University of Pennsylvania

Network Planning Task Force

October 13, 2014

Deke Kassabian
dekte@isc.upenn.edu
NPTF Membership

Daniel Alig / Joe Cruz, Wharton
Charles Buchholtz, SEAS
Lena Buford / Tejash Patel, Annenberg
Cathy DiBonaventura, School of Design
Brian Doherty, SAS
David Domico, SRFS
John Eckman, Housing Services
Jeff Fahnoe, Dental
Mike Herzog / Didi Sariyska, GSE
Andre Jenkins / Michael Morris / Robert Colligon, PSOM
Victoria Iannotta / Marilyn Jost, FRES
Sue Kennedy, Business Services
David Kern, Public Safety
Kay McDonnell / Christine Droesser, Law
Grover McKenzie, Library
Donna Milici / Sam Smith, Nursing

Dominic Pasqualino, OACP
Smith Ragsdale / Brian Sherman, VET
Joseph Shannon, Finance
Mary Spada, VPUL
Marilyn Spicer, College Houses
Michael Weaver, Budget Mgmt. Analysis
Ira Winston, SEAS, SAS, Design

ISC Representation
Deke Kassabian, ISC (Chair)
Mark Wehrle, ISC
Jim Choate, ISC
Josh Beeman, ISC
Michel van der List, ISC
Mark Aseltine / Amy Phillips, ISC
Gary Delson / Geoff Filinuk, ISC
NPTF 2014 Schedule

- July 21st: Information Security Update
- September 8th: Network & Server Infrastructure (other than wireless)
- October 13th: Wireless, Identity & Access Management, and Penn+Box
- November 10th: Next Gen WWW, Yammer, & working through FY16 Rates
FY’14 CSF Bundle of Services

- Campus Backbone Infrastructure
- Internet and Internet2 access
- Rate limits on ResNet
- IPv6, Multicast, and Advanced Networking
- Public Wireless Subsidy
- Cap on billable wireless IPs
- NAP Operations/Fiber and Cable Management
- NOC Services and Network Management
- Penn's Main Web and Central Pages
- Online Directory and LDAP access
- Classlists and SMTP Mail Relay
- University Calendar Service
- Infrastructure Software Services
  - DNS, DHCP, NTP
- Penn+Box Storage & Collaboration (FY’14)
- Enterprise InCommon Certificate Service
- Enterprise Social Networking
- Security/ID Management
- Kerberos, KITE, RADIUS
- Penn WebLogin (CoSign and Shibboleth)
- The InCommon Federation
- Authorization (Penn Groups)
- PennNames and Penn Community Services
- Wireless Authentication & Support
- NetReg
- DNSSEC
- Vulnerability Scanning
- Security Tools, Education, and Response
- PennKey School Support
- PGP Whole Disk Encryption LSP Support
- XpressConnect
- Enhanced AirPennNet Guest Services (FY’13)
- Intrusion Detection System
- SafeDNS
Today’s Agenda

- AirPennNet Wireless and related networks
- Internet of Things and EAP-TLS
- Eduroam
- DAS
- Identity and Access Management
- Penn+Box
- Open discussion
Penn has a set of WiFi networks that together are designed to meet community connectivity goals:

- **AirPennNet** is the University’s enterprise wireless network
- **AirPennNet-Help** is a wireless network that is used to configure and connect end-users devices
- **AirPennNet-Guest** is an alternate wireless “guest” network for campus visitors
- **AirPennNet-Device** is a specialized wireless network in student residences that supports non-authenticating devices (Kindle, Nook Color, Roku XD, PlayStation 3, and Xbox 360)
Penn Wireless Network Infrastructure:

- 3,778 wireless access points
- 11 production controllers connected at 10 Gbps
- Supported wireless standards (and data rates) up to 802.11AC Wave 1 and down to 802.11g
- Coverage in 215 of 283 Penn buildings with PennNet service
- 167 high density wireless locations
Each year, there is significant growth in demand on Penn wireless networks

- Growth in number of users of wireless networks
- Growth in number of devices per user
- Growth in total data handled
University of Pennsylvania - Network Planning Task Force
Wireless Device Count on AirPennNet in September

<table>
<thead>
<tr>
<th>Year</th>
<th>Device Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY12</td>
<td>34050</td>
</tr>
<tr>
<td>FY13</td>
<td>49602</td>
</tr>
<tr>
<td>FY14</td>
<td>59861</td>
</tr>
<tr>
<td>FY15</td>
<td>65360</td>
</tr>
</tbody>
</table>
Devices per Person in September

- FY12
- FY13
- FY14
- FY15
Wireless Data Statistics

Total Traffic in September (in TB)

- FY12: 204.22TB
- FY13: 286.63TB
- FY14: 289.09TB
- FY15: 342.44TB

University of Pennsylvania - Network Planning Task Force
New RADIUS servers

- Previously, 4 production servers each ran 3 instances of RADIUS (12 total)
- New server is a single (replicated) server that runs a single instance capable of handling 15x the RADIUS authentications per second

IPv6 available on all AirPennNet subnets

- AirPennNet-Guest cannot use IPv6 today because of a lack of support by one of its primary components (NetReg)
Next Generation Access Points: Evaluating Wave2 AC

- 2800+ APs are reaching end of life (AP124 & 125)
- Paper evaluations of wireless vendors
- Must weigh timeline for Wave 2 maturity and replacement
- Targeting end FY2015 to solidify strategy and direction

Preparations

- Installing AC (Wave 1) APs as new wireless default
  - 110 APs are located in various buildings
- Began adding second Cat 5E wires in late 2013
- Monitoring APs for BW thresholds
- Cost differences (if any) are to be determined
Increasingly, we have devices on campus that need network connectivity but that aren't associated with an individual user

- Public safety cameras
- Sensors and door locks
- Scientific equipment

Need a mechanism to authorize devices to access campus networks without requiring a username and password

We plan to extend the RADIUS service to support certificate-based authentication using EAP-TLS
EAP-TLS supporting IoT will leverage earlier work done to upgrade our campus RADIUS servers.

A project is underway to develop a broadly deployable version during Spring 2015.

Pilot deployments in a few locations on campus could take place earlier in 2015.

Existing pre-authenticated devices (door looks and sensors) will continue to be supported until production transition.
Eduroam is the secure, world-wide roaming access service developed for the international research and education community.

It allows members from participating institutions to obtain network connectivity when visiting other participating institutions by authenticating to the Eduroam WiFi network with their home credentials.

Thousands of deployments exist in Europe, Asia and Africa. Hundreds (and growing) are available in the US.

Eduroam was funded for development and deployment at Penn by the NPTF for FY15.
Eduroam in Operation

Flow of Network and Authentication Traffic for eduRoam

- Princeton University
  - Local Controller
  - Local RADIUS
  - Princeton Network

- eduRoam
  - Routing RADIUS

- University of Pennsylvania
  - Local RADIUS
  - PennKey
  - Exchange Server
  - PennNet

Legend:
- Green: Network Traffic
- Red: Authentication Traffic
Eduroam Status and Next Steps

- *Eduroam* will leverage earlier work done to upgrade the campus RADIUS servers
- A project is underway to develop a broadly deployable version of Eduroam during Spring 2015
- Pilot deployments in a few locations on campus could take place earlier in 2015
- Must adhere to minimum *Eduroam* network requirements:
  - Limited port requirements
  - Use of NAT should be avoided
  - 802.1x and no use of application or intercept proxies
Many requests to use AppleTV (AirPlay) and Chromecast on Penn networks

Working model suitable for home use, but incompatible with most large enterprise networks
Status and Next Steps

- Some small-scale deployments completed by ISC with performance impact (trade off performance for functionality)

- Medium Term: Larger and scalable deployments possible using Aruba Clear Pass Policy Manager
  - $35K one-time; approx. $7K/year for operations

- Long Term: Enterprises and network vendors hope to influence Apple, Google and others for more scalable and cost effective approaches

- **NPTF Input requested:**
  - Does NPTF want ISC to pursue scalable deployments as described above (“medium term”)?
  - Aruba CPPM product could play a role in a next-gen guest network
6 different ways to gain access to AirPennNet-Guest:

- Traditional PennKey
- Non-persistent guest PennKey (bulk)
- Sponsored hardware address
- Penn-affiliated assisted registration
- Guest access code registration
- Group event and conference access

The majority (about 80%) of AirPennNet-Guest users are Penn affiliates with traditional PennKey usernames and passwords.
AirPennNet-Guest Utilization by Registration Model in September 2014 (excludes regular PennKey registrations)

- Non-Persistent Guest PennKey: 325
- Individual Guest Code: 363
- Group/Conference Code: 88
- Affiliate-Assisted: 118
- Sponsored Hardware Address: 2194

Plus 12,051 users accessing APNG using traditional pennKeys
AirPennNet-Guest Evolution

- AirPennNet-Guest will soon join the SafeDNS pilot
  - APNG users will receive SafeDNS server addresses
  - Pilot will run 10/13/14-11/7/14
  - Review of pilot will take place the week of 11/10/14

- Evaluate next generation guest wireless designs
  - Alternative vendor products capable of supporting an integrated campus-wide Guest Network infrastructure
  - Also considering moving to an ISP-supported version of AirPennNet-Guest
    - If cost effective and able to support all main AirPennNet-Guest uses
    - Could recommend port and rate limitations to this service
DAS Update

Mark Wehrle
Distributed Antenna System (DAS)

- DAS – What is it?
- What are the drivers for investigating DAS solutions?
- Challenges
- Opportunities
- Proposed strategy
A Distributed Antenna System (DAS) is a network of spatially separated antennas that can boost cellular and radio frequency and WiFi signals in communications “dead spots”

Antennas are connected to cabling (coax or fiber) either directly to the carrier systems via circuit or to a donor rooftop antenna through “head end” equipment

A DAS can:
- Increase of cellular communication networks
- Help to extend cellular RF coverage inside of buildings
DAS - Typical System

Source: onepath systems
DAS - Drivers

- Changes in carrier frequencies
- Limited macro sites
- Use of ENS applications
- Increased reliance on smart phones
- Reliance on emergency frequency propagation
  - Regulations require coverage of police and emergency RF bands in new construction*
- Building construction
  - LEED-certified building materials can weaken or block RF signal in building interiors
  - Increased building density weakens signals

Would address critical campus communications needs

- Poor signal in some building interiors
  - Upper floors of campus high rise buildings may be negatively impacted due to Low–E glass
  - Poor RF coverage in lower-level and underground rooms (dirt and concrete also impact signal)
  - Increased building density weakens signals

- Currently, no reported issues with campus outdoor areas. However, potential stressors could be:
  - Increased device cellular data and voice needs
  - Dense areas that support people/call/data volume - e.g. sports arenas and stadiums

Public Safety requirements could share infrastructure
DAS - Challenges

- DAS is both expensive and complex
  - To date, DAS costs are included in construction projects
  - Historical projects ranged from $80k - $100k or higher
  - No leverage efforts with carriers to share cost
- No common DAS integrator for design strategy exists today
  - Balkanized installations further increase costs
  - Integrator selection can be binding for multiple years
    - *Contractual and legal issues*
    - *Neutral vendor solutions are costly but offer flexibility*
    - *Carrier negotiations can be lengthy but can still offer payoffs*

These drivers and challenges are not unique to Penn
Would capitalize on very good outdoor cellular and RF coverage available in Philadelphia metro area

Would leverage Penn’s existing agreements with local cellular carriers to place donor antennas on some Penn-owned buildings to boost outdoor coverage on campus

NGP fiber plant, key NAP locations and South Bank provide opportunities for a diversified yet simple system

Some cost savings opportunities exist with FRES, ISC, and UPHS
DAS - Proposed Strategy

- Continue to test spot solutions
  - Not scalable, but provide short-term fixes
  - Carrier signal drops are an issue – disconnects

- RF survey for parts of campus
  - DAS integrators offer this service
  - Hire an independent expert (Cornell University did this)
  - Identify typical buildings (High Rise to determine ResNet coverage; buildings with below-surface occupied spaces)

- Identify all existing DAS systems to determine capacity
  - Who owns these?
  - Do we look at common system designs and shared head-end equipment?

- Develop business case for central DAS for problem areas
  - Commission independent RF survey and carrier counts to leverage cellular provider subsidies
  - Leverage NGP fiber and NAP infrastructure and diversification to provide a cost effective strategy
Identity and Access Management Update

Deke Kassabian
Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons

- Central IAM is (roughly) Penn Community + PennKey + PennGroups + PennCard
- Schools & centers also maintain IAM infrastructure (e.g. AD, local credentials)
  - *Due to the diversity of IAM systems and technologies cross campus integration is currently challenging*
Current State of IAM in ISC

♦ Things that work well today
  • Collegial and highly engaged staff
  • Deep domain and Penn expertise
  • No duplication of effort
  • Flexible and well performing services (e.g. 2-factor)

♦ Challenges today
  • No central Penn direction and governance
  • No single point of responsibility for IAM within ISC
  • Difficult to allocate and manage resources across units
    – Slow improvements
    – Customer requests managed through multiple channels
We like to think…
IAM at Penn – Organization

But in reality…

Kerberos
CoSign
Shibboleth

PennNames
PennKey
Policy Support

AuthNProxy

eForms
PennGroups

PennCommunity
Challenge-Response
PennKey ASAP

FAST
Two-Step Verification

ISC Unit

AIT/DA
ASTT
N&T

InfoSec
TSS
SEO
N&T
Future for IAM at Penn

Proposal for consideration

- Create an advisory board
- Appoint leadership in ISC
- Consolidate ISC IAM staff reporting to new position
Co-led school/center and ISC IAM leadership

- Cross-campus team with representation from schools and centers
- Representatives from
  - Schools and centers, including Business Services, Public Safety, DAR
Proposed IAM Leadership

♦ Designated leadership position for IAM in ISC
  • Manage core competencies for IAM
    – Together with advisory board
    – Understands school & center needs and works collaboratively with IT leaders to identify solutions
    – Solicits feedback and builds consensus with schools and centers for Penn IAM needs
  • Single point of responsibility and authority
  • Reports to University Information Security Officer

♦ Aligns with peer institutions ISC surveyed
  • Columbia, Brown, Harvard, Cornell, and a dozen others
Proposed Focused IAM Team

Dedicated IAM Team

Leadership

Data & Business Processes

Services & Technology

Application Services

Client Care

Platform Services

Current ISC IAM Staff – ~10*

* Peers surveyed have centralized IAM core teams of 10-25
Coming Soon: New PennKey Site

♦ Proposed site is live at:
  http://www.upenn.edu/computing/pennkey/pennkey_cs6/index.html

♦ We request your feedback by October 23rd

♦ Email penncommda@isc.upenn.edu
Penn+Box is a collaboration service in the cloud for sharing files and folders.

In addition to file sharing, Penn+Box offers a set of applications and tools that facilitate collaboration and data sharing.

<table>
<thead>
<tr>
<th>Penn+Box Storage</th>
<th>FY’14</th>
<th>FY’15</th>
</tr>
</thead>
<tbody>
<tr>
<td>50GB (Default)</td>
<td>$0.00/month</td>
<td>$0.00/month</td>
</tr>
<tr>
<td>Supplemental Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>500 GB*</td>
<td>$50.00/month</td>
<td>$50.00/month</td>
</tr>
<tr>
<td>750 GB</td>
<td>$75.00/month</td>
<td>$75.00/month</td>
</tr>
<tr>
<td>1TB</td>
<td>$100.00/month</td>
<td>$100.00/month</td>
</tr>
</tbody>
</table>

*Supplemental storage of 250 GB customers will be charged in increments an additional fee of $25.00/month.
Penn + Box - Growth over past year

- User base nearly doubled (9,056 to 16,541)
- Storage utilization tripled (7.5 TB to 24.1 TB)
Several 3rd-party applications with Box integration activated in the past year, including:

- GoodNotes
- iThoughts
- DocumentsToGo
- IFTTT
- SlideShark
- Outline+

Handling files larger than 5 GB is in development at Box. Penn will plan to deploy this feature when it becomes available in full production.
Penn + Box - 3rd Party Apps

Top Apps

- Box Sync for Windows: 1,060
- Box Sync for Mac: 969
- Box Edit: 650
- Box for iPad: 581
- Box for iPhone: 557
- Box Notes: 448
- Box for Android: 179
- Web Documents: 105
- Box for Office: 62
- Notability: 47
- Box for Android Tablet: 42
- Box for Windows 8: 41
- CloudOn: 23
- iAnnotate PDF: 22
- Box FTP Server: 13
- Email Folder: 12
- GoodNotes: 11
- Box for Windows Phone: 7
- Thunderbird: 7
- Box SimpleShare: 5

Number of Distinct Users
NET+ Box Community Internet2 and Box signed a new master business agreement in 2014

- After many months of community work and leadership by the Internet2 NET+ Box Advisory Board, the community-developed Business Associate Agreement (BAA) was added to the program
- In addition, the Enterprise Customer Agreement (ECA) was updated to reflect advancements in service, business terms, development options, and over two years of community feedback on the original ECA that was developed in 2012
Penn signed the NET+ Box Business Associate Agreement (BAA)
  • The BAA is the legal compliance document that takes the first step in enabling a HIPAA compliant Box instance

Penn adopted the new NET+ Box Enterprise Customer Agreement (ECA), which includes:
  • Doubled storage capacity for the same base price
  • Updated security and data handling information
  • De-provisioning of student accounts into free personal accounts for life
  • Refined support SLA and inclusion of Premier Support option
  • Improved language about Accessibility reflecting the ongoing work by Box and the campus accessibility working group
Thanks to everyone who contributed to the September and October NPTF presentations:

- Mark Aseltine
- Jeff Ballentine
- JoDe Beitler
- Stacey Carlin
- Jeff Edwards
- Geoff Filinuk
- Peter Heverin
- Deke Kassabian
- Sarah Katz

- John O’Brien
- Greg Palmer
- Charles Rumford
- Mark Sirota
- Eric Snyder
- Michel van der List
- Mark Wehrle
- Peggy Yetter
Open Discussion
Next Meeting

• November 10th
• Currently planned topics
  • Remaining topics
    • NextGen WWW
    • Yammer
  • New topics requested by NPTF members
  • Final rate setting for FY16