

ILLINOIS STATE UNIVERSITY
CAMPUS NETWORK PLANNING COMMITTEE
REPORT

August 27, 2002

Approved by ECAT 8/27/02

CAMPUS NETWORK PLANNING

INTRODUCTION

On November 30, 2001 the Campus Network Planning Committee met to begin the process of reviewing the University network known as ISUnet and to help Telecommunications and Network Support Services formulate a number of special multiyear network project recommendations. The Committee was comprised of members who represented major academic, administrative and operational segments of Illinois State University and each member was well positioned to provide insight into the networking needs of the University as well as insight into the networking needs of their area or department. This planning document has been reviewed by the Executive Committee for Academic Technology (ECAT), revised, and was approved by ECAT on August 27, 2002.

CAMPUS NETWORK PLANNING COMMITTEE

Bill Blomgren (Committee chair)

Tak Cheung (CAS/Biology/department chair)

Ken Fansler (COE)

Scott Genung (TNSS)

Anu Gokhale (Technology/faculty)

Eric Hodges (VPFP/VPUA)

Krena Hoyt (Milner)

Susan Kossman (MCN/ECAT)

David Kuntz (CFA)

Melissa Enderlin Pitcock (VPSA)

Kate Plantholt (CAST/ECAT)

Rudy Radosevich (CISS)

Dave Schaafsma (COB)

Jason Tucholke (RESNET)

OVERVIEW OF THE PLANNING PROCESS

The purpose of the Campus Network Planning Committee was to provide Telecommunications and Network Support Services (TNSS) with guidance in terms of its 3 year planning efforts for ISUnet. During the initial meetings TNSS provided the Committee with a detailed overview of current ISUnet projects and future TNSS network initiatives. This review was designed to help familiarize the Committee with the overall direction of TNSS.

Areas Reviewed

- Desktop Fast Ethernet
- Gigabit over copper
- Wireless (11b, 11a, 11g)
- VPN (Virtual Private Network)
- Public access networks (public jacks)
- IDS (Intrusion Detection System)
- ResNet
- Internet connectivity
- Cable modem access
- QoS (Quality of Service)
- Peering with apartment complex networks
- VoIP
- Content caching

The Committee was then asked to discuss potential network projects that they felt should be recommended to TNSS for completion during a 3 year time frame between FY03 and FY05 and to rank these projects in their order of importance.

RECOMMENDATIONS

The Campus Network Planning Committee spent a considerable amount of time reviewing the direction of Telecommunications and Network Support Services (TNSS) as this direction relates to ISUnet and the networking needs of the University. The recommendations contained here are intended to identify areas of greatest importance to the overall University community. These recommendations are also intended to serve as a guide to help TNSS prioritize their resources and work efforts over the next 3 years.

Expand Internet Capacity: Expansion of Internet capacity is the single most important project that should be undertaken by TNSS over the next 3 years. It is recommended that during the summer of FY03 the University's Internet capacity be increased by at least 35% to around 90 Mbps. This is viewed as necessary to address the projected increase in Internet users resulting from the completion of

the Watterson (RESNET) project in January of 2003. By the Summer of FY04 it is recommended that Internet capacity be at least 110 Mbps and by FY05 at least 130 Mbps

The practice of maintaining at least two separate Internet service providers should be continued. One of these should be the Illinois Century Network (ICN) and the other should continue to be from a non-state network to provide better redundancy in the event of a single network failure. As the University begins to move forward with Internet 2 connectivity, additional Internet capacity will be required.

Changes are also recommended in the local delivery method between Verizon and the University. The current multiple DS-3 (45 Mbps) connections between Verizon and the University should be replaced with a more efficient and cost affective OC-3 (155 Mbps) connection. TNSS should continue to pursue a second point of local network entry into the campus to further safeguard the local delivery of service in the event of a Verizon local access network failure.

The continued use of packet shaping technology and quality of service (QoS) applications are critical to the effective use of both the University's Internet resources and for the control of future Internet access costs. The use of these controlling technologies should be continued and augmented as necessary to manage the Internet resources of the University.

Year 1: Increase Internet capacity to at least 90 Mbps and add a connection to Internet 2.

Year 2: Increase Internet Capacity to at least 110 Mbps and continue to explore opportunities for a second local network access point for the campus other than Verizon.

Year 3: Increase Internet capacity to at least 130 Mbps and expand Internet 2 connectivity through the ICN or other means.

External Off Campus Access: Secure off campus network access services were not widely available from the business community when the University modem pool and Verizon DSL service agreements were first developed. Faculty, staff and students are now being offered an ever-increasing number of convenient off campus network access choices by non-university service providers such as Verizon and Insight Communications. These choices include technologies such as DSL, cable modems, telephone dial up modems and wireless network access all of which are offered at competitive prices. With the development of these new network connectivity options, by the business community, the role of the University as an Internet service provider and private modem pool operator for off campus users is no longer as essential as it once was.

In today's world, personal off campus access to the network resources of the University needs to be global in nature, secure, and yet locally available to faculty, staff and students at a competitive price. To accomplish this, faculty, staff and students must be free to use whatever personal off campus access method best meets their personal and financial needs.

In support of a secure, global access concept, TNSS should develop a virtual private network concentrator (VPN) solution. This solution should allow faculty, staff and students to gain secure, off campus access to the network resources of the University using any Internet Service Provider of their choice. This solution should permit access through off-campus cable modems, DSL service over telephone lines, service through commercial modem pools and access through off-campus apartment networks and wireless. By developing a VPN solution it is anticipated that the University would no longer need to operate a private modem pool service or serve as a private Internet service provider for ADSL subscribers.

The extent to which TNSS should continue to act as an Internet service provider and private modem pool operator for off campus users will need to be determined by early FY05. Cisco Systems has announced that within 3 years they will no longer support the current modem pool hardware and software used by the University. If the University is to remain in the modem pool business this hardware and software will need to be replaced. This replacement cost is estimated to be in excess of \$100,000 and would be in addition to the annual modem pool telephone line and maintenance cost of about \$180,000. The cost of subsidizing Internet service for more than 500 off campus University DSL subscribers and the associated service issues, such as help desk and network support, should also be addressed in this same time frame.

Year 1: Set up a VPN concentrator, distribute free VPN client software to faculty, staff and students and promote off campus network access through non-university service providers.

Year 2: Expand the VPN solution and continue to promote off campus network access through non-university service providers. Monitor for reductions in modem pool usage and reduce modem pool size accordingly.

Year 3: By early FY05 determine the extent to which TNSS should continue to act as an Internet service provider and private modem pool operator for faculty, staff and students to gain access to the network resources of the University.

Gradual Deployment of Fast Ethernet and Gigabit Ethernet: Fast Ethernet and Gigabit Ethernet should be allowed to expand at a natural rate based on user need and the availability of funds. The current economic conditions will also have

a slowing affect on the number of new users able to deploy Fast Ethernet, at least in FY03. It is recommend that TNSS begin to allow the deployment of Fast Ethernet to the desktop starting in FY03. The use of Gigabit Ethernet for high capacity centralized server applications should also be piloted in FY03. By FY04 it is recommended that Gigabit Ethernet for servers move from a pilot project to a chargeable production service. At that same time there should be an incentives program established to encourage departments to move high capacity servers to Gigabit Ethernet. By FY05 TNSS should be positioned to support service requests for the deployment of Fast Ethernet to the desktop in most areas of the University outside of the residence halls. At this point, Fast Ethernet my also become the new University desktop standard and if so, a possible downward adjustment in installation and monthly service charges should be considered to bring it in line with current Ethernet pricing.

Year 1: Begin offering Fast Ethernet to the desktop, where service and wiring is available, and conduct a Gigabit Ethernet pilot.

Year 2: Offer Gigabit Ethernet for servers and an incentive program to move high capacity servers to Gigabit Ethernet. Continue to expand Fast Ethernet service as required.

Year 3: Be prepared to support Fast Ethernet to the desktop in most areas of the University and review service charges for Fast Ethernet should it become the desk top standard.

Limited Type 1 (Legacy) Data Wiring Replacement: While existing type 1 data wiring is viewed as a constraint to the deployment of Fast Ethernet and Gigabit Ethernet this constraint is not wide spread enough to support the expense associated with a total campus wide rewiring effort. It is recommended that the removal and replacement of type 1 data wiring be considered on a case-by-case or individual project basis.

This recommendation is based on issues related to overall network bandwidth capability, both on and off campus, current utilization rates of campus servers, current demand for high-bandwidth desktop applications, building network wiring constraints, and a lack of funding for additional network resources.

The majority of current desktop users have yet to fully utilize the capacity of their existing Ethernet connection and the majority of servers connected to ISUnet with Fast Ethernet have sustained network utilization rates below 40% of their Fast Ethernet connection capability. The one future application demanding the most bandwidth is likely desktop videoconferencing, but simply increasing campus network bandwidth capacity at the desktop will do little to provide faster access to and from off campus Internet resources that are often beyond University control.

Year 1-3: Review and update existing building data wiring summary information and continue to support building data wiring replacement as part of routine renovations and new building projects.

Wireless Network Expansion: The questions of wireless network expansion and the concept of access to service from off-campus versus on campus was discussed in much detail. As the use of wireless technology expands, the University's airspace policy will become critical in controlling and managing wireless airspace requests on campus. It is important to remember that today's wireless technology is designed to complement and not replace the existing wired network infrastructure of the University.

Wireless network access, when away from the main campus, is viewed as a separate issue from that of on-campus wireless network access. It is felt that off-campus wireless network access will have to be achieved through such things as State of Illinois contracts directly associated with cellular service providers or some other special non-university programs. These programs will become more prevalent over the next few years as cellular service providers begin to deploy new 3rd generation (3G) cellular technology. This new technology will eventually provide statewide and nationwide wireless network services with greatly improved network speeds.

It is recommended that TNSS should focus any future funds for wireless network expansion on the main campus and should continue to rely on the 802.11b type of service offerings. It is believed that wireless standards are beginning to solidify and that multi vendor solutions may be possible by the end of FY03 or the start of FY04. Until such time as universal standards for vendor interoperability and security are in place, it is recommended that TNSS move slowly but continue to work within the framework of the existing Cisco security solution, which is based on these emerging standards. TNSS should concentrate its efforts on expanding wireless network service in public access spaces such as the residence hall food courts, the library and other social and meeting spaces where faculty, staff and students can more easily gain wireless network access while on campus. As wireless technology becomes more mature, this technology should be more seriously considered in connection with renovation projects and new building construction and classroom environments.

The ability of TNSS to expand the wireless network will depend on the final cost of this service to both the end users and to the University. Following the conclusion of the current wireless pilot in January of 2003, it is recommended that TNSS develop a cost recovery plan for wireless service in line with the current TNSS charge structure. This plan should take into account both the needs of the student population for casual/recreational use and the needs of the academic and administrative community for more mission critical use. By FY04 it is recommended that wireless network access become a true production service

within TNSS. A more rapid expansion of wireless services should then take place in non-public areas such as classrooms and conference rooms. As the University expands the wireless solution it will be important that there be coordination with community efforts such as those of the local school districts.

Year 1: Complete the industry standards research phase of the project and the wireless pilot and begin to develop a cost recovery strategy in line with the current TNSS charge structure.

Year 2: Establish a development plan with an acceptable cost recovery model and move wireless network access to a true production service with expansion into non-public areas such as classrooms and conference areas.

Year 3: Wireless network access should be more seriously considered in connection with renovation projects and new building construction and should be more rapidly expanded into non-public environments such as classrooms. The deployment of wireless technology should be treated as an enhancement to the total network plan of the University and not treated as a replace for the wired network infrastructure.

Improved Security Administration: The matter of network and desktop security has grown in complexity to the point where it is becoming difficult to effectively manage the technical aspect of security at the departmental level. Things such as intrusion detection system software, firewall requirements and controls for public access to network resources all have added to this complexity. It is recommended that a new central security administrator position be established and supports the recommendations of the University's Technology Support Advisory Consortium (TSAC). This position should have authority to oversee all University security issues related to computer and network operations and should be responsible for identifying, coordinating and communicating a consistent technical security plan to help safe guard the electronic resources of the University. The creation of this new security position is viewed as a very important matter. The actual reporting line (within or outside of TNSS) is less important, however, than the creation of this the new position.

Year 1-3: Support the recommendations of the University's Technology Support Advisory Consortium (TSAC) as they relate to the creation of a new central security administrator position.

Develop Network Multicasting, Streaming and Internet 2: It is recommended that the entire area of video and audio conferencing, as it relates to the Internet, be addressed as a single component. Based on current discussions surrounding possible Internet 2 access for the University and with the increased potential for

collaborative video and audio conferencing opportunities through the Illinois Century Network, it is recommended that TNSS proceed to develop an Internet multicast architecture within ISUnet that will support these new video and audio initiatives. Given the complexity of this undertaking, it is recommended that this be accomplished over a 12 to 18 month period with the completion of a production multicast deployment some time in FY04. By FY05 TNSS should have in place the capabilities within ISUnet to support desktop video and audio conferencing from nearly any network access point on-campus. The Committee recommends that TNSS continue to actively work with other University areas and departments to provide expanded central services for streaming audio and video and continue efforts to bring Internet 2 access to the University in support of future departmental research and education projects. It is believed that distance education training based on Internet technologies will become much more important during the next 3 years.

Year 1: Begin work on an Internet multicasting architecture for the University data network that will complement future collaborative video and audio conferencing opportunities through Internet 2 and other Internet resources.

Year 2: Complete the Internet multicast project and introduce it as a production service and expand upon video streaming and Internet 2 opportunities.

Year 3: Assist with the migration from a dedicated room based audio and video conference setting to more mobile desktop Internet audio and video conferencing capabilities.

CONCLUSIONS

As the funding and the direction of the University continue to change, the process of regular network reviews, like this one, will become increasingly more important in helping Telecommunications and Network Support Services prioritize their network resources and work efforts to better meet the future needs of the University.

GLOSSARY OF TERMS

3G Wireless – This is the term for the third generation of cellular telephone service. This service will provide high-speed data up to 2 Mbps as well as voice service and support of multimedia services. The 3G wirelesses should start to become available in the next few years.

802.1x Network Access Control - This is the term for the port based access and authentication standard used for wireless ISUnet user authentication. This standard is the shell under which the 802.11i wireless security standard operates.

802.11a Wireless – This is the term for a new wireless network technology that will operate in the unlicensed 5.0 GHz radio spectrum and may eventually provide up to 54 Mbps of shared network connectivity.

802.11b Wireless – This is the term for a wireless network technology that operates in the unlicensed 2.4 GHz radio spectrum and uses 11 Mbps of shared network connectivity. 802.11b is the current standard for wireless ISUnet.

802.11g Wireless – This is the term for a new wireless network technology that will operate in the unlicensed 2.4 GHz radio spectrum and may eventually provide up to 22 Mbps of shared network connectivity.

802.11i Wireless Security – This is the term for the wireless network security standard. This standard works in conjunction with the 802.1x network access control switching standard to dictate how wireless security systems should be designed and operated.

Cable Modem – This is the term for a modem connected to an Internet service provider through the television cable in your home. Cable modem service is normally 15-20 times faster than conventional modem pool service. Local cable companies like Insight Communications offer this service.

Cat 5 - This is the term for a type of wire known as category 5 that is the current ISUnet wiring standard. This wire works with Fast Ethernet and Gigabit Ethernet service.

Content Caching - This is a term for software and hardware that stores commonly used Internet web pages locally on-campus so that critical Internet resources of the University can be protected for other uses. For example, if the same IRS tax form is loaded by on – campus computers 50 times a day from the Internet it could be automatically cached on one central University computer. When someone on-campus goes to download this tax form from the IRS the form would be down loaded locally rather than over the Internet.

DS-3 – This is the term for a digital circuit designed to carry 45 Mbps of digital data.

DSL – This is the term for a digital subscriber line. This is a high-speed data circuit used over a conventional telephone line to connect a home computer to the Internet or to another data network. DSL service is normally 10 - 15 times faster than conventional modem pool service. Local telephone companies like Verizon offer this service.

Fast Ethernet – Conventional Ethernet operates at up to 10 Mbps. Fast Ethernet operates at up to 100 Mbps or up to 10 times faster.

Firewall – This is the term for an electronic barrier set up to control access to or transfer of data within a network. Firewalls can be on individual computers (desktops) or part of larger systems like a network or a connection to the Internet (host based).

Gigabit Ethernet - Gigabit Ethernet operates at up to 1000 Mbps. This can be up to 10 times faster than Fast Ethernet and up to 100 times faster than conventional Ethernet.

ICN – This is the term used to describe the Illinois Century Network. This is a State of Illinois data network that provides Internet service and links grade schools, high schools, community colleges, and universities through Illinois.

IDS – This is a term for intrusion detection software. This is a method of scanning a network to identify computers that are attempting to gain access (intrude) into network resources, which they are not authorized to access.

Internet 2 – This is the term for the second generation of Internet, which is being designed to interlink educational and research institutions throughout the world. Internet 2 will provide higher speed connections, less commercialization and a platform from which to test new technologies.

Internet Multicasting – This is the term used to describe a special software program operating on a network that will allow multiple locations to receive the same information without overtaxing the resources of the network. Internet Multicasting is often used to support video conferencing, electronic whiteboards, and other multimedia uses. It can also be used to update software on a large number of computers simultaneously.

ISP – This is the term for Internet Service Provider. This is the provider that actually connects you to the Internet. In the case of the University, Telecommunications and Network Support Services serves as the ISP.

ISUnet – This is the term for the network that connects all University computers to the Internet and to each other.

Mbps – One million bits of data information per second also called megabits per second.

OC-3 – This is the term for an optical circuit or fiber connection designed to carry 155 Mbps of digital data.

Packet Shaping – This is the term used to describe a system of hardware and software that is used to identify certain software applications by examining their data packets and then limiting or controlling their network usage. This function is often used to control large file transfers of music or video to and from the Internet on an individual application basis. Packet shaping is a form of QoS.

Peering - This is a network transport method where off-campus locations such as apartment houses can directly connect (peer) their networks with ISUnet for the delivery of computer information that goes only to the University. Peering allows computer information like local e-mail to be transferred to the University without using the valuable Internet resources of the University.

Public Access Network – This is a term used to describe the installation of network jacks in public places throughout the campus so faculty, staff and students can jack in their laptop computers when away from their room or office. Public jacks are protected with a security system and cannot be access by the general non-university public even though they are located in public areas like the Bone Student Center.

QoS – The term for Quality of Service. This is the process where by hardware and software are used to guarantee minimum amounts of network capacity to specific applications so they will run correctly. Voice and video applications are examples that need prescribed minimums. Packet shaping is a form of QoS.

RESNET – The term for the University residence hall network that provides Internet access to residence hall student rooms. RESNET is a subset of ISUnet.

Streaming – This is the term used to describe audio or video that is transmitted from one computer to a number of computers on demand over a network. A classroom presentation can be distributed to a number of users over the Internet using a streaming video server. Streaming servers are most effective when used as a central resource.

Type 1 Wiring – This is the term used to describe a type of wire that was the original IBM network wiring standard. Type 1 wire was used as the first ISUnet wiring standard. This standard was changed because the type 1 wire would not work with Fast Ethernet and Gigabit Ethernet service.

VoIP – This is a term used to describe Voice over IP or voice over the Internet. This is the idea that the Internet can be used as the method to send and receive telephone calls rather than using a conventional telephone line.

VPN Concentrator – This is a system of hardware and software that is used to restrict, which computers can access, and travel over ISUnet. It is also used to create a secure pathway for these computers to travel over regardless of who the Internet service provider is. VPN is short for Virtual Private Network.