IT Orientation

Networking & Telecommunications
ISC Technology Services

June 2015
Agenda

• PennNet Definition
• Wired PennNet
• AirPennNet and Other Wireless Networks
• PennNet DNS Services
• Penn WebLogin and other Network Authentication and Authorization
• PennNet Phone
• Central Communication and Collaboration Services: Web, Email and Penn+Box
• Penn Video Services
• Policy and Planning
• PennNet Futures
PennNet Definition and Wired PennNet
PennNet: The University’s Network

• Interconnects 50,000+ devices in more than 230 Penn buildings
• Provides 3 distinct connections to two national ISPs, and 1 connection to Internet2
• Provides core services such as DNS, DHCP, Time Sync, & Authentication.
PennNet Building Network
PennNet Building Network
PennNet Building Network
PennNet Building Network
PennNet Building Network
PennNet Building Network
PennNet Backbone
PennNet Backbone
PennNet Backbone
PennNet Backbone, With Building Connections
PennNet Backbone, Redundant Building Connections
PennNet – Internet
PennNet – R&E Networks

- Internet
- Internet-2
- MAGPI

Diagram showing network connections and hardware components.
AirPennNet and other Wireless Networks at Penn
A Deeper Look
AirPennNet

- Primary SSID for Upenn
- Supports 802.11a/g/n/ac
  - 2.4GHz and 5.8GHz
  - Working on larger scale AC deployment
- Speeds up to 300Mbps
- Authenticated with PennKey
  - 802.1x
  - EAP-TTLS/PAP
  - EAP-TLS
A Deeper Look
AirPennNet-Guest

- Primarily for guests to campus
  - 802.1x incapable devices also
- Registrations last 1 week
- Protected by PennKey
A Deeper Look
AirPennNet-Guest (cont.)

• Conference Model
  – For large groups, conferences and the such

• Sponsored Guest Access Code
  – For small groups and such

• Sponsored MAC Address
  – Register device for guest via MAC Address

• Direct PennKey
A Deeper Look
AirPennNet-Help

• Configuration of Devices for AirPennNet
  – XpressConnect

• Captive Portal to instruct users

• Supports a wide range of devices
A Deeper Look

EduRoam

- Federated Wireless Access at Participating Institutions
- Uses PennKey to authenticate
- Configure Device before leaving campus
  - Can be configured off campus, but no way to test
The Stats
April 2015

- Access Points: 4,002
- Wireless Devices: 77,349
- AirPennNet devices/user: 1.98
- TB of Data Transmitted Wirelessly: 542.22
PennNet DNS Services
DNS Service Layers

• Assignments Service
  – Purpose: name/address management
  – Users: ISC and local IT staff
  – DNS “hidden master”

• DNS Authoritative Servers
  – Purpose: Publish Penn’s zones to the world
  – Users: Downstream, off-campus resolvers

• DNS Resolvers (recursive servers)
  – Purpose: Resolve names for local end-points
  – Users: All nodes on PennNet
Standard DNS Resolver Service

- rdns1a
- rdns1a
  - rdns1
    - 128.91.18.1
    - Primary
  - rdns2
    - 128.91.49.1
    - Secondary
  - rdns3
    - 128.91.94.1
    - Tertiary

PennNet DNS client
SafeDNS Resolver Service

sdns1a -> sdns1b
sdns1
128.91.18.2
Primary

sdns2a -> sdns2b
sdns2
128.91.49.2
Secondary

PennNet SafeDNS client
DNS Resolvers — Network Design

- **huntsman**
  - rdns1a
  - **sdns2a**
  - rdns2b

- **nichols**
  - **sdns1b**
  - rdns2b

- **hnt-brdr**
  - rdns2a
  - **levy**
    - rdns3a
    - **modv**
      - rdns3b
      - rdns1b

- **vag-brdr**
  - **vagelos**
    - **sdns1a**
    - sdns2b

The diagram illustrates the network design, where servers are interconnected via DNS resolvers (rdns) and secondary DNS servers (sdns).
DNS Resolvers — Network Design

- **DNS Resolvers:**
  - `rdns1a`
  - `rdns2a`
  - `rdns3a`
  - `rdns1b`
  - `rdns2b`
  - `rdns3b`

- **Nodes:**
  - **Huntsman**
  - **Nichols**
  - **Huntsman-Brdr**
  - **Nichols-Brdr**
  - **Vag-Brdr**
  - **Modv**
  - **Vaglos**
  - **Levy**

- **Links:**
  - `rdns2` between Huntsman and Nichols
  - `rdns1` between Huntsman-Brdr and Nichols-Brdr
  - `rdns3` between Levy and Vag-Brdr

- **DNS Servers:**
  - `sdns1a`
  - `sdns1b`
  - `sdns2a`
  - `sdns2b`
  - `sdns3a`
  - `sdns3b`
DNS Resolvers — Network Design
Penn WebLogin and other Network Authentication and Authorization
Some Definitions

• **AuthN**: Authentication
  – The process of proving that I am ‘jorj’

• **AuthZ**: Authorization
  – Granting the user ‘jorj’ some privilege

• *I may be able to Authenticate as ‘jorj’, but I am not Authorized to give you a raise in the payroll system.*
Some Systems of Interest

![Diagram of systems: KITE, CoSign, Kerberos, Shibboleth, PennCommunity, PennNames, PennGroups]
Who are you again? (AuthN)

• The piece of this that you will likely see the most is the PennKey
  – Made up of a PennName ("jorj") and a password ("<redacted>")

• PennNames are mutable, but you also have an immutable identifier: your PennID number
  – These are not private information like SSNs
  – Mine is 10018604
What can you do? (AuthZ)

- Penn Community holds information about your role at Penn
- PennGroups contains groupings of PennNames which are, in some sense, similar
  - Faculty/Staff/Student
  - System Administrators For CETS
  - Residents Of Suite 337

- Applications decide how to apply authorization rules based on this information about you
How Do You Do It?

• Authentication is performed by our central servers
  – Generally speaking, your PennKey password should only be handled by web pages on *.pennkey.upenn.edu
How Do You Do It?

• Some other ways in which your PennKey is used:
  – AirPennNet
  – Library services
  – Jabber (instant messaging)

• Optionally, you might also enroll in “Penn 2-Step”
  – 2-factor technology reduces the risk of someone stealing your identity and attacking Penn
  – Uses Google Authenticator

A Quick Aside…

• The things I’m discussing can be found easily via Google.

site:upenn.edu two-step
… and the red-headed step-child, KITE

- KITE is a Windows Active Directory which is managed by ISC, populated with Penn faculty/staff/student account lists
  - http://www.upenn.edu/computing/kite
PennNet Phone
What is PennNet Phone?

- Penn’s primary phone system
  - Polycom telephone sets
    - Polycom 321
    - Polycom 550
    - Polycom 650 (plus optional sidecars)
    - Polycom 6000
How do I use PennNet Phone?

• It’s a phone.

• It has a web interface.
  – [http://pps.voice.isc.upenn.edu](http://pps.voice.isc.upenn.edu)

• Google can help you.
  – site:upenn.edu pennnet phone

Some PennNet Phone features

• Bridged Line Appearances
• Call Forwarding
  – Advance One
  – Call Forward Ring No Answer
  – Call Forward Busy
• Ring Groups
• Scheduled call forwarding
• Voicemail
• … and a cast of thousands a bunch
Features and Voice Mail Settings - 215-746-3850

Your current PennNet Phone services are listed below. You can change your selections at any time. Changes will take place immediately after clicking the submit button unless the setting is marked as "Handset restart required".

PennNet Phone Settings

**Advance One**
- Advance One: on/off
- Destination Number: 5 digit PennNet Phone Number

**Call Forward All**
- Call Forward All: on/off

**Call Forward on No Answer**
- Call Forward on No Answer: on/off
- Call Forward on No Answer Destination: (see valid formats)

**Call Forward on Busy**
- Call Forward on Busy: on/off
- Call Forward on Busy Destination: (see valid formats)

**Call Waiting**
- Call Waiting: on/off

**Caller ID**
- Reject Anonymous: on/off
- Blocked Caller ID: on/off

**Ring Settings**
- Ring Caller ID: on/off

ps.voice.upenn.edu
Central Web, Email, and File Storage/Collaboration
Web Services

- Primary campus web server, http://www.upenn.edu
- Over 900,000 local server hits per day, and over 2 million hits on globally distributed Akamai servers
- Web sites for over 120 academic and administrative offices
- Virtual hosting services for 31 Penn sites including
  - http://www.alumni.upenn.edu
  - http://www.archives.upenn.edu
  - http://www.business-services.upenn.edu
  - http://www.dental.upenn.edu
  - http://www.facilities.upenn.edu
  … and many others
Zimbra and Exchange

- Two collaboration suite offerings from ISC
  - Email, Calendar, Tasks and more
- Both provide spam and virus filtering
- Both support hosted domains (user@domain.upenn.edu)
- Both support user@upenn.edu addressing
- Both use fully replicated servers and storage
- Both are monitored around the clock. Reports at http://status.net.isc.upenn.edu
Rapid Recovery Design

MOD5 NAP

Zimbra

Levy NAP

Zimbra (standby)
Exchange Service

- Integrated email and calendar for Outlook and Entourage users, with web access available
- Launched in 2007
- Currently about 4,200 accounts
- Details at
  - [http://www.upenn.edu/computing/email/exchange/](http://www.upenn.edu/computing/email/exchange/)
Zimbra Service

• Integrated email and calendar for users of open standard email tools, with advanced web access available

• Launched in 2008

• Currently about 13,200 accounts

• Details at
  – http://www.upenn.edu/computing/email/zimbra/
Email Forward-Only Service

• Allows for handling of
  – Users within a domain on our services who wish to retain that address but use an outside email service.
  – Users of any Penn mail system who wish to use a user@upenn.edu mail address.

• Over 4,000 Forward Only accounts supported today
Electronic Mailing Lists

- General access listservs
  - Restricted access, moderated content, archived
  - About 4,600 in use
  - [http://www.upenn.edu/computing/list/listmgmt.html](http://www.upenn.edu/computing/list/listmgmt.html)

- Class mailing lists (Classlists)
  - Over 10,000 each semester
  - [http://www.upenn.edu/computing/classlist/](http://www.upenn.edu/computing/classlist/)
Cloud Services – Penn O365

• A campus-wide collaborative project involving most schools and centers

• Taking several separate campus email & calendar services to Microsoft O365 in the cloud

• Includes 5 copies of Desktop Office Suite for faculty and staff at participating schools and centers, and for all students

• New service coming online in the second half of 2015
Cloud Services – Penn+Box

A place for users to store and work with files and folders

A built-in set of collaboration and productivity tools

Mobile access, web portal, and desktop file sync

Appropriate and safe for (most) University data

http://www.upenn.edu/computing/box/
Penn Video
Penn Video Network

- Provides professional, high-definition broadcast video production to the campus community
- Provides live and archived flash streaming to computers and IOS devices for many education, research and special events at Penn
- Manages Penn’s iTunes University podcast platform in coordination with many schools and departments
- Active in several AV/Video forums on campus such as AVSIG, VideoSIG and others
PVN and Coursera

- Penn is a major player in Massive Open Online Courses (MOOCs), with 34 course offerings to date from schools around the University

- N&T’s Penn Video Network (PVN) team supports Penn’s participation in Coursera

- PVN has produced 16 Coursera courses, with six more planned for FY’15

- Provides professional, high-definition broadcast-video production

- PVN has the expertise and infrastructure to support the creation of Coursera content

- PVN staff co-chair Penn’s Technical Advisory Committee

- [https://www.coursera.org/penn](https://www.coursera.org/penn)
Penn Broadcast Studio

• Completed in April 2012

• Operated by PVN team

• On-campus, dedicated HD video studio space that enables live and pre-recorded interviews and events to be transmitted directly to over 300 national and international news outlets, such as CNN, MSNBC, and Fox News

• One of only 20 university-based broadcast facilities nationwide that utilize IP-based video for transmission
PVN Cable TV Overview

- Installed in the early 1990s, with complete satellite dish farm, head-end, and Penn-owned distribution infrastructure

- Campus wide cable services of 75 standard def and HD channels to 60+ buildings, to some 9,000 students, many central pool classrooms, staff buildings.

- Penn-specific Movie Channel service – two 24-7 cable channels and a select online viewing service. Features “blockbusters” and faculty requests related to courses

- Full lineup, more info, request forms, troubleticket reporting at www.upenn.edu/video
Recently Added:
- BBC World-HD
- FX-HD
- The Knowledge Network
- Bloomberg News-HD
- CNBC-HD

"Resident Select" streaming movie service:
- On-campus users can view 20-30 on-demand films each month, including new releases and class support films
Policy and Planning
Policy and Planning

• Network Planning Task Force
  http://www.upenn.edu/computing/group/nptf/

• Network Policy Committee
  http://www.upenn.edu/computing/group/npc/
  – Some approved policies:
    • Use of PennNet IP Address Space
    • Use of @upenn.edu domain name
    • Social Security Number policy
    • Operation of DHCP Servers
    • Operation and Registration for Wireless Access Points
    • Authenticated Access to PennNet
    • PennNet Computer Security
PennNet Futures
Science DMZ

• In April 2014 we reported that Penn was successful in getting a Campus Cyberinfrastructure award from the National Science Foundation.

• This award was primarily for bringing high bandwidth to campus researchers and establishing a Science DMZ.

• A Science DMZ is “a portion of the network designed to optimize for high-performance scientific applications rather than for general purpose business systems or enterprise computing.” *

* Definition from ESNet:  [https://fasterdata.es.net/science-dmz/](https://fasterdata.es.net/science-dmz/)
Science DMZ Progress at Penn

- Campus 100 Gbps connection now operational.
- Dedicated 100 Gbps Science DMZ switches and circuits deployed.
- Initial connections provisioned or underway.
  - Connection to South Bank for Dr. Srolovitz (the PI on the Penn grant proposal) is underway.
  - Other interfaces soon to be allocated to researchers who wrote support letters.
- Deployment of measurement infrastructure and OpenFlow test lab equipment is in progress.
- Please see the diagram in subsequent slide.
PennNet Core, Border, and Science DMZ Topology

100Gbs Core Ring

Internet

Internet2
TR-CPS – AL2S

Border Router VAG
Core Router NIC
Core Router MODV
Core Router LEV
Core Router HNT

ScienceDMZ Switch

Researcher (Lab or Data Center)
Servers

InterDomain Controller (IDC)
Fast Data Transfer (FDT) Server
Network Architecture And Security Working Group (NASWG)

• In 2013 we introduced the idea of a new group to take a fresh look at PennNet design, particularly in the areas of segmenting and protecting networks.

• Since then, a large collaborative team has formed.
  – Participation from many schools and centers, sharing local network designs, challenges, solutions
  – Participants joined forces to look at new approaches to solving common problems in
    • network segmentation and extension,
    • network filtering,
    • network access management,
    • secure remote access, and
    • network visibility.
Network Architecture And Security Working Group (NASWG)

- Current methods of achieving network segmentation:
  - Routed Virtual LAN (VLAN) segments within a building
  - Dedicated fiber circuits between buildings
  - Routed private VLANs protected by Access Control Lists (ACLs) on the routers
  - Site-to-Site infrastructure Virtual Private Networks (VPNs)

- Current methods do not scale in a cost-effective way, nor do they meet all segmentation and reach use cases.

- Virtualization and overlay technologies would enable new approaches to network segmentation and extension.
In combination with the goals of the IRC, and leveraging what is being built for the Science DMZ, NASWG can bring new opportunities for PennNet architecture and security design.
In combination with the goals of the IRC, and leveraging what is being built for the Science DMZ, NASWG can bring new opportunities for PennNet architecture and security design.
Acknowledgements

Thanks to the following ISC Staff members for assembling and delivering this ITO content:

- Jeff Ballentine
- Jorj Bauer
- JoDe Beitler
- Jeff Edwards
- Deke Kassabian
- John O’Brien
- Charles Rumford
- Mark Wehrle