Mobile Madness 2011

Educational Session

Mobile Madness 2011

Overview

- Site surveys and physical challenges
- Network Topology and Roaming Devices
- Cellular Data Networks
- Choosing Devices
- Mobile Device Deployment
- Mobile Browser Security
- Authentication and security

Wireless Survey

Save Yourself Some Pain!

- Initial Survey
  - Establish location of APs
  - Evaluate network coverage
  - Evaluate user needs/security
- Periodic surveys
  - Discover rogue wireless devices
  - Evaluate network coverage
    - Weak areas for signal increase
    - Strong areas for signal decrease to prevent unwanted coverage
  - Test security measures

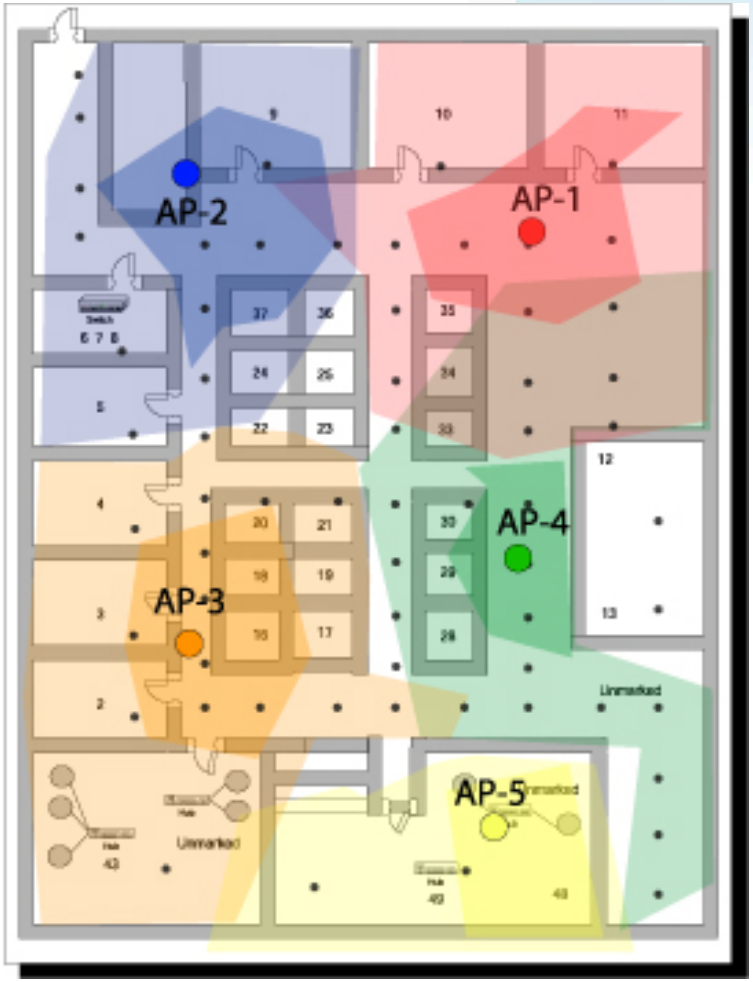
Wireless Survey

Physical Challenges

- Walls/Ceilings/Floors
  - Lead lined MRI/X-Ray rooms
  - Elevator shafts
  - Some negative pressure rooms
  - Unseen pipes
  - Concrete (wire mesh/rebar reinforcement)
- Windows
  - Can be a good thing if window is to the outside
- Doors
  - Solid core/Fire doors

Wireless Survey

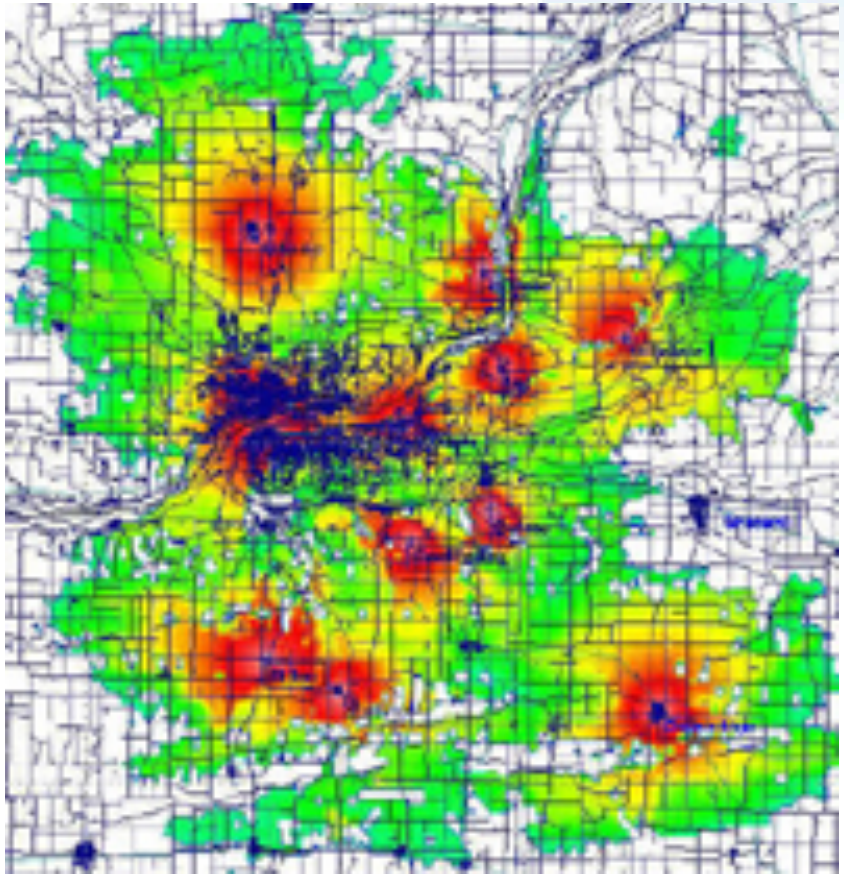
Continued



Your individual survey will show your weak and strong areas: walls, doors, pipes, ducts, windows, etc. Any large object can have an effect on your wireless coverage.

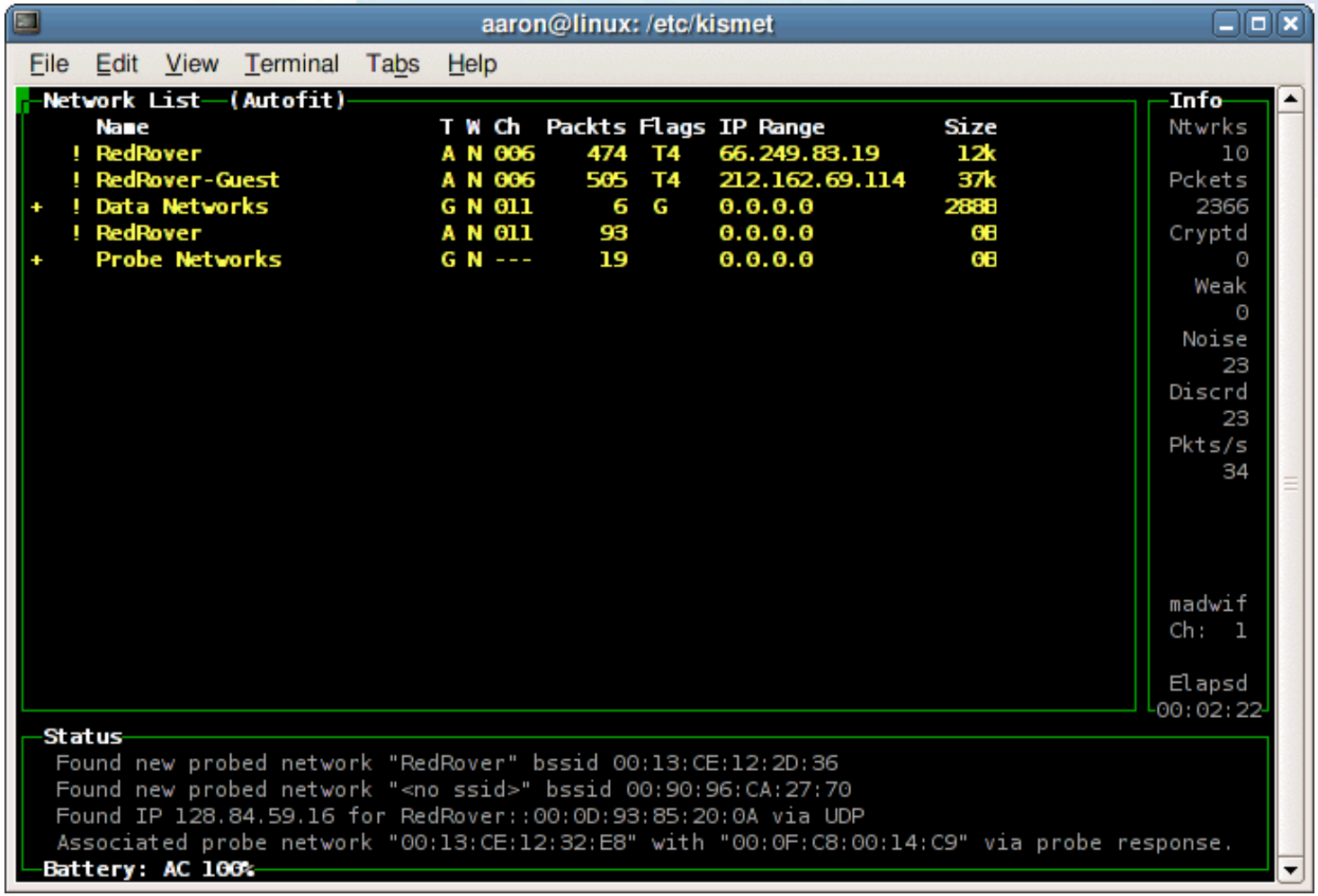
Wireless Survey

Continued



It may look like a weather map, but this is the result of two pieces of software: Kismet and GPS Visualizer.

Kismet


aaron@linux: /etc/kismet
File Edit View Terminal Tabs Help
Network List (Autofit)
Name T W Ch Packts Flags IP Range Size
! RedRover A N 006 474 T4 66.249.83.19 12k
! RedRover-Guest A N 006 505 T4 212.162.69.114 37k
+ ! Data Networks G N 011 6 G 0.0.0.0 288B
! RedRover A N 011 93 0.0.0.0 0B
+ Probe Networks G N --- 19 0.0.0.0 0B
Info
Ntwrks 10
Pckets 2366
Cryptd 0
Weak 0
Noise 23
Discrd 23
Pkts/s 34
madwif
Ch: 1
Elapsd
00:02:22
Status
Found new probed network "RedRover" bssid 00:13:CE:12:2D:36
Found new probed network "<no ssid>" bssid 00:90:96:CA:27:70
Found IP 128.84.59.16 for RedRover::00:0D:93:85:20:0A via UDP
Associated probe network "00:13:CE:12:32:E8" with "00:0F:C8:00:14:C9" via probe response.
Battery: AC 100%

Wireless Survey

Software

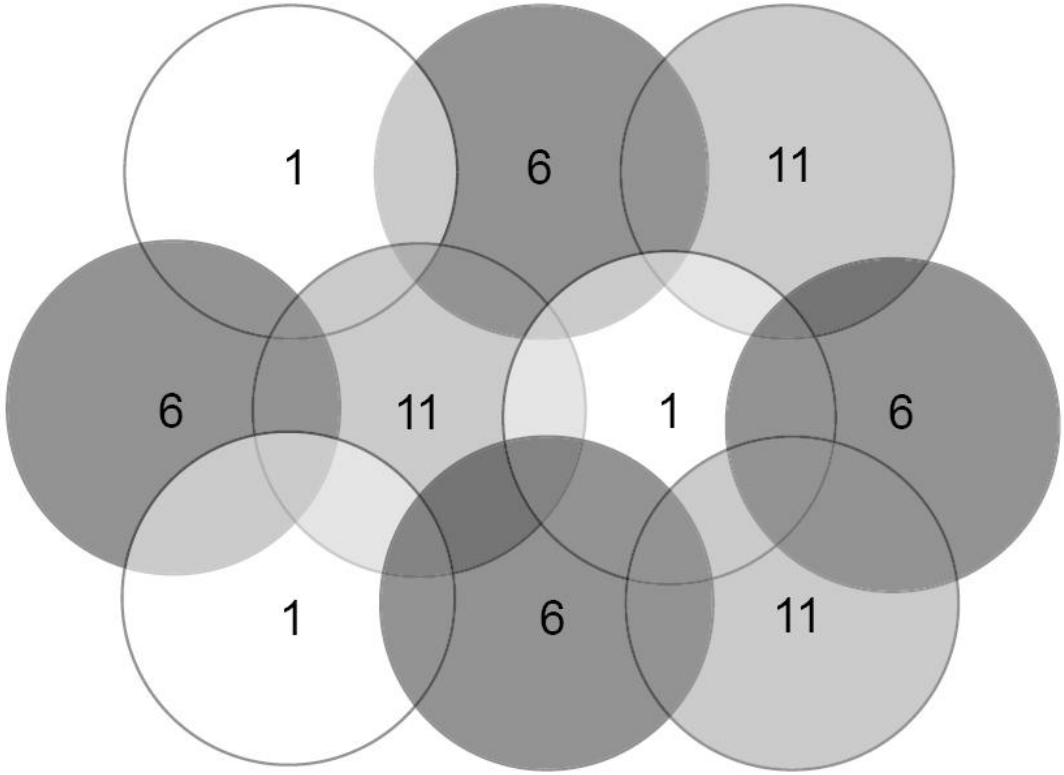
	AirMagnet	WaveDeploy	Ministumbler	Ekahau	WiFiFoFum
Estimated Price	$2250	$5000-6000	Free	$300-5000	Free
OS Compatibility	Windows XP, Windows 7 Netbook edition	Win XP-7, Mobile 6.0, Apple iOS, Linux, Mac OS X	PocketPC 2002/3, Mobile 2003	2000, XP, Tablet PC, Android 2.1,2.2	PocketPC 2003/Mobile 5.0 & 6.0
802.11 Compatibility	a/b/g/n	a/b/g/n	a/b/g	a/b/g/n	b/g
Spectrum Analysis	Optional	Optional	None	Optional	None
Site Map	several	gif, jpg, png, bmp, tiff	None	bmp, jpg, png	None
Device Compatibility	Laptops, Tablet, Netbook	Laptops, PDA using Pocket PC	Handhelds	Laptops, Tablets, Android phones	Handhelds

Network Topology

- Network topologies for wireless usage
  - Star
  - Mesh (partial and full)
  - Tree
  - Line
- Generally a wireless network will be a combination of different topologies
- SSIDs, Authentication/Encryption settings and IP/Subnet should be consistent across APs
- Channel should be different between APs within each others range

Network Topology

Channels



Device Roaming

- Disassociate: Client drops its connection from old AP
- Scan: Client scans for new AP
- Reassociate: Client attaches to new AP. Client informs new AP of the AP it was just connected to.
- Authenticate: Client provides credentials for networks authentication method

Cellular Mobile Connectivity

- Works well where:
  - Sufficient coverage exists
  - Intermittent connectivity is tolerable
  - Bandwidth is sufficient for the application
- Problem Areas
  - Truly mobile workers will switch towers and leave coverage for a few moments
  - Bandwidth is shared among subscribers on the same tower
  - Latency can be very high
  - 3G is a marketing term – not a bandwidth

Cellular Mobile
Recent experience

- Backup Connectivity
  - Great for your facility or connection
  - Good for mobile workers
  - Bandwidth on 3G is sufficient for most uses
- Problem Areas
  - Not so good when everyone in the area is out of power or connectivity
  - Not good where there are large concentrations of devices

Choosing Devices

- How will the device connect to the data network? OS Requirements?
- Where will this device be used?
- Who will be using the device?
- Battery capacity and recharge time?
- Does the device require a barcode reader?
- Will the device be used in low light?

Where will the handheld be used?

- Loading Dock
  - Hot in the summer, Cold in the Winter
  - Dusty
  - Occasionally wet
- Emergency Department, Surgical Areas, Isolation Rooms
  - Very Frequent Cleanings with chemicals and exposure to various fluids
- Nursing Areas, Emergency Department
  - Spills, Fluids, frequent knocks

Sealing Standards
Ingress Protection

IP # #

Solid Objects

0: non-protected

1: 50mm diameter

2: 12.5mm diameter

3: 2.5mm diameter

4: 1.0mm diameter

5: dust-protected

6: dust-tight

Water

0: non-protected

1: vertically dripping

2: dripping (15-degrees)

3: spraying

4: splashing

5: jetting

6: powerful jetting

7: temporary immersion

8: continuous immersion

Who will be using the device?

- Doctors
  - Don't want another device to carry
  - Usually willing to switch for features
  - Want their own device
- Nurses, Phlebotomists, etc.
  - Often have higher personnel turnover
  - Will want to use devices supplied to them
  - Need barcode recognition
- Other support staff
  - Typically need barcode recognition

Mechanical Shock
Drop ratings

Ruggedized, Semi-Rugged, and Ultra-Rugged Devices

- As a device class, mainly a marketing term
- Look for drop ratings
  - Ability to survive a 4ft drop to concrete
  - Tested functional after 500 1.6ft drops in a rotating drum
  - Tested for repeated (26) 5ft drops to concrete

Mechanical Shock Specifications

Key Terms

- MIL-STD/MIL-SPEC – US Military Standard
- IEC – International Electrotechnical Commission

•Statements

- Tested to exceed MIL-STD and IEC specifications
- Thousands of standards
- MIL-STD 810F Method 514.5 – Vibration
- MIL-STD 810F Method 516.5 - Shock
- IEC 68227 – Mechanical Shock Test

Battery capacity and recharge time?

Example

- Battery capacity (which scanning barcodes and checking the network): 5 hours
- Battery recharge time: 16 hours
- Required duty cycle: 24 hours

Suggestions

- Replaceable Batteries
- Charging stands
- Battery chargers

Barcode Reader considerations

Symbologies

- 1D or 2D barcodes

Light Conditions

- Red Laser types usually read even in low or no light
- Imagers with lighting are questionable in a patient room in low light
- Newer low light imagers should be tested prior to purchase

Device Juggling

- Separate bluetooth or wireless readers

Handheld Deployment

- AirBEAM
- Wavelink Avalanche MC
- Microsoft Mobile Device Manager
- Features:
  - Ability to configure devices without pre-staging
  - Updating firmware, drivers and software remotely (some devices)
  - Inventory and tracking

Application Deployment

- Hosting from a Web server
  - Devices will need network access
- Activesync
  - Some handheld manufacturers have multiport cradles that allow multiple device syncing and configuration
- Memory Card
- Management Solution
  - Avalanche
  - AirBEAM
  - Mobile Device Manager

Deployment Costs
Employee

	Handhelds	Printers
Initial OS Load	60min	15min
Update time/Year	60min	15min
App Load	20min	
App Update	10min	
Time/Device/Year	150min	30min
# Devices	10	10
Hours/Year	25	5
Cost/Hour	$50	$50
Total	$1250	$250

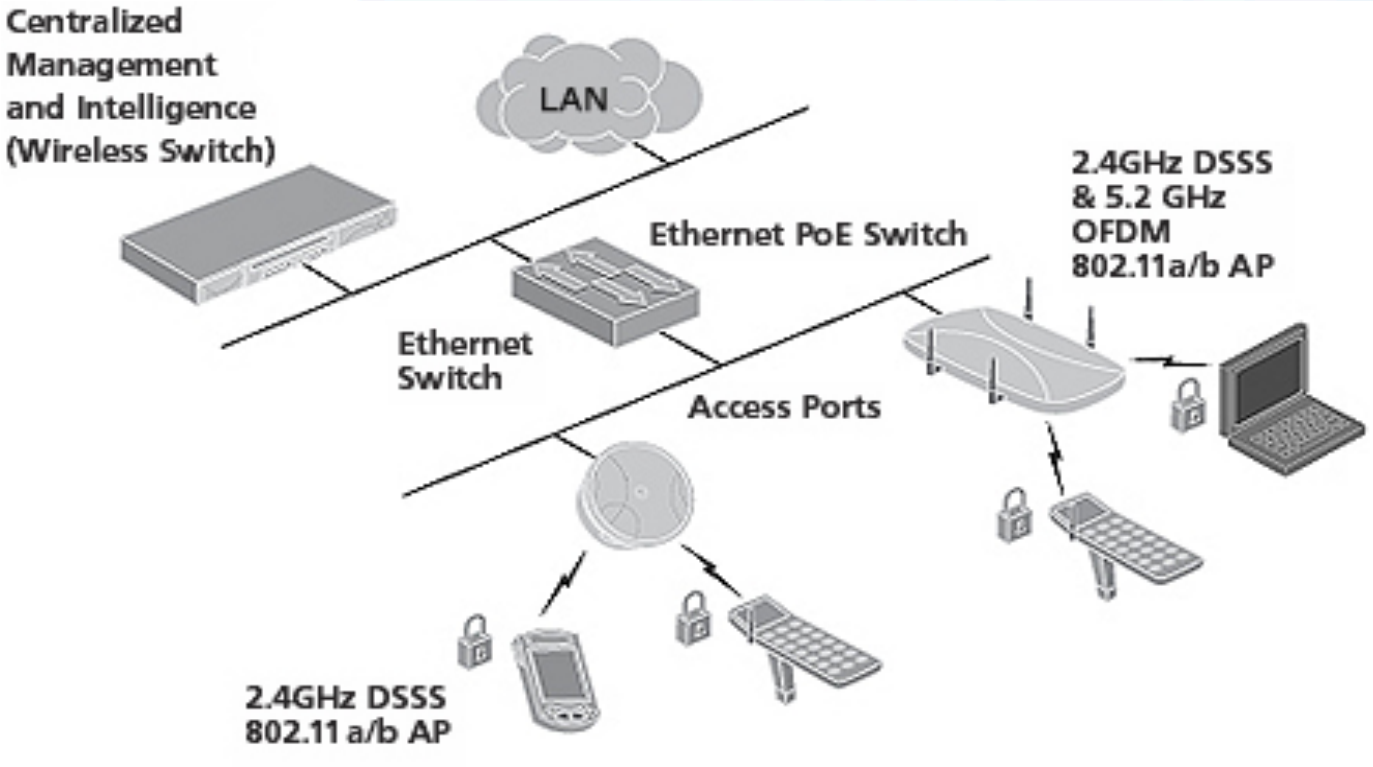
Deployment Costs
Management System

	Handhelds	Printers
Initial OS Load	60min	15min
Update time/Year	60min	15min
App Load	1min	
App Update	1min	
Time/Device/Year	122min	30min
# Devices	10	10
Hours/Year	20.33	5
Cost/Hour	$50	$50
Management Platform	$3000	
Client Licenses	$570	
Total	$5,176	$250

Wireless Access Point Management

- Thick Mode:
  - Fully independent
  - Management is done at the AP level
  - Resembles most standard home APs
- Thin Mode:
  - Light weight AP, limited number of low level functions (encryption, packet transmission, SSID announcement, etc.)
  - Centrally managed by a Wireless Switch Manager
  - Able to be placed anywhere on the network as long as they have a patch back to the Wireless Switch Manager

Wireless Access Point Management



VLAN

- Operate at Layer 2 of the OSI model, but normally configured to involve Layer 3 (IPs or Subnets)
- Logically another network, physically a switch or group of switches managed to be within the same logical network.
- VLANs can be used to control buildings, floors, groups of computers/users/resources.

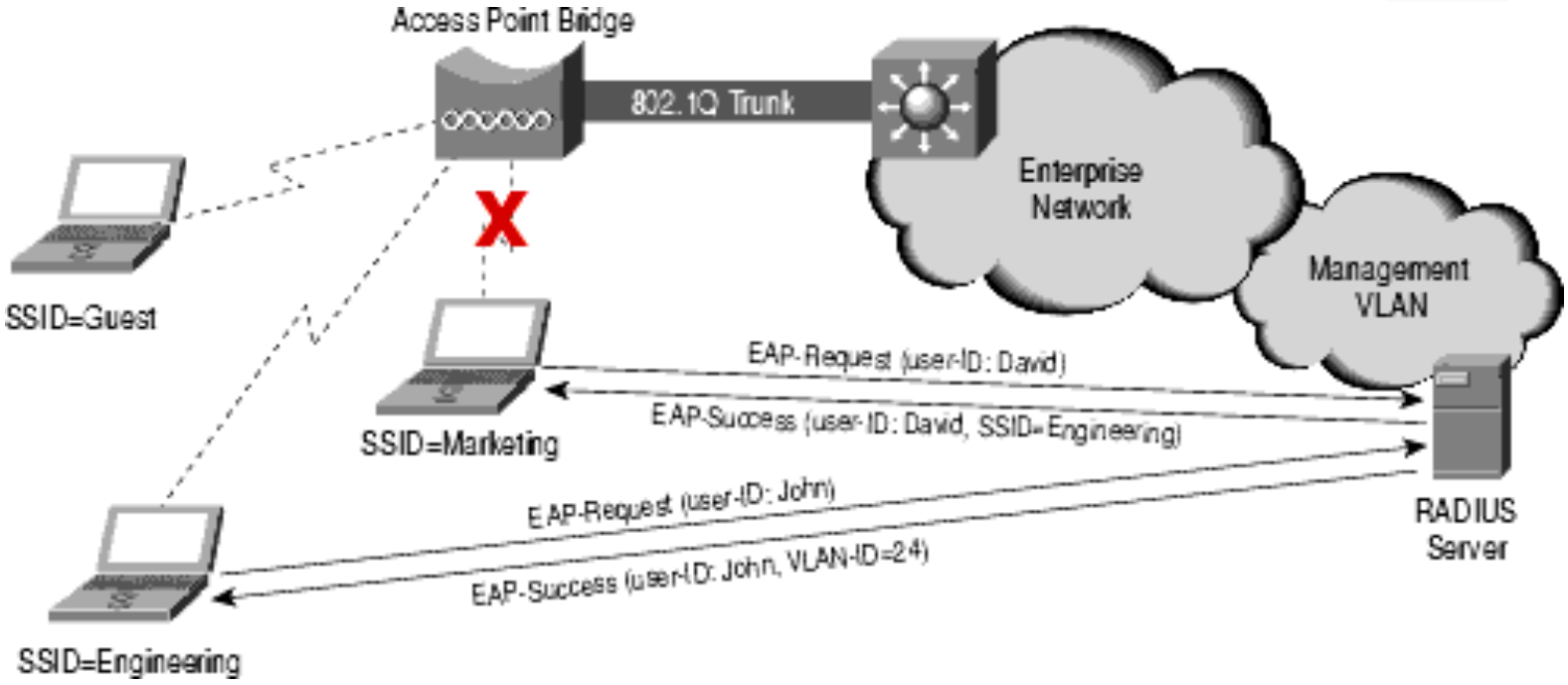
VLAN Wireless Application

- A VLAN can be associated with a specific SSID.
- Even further, specific SSID user access can be controlled by including a RADIUS server.
- Instead of using multiple APs for each SSID, 1 AP can handle multiple SSID/Networks.
- Each SSID can have different authentication/ encryption standards applied. From open/guest access to 802.1x+ dynamic WEP + TKIP/MIC.

VLAN Wireless Application

- In the following example, multiple machines are accessing different SSIDs at the same AP
- David is attempting to connect to Marketing, however, RADIUS only shows him having access to Engineering. His connection is denied.
- John is attempting to connect to Engineering. RADIUS shows John has access to Engineering and is granted access.

VLAN Wireless Application



Wireless Security Pitfalls

- No barrier to entry (no wall jack to find)
- Data is accessible to anyone within range and with a proper NIC.
- 802.11b/g fair range, relatively cheap, many devices at same frequency
  - Microwave ovens, cordless phones, security radios/monitors)
- 802.11a has a shorter range, higher cost, fewer devices at same frequency

Solutions to Pitfalls

Creating Barriers

Authentication:

- WEP
- MAC Address
- Web Authentication
- 802.1x+RADIUS (WPA & WPA2)

WEP

- Wired Equivalent Privacy
- Generally looked at as “better than nothing”
- 64 and 128 bit, however, 24 bits are used by the Initialization Vector (40 and 104)
- Limited number of IVs leads to repetition of IVs, thus allowing attackers to compare and extrapolated the key.
- Can you remember 26 character Hex key? Leads to users printing it “temporarily”

MAC Filtering

Media Access Control Address

- Mostly unique address assigned to each NIC.
- Normally the very first thing found by an attacker.
- Most operating systems/NIC drivers have the ability to “spoof” a MAC address built in.

Web Authentication

- Typically best for guest access situations
- Unless another encryption method is being used, there is no data protection.
- Typically the website uses SSL and the username/password is encrypted.

802.1x

- Able to be used on wired and wireless installations
- Uses EAP, Extensible Authentication Protocol
- Also referred to as “Port Based Authentication”
- Each step is encrypted and secured to ensure beginning to end security
- Offers not only secure authentication but also secure data transfer

RADIUS

- Remote Authentication Dial-In User Service
- User information can be verified by querying a DC (ADS domain controller), LDAP, SQL, Kerberos, etc.
- Different options for a RADIUS server:
  - Microsoft Internet Authentication Service (IAS)
  - FreeRadius
  - Cisco Access Control Server (ACS)
  - OpenRadius

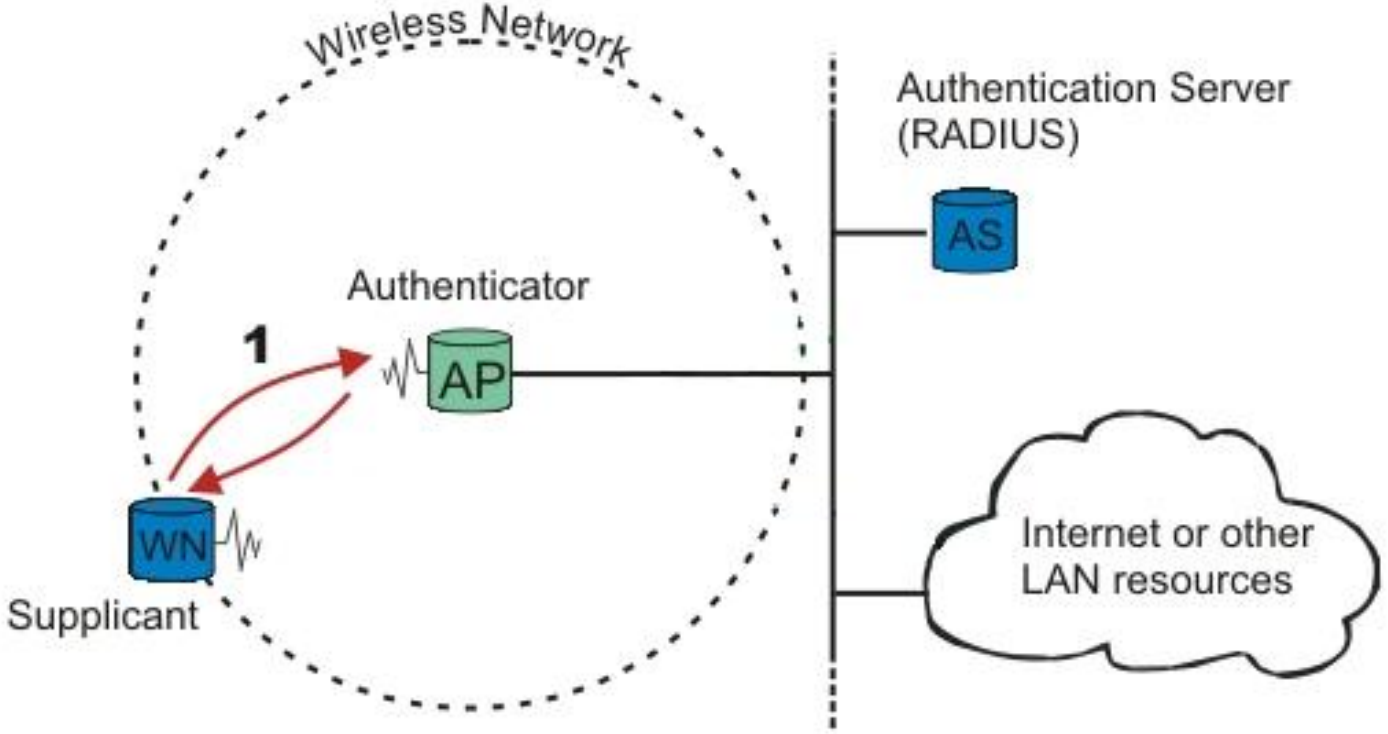
802.1x

Step 1

- Authenticator sends an “ EAP-Request/Identity”
- Supplicant sends an “EAP-Response/Identity”, that is automatically forwarded on to the Authentication Server (RADIUS)
- Authentication Server sends back a challenge to the Authenticator. The Authenticator then unpacks this from IP, repackages it to EAPOL and sends it to the supplicant.

802.1x Authentication

Process



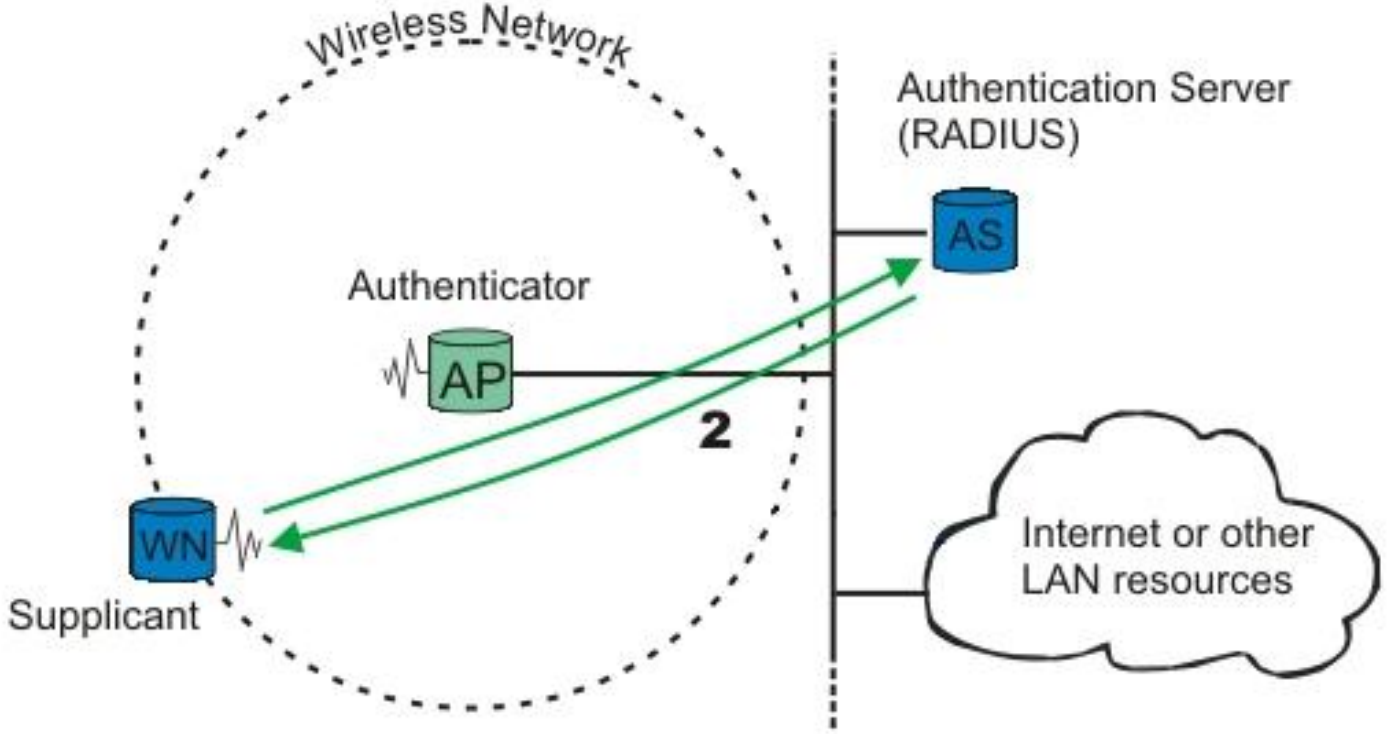
802.1x

Step 2

- Supplicant responds to the challenge via the Authenticator and passes the response onto the Authentication Server.
- If the Supplicant provides proper identity, the authentication server responds with a success message to the Supplicant.
- If the Supplicant does not provide proper identity, the Authentication Server responds with a reject message and the Supplicant is not allowed access.

802.1x Authentication

Process



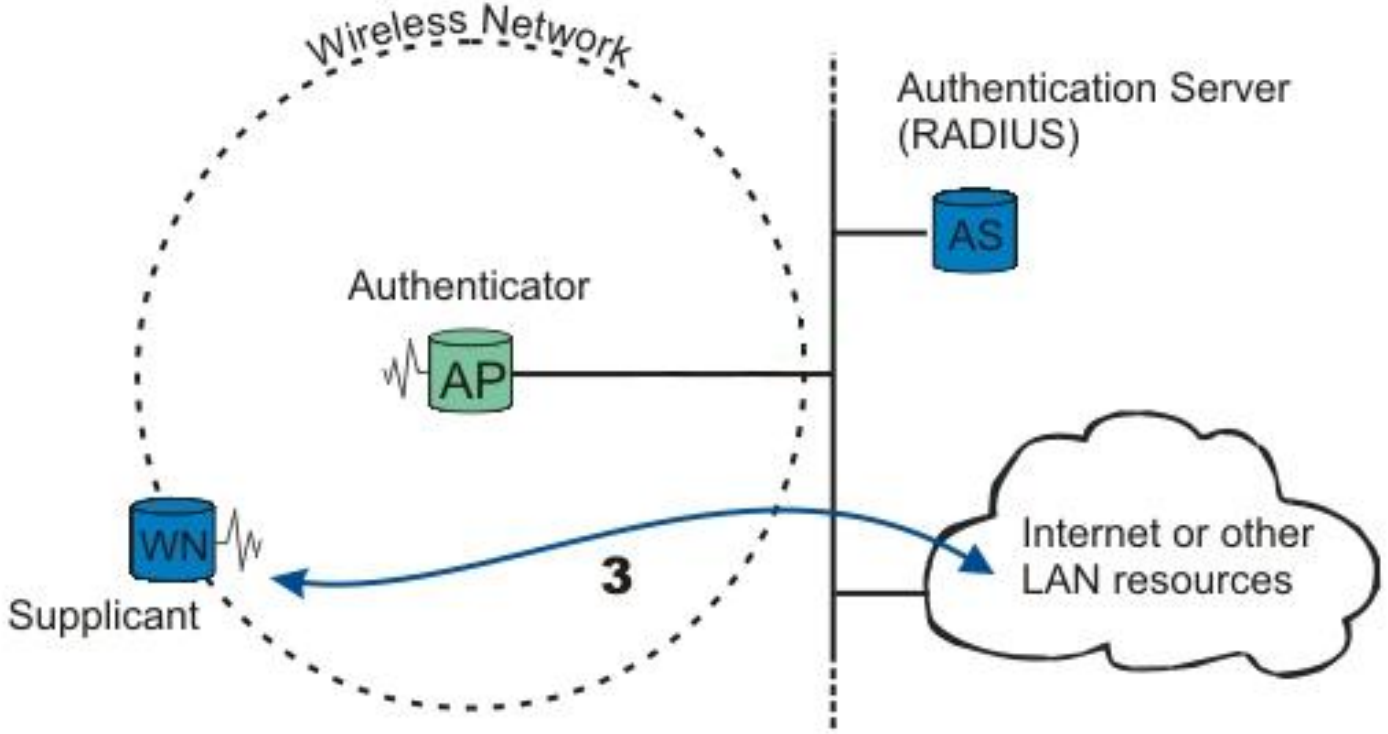
802.1x

Step 3

- Authenticator not allows the Supplicant access to the Internet or other resources
- At this point, the Authentication Server sends a Master Key and series of handshakes work to build the shared keys between the Supplicant and the Authenticator.

802.1x Authentication

Process



802.1x Support

- Windows XP/Vista/7: Built in and only limited by NIC capabilities
- MAC OS X 10.3 began supporting natively.
- Most, if not all, Linux distributions have 802.1x support, only limited by NIC capabilities

Device Wireless Capability Survey

	EAP Type				Encryption			Client Type(s)
Device	TLS	TTLS	PEAP	LEAP	WEP	WPA	WPA2	
Intermec CN2B	X	X	X	X	X	X	X	Intermec
Laptops	X		X		X	X	X	Windows
Laptops	X	X	X	X	X	X	X	Aegis
Palm Tungsten C				X	X			Aegis
Symbol PPT8846	X	X	X	X	X	X	X	Aegis
Symbol MC70	X	X	X	X	X	X	X	Aegis
Zebra QL220 Symbol 802.11b Radio				X	X	X		Zebra
Zebra QL220Plus Zebra or Symbol 802.11b Radio	X	X	X	X	X	X		Zebra
Zebra QL220Plus Zebra 802.11g Radio	X	X	X	X	X	X	X	Zebra

I Can Help!

Steve Walker

Director Application Development

Iatric Systems, Inc.

Phone/Fax: (978) 805-4180

E-mail: Steve.Walker@Iatric.com

Attend our free monthly webcasts.

Subscribe to our newsletter.

Mobile Madness

Thank you for attending!