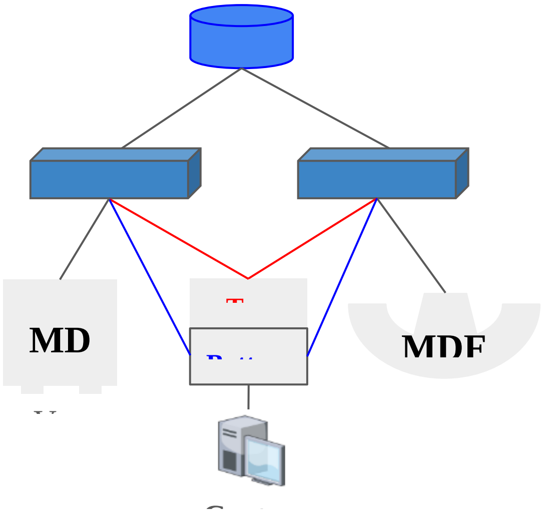
Georgia Tech Network Infrastructure Study

Infrastructure Deployment

The campus is based on a dual 10 Gbps feed for each building, where each building has a MDF (Main Distribution Frame) set of redundant switches, and each switch has a 10 Gbps connection to the core. It runs on a single mode fiber LR. This setup satisfies the majority of campus needs, and the largest tracked bandwidth spike was only 5 Gbps for only a short period of time.

Nonetheless, a solution exists to fulfill high bandwidth requirements. In such cases, vapor switches will be installed. Since the main campus distribution fabric is the VXLAN fabric at the core, these switches will be set up as fabric leaves and will connect back to the fabric spines in the campus interconnects. If redundancy of switches is not required, a single vapor switch will be sufficient. Otherwise, a pair of vapor switches will be deployed, comprising a top switch and a bottom switch. Both the top and bottom switches will have two 100 Gbps connections to spine 1 and spine 2, resulting in an aggregate of 400 Gbps connections. The spines are Cisco Nexus 95 switches with 100 Gbps line rates, allowing the switches to be used by only one user with no traffic on the backbone.



Key

<u>Core</u>: runs on VXLAN fabric

<u>Interconnect Spine</u>: Nexus 9508 with quad 100 Gbps

<u>MDF Switches</u>:

The hardware of IDC is deployed in three main locations: Klaus, Van Leer, and Bobby Dodd Stadium, each employing unique deployment methods. Notably, compared to the rest of campus, Klaus runs on a multi-mode fiber, because SR optics were significantly cheaper than LR optics at the time. Although not facing the same cost constraints as Klaus, Van Leer frequently encounters bottlenecks due to challenges in upgrading its networking system. This difficulty arises from the presence of asbestos in the building, which renders the installation of new fiber and copper cables extremely expensive. Hence, the only viable solution is to deploy individual switches with a single 10 Gbps uplink connection.

Finally, Bobby Dodd Stadium presents the most intricate and complex deployment challenge. The switches within the stadium connect and communicate with the broader GT network and are managed and monitored by OIT. However, the athletics department operates independently and autonomously when it comes to hardware deployment; thus, the ability to deploy a centralized solution becomes a difficult challenge.

Hardware Management

Hardware management on campus is dependent on the "book of knowledge" and manual labor. The "book of knowledge" serves as the routine, day-to-day management method. Originally a physical binder containing network information, it has since evolved into a digital repository documenting hardware across all campus locations. Specifically, it keeps a full building index, and each building has a "book of knowledge" to facilitate active monitoring of hardware. For instance, OIT can easily monitor the status of a particular hardware by accessing a switch from the interface system.

An alternative for the book of knowledge relies on console devices over SSH to run standard Cisco commands on the switches. However, this method requires the campus to completely adopt Cisco's Digital Network Architecture (DNA) Center that runs on Software-Defined (SD) Access, which is incompatible to address all campus needs. In terms of the architecture, Cisco is reluctant to inform OIT on the mechanisms of their DNA center, which results in reliability and trust issues. As a result, OIT has resorted to physically managing hardware and manually configuring switches.

There is a physical warehouse at the edge of campus that stores all the hardware, fibers, and testing racks. Before deployment, all the equipment that needs to be installed undergoes mock-up scenarios, and the switches are staged with initial configurations. Therefore, during installation, OIT simply connects the fiber in the building to the switch, as long as there are MDF fiber links configured on either side. Finally, the network infrastructure team will cable from the patch panel in the closet to the installed switch. Although this method fulfills campus needs, it is highly susceptible to human error, where a single typo can bring a significant amount of connectivity down.

Despite recognizing that the current methods are outdated, the team faces barriers to adopting powerful management products in the market, such as Arista for cloud computing, or creating solutions from scratch due to the layer 8 issue. In this case, their execution is impeded due to the management problems and shortage of developers, where they only have five or six people managing 280 buildings and around 5,000 switches on campus.

Data Management, Transfer, and Localization

The extent to which OIT handles data management on campus is through a "syslogs receiver system," an extensive history of logs generated by each switch in each router. These logs are held by one common server that can store these logs for a variable number of days. Even when the common server runs out of storage to hold logs or the logs would expire, the cybersecurity team has a system called Elasticsearch, otherwise called Kibana, that also stores log entries into a much larger database with the capability to hold all of the syslog infrastructure OIT needs for campus.

In terms of monitoring this data, while there are multiple different solutions the universal solution is using SolarWinds. SolarWinds allows for the monitoring of the status of devices under OIT, such as tracking if they are responding, have a high temperature, have low storage, and any other type of errors. This system also sends alerts to OIT about any device having such an error, allowing for an automated flow of data monitoring. In combination with syslogs, SolarWinds provides the most effective way for OIT to monitor all their logs of data.

In general, OIT's data management system is more focused on deploying solutions within their costs instead of running extensive experimental tests and collecting large chunks of data to test. This means that OIT is not tasked with much direct experimentation of campus data and instead focuses on maintaining existing technology that meets industry standards and evaluates their solutions to meet such standards rather than experimenting.

For data transfer, OIT focuses on providing high bandwidth over the campus network since it would naturally correlate to having high speed or low latency. To do this OIT is required to consider what is the bottleneck, or weakest link, in the network that prevents higher bandwidth, and this can lead to a variety of different devices involved in a 10 Gbps network chain. In terms of improving the current system, newer and improved technologies such as fast SSDs that allow for fast direct memory access are constantly being developed which can remove more of the bottlenecks involved in data transfer, such as making the speed at which data directly leaves from your CPU faster through improved SSDs.

Finally, in terms of direct localization, OIT does not handle those cases and instead just focuses on figuring out what devices are associated with what API. This still allows OIT to easily locate a device's building and room number through their API but has no focus on localizing over wireless connections with any form of strong accuracy.

Policy & Regulations

Ensuring a uniform standard of network connectivity and deploying a defined set of hardware to all campus managed buildings, OIT streamlines the administrative processes with minimal paperwork and policies. This process is rather self-explanatory: when a new building is built, there will be network infrastructure and connectivity automatically deployed within the building.

When it comes to the regulations governing hardware deployment, OIT has established specific feature sets (i.e., requirements) that the switches must meet and satisfy. One such requirement is edge port security.

With an unmanaged switch, the default behavior is to learn as many MAC addresses as possible on the interface and forward all the incoming traffic. This can lead to two potential issues: either the switch's memory is filled, or the CPU is taxed. However, with a managed switch, it can only process a predefined number of MAC addresses on the port. This limitation prevents someone from connecting an additional, unauthorized layer of infrastructure to the switch, which is very unstable for the network.

Moreover, this poses a big security risk to the security pillars of confidentiality, integrity, and availability. Specifically, the availability of the switches is compromised, which was the main contributing factor to the numerous network outages on campus. Hence, the utilization of DHCP is either highly restricted or entirely prohibited. As OIT's DHCP and consumer’s DHCP will both attempt to assign addresses on the network, the simultaneous activity will result in conflicts and network outages. Therefore, OIT's DHCP is configured to exclusively offer and acknowledge packets from the uplinks of the switch, never those from the downlink port.

Additionally for the downlink port, due to the spanning tree protocol, OIT will deactivate a port upon detecting any bridge protocol data units arriving from other switches. This indicates the presence of infrastructure that OIT does not manage from the downlink switch, which poses both security and reliability concerns.

Another aspect of OIT’s campus wide policy is the property to keep the network segmented. This policy enforces each department to their own level of firewalling through VLANs. The VLANs are specific to each department/unit on campus and all devices associated with said department/unit are registered to their respective VLAN through a Mac address. This dynamic assignment of devices through the campus network allows for the segmentation of the network to be possible.

Each VLAN on campus has a firewall instance with a department specific policy that can deny connections with outside departments/units unless the policy specifies to accept outsiders. However, it is important that department level policy limits outbound data for security purposes due to the ability for such data to leak information from the central server.