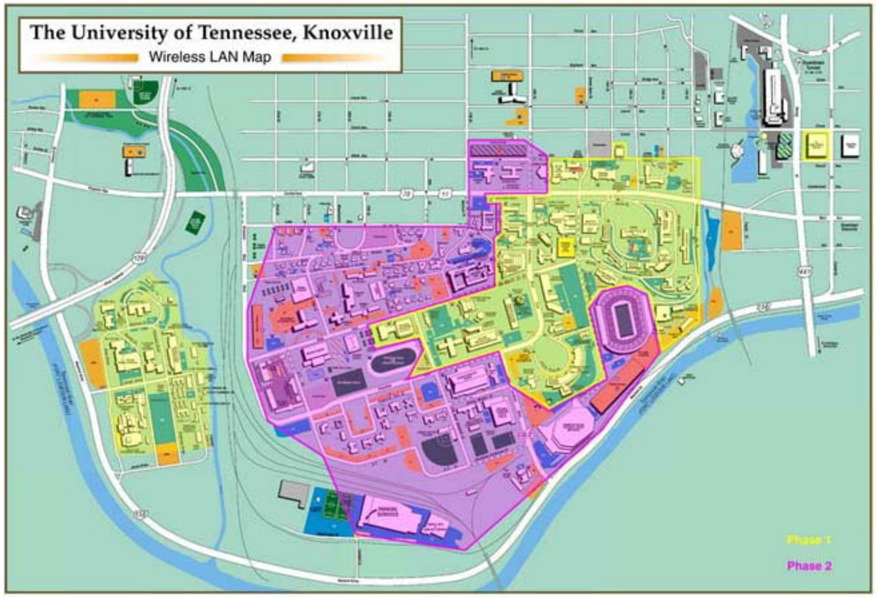
Large-Scale Wireless Networks
UT’s case

Philippe Hanset
The University of Tennessee
phanset@utk.edu

The University of Tennessee

- ~26K Students, ~4K faculty/staff at the Knoxville Campus, 15M assignable Sq Feet



History of WLAN at UTK

- 8 pilot projects by early Summer 2000 (Lucent's donation)…total success
- President instructed a campus wide WLAN in one year, an a plan in 3 days (pilots and active ethernet required)
- Started in January 2001, mostly accomplished by March 2002

Critical Design Factors

- Power over Ethernet (802.3AF)
  - Project unthinkable if AC had to be pulled for 1200 APs
- 802.11b with 802.11a in mind (25 dB at 2.4 GHz extrapolates to 18 dB at 5 GHz)
- 4 channels instead of 3

Aggressive Deployment

- Knowledge of campus wiring comes first, wireless can be taught
- Survey the survey (maps before and after)
- Scripting 101 for Contractors
- Centralize cat5 drops to save power injectors
- Centrally deployed, with AUP (UT “owns” 2.4 and 5 GHz)
- Access is a key factor

Surveys

- Substantial variation in WLAN cards sensitivity
- Same antennas before and after
- Empty/Full buildings
- Inter-Building interferences
- Vertical usually better than Horizontal
- A dolly with a 12V battery and a power inverter

A few Big VLANs

- Considering the complexity and early stage of Mobile IP, UT decided to provide roaming to wireless users through the extensive usage of VLAN-trunks. A few huge flat networks. The main one has 920 APs
- Wireless-VLANs prevents IP contention in local subnets
- On average, 40Kbps of broadcast traffic (no multicast nightmare…so far)

Private IPs for APs

- Saves 1200 IPs in UT’s case
- Security by obscurity
- Easy to extract from ARP (home grown monitoring tool)
- Impersonate an AP gets you nowhere (web authentication gateways)
- Permits a practical IP numbering,
  quite useful to locate APs in huge VLANs

Numbering and Naming

- WSS13 is a wireless device in Student Services, first floor, 3rd AP.

  WHTAG is a wireless device in Huge Tower 10th floor, 16th AP (36 floors, 35 APs MAX)
- If DNS fails: AP is in VLAN1 connected to same switch as local wired subnet 160.36.24.0/24, its IP will be 10.1.24.x
- Unrelated but useful: color coded patch cables

Management

- APs are everywhere
  - Hide and Seek (sticker or not)
  - Location Maps with accurate positioning (XP doesn’t reference AP-ID)
  - Naming convention
  - Active Ethernet (remote control)
- PERL/SNMP at the moment
- New niche for management software
- Cannot VLAN-trunk everywhere

Security trends

- Original test was wide-open
- Tried to enforce WEP with pilots: Unmanageable, no support for Apple at the time. WEP+ is fine for PTP
- Massive deployment used a fully authenticated and encrypted solution (1200 firmware changes in 5 days!)
- Semi-open at the moment with silent monitoring based on DHCP registration

No Security

- **Important Information Regarding WIRELESS SECURITY** **The new wireless network offers NO security features**. Anything that you send across the wireless network will be visible to others. If you check your email on the wireless network using one of the typical email clients (Outlook, Outlook Express, Eudora, Netscape Mail, etc), your username, password, and email will all be visible to anyone in the general area. This does not mean that you cannot check your email on the wireless network. It only means that you must be careful how you do so. Here are some things you should do:
- 1. USE WEBMAIL -- https://webmail.utk.edu is a secure site, so you can securely check your email via Webmail.
  2. USE SSL -- When visiting websites that need to be encrypted (online banking, etc), make sure that you are connected to the site securely by checking for the glowing or locked padlock in your web browser. If you are connected to the site securely, then all of your communication with that website is encrypted.
  3. USE VPN -- A more complete solution is offered by using a Virtual Private Network client while connected to wireless. A Virtual Private Network (VPN) creates an encrypted tunnel through which you transmit data. Using a VPN connection, all of your traffic over wireless will be encrypted.
- More information about the above issues, including a link to the VPN client, is available

  at http://wireless.utk.edu/security.

Home Grown solution

- ARP tables of Wireless VLANS are collected every 5 minutes
- Checked against DHCP registration database, which resides on LDAP
- Un-identified MAC are filtered at the switch, in CAM table.
- In 8 months, only 6 cases

Off-the-shelve Authentication

- UT explored off-the-shelve solutions, WEB based
- Integrates with most existing solutions (LDAP, RADIUS, SQL…)
- Provides "a la carte" services based on users identity (can be contoured)

  as a faculty said "just beat the cheating curve"
- Visitors…show me the credentials, sponsors

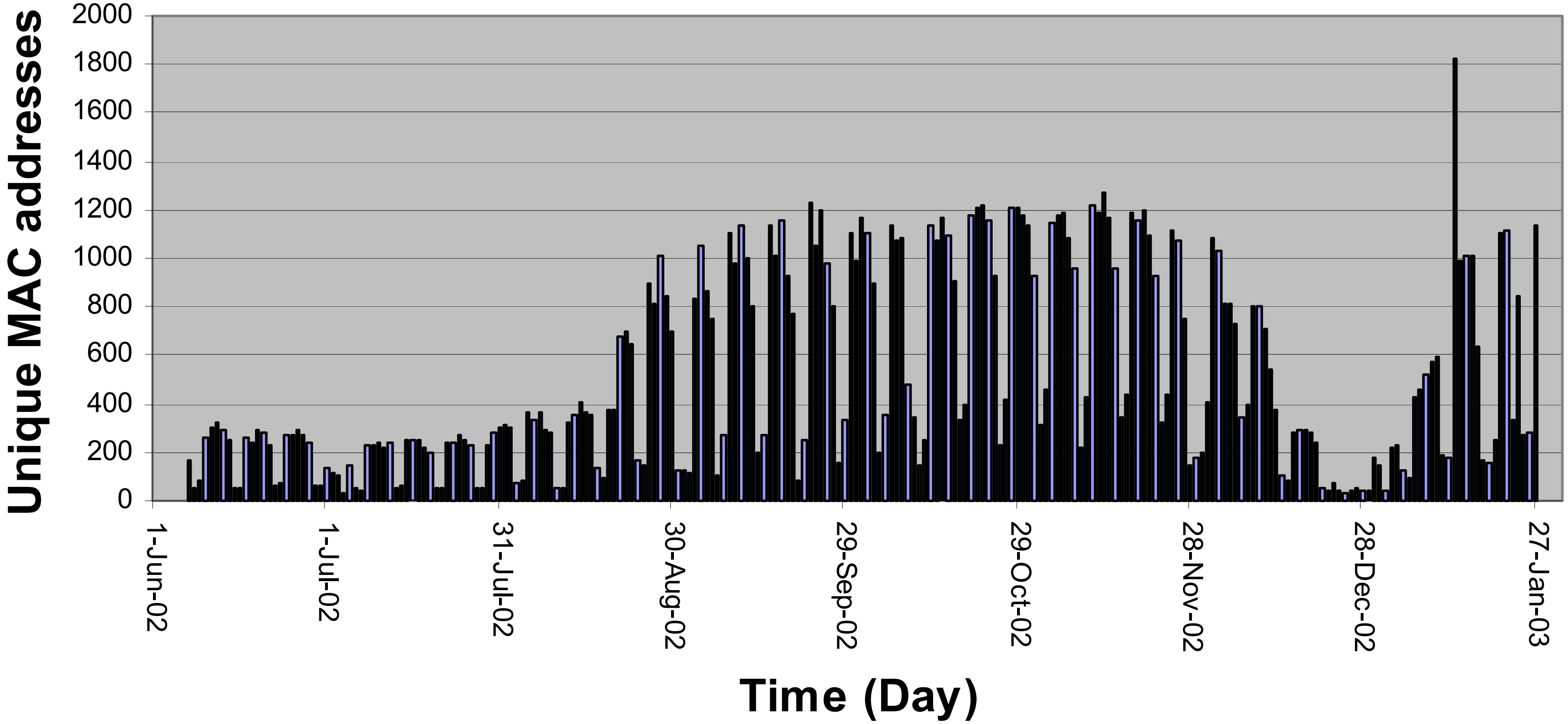
Encryption

- Convenience before Security
- We had it, it failed…better be perfect before another essay (802.11i)
- Make it as ubiquitous as PPP
- Our worst nightmare: POP and IMAP (What about Ebay?)
- use VPN if your info is sensitive

Interesting Happenings

- Rogues APs, where service is not available (eg: Dormitories)
  - How to detect rogues APs (MAC, driving)
- Faculty wanting to stop services during exams (jammers illegal in US)
- WISP without consent
- Unknown Boxes in ceilings

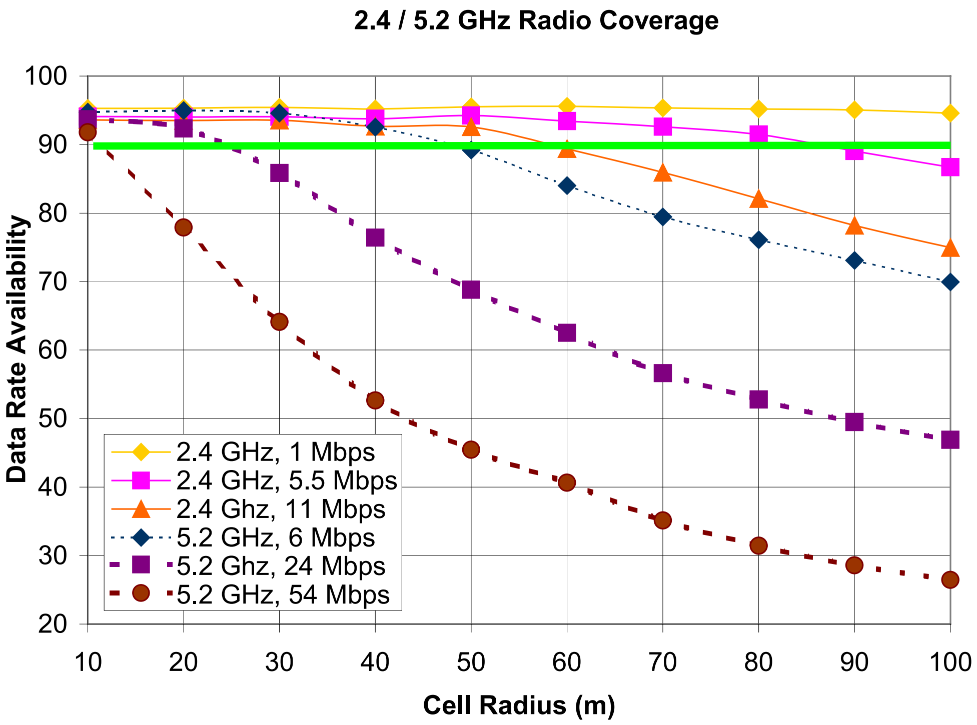
Wireless Utilization (4000 registered users)



b a g

- b works
- a is not practical, mostly because of antenna restrictions
- g keeps coming
- Every b joining the AP will slow down the gees

a and b ranges



Courtesy of :

agere systems