UVI Infrastructure

Report to the UVI Foundation Board

October 27, 2008
University of the Virgin Islands
Tina M. Koopmans

University of the Virgin Islands
Information & Technology Services

PROVIDING THE TECHNOLOGY SOLUTIONS AND THE INFORMATION RESOURCES TO ACHIEVE VISION 2012

The Challenge

From August of 2005 to February of 2006, several evaluations of the networking infrastructure at the University of the Virgin Islands were undertaken. These revealed a number of deficiencies.

1. **There was no obvious design of the network.** The infrastructure was built in a piecemeal fashion without sufficient time for planning. This is not uncommon as the technology changed quickly and there were many disparate needs.
2. **The network was unsecured.** The UVI network was an unsecured custom configured, complex 10/100 megabit network. Additionally, it was configured outside of industry networking standards and best practices.
3. **There was little or no redundancy in systems.** This was especially true in the major network components and the single point of failure created by a single CISCO router that was running at 90% capacity and the inter-island microwave.[1]
4. **There was no network documentation.** There was a lack of clear guidelines for server installation, routing design or maintenance schedules. In addition, network operations was highly reliant on shell scripts (files containing executable commands) that were undocumented. [2]
5. **The network equipment was aging.**
6. **Internet capacity was extremely low.**

The Solution

In March of 2006, the University of the Virgin Islands Foundation (FUVI) approved $919,627 as part of Project Leap Frog for the redesign and implementation of the networking infrastructure for the entire University. This included a three phase plan:

1. **Phase 1:** The replacement of network electronics ($299,460)

[1] **It was the lack of redundancy and maintenance on the inter-island microwave that led to the network problems experienced September 2007 and the traffic was a factor in the router problem that occurred in October of 2007.**

[2] **The lack of documentation, especially on the mail routing and user creation systems caused the UVI student email system to be replaced with Google mail. New users could not be added after November of 2007 and the system became inoperable in May of 2008 when new mail systems were installed.**

2. **Phase 2:** The implementation of appropriate security measures and improvement of network services ($320,167)
3. **Phase 3:** The implementation of redundancy and increased capacity of the systems ($300,000)

In addition, the University used Title III and operational allocations, EPSCoR funding and University plant funds to:

1. Redesign the network ($20,000).
2. Replace aging server infrastructure ($145,320).
3. Redesign the active directory/LDAP implementation ($98,144).
4. Perform necessary remediation to sustain existing systems ($144,800).

The Status

As of September 2008, the UVI network has been securely rebuilt in accordance with industry network standards and best practices. Documentation has been compiled for all upgrades or modifications made.

To date, the following projects have been completed successfully:

1. Layer 2 switching upgrade from 10/100 megabit to 1000 gigabit. The upgrade has allowed for better and faster data transmission throughout the network.
2. Redundant firewalls were installed on both campuses to protect University systems from outside intruders.[3]
3. New mail gateways were installed to deliver and handle mail in an industry standard way.[4]
4. Student email was moved to Google mail and is accessible via http://www.google.com/a/myuvi.net.
5. Web filtering proxy appliances were installed to protect the open ports on the firewall.
6. Domain Name Services were re-implemented according to industry standards. This service now resides on seven different servers, providing recommended redundancy.[5]
7. Disparate LDAP systems were replaced by a single redundant system to better manage our users, improve security and allow the use of the Banner database as

---

[3] This eliminated frequent virus and outside user attacks on the UVI network.

[4] This eliminated the use of the UVI mail server as a resend point for Internet spam. The UVI email system had an "untrusted rating", preventing UVI mail from being accepted by some institutions. This rating has now improved to "trusted".

[5] The legacy DNS system failed in April of 2008. The re-implementation and redundancy prevents such an event from re-occurring. There are now a total of seven DNS servers, five of which are AD and internal DNS servers while two are external DNS servers.

the single source of information for users across the network. Seven redundant Domain and Active Directory servers have been installed and the Active Directory database cleaned up, modified, and documented in accordance with Microsoft best practices.[6]

8. A Virtual Private Network (VPN) solution has been implemented to facilitate access to University systems via an at home Internet connection of at least DSL speeds or greater.[7]
9. The DHCP system has been re-implemented using industry standard technology.
10. An enterprise tape backup system (IBM's Tivoli) has been installed and is now backing up mission critical data to tape each night. Non-critical servers are backed up weekly.
11. Storage Area Network (SAN) devices were installed to provide additional storage space for Banner, Exchange, EPSCoR and Blackboard.
12. Network monitoring tools have been installed. These systems detect problems with network switches, allowing for repair or replacement before they become apparent to users.
13. Failover capabilities have been engineered for Blackboard.[8]
14. The Exchange servers were re-engineered according to industry standards.
15. Documentation was created for all new and existing network components:
    a. Newly installed server configuration documentation includes server names, network connectivity, role specific, operating system and hardware configuration information.
    b. Troubleshooting documentation on how to troubleshoot specific problems with newly installed UVI network appliances.
    c. Active Directory documentation provides detailed documentation on how Active Directory, Domain name server (DNS), and Dynamic Host Configuration (DHCP) Protocol are set up.
    d. Exchange Mail Services documentation including how Exchange is configured and how mail is routed internally.
    e. Network Security documentation on how the UVI network is secured.
    f. Layer 2 Gigabit switching documentation including documentation on switches and configurations for all UVI switches.
16. Training and certification was achieved by the networking staff.
    a. Burt Chesterfield – Red Hat Linux Essentials RH033.
    b. Cecil Stanfield – Microsoft Windows Server 2003 System Administrator, Cisco Certified Network Professional, Cisco Certified Design Professional, and Hewlett Packard ASE Proliant Servers 2007.
    c. Mark Bough – Microsoft Windows Server 2003 System Administrator and Cisco Certified Network Administrator
    d. Kelly Harrigan - Cisco ASA firewall, Ironport, and Active Directory

[6] **The single LDAP system is secure and will allow UVI to implement a single-sign-on solution.**
[7] **This replaced the failing modem pool.**
[8] **This will eliminate Blackboard server downtime, as experienced during the Fall 2007 semester.**

The Next Steps

There are several tasks that need to be accomplished to complete phase 3:

Completion of legacy issues:

1. GFI scanning (spam filtering) needs to be eliminated from the Exchange servers. ~~Complete 10-17-08~~
2. Internet usage tracking software needs to be implemented.
3. New file servers need to be implemented to replace the X drive[9], the current enterprise storage space available to the UVI community.
4. The acceptable use policy, currently in draft format, needs to be adopted.
5. Implementation of new web servers with possible off-campus hosting.
6. Completion of network management implementation, including the installation of call out alarms and server monitoring alarms.
7. Remediation of F5 load balancers[10] allowing them to properly manage web application traffic.
8. Implementation of enterprise print servers, eliminating the deployment of small LaserJet printers throughout individual offices.
9. Port assessment to validate network traffic/routing.
10. Adoption of an infrastructure maintenance policy.
11. Migration of Self-Service Banner (Banweb) to Linux servers, one on St. Thomas and one on St. Croix.
12. Implementation of single-sign-on, providing users' one login to all authorized applications.
13. Completion of Banner failover using Dataguard.
14. Training for staff.

Redundancy Implementation (Phase 3)

1. Training for staff.
2. Design and implementation of campus wireless systems.[11]
3. Enhancement of physical security of networking closets.
4. Additional fiber runs.
5. Increase of commodity Internet available to the St. Thomas Campus.[12]
6. Replacement of the inter-island microwave; delivery of Internet2 to the St. Thomas Campus.[13]

---

[9] The X drive has been unmaintained and is now out of disk space. Old unused files need to be eliminated.

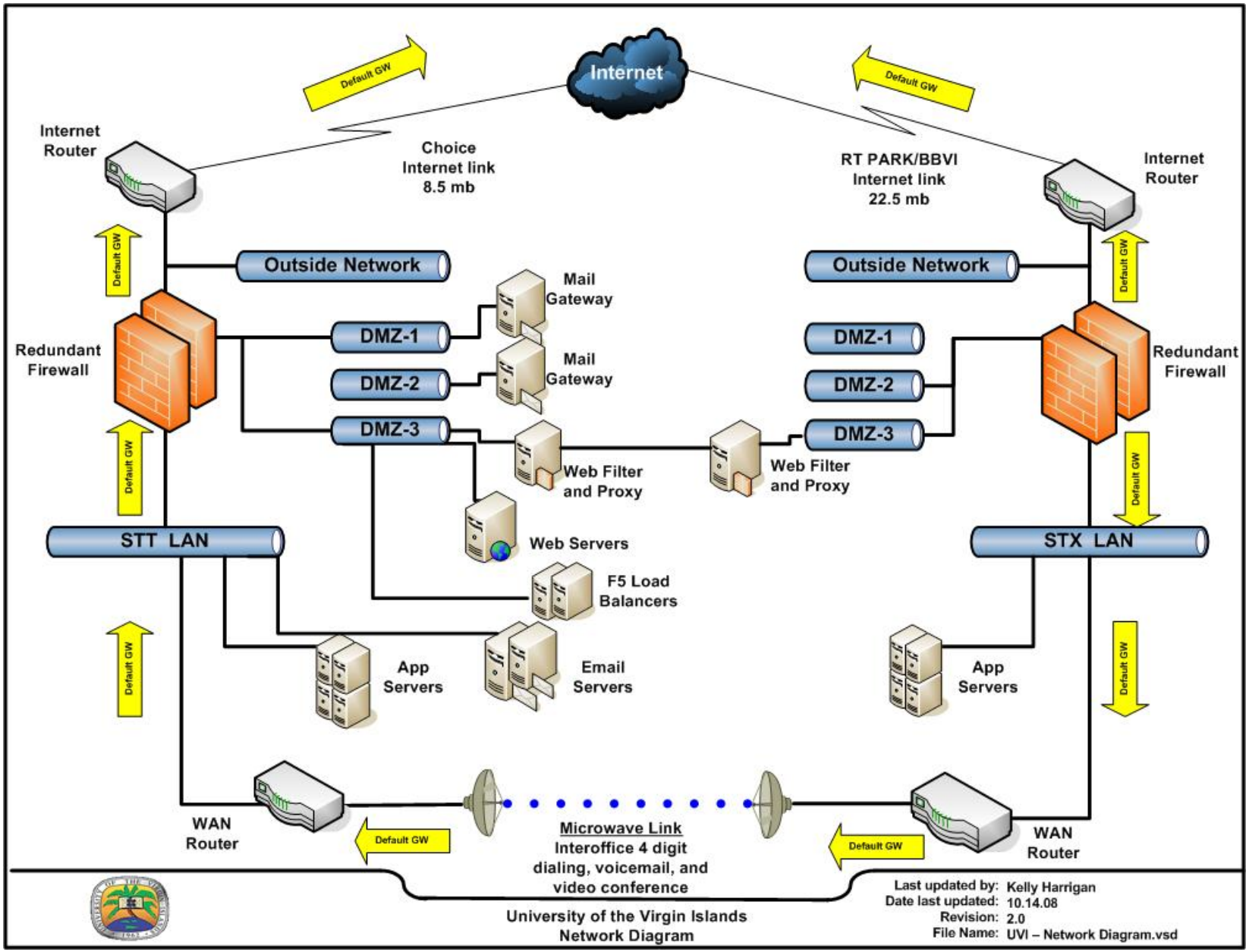
[10] The F5s caused a network outage in August of 2008. Although the problem was remediated, it uncovered that local changes had been made in the configuration that were not documented and did not allow the failover of these devices to work properly. This is scheduled to be remediated in December of 2008.

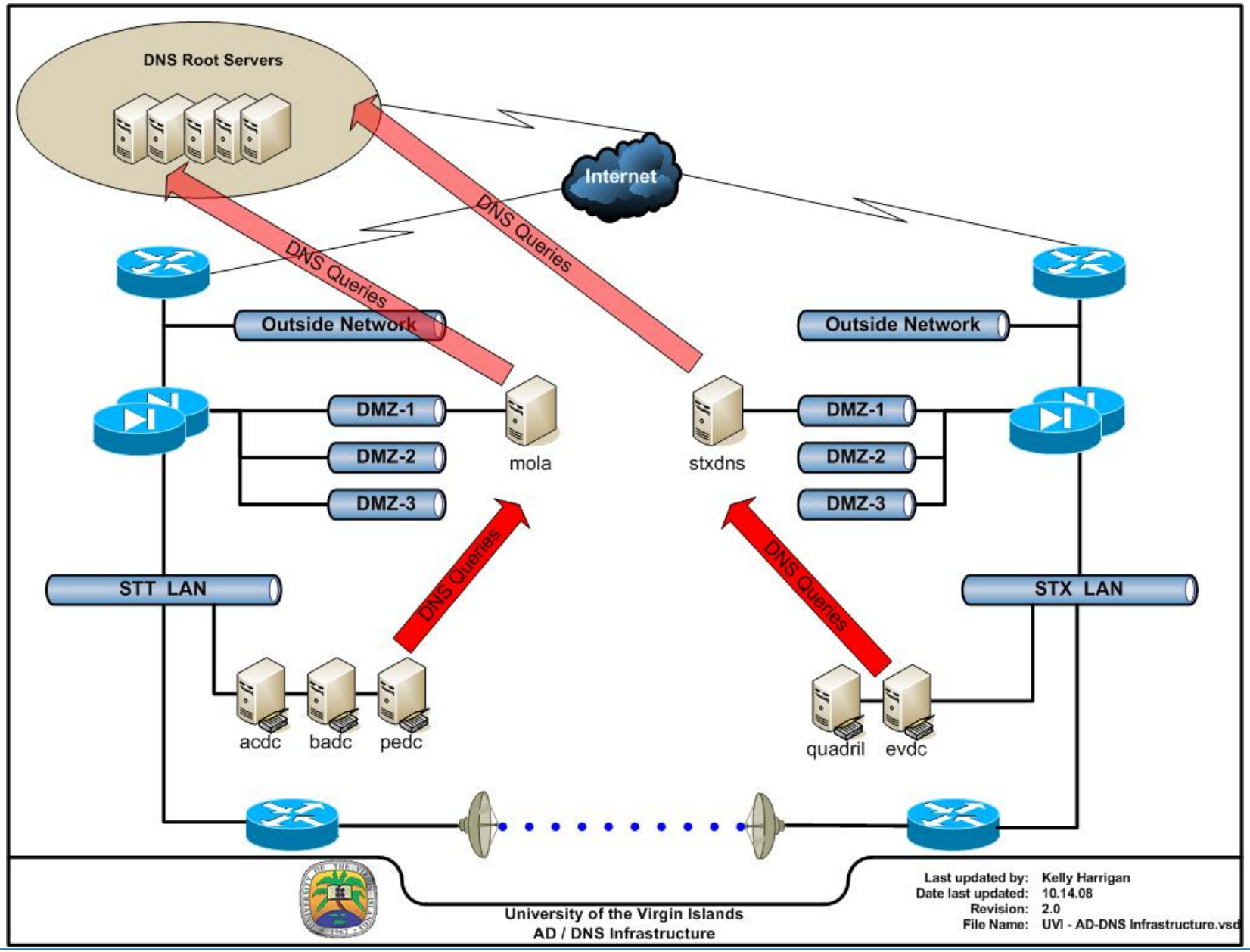
[11] Wireless access in the dorms is scheduled to be implemented in January of 2009. The wireless implementation as a whole is scheduled to begin in January 2009.

[12] Necessary to eliminate slow Internet response times.

7. Implementation of mail bagging, providing a storage space for mail during disruptions to campus Internet or email services.
8. Implementation of failover capabilities among Internet providers.
9. Locate an EXCHANGE server on St. Croix for added redundancy.
10. Planning and implementation of a remote data center.
11. Development of a cyber-infrastructure strategic plan

[13] **This is being done in conjunction with the UVI RTPark and EPSCoR.**


Internet
Default GW
Default GW
Internet Router
Choice Internet link 8.5 mb
RT PARK/BBVI Internet link 22.5 mb
Internet Router
Default GW
Outside Network
Outside Network
Default GW
Mail Gateway
Redundant Firewall
DMZ-1
DMZ-1
Mail Gateway
Redundant Firewall
DMZ-2
DMZ-2
DMZ-3
DMZ-3
Default GW
Web Filter and Proxy
Web Filter and Proxy
Default GW
Web Servers
STT LAN
STX LAN
F5 Load Balancers
Default GW
App Servers
Email Servers
App Servers
Default GW
WAN Router
Default GW
Microwave Link
Interoffice 4 digit dialing, voicemail, and video conference
Default GW
WAN Router
University of the Virgin Islands
Network Diagram
Last updated by: Kelly Harrigan
Date last updated: 10.14.08
Revision: 2.0
File Name: UVI – Network Diagram.vsd


DNS Root Servers
Internet
DNS Queries
DNS Queries
Outside Network
Outside Network
DMZ-1
DMZ-2
DMZ-3
mola
stxdns
DMZ-1
DMZ-2
DMZ-3
DNS Queries
DNS Queries
STT LAN
STX LAN
acdc
badc
pedc
quadril
evdc
University of the Virgin Islands
AD / DNS Infrastructure
Last updated by: Kelly Harrigan
Date last updated: 10.14.08
Revision: 2.0
File Name: UVI - AD-DNS Infrastructure.vsd