UFNet2 – Standards

Scope

UFNet2 is the name of the next-generation, single network infrastructure for the University of Florida. With modern technology is a possible to provide a single, common, robust, high-performance network infrastructure that can meet all performance and security requirements the institution has to meet, while at the same time provide the flexibility and agility to respond quickly to needs of the education and research communities. Thus UFNet2 is an enabler to bring UF to the Top 10.

The technical foundation of UFNet2 is Multi-Protocol Label Switching (MPLS) coupled with Virtual Routing and Forwarding (VRF) which provide for Layer 3 Virtual Private Networks (L3VPN). As of August 2014 the backbone of the UF network, including the Academic Health Center (AHC) has fully deployed these technologies. Furthermore, most building networks on campus already support these technologies, which can be enabled with minor changes. By deploying multiple L3VPNs across a single common network architecture, a collection of computer systems, data, and users which play a common role and have compatible needs, security posture and access requirements, may be collected into a virtual network environment, no matter their location on campus, which is tailored to fit those needs. See the accompanying "UFNet2 Vision" document for more information.

To create a useable network infrastructure it is necessary to set and meet expectations for the operation of the infrastructure.

1. All requests for changes to UFNet2 network environment association should be made in consultation with the local IT support group. Individual users need to be made aware of the implications of changing from one environment to another.
2. Any computer connected to a network environment will also use services from that network beyond the simple connectivity to the network and the Internet. The section below provide details on how to handle these services and to make sure they are set up correctly.
3. Monitoring infrastructure is being deployed, with easy access to any user, to check and verify the performance characteristics of the network links crossing the campus.
    a. This will allow users to make an initial assessment whether problems are due to UFNet2 or to local or remote end-point devices.
    b. It will also allow network engineers to go back in time and check the network activity around the time a user noticed a problem, rather than having to wait for the problem to occur again.

Services

Whenever desktop and laptop computers are connected to one of the virtual Network Environments (vNE), namely Academic, Administrative, Health, ScienceDMZ, External, the users of these computer systems will need access to the usual list of network services.

Some services come naturally with the vNE, such as DHCP, DNS, but others are typically provided by local IT support. The most prominent are:

1. Printing service, including multi-function devices for copying and scanning.
2. Network data storage service.
3. Web pages and web services that have access restricted to certain subnets, including VPN.

This document only describes a minimal set of the most common services. Different colleges and departments may provide additional services that need to be taken into consideration.

Standards and procedures: Printers

- Printers are provided by the organization responsible for the users.
- For areas with "mixed environment" users:
    - Printing may be accomplished either via print servers, or via direct IP printing.
    - In the case of print servers, the owner of the environment will provide the print servers, and standard printing protocols such as LPR, or RAW will be used to communicate between the print server and printer.
    - In the case of direct printing, the user is able to directly communicate with the printer using LPR or RAW.
    - The owner of the users will permit either the print server or end users to cross environments and print to the printers on a per-printer basis for existing printers.
    - It is encouraged for new printers to be set up in this way by default.
- If entire departments or colleges are relocated into an environment, and there are no "mixed environment" users, their printers may move with them. This is decided on a case by case basis.
- Best practices dictate that network printers and multi-function devices be connected to special VLANs and/or subnets to control access to them from the Internet and parts of the UF campus that do not need access. This principle is carried forward in the vNE design.
- The University printer management program has brought many printers into a special VLAN already to allow management and tracking by the vendor (Xerox). More printers will be configured this way as the program grows across the campus.
- Printers housed in the Health environment will be exposed to all vNEs by moving them into the AHC "campus" zone. Additionally, all AHC users are moving to a direct IP printing model, so no print servers are necessary. AHC has developed a process to accomplish all necessary tasks using existing provisioning tools.

Standards and procedures: Multi-function devices scanner and FAX

- Multifunction devices typically provide copying, scanning, and faxing capability
- Copying has no reliance on the network, thus is not affected by this service.
- Scanning typically may use either e-mail or a file-share to store data. Scan to email will work without any changes required. This is the recommended solution. Scan to file-server is the recommended solution for HIPPA or Restricted data when the printer and the file-server are in the same environment, and is not affected by this service.

- Standard faxing is not affected by this service as it uses either analog lines or emulated analog lines over VoIP.
- Fax to IP using the campus Fax server will be supported by all environments since it's an "outbound" service once a printer is made accessible to other environments through the normal printing process outlined above. This service is not yet widely used around campus.

Standards and procedures: Network data storage

- The purpose of the vNE is to increase flexibility and configurability of network access for faculty and staff, while at the same time maintaining the highest standards in security and regulatory compliance. Therefore network data storage servers in one vNE can allow access only from devices in vNE with the same or higher levels of restrictions on data access and data mobility.
- It is quite likely that a single server shares data of multiple types. For example a server in the Health vNE may hold unrestricted data for faculty and staff who never use PHI data as well as PHI data for researchers who work with such data every day.
- To allow the faculty and staff who never work with protected health information (PHI) data to be moved to another vNE, such as Academic or Administrative, it will be necessary to provision their data from a different server.
- Shared file storage will be provided by the "owner" of the network environment using existing storage infrastructure. Data can be moved without the need for significant investment in equipment or staff so that the faculty and staff have access to their data on their vNE after their computers are moved to the new vNE. AHC will continue to be responsible for the Health vNE, and UFIT-EIO will provide storage for AHC users in the Academic Environment. Research Computing will provide ScienceDMZ specific shared storage for devices in that vNE.
- The process to move data from one environment to the other should be agreed to by the owners of both the old and new environments. This process will also examine the data and verify it is appropriate to move to its new location.
- Unit IT support staff will be provided the necessary access to manage shared storage in any vNE their users have access to, and to coordinate any changes.
- The reorganization of network data storage servers such that those that hold restricted data are clearly separated from those that hold only unrestricted data will reduce the risk to the University and improve the manageability and auditability of restricted data assets at the University.