**IPv6 Deployment**

**Proposal**

11/12/09

Draft v5

Summary

Recently ARIN sent letters to University Presidents and CIOs, asking them to begin the deployment of IPv6. The world is running out of IPv4 address space. In fact, it may be all gone within 2 years. Organizations now dependent on the Internet are beginning the lengthy process required to migrate to IPv6 addressing. UF needs to participate in this worldwide effort, and begin to deploy production IPv6 across the UF network and applications base. There is risk in delay -- in that UF sites will not be able to interact with external IPv6 only sites and users. This is an important issue for top research Universities worldwide, and may become a factor in winning grant proposals.

IPv6 space needs to be tested and deployed on the UF network. This process will likely take several years to complete, so the work needs to be scheduled to insure steady progress. All aspects of network management should be considered including security. Network and security technology will be the early focus. Then some pilot servers will be deployed on IPv6 to gain experience and prepare for a full rollout in the coming years.

Background

UF is on the leading edge of IPv6 research and testing. In 2009, ARIN asked CEOs to begin the process of deploying IPv6. We are now just getting started with production use.

And we are not alone:

<http://www.oit.umn.edu/network/prod/groups/oit/@pub/@oit/@web/@network/documents/asset/oit_asset_131424.pdf>

CNS recently completed installation of newly assigned IPv6 address space on the core network and in the network lab. We are now ready to extend IPv6 to servers and hosts.

Purpose

It will take several years to make all UF servers and hosts fully IPv6 compliant. To assure timely progress, UF must start now upon a coherent, multi-year, deployment project. The deployment should be divided into a Startup Phase, followed by 2 Rollout Phases.

Objectives

Goals for the Startup phase are:

1. Build a working IPv6 on selected systems/hosts including some enterprise systems.

2. Develop tools and define tasks needed to add IPv6 to any server or workstation.

3. Create detailed plans for the Phase 1 and Phase 2 rollouts.

Approach

From a policy and management perspective, IPv6 is just like IPv4. The UF President via delegation to the CIO, manages UF IPv6 address reservations and assignments from FLR. Implementing IPv6 provides an opportunity to refresh network-addressing standards and possibly tie these into a future UF-wide IPAM project.

CNS Network Services will coordinate both initial startup and Phase 1 IPv6 deployment activities, because technical issues remain to be resolved in network configuration and management. NS will work with the IT Security group and others to develop an overall list of issues to be addressed. A small, representative, IPv6 Working Group of technical experts will be created to perform pilot tests and resolve problems. The Working Group will also identify, analyze, and refer any issues needing further review to the UF IT committees in the existing and emerging governance structures.

The Working Group will meet monthly and additionally as required to insure progress. They should begin with the larger issues and gradually expand to include all network and system design issues. Budget needs should be identified sooner rather than later.

Scope

Work will be completed in two formal phases divided along Fiscal Year (FY) boundaries. Our goal is to deploy IPv6 on every external-facing UF server by June 30, 2012. Although that may seem like a rush to some, others worry it may not be aggressive enough. Governance and external factors such as the emerging IPv4 shortage will help to determine the urgency and pace of Phases 1 and 2.

Startup – FY 09-10

We will start work with a series of tests, tools development, network design standards and pilot installations. Next, we will complete evaluations of IPv6 readiness for all network-based services. And then, we will address DHCP and host/server issues. End user departments may ask the Working Group to join these early IPv6 trials. Due to security concerns, HIPPA and PCI subnets will most likely be deferred until Phase 1.

Phase 1 – FY 10-11

Phase 1 will include all UF enterprise systems, all E-Mail servers, and many web sites. The goal is to make many external facing UF services available via IPv6 by June 30, 2011. A large number of hosts in distributed networks should also be working on IPv6 and form a test base. A list of all external facing servers will be developed in Phase 1, in order to plan the remaining Phase 2 work, and deadlines for all servers will be set.

Phase 2 – FY 11-12

All remaining servers will be deployed on IPv6. All end user workstations should also be deployed on IPv6. Special case may be granted an extension, with a completion plan.

Architecture

The dual-stack approach will be used starting with DNS servers because tunneling and other technologies will break many applications. Research on IPv6 tunneling and other technologies may occur also, but is outside the formal scope of this project.

Startup Schedule

11/09: Develop and approve the project Charter. Form the IPv6 Working Group, and hold the first meeting late in the month. Finalize the IPv6 approach and address space assignments on campus. Ask HSC/Shands if they wish to apply to UF for a separate /48 delegation from UF’s reservation. This will likely be approved if a reasonable use plan is presented, and this step may be done now or at a later date. Review the rationale and seek endorsement of the project plan address scheme at ITAC-NI, ITAC-ISM, and other committees as appropriate.

12/09 – Ask the UF Interim-CIO to approve the IPv6 address plan. Engage the Security group on tool development and quarantine/zone methodologies to enable testing to begin. Begin installing new code on the UF core network to better support IPv6. Develop DNS procedures and standards. Begin DNS deployments.

1/10 – When the new CISO is hired, invite a few key web and server administrators to participate in IPv6 trials. DNS deployment should now be complete. Evaluate Bluecat and other DHCP mechanisms and standards. ITAC-ISM should consider exceptions for IPv6 pilot tests. Develop and deploy IPv6 validation tools in the NS lab.

2/10 – Security begins testing new IPv6 tools and applications. Begin investigation of stateless DHCP. Begin a targeted PR campaign. Add IPv4 counters to UF IT web pages to raise awareness. Create a web page for public information about the IPv6 Initiative.

3/10 – Review plans with new IT Infrastructure committee when it is convened. The Working Group will present options for stateless DHCP. Pilots of IPv6 can now begin on production servers.

4/10 – When the new CISO comes on board, review again all project work to date. CNS will develop plans for the FY 10-11 budget to support IPv6. New costs should be minimal and will likely be absorbed within the normal budget process.

5/10 – Order additional equipment as required. Technical evaluations continue. Prepare a summary report on all Startup activities and results.

6/10 – The new CIOs for both UF and the Shands/Health Science Center should now be on board. They will review progress in the Startup Phase, and confirm the approach and priorities for the formal Phase 1 task plan.

Organization

Project Lead

Dan Miller is responsible for overall project management, work plans, and scheduling of the Working Group tasks. Chuck Frazier, Tim Fitzpatrick, and Mike Conlon will serve as project sponsors.

CNS Network Services - Core Network Engineers

Explore IPv6 design decisions re routers, ACLs, firewalls, wireless, and related issues.

CNS Network Services – Software Team

Explore IPv6 design decisions re DNS, DHCP, and network/host monitoring.

UF IT Security and Compliance Group

Develop IPv6 security standards and related tools. Together with CNS Network Services, co-approve IPv6 early adopter requests from campus departments.

Proposed Early Adopters in the Startup Phase:

CNS OSG

AD Team

DHNet

Budget

CNS and UF IT Security and Compliance will begin planning for any needed budget expenditures to support IPv6 in FY 10-11.

Considerations

Intrusion Detection System is a concern regarding support for IPv6. Support there will be necessary in order to rollout IPv6 to significant servers and user populations. Network analyzers such as “sniffers” can decode IPv6 because it is just another protocol so the IDS should be a major barrier to progress.