

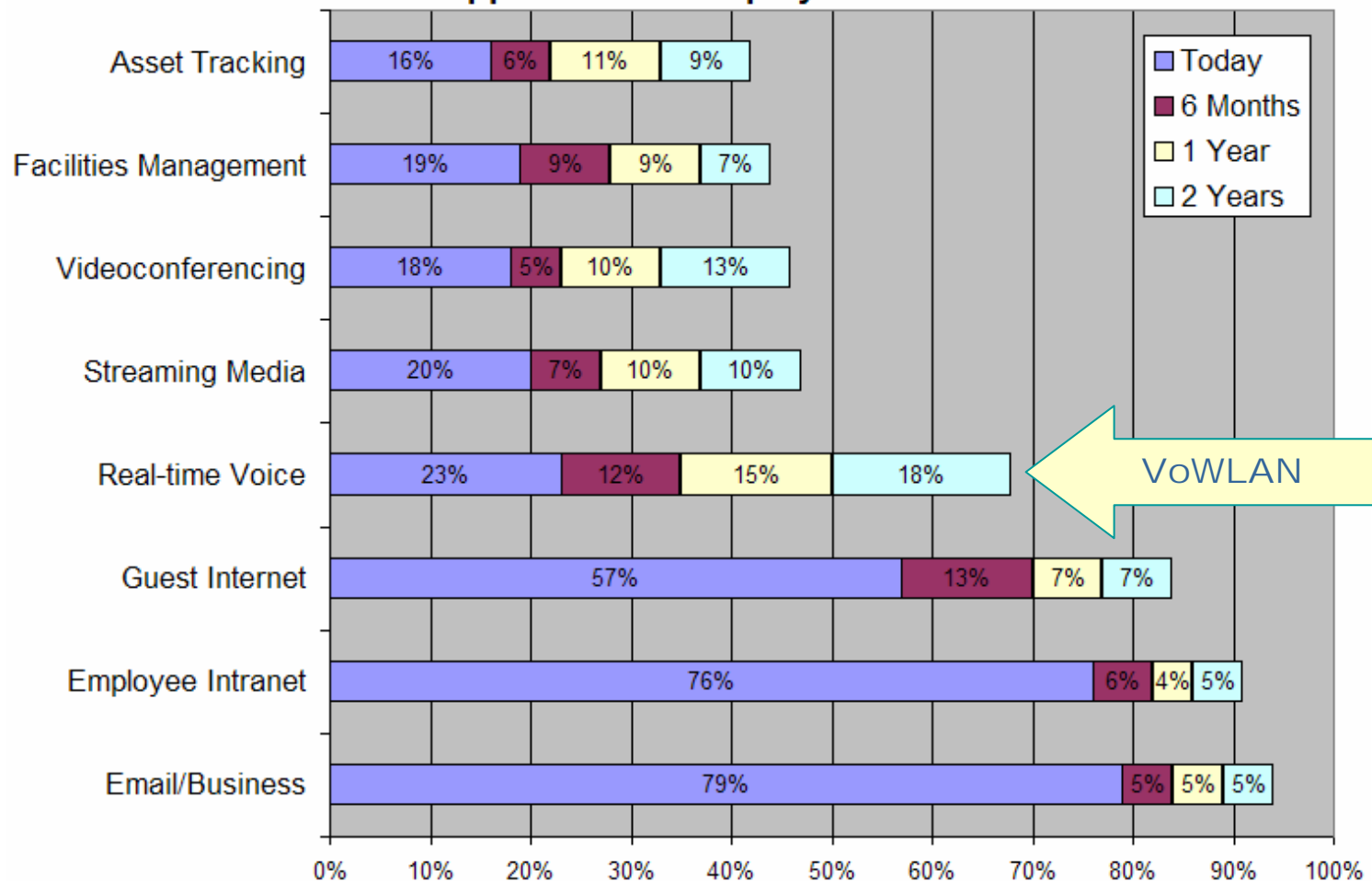


Wireless LAN Security

Lisa Phifer
Vice President
Core Competence Inc.
www.corecom.com

Voice over WLAN: poised for growth

2006 WLAN State of the Market Report
WLAN Applications -- Deployment Timeframe



WLAN security is a key enabler

- ◆ Pervasive WLAN coverage is required to support voice users as they roam throughout the workplace
 - This creates new vectors through which to access or attack voice services – *and the corporate network*
- ◆ 802.11 security has improved, but concerns remain
 - What major threats face today's WLANs?
 - How can we mitigate them?

Most Challenging Factors in Justifying or Deploying Wireless	
Security Concerns	70%
Managing & Troubleshooting WLAN	38%
Interference & Performance Problems	37%
Lack of RF Expertise	20%
Fast user roaming across subnets	20%

Source: 2006 WLAN State of the Market Report

802.11 Data Attacks

- ◆ Anything sent as cleartext over wireless is inherently vulnerable to eavesdropping, forgery, replay
 - Example: Voice over Misconfigured IP Telephony (vomit) captures/converts RTP packets into .wav file

- ◆ Devices that are especially vulnerable
 - Printers, PoS terminals, bar code scanners, and small/embedded devices that lack encryption
 - Legacy 802.11b devices that are limited to easily-cracked Wired Equivalent Privacy (WEP)
 - Devices used in open hotspots, including VoIP handsets like Vonage WiFi UTStarcom F1000

- ◆ New standards mitigate 802.11 Data attacks
 - But Management frames can still be forged...



Denial of Service (DoS) Attacks

- ◆ Wired DoS attacks experienced by 1 in 3 companies
 - Absence of physical containment and competition for unlicensed spectrum make WLANs more vulnerable

- ◆ Many WLAN DoS attacks use forged or replayed 802.11 Management or Control frames
 - Break connections using spoofed Disassociate, Deauthenticate, 802.1X Logoff messages
 - Exhaust WLAN resources using spoofed Associate, Authenticate, 802.1X Start messages
 - Flood the air with phony WLAN Beacons, Probes
 - Hog the channel with Clear-To-Send frames

- ◆ Or good old fashioned RF interference from other WLANs, microwave ovens, Bluetooth devices



Rogue Access Points

- ◆ For most companies, a top security concern about adding wireless is enabling unauthorized access to
 - Wired corporate network
 - Business systems and services
 - Private data stored therein
- ◆ Unauthorized “rogue” wireless Access Points (APs) can open long-term, unprotected backdoors
 - Employee-installed or malicious attacker APs
 - Can be small: Thumb-Drive Soft APs
 - Can be “invisible”: Unusual RF channels, bands
- ◆ For example: 2005 CERT Survey
 - 21% of company networks breached by rogue APs
 - 72% of those breaches involved consumer APs



- ◆ Unauthorized WLAN clients are extremely common
 - Most sites visited daily by unknown devices carried by neighbors, visitors, delivery trucks, employees...
 - Even at “no Wi-Fi” facilities
- ◆ Differentiating between known-trusted, untrusted-harmless, and malicious devices is critical
 - Doing so reliably, in real-time, is challenging
- ◆ Attackers use tricks to extend reach
 - 802.11 Guinness Record = 192 miles!
 - Higher Tx power, Rx sensitivity, Antennas
- ◆ And elude detection
 - MAC address spoofing, Raw packet injection
 - Movement and short-duration attacks



Misconfigured Access Points

- ◆ Defined WLAN policies must be enforced to
 - Protect data (and voice) sent over the air
 - Prevent unauthorized network access
- ◆ According to Gartner, misconfiguration will account for 70% of successful WLAN attacks thru 2009
 - APs with default names, disabled security settings
 - APs that exhibit unusual / known-risky behavior
 - Is it a rogue AP? Is it a malfunctioning AP?
- ◆ Caused by operator error or AP bugs, for example:



WVE-2005-0062	Linksys WRT54G 'restore.cgi' Arbitrary Config Upload
WVE-2005-0064	Authentication Vulnerability in Belkin Wireless Routers
WVE-2006-0055	Cisco AP Web Interface Authentication Bypass

Source: www.wve.org (Wireless Vulnerabilities and Exposures)

Misbehaving Clients

- ◆ WLAN clients are notoriously hard to control
 - 87% associate accidentally to unknown APs
 - Others do so intentionally to bypass policies that ban Peer-to-Peer apps or “no Wi-Fi”
- ◆ 2 out of 3 clients try Ad Hoc connections
 - Clients previously connected to AP may automatically reconnect to Ad Hoc device with same name (SSID)
- ◆ Misbehavior places client and company at risk
 - Eavesdropping, exposed fileshares, viruses/worms
 - Infected client can compromise corporate network
 - 37% of clients have network bridging enabled, creating wireless backdoor onto Ethernet LAN



802.11 Endpoint Device Attacks

- ◆ Client device vulnerabilities are new battleground
 - Hotspots and Home WLANs will be the major access routes for damaging attacks (Gartner)
 - Many 802.11 client devices have bugs that can be exploited to compromise the endpoint, for example:



WVE-2006-0062	Centrino Driver Malformed Frame Privilege Escalation
WVE-2006-0060	Mac OS X Driver Malformed Frame Remote Code Execution
WVE-2006-0071	Broadcom Driver Probe Response SSID Overflow
WVE-2006-0025	Zyxel P2000W 802.11 VOIP Phone Undocumented Open Port
WVE-2006-0009	Open UDP Debug Port in Cisco 7920 Wireless IP Phone
WVE-2006-0063	FiWin SS28S VoIP Phone Unauthenticated Access
WVE-2006-0010	Hitachi IP5000 802.11 VOIP Phone Hard-coded Password

Source: www.wve.org (Wireless Vulnerabilities and Exposures)

WLAN Man in the Middle (MitM) Attacks

- ◆ MitM attacks are just easier on a WLAN
 - Public venues, 802.11 client promiscuity
 - No physical facility / LAN port access required

- ◆ WLAN MitM starts with a Honeypot or Evil Twin AP
 - An attacker's AP that mimics authorized AP
 - Nearby clients lured into connecting to Honeypot using higher Tx power, forced disassociates

- ◆ Platform for launching higher-layer MitM attacks
 - Hotspot MitM attacks: phony hotspot login portals, URL redirection, SSL/SSH tunnel interception
 - VoWLAN MitM attacks: VoIP server impersonation, call redirection, call hijacking

- ◆ Fortunately, many WLAN threats can be addressed
 - Identify threats most important to your business
 - Adopt a policy that meets *business needs* while *reducing business risks* to acceptable level

- ◆ Implement policy by complementing existing network security with new measures that audit and control
 - Wireless Access to your Network
 - Wireless Clients used by employees
 - Wireless Airspace inside your buildings

- ◆ What standards and technologies are relevant?
 - And how do they complicate the ability to deliver acceptable-quality voice over your WLAN?

Wired Equivalent Privacy (WEP)

- ◆ Defined by the original 802.11 standard
 - Supported by every Wi-Fi certified product
 - For a list, visit <http://www.wi-fi.org>
- ◆ WEP can
 - Encrypt data frames using RC4 and static keys
 - Authenticate everyone using 1 of 4 Shared Keys
 - Stop those without key from connecting to WLAN or eavesdropping on over-the-air data/voice
- ◆ WEP cannot
 - Identify WHO is using your WLAN
 - Stop employees from hearing each other
 - Stop attackers from “cracking” WEP keys
 - Help you distribute or update those keys



Wi-Fi Protected Access (WPA)

- ◆ Defined by October 2002 draft of 802.11i
 - Required in Wi-Fi products since Sept 2003
 - Over 1600 WPA products certified to date
- ◆ WPA encrypts data using RC4 and per-packet keys
 - Stops WEP key cracking
 - ◆ Temporal Key Integrity Protocol (TKIP)
 - Detects data frame forgery
 - ◆ Message Integrity Check (MIC)
 - Prevents data frame replay
 - ◆ Message sequencing
- ◆ Two flavors: WPA-Personal and WPA-Enterprise



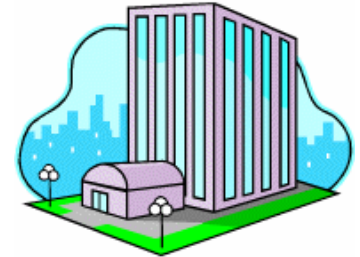
WPA-Personal uses PSK

- ◆ For home and small office WLANs
 - Where everyone trusts everyone else
 - Where IT staff / infrastructure is absent
- ◆ WPA-Personal can
 - Authenticate everyone using PreShared Key (PSK)
 - Stop those without PSK from connecting to WLAN or eavesdropping on over-the-air data/voice
 - PSK is mixed to create per-packet TKIP keys
- ◆ WPA-Personal still cannot
 - Tell you WHO is using your WLAN
 - Stop attackers from guessing short, simple PSKs
 - To reduce risk, use random strings > 20 characters

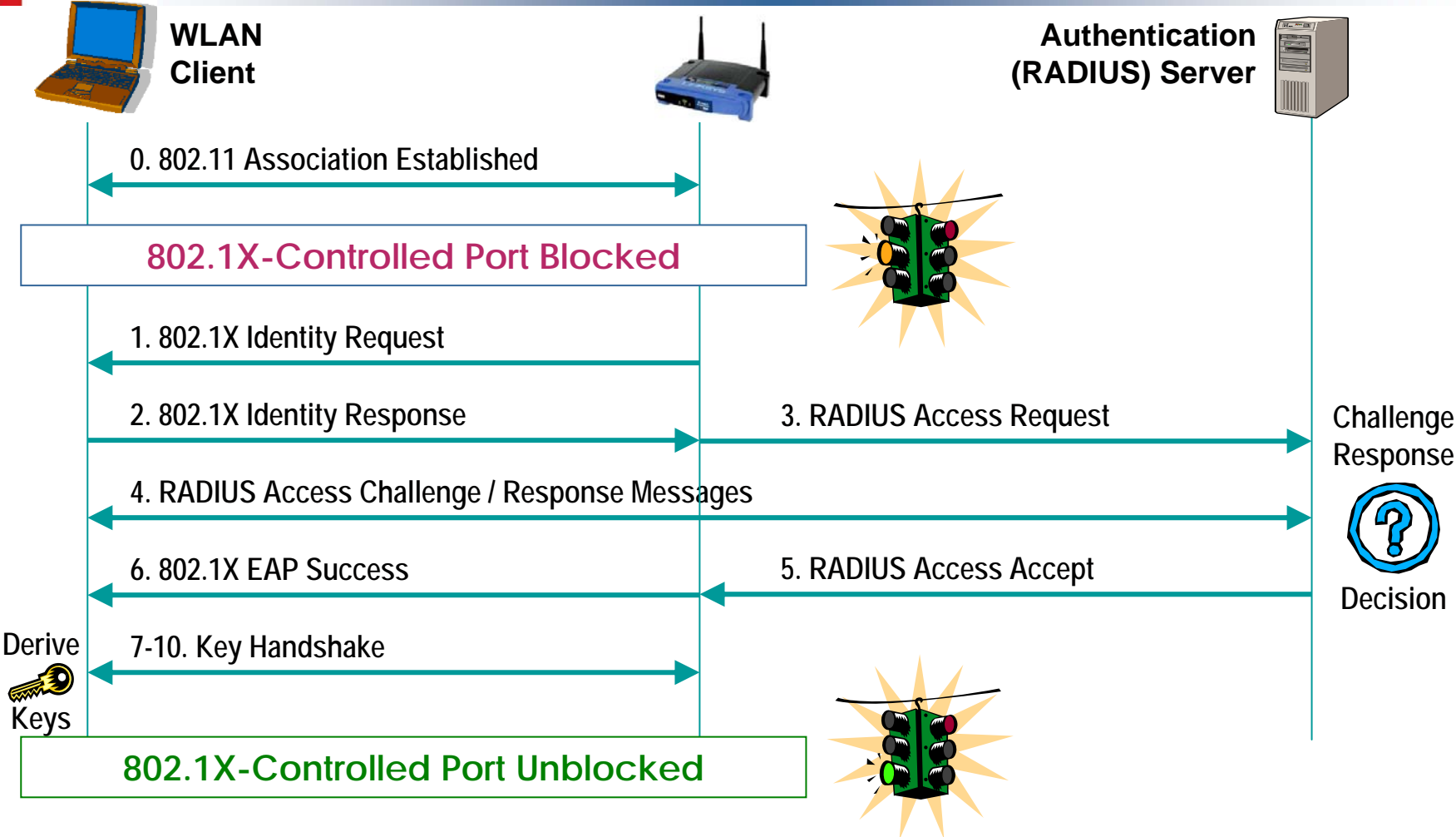


WPA-Enterprise uses 802.1X

- ◆ For most business WLANs
 - Where granular security is required
 - Level of trust and access rights vary
 - IT expertise & infrastructure available
- ◆ WPA-Enterprise can
 - Control access to wired or wireless LAN “ports”
 - Enable individual user authentication
 - Deliver fresh master keys to individual users so that TKIP can stop *everyone* else from eavesdropping
- ◆ WPA-Enterprise still cannot
 - Minimize bandwidth / CPU overhead
 - Satisfy US government strong crypto requirements



802.1X Port Access Control



Authorization determined by Server

- ◆ Server accepts or rejects “port” access
 - Central control over who enters network from AP
 - Supports individual user/device authentication without relying on easily-spoofed MAC address
 - Tracks usage for accounting, auditing purposes

- ◆ Server response can also limit user/device access
 - WLAN session timeouts
 - Permitted SSIDs (WLAN names)
 - Virtual LAN (VLAN) tags to segregate traffic

- ◆ Different users/devices can be granted different access, based on authenticated identity and defined policies

Supports many authentication methods

- ◆ 802.1X conveys Extensible Authentication Protocol (EAP) messages between Server and Client
 - Over 50 EAP Types have already been defined

- ◆ Some common EAP Types
 - EAP-TLS: Transport Layer Security
 - EAP-TTLS: Tunneled Transport Layer Security
 - PEAP: Protected EAP (versions 0 and 1)
 - LEAP: Lightweight EAP (Cisco proprietary)
 - EAP-SIM: Subscriber Identity Module
 - See <http://www.iana.org/assignments/eap-numbers>

- ◆ Considerations: security properties, credential types, performance, administrative effort, device support, vendor interoperability, target environment

- ◆ RSN is defined by final 802.11i standard
 - WPA2 is certification program for 802.11i
 - Required for all new Wi-Fi products
 - Over 700 WPA2 products certified to date

- ◆ WPA2 / RSN adds
 - Advanced Encryption Standard (AES) and Counter Mode CBC-MAC Protocol (CCMP)
 - ◆ Provides faster, robust data frame encryption
 - ◆ Better protection against data forgery and replay
 - Supports both Infrastructure & Ad Hoc WLANs
 - Key Caching / Pre-Authentication Options

- ◆ Two flavors: WPA2-Personal and Enterprise



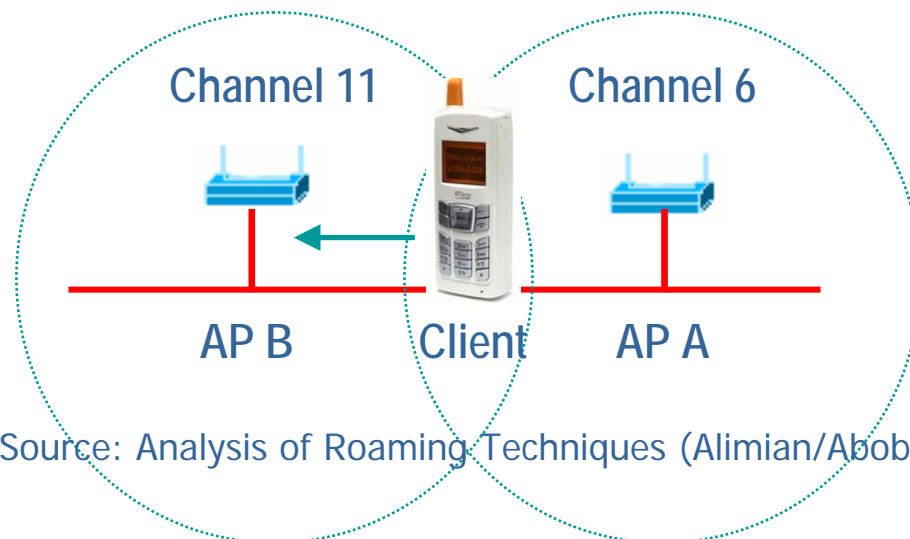
WPA2 “fast handoff” options

- ◆ WEP’s static shared keys simplify handoff
 - Client moving from AP to AP continues using same key for encryption, without re-authentication
- ◆ WPA/WPA2’s dynamic keys strengthen security
 - But also greatly increase AP handoff delay
 - Hassle in WLANs where users roam frequently
 - Deal-breaker for Voice / Video over WLAN
- ◆ 802.11i “fast handoff” options reduce delay by
 - Authenticating with new AP before handoff, or
 - Letting APs share dynamic key, cached by switch



Challenge: 802.11 Roaming

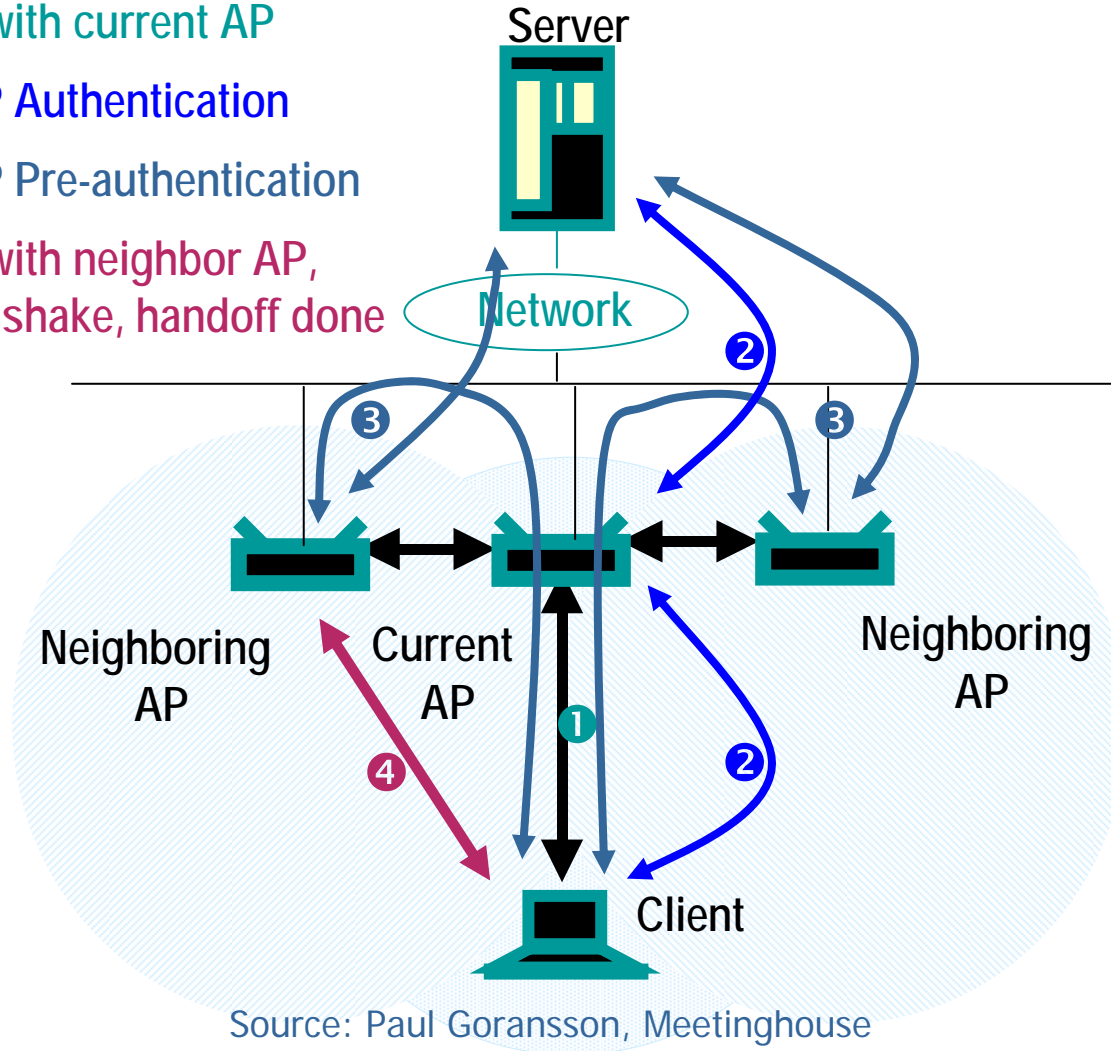
- ◆ Client associates to A, authenticates via 802.1X
- ◆ When signal strength falls below threshold, Client scans passively or actively, selects B as candidate
- ◆ Client tunes radio to channel 11, (re)associates to B, then authenticates again via 802.1X
- ◆ But full 802.1X authentication takes 750-1200ms
 - VoWLAN target is 50ms!



Source: Analysis of Roaming Techniques (Alimian/Aboba)

Solution 1: Pre-Authentication Option

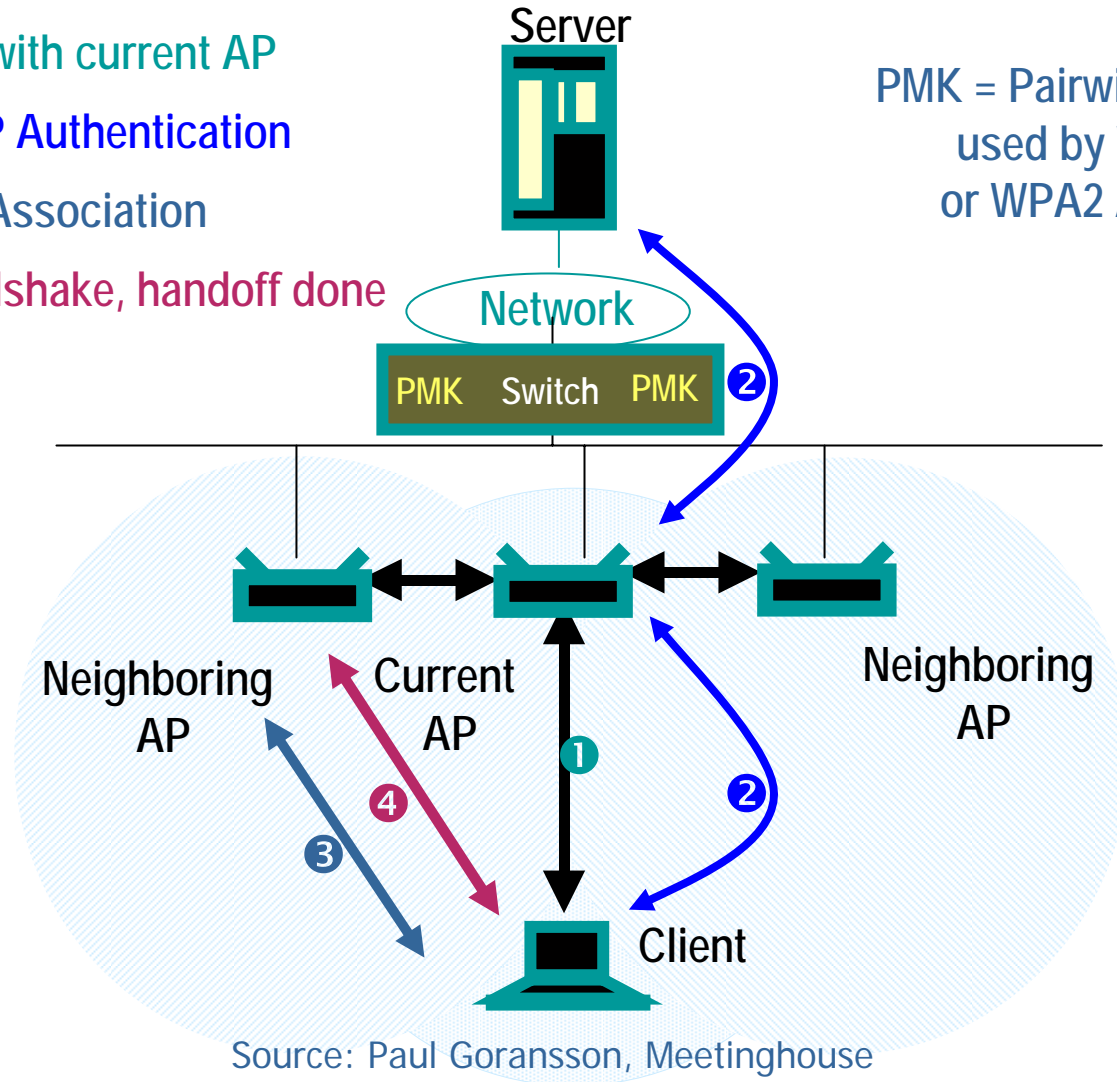
- ① Associate with current AP
- ② 802.1X/EAP Authentication
- ③ 802.1X/EAP Pre-authentication
- ④ Associate with neighbor AP, 4-way handshake, handoff done



Solution 2: Opportunistic Key Caching

- ① Associate with current AP
- ② 802.1X/EAP Authentication
- ③ 802.11 Re-Association
- ④ 4-way handshake, handoff done

PMK = Pairwise Master Key
used by WPA TKIP
or WPA2 AES-CCMP



- ◆ From Analysis of Roaming Techniques (Alimian/Aboba)
 - 802.1X Full Authentication = 750-1200ms
 - 802.1X Fast Handoff (4-way handshake) = 10-80ms

- ◆ Available today in homogeneous enterprise WLANs
 - Opportunistic key caching by WLAN switches, or
 - Proprietary inter-AP protocols like Cisco's CCKM

- ◆ But 802.1X is just one part of handoff latency
 - AP search time, IP address renewal, TCP adjustment
 - More is needed to roam across networks (WLAN/3G)

- ◆ Related standards initiatives
 - 802.11r: Fast BSS Transition
 - 802.21: Media Independent Handover

Current WLAN security standards

	Original	WPA	WPA2
Encapsulation	WEP	TKIP	CCMP
Encryption	RC4	RC4	AES
Integrity	None	MIC	MAC
Group Authentication	Shared Key	PreShared Key (WPA-Personal)	PreShared Key (WPA2-Personal)
User Authentication	None*	802.1X (WPA-Enterprise)	802.1X (WPA2-Enterprise)
Ad Hoc Support	Yes	No	Yes
Key Caching & Pre-Authenticate	No	No	Yes
Standard	802.11:1999	802.11i Draft	802.11i:2004

* 802.1X can also be used with WEP, but this combo is not in 802.11 standard

Finally, standards only go so far...

- ◆ Secure your Network Infrastructure
 - Configure & harden APs like other edge devices
 - Track, assess, and fix AP/switch vulnerabilities
 - Use VLANs and ACLs to segregate WLAN traffic

- ◆ Secure your Wireless Clients
 - Start with common laptop/PDA defenses
 - ◆ Easier for softphones than VoIP handsets
 - Track, assess, and fix client/device vulnerabilities
 - Centrally-administer WLAN settings
 - Monitor wireless activity on-site and off-site

- ◆ Deploy a WLAN Intrusion Prevention System (WIPS)
 - Audit wireless activity throughout your airspace
 - Auto-block/impede unauthorized wireless activity