# ARCADIA UNIVERSITY CYBERINFRASTRUCTURE PLAN

1. **Introduction**

Information Technology (IT) at Arcadia University provides services to faculty, staff, and students across two schools and 3 colleges including Arts and Sciences, Health Sciences, Education, Global Business, and Global Studies. Additionally, a large study abroad program is offered through its College of Global Studies that operates in 13 countries.

Arcadia’s main campus location is located in Glenside, PA and a satellite office operates in Christiana, DE (refer to Figure 1). The Glenside campus has two server rooms and a disaster recovery site in a data center 20 miles west of Glenside in Valley Forge, PA. The Delaware satellite has a small server room/network closet that contains all equipment to support that site.

**Figure 1.** Arcadia’s Enterprise Network



In 2012, Arcadia contracted R&R Voice and Data, Inc. (R&R) to provide a complete upgrade and overhaul of the Glenside campus’ fiber infrastructure. The networking infrastructure specified by Arcadia University deployed a 3-tier model: Core–Distribution–Access layer switches. In doing so, the university moved from a single core switch, located in Boyer Hall, to a two core switching environment, one each located in Landman Library and Brubaker Hall. The network was designed with a “no single point of failure” methodology.

On Arcadia University’s main campus there is a 24-pair redundant fiber ring that connects all of the campus buildings together. Currently, only 2 pairs (4 strands) are utilized on the network which has been adequate to support administrative needs. Arcadia has dark fiber that connects the Valley Forge co- location with the Glenside campus and a site-to-site VPN that connects the Delaware office to the Glenside campus. Before the grant, Arcadia used to provide a 1 Gbps Internet connection for the students, 600 Mbps connection for faculty/staff, and 400 Mbps connection at the Delaware campus.

# Current Enterprise Network Environment

The University’s LAN environment comprises three levels of switching, covering a typical collapsed core to distribution to edge model. Being a “collapsed” core, all routing for any remote sites is performed within the Core Router/Switch itself for all the VLANs, (Virtual LAN Interfaces, supporting various routed networks).

The Core consists of two (2) Ethernet/Routing chassis with an assortment of blades and modules to support supervisory functions as well as providing fiber links to down level distribution switches. Both chassis are bonded as a function of HP’s Intelligent Resilient Framework (IRF) technology which creates a large IRF fabric from multiple switches to provide data center class availability and scalability. Essentially, this technology bonds each chassis into a single “Virtual” chassis. This bonded function allows for a failover to occur for both routing and switching, protecting all of the core functions and providing continuous operation should a failure occur.

Arcadia’s IT staff has facilitated links to the distribution switches to be redundant, allowing for two paths in 10 GE (10 Gigabit Ethernet) bonded trunks, or Link Aggregation Control Protocol (LACP). With this in place, should one core suffer a failure, the LACP-bonded interfaces would continue to flow traffic to the other chassis without interruption. Each distribution location consists of a pair of Switches, which are also stacked or bonded together to provide a single “Virtual Switch.” As in the Core, the bonded switch will continue to support their uplinks to the Core as well as their downlinked Edge switches.

Arcadia owns IPv4 and IPv6 blocks from ARIN information below:

|  |
| --- |
|  |

# Wireless Access

In the past year, Arcadia implemented HPE Clearpass in conjunction with joining Eduroam. A complete rebuild of the wireless network was performed. The Clearpass replaced the Bradford Network Access Control that was just on the student network. Currently, the Clearpass is across that network handling the Network Access Control for faculty, staff, students, and guests. Secure access for BYOD devices is provided as well. Role-based policies, enterprise-grade AAA with RADIUS/TACACS+, built-in device profiling, Apple Bonjour and DLNA device sharing, and integration with third-party MDM solutions – all through a single web interface.

# Firewall and Data Storage

Arcadia has Firewalls located in front of each of the Internet Routers. One for faculty/staff and another for students. The Internet Routers are a redundant stacked pair, but the availability of the Firewalls directly affects the availability of the Internet access on campus.

Arcadia has a capacity of 50 TB of a Storage Area Network (SAN). The SAN is used for storing faculty and student files. Additionally, all backups on the network are stored in the SAN as well.

# Servers

In 2010, the IT department deployed a VMWare ESXi Cluster to host different specialized applications on request.

# Identity and Access Management

Current authentication aspects include: Eduroam, G Suite, Self-Service, AD, LDAP, and CAS.

At Arcadia, there is an internal push to start moving to Software as a Service applications (SaaS). The first we will be implementing next month, migrating from internally hosted Client Access Server (CAS) for Single Sign-On over to a cloud identity management platform, PortalGuard.

# Phone System and Surveillance Video

In 2010 Arcadia contracted R&R to implement security cameras across campus. This involved connecting the cameras to the network as well as storage for all these aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

In 2015 Arcadia worked with ShorTel, now Mitel, to implement a pilot VoIP system. Currently we have a dozen phones on the network using a VoIP VLAN. At some point in the future we will increase that footprint. All the network configuration is completed and management of the system is performed via VMWare ShorTel appliance.

# Education Applications

Arcadia outsources educational platforms to Canvas and Google Suite Apps including its email system. In addition, Arcadia provides faculty with access to distant learning tools such as Panopto Recordings, Zoom, and BigBlueButton. At the same time, Arcadia hosts Rolodex, Event Management System, and Self-Service on the premises.

# Planned Arcadia Science Network Environment

* 1. **Objectives**

The main goal of Arcadia’s Cyberinfrastructure Plan is to transform the institution’s infrastructure to meet the increasing demands of data-driven research and education conducted by its faculty and students.

Arcadia desires the ability to perform high speed data transfers that the researchers currently need and that faculty will introduce into the classroom as part of the academic plan to integrate data analytics skills into all of our undergraduate studies. The new capability will be called Arcadia Science Network. From a University-wide perspective, we are moving toward an intentional enterprise architecture that addresses research, education, and administrative needs. The enterprise architecture adopts a cloud-first approach; includes a science DMZ and network; and aligns our security, services, applications and monitoring. This will shift our design from on-campus tools, storage and perimeter focus to one operating in a hybrid model that moves seamlessly between internal and external capabilities. The project’s objectives include the following:

1. Provide high performance, secure ESnet Science DMZ network capabilities for large datasets sharing and cloud-based education.
2. Eliminate the technical barriers for faculty through a dedicated, friction free path to Internet2, PennREN, and other high-performance computing and data resources.
3. Leverage authentication and authorization mechanisms to support our faculty science drivers and join InCommon Federation.
4. Enable the future scientific possibilities and unleash innovation for student & faculty researchers.

# Planned Deliverables for the Proposed Arcadia Science Network



**Figure 2.** Proposed Arcadia Science Network

To address the above- mentioned objectives, we pursued the following deliverables.

* Implement the proposed Science DMZ design.
* Upgrade the backbone connections of the network from 1 to 10 Gbps. We plan to quote different Bandwidth Service Providers to select the best fit for dark fiber and providing a pipeline to Internet2 and PennREN
* Add cores to each of the server rooms, Glenside campus, with 10 Gbps interconnect to each building. We plan to connect 2 buildings to the Science DMZ as a Proof of Concept: Brubaker and

Boyer Halls. Both of those buildings house data-intensive curriculum and research projects. Boyer houses Computer Science and Math Departments and Brubaker houses Physical Therapy and Public Health Departments.

* Implement perfSONAR, the networking performance measurement tool.
* Complete our path to InCommon Federation and identity management for services & applications.
* Implement IPv6 strategy within the new Arcadia Science Network as the Arcadia Administrative Network is not ready to handle transition from IPv4.
* Implement security mechanisms on the perimeter.

The proposed Arcadia Science Network (High speed Science DMZ network) was brought up alongside the current administrative network. The new science network provides 10 Gbps connectivity to two crucial locations on campus that are major hubs of high-performance networking research and education needs (Boyer and Brubaker Halls). The new border routers replaced the older border routers (limited to 1 Gbps) to provide support for 10 Gbps. This allowed our current infrastructure to keep functioning while the new Arcadia Science Network has been being built from the ground up. Once the new cyberinfrastructure for Arcadia’s Science Network is running in a high-quality manner, future steps will include providing the enhanced capability to all areas and campuses.

# Additional Network Monitoring

Each connection to Arcadia’s Administrative Network will have a Firewall before the Border Routers that have access to the Internet. This adds an extra layer of security between the university and the Arcadia Science Network. We will be able to monitor the activity at the router level within perfSONAR.

The Border Routers connecting to the Science DMZ will not be passing through the Administrative Network firewall to allow science traffic to remain friction-free. Within the Science DMZ we will have our distribution layers switches and a Data Transfer Node that will have a direct connection to the SAN.

We plan to utilize:

* + perfSONAR will be installed to monitor activity at the distribution level within the Science DMZ.
	+ Splunk which offers us the ability to search, monitor, and analyze machine-generated big data (including the network traffic) from one centralized web page.
	+ Snort in conjunction with Cisco networking equipment. Snort is a free open-source network Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
	+ to monitor internal and external addresses for any security concerns.
	+ to monitor all of its servers and network devices with the purpose of centralizing its monitoring from the several locations that are currently being used.

# Enhanced Identity Management and Security

We implemented PortalGuard, a cloud-based SSO solution. We have focused on SAML & Shibboleth and are currently authenticating with eduroam.

At a device level, we have to Dell EndPoint Security Suite Enterprise System (ESSE). This included both AntiVirus and encryption products, which will allow for managing authentication and encryption as well as preventing malware via one centralized, remote console.

We worked with KINBER, as our Leadership Institution, and our external consultants to assist us in the effective configuration of our border router’s Access Control Lists and get access to PennREN and Internet2.

With respect to physical security, the campus is outfitted with key card access and cameras throughout. Data centers and network closets are secured with limited access based on roles.

Finally, we have a third-party provider scanning our environment and as we enhance the network, we intend to contract for periodic intrusion testing.

# Sustainability

We feel confident that this grant positioned us well for sustainability as we put the cyberinfrastructure in place to manage our growth through a dark fiber option and alignment of our science traffic through PennREN and Internet2.