Networking & Telecommunications
ISC Technology Services

September 2017
Agenda

- PennNet Definition
- Wired PennNet
- AirPennNet and Other Wireless Networks
- University Firewall
- PennNet DNS Services
- Penn WebLogin and other Network Authentication and Authorization
- PennNet Phone
- Penn Video Services
- Other IT Services
- Policy and Planning
PennNet Definition and Wired PennNet
PennNet: The University’s Network

- Interconnects 50,000+ devices in more than 230 Penn buildings
- Provides 4 distinct connections to two national ISPs, and 1 connection to Internet2
- Provides core services such as DNS, DHCP, Time Sync, & Authentication.
IT Orientation – ISC Technology Services
wallplate
PennNet Building Network

Switch stack
PennNet Building Network
PennNet Building Network
PennNet Building Network
PennNet Building Network

Building Entrance Router

Building
PennNet Backbone
PennNet Backbone, With Building Connections
PennNet Backbone, Redundant Building Connections

- Huntsman
- Nichols
- VAG-BRDR
- Vagelos
- Levy
- MODV
PennNet – Internet

Internet

- Huntsman
- Nichols
- VAG-BRDR
- Vagelos
- Levy
- MODV

IT Orientation – ISC Technology Services
PennNet – R&E Networks

Internet

Internet2

Huntsman

Nichols

VAG-BRDR

HNT-BRDR

Vagelos

MODV

Levy

IT Orientation – ISC Technology Services
AirPennNet and other Wireless Networks at Penn
Wireless Architecture

Building A
- Local Controllers
- Master Controller
- Primary RADIUS

Building B
- Local Controllers
- Secondary RADIUS
- Master Controller

Huntsman
- Local Controllers
- HNT-BRDR

Nichols
- Local Controllers

Vagelos
- Local Controllers
- VAG-BRDR

Levy

MODV

Secondary RADIUS
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
AirPennNet-Guest

- Exclusively for guests to campus
  - Non-PennKey holders

- Rate-limited and port-restricted

- Registrations last until midnight

- On-boarding:
  - Agree to terms
  - Supply valid email

Upgraded April 2017
AirPennNet-Device

- For IoT devices
  - Monitoring
  - Entertainment
  - Managed loaner pools
  - Non-802.1x-capable

- Self-serve MAC-address registration
  - https://penndevice.aws.cloud.upenn.edu/

- Personal registration
  - Five devices per PennKey-holder

- Group registration
  - Unlimited devices, custom configuration

Upgraded/expanded
August 2017
AirPennNet-Help

- Configuration of Devices for AirPennNet
  - XpressConnect

- Captive Portal to instruct users

- Supports a wide range of devices
eduroam

• Federated Wireless Access at Participating Institutions

• Uses PennKey to authenticate
  – <PennName>@upenn.edu

• Configure device before leaving campus
  – http://eduroam.upenn.edu
Wireless Network Statistics
September 2017

• **Access Points:** 4,600

• **Wireless Devices**
  – AirPennNet: 67,000
  – AirPennNet-Guest: 93,000
  – AirPennNet-Device: 1,100
  – eduroam: 9,400
University Firewall
University Firewall Project

• In 2014, the **Institutional Risk Management Committee (IRC)** selected Information Security as its inaugural topic.
University Firewall Project

- In 2016, ISC Technology Services deployed a large-scale firewall at the PennNet border.
University Firewall

• I’m Just A Firewall Policy
## University Firewall

- **I’m Just A Firewall Policy**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Group(s)</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create/revise</td>
<td>Governance Board</td>
<td>Accept input from constituents and advisors. Define firewall policy.</td>
</tr>
<tr>
<td>Design</td>
<td>Network Engineering</td>
<td>Interpret policy and design implementation. Test in a lab environment.</td>
</tr>
<tr>
<td>Validate</td>
<td>Network Engineering and Information Security</td>
<td>Process live PennNet traffic in alert-only mode. Review and analyze alert logs. Consult with affected areas.</td>
</tr>
<tr>
<td>Block</td>
<td>The NOC and IP Engineering</td>
<td>Respond to trouble reports. Conduct diagnostics and resolve service impacts.</td>
</tr>
</tbody>
</table>
University Firewall “Known Bad”

- **Malicious hosts**: using Palo Alto intel categories
  - Malware
  - Phishing

- **REN-ISAC Feeds**: of malicious domain names, URLs, and IPs

- **Vulnerability exploits**: based on specific CVEs

- **Malware ("anti-spyware")**: with signatures marked “critical,” “high,” or “medium”

- **Malicious netblocks**:
  - Spamhaus DROP, EDROP, and BGPCC feeds
Blocked by border router ACLs

- Inbound and outbound SNMP (UDP/161)
- Inbound CHARGEN (UDP/19)
- Inbound Windows file sharing (TCP&UDP/135, 137, 138, 139, 445)

• These apply to nearly all traffic, regardless of firewall bypass
PennNet IP Address Space

- 262,652 publicly routable IPv4
  - Quickly approaching exhaustion

- 79,228,162,514,264,337,593,543,950,336 IPv6

- RFC 1918 private address
  - routed through the PennNet core
  - often deployed locally behind a departmental NAT

- All addresses in use on PennNet must be registered
PennNet IP Address Space

• Public IPv4
  – 128.91.0.0/16
  – 130.91.0.0/16
  – 158.130.0.0/16
  – 165.123.0.0/16
  – 192.84.2.0/24
  – 192.5.44.0/24

• Private IPv4 (RFC 1918)
  – 10.0.0.0/8
  – 172.16.0.0/12
  – 192.168.0.0/16

• Public IPv6
  – 2607:f470::/32
IPv6 adoption at Penn

World IPv6 Launch IPv6 measurements of AS55

IPv6 Deployment

<table>
<thead>
<tr>
<th>Month</th>
<th>0%</th>
<th>10%</th>
<th>20%</th>
<th>30%</th>
<th>40%</th>
<th>50%</th>
<th>60%</th>
<th>70%</th>
<th>80%</th>
<th>90%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun-2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sep-2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dec-2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar-2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sep-2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dec-2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar-2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sep-2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dec-2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar-2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sep-2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dec-2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar-2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sep-2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dec-2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sep-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
- rdns2a
- rdns2a
- rdns3a
- rdns3a

- rdns1
  - 128.91.18.1
  - Primary

- rdns2
  - 128.91.49.1
  - Secondary

- rdns3
  - 128.91.94.1
  - Tertiary

- PennNet DNS client
SafeDNS Resolver Service

128.91.18.2
Primary

128.91.49.2
Secondary

PennNet SafeDNS client
DNS Resolvers — Network Design
DNS Resolvers — Network Design
DNS Resolvers — Network Design
Penn WebLogin and other Network Authentication and Authorization
Some Definitions

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

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

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

CoSign to retire October 2018
Who are you again? (AuthN)

- The piece of this that you will likely see the most is the PennKey
  - Made up of a PennName ("obrienjw") 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 20810858
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
  – Canvas, Box, …

• Use Penn Two-Step Verification!
  – 2-factor technology reduces the risk of someone stealing your identity and attacking Penn
  – Uses DUO mobile
    – https://www.isc.upenn.edu/two-step-verification
Two-Step Verification

Penn WebLogin

Additional authentication is required.

- Trust this browser (What's This?)

Two-step verification code:

Log in

Call or text me a code

Call a friend

Enroll
KITE

- KITE – Kerberos Intermediary Trust Environment

- 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](http://www.upenn.edu/computing/kite)
PennNet Phone
What is PennNet Phone?

• Penn’s primary phone system
  – Polycom telephone sets

• Polycom VVX 401
• Polycom VVX 201
• Polycom 6000
• Polycom 650 (plus optional sidecars)
• Polycom 321 (End of Sale)
• Polycom 550 (End of Sale)
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
  – [https://www.isc.upenn.edu/pennnet-phone](https://www.isc.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 more
Features and Voice Mail Settings - 215-573-2628

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**

- Destination Number

**Call Forward All**

- Call Forward All

**Call Forward on No Answer**

- Call Forward on No Answer

**Caller ID**

- Reject Anonymous

**Blocked Caller ID**

- Blocked Caller ID

**Blocked Callers List**

**Ring Settings**

- Ring Duration

**Music on Hold**

- Music on Hold

- Music Source

Submit
PennNet Phone (UC interviews)
• Professional, high-definition broadcast-video production

• Live streaming videos for many education, research and special events at Penn

• Campus Television service, now including Xfinity on Campus

• Active in several AV/Video forums on campus such as AV-SIG
PVN and Coursera

• Penn is a major player in Massive Open Online Courses (MOOCs)

• Penn Video Network (PVN) supports Penn’s participation in Coursera, and provides production services to the Office for Online Learning for these courses, frequently collaborating with local school resources

• https://www.coursera.org/penn

• PVN co-chairs Penn’s Technical Advisory Committee for Online Learning
Penn Broadcast Studio

CNBC

FOX NEWS

MSNBC
Other IT Services
ISC Service Catalog

• Web hosting
• Email and calendaring (PennO365)
• Forward-only email
• Mailing lists
• File storage and sharing (Penn+Box)
• … and more

https://www.isc.upenn.edu/services
Policy and Planning
Policy and Planning

- IT Planning Task Force
  - Financial focus

- 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
Acknowledgements

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

– Jeff Ballentine
– JoDe Beitler
– John Breen
– Chris Cook
– Jeff Edwards
– Mayumi Hirtzel
– John O’Brien
– Charles Rumford
– Mark Wehrle
Backup slides
External Connectivity Locations

3701 Market

2929 Walnut

401 N Broad