics are monitored by Networking and reported for governance purposes. All metrics exceeded agreed-upon measures as of 5/2017:

	Metrics	Achieved	Goal
✔	Campus Network Backbone Availability	100%	>99.950%
✔	PRC Network Backbone Availability	100%	>99.950%
✔	Wireless Core Availability	100%	>99.900%
✔	Data Center Network Availability	99.991%	>99.960%
✔	Commodity Internet Availability	99.998%	>99.50%
✔	Commodity Internet Use	92%	<95th%
✔	Average Building Network Grade	81 (B-)	n/a
✔	DNS Availability	99.997%	>99.980%
✔	DHCP Availability	100%	>99.950%

Outage reports are available: https://wikis.utexas.edu/x/B1x9 (university restricted).

A satisfaction survey of Technical Support Contacts (TSC) representing the federated units was taken in March 2017 yielding the results depicted in Figure 2.

TSCs expressed high scores for operational measures but had notable declines in satisfaction with Networking staff response times and continued dissatisfaction with the tools provided. Those tradeoffs in operational measures and staff response times were an expected and conscious prioritization, given fixed central staffing. Both organizational and technical strategies (e.g., Site Networking, General Networks), are being implemented to slow this trend.

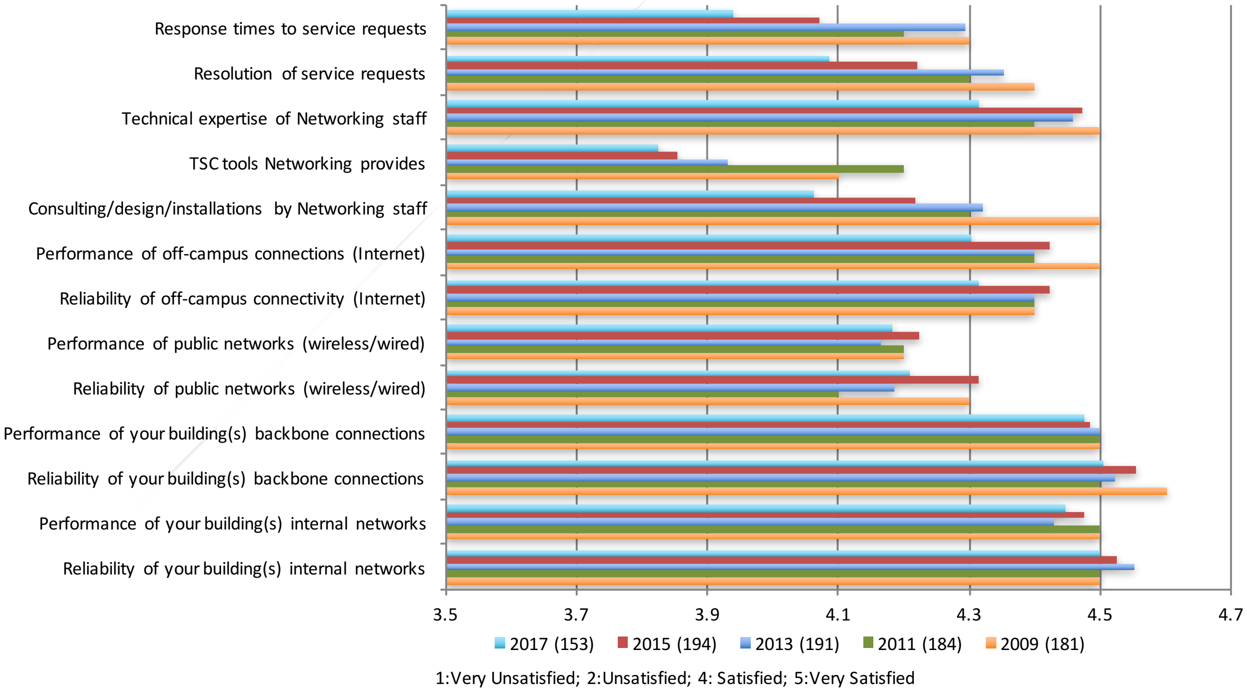


Figure 2: TSC Satisfaction Survey

4. The University Network

4.1. *Core Operations*

The network core interconnects all network services. Core availability was 100% year-to-date, exceeding the SLA goal of 99.950%.

Traffic through the core of the network grew 34% from the previous year (Figure 3). The number of routed networks increased 5%, driven by both growth and additional network segmentation as a security measure (Figure 4).

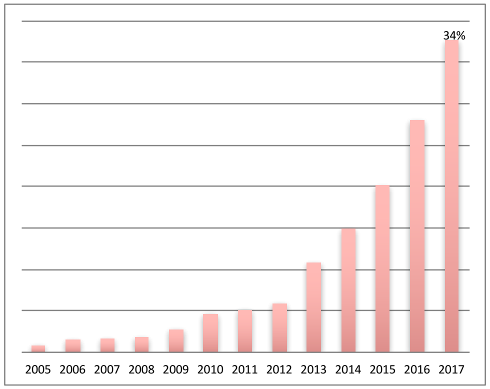


Figure 3: Core Traffic Growth

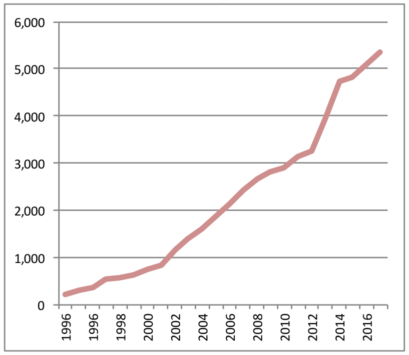


Figure 4: Subnet Growth

Two Network Operation Centers (NOC) each house half of the core network equipment providing survivable operations. Buildings connect to both those NOCs through a geo-diverse fiber plant (Figure 5). Clusters of buildings are geo-diverse, but most individual buildings lack geo-diversity. Construction activities and projects (e.g., Distributed Antenna System, Longhorn Network) have increased capacity and diversity of the fiber plant along central routes.

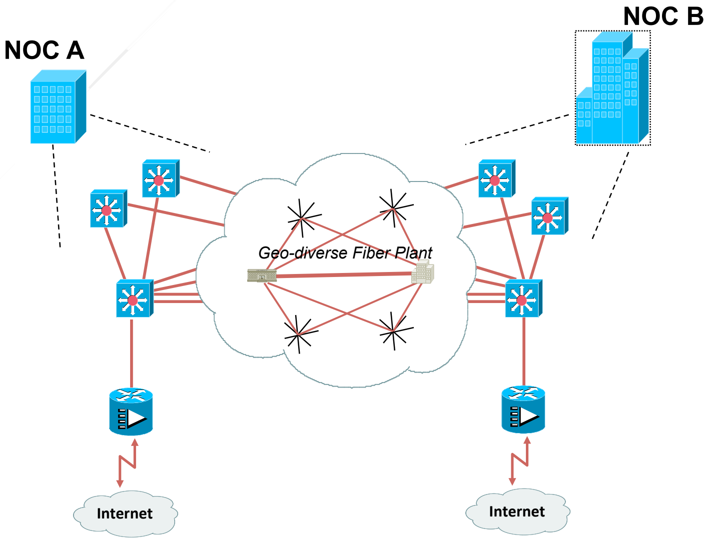


Figure 5: Basic Topography

A replacement for the primary NOC was funded as part of a university capital improvement project to serve both the UT Austin campus and also UT System for the next 20 years (Figure 6). Construction is scheduled to complete in 2017, followed by transition of services to the new facility and decommissioning of the old site (expected to begin in calendar year 2018).

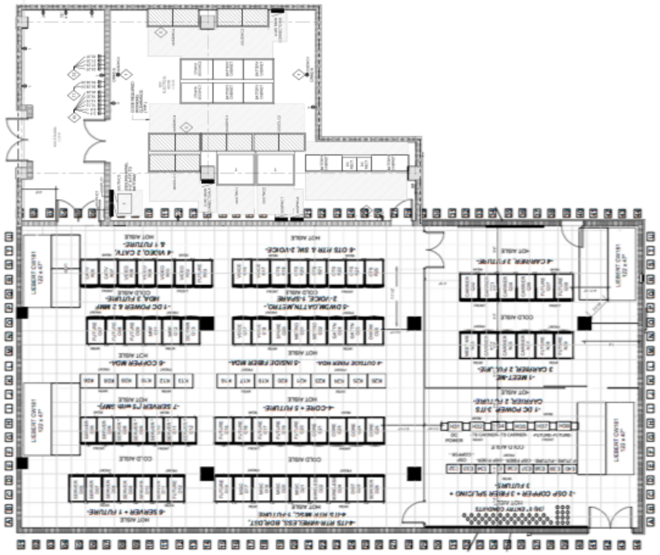


Figure 6: New Network Operations Center

Since the last report:

Multiprotocol Labeled Switching (MPLS) capability was deployed in the core and to supporting access routers to enhance segmentation and isolation for security (Figure 7). Special arrangements are still being configured for routers not supporting MPLS and should be completed this fall. Initial network address spaces were provided to owners of the new networks, so that they may begin the long transition process of renumbering their devices, prior to isolation and customized policies. Virtual Routing and Forwarding (VRF) instances have been limited to those willing to fund service center expenses (five to date). Funding requirements have discouraged other appropriate uses that would help secure campus and reduce overall support costs (e.g., printers, classroom media technology, etc.).

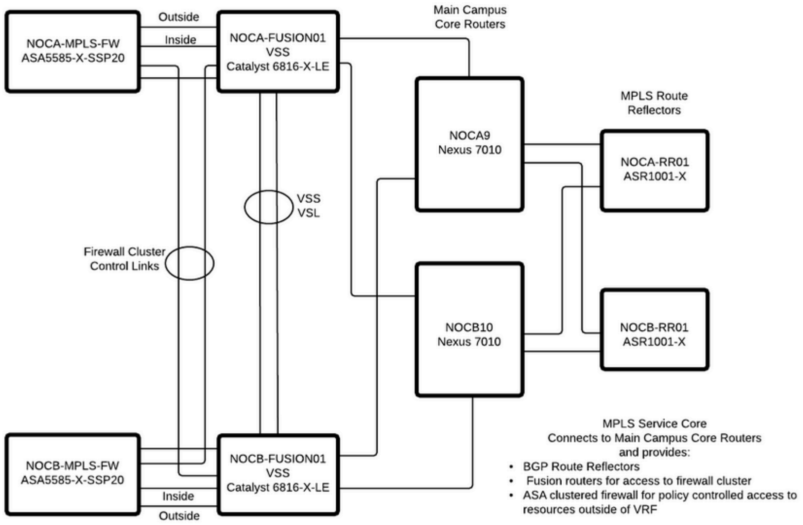


Figure 7: MPLS Architecture

Small building shared routers: Six pairs of distribution routers supporting the proposed small building model mentioned in the last report were installed and have been providing expected services levels and savings (Cisco 6840-X VSS pairs). Enough new sites have committed to justify a request for three additional pairs with building conversions expected through summer 2018.

Dense Wave Division Multiplexing (DWDM) system supporting the Pickle Research Campus (PRC) and Dell Pediatric Research Institute reached end of support and was upgraded to an Adva FSP 3000. An additional 100Gbps circuit was added for the Texas Advanced Computing Center (TACC) to provide resiliency across the mostly aerial metro fiber plant (combined 200Gbps to the main campus). Additional 10Gbps circuits were added to support small building distribution routers for the PRC campus -- connecting them directly to the main campus core.

Border Routers were lifecycled this summer to a geo-diverse pair of Cisco ASR 9004 (previously 6509s), providing 100Gbps connectivity between upstream providers and the core. The Network Address Translation (NAT) appliances from A10 were moved from the border to the core to enable finer segmentation in the future, and for cost avoidance related to network monitoring taps. The core remains a pair of Cisco 7010s, which are expected to be lifecycled to Cisco 7710s next AY as part of migration to the new NOC.

The overall core architecture is illustrated in Figure 8. It continues to evolve as required to support the university's mission.

Management Systems used by Networking and units have not been upgraded due to staffing shortages and are beginning to fail regularly (some key databases are running on 10-year-old hardware). Delays to other ITS and unit projects will occur as these upgrades are prioritized to sustain operations.

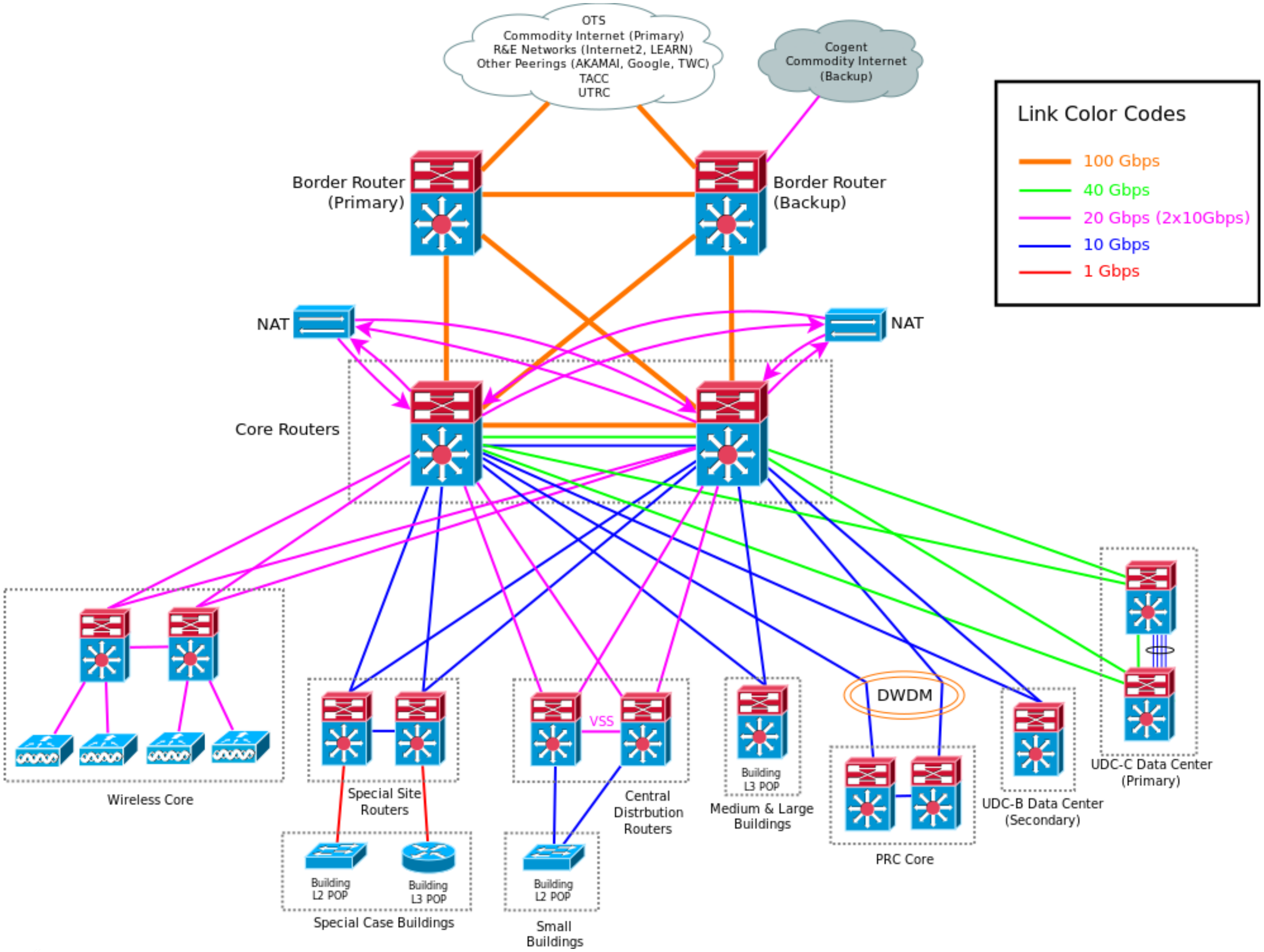


Figure 8: Core Architecture (Summer 2017)

4.1. Core Wireless Operations

Core wireless availability was 100% year to date, exceeding the SLA goal of 99.900%. The core wireless network was upgraded in summer of 2017 to a cluster of four geo-resilient Cisco 8540 controllers connected to a dedicated Cisco 6840-X pair (non-VSS). Additional controllers/routers are on order to meet specialized service requirements of Dell Medical School. The previous generation of Cisco WiSM2 controllers in 6500 series routers served the university for over seven years and a 500% increase in end-user devices.

Growth in device count, connect hours and users is slowing (Figure 9). In spring 2017, 203,000 devices authenticated with university credentials and over 860,000 associated with the guest "attwifi" network. There were over 51 million authenticated connect hours. Over 59,000 clients connected simultaneous, and there were over 80,000 one-hour DHCP leases on a busy day.

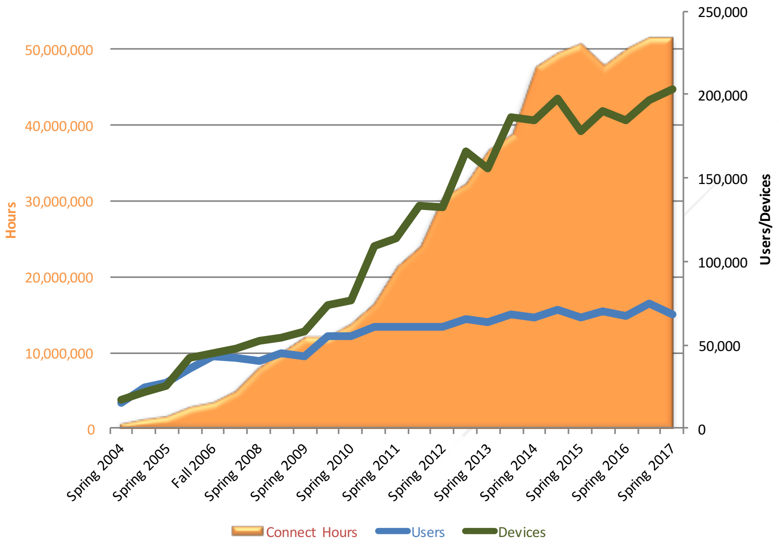


Figure 9: User, Device, Connect Hour Growth

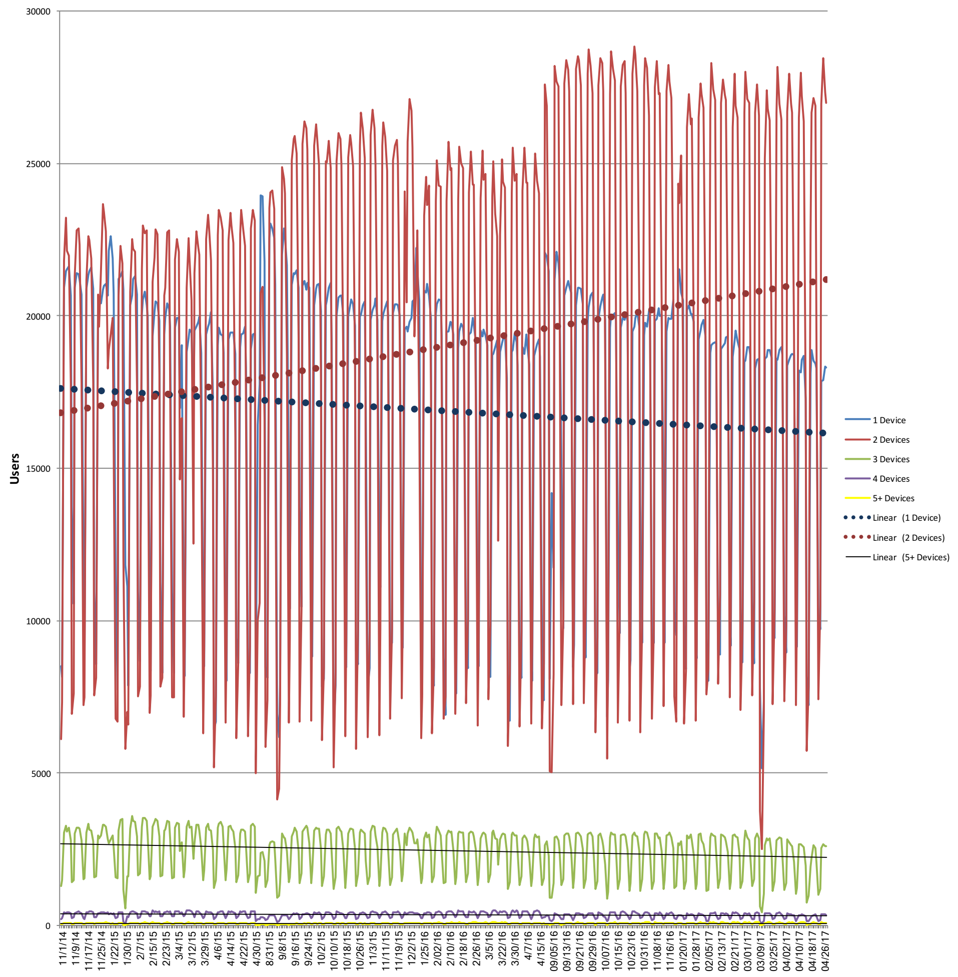


Figure 10: Wireless Devices Per User

The number of devices per user continues to grow (Figure 10), red dotted trend line shows two devices per user increasing, blue trend line single devices decreasing). Three and more devices are decreasing, but future Internet of Things (IOT) devices may change that.

In a continuing trend, wireless increased its dominance over wired commodity traffic consumption (Figure 11).

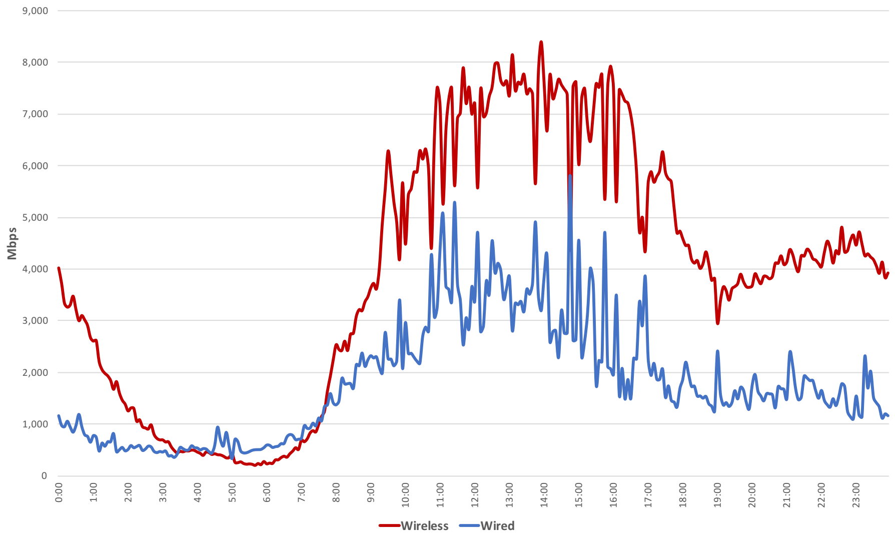


Figure 11: Wireless vs. Wired Traffic (9/2017)

RADIUS (wireless authentication) infrastructure consists of four geo-resilient servers running a locally modified version of FreeRADIUS, with busy-hour load of 666 queries per second (802.1x renewals at 16 hours). Re-architecture of the controller environment changed quarantine and bandwidth accounting methods to rely on RADIUS accounting records.This has driven higher load on the servers and will require additional resources shortly.

5GHz Trends: Devices continued to move to 5GHz frequency ranges (Figure 12 and Figure 13). This is important to promote because there is seven times the capacity available in the 5GHz range as compared with the 2.4GHz range. The 2.4GHz range had been collapsing from overload in densely populated areas (e.g., classrooms and study lounges) in years past but has stabilized as fewer clients use 2.4GHz now.

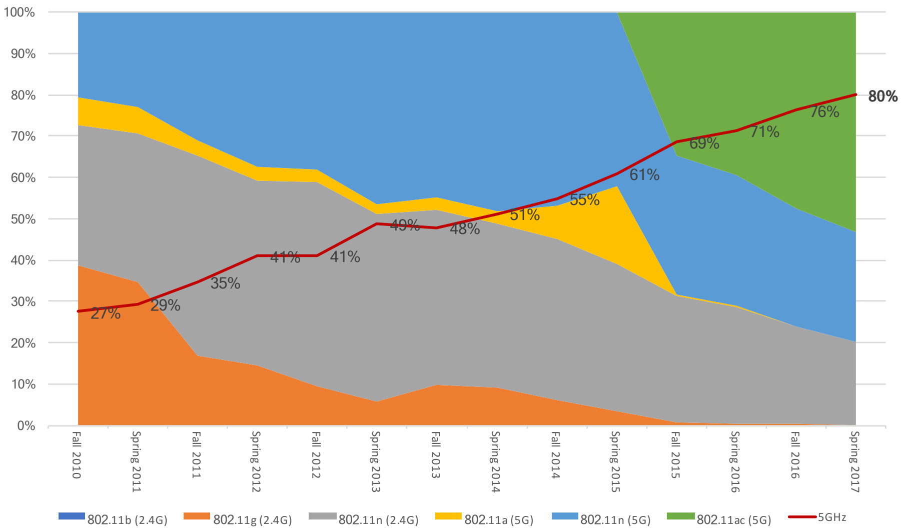


Figure 12: % Data Transfer over Frequency/Type

The IEEE's decision to support only 5GHz for 802.11ac, unlike the earlier 802.11n standard which also supported 2.4GHz, no doubt influenced the drive to 5GHz. In Figure 12, APs supporting 802.11ac-supporting APs debuted in fall of 2015, where over 35% of data transferred began utilizing 802.11ac at 5GHz. Comparatively, in 2010 when 802.11n APs were introduced (supporting both 2.4GHz and 5GHz), only 20% of data transfers utilized 802.11n at 5GHz, even though the number of APs supporting 802.11n in 2010 were higher than 802.11ac supporting APs in 2015. As more 802.11ac APs are deployed as part of lifecycle refreshes, those 5GHz percentages will continue to grow.

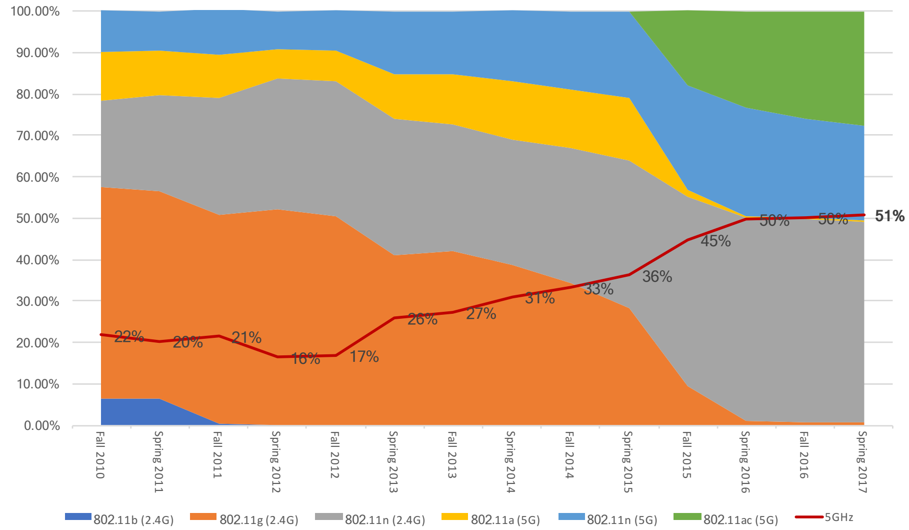


Figure 13: % Associations over Frequency/Type

Figure 13 shows flat 5GHz association growth from 2016 to 2017. This flat growth is likely related to the lack of ubiquitous coverage, especially outdoors where many active mobile devices associate without user interaction using 2.4GHz that travels further—which could additionally explain the difference between association and transfer percentages. There was also no campus-wide lifecycle program in progress during that period.

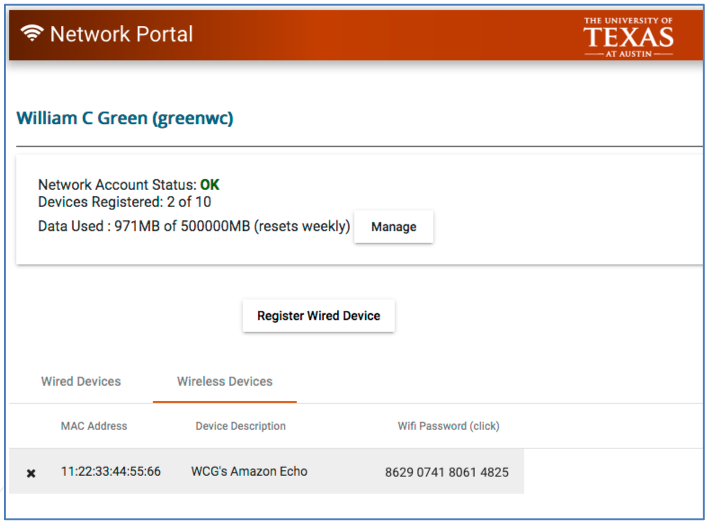
Units can provide better performance for their users by deploying the newest AP models (supporting 802.11ac wave 2). It is hoped that the forthcoming 802.11ax specification will aid dense classroom environments.

Much of the radar avoidance problem mentioned in the previous report has been mitigated, but connections are still being dropped due to false signatures in dense environments. Work continues with the vendor to identify and implement solutions, but some of the solutions require different AP hardware which is problematic when expected lifecycles are six to ten years.
New uses of unlicensed frequencies by other services (e.g., LTE-U proposed by cellular carriers) may interfere with the university's system and will be closely studied. Carriers have begun to pilot LTE-U, but there has been disagreement over coexistence test plans between carriers and the Wi-Fi Alliance to determine the level of interference between the different technologies.

Guest access: The previous agreement with AT&T for its "attwifi" network was extended. Units may acquire single or group coupons, existing AT&T customers may use the service directly and unaffiliated persons may pay by credit card for use. An open bid for similar guest services is expected during the next two years as this agreement expires. Networking has not allocated resources to research supporting additional guest access vendors via Hotspot 2.0 technology discussed previously, but continues to learn about the technology and await its maturation and better client support.

The wireless "eduroam" service is not available at the university, or for university members at other institutions. Current interpretation of the laws and policies surrounding use of state resources is that eduroam use is prohibited on university properties. Enabling university members to access eduroam at other institutions is possible, but raises support and security concerns. Those concerns could be overcome with the proper resources to secure and manage eduroam usage. Known minor support complexities would be borne by the user in the form of alternate credential methods (e.g., different passwords/accounts for eduroam or use of digital certificates).

Internet of Things (IOT): While growth of devices usually associated with Wi-Fi is slowing (e.g., laptops, cellphones, tablets), new types of devices are being created and existing devices that were not Internet-enabled are being connected with Wi-Fi. Many of those devices are not compatible with the authentication technology, WPA2-Enterprise, utilized for the university's wireless network, and only support WPA2 (a home version of wireless network authentication). Networking proposed to its vendor and has been working with them to develop a scalable and compliant approach that will support devices utilizing WPA2, with self-service unique private pre-shared keys (PPSK). Beyond new IOT devices, PPSK is expected to simplify support for many other consumer devices already in use in university facilities (e.g., AppleTV, classroom media systems, printers). It should further support a shift of devices from wired to wireless reducing network costs while increasing flexibility. Early testing is promising, but the technology is only available in early release software, which will require some time to reach stability.



William C Green (greenwc)

Network Account Status: OK
Devices Registered: 2 of 10
Data Used : 971MB of 500000MB (resets weekly)

	MAC Address	Device Description	Wifi Password (click)
✖	11:22:33:44:55:66	WCG's Amazon Echo	8629 0741 8061 4825

Figure 14: Beta IOT Portal

4.2. External Bandwidth

Availability to the commodity Internet was 99.98% year-to-date, which exceeds the SLA of 99.950% uptime.

Daily commodity inbound traffic increased by 33% from spring 2016, as graphed by 95th percentile utilization (red lines across the graph for inbound and outbound traffic flows in Figure 15).

The 95th percentile is used because long-term average and peak utilization graphs either understate or overstate the real traffic utilization rate. To anticipate traffic growth and make informed purchase decisions for increased bandwidth, a network provider needs a better measurement that reflects the utilization of most traffic flows. The 95th percentile is calculated by collecting traffic rate samples for a period of time (e.g., monthly), sorting the values from highest to lowest, and discarding the highest 5 percent (peak traffic rates) of the samples.

The average monthly 95th percentile usage rate was at 92% of the purchased committed access rate and grew 23% from 2016. Monthly growth is similar to Cisco 2016-2021 global projections, but busy hour growth trails projections.

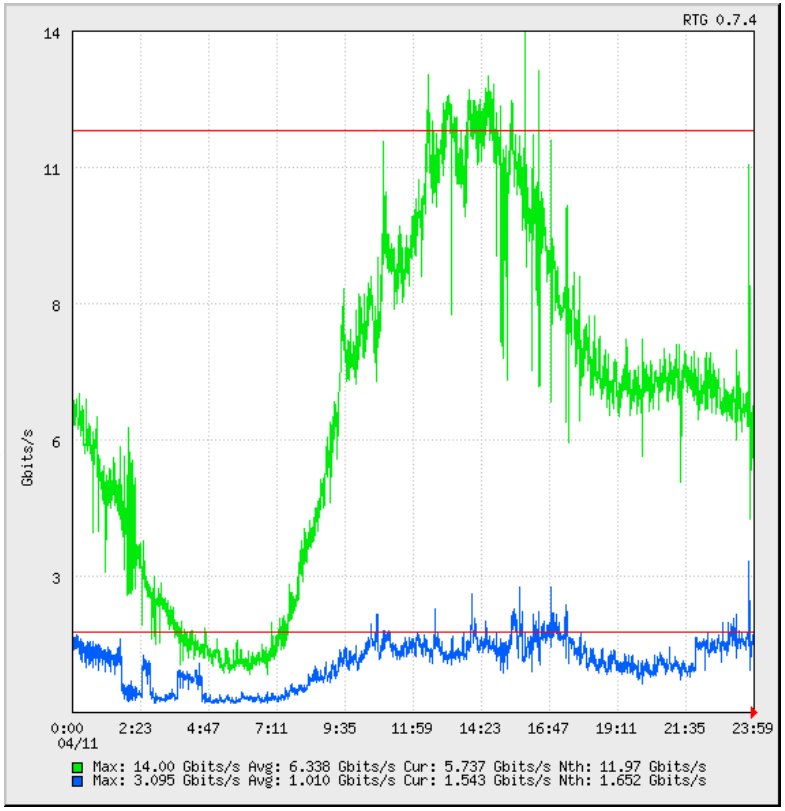


Figure 15: Busy Day Commodity Bandwidth (4-11-2017, 1-Minute Sampling)

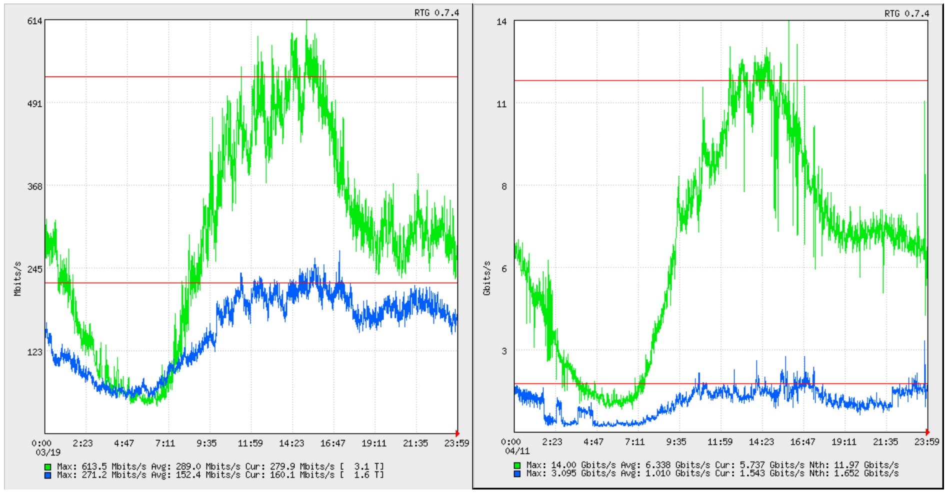


Figure 16: Busy Day Commodity Bandwidth 2007 vs 2017

Figure 16 compares consumption patterns 10 years apart. Inbound to outbound ratios increased from 2:1 to 7:1, as users continue to shift to video consumption and related activities. Consumer-oriented daily usage patterns are exemplified (university network-based devices are less relevant as a traffic provider).

Consumption for the academic year is shown in Figure 17, and reflects normal periodicity and steady growth.

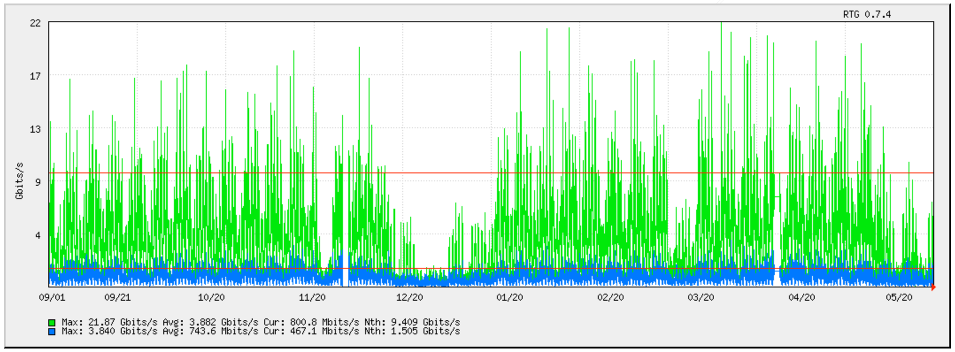


Figure 17: AY16-17 Commodity Bandwidth

Figure 18 provides sample aggregate top sources consumed, although should be taken with caution, as Content Delivery Networks (CDNs) mask true consumption levels of individual services.

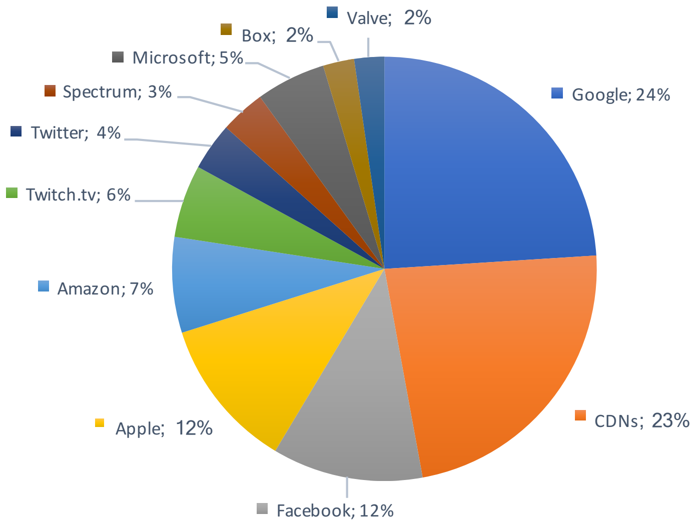


Figure 18: Aggregate Bandwidth Sources (4/1/2017-4/30/2-17)

Consumption is growing across constituencies (Figure 19). IT governance recommended continuing data consumption accounting for students, but at a higher default allocation (pending funding). Student population versus data plan consumption over time are shown in Figure 20. After exceeding their allocation, a student is moved to a network limiting connection speeds to 256Kbps per device for the remainder of the week, or until a higher data plan is purchased. Over half of students (non-employed) purchased data plans last FY. For fall 2017, non-residential data plans ranged from $4-$10 for the entire semester.

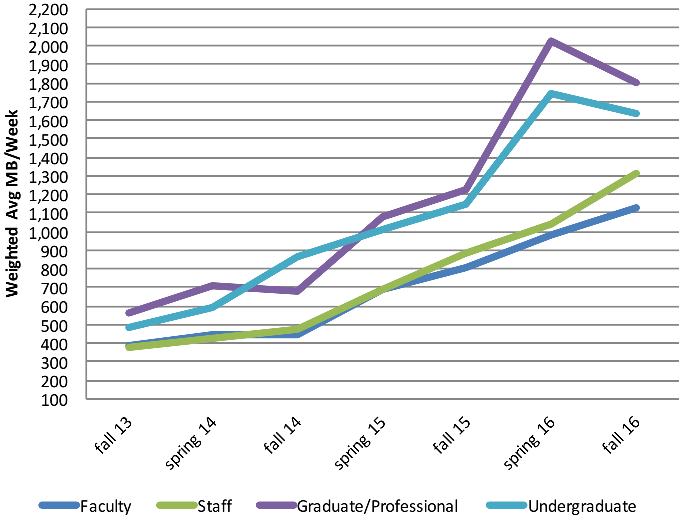


Figure 19: Non-residential Wireless Consumption

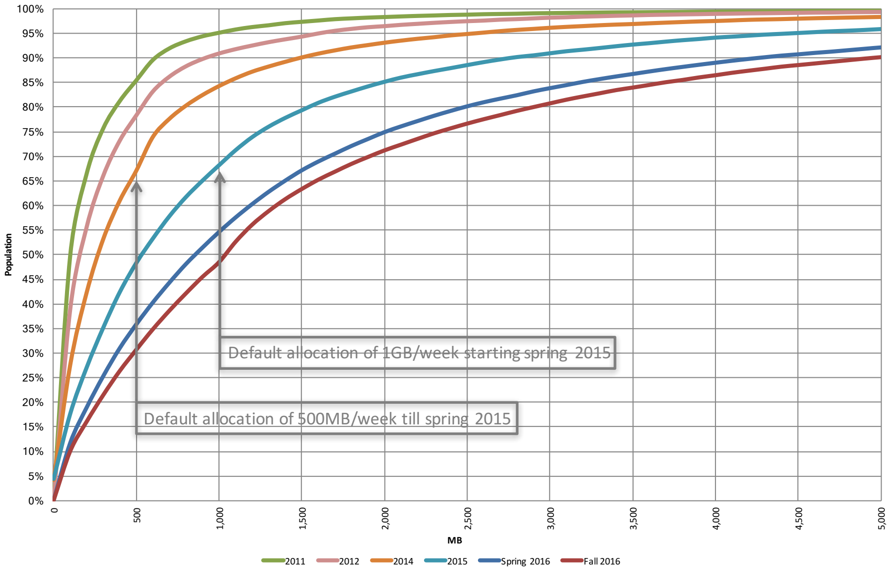


Figure 20: Student Population vs Consumption

External interconnects changed in summer 2017 from aggregated 20G links to 100G links at geo-diverse locations, provided by the UT System Office of Telecommunication Services (OTS). OTS added both Netflix and Facebook caching last year, along with peerings at regional co-location facilities to many different providers, increasing access speeds and decreasing bandwidth charges.

An aggregated 20G connection to a backup commodity Internet provider was acquired across a metro DWDM system; configured to be idle unless needed to conserve expenses. While OTS has diverse ISPs in different cities, this additional layer protects against outages within OTS's network and mitigates against DDOS attacks launched toward their other customers – both of which have caused previous outages. Figure 21 illustrates the new external interconnections.

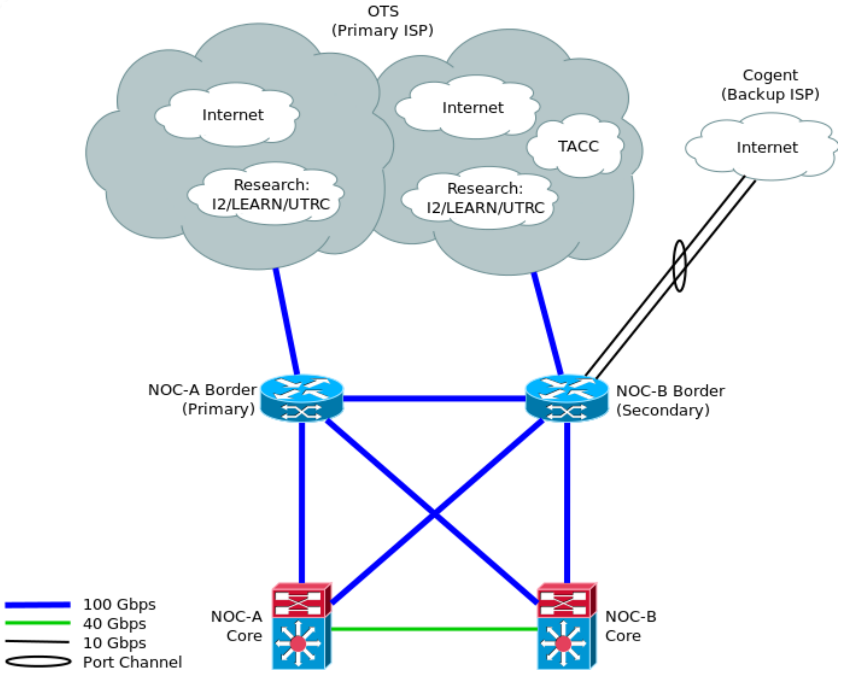


Figure 21: External Connectivity

Research Networks: The network is connected to global, national and regional research networks through its two geo-diverse 100G connections into the OTS backbone. OTS cooperates with other institutions in Texas through the Lonestar Education and Research Network (LEARN) to obtain Internet2 (I2) (100G in Houston and 100G in Dallas) and ESnet (100G in Houston) connections, along with many peering opportunities. Units may fund equipment to connect into the campus network at up to 40G to utilize these advanced services or leverage the resources of the Texas Advanced Computing Center (TACC).

TACC's external connectivity was upgraded in early 2017 to two 100G connections into the statewide networks, and one 100G dedicated circuit to research networks in Houston.

University usage of I2 is mostly related to commodity peering connections I2 implements for Net+ services, and would take commodity paths should there be no I2 services. TACC utilizes its own I2 connections, as noted, for both standard I2 routing and AL2S offerings. TACC's usage is to other I2 members primarily. Standard I2 route bandwidth consumption is shown in Figure 22 and Figure 23. TACC bursts far higher than represented in these weekly five-minute samples – having been clocked with single flows at 90G.

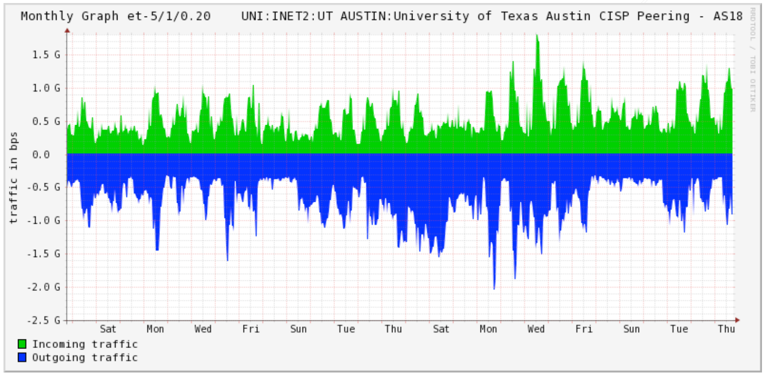


Figure 22: University Internet2 Peering (2017)

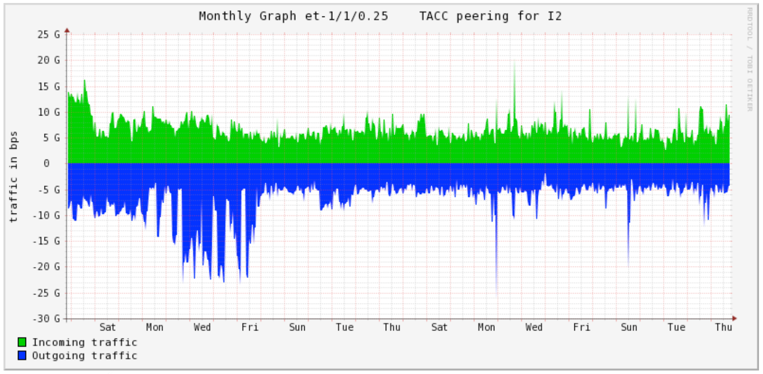


Figure 23: TACC Internet2 Peering (2017)

4.3. Device Population

Over the last year, 295,000 unique devices were detected on the university's network. Growth of devices slowed to 2% in 2017. In Figure 24, "Unit" represents wired devices on networks operated by a unit. "General" includes devices on non-unit specific networks – mostly wireless and the residential networks. There are additional devices that are not detected by our monitoring systems due to various network security measures.

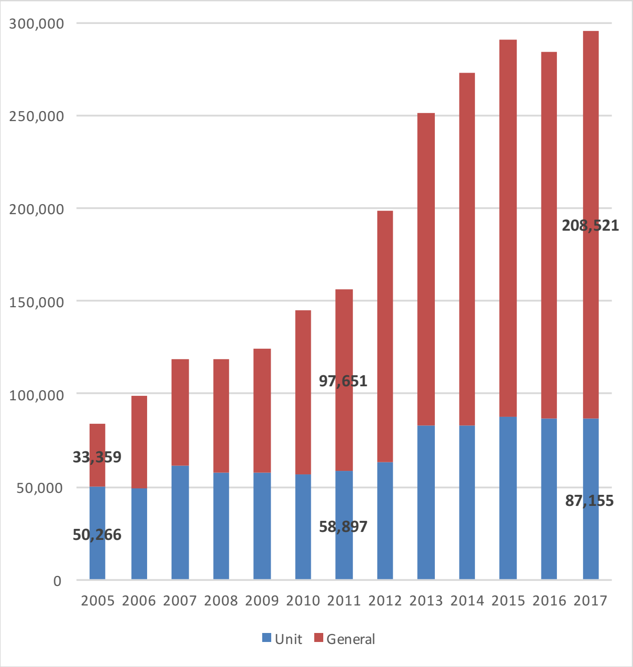


Figure 24: Devices on Network

The unit wired device population was essentially unchanged, despite a 10% increase in wired port counts since the last report. Users appear to be adopting a wireless strategy, even if units have not adjusted their investment strategy (see Wireless General Networks).

4.4. Vendor OS Population

Network signatures are analyzed to estimate the percentage of different vendors' operating systems that are in use as the devices communicate externally. While the methods employed are imperfect, at the macro scale they are believed representative for gross planning purposes.

Apple dominates wireless mobile devices, gaining 4% from the last report. For wireless traditional Operating Systems (OS) Apple sustained its majority, while Microsoft lost 2% share to Linux from the previous report (Figure 25 and Figure 26). Microsoft holds the majority for wired unit network devices but lost 5% to Linux, and 4% to Apple (Figure 27). Linux holds a double-digit share for the first time since reporting began.

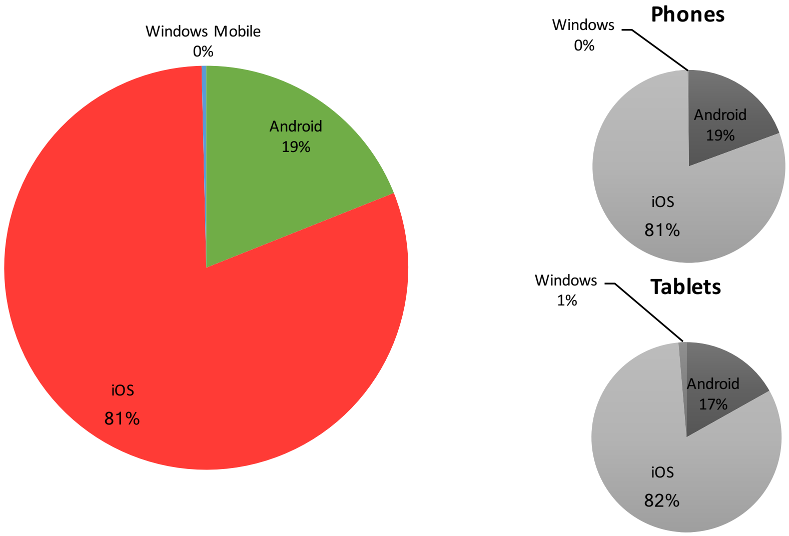


Figure 25: Wireless Mobile Device OS Vendors (Spring 2017)

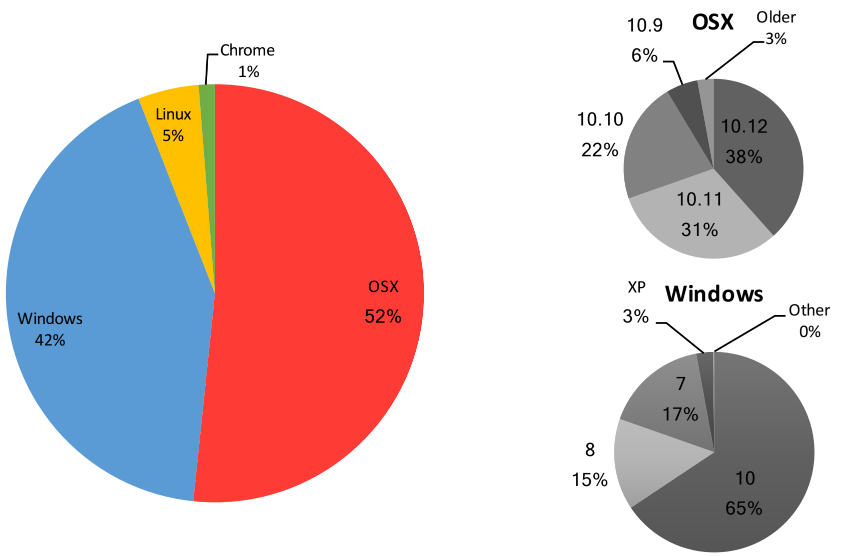


Figure 26: Wireless Traditional Device OS Vendors (Spring 2017)

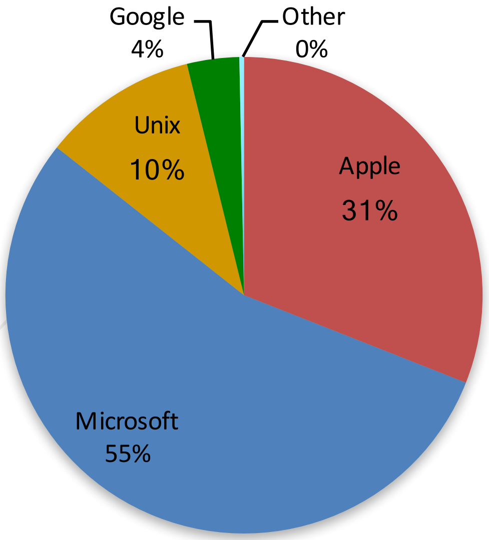


Figure 27: Wired Traditional Device OS Vendors (Spring 2017)

4.5. IP Address Management

Domain Name System (DNS) availability was 99.997% year-to-date, which exceeds the SLA of 99.980%.

Over 353,000 objects are managed in the Internet Protocol Address Management (IPAM) system (lower than the previous system's representation of 1.4 million). Transition of authoritative services to Infoblox's IPAM system was completed last year. Units may now self-manage and update their own zones in real time, and APIs were enabled for the central VMware environment to make changes as virtual machines are provisioned. Previously, tickets were submitted for staff to manually edit text files for twice-daily reloads.

Queries for the DNS caches peak at over 6,700 per second at the busy hour (Figure 28). Bind was utilized for user-facing responses in multiple geo-diverse resilient clusters which support the majority of DNS load. A project is underway to deploy additional caches operating different software as a resiliency measure. DNS lookup services are only available to devices connected directly to the university's network (following security BCPs).

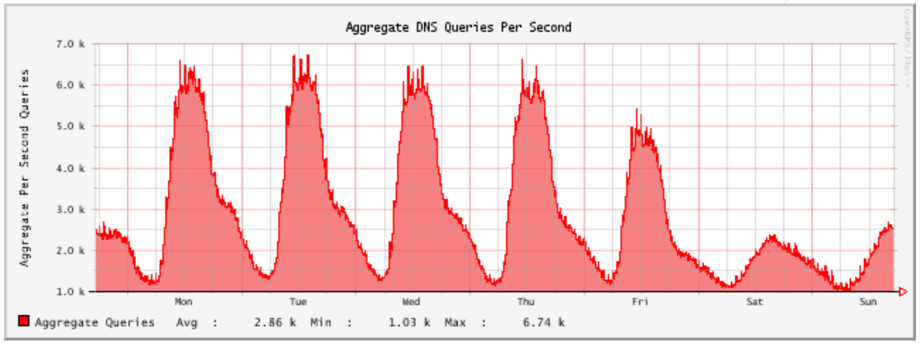


Figure 28: DNS Queries (5/2017)

Security scanning triggered firewall resource exhaustion on the caches this summer, resulting in a cascading failure reflected in availability metrics. The firewalls have been adjusted to remove this vulnerability.

Dynamic Host Configuration Protocol (DHCP) availability was 100% year-to-date, which exceeds the SLA of 99.980%.

Networking maintains separate geo-diverse resilient clusters of DHCP servers for unit and general/wireless networks using Internet Software Consortium software. 490,000 addresses are configured across the servers. Figure 29 shows typical lease activity for the wireless networks (the largest consumer/cluster).

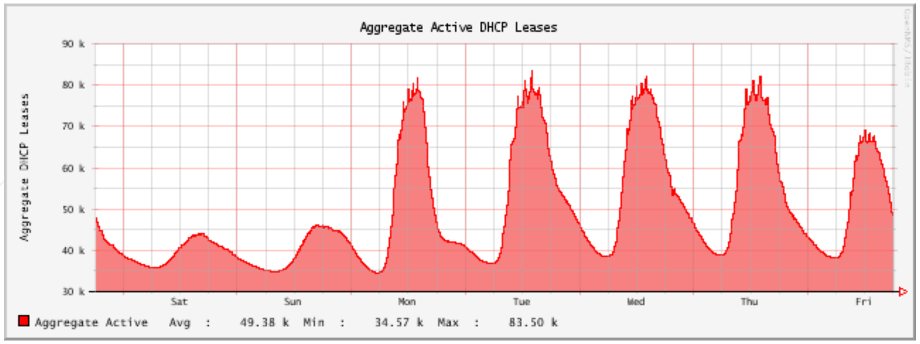


Figure 29: Wireless DHCP Leases (5/2017)

The Infoblox IPAM product has the capability for DHCP management, but it has not been enabled. Dynamic DNS (DDNS) services desired for the General Network and the ability to offer more local features (e.g., custom boot servers operated by units) may influence its future adoption.

Some units use their own DNS and DHCP servers. There are valid reasons to do so, including support for special options not offered by Networking's service. Use of local servers deprives users of centrally engineered resiliency/redundancy and may interfere with information security investigations. The Network Operations Manual requires all DNS caches to be configured to resolve through the Networking operated caching/resolver system.

4.1. Virtual Private Network (VPN)

Client VPN Services: A central client VPN service is provided to all faculty, students and staff in a split tunnel configuration. When created, the service was intended to provide access to resources restricted by university network address ranges and encryption for software packages that did not support encryption. It has also become a tool to add an additional layer of authentication and additional network isolation for system administrators.

The client VPN is lightly used compared with other network services. Utilization peaked at 480 users during AY1617. Figure 30 illustrates the typical diurnal pattern expected of locally human mediated-services.

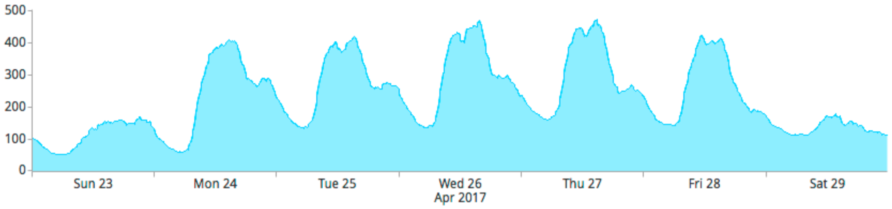


Figure 30: Client VPN Connections (5/2017)

Provided by a geo-resilient pair of Cisco ASA 5585s, the service will support up to 5,000 simultaneous SSL VPN clients, and up to 1Gbps throughput. Leadership requested the high session count to support remote access in disaster scenarios. The high session count was also desired due to the belief that a UT System mandate that all institutions utilize two-factor authentication for computer system administrator access would increase usage (that many systems would not support two-factor authentication or implementation would prove too difficult for administrators). Duo Security was selected as the two-factor method for the university, and integrated with the VPN service. There was a 25% increase in simultaneous connections from 2015, and broadening of evening access patterns, likely attributable to the mandate regarding system administrators.

IT staff should be cautious of requiring VPN use to access their popular applications. VPNs can create incompatibilities and conflicts for the end user, and add an additional layer of complexity, performance problems and failure points.

Point to Point VPN Services: As part of the Administrative Systems Modernization Project, a non-geo-resilient Cisco ASA 5585 was acquired to connect a legacy mainframe-based environment to an Enterprise Service Bus (ESB) hosted in Amazon Web Services (AWS). The ESB translates secured API calls to the legacy environment, among other tasks. The tunnel experiences frequent outages by the standards of Networking's other services – usually a result of maintenance by the ESB provider. The ESB is very lightly utilized at this time, so it is unclear if the service level is acceptable.

Requests for additional tunnels to AWS, and other providers, have been deferred pending network project prioritization or additional staff resources. For narrowly defined access to less sensitive environments, tightly restricted end user operated VPNs might be an appropriate strategy (as approved). A StrongSwan VPN operating on the central virtual machine farm was implemented for a recent high priority request, and turned over to the user's support staff for ongoing maintenance.

Best practice for cloud architectures is to use secured API calls, which are more secure and do not require these brittle VPN technologies. But until transition to fully cloud-based architectures is completed, a limited set of VPN tunnels will be necessary. A question for IT Governance will be how to encourage best practices when stop gaps like VPN tunnels are available.

4.2. Data Center Operations

Network availability for the primary Data Center was 100% for the core and 99.991% for all rows year to date, exceeding its SLA of 99.960%.

The architecture remains a stock hierarchical design (circa 2010) of a dual A/B Nexus 7010 core, dual A/B End Of Row (EOR) Nexus 5020-5596 switches (depending on purchase cycle), and dual Top Of Rack (TOR) in A/B rack pairs of Nexus 2248-2232 extenders (depending on purchase cycle). Servers must utilize LACP bonding to the A/B extenders to achieve stated service levels (which has been challenging for some operating systems). In Service Software Upgrades have been exercised on multiple occasions without impacting compliant host operations. Firewall services are provided by a Cisco ASA 5585 resilient cluster. Out-of-band networking is provided for console access with a Cisco 6840-X. (Figure 31)

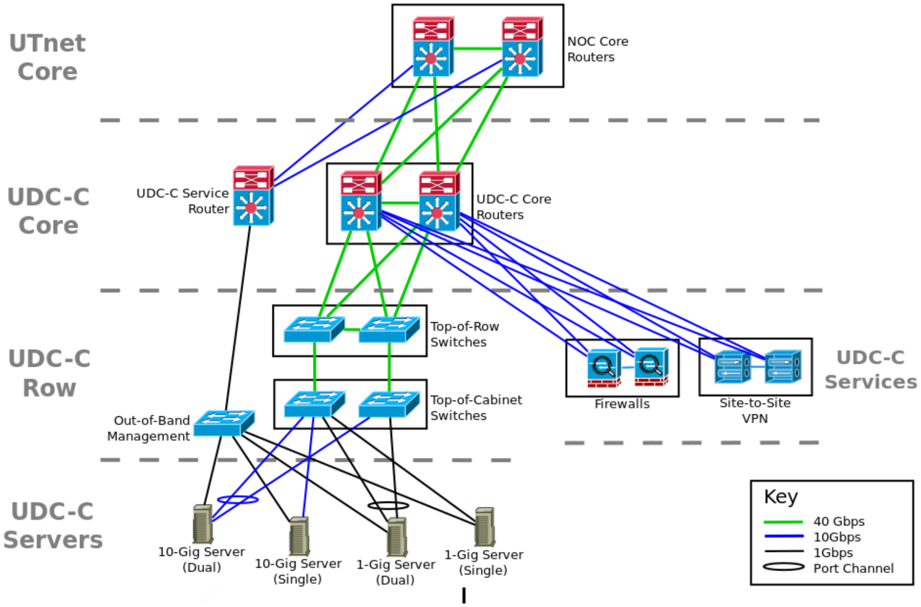


Figure 31: Primary Data Center Network Architecture

Data Center Upgrade: Lifecycle upgrade equipment was recently purchased, consisting of a design similar to 2010: Cisco Nexus 7710 A/B core, 5624 A/B EOR, 2348 A/B TOR. Core, EOR and TOR uplinks went from multiple 10G to 40G uplinks. Client links from mostly 1000Base-T to 10GBASE-T, although some 10GBASE-CX4 servers will need to convert to 10GBASE-T or move to a legacy rack supporting CX4 connections. The equipment is being installed in parallel and interconnected with the legacy network, for transitions at A/B TOR granularity daily through January 2017. Server by server impact should be limited to minutes. One brief data center-wide interruption will occur to shift routing once the plurality of devices has transitioned to the new network.

Major clients of the data center were interviewed and stated they had no need for advanced features (e.g., SDN, VXLAN, TRILL, etc.). They wanted to maintain the current SLA for both the core and rows, including link aggregation for server network resilience, despite only 25% of the servers utilizing the aggregation. This limited the lifecycle to a turn of hardware instead of a re-architecture which may have offered additional features and/or lower initial costs. It is a less disruptive transition leveraging existing staff expertise and requiring less lab/spare equipment because it is also the same platform planned for the campus core lifecycle.

Co-location: The primary data center was made a “UT System Regional Data Center” this past year, and has begun co-locating equipment from other institutions across the state system in a set of isolated racks. Institutions bring their own network equipment, and receive external connectivity from the UT System Office of Telecommunication Services transported across the university’s fiber plant.

5. Unit Networks

Units fund the cost of all network equipment and infrastructure for buildings they occupy.

Over 90% of building network equipment is co-managed with Networking, which provides complete FCAPS (ISO Telecommunications Management: Fault, Configuration Management, Accounting, Performance and Security) for these unit networks as a "common good." FCAPS are required of all networks per the Network Operations Manual.

Due to this federated funding approach, IT Governance requested Networking establish grades for buildings based on standards and report regularly to ensure units were funding their networks appropriately. The weighted average grade for unit building networks, as determined by the Building Network Report Card tool, described below, was 81 (B-), up from 74 (C) in the previous report (un-weighted grade this year was 74). Distribution of overall building grades is shown in Figure 32 and Figure 33. Smaller buildings, such as those located on the Pickle Research Campus, typically received lower grades. 84% of wired ports were in buildings with at least a C-.

While equipment was upgraded, changes in scoring methodology had more impact on the grade increase and is discussed below.

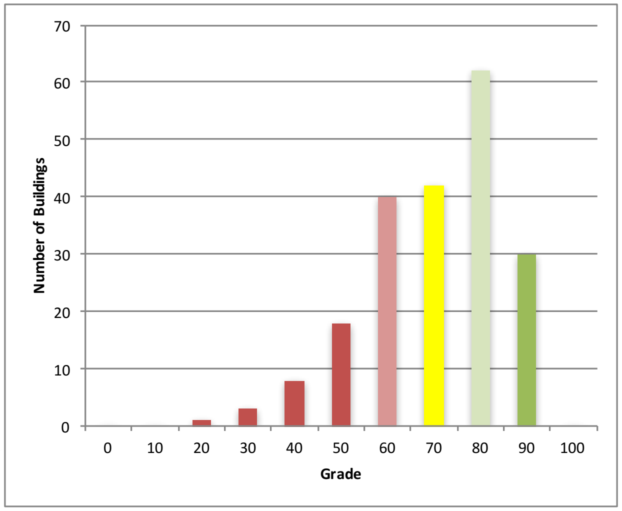


Figure 32: Histogram of Building Grades (Summer 2017)

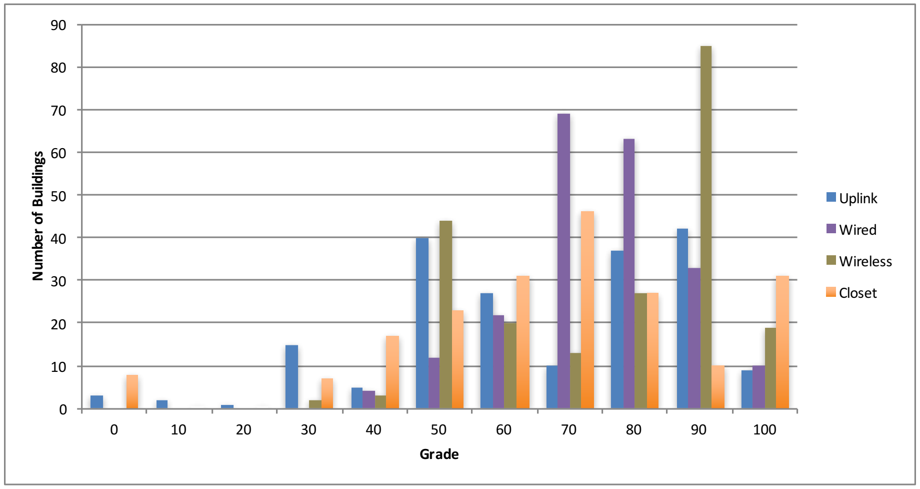
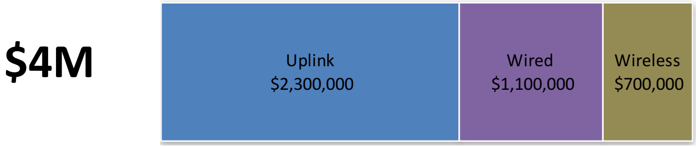


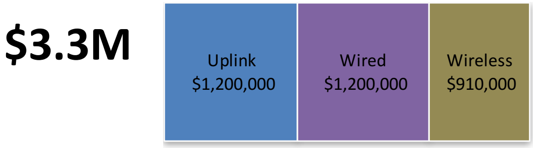
Figure 33: Histogram Building Component Grades (Summer 2017)

5.1. Recommended Investments

As of July 2017, the Building Network Report Card tool recommends equipment upgrades by units of:

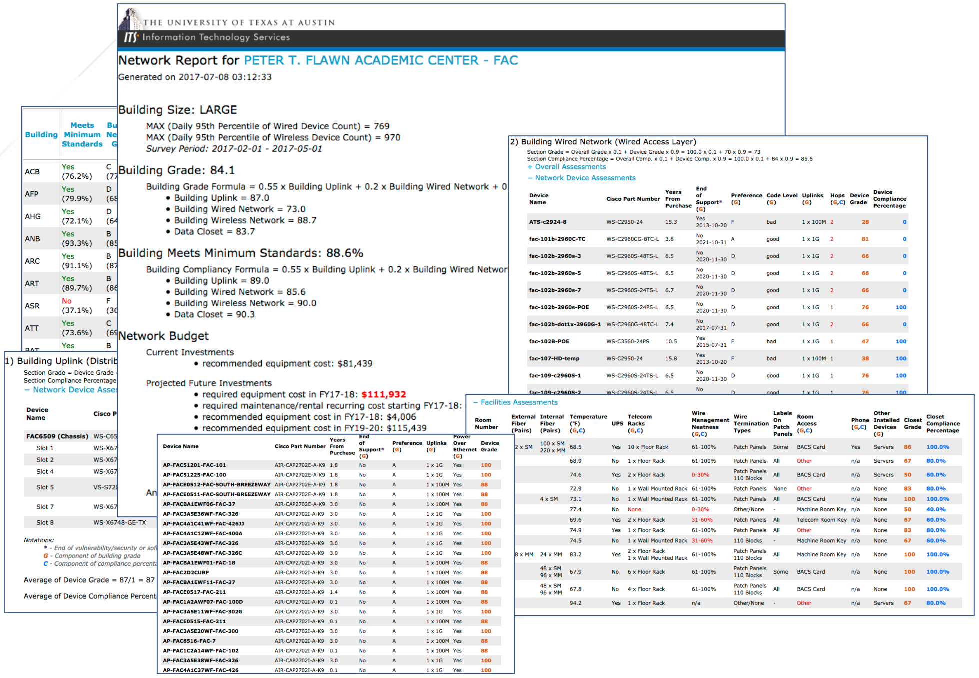


At the current network scale, it projects annualized equipment lifecycle expenses to units of:



Large swings of both deferred investment and annualized lifecycle resulted from (in order of influence):

- A community-requested change to calculate building access switch grades based on end of hardware support, as opposed to the previously used IT Governance recommended lifecycle (seven years), which reduced deferred investment of access switches by nearly $4 million. Vendor performance has exceeded governance lifecycle recommendations. Networking had previously recommended an eight-year lifecycle, not adopted by governance. Because access switches do not expose others on campus and have a small risk profile, there are no required upgrades, unlike routers. Future network security directions, typically requiring greater equipment capability (newer), may call the wisdom of this grading change into question.
- Use of non-OEM optics reduced projected annualized expenditures from previous reports by 20%. Non-OEM optics had caused outages on campus in the past. However, new and increasing use of fiber for 10Gbps uplinks of access switches, and the higher delta in 1Gbps vs 10Gbps OEM/non-OEM costs led Networking to re-evaluate and locate reliable suppliers to begin offering non-OEM optics prior to the 2015 report (software was not revised until recently). It is unlikely vendor equipment preventing use of non-OEM optics would be utilized at current price spreads going forward. OEM optics are still utilized for core and high-speed components, which there are fewer of, and where risk and impact outweigh smaller savings.
- Adoption of the shared small building distribution router model for small buildings also reduced annualized Uplink costs.



THE UNIVERSITY OF TEXAS AT AUSTIN
ITS Information Technology Services

Network Report for PETER T. FLAWN ACADEMIC CENTER - FAC

Generated on 2017-07-08 03:12:33

Building Size: LARGE

MAX (Daily 95th Percentile of Wired Device Count) = 769
MAX (Daily 95th Percentile of Wireless Device Count) = 970
Survey Period: 2017-02-01 - 2017-05-01

Building Grade: 84.1

Building Grade Formula = 0.55 x Building Uplink + 0.2 x Building Wired Network + 0

- Building Uplink = 87.0
- Building Wired Network = 73.0
- Building Wireless Network = 88.7
- Data Closet = 83.7

Building Meets Minimum Standards: 88.6%

Building Compliancy Formula = 0.55 x Building Uplink + 0.2 x Building Wired Networ

- Building Uplink = 89.0
- Building Wired Network = 85.6
- Building Wireless Network = 90.0
- Data Closet = 90.3

Network Budget

Current Investments

- recommended equipment cost: $81,439

Projected Future Investments

- required equipment cost in FY17-18: $111,932
- required maintenance/rental recurring cost starting FY17-18: $
- recommended equipment cost in FY17-18: $4,006
- recommended equipment cost in FY19-20: $115,439

2) Building Wired Network (Wired Access Layer)

Section Grade = Overall Grade x 0.1 + Device Grade x 0.9 = 100.0 x 0.1 + 70 x 0.9 = 73
Section Compliance Percentage = Overall Comp. x 0.1 + Device Comp. x 0.9 = 100.0 x 0.1 + 84 x 0.9 = 85.6

+ Overall Assessments
– Network Device Assessments

Device Name	Cisco Part Number	Years From Purchase	End of Support* (G)	Preference (G)	Code Level (G)	Uplinks (G)	Hops (G,C)	Device Grade	Device Compliance Percentage
ATS-c2924-8	WS-C2950-24	15.3	Yes 2013-10-20	F	bad	1 x 100M	2	28	0
fac-101b-2960C-TC	WS-C2960CG-8TC-L	3.8	No 2021-10-31	A	good	1 x 1G	2	81	0
fac-102b-2960s-3	WS-C2960S-48TS-L	6.5	No 2020-11-30	D	good	1 x 1G	2	66	0
fac-102b-2960s-5	WS-C2960S-48TS-L	6.5	No 2020-11-30	D	good	1 x 1G	2	66	0
fac-102b-2960s-7	WS-C2960S-24TS-L	6.7	No 2020-11-30	D	good	1 x 1G	2	66	0
fac-102b-2960s-POE	WS-C2960S-24PS-L	6.5	No 2020-11-30	D	good	1 x 1G	1	76	100
fac-102b-dot1x-2960G-1	WS-C2960G-48TC-L	7.4	No 2017-07-31	D	good	1 x 1G	2	66	0
fac-102B-POE	WS-C3560-24PS	10.5	Yes 2015-07-31	F	bad	1 x 1G	1	47	100
fac-107-HD-temp	WS-C2950-24	15.8	Yes 2013-10-20	F	bad	1 x 100M	1	38	100
fac-109-c2960S-1	WS-C2960S-24TS-L	6.5	No 2020-11-30	D	good	1 x 1G	1	76	100

Figure 34: Network Building Report Card

The Building Network Reporting tool, available to TSCs, provides a detailed analysis of a unit's networks, along with inventories, generic recommendations and rough cost estimates anytime (Figure 34). It automatically collects information about the age of building network equipment, how it is interconnected and the software it is running; then calculates the minimum requirements established in the Network Operations Manual. This year it was updated to provide multi-year budgeting data for building owners. Networking should be consulted for specific and customized recommendations.

Trends: Construction has been running at 2.6 million square feet per decade (Figure 35), much of the construction is new space needing additional network equipment (e.g., a wireless access point every 2,000 square feet for standard open office environments). $1.4 billion in capital projects are planned over the next five years. Capital projects typically fund the initial equipment acquisition, but lifecycle equipment costs come from the units' operating budgets.

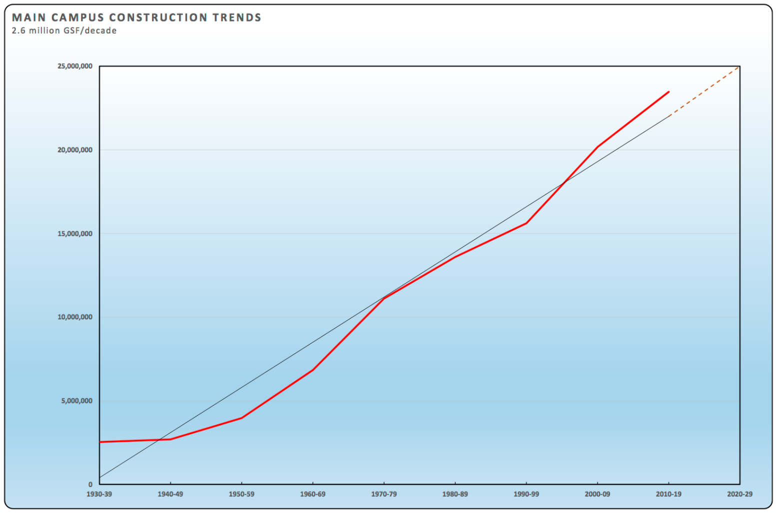


Figure 35: Capital Construction Trends

There has been no corresponding central funding for additional network staffing to support the units with these square footage increases or other documented growth. Networking has created "service centers" to charge for enhanced offerings, such as MPLS VRFs, so that it can acquire staff and provide an outlet for units requiring more than is available through central funding. Additionally, Networking is re-prioritizing efforts to automate functions and is withdrawing customizations that are not scalable or cost justified. It also utilized its VoIP migration to create a new Site Networking group to focus on unit moves, adds and change, combining staffing functions. Future strategies are noted in the sections below.

5.2. Building Uplinks

There were 187 point of presence devices utilized to connect buildings to the network. The Network Operations Manual minimums require current vendor support, dual uplinks, at least 1G in speed, and routing for building networks. Upgrades require 10G for on-campus sites. Recommended age for uplink equipment is less than 8 years. (Figure 36)

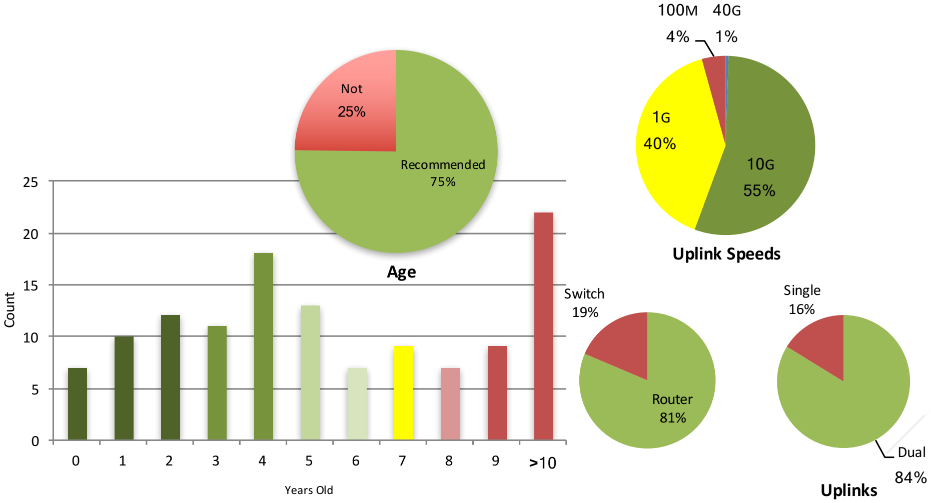


Figure 36: Building Uplinks (8/2017)

Buildings not meeting the minimums are generally small or auxiliary units. The deferred investment to meet requirements and recommendations is $2.3M across all buildings.

Off-campus locations are exempted from on-campus connection speed criteria and typically uplink via leased 100Mbps service (seven of the ten 100Mbps sites shown in Uplink Speeds in Figure 38).

Out of Support: Units were not maintaining lifecycle funding of their routers. In 2016, nearly 70 buildings lacked vendor support, leading to an IT Governance task force to review how the university's federated funding and network model was working. Networking has worked with units to narrow that support gap to fewer than 11 buildings since that time and will be forced to drop connectivity for any sites unable to maintain a supported platform. The task force had been exploring a third-party review of efficiencies and costs obtained from central operations before larger central IT funding issues paused the effort for an overall IT analysis by the newly formed Central Information Technology Executive Committee (CITEC).

Networking recommended to CITEC that uplinks be funded centrally because there was little for units to optimize. Routers are selected and operated solely by Networking. Underinvestment by any single unit impacts all other units should the device be compromised. With the preeminence of wireless, which relies on the uplinks, all users suffer from underinvestment by any unit.

The shift of small buildings from a CAPEX to OPEX rental model helped greatly in bringing buildings into support, and ensures stability and predictability for units in the future. (Figure 37)

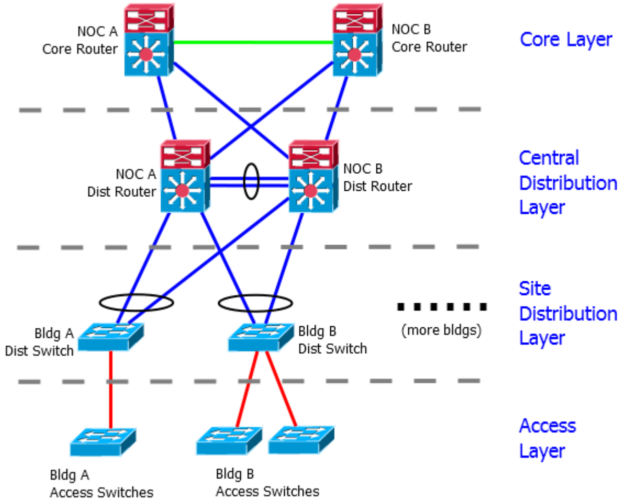


Figure 37: Shared Small Building Distribution Router

5.3. Building Wired

There were nearly 3,400 access switches connecting wired computers and other equipment to building networks, a reduction from previous reports as older 24-port switches were lifecycled to more cost-efficient 48-port models. Minimums require at least 100Mbps wired port speed for end-user equipment (being met across the university) and recommends a switch age of less than eight years (Figure 38). Equipment has been functioning beyond anticipated lifecycles, however, the slower/older equipment lacks features, experiences more frequent failures, and may be limiting higher bandwidth application performance. For example, equipment older than eight years cannot participate in the wired General Networks discussed below.

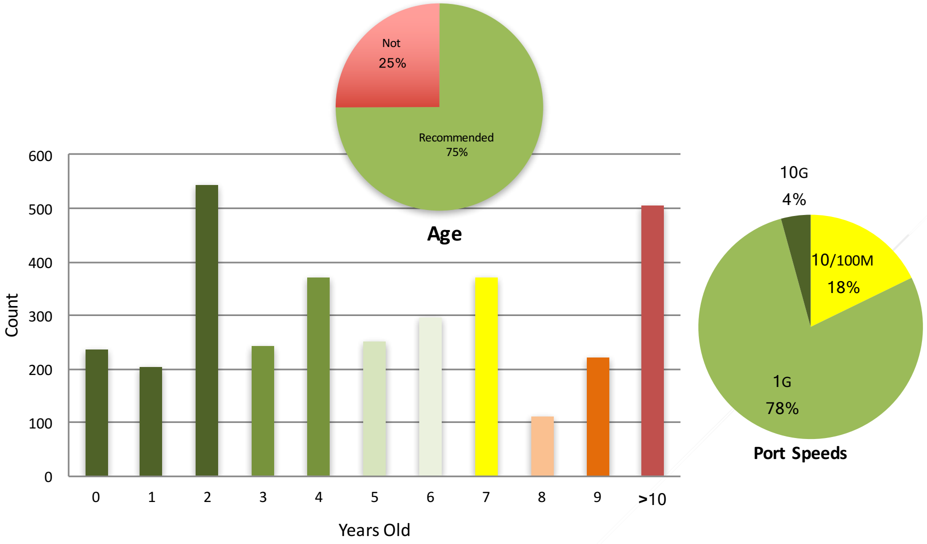


Figure 38: Building Wired Equipment (Summer 2017)

Access switch model by share are shown in Figure 39.

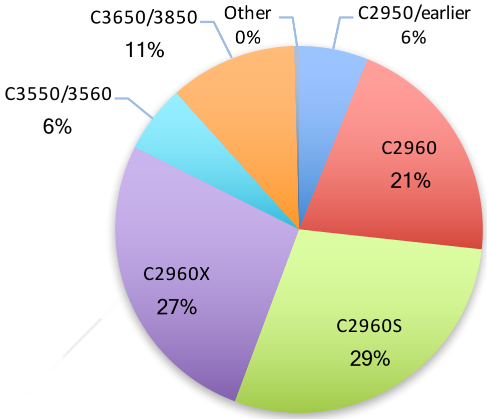


Figure 39: Access Switch Models (Summer 2017)

There were over 194,000 wired Ethernet ports at the university (inclusive of infrastructure ports, like those used to connect to wireless access points or interconnect network devices). The trend line in Figure 40 shows the total wired ports deployed yearly by Networking, inclusive of both new ports and lifecycled ports. This port count was a 10% growth from the last report. New ports in 2017 were mostly a consequence of new building construction for the Dell Medical School, lifecycle of older POE switches required to meet higher power requirement of the new access points, and refresh of the data center equipment.

Port utilization was monitored at approximately 42% over a 90-day period (down from 47% from the last report). Units could save on equipment lifecycle costs by pruning unused but patched ports and eliminating switches when possible (utilization goal is 60%).

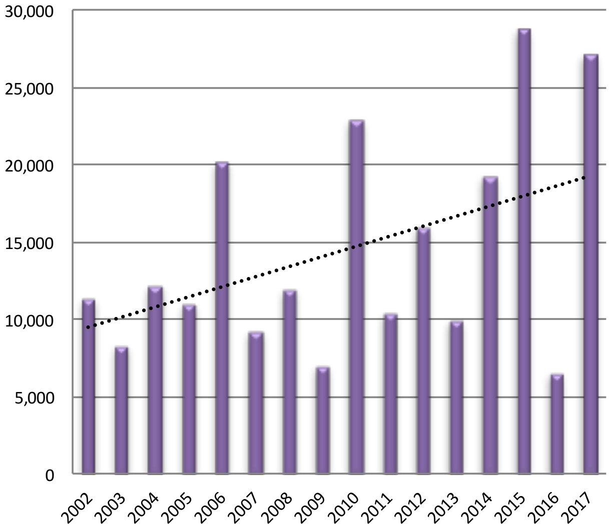
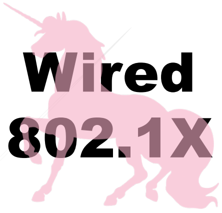


Figure 40: Wired Ports Acquired by Networking

Wired 802.1X: The third generation of wired 802.1X was successfully deployed in the residential networks in the summer 2016. Key differences from earlier efforts:



1) Access Control Lists were applied to ports in differing Extensible Authentication Protocol states instead of changing VLANs (fewer port toggles and no IP changes for the host or services managing the host).
2) A web redirect final state was added, directing unencrypted web sessions to a MAC Address Bypass (MAB) registration portal. Security concerns with MAB (any user masquerading as another using Ethernet Media Access Control addresses), were ameliorated by binding the user ID, MAC and switch port tuple in the RADIUS backend (local FreeRadius modifications including auto-detection/learning of the MAC address and port).
3) A lifecycle upgrade of remaining residential switches supporting these features made it possible to deploy this system in the residential network, which is considered a support and security hostile environment. While most residential users connect via the wireless system (802.1x only), 25% still registered a wired port (e.g., gaming system, hi-end desktop)—mostly via MAB. Relatively few support calls were generated. Across the rest of the university, 88% of access switches will support this third generation.

Issues with 802.1x include: Windows platforms have poor wired 802.1x support, requiring installer software or deployment of Group Policy Objects (manual configuration is not realistic for a typical user), encounter occasional disruptions from some operating system upgrades, and difficulty returning from sleep. MacOS platforms have 802.1x configured by default, and while working generally well, sometimes experience delays in authenticating when returning from sleep (related to the operating systems use and activation of Ethernet dongles; and switch timeouts configured while attempting to supply both 802.1x and MAB functions).

Issues with MAB include: switch-based web-redirects being a slow experience for end users (20–120 seconds depending on browser and operating system-- related to encryption of the web in general and browser specific behaviors); casual use of Ethernet dongles with equipment lacking Ethernet ports (and therefore associated MAC addresses) breaking the desired binding of device to user.

Of the two approaches, MAB has been the end-user preference. No platform-specific configuration is needed, and performance is consistent.

Wired General Network: 802.1X/MAB technology was configured on 76% of departmental access switches this summer in an attempt to bring the benefits of the Wireless General Network to the wired environment (the remaining 12% of supporting switches will be configured later in the fall). Unit support staff may choose their level of participation.

Attributes consistent with the wireless General Network include:

1) For end users, no technical support is required, activation is instant, and in many cases transparent. Yielding increased user satisfaction and decreased local support time (less technical capability from support staff required). Consumerized.
2) No sensitive networks are exposed accidentally, usage is assigned to a university operated network/address space (not a unit's space).
3) Use is authenticated, and pre-authorized as a "birthright" for the university community, just as wireless. Ubiquitous.
4) Identity/usage is registered and available for security processes.
5) Ports are automated and updated in mass with single policy.
6) Default network security is applied. Initially Network Address Translation at the border of campus. To be funded centrally with a reducing perimeter over time.

Strategically, this is one part of Networking's attempt to change population and compliance cost curves (Figure 41). **<u>Put simply, shift devices to a consumerized model as the rest of the world has already done</u>.**

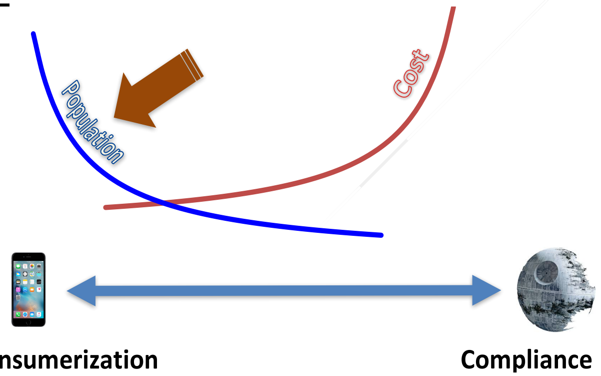


Figure 41: Shifting Cost Models

Compliance continues to increase network complexity and cost. Compared with commercial business networks, the university lags and can expect further requirements imposed. Many units operate their networks as they did a decade ago, and their funding models do not support moving large device populations to an increased network security posture based on traditional network deployment approaches. Networks are brittle (expensive, long lifecycled, hardware-focused, requiring esoteric knowledge).

For users, information technology has become consumerized. Key applications have moved to the cloud (e.g., email, storage, course management) and made mostly self-service. University work is accessed most often outside the local unit network or other university networks. Security necessarily moved to the application layer (where it could always be more effective). Many of the reasons for network policy and security applied at the local network due to locally hosted applications no longer exist.

Networking advocates the obvious: shifting the majority of devices to a consumerized model, the General Network, which is very similar to a home network (with scaling and compliance). Networking did that with the Wireless General Network years ago, and now plans to do it with most of the remaining wired device population, which only represents a third of the devices on the networks. Automation, as offered through this approach, is the only remaining viable option to scale to meet current and future demands at desired investment levels.

Compliance and security is and always will be important. The General Network already has more security than the majority of unit networks, implemented in a transparent manner. Moving the majority of unit devices to the General Networks would provide those devices automated, consistent, and compliant security.

Many units end up with little to no network security or insufficient security for the sensitive devices. Networking proposes new "Fortified

Networks," with enhanced network security for devices requiring it. More could be spent (time/funding) on those security-sensitive devices because there would be fewer of them, and less spent for the plurality of devices on the General Network. There would be a remaining set of wired devices that would most appropriately be kept on wired networks as traditionally operated "Legacy Networks."

Barring additional findings from unit pilot tests of the Wired General Network, Networking is expected to begin requiring usage in all non-secured spaces, and, driven by audit findings, to many secured spaces as well, as called for in the Network Operations Manual (with appropriate governance review).

Wireless General Networks: Additional efficiencies could be achieved by shifting more wired devices to the wireless General Network (again, as most of the rest of the world already has). Fewer cables to install, less wired network equipment to lifecycle, and increased flexibility. Wireless investment is a given. Re-enforcement of wireless infrastructures is also a given for most units, whether budget realities have caught up. The advent of 802.11ac has increased performance and reliability of wireless networks to a level that is sufficient for the majority of activities.

Over $1 million per year in annualized wired network expenses could likely be avoided if just 50% of current wired devices were gradually shifted to wireless (inclusive of equipment, cabling, labor, electrical etc).

These changes would not be effort or cost-free, and there are reasons units have not moved already (though many of their users have). There are decades of technical debt and operational culture around the legacy networking model. Workstations would need to be managed differently, but many of those changes are long overdue as users have shifted to a more consumer and wireless model of operating. Central services are needed (e.g., printer servers, RDP gateways, boot servers).

The growth of the network (discussed in this report) and flat or declining staffing have also been impacting the units, and their ability to invest in new efforts. Networking has observed unit technical capabilities have been decreasing, and elimination of funding to train them has resulted in a decline in the ability to support the local networks. Moving the entire university quickly to General Networks would require additional resources at the unit level (e.g., as was done with the VoIP deployment contractor) or institutional prioritization – likely both.

Networking has made the General Network, both wired and wireless, available for units that are able, and believes the time invested will pay recurring dividends in lowered support cost, increased user satisfaction, and increased security and compliance. As part of its CITEC recommendations, Networking proposed wireless be funded centrally as a "common good," and that "Legacy Network" ports incur a charge to encourage more efficient and effective university operations.

5.4. Building Wireless

Approximately 7,800 wireless access points (AP) connect student, faculty, and staff wireless devices to building networks. All APs meet current minimum requirements (802.11g), but not age recommendations (five years – see Figure 42). Unlike traditional wired equipment, once a wireless access point is no longer supported by the vendor, it ceases to operate due to the central controller architecture used by most of the industry. Over the last decade, the university has obtained 5-10 years of service from an AP depending on when it is purchased in the model's lifecycle. AP lifecycle alone costs $966K/year for units (see more W*ireless Costs* below).

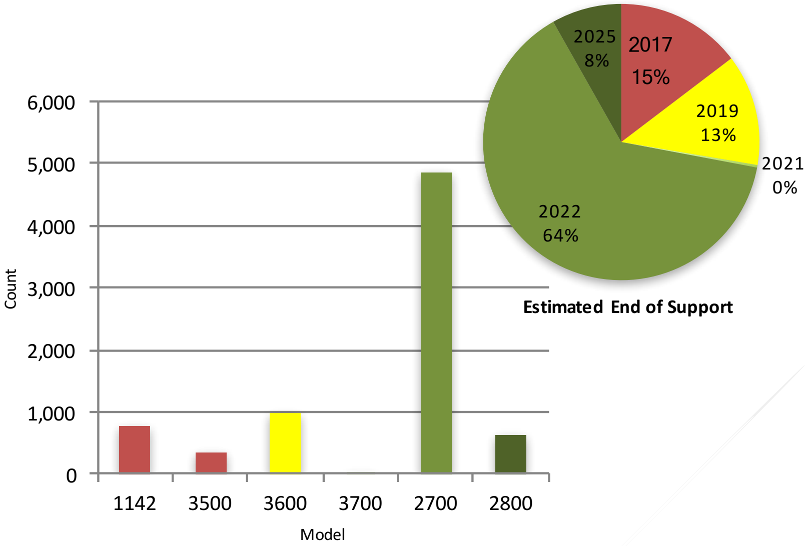


Figure 42: Building Wireless Equipment (7/2017)

AP upgrade program: In fall of 2016 a special program was offered to replace Cisco 1142 and 3500 models (23% of inventory at the time). Figure 42 reflects inventory in July 2017, when just over half the new Cisco 2800s replacing the older models had been swapped out. Beyond support, the newer APs provided 200% increased throughput over the older units being replaced in testing.

Nearly one hundred older APs were not upgraded by units planning to move their offices. The future unit occupying the space will incur a higher cost of replacing the unsupported APs outside the special program (one of the many costs of a decentralized infrastructure).

Power Over Ethernet (POE): The upgrade program was more difficult than previous ones, because the increased power draws by the new APs required coordination with POE switch capacities. Most of the problems encountered were with POE+ switches which had enough power on a given port but insufficient power across the switch to drive the number of newer APs connected. When possible, ports were rebalanced with lower requirement POE devices (e.g., VoIP phones) throughout a closet to delay switch upgrades. Federated operations created problems with port allocations (units utilized ports reserved for the project), and may portend future wireless stability problems as federated staff move devices leading to AP outages. During the program, units were presented with both POE+ and Cisco's UPOE options to provide more capacity and some future proofing against increased power by newer AP models (40% selected UPOE). Very few data closets required electrical upgrades to date (proactive or reactive), which had been feared. A more expensive option rejected by the general community was dedicating switches to APs and maximizing electrical sources for those dedicated switches to their full potential draw.

Variable power consumption of POE switches has complicated data closet power management because it can vary by a multiple of 15 (e.g 70 watts for the smallest models up to 1,100 watts for other models, with new standards to push even higher). Before the widespread adoption of POE, a closet with 10 switches used to require under a 1,000 watts of electrical draw; in the future that could range to 11,000 watts and higher. Most data closets were not designed to handle those kinds of electrical or cooling loads (understanding much POE heat occurs at the end device). How will POE electrical requirements be managed as the number and type of POE devices continue to increase?

Networking purchases equipment with power management capabilities, however, the rest of the electrical system lacks that intelligence. Intelligent electrical systems are sold but not typically implemented at the university due to their expense, and there is no mechanism to allow a POE device, such as an AP, to negotiate with the generator of the electricity. Instead, rough industry guides are used for loading. This leads to outages when breakers trip due to overload from the last POE device connected or from any device dynamically changing its consumption.

Wireless Costs: Annualized unit and central costs are presently $2.8M/year. All MO&E for an AP to be functional is broken out in Figure 43**.** Since the last report, Power Over Ethernet (POE) increased from 8% to 17%. Fifty-one percent of costs are born centrally as a "common good."

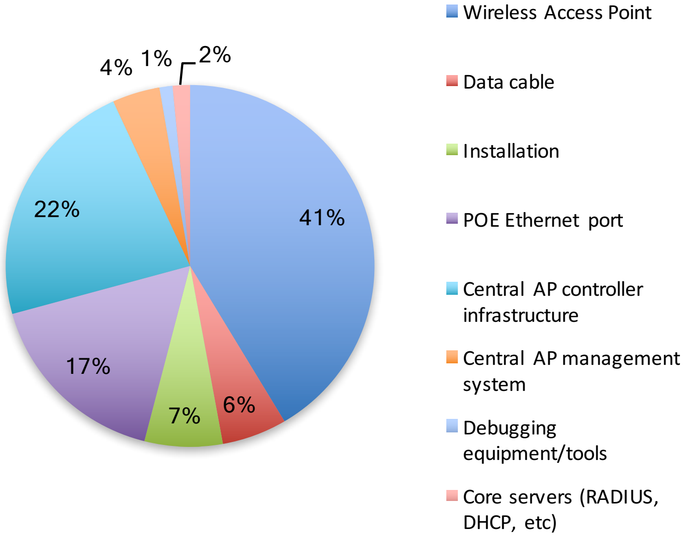


Figure 43: Annualized Wireless Access Point Costs (5/2017)

When accounting for total wireless costs, units are now spending $1.4M on lifecycle— more than their projected spend on wired network lifecycle. Yet the task is not complete. Coverage models indicate 77% of the equipment needed to meet desired density and quality levels has been installed. An additional $3.3M one-time spend is projected to meet density goals for general building spaces, leading to $3.7M in lifecycle expenses (unit and central, or $1.8M unit) when done.

A separate estimate for high-density coverage in all classrooms projected $5M in remaining investments, although there is substantial overlap between the two figures (likely under $6M for both building and dense classroom coverage).

Classrooms pose a challenge to the federated funding models because most classrooms do not belong to units, rather are "general use." Units in principle agree to fund lifecycle technology costs for classrooms in buildings they occupy, but not initial installation. Large classrooms are difficult to provide stable wireless at full occupancy unless properly designed. No additional funding was provided to expand coverage in large classrooms since the last report (the Provost previously funded 8,800 large classroom seats). Complicating large classroom matters, units operating the database of classroom capabilities listed all classrooms as having wireless coverage based on sampling for signal for some number of rooms. Networking objected that this did not account for density. In large rooms, it could set incorrect expectations of room performance for faculty and impact instruction (only a small portion of students could use wireless). Specific rooms were identified that would fail as examples, but the group continues to list all rooms as having coverage with no provisos.

Outdoor coverage is also sparse, because like general purpose classrooms, no unit owns outdoor space. Units are only required to provide coverage adjacent to their building. Some mobile devices do not perform well in this environment, holding on to weak signals when passing buildings instead of moving to cellular data networks (the university has an outdoor Distributed Antenna System providing adequate outdoor cellular coverage). Networking leverages limited funding from other infrastructure projects to add wireless coverage to popular areas when possible (e.g., use of Emergency Call Towers and cameras).

DAS and Wi-Fi Calling: In fall of 2015 "Wi-Fi Calling" was adopted in lieu of indoor Distributed Antenna Systems (iDAS) as the cellular phone coverage strategy for the majority of indoor spaces. All major carriers and smartphones now support the feature. iDAS cost $3-$5/sq ft and are generally not funded by carriers. At $30M-$80M to cover university indoor spaces with iDAS, assuming carriers would participate with base station equipment, Wi-Fi was clearly the more economical and higher performing option. iDAS are still appropriate for venues serving large numbers of public patrons (e.g., arenas). The university continues to work with carriers on expanding and enhancing the outdoor DAS and expects the advent of outdoor small cell systems to further increase outdoor and indoor coverage.

Safety: The university created a safety campaign encouraging students to call 911 in preference to mobile safety applications. The phone calls enable interaction with 911 operators to verify location and make better assessments of the situation. Carriers report they are beginning to use Wi-Fi location services on some devices and operating systems to improve locations reported to 911. A concern raised is that some students turn Wi-Fi off on their devices in the belief that it conserves battery (this is especially true in areas of poor Wi-Fi coverage). Besides creating location inaccuracy, turning off Wi-Fi also disrupts the ability to utilize Wi-Fi Calling inside buildings to place 911 calls.

A study by the Electrical and Computer Engineering department ["Location Based Safety Apps Testing", by Zhang, Edelman, Lu, August 2016] found phones with Wi-Fi-enabled outperformed phones with Wi-Fi disabled in location accuracy. Figure 44, from the study, shows lines drawn from the sample points to reported location when Wi-Fi was disabled.

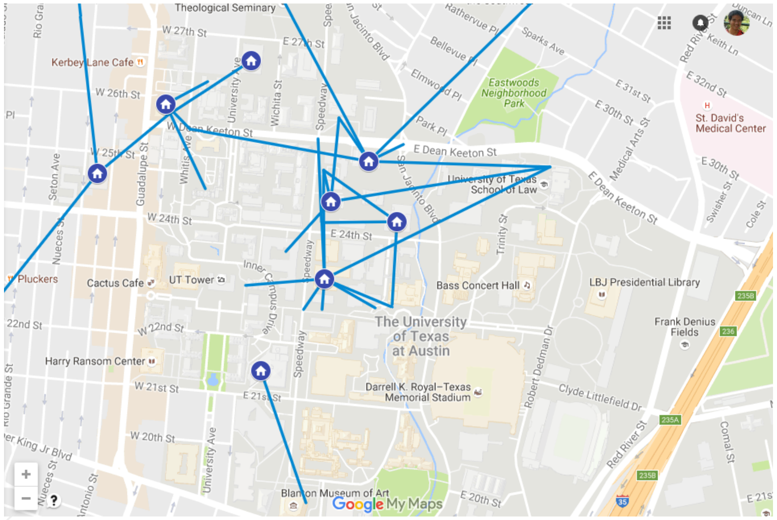


Figure 44: Location Variance with Wi-Fi Disabled

It also reported Wi-Fi density and construction materials' impacted accuracy; new APs were picked up quickly by location databases, but changing existing AP locations was slower to be updated with new locations; less accuracy was reported on higher floors; and transitions from indoor to outdoor could be problematic, with densely covered buildings outperforming sparse buildings. Discussions are ongoing regarding funding for additional Wi-Fi coverage along popular walking paths and high-use student spaces with sparse coverage to increase location accuracy and for making 911 calls.

Future coverage: Networking continues to advocate, as it has with CITEC, that wireless coverage should be centrally funded. As a "birthright" service, wireless supports all students, faculty, and staff – not just the unit occupying a particular building or space. There is little opportunity for a unit to fund wireless more efficiently given the goal of full coverage, and few optimization choices that can be made by a unit due to the need for ubiquitous operations across campus. Smaller units find it difficult to budget for the lifecycle expenses that now exceed their wired network expenses (even with the projections provided in the Building Report Card).

Due to the federated funding of wireless, there is no specific plan to provide desired coverage levels, and it is likely that users will encounter locations where wireless does not function well, or at all.

6. Overall Costs

Inclusive of equipment, maintenance, staff, operations and bandwidth, the cost to operate the network is estimated to be $14 million following governance recommendations. This 11% reduction from the last report is a combination of savings and changing models, referred to earlier, and increase accuracy of expense projections.

The amount does not include costs such as electrical/mechanical, space or cabling. Figure 45 shows this cost by various metrics (such as port counts).

	Annualized Network Cost Metrics Divisor:							
	Gross SqFt	Faculty & Staff FTE	Student	All Headcount	Ethernet Ports	Devices on Unit Networks	Devices on General Network	All Devices
Central Costs	$ 0.35	$ 419	$ 165	$ 119	$ 44	$ 98	$ 41	$ 29
Decentral Costs (in-building)	$ 0.20	$ 234	$ 93	$ 67	$ 25	$ 55	$ 23	$ 17
Total	$ 0.55	$ 653	$ 258	$ 186	$ 69	$ 153	$ 64	$ 46

Figure 45: Annualized Network Cost by Different Metrics (8/2017)

7. Looking Forward

7.1. Recommendations

- Invest in the $4M of deferred network maintenance
- Shift the compliance and cost curves by moving more devices to consumerized networks:
  - Wireless General Network
  - Wired General Network
- Save funds by moving more devices to wireless and reducing wired port counts
- Introduce Fortified Networks for devices with high security requirements to focus attention and resources
- Extend wireless coverage where insufficient, and invest in newer APs (802.11ac) to improve end user performance
- Centralize funding for buildings uplinks and building wireless

7.2. Future Activities

- Migration to new primary Network Operations Center
- Lifecycle of network core equipment
- Lifecycle of core NAT equipment (future reduction in perimeter sizes)
- Network upgrade for primary data center
- Encourage use of new Wired General Networks
- Complete MPLS deployments
- Per User Pre-Shared Key (WPA2) support on wireless for IOT devices
- Upgrades to network management systems