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

Minutes from Oct. 11, 2005 – Approved

DNSone appliance for DHCP and IP management – Kevin
ITSS is planning to purchase additional DNSone appliances to provide domain name services for private
networks at UND. We are planning to delegate DNS administration for sub-networks to LAN
administrators where possible. Harold Bruce volunteered to work with ITSS when ready to test the
delegation for these sub-domains. We are still waiting for final approval of a change in NDUS DNS policy
that will allow institutions to be authoritative for A records, using institution.edu, rather than
institution.nodak.edu, for their IP address space. The appliances will also be used for DHCP services.

Planning for demonstration of Microsoft’s Live Communications Server integration with Polycom’s
MGC100 MCU – David
Polycom recently announced that they are working with Microsoft to provide a seamless integration with
Polycom’s videoconferencing endpoints and bridging equipment with Live Communication Server and
clients for voice, data and video collaboration. When meeting with Polycom last week we asked them to
put together a demonstration of this joint venture and we hope to get it scheduled for some time in
December. The demo will be offered statewide and the location hasn’t been determined yet. David
provided handouts of related information.

Clean access and guest access for campus wireless - Kevin
After numerous ongoing conversations with this group about wireless and open network port access we’ve
looked into providing a limited guest level access that wouldn’t require authentication or checks for
updated patches. We contacted Cisco to discuss different options with existing solutions, such as Cisco
Clean Access (CCA), switches with 802.1x support, Infoblox DNSone, etc. Because we don’t have
knowledge or control of the many diverse end stations on the network, CCA seems to be the best solution
for UND at this time. It could be set up so that client access would not be required for a guest level of
network access. With agreement within this group, we’d like to recommend that a role be created in CCA
that would not require a client download, nor the need to check for clean and updated systems. A web
browser window would be presented when accessing the wireless or open port network that would provide
a choice to either authenticate (requires entry in UND LDAP) for full network access or guest level access
without authentication for limited access to services as recommended by our group and approved by
campus. The authentication process would be encrypted however this solution would not encrypt the rest
of the traffic. Details of authentication, or use of CCA in labs, will continue to be discussed along with the
possibility of a particular set of users having a specific profile to be allowed access to particular resources,
such as the School of Medicine clinicians. CCA roles are based on VLANs. There are many possibilities,
but it needs to be manageable.

Prior to putting a lot of effort into testing guest access Kevin asked for recommendations for specific ports
that are most likely to be needed. Ports 80 and 443 for web and secure web were agreed upon. SFTP was
proposed as a possibility. Telnet was discussed but dismissed as insecure. Guest level access would
possibly start with a test and move to a pilot at some location prior to implementing campus-wide.

The benefits of authenticated and clean access to the network are understood and accepted by members of
this group. Concerns for ease of appropriate access and for adequate support for related issues remain,
while at the same time there is interest in having the capabilities of CCA available throughout campus.
Aerospace is considering 802.1x for user authentication. If they make a choice to provide CCA services they would run their own server on the Aerospace network. Users moving between the Aerospace network and the rest of the campus network would not be impacted if different solutions were implemented due to the built in support for 802.1x in Windows XP. Currently there is some confusion for Aerospace students when they try to connect to the ITSS supported wireless networks if they are not accustomed to using their U-mail login. ITSS could set up RADIUS to query the Aerospace LDAP server to get around this issue. Michelle suggested that Aerospace may want to consider installing the CCA agent on the laptop images they set up and support for students. There were a lot of issues in the residence halls with these laptops at the beginning of fall semester. John suggested that Michelle call Rodger Copp at the Aerospace Helpdesk to make this request.

**Nessus**
Chad Gratton asked about checking the integrity of some of servers for which he is responsible. He brought up NMAP and Ethereal as possible tools. A Nessus server was available and offered to this group some time ago but due to problems on that system it was shut down. A different server was brought up but the account information wasn’t carried over. The current system at ITSS is not adequate for production use. If there is an interest within this group for continued use of Nessus we will attempt to identify a system and get the application installed and then inform this group so accounts can be requested from Network Services. These accounts are set up to allow LAN administrators access for scanning systems on their local VLAN.

Brad will be working with the different areas of campus to help assess vulnerabilities as he begins with security assessment. He is considering Nessus output as one of the tools for this process.

John cautioned our group on the risks associated with vulnerability scanning with Nessus. Some systems or processes will become inoperable during a scan. Only a system administrator who has knowledge of the system and can take corrective action should scan a system, and then only during a time when it is acceptable to assume the risk.

Until the ITSS Server Team has an opportunity to get a Nessus server up and running again Terry Meland offered to assist anyone with scanning their systems.

**Email servers - status of filtering – Kevin and Brad**
Email port filtering is being discussed because NDSU was blacklisted from SMTP1.nodak.edu. The main SMTP gateway for the nodak domain was being used as a relay. Kevin requested that valid email servers be identified so a filter could be established that only allows known email servers access for port 25. Kevin and Brad are working with ITSS email administrators to develop policies for handling spam. Brad expects to get subject matter experts, or people who are administering email servers, from around campus together to identify some best practices and decide how we can improve email security. This might involve network level practices as well as email system administration. The Business School has asked Network Services to block outbound port 25 from their subnet.

**IT Security update – Brad**
The slides from the IT Security Conference held in Fargo last week will be made available for anyone who is interested. Jack Suess from the University of Maryland, co-chair of the Internet2 Security Task Force, talked about where many universities are going with security initiatives, focusing on data privacy and classification, user education and awareness, incident detection, handling and response. These are the same issues that UND is currently addressing. Email statistics showed that as much as 60-80% inbound email is spam, 15% inbound email has an attached virus, and phishing for personal information for purposes of identity theft has increased.

The 8.x version of McAfee, which is available at UND, includes anti-spyware. After a short discussion of anti-spyware functionality in the existing NDUS McAfee solution, and the value of other products, Brad agreed to look into the existing McAfee contract. He will take a recommendation forward from this group to consider additional functionality in future anti-virus and anti-spyware solutions.
Tracy Mitrano, from Cornell University, did a presentation of the history and concerns of copyright violations in higher education. President Kupchella’s updated strategic plan includes a direction to implement approved policies, standards and practices to address copyright concerns (e.g., publicize and communicate the requirements of the Copyright Law and the DMCA).

Brad plans to address handling and education of copyright in the incident response and acceptable use planning activities that he will be doing throughout campus.

The Communication Assistance for Law Enforcement Act (CALEA), originally only addressing telecom carriers, has recently become a concern to higher education because the FBI and DOJ went to the FCC and requested compliance for the capability to tap into communication from broadband internet providers. As it reads now, we have 18 months to be in compliance with CALEA, however higher education is working toward a request for exemption. Compliance would likely require major network upgrades. Real-time remote monitoring would need to be in place. Both Educause and ACUTA are gathering information and working toward a request for a higher education exemption for strict compliance with CALEA.

Brad showed our group the area of his web site, itsecurity.und.edu, where we should look for information on security policy development. There is a draft available of the process used for developing security policies and guidelines for the campus. Two policies currently being worked on include student acceptable use and incident response. Information and tracking of the ongoing development of policies, guidelines, and procedures will be available. The IT Policy Review page will show the progress and will have schedules of related events. Brad encouraged participation from anyone in our group in areas of interest.

Status and next steps with campus infrastructure upgrades

- **FY06 plans and funding**
  Funding for the FY06 campus network plan will be considered, along with other pending budget requests, after final enrollment figures are available for spring semester. We may learn more at our February meeting.

- **Cabling**
  Cabling still continues in some areas with carry-over funds from last fiscal year. John requested consideration of cabling in a couple of areas in Ryan Hall where Cat6 upgrades should be done. John will email the information to Larry.

- **Equipment**
  Gigabit distribution switch upgrades are complete in most of the locations planned for FY05. Kevin is checking quality-of-service configurations for NDIVN locations to verify correct settings. FY05 upgrades should be complete before our next meeting and we will provide a complete list at that time.

Next meeting – Dec. 13, 2005