Campus Network  
December 13, 2005

**Present:** Carl Warrene, Don Larson, Chad Gratton, David Belgarde, John Wold, Tony Houdek, Jay Smith, Kevin Danielson, Brent Logan, Jeff Cox, Jing Wang, Brad Miller, Josh Jones, and Bonnie Jundt  
**Absent:** Dale Ricke, Barry Pederson, Roy Beard, Larry Fisk, Doug Osowsk, Renetta Johnson, Karl Martin, Corey Quirk, Harold Bruce, Michelle Rakoczy, and Corey Shock

Minutes from November 8, 2005 – Approved.

Announcement: Jim Shaeffer left his CIO position at UND in November. Dorette Kerian has been named the interim CIO and is therefore leading the UUTC.

**Clean access and guest access for campus wireless and open ports** – Kevin  
After discussion in our last meeting, Kevin developed a document to summarize and provide a plan to move forward with network authentication for wireless and open ports. It was emailed to the Listserv. It specified the desire for the following:

1. Limited guest access with no end user configuration.  
2. Full network access after authentication with a username and password.  

This document also provided design details and considerations. We began looking at options in Cisco Clean Access and it appears that it is capable of providing this function; however we haven’t done any testing. Limitations were noted as follows:

1. Only the authentication process would be encrypted, but not the actual transfer of the other data.  
2. This design relies on the application to provide for the security and privacy of sensitive information.  
3. An agent must be installed on all systems where authentication is required for full network access. This involves automatic remediation process to get the Clean Access agent, Windows updates, and up-to-date antivirus software.  
4. There are some operating systems that don’t have Clean Access Agent support.

Craig Cerkowniak noted concerns from the IT Support Sub-council as follows:

- Support issues: who would provide support at the Union and Library, the first two places where this service is likely to be implemented? Are administration and staff in these two locations informed and aware? Most questions or problems are likely to go to the Info Desk and the Reference Desk, therefore it is important that there be an awareness and acceptance. Neither Jay nor Tony were overly concerned, as they indicated that are providing the support for wireless network users in these two locations already, but it was decided to set up a meeting as soon as possible to discuss the details.
- Which applications should be allowed in the guest access role? It was suggested that web and secure web might be adequate.

Additional discussion and suggestions included:

- UND could consider securing commercial links for unauthenticated access to protect the und.nodak.edu domain from being blacklisted (there may be legal issues with this).
- Desire flexibility with consideration for additional applications that might be requested for use on wireless and open port networks. IPSec VPN was suggested as a secure application that will be required.
- There will be issues to resolve with authenticating unusual devices, such as PDAs with Palm operating system.
- Network Services will begin with the setup and testing and work with User Support to develop the user information. Providing that things go well, the first week in January was suggested as a possible target for implementation at the Union and Library.
- Authentication using multiple LDAPs across campus is desired and recommended by this sub-council.

**Nessus status** – Kevin  
At our last meeting we had an inquiry regarding the use of Nessus for vulnerability scanning. At that time the ITSS’ system running Nessus was not adequate for production use. Since then a different system was brought up and it is now available for system administrators across campus who are interested. These
accounts would be set up with access permissions for the local area network that supports the systems for which the system administrator is responsible. Anyone wanting an account should contact either ITSS Network Services or ITSS Helpdesk. Because the Nursing VLAN is behind a network firewall, they are not currently able to scan the systems that are using private numbers. This will be true for all firewalled networks. There is a possibility of allowing Nessus inbound through the firewall, but security implications need to be considered prior to making that change.

**McAfee update** – Brad
The NDUS currently has an enterprise license agreement with McAfee which will expire in June 2006 and is in the process of negotiating a new agreement with McAfee, while also looking at other products. Brad brought forth the interest expressed from this group in adding anti-spyware into the new agreement. Jeff Cox suggested that anyone can get a login for the McAfee site and download a number of products covered in our current enterprise license agreement. The grant number to gain access is 809465-NAI.

Brad inquired if there is any other security software that might be of general interest that should be considered for licensing across NDUS campuses. Products that have been suggested are Blink, Roving Planet or Cisco Security Agent. Multiple areas on campus at UND as well as other institutions are using Deep Freeze.

**Status and next steps with campus infrastructure upgrades**
- **Cabling update**
  - Work has recently been done in Carnegie. With the move of Enrollment Services from Twamley to Carnegie some cabling upgrades and communications room improvements were required.
  - Aerospace requested some improvements in Ryan Hall which is next on the schedule.
  - As the mainframe equipment and cabling are removed there may be some needs for cabling upgrades in Merrifield and UpsonII that should be considered along with other areas of campus.
- **Equipment**
  - We’ve been moving forward with connecting buildings with gigabit fiber links to the campus core network. The most recent upgrades have been Abbott, Starcher, Witmer, O’Kelly, McCannel, Hughes Fine Arts, Hyslop, Leonard and the Housing Office. We are ready to connect the Medical School.
- **Review of plan and FY06 funding request**
  - We will continue to identify where there are needs for network infrastructure updates to be prepared to utilize any funding that is approved for this purpose. At this time no funding has been approved for FY06. In April 2005 the requests taken forward for FY06 included:
    - Continue cabling upgrades as needed (intra-building risers have been noted as inadequate in numerous locations),
    - Wireless networking support
    - Gigabit and power-over-ethernet switches
    - Network security solutions (firewall, intrusion detection and prevention, etc.)

**State network, network equipment, and wireless RFP updates** – David
There was a wrap-up meeting in Bismarck yesterday for the state RFPs.

The network equipment contracts have been signed. Both Corporate Technologies and Qwest were awarded contracts for network equipment.

Negotiations are still in progress with Dakota Carrier Network (DCN), the current contract holder for STAGENet, for the network transport. The length of the new contract is 7 years with the possibility of three one-year extensions. The new network will consist of gigabit fiber rings around the state with nodes in Bismarck, Fargo, Grand Forks and Minot. There are four distinct rings defined: one each for state government, higher education, K12 education, and the fourth for research and special needs. The existing contract has postalized rates for T1 access links. That part of the contract was renegotiated to include two different rates, one for rural and one for urban, with the rural increasing about $130 and urban decreasing about $50.
The Internet access contract was signed with Sprint, the current provider. The capacity will remain at 622 Mbps on each side of the state.

Responses to the cellular and wireless data networking RFP were not acceptable. Alltel and Verizon responded but the coverage and speed for data wireless networking aren’t adequate throughout the state.

**Networking updates from around campus – Attendees**

**Jing**
CILT is working with ITSS to implement networked monitoring of equipment in the classrooms. A private VLAN will be built for these classrooms which will communicate with the private VLAN that was recently built for CILT.

**Kevin**
We had someone here last week from Infoblox, our DNS vendor, to provide direction and assist with DNS configuration for internal networks that are behind the firewall module.

Kevin, Brad and Jeff led a discussion on the warning of the Sober virus/worm that is supposed to begin spreading via email on Jan. 6th. Kevin suggested that sites might be blocked at the campus gateway or a null route added to prevent outbound propagation of Sober infected email. A group of people, including Brad and Kevin, began talking about how to address SPAM on campus. Brad said he will continue working with others across campus to address general email policies and procedures, including email security. A network person will be included for discussion on DNS, blocking ports or sites, etc.

We are working on the networking for an identity management project that will provide a single sign-on solution for web based services through a portal. A consultant is scheduled to be here early in January so we will have more information at our next meeting. At that time we will be encrypting U-mail, using the load balancing switch that will be installed for this project.

**David**
Three have been some issues with video quality and VBR throughout the entire network. IVN will be doing some testing with a Fathom analyzer, from Applied Global Technologies, which is designed specifically for real time analysis of H.323 audio and video. It does test calls with video end points and monitors the traffic to isolate and identify faults.

**John**
We’ve been working with Snort for intrusion detection and currently have two sensors running. It’s been educational; we’ve learned a lot about what is on the network. This allowed us to get the firewall locked down completely, with minimal impact to services. Snort alerts have gone down to about 100 per day from 20,000 when we started. We’re also considering the LaBrea Tarpit to prevent scanning.

Aerospace will be working with wireless and WLSE over the holiday break.

Next meeting – February 14, 2006