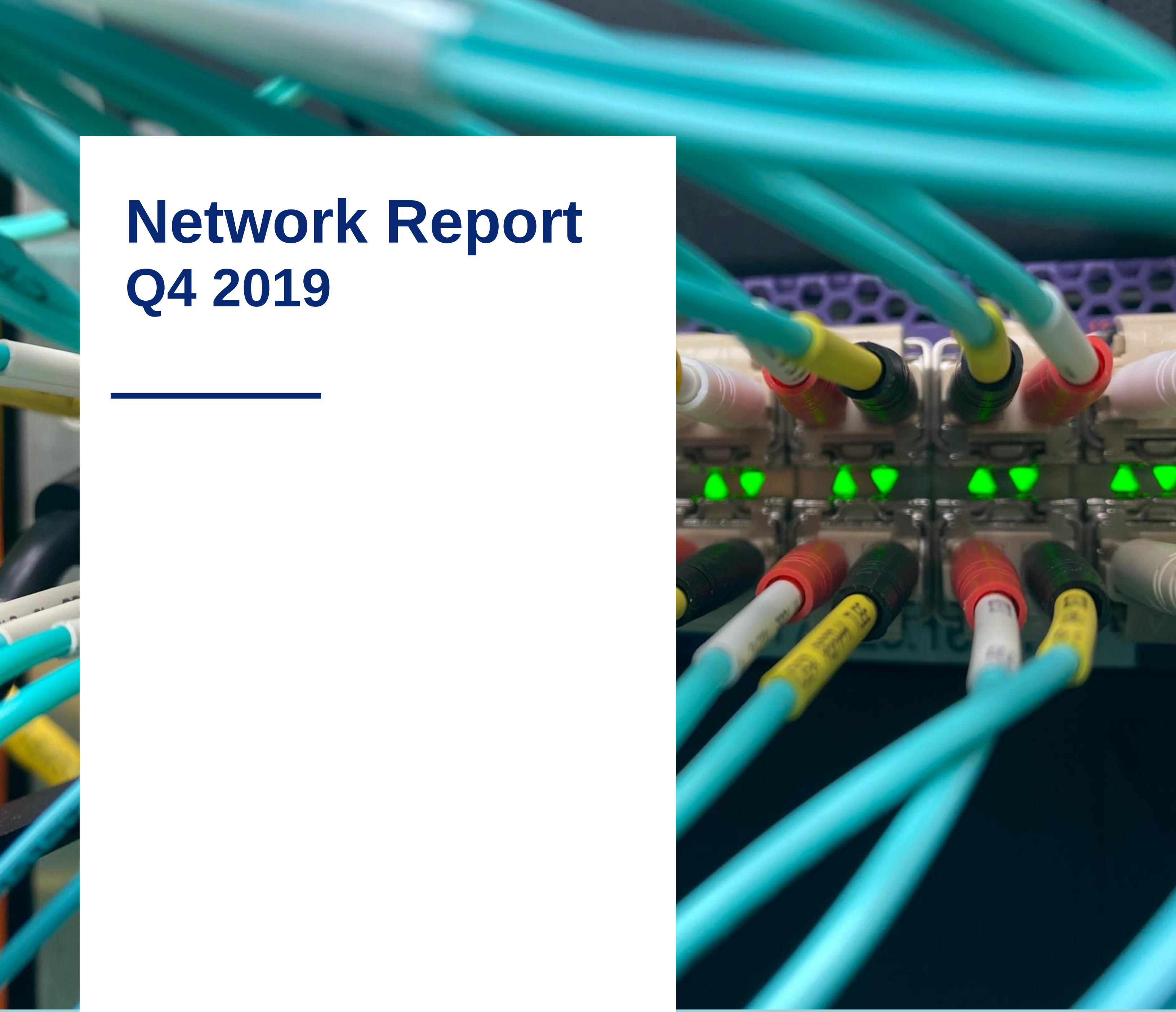


Network Report
Q4 2019

January 6, 2020

Information Technology Services
Communication Technologies: Networking

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

UNC | INFORMATION TECHNOLOGY SERVICES

QUARTERLY NETWORK REPORT — October 2019 – December 2019

Introduction:

We hope that you will find this report informative! It is our intent to publish this once per quarter. We would appreciate feedback from our customers and the user community on how this report is received, and if there are improvements we can make.

The report has several sections. The first section goes over some key metrics that you might find interesting. With subsequent reports, there will be comparisons to previous periods. As we receive feedback, things may be added or removed.

The second section will review major initiatives. These are items that are top of mind at the time we wrote the report, or things that progressed significantly during the previous quarter. Things will come and go from report to report.

The third section is the life cycle section. We are continually life cycling large quantities of switch, UPS, and wireless access point inventory. The life cycling of this equipment requires a lot of time and effort from the Network Deployment group. This section is intended to show you where we have focused our efforts in the last quarter. It omits small changes.

The final section is for critical incidents. Internally, we have three classifications for incidents: Critical, Major, and Minor. For the purposes of this report, Major and Minor incidents will be ignored. Critical incidents are those events that had substantial impact for a large part of campus. We will attempt to explain what happened and explain any lessons learned.

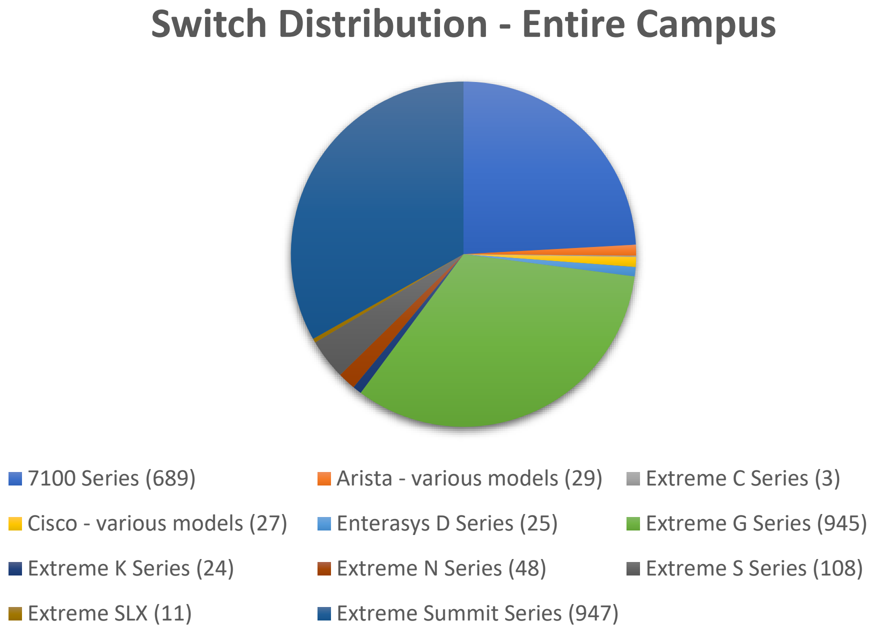
Thank you all for your time in reviewing this report. We appreciate everything you do to help make us successful.

Sincerely,
Ryan Turner
Head of Networking

Key Campus Metrics

WIRED

Number of switches on campus:	2,873
Number of ports:	173,187
Peak download rate:	20 Gbps (November 14)
Peak upload rate:	9.9 Gbps (December 12)
Traffic sent to Internet	3.7 Petabytes
Traffic received from Internet	5.5 Petabytes



- We have eliminated almost every C series switch on the campus.
- We are now focusing on G series which just recently went end of support. We expect to have G series life cycled in under 3 years.
- N series will be life cycled in the next year
- We will be exploring new options to replace our Tier 1 locations with next generation 40G/100G switches.

Explanation of major model types:

Cisco Nexus 7706 – These chassis-based routers act as the core of our network and feature high density 40G/100G capabilities. These switches provide almost all core routing for campus and were the part of our major core redesign in 2018. They also serve as the layer 3 core for ITS data centers, providing an aggregate of 400 Gbps from ITS Franklin and ITS Manning.

Arista – We used a variety of Arista switch models to provide high-density high-speed connections to ITS Research Computing as well as other research entities across campus.

Extreme Summit Series – Comprised of the most current generation fixed format of switches in our network and are divided into many sub-categories (not shown). As we eliminate the older generation switches, we will break down this category into more granular models. These switches have a minimum of 1G to the desktop, 10G to the server, and either 10G, 40G or 100G uplinks. They come in copper or fiber-based form factors. Most will support 802.3at power over ethernet. Newer models will support 802.3bt power over ethernet.

Extreme SLX series – These high density 40G/100G switches are currently used as spine layer switches in the new data center design. They can support a high number of 100G ports, will support 400G in the future, and feature a deep packet buffer system that can eliminate packet drops from a congested network. They come in chassis and fixed format, and we will be considering this line for replacement of our current distribution tier 1 switches (S series).

Extreme 7100 series – Currently supported previous generation of fixed format switches that feature 1G to the desktop, 10G to the server, and 10G or 40G uplinks. This switch is no longer available for purchase and runs a network operating system that will eventually be deprecated by the manufacturer. Most will support 802.3at power over ethernet.

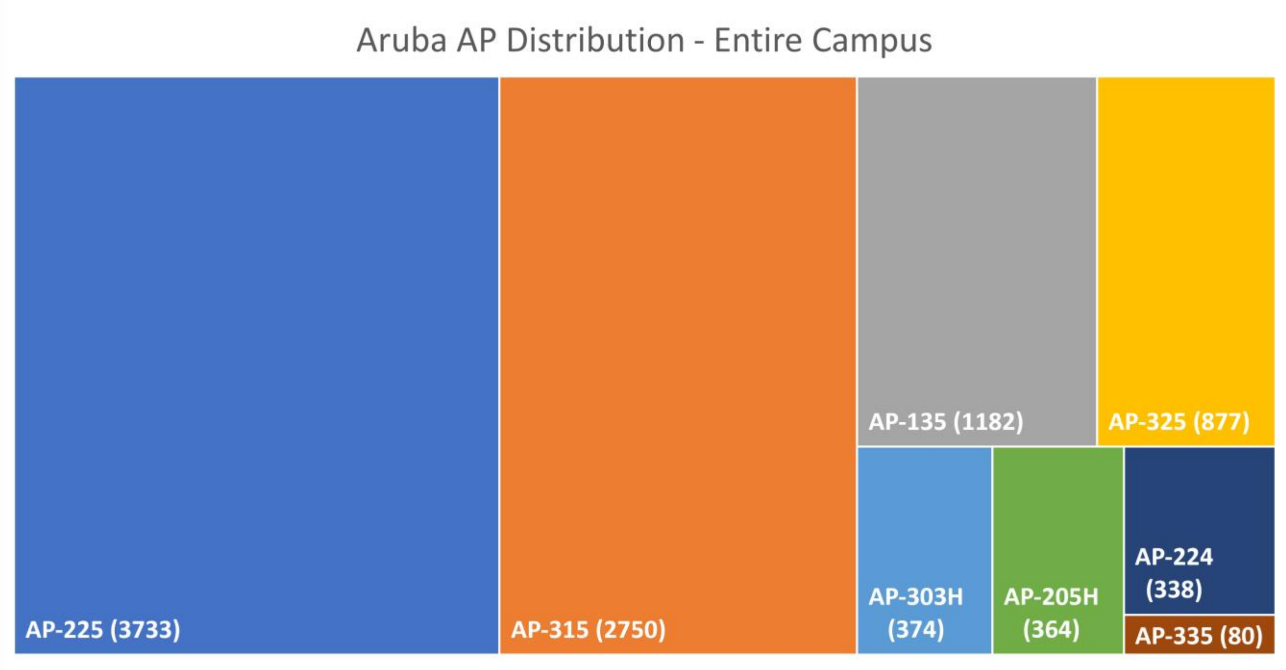
Extreme G series – Past generation of modular switches that feature 1G to the desktop. They are no longer available for purchase and have no software support. As modular switches, they can support up to 4 cards of 24 ports each. These switches will support only 1 card of 802.3af power, and its 10G capability is channelized, substantially limiting its ability to carry high data rates. These switches will not be adequate for the power needs of the current generation access points and replacing them is a priority as we life cycle.

Extreme K / S series – These past generation of chassis-based and fixed format switches act as the workhorses for many of our key distribution points across campus. They currently carry software support. They support 10G connectivity at density, but lack in their 40G capabilities. Many of these switches will be replaced in the next 2 years as we attempt to move away from chassis-based switching in as many places as possible, toward fixed format high density 40G/100G switches.

Extreme N series – These are switches that were introduced over 10 years ago and still exist in limited parts of campus. They are 1G switches. These are a priority for replacement during the next year. Few exist on the campus network.

WIRELESS

Number of APs on campus:	9,846
Peak concurrent connections:	47,100 (November 5th)
Devices onboarded to eduroam:	11,239
Top Onboarded OS:	iOS with 51%



- AP-1XX series access points will go end of support in August of 2021. We have replaced over 1,000 AP-1XX series access points on main campus in the past year
- With additional funds from Housing, we are at the beginning of a 5-year life cycle plan to do the same thing for ResNet.
- With pervasive funding, we are targeting the life cycle of around 1,200 access points each year.
- We have started replacing AP-2XX on main campus for new Wi-Fi6 APs (802.11ax) AP-5XX.

Explanation of major model types:

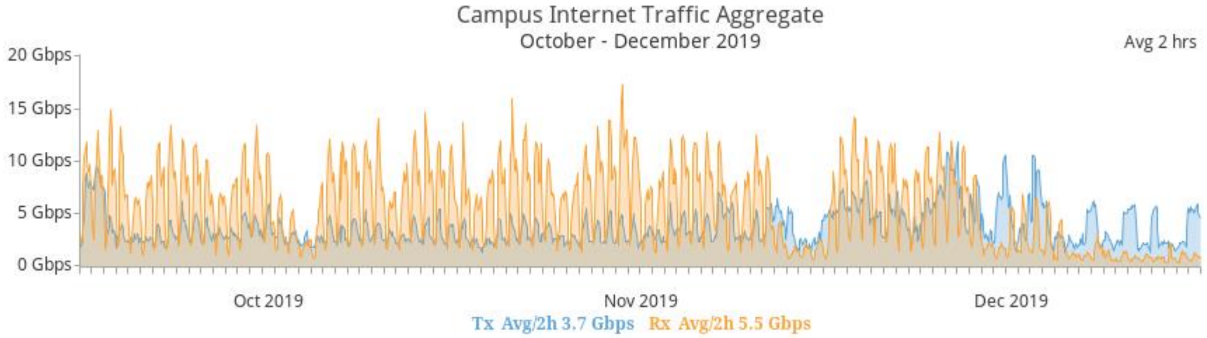
AP-1XX – Aruba access points that feature 802.11n capabilities. Aruba has set the end of support date for AP1XX access points as some time in 2021.

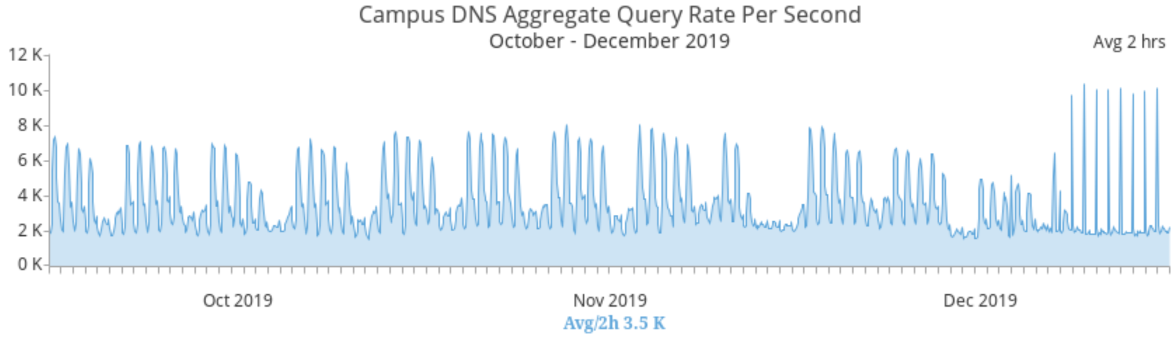
AP-2XX – Aruba access points that feature wave 1 of 802.11ac capabilities. Aruba has set the end of support date for these access points as some time in 2023.

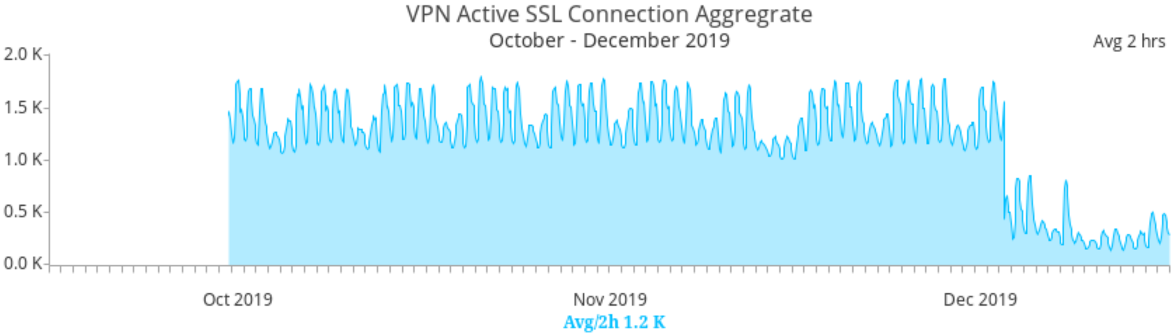
AP-3XX – Aruba access points that feature wave 2 of 802.11ac capabilities. Aruba has not set the end of support date for these access points, and we consider these still current generation.

AP-5XX – Aruba access points that feature wave 1 of 802.11ax capabilities (pre standards ratification). We will be installing these access points as standard beginning in 2020.

ADDITIONAL GRAPHS


Campus Internet Traffic Aggregate
October - December 2019


Campus DNS Aggregate Query Rate Per Second
October - December 2019


VPN Active SSL Connection Aggregate
October - December 2019

Major Initiatives Review

New Data Center Architecture

ITS Networking has been working on implementing a new data center architecture beginning in June of 2018. This new architecture is called 'Spine / Leaf' and features redundant pod switches for server connectivity, ultra-highspeed throughput across data centers, and a redundant design that will allow us to do firmware updates and switch reboots with no disruption to services. The new architecture has now been implemented, and we have been working with customers across the campus to migrate from the old architecture to the new architecture. ITS UCS is now entirely connected through the new infrastructure. Please submit a request to Networking today if you want to know more.

UNC Chapel Hill and UNC Hospital Network Extension

To provide more consistent connectivity between our two institutions, we have agreed to begin work to extend Skynet (SSID for Hospital) into School of Medicine locations, and the Hospital is working to extend eduroam to all their sites. In addition, both institutions will be extending wired connectivity across network boundaries as well. This is a very large and complex project and has the potential to substantially improve the way our two institutions coexist.

New option for providing connectivity to remote sites

We are working with Tom Gray and TEACCH to validate a new method of connecting remote sites back to campus without the need of expensive metro ethernet services. Currently, if you have an off-site location, you have three choices: The first choice us to utilize a business class ISP and not connect back to campus. The second choice is adding a site to site VPN to the first choice. This does give you access to campus resources but won't allow you to utilize many networking services (wireless and managed switching). The third option is a metro ethernet solution. It ties the site directly back to campus and we can extend campus VLANs and wireless, but it comes at a substantial recurring monthly cost. The new option will allow you to utilize a relatively inexpensive business class ISP connection, and still have the option to use campus switching, campus VLANs and wireless. We expect to have this implemented at a test site in the next quarter and hope to have it offered as a service during the next 2-3 quarters. The departments will be responsible for paying for the upfront hardware and upfit fees as well as ISP fees. Once we validate the service, we will make an announcement on CTC.

Direct connection for GCP

In a partnership with Google, UNC is now directly connected (without using a VPN) to GCP through a direct 10G connection to their Atlanta presence. We expect to increase this to 2x10G when we increase our usage of the service, and Google has assured us that they will increase our connection speed as we show the demand for increased speeds.

Server Proxy Service to be launched

We have been evaluating two of the big players in the proxy arena and will be purchasing a solution during this quarter to be used for server (not client) patching. Currently, departments must run their own proxy servers when they have a server on private IP space that needs to communicate to the outside world. We will announce this as a new service on the CTC when it is time.

Four-year user certificate for eduroam

On January 2nd, we officially changed our onboarding platform to utilize a cloud PKI serving up 4-year user certificates. Unless you clear or reset your device, you only need to onboard a device one time every four years.

Life Cycle Update:

The following locations have received substantial new switching gear during the past quarter:

Physicians' Office Building
Bondurant

The following locations have received substantial new wireless gear during the past quarter:

Koury Oral Health Science
Ackland Art
Howell
Gardner
Murphy
Lenoir
Van-Hecke

The following locations are being **targeted for upgrades** in the coming quarter (subject to change):

314 Cloister Court
Hanes Hall
Quadrangle Building 4
720 Martin Luther King
Carmichael Auditorium
Woollen Gym
Boshamer
Bell Tower Parking Deck
Botanical Gardens
Steele
Bynum

Critical Incidents Review:

December 18, 2019 ITS Data Center Power Outage

Due to a power outage in ITS Manning at around 11AM, networking equipment in ITS Manning hard rebooted. This included ITS Security maintained equipment such as the Manning based firewalls and Intrusion Prevention systems (IPS). Some equipment did not come back up cleanly, and many hours were spent coordinating and collaborating with numerous other ITS entities to bring services back online. The last major networking issue was resolved around 4:30 PM. During the outage, we experienced a firmware bug that prevented wireless from properly failing over in select locations on campus, a disruption of communications through the data center Palo Altos after failover, a partial link failure in a port channel on Manning-loco (old Manning data center core that still has critical services attached) that was 'up' but nonfunctional, and a significant disruption to F5 services. The F5 service issues were the victim of the partial link failure on Manning-loco. Any one of these issues can be tricky to resolve, but we were forced to deal with them all at once. We will be developing a plan based on things we learned during this event to aid us in the future.

November 20, 2019 Slow Internet Connectivity

Around noon, we experienced and received reports of slow internet connectivity. It was determined that there were an extremely high level of traffic drops at one of the border IPS units. ITS Security made some modifications, and to date, we have not seen this issue reoccur. The disruption lasted between around 11:55AM through 12:13PM.

November 19, 2019 DNS Resolution issues

One of our internal DNS servers was being hit by so many requests (from a local host) that it was periodically unable to handle incoming queries. Our reporting of this incident has changed from the initial report. Initially, we suspect it was an external host hitting DNS, but research would indicate this was a local attack. It is likely it was a misconfigured host. During our post event analysis, we believe the problem started the previous evening around 10:30 PM, however neither our tooling (nor customers) were able to initially identify DNS as a root cause of minor service alarming. We confirmed an issue with DNS around 8:00AM and mitigated the effect of the denial of service shortly after. We are looking at ways to make the service more resilient to incidents like these.

November 13, 2019 Med School Network Degradation

While bringing on a new monitoring platform, the platform pulled too much SNMP data from the Med School Tier 1 switch, bringing the CPU to 100%, and stopping much of the traffic through the School of Medicine. This caused a significant degradation to network performance for most of the Med School for about 10 minutes between 2:05 PM to 2:15 PM.

October 22, 2019 Recursive DNS failure

We point all our external (non-UNC) DNS queries to a security DNS service provided by Akamai. Due to a link issue deep within MCNC’s network, our connections to the Akamai service were severely disrupted. We had to bypass the Akamai service. Our DNS service began to throw away queries when Akamai stopped responding. The service was disrupted from around 12:45 PM until 1:30 PM. We are still looking for ways to monitor the Akamai service and programmatically switch away from it when it is no longer performing appropriately.