



Trends in WLAN management

Philippe Hanset,

University of Tennessee, Knoxville

phanset@utk.edu



Agenda: a few models

- UT Knoxville Wireless
- Deployment Models
- Cost Models
- Design Approaches
- Roaming Models
- Rogue Wireless Device Detection
- Special Projects

UT Knoxville Wireless



- ~26,000 Students
- ~4,000 Fac/Staff
- 1270 Access Points
- 12,000 Registered Wireless Users
- up to 1500 Concurrent WU
- 2000 daily WU



Decentralized Deployment

- Often happened by accident, over time
- no ip roaming
- no guaranteed service
- RF nightmare
- security, a la carte
- Can lead to interesting developments
(Univ of Utah's 802.1x RADIUS proxy)
- Get a CIO on Steroids, an AUP and an attractive cost model



Centralized Deployment

- Choice of IP roaming
- Integrated RF planning
- One time registration
- One phone number to complain!
- Allow Exceptions for your peace of mind (FBI grants, Scientific apps...)

Exceptions?

Collaborative Robots from Prof. Parker's Lab at UTK



Joint-Techs, Salt Lake City





Cost Models: Free

- “Free” (centrally funded)
 - works well if wired is free too
 - wired tends to be replaced by wireless otherwise
 - Minimizes Rogues
 - Monitor usage (constantly connected, bandwidth hogs, ...)



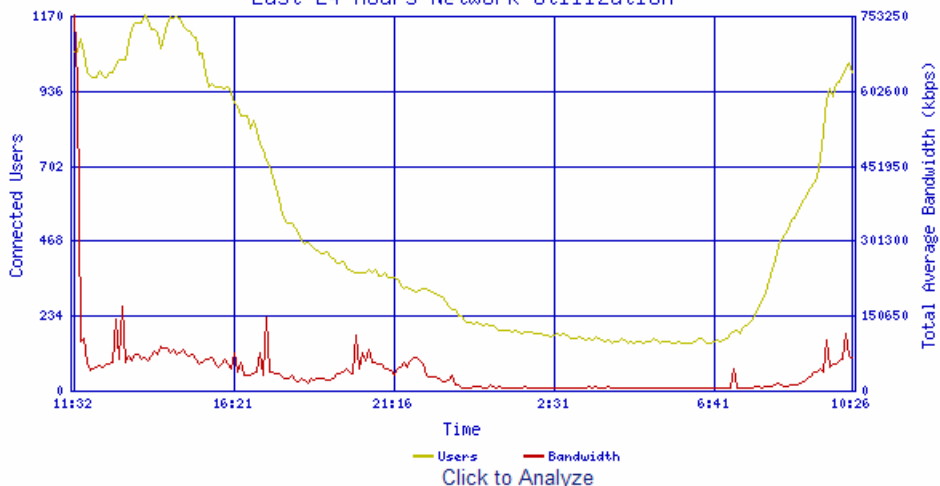
Status

Total APs: 1182
Total Users: 12257

Users Last Cycle: 559
Users Last 24 Hours: 3070

Average Bandwidth: 538.16 Mbps
Average Bandwidth/User: 175.30 kbps

Last 24 Hours Network Utilization



Dead APs (18)

- WTC31 (10.1.135.133)
- WPD11 (10.1.136.66)
- WTB03 (10.1.21.4)
- WTB04 (10.1.21.5)
- WPH32 (10.1.28.14)
- WPH02 (10.1.28.8)
- WHE15 (10.1.54.13)
- WHE25 (10.1.54.19)
- WHE2E (10.1.54.28)
- WHE3B (10.1.54.39)
- WHE3D (10.1.54.41)
- WHE42 (10.1.54.44)
- WHE06 (10.1.54.7)
- WHE07 (10.1.54.8)
- WSC11 (10.1.8.2)
- WVM1AA (10.2.62.41)
- WPO04 (10.249.14.6)
- W1X01 (10.5.1.12)

Top Bandwidth Users

(Last 24 Hours)

Rank	MAC	Total Data (kB)	Average BW (kbps)
1	000C415EAE55	15778915.73	1461.01
2	00904B630339	10935065.74	1012.51
3	000D9384FC99	10654146.33	986.50
4	000FEA9134B7	10621096.55	983.43
5	000475E579B0	9697262.81	897.89
6	00042377DF45	8726433.59	808.00
7	00904B0A5DA5	7592084.11	702.97
8	00408C682DA3	7171645.82	664.04
9	00045A0E35D7	6326213.10	585.76

Top Bandwidth APs

(Last 24 Hours)

Rank	AP	Total Data (kB)	Average BW (kbps)
1	WLB33	33876442.78	3136.71
2	WAA34	33186233.28	3072.80
3	WAA41	26867895.07	2487.77
4	WSE22	25876537.99	2395.98
5	WVM1X	24641082.35	2281.58
6	WFH33	24156662.57	2236.73
7	WAA43	22081250.15	2044.56
8	WMH34	21627471.32	2002.54
9	WHL38	21299204.38	1972.15

Status

Admin

Monitoring

Commands

Reports

Search

Tasks

Logs

Help

Log Out



Cost Model: Charge

- Management/Accounting nightmare
- Subcontract with a Provider, which might lead to interesting Cellular/WiFi integrations
- Rogues?
- WLAN2 for advanced applications ;-)



Design Approach (vendor)

- Aggregated APs with controller
 - One proprietary switch port per proprietary AP or non prop. AP but with loss of functionality
 - Controller takes care of registration and authentication
 - Lots of features
 - In-line technology: reliability of switch? (PC based)



Design Approach (vendor)

- Tunneled APs with controller
 - One proprietary tunnel per AP to decentralized controller
 - not forced to use vendor port for AP
 - Controller takes care of registration and authentication
 - Lots of features
 - In-line technology: reliability of switch, capacity for 802.11n?



Design Approach (vendor)

- Everything through gateways, any AP
 - Can do 802.1x, MAC, visitors
 - Traffic control
 - IP roaming
 - in-line, PCs passing traffic
 - ...lots of subnets, lots of gateway
 - How much CPU required with 802.11n?



Design Approach (in-house)

- VLAN/SSID
 - SSID for Registration and visitors
 - SSID for 802.1x
 - SSID for MAC authentication (RADIUS)
 - SSID for Voice over WLAN
 - Does require SSID juggling for users
 - Does not require in-line devices
 - Separate management of AP from traffic



Design Approach

- Home-Grown (cont.)
 - Prevent static IPs by correlating ARP/DHCP/AP
(some AP vendors provide IP info)
 - Monitor traffic through polling of APs
(IP-MAC-Signal Strength-in/out packets)
 - Decrease MAC authentication over time
and limit it to special cases



Roaming Models

- Vertical Subnetting (to limit broadcast)
 - Trunk multiple Wireless VLAN in parallel.
 - Assign VLAN according to specific criteria (with VLAN assignment through 802.1x, part of the Identity Based Networking concept)
- Horizontal Subnetting
 - gateways or controller with IP Mobility
 - proprietary agents (requests client software)
 - Wait for a standard IP Mobility



Rogue Device Detection, APs

■ Wired Side

- OUIs (first 24 bits of MAC)
 - not always trivial since some vendor use same OUI for ethernet cards and APs
- Fingerprinting
 - HTML, telnet, SSH, except when the device is firewalled
- TTL (NAT boxes and APs)
 - These devices have often different TTL than OSes
- Our NetReg can detect NAT as well: compare MAC from DHCP lease and MAC from the executable that runs on machines during NetReg



Rogue Device Detection, APs

- Wireless Side

- Rogue AP Detection built-in AP. Compare Detection report (eg: SNMP trap sending MAC/Signal Strength) to exclusion list. Use RAD report from multiple APs to triangulate location on maps, or directional antenna
- QA of coverage comes for free in the process. Use RAD reports to measure the health of your wireless network
- Use your segway and a laptop with netstumbler



Rogue Device Detection, Ad-Hoc

■ Detection

- MAC addresses of Ad-Hocs are random (cannot correlate with MAC of NIC)
- Local search with directional antenna can only show culprit (or local probes)
- Good luck in an Auditorium with 200 laptops

■ Remediation

- Configure Windows (infrastructure only) and Macs (uncross “allow computer to create networks”) appropriately
- Use defensive devices to disrupt Ad-Hoc traffic



Special Projects

- Put UT's WLAN on Uninterruptable Power Source. Batteries from Core to User.
- APs on Solar Panels
- Prevent our Physical Plant people from Sheet-rocking APs.
- Have a way to Authenticate an infrastructure, besides using EAP-TLS