Penn IT Orientation

Wireless @ Penn

An Overview to Operating Wireless Networks on PennNet and an Update on AirPennNet & AirPennNet-Guest

Wednesday, August 19, 2009
9:00 - 10:30 AM
Sansom Place West, 37th & Chestnut
Room 306, the "Bits & Pieces Room"
Things we will cover today

- An easy-to-understand explanation of PennNet Policies related to wireless and what they mean to you as a Local Support Provider
  - Things to consider before deciding to install and maintain a wireless device for your department on your own
- What you get with a PennNet wireless access point and what you pay for this service
- What ISC Networking & Telecommunications does during a wireless site survey
- What’s behind the scenes of Penn’s wireless implementation and what’s new in campus wireless upgrades
  - Current wireless projects
  - Plans for FY09 and FY10
Who creates the network policies?

Network Policy Committee (NPC)

http://www.net.isc.upenn.edu/policy/policy-list.html

Who is in NPC?

- IT professionals from ISC, SAS, Med School, Wharton, Office of Audit Compliance and Privacy, Residential Computing Support

What is their responsibility?

- To develop and review network policies and to recommend policies for approval

How is a policy created?

With a 6 step process: Identify, Draft, Discuss, Review, Create final draft, Seek approval
Approved Policies Relating to Wireless

- Policy on Deployment, Operation, and Registration Requirements for Wireless Access Points on PennNet
- Policy on the Operation of DHCP Servers on PennNet
- Policy on the Use of PennNet IP Address Space
- Policy on Routing Devices on PennNet
- Critical PennNet Host Security Policy
- Policy on Requirements for Authenticated Access to PennNet
- Policy on the Installation and Maintenance of Network Wiring
- Policy on Troubleshooting Charges for PennNet
Wireless Access Point on PennNet Policy

Policy on Deployment, Operation, and Registration Requirements for Wireless Access Points on PennNet

Points of Policy

• Any individual wishing to set up a new wireless LAN must first determine if wireless service already exists in the area to be covered. This includes consulting with ISC's registered access point database and performing site surveys. Interoperability of the intended installation and any existing wireless infrastructure must be addressed among the affected groups.

• Anyone that wants to then proceed with installing a wireless LAN must complete a registration form at http://www.upenn.edu/computing/pennnet/AP for the proposed number of APs. This form must be reviewed by ISC Networking & Telecommunications before any wireless AP's can be installed. ISC Networking & Telecommunications reserves the right to disallow the registration and operation of an AP if it would result in a conflict with another AP or networking device serving the same area.

• All AP registrations must be validated annually. ISC Networking and Telecommunications will send a report of registered AP's by contact name, to the responsible parties, at the beginning of each fiscal year.

• Existing APs that are part of a wireless LAN will have to be disconnected from PennNet and may need to be shut down or reconfigured at a later date, if/when Wireless PennNet or a School/Center or Department Supported Wireless network is to be installed in the same area or proximity.
Wireless Access Point on PennNet Policy

Policy on Deployment, Operation, and Registration Requirements for Wireless Access Points on PennNet

Points of Policy

• Requests to install new wireless LANs in buildings that already have Wireless PennNet or a School/Center or Department Supported Wireless network service may be denied.
• AP devices acting as DHCP servers must comply with the Policy on the Operation of DHCP Servers on PennNet at http://www.net.isc.upenn.edu/policy/approved/20000530-dhcpserver.html
• All IP addresses handed out by an AP must be registered in accordance with the Policy on the use of PennNet IP address space at http://www.net.isc.upenn.edu/policy/approved/20000124-ipaddress.html
• AP devices acting as routing devices must comply with the Policy on the Operation of Routing Devices on PennNet at http://www.net.isc.upenn.edu/policy/approved/20030310-routing.html
• All private wireless LANs must comply with the Policy on Requirements for Authenticated Access at Public Jacks, Kiosks, Wireless Networks, and Lab Computers on PennNet at http://www.net.isc.upenn.edu/policy/approved/20010910-netauth.html
Wireless Access Point on PennNet Policy

**Recommendations**

- Check with your School or Center computing director before planning a wireless LAN. Plans may already exist for broader building-wide wireless LAN initiatives.
- Careful planning of wireless LANs, including use of a formal site survey process, can significantly reduce later frequency conflicts and network performance problems. ISC Networking & Telecommunications can provide assistance in wireless LAN site surveys upon request.
- Wireless LAN "center frequencies" should be chosen such as to avoid frequency overlap. The use of only channels 1, 6, and 11 in 802.11b and 802.11b/g wireless LANs can help to avoid overlap.
- Wireless APs should be configured as bridging devices with DHCP services disabled. Configuring wireless APs as routing devices should be avoided as this can make troubleshooting and technical support more difficult and time consuming.
- In cases where access points have variable radio power levels, the minimal power level that provides the intended coverage should be chosen so as to limit interference with other devices operating in that frequency range.
- Users or departments that operate a private wireless LAN should periodically scan their building or area to ensure that there are no rogue access points.
Main points to follow (Simplified)

• AP Policy
  – Register your APs

• DHCP Policy
  – Register your DHCP servers

• IP Address Policy
  – All IP addresses must be tracked in Assignments (This includes non-globally routable address ranges)

• Routing Policy
  – Devices must comply with the critical host policy
Main points to follow (Simplified)

• Critical Host Policy
  – Administrators must have authenticated access to the APs (via Username/Password)

• Net Auth Policy
  – Must Authenticate users not devices
  – Must maintain access records for 60 days
    • Logs must include
      – Identity of user
      – IP Address
      – Date and time of Connection
Questions about policies?
What you get with a PennNet wireless access point and what you pay for this service

• Survey and Installation
  – Initial Walkthrough
  – Site Survey
  – Cable Installation (by union contractor)
  – Equipment Configuration and Activation
  – Final Site Survey
  – Documentation (enables monitoring, and billing)

• You do not pay upfront costs for the wireless Access Points (APs)
What you get with a PennNet wireless access point and what you pay for this service

• Post Installation Monitoring and Support
  – 24x7 polling and alarming
  – Failure notification
  – On-call support
  – Hardware replacement

• Fully Compliant with Policies
  – Central authentication using PennKey and Password
  – Authentication logs retained

• 4 Year Replacement Cycle
  – Allowing for deployment of advanced features
What ISC Networking & Telecommunications does during a wireless site survey

• Meet to discuss requirements
  – Areas to be covered
  – Wireless client density
  – Type of use (Web browsing, Special Applications)

• Survey areas
  – Determine placement and number of APs required to provide to provide requested coverage
  – Use wireless test tools to measure signal strength from various points around a test AP
  – Check RF signal strength through walls and floors
  – Mark recommended AP locations on floor plans
What ISC Networking & Telecommunications does during a wireless site survey
What ISC Networking & Telecommunications does during a wireless site survey

• An estimate is created from the survey results
• Labor is charged for the survey
  – Charges are based on published hourly rates
  – Labor rates can be found at http://www.upenn.edu/computing/isc/networking/rates/labor.html
• Rough estimates for AP installations can be found at http://www.upenn.edu/computing/isc/networking/rates/data/wireless.html
• Installation can be scheduled by sending an email to service-requests@isc.upenn.edu
How do I request a wireless survey?

- Send an email to service-requests@isc.upenn.edu
- Or call 746-6000
- Always remember to provide:
  - 26-digit budget code
  - Coverage area information
  - User density
  - Type of use
Questions about surveys or installation costs?
What’s behind the scenes of Penn’s wireless implementation and what’s new in campus wireless upgrades

Existing Cisco APs being replaced with Aruba

• 1400 Aruba APs and 4 controllers have been purchased
• The controllers are licensed to support 500 APs each
• Over 700 of the APs have already been upgraded
• What are the differences between our Cisco and Aruba wireless networks?

  – Current Cisco APs running full “Fat” IOS
    • Full configuration file managed for each AP
    • APs operate independently from each other
    • Authentication is handled at the AP
    • Routing is local with the building
    • APs continue to operate if the central management system fails.
Gateway for building wireless networks

Gateway for building wireless networks

RADIUS Server

Cisco AP Management Server
What’s behind the scenes of Penn’s wireless implementation and what’s new in campus wireless upgrades

Existing Cisco APs being replaced with Aruba

• What are the differences between our Cisco and Aruba wireless networks?
  
  – New Aruba APs running “Thin” OS
    
    • Minimal configuration needed on the AP
    • Centralized controller holds full configuration for groups of APs. We currently create a separate group per building
    • Authentication is handled at by the controller
    • Routing of all wireless traffic is handled in the PennNet core
    • Redundant controller configuration minimizes downtime
      
      – APs automatically discover the master controller
      – Master controller downloads configuration to the AP
      – AP is handed off to its local controller
      – AP will failover to the master controller if its local controller fails
Primary gateway for all wireless networks

Secondary gateway for all wireless networks
What’s behind the scenes of Penn’s wireless implementation and what’s new in campus wireless upgrades

Plans for FY09 and FY10

- Currently running two association methods
  - DynamicWEP (Open/WEP) (Old standard client config)
  - WPA (WPA/TKIP) (FY09 standard client config)
- Need to remove DynamicWEP in favor of WPA2
  - How many clients are still running DynamicWEP?
  - WPA (WPA/TKIP)
  - WPA2 (WPA2/AES) (Possible FY10 standard client config)
- This will allow for deployment of 802.11n
  - Association rates up to 300Mbs
  - Requires WPA2/AES
- IP Multicast support

WEP - Wired Equivalent Privacy
WPA/WPA2 – Wi-Fi Protected Access
TKIP – Temporal Key Integrity Protocol
AES – Advanced Encryption Standard
Q&A

Thank you for attending.