

SUG – ISC N&T “State of the Union”

March 9, 2009

Michael Palladino

Agenda

- ▶ Major projects and initiatives
- ▶ FY '10 rates
- ▶ N&T resources
- ▶ General discussion

Major Projects and Initiatives

- ▶ Next Generation PennNet/Network Upgrades
- ▶ Unified Communications
- ▶ Secure IM/Jabber
- ▶ Wireless
- ▶ Strengthening PennKey
- ▶ Multicasting/IPv6
- ▶ Streaming/HD content
- ▶ Rates

Next Generation PennNet

- ▶ Project initiated in 1999 to reduce risk of catastrophic failure. All fiber and electronics were centrally located in one “data center” in sub-basement of College Hall.
- ▶ Distribution of the PennNet routing core
 - ▶ Constructed 5 hardened Network Aggregation Points (NAP's)
 - ▶ Dual 10 Gigabit Ethernet switching core
 - ▶ 8 High-Speed Core and Gateway Routers
- ▶ Enhanced capacity & reliability to all areas of campus
 - ▶ Provide Gigabit Ethernet to campus buildings (166 of 229)
 - ▶ Dual uplinks to the most critical buildings (56 of 96)
 - ▶ All Building Entrance Routers upgraded by end of FY'09
 - ▶ All closet electronics 10/100/1000 capable by end FY'09

Next Generation PennNet

- ▶ Increased reliability as converged (data, voice and video) networks grew more critical
 - ▶ Striving for 99.99 at building level
 - ▶ Goal <1 hour of unscheduled downtime/year
 - ▶ Network infrastructure services
 - ▶ Goal is <2 hours of unscheduled downtime/year
 - -.34 hours first 6 months
 - ▶ Network user services
 - ▶ Goal in is <9 hours of unscheduled downtime/year
 - – 1.68 hours aggregate first 6 months
 - Exchange – 0.51 hours
 - Zimbra – 6.44 hours
 - ACD – 0.01 hours

Next Generation PennNet Goals (Future)

- ▶ 100 gig routing core
- ▶ 10 gig building connections
- ▶ 10 gig backbones in building
- ▶ Single mode fiber to buildings
- ▶ Gig connections commonplace
- ▶ Larger Internet and Internet2 connections
- ▶ 6th Network Aggregation Point for East campus (when needed)

Unified Communications - VoIP

- ▶ PennNet Phone, ISC's Voice over IP alternative to analog telephony, is the telephone service of choice
 - ▶ Over 10% of faculty and staff have PennNet Phones
 - ▶ Over 90% of PennNet Phone customers have VM
 - ▶ 25% lower cost than comparable Centrex service
 - ▶ 70% lower cost than analog VM
 - ▶ 10% of LSPs with PennNet Phone Service
 - ▶ Collaboration with Columbia

Unified Communications – VoIP

▶ Current Status

- ▶ Highly reliable infrastructure, though early adopters did experience some problems.
- ▶ Continuous feature development
 - ▶ Numerous multiline features now in use
 - ▶ March 31 feature release includes Configurable Call Waiting, Call Forward Busy fix and Bridged Line Appearance
- ▶ Upgraded Cisco phones with lower-cost Polycom phones
 - ▶ Model 320 – basic single line set
 - ▶ Model 550 – standard 4 line set
 - ▶ Model 650 – 6 line set with sidecar option for additional lines
 - ▶ Model 6000 – conference room set

Unified Communications - VoIP

▶ Support

- ▶ Strong support from TSS, LSPs, and BAs
- ▶ Monthly lunch-time learning sessions
- ▶ Will host PennNet Phone SIG to meet quarterly to discuss service roadmap
- ▶ Website – www.upenn.edu/computing/voice

Unified Communications - VoIP

▶ Future Targets

- ▶ FY '09 – 2000+ customers
- ▶ FY '10 – 6000 customers
- ▶ FY '11 – 11,000 customers
- ▶ FY '12 – 16,000 (All faculty and staff phones)
- ▶ Developing plans to greatly reduce or eliminate voice building to building copper infrastructure

Jabber IM Service

- ▶ Production date July 2008
- ▶ All ISC email and VoIP customers have accounts enabled at no cost
- ▶ Over 500 active users
- ▶ Data encryption from end-to-end is more secure for University business
- ▶ Facilitates collaboration among co-workers, even those offsite
- ▶ Simultaneously connect to Yahoo Messenger as well as Penn's IM.
- ▶ Group Chats
 - ▶ Persistent "chat rooms" (like SUG, MacNet, PCNet, etc)
 - ▶ Ad Hoc group chats - great for quick communications and troubleshooting sessions
- ▶ Formal campus evaluation team surveyed IM clients last Spring
- ▶ Supported clients: iChat and Adium for Mac OS X and Pidgin for Window
- ▶ Kerberos authentication for compatible clients (Adium and Pidgin)

Jabber IM Next Steps

- ▶ Reconvene last year's evaluation team to clarify IM client support
- ▶ Investigation of integration with the Asterisk voice mail system and with Zimbra
- ▶ Testing and possible piloting of mobile clients for Palm, BlackBerry, iPhone, and Windows Mobile
- ▶ Exploratory work on voice and video integration

Wireless – AirPennNet (Mark)

- ▶ **Great progress in the last 12 months**
 - ▶ AirPennNet with native 802.1x authentication
 - ▶ Over 1400 APs have common log-on campus-wide
 - ▶ Developed a web-based guest wireless network using Netreg infrastructure for authentication
 - ▶ Need only PennKey and password
 - ▶ Evaluated next generation wireless “802.11N”. Controller based architecture
 - ▶ Pilot in TSS, SAS and CHC beginning Spring Break
 - Testing new features such as failover, increased bandwidth with 802.11N, and coverage
 - ▶ If successful, 100% roll-out in ResNet in Summer of 2009
 - ▶ Rest of campus will be upgraded by end of FY 2010
 - ▶ New wireless will offer 802.11 a b/g /n
 - ▶ Good trade in costs and strong negotiations helped to keep under our projected monthly support costs for FY10

Next Generation Wireless

- ▶ Advantages include
 - ▶ Speed – up to 100mbps
 - Uses new and improved MIMO technology; equates to more bits per second per hertz of bandwidth and link reliability or diversity which reduces signal fading
 - ▶ Performance
 - Ability to support legacy 802.11b clients without downgrading higher speed clients on same access point
 - Provides framework for QoS (Quality of Service) for next generation applications over wireless: Voice over WLAN, video streaming, location services
 - Enables client mobility and eliminates client roaming tendency problems between AP's from other wireless subnets
 - ▶ Operational Efficiencies
 - Potential savings in staff time (installation, management & support)
 - Dynamic wireless coverage and signal strength
 - Coverage adjustment upon AP failure, automatic AP configuration
 - Rogue AP detection and elimination
 - Ability to stage 802.11n roll out if desired



Next Generation Wireless

▶ Future Plans

- ▶ WPA2 conversion by Fall 2010
 - Offers better encryption of data
 - Would require communications on client reconfiguration
- ▶ Explore VoIP and/or Video over wireless
- ▶ Continue to monitor other wireless technologies (WiMax, FMC)

Strengthening PennKey (Shumon)

- ▶ An ISC-wide project, with strong participation from around campus, is addressing improvements to numerous elements of Authentication and Authorization at Penn
- ▶ Some key elements include
 - ▶ An upgrade to Websec, replacing it with Penn Weblogin
 - ▶ Deployment of Shibboleth, to make inter-institutional web authentication practical
 - ▶ Deployment of PennGroups, an LDAP-based Authorization service
 - ▶ Pilots with two-factor Authentication, to help move past the weaknesses of reusable passwords
- ▶ ISC will be back with an in-depth look at Strengthening Pennkey at a future SUG meeting

Strengthening PennKey

▶ **Replacement of Websec by Penn WebLogin/CoSign**

- ▶ Documentation, available at <http://prowiki.isc.upenn.edu/wiki/Category:WebSec/Cosign>, and a support plan have been put in place
- ▶ Support sessions focusing on the Apache and IIS6 platforms were held in late Fall and Winter. Requests for support can be submitted through the ProDesk
- ▶ SEAS has successfully converted applications as an early adopter, ISC staff are working on their applications, and planning and migration are underway in other Schools and business units
- ▶ In addition, the team regularly sends reminders to IT-Announce advising developers and system administrators of timelines and resources, and encouraging those who have not yet contacted the team to send in information regarding their plans via a form on the WebLogin web site <http://www.upenn.edu/computing/weblogin/>
- ▶ Initially thought that 550 applications needed to be converted, through further investigation only 36 conversions are necessary
- ▶ New deadline for conversions is 12/21/09



Strengthening PennKey

▶ **Streamlining PennKey (On schedule)**

- ▶ A background survey about how other schools handle authentication, remote, ID proofing, and distribution of setup codes has been completed
- ▶ Development began in January on an application that will allow certain categories of users (first, alumni, later others, such as incoming students) to verify identity and obtain a setup code remotely
- ▶ Limited deployment is planned for May/June 2009. The Levels of Assurance component of this project has been split off into a separate project (see below)

Strengthening PennKey

▶ **Introduction of Shibboleth (New)**

- ▶ Shibboleth is an open source web single sign-on (SSO) authentication and authorization service which will be implemented as a front end for CoSign authentication
- ▶ Shibboleth supports federated authentication (use of “home” institution credentials to access resources at federated institutions)
- ▶ It also supports integration with 3rd party academic and business applications requiring Penn authentication
- ▶ N&T is coordinating development efforts with the Library through March 2009. A pilot will follow, with general University availability in August 2009

Strengthening PennKey

▶ **Introduction of Two-Factor Authentication (Scope change)**

- ▶ The goal of this project is to implement a second authentication factor to supplement reusable PennKey passwords for use with applications that require additional security
- ▶ The initial vision was to implement hardware tokens that generate one-time PINs
- ▶ Currently the team is evaluating a hardware-based option and a phone-based option from a cost and technology perspective
- ▶ A two-factor strategy recommendation is expected in April 2009, and ISC expects to launch a pilot in FY 10

▶ **Central Authentication Logging (Scope change)**

- ▶ The original project has been scaled back for cost reasons and replaced with a logging “lite” effort
- ▶ Logging lite will provide data about authentication attempts to ISC Information Security
- ▶ The data will be available for proactive analysis and fraud detection, and great care will be taken to protect its privacy
- ▶ Development is planned for June through September 2009, with availability expected in October 2009

Strengthening PennKey

▶ **Levels of Assurance (LoA) (Scope change)**

- ▶ Originally a part of the Streamlining PennKey project, Levels of Assurance, because of its strategic importance, is now a standalone project under the Office of Data Administration
- ▶ Efforts are currently underway to define the scope of the project
- ▶ A well thought-out LoA policy and infrastructure will lay the foundation for other initiatives, such as two-factor authentication, federated authentication, and single sign-on (SSO)
- ▶ A timeline has not been established

▶ **Switch to Passphrases (On hold)**

- ▶ The phased introduction of 15-34 character passphrases to replace complex passwords, originally scheduled to begin in March 2009, has been placed on indefinite hold
- ▶ As a result of further analysis prior to ISC's formal "go/no go" decision, ISC determined that we cannot find the appropriate balance between the reduction of vulnerabilities and ease of use that would warrant forcing all PennKey holders to change to passphrases

Central Authentication and Single Sign On

- ▶ *“PennKey was originally intended to be both single sign on AND secure enough for every application. With keyloggers (as opposed to network sniffing) becoming the greatest threat, no reusable password can be used for all applications and also be secure enough for the most sensitive applications. Should we stop using PennKey for high frequency / low security purposes such as email (as SAS has done), or should we stop using PennKey for low frequency / high security purposes? Or is there another option?”*
- ▶ Central authentication and Single Sign-On can provide high levels of security and convenience for users
- ▶ Risks exist for password authentication. Passwords are compromised in a variety of ways. Social engineering through phishing and other means, password guessing, sniffing, keystroke loggers and other malware
- ▶ No “magic bullet” exists to fix all of these problems entirely
- ▶ Host security is an important defense against key stroke loggers and other malware
- ▶ Good risk mitigation approaches exist for most or all of the risks
- ▶ ISC is pursuing approaches like Levels of Assurance (LoA) and 2-Factor authentication as part of the Strengthening PennKey project

Multicast

- ▶ Multicast is fully deployed in the campus (wired) network
- ▶ External multicast is available to Internet2 connected schools
- ▶ External multicast is not available to the commercial Internet
- ▶ Multicast makes very efficient use of the network
 - ▶ A good choice for applications sending the same data to lots of different clients
 - ▶ Streaming video, IPTV, Ghost, etc.
- ▶ Some users have had problems deploying Ghost
 - ▶ We can discuss details and specific solutions offline

Questions on Multicast

- ▶ *“Policies/procedures/best practices for multicast?”*
- ▶ *“Network impact of deploying multicast video streams?”*
 - ▶ ISC enables multicast for the wired network
 - ▶ Testing methodology
 - ▶ Don't block multicast control messages (IGMP) on firewalls, hosts...
 - ▶ Layer-2 switches should have “IGMP-snooping”
 - ▶ Choosing multicast group addresses

IPv6: Internet Protocol, version 6

- ▶ IPv6 – the next generation Internet Protocol
- ▶ Impending exhaustion of IPv4 addresses
 - ▶ ~ 2011/2012
- ▶ Bad consequences for non-deployment of IPv6
 - ▶ Sanctioned/unsanctioned IPv4 transfer markets
 - ▶ More and more layers of NAT
 - ▶ Disruption of universal connectivity
- ▶ Penn should have an aggressive plan to deploy IPv6 in its network and applications

IPv6 Deployment at Penn

- ▶ **MAGPI (Internet2 GigaPoP) ~ since 2002**
 - ▶ IPv6 fully deployed and connected to global IPv6 network
 - ▶ Provides IPv6 connectivity to Princeton, NJEdge, Penn
 - ▶ Services: Web, DNS, NTP, SSH
- ▶ **PennNet -- deployment began 2005**
 - ▶ Central network infrastructure done
 - ▶ Border routers, core routers, external peering
 - ▶ A few server and enduser subnets
 - ▶ SEASnet
- ▶ **Application services:**
 - ▶ DNS, NTP, SSH, Jabber
 - ▶ Assignments supports the IPv6 DNS records (AAAA)

IPv6 Next Steps

- ▶ Rollout to the rest of campus networks
- ▶ Communication plan / training for LSPs
- ▶ Continued deployment of application services:
 - ▶ Web, E-mail, Authentication, Directory, DHCPv6
- ▶ Issues/caveats:
 - ▶ Tunnelling: 6to4, teredo
 - ▶ Middleboxes: firewalls, ids, vpn, slb
 - ▶ 3rd party service providers (Akamai, Message Labs ..)
 - ▶ Billing

IPv6 References

- ▶ Penn IPv6 presentation at Educause MidAtlantic Conference:
 - ▶ <http://connect.educause.edu/Library/Abstract/IPv6DeploymentattheUniver/47977>
- ▶ General IPv6 Information:
 - ▶ <http://www.ipv6.org/>

Streaming Services (Deke)

- ▶ iTunes U and Penn on YouTube continue to be very popular platforms for campus video delivery to a worldwide audience
- ▶ A project is underway to update our existing streaming solution
 - ▶ Flash support is likely the key technology driver
 - ▶ Real Player requirement will be phased out
 - ▶ Support for live and stored streams must be included
- ▶ Commercial and Penn developed solutions are being considered including
 - ▶ Akamai Stream OS
 - ▶ Wowza Media
 - ▶ Veotag
 - ▶ Mediasite

HD Content (Deke)

- ▶ PVN is exploring several opportunities for delivering High Definition content on PVN Cable
 - ▶ Delivery of Off Air Channels through partnerships with Campus TeleVideo and / or Comcast
 - ▶ Leveraging new technologies like a recently established fiber connection to Comcast's "HeadEnd In The Clear"
- ▶ IPTV provides other opportunities for delivering HD content on a Next Generation PVN
 - ▶ A cross campus team has begun initial evaluations of IPTV options
 - ▶ Partnering with other universities like Michigan Tech, North Carolina State, and Notre Dame through AHEHCTA to learn from their IPTV implementations
- ▶ We are beginning to work on a Next Generation funding model to go along with the NG services

Operational Efficiencies (Mike)

- ▶ Continuously exploring alternatives that lower N&T costs doing selective outsourcing and insourcing
- ▶ Our 5-year budget shows an 8% decrease in expense
 - ▶ Operator services outsourced to a third party provider
 - ▶ Deferred upgrades of core routers by one year
 - ▶ Lengthened depreciation from 3 to 4 years on both wireless infrastructure closet electronics
 - ▶ Telephone audits already reduced customer expense by \$75k in FY '09, projecting \$100k-\$150k in FY '10
- ▶ Microsoft Live for student email

Network Planning Task Force

- ▶ The NPTF approved funding of all base services and many security and identity management projects including:
 - ▶ Next Generation PennNet
 - ▶ Gig to all buildings/Dual Gig to 96 buildings/Single mode fiber to buildings
 - ▶ Security/ID Management
 - ▶ Central Authorization (PennGroups)
 - ▶ Shibboleth –and joining the InCommon Federation
 - ▶ Communication Name
 - ▶ PGP whole disk encryption support for LSPs
 - ▶ For-fee local intrusion detection service
 - Firewall integrated (TSS)
 - Stand alone (N&T)
 - ▶ Penn WebLogin (Cosign) replaces websec
 - ▶ A small-scale Central Logging project
- ▶ ISC funded the 2-factor authentication pilots for FY'10

Rates (Telephone)

Voice Rates (month)	Centrex	VoIP FY 2009	VoIP FY 2010
Centrex line/VoIP line	\$16.50	\$15.32	\$16.50
Phone Set w/maint.	\$10.03	\$8.00	\$3.00-\$5.00
Voicemail	\$9.75	\$3.00	\$3.00
Port	\$0.00	\$6.03	\$5.25
Subtotal	\$36.28	\$32.35	\$27.75-29.75
Usage (Average user)	\$6.00	\$3.00	\$3.00
TOTAL	\$42.28	\$35.35	\$30.75-32.75
Conversion Fee	N/A	\$80 waived	\$80 waived



Rates (Network & Email)

Starting in January 2009, the default port connection will be 100meg half duplex.

<u>Data Rates</u>	<u>FY 2009</u>	<u>FY 2010</u>
Port Rental and Connection maintenance Fee		
10Base-T	\$6.03	\$5.25
100Base-T	\$7.03	\$5.25
1000Base-T	\$30.00	\$30.00
IP Address fees	\$4.29	\$1.73

<u>Email Services</u>	<u>FY2009</u>	<u>FY2010</u>
Zimbra-Basic Authentication Security	\$350/month	\$350/month
Zimbra-Enhanced Authentication Security	\$300/month	\$300/month
Forward only	\$150/month	\$150/month
Microsoft Exchange 2007 with integrated calendaring	\$750/month	\$750/month
Blackberry with Exchange	\$1350/month	\$1350/month
Quota over 1GB- One time setup fee	\$5000	\$5000

Base quota is 250MB. Additional quota is \$15/user/yr for 250 MB up from \$12 in FY '09.

Rates (Wireless & PVN)

<u>Wireless Rates</u>	<u>FY 2009</u>	<u>FY 2010</u>
Port	\$7.03	\$5.25
vLAN	\$1.25	\$1.25
AP	\$26.00	\$28 - \$31.5
TOTAL	\$34.28	\$34.5 - \$38

<u>Video Rates (Monthly)</u>	<u>FY 2009</u>	<u>FY 2010</u>
PVN Outlet	\$15.50	\$16.50

The **Penn Video Productions** group offers a full range of production, storage, and distribution services. For a complete description of rates and available services, see www.upenn.edu/video/pvp/.

N&T Resources

- ▶ Ordering N&T services
 - ▶ <http://www.upenn.edu/computing/isc/networking/orderforms.html>
- ▶ Rates
 - ▶ www.upenn.edu/computing/isc/networking/rates/
- ▶ Zimbra and Exchange
 - ▶ <http://status.net.isc.upenn.edu>
 - ▶ <http://www.upenn.edu/computing/email/>
- ▶ Wireless - AirPennNet
 - ▶ <http://www.upenn.edu/computing/wireless/>
- ▶ Network Upgrades
 - ▶ <http://www.upenn.edu/computing/pennnet/maintschedule.html>

Discussion
