Wi-Fi Roaming Variations Cheatsheet v1

Information in this sheet has been taken from Andrew Von Nagy's article: Wi-Fi Roaming Analysis part 2 - Roaming Variations (bit.ly/AVN_Roam)

➢ **Simple Authentication & Roam**: Non-802.1X methods, lower security, roam time < 50mS

➽ **Full 802.1X Authentication & Roam**: Full 802.1X auth, RADIUS server req, typically > 600mS roam time

➪ **Fast Roaming**: Initial 802.1X auth, followed by fast roam method to ensure <100mS roam req by voice traffic

Simple Authentication & Roam

Open Network
➢ Typically used on guest hotspot solutions
➢ User traffic un-encrypted at layer 2
➢ Authentication generally via captive portal
➢ Data flow after 802.11 open auth & 802.11 assoc frames exchange

Static WEP
➢ Layer 2 encryption, but easily cracked
➢ Data flow after 802.11 open auth & 802.11 assoc frames exch (plus WEP encryption)
➢ "Data protection" bit in 802.11 header indicate WEP encryption used

Static WEP Shared Key Authentication
➢ Variation of Static WEP, but less secure
➢ AP & client perform additional exchange to verify correct key held by client
➢ Desire to use key auth signalled in auth req & resp frames (auth algorithm field)

WPA/WPA2 Pre-shared Key
➢ Client & AP configured with shared PSK
➢ 802.11 open auth & assoc exch before 4 way handshake for exch of nonces
➢ Passphrase, STA addr, 4W h/shake nonces & SSID used to produce keying material
➢ Scalability issues as all users have same passphrase (revocation?)
➢ Knowledge of PSK & observation of 4W handshake allows data decryption
➢ Also known WPA2-Personal, use in SOHO market only

Full 802.1X Authentication & Roam

Dynamic WEP
➽ Vendor proprietary method (Cisco)
➽ Combines use of WEP & 802.11X/EAP (mainly Cisco's LEAP)
➽ Unicast & broadcast keys assigned via 2 EAPoL key frames after EAP auth, providing dynamic unicast keys (no longer static WEP keys)
➽ Still flawed as uses WEP
➽ Dynamic WEP not signalled in 802.11 frames, static config on client & AP

WPA/WPA2 Full Authentication
➽ User credentials verified via AAA auth server
➽ EAP auth performed after 802.11 auth & assoc frame exchange
➽ EAP protocol may require many frame exchanges for auth, creating roaming delay
➽ For each client roam, EAP auth required before data flow (data path broken in each roam)
➽ AAA server & client derive unique session master key (sent to AP/WLC by AAA server)
➽ AP & client perform 4 way handshake to generate temporal key from master key for data encryption
➽ Auth delay when roaming causes issues for voice & video traffic
➽ WPA & WPA2 created by Wi-Fi Alliance
➽ Popular EAP methods: EAP-TLS, PEAP

Fast Roaming

CCKM
➪ Cisco proprietary fast roam method
➪ Supported on autonomous & lightweight APs
➪ When roaming, client increments re-key # and derives new PTK key using AP BSSID
➪ Client indicates CCKM support via proprietary IE (requires CCX support on client)
➪ AP Support indicated by vendor AKMP in beacons & probe responses
➪ EAP auth & 4W handshake not req
➪ Roam time usually < 50mS
➪ Supports TKIP, AES, LEAP, PEAP, EAP-TLS

WPA/WPA2 EAP Session Resumption
➪ Also called "Fast Reconnect"
➪ Following full 802.1X auth, TLS session & security context cached on client & server
➪ Presence of cached TLS session implies successful previous auth, inner client auth may be skipped when roaming
➪ Typically 50% reduction in frame exchange on roam & re-auth
➪ Typically < 300mS roam time (network architecture dependant)
➪ Not fast enough for real time apps (e.g.voice)
➪ Proprietary method requires support on auth server & client

WPA2 PMK Caching
➪ Also known as Static PMK caching & Fast/Secure Roam-back, part of 802.11i
➪ Client re-uses PMKSA from previous 802.1X auth
➪ 4W handshake only (if AP has cached PMKID)
➪ Roam time typically < 100mS
➪ Only useful when returning to AP after previous auth

WPA2 Proactive Key Caching (PKC/OKC)
➪ Also known as OKC, proprietary method
➪ Extends WPA2 PMK by allowing re-use of single cached PMKSA across group of APs (e.g. on same WLC)
➪ On roam, client calcs PMKID based on new AP BSSID
➪ Allows EAP auth to be skipped, 4W handshake only req
➪ Roam time < 100mS

WPA2 Fast BSS Transition
➪ Standardized, secure fast transition support - 802.11r
➪ Support advertised by MDIE in beacons, probe resp & (re)assoc responses by AP
➪ Client indicates support in auth & (re)assoc frames
➪ After initial full 802.1X auth, keys distributed to other APs
➪ 802.1X & 4W handshake skipped on roam, < 50mS roam
➪ Over the air & over DS methods supported

Useful Links:
- Wi-Fi Roaming Analysis part 2 - Roaming Variations - (http://bit.ly/AVN_Roam)
- Robust Security Network (RSN) Fast BSS Transition (FT) - (http://bit.ly/CWNP_FT_PDF)
- Standardized Fast Secure Roaming whitepaper - (http://bit.ly/AVN_FTWP)

(V 1.3 May 2018)
Latest version of this sheet: www.wifinigel.com Feedback: wifinigel@gmail.com