IATRIC systems

Mobile Madness

Educational Session

Steve Walker

Seminar Overview

- Wireless Basic Overview
- Site Surveys and Physical Challenges
- Wireless Pitfalls
- Authentication and Security
- Access Point Management
- VLANs
- Network Topology and Roaming Devices
- Application & Handheld Deployment
- Bandwidth Considerations
- Stories From The Road

Wireless Networking

Can you hear me now?

- **Most common is 802.11b/g (2.4Ghz)**
- **Less common is 802.11a (5.8Ghz)**
- **11/54 Megabits in theory**
- **EMI Sensitive (Very)**
- **Usually implemented with an “Access Point”**
- **Very insecure “out of the box”**

Wireless Survey

Save yourself some pain!

- **Initial Survey**
  - **Establish location of AP's**
  - **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**

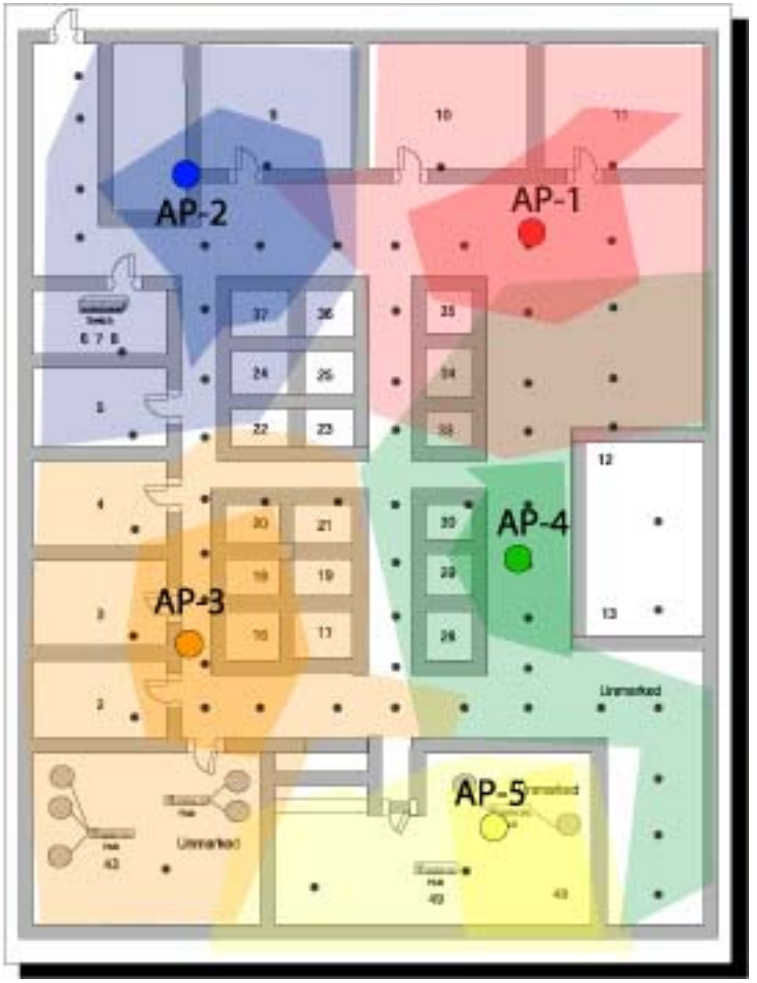
Wireless Survey

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 the window is to the outside**
- **Doors**
  - **Solid Core/Fire doors**

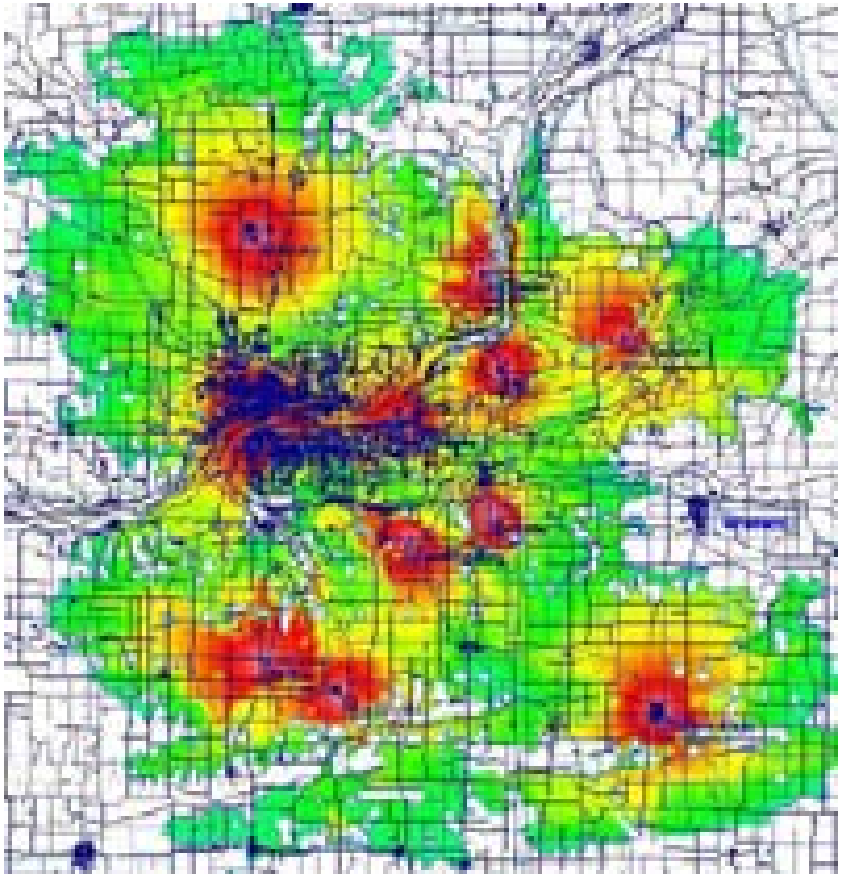
Wireless Survey (continued)

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



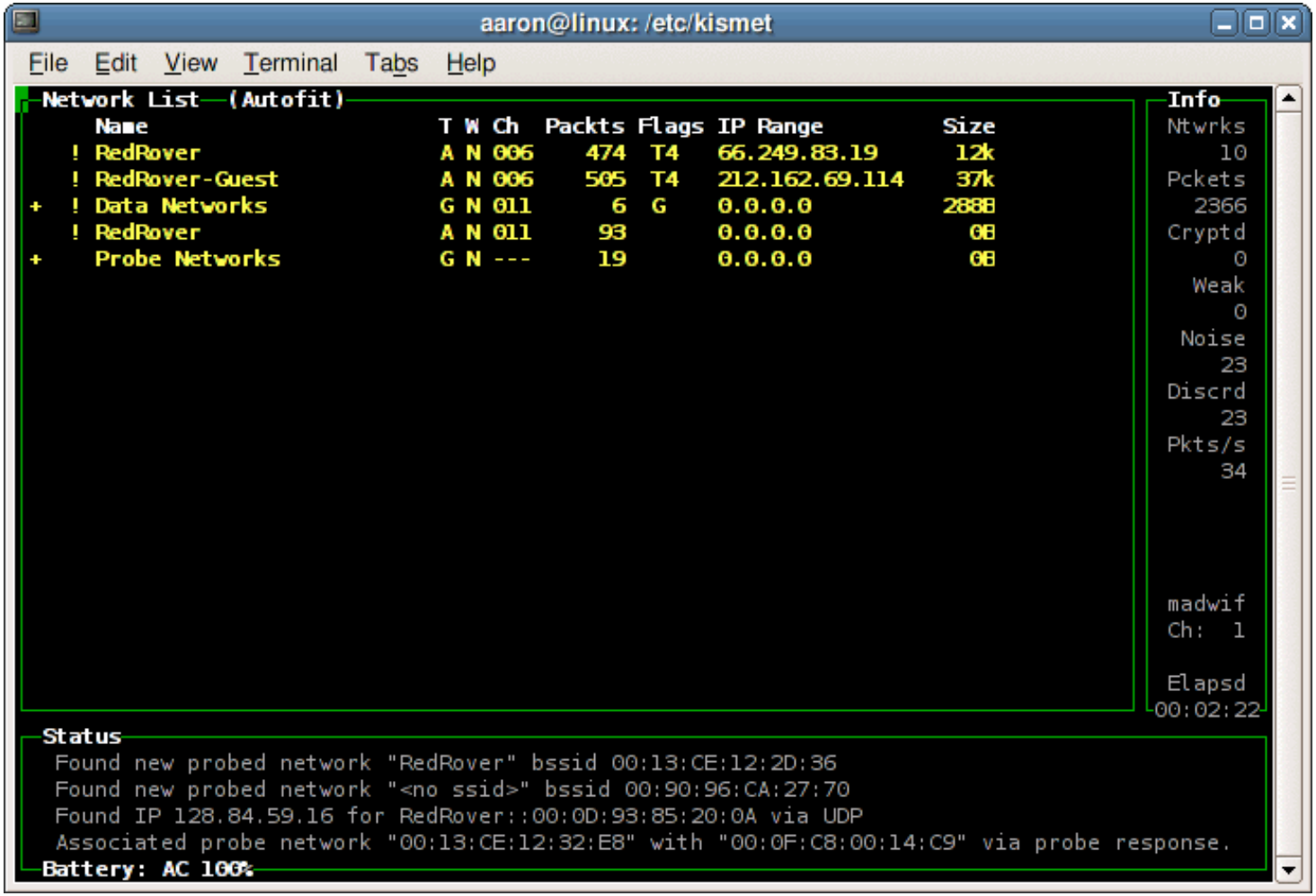
Wireless Survey (continued)

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



IATRIC systems

Kismet



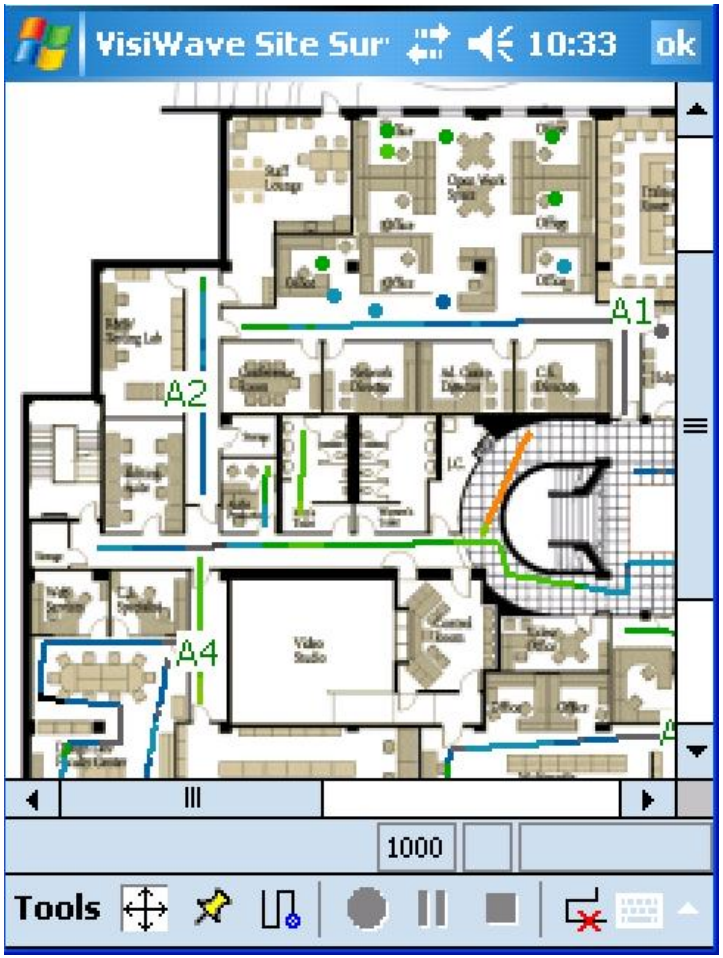
Wireless Survey (continued)

Software

	AirMagnet (Handheld Analyzer)	VisiWave	Ministumbler	Ekahau	WiFiFoFum
Est. Price	$2250	$550	Free	$2500	Free
OS Compatibility	Pocket PC 2003/Mobile 5.0	XP, Mobile 5.0, Pocket PC 2002/3/5	PocketPC 2002/3, Mobile 2003	2000, XP, Tablet PC	PocketPC 2003/Mobile 5.0 & 6.0
802.11 compatibility	b/g	a/b/g/n	a/b/g	a/b/g/n	b/g
Spectrum analysis	Optional	Optional	None	Optional	None
Site Map	bmp, jpg, gif	gif, jpg, png, bmp, tiff	None	bmp, jpg, png	None
Device Compatibility	Limited for Handhelds	Laptops, PDA using Pocket PC	Handhelds	Laptops, Tablets	Handhelds

IATRIC systems

VisiWave



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 shorter range, higher cost, fewer devices at same frequency

Solutions to Pitfalls

Creating barriers

- **Authentication**
  - **WEP**
  - **MAC Address**
  - **Web Authentication**
  - **802.1x + RADIUS**

WEP

- Wired Equivalent Privacy
- Generally looked at as “better than nothing”.
- 64 & 128 bit, however 24 bits are used by the Initialization Vector (40 & 104).
- Limited number of IV’s leads to repetition of IV’s, thus allowing attackers to compare and extrapolate 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.

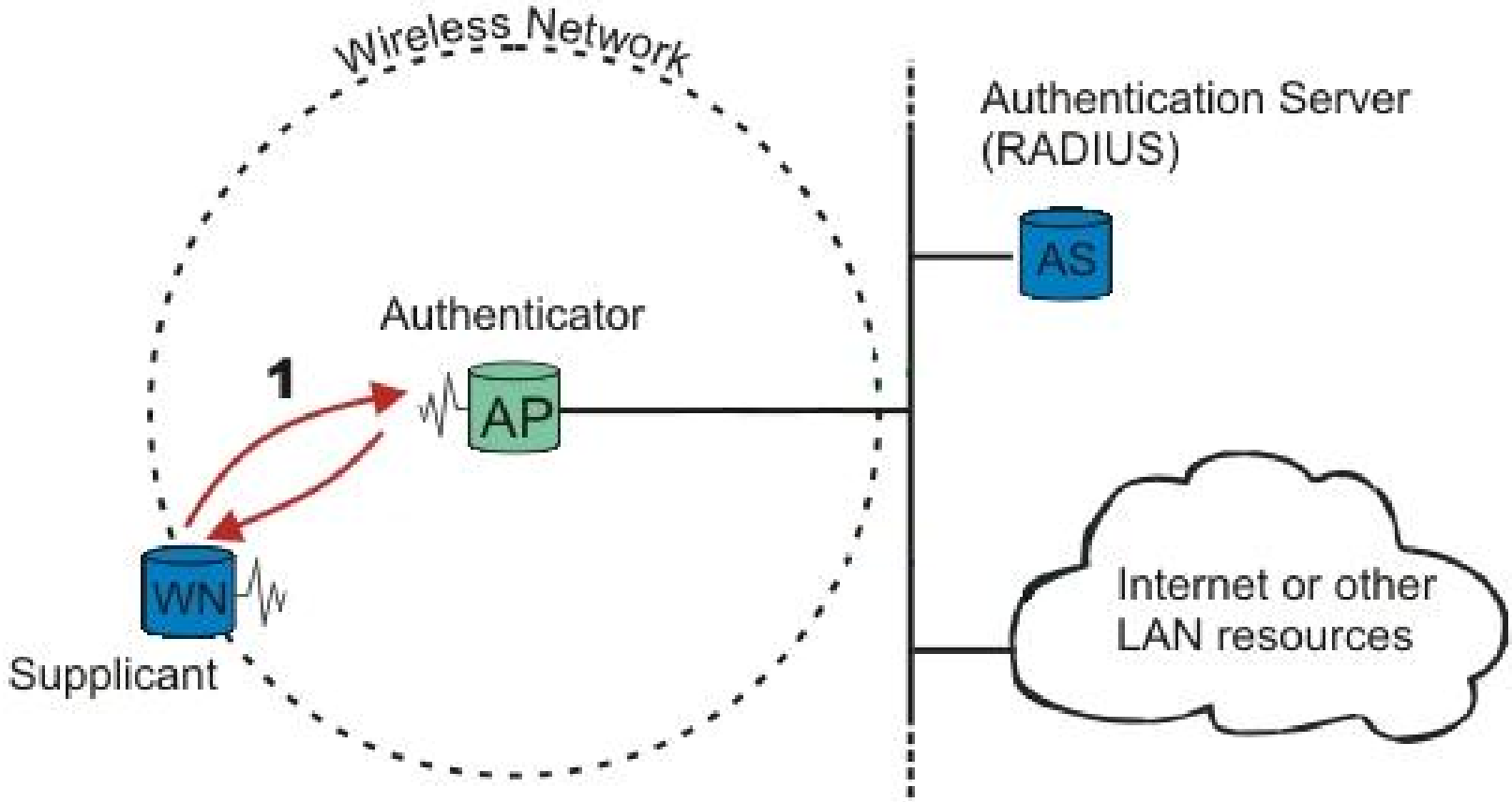
RADIUS

- 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, who then unpacks this from IP and repackages it into EAPOL and sends it to the supplicant.**

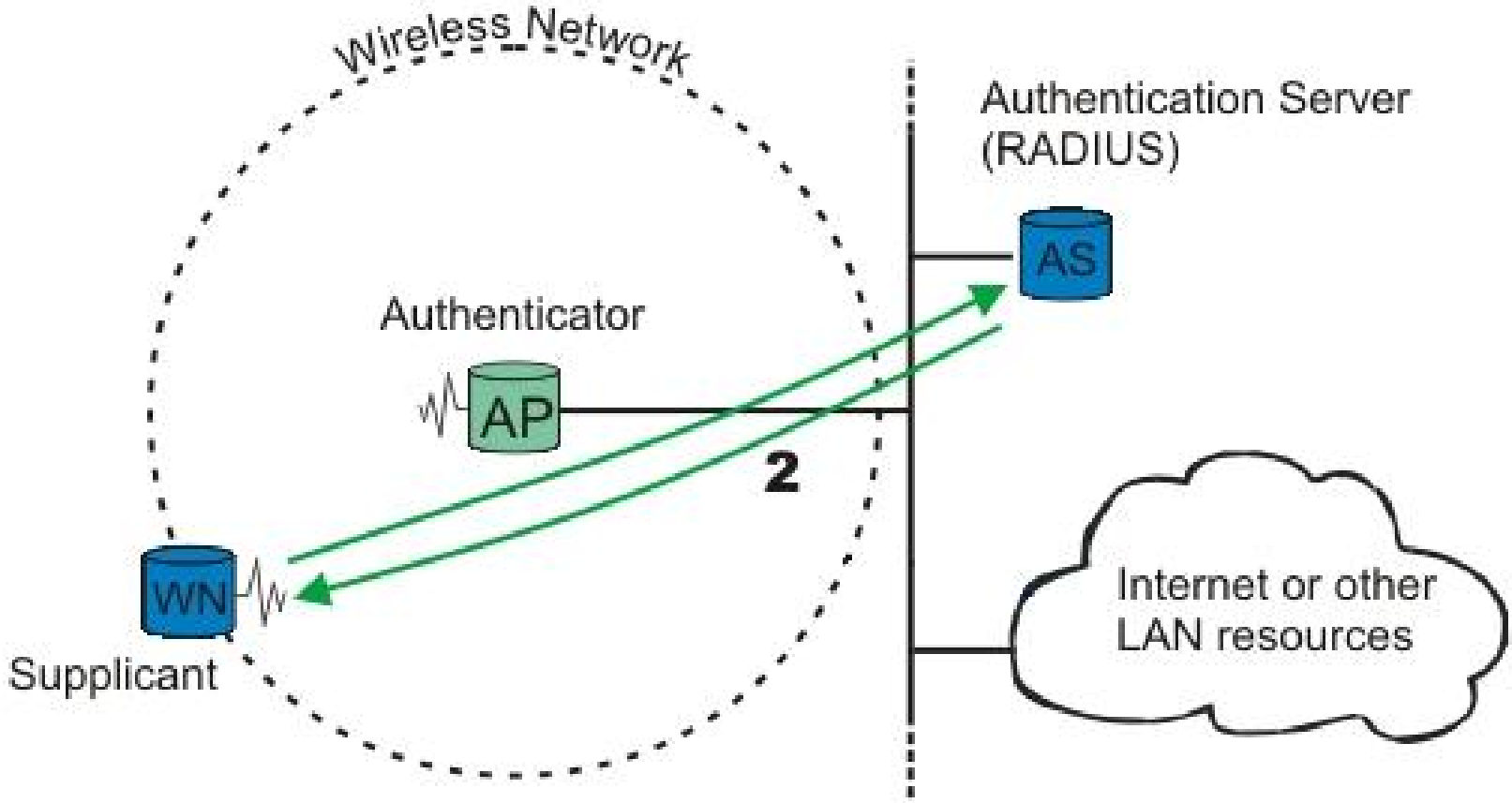
802.1x Authentication Process



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.

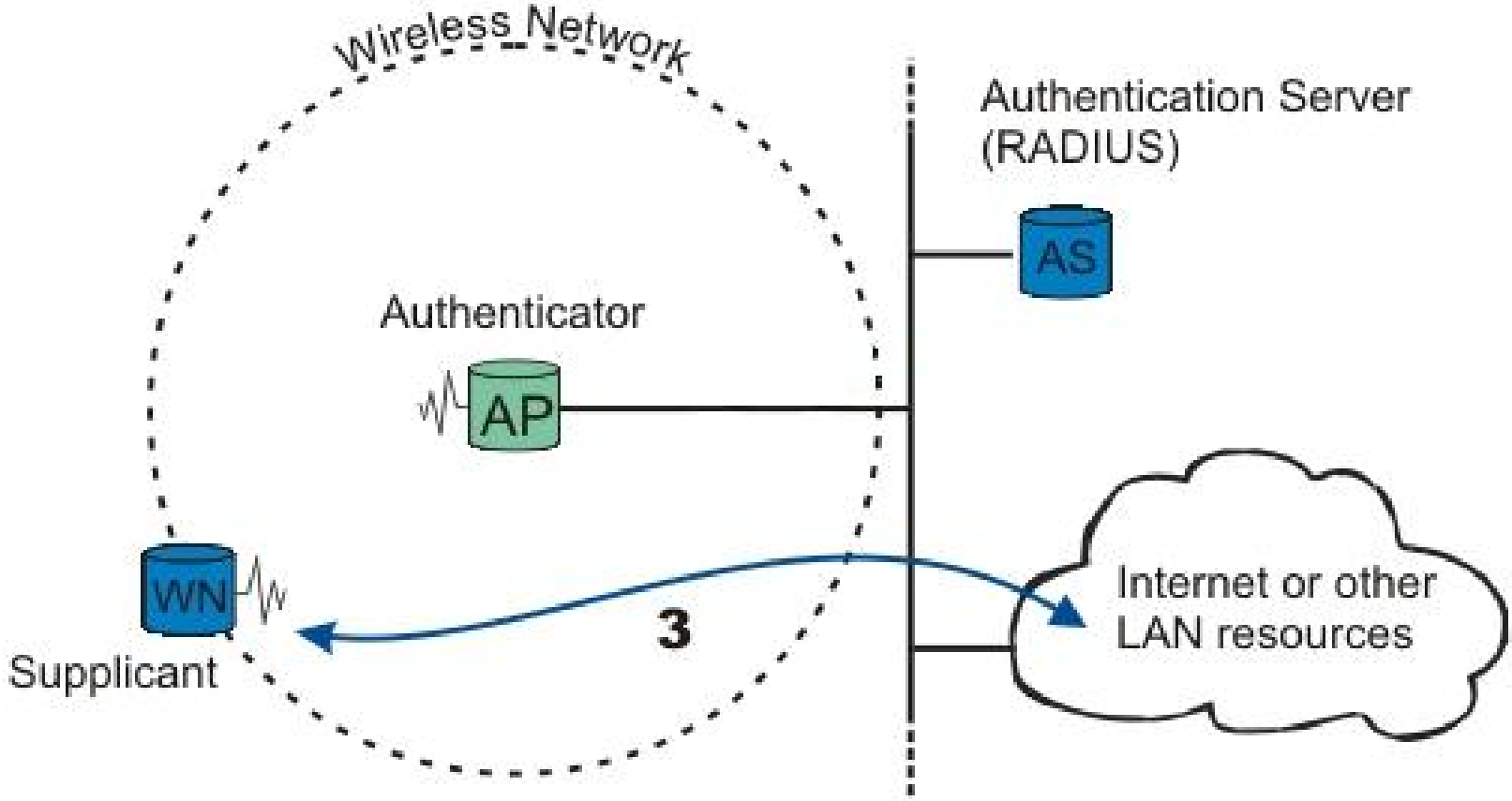
802.1x Authentication Process



802.1x
Step 3

- **Authenticator now 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



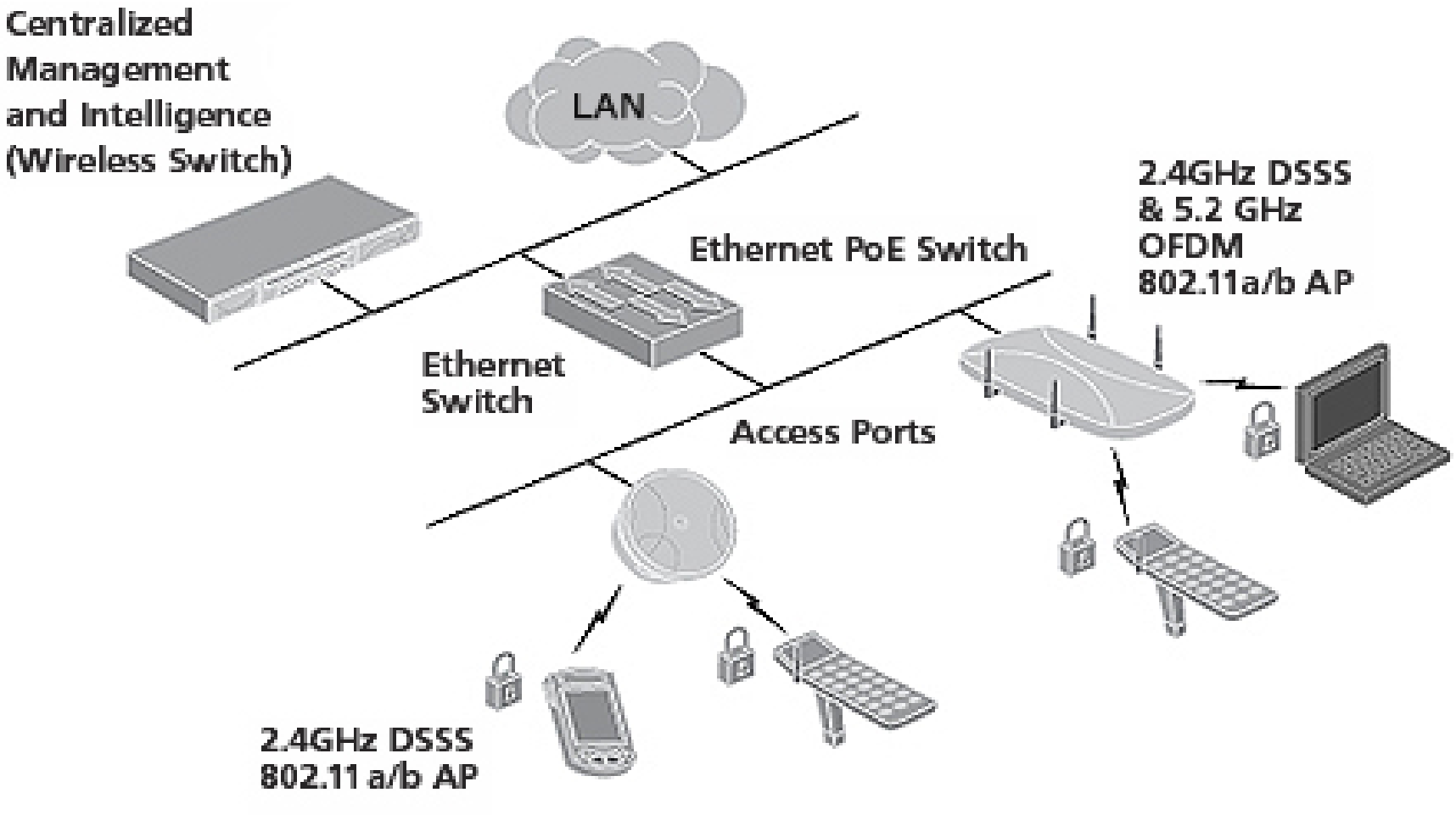
802.1x Support

- **Windows XP – 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.**

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



IATRIC systems

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.

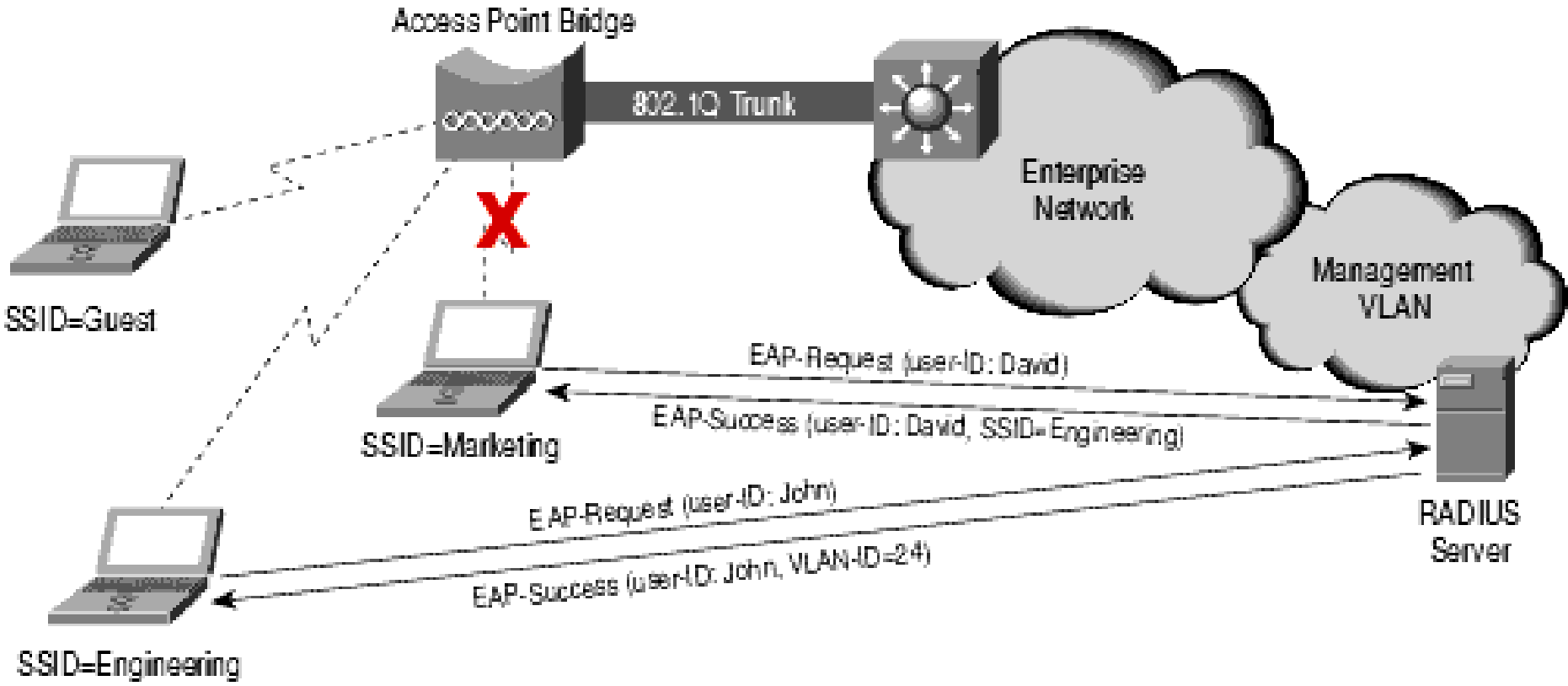
VLAN Wireless Application

- **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 AP's 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

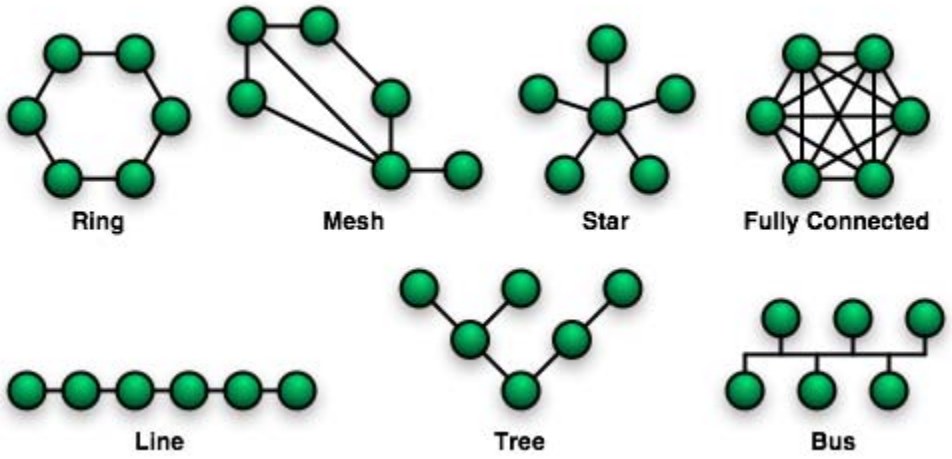


Device Wireless Capability Survey

	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

Network Topology

- **Standard network topologies**
  - **Ring**
  - **Mesh (partial & full)**
  - **Star**
  - **Bus**
  - **Tree**
  - **Line**

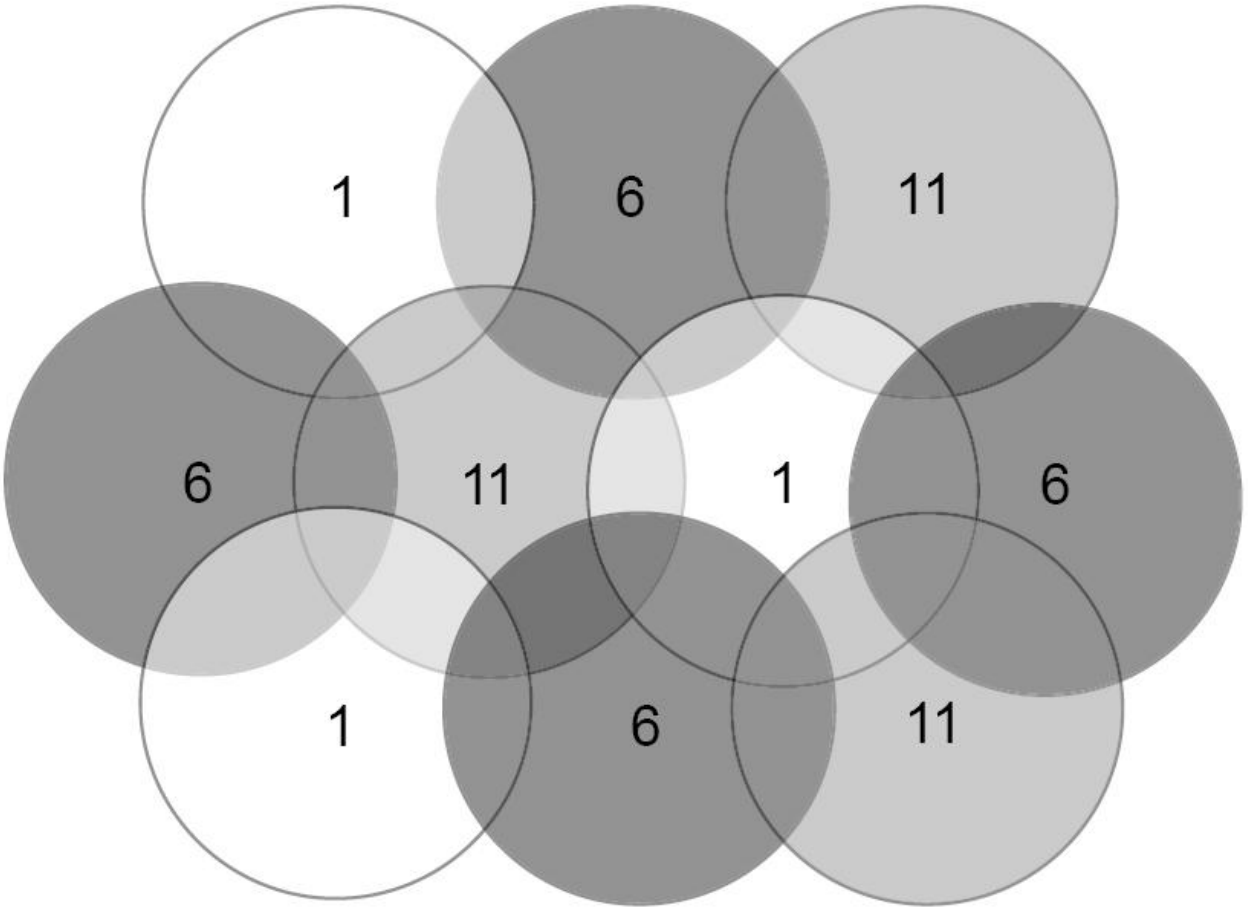


Network Topology

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

Network Topology

Channels



Device Roaming

- **Disassociate**
  - **Client drops it's connection from old AP**
- **Scan**
  - **Client scans for a 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**

Handheld Deployment

- AirBEAM
- Wavelink Avalance MC

- Features:
  - Ability to configure devices without prestaging
  - Updating firmware, drivers, and software remotely
  - Inventory and tracking

Application Deployment

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

Stories From the Road

Questions?

Steve Walker
Director Application Development
Iatric Systems, Inc.

Phone/Fax: (978) 805-4180
Email: Steve.Walker@Iatric.com

Attend our free monthly webcasts.
Subscribe to our newsletter.

Mobile Madness

Educational Session

For More Information

Please Contact your **Iatric Account Manager**
or send an email to **info@iatric.com**

Thank you for attending!