Rome wasn’t built in a day...

and neither is roaming!

2016 • NEW ORLEANS

WIFI TREK

Who am I?

David Coleman

Senior Mobility Leader - Aerohive Networks

CWNE #4

@mistermultipath

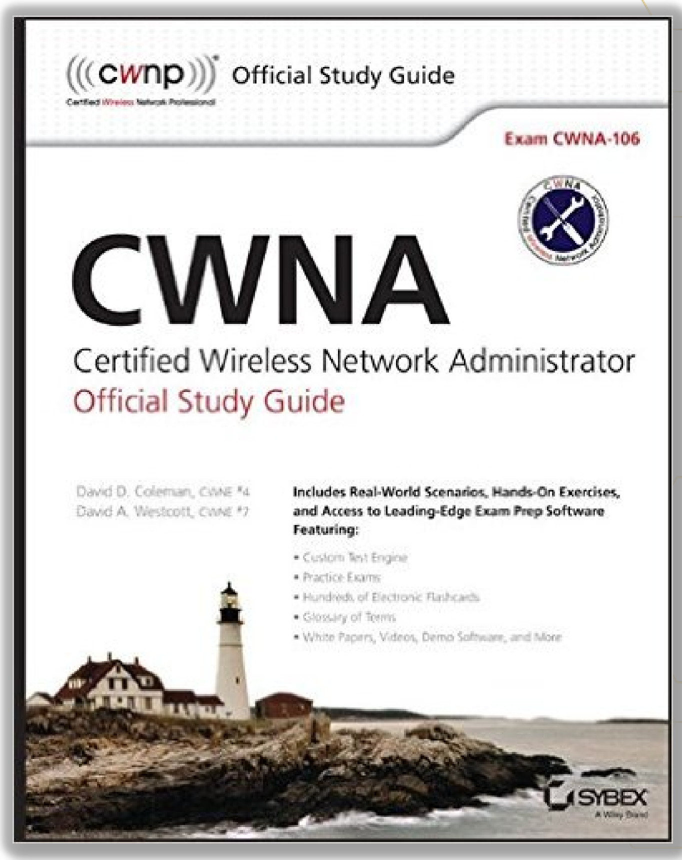
Who am I?

Co-author of:

Sybex CWNA Study Guide
4th Edition

ISBN: 978-1118893708

Amazon:
http://a.co/c6aNiRb



cwnp Official Study Guide
Certified Wireless Network Professional

Exam CWNA-106

CWNA
Certified Wireless Network Administrator
Official Study Guide

David D. Coleman, CWNE #4
David A. Westcott, CWNE #7

Includes Real-World Scenarios, Hands-On Exercises, and Access to Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Practice Exams
- Hundreds of Electronic Flashcards
- Glossary of Terms
- White Papers, Videos, Demo Software, and More

SYBEX
A Wiley Brand

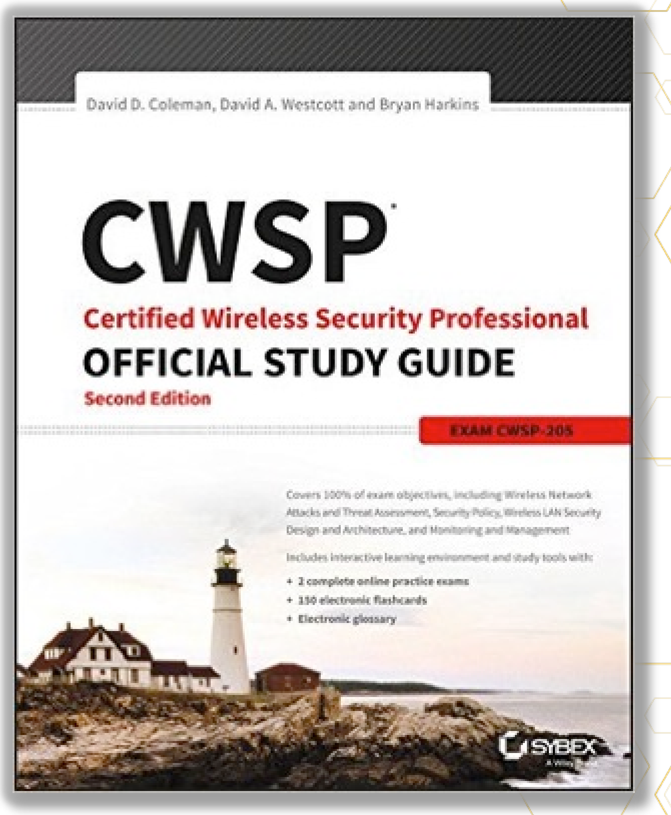
Who am I?

Available now:

Sybex CWSP Study Guide
2nd Edition

ISBN: 978-1119211082

Amazon:
http://amzn.com/1119211085



David D. Coleman, David A. Westcott and Bryan Harkins

CWSP

Certified Wireless Security Professional

OFFICIAL STUDY GUIDE

Second Edition

EXAM CWSP-205

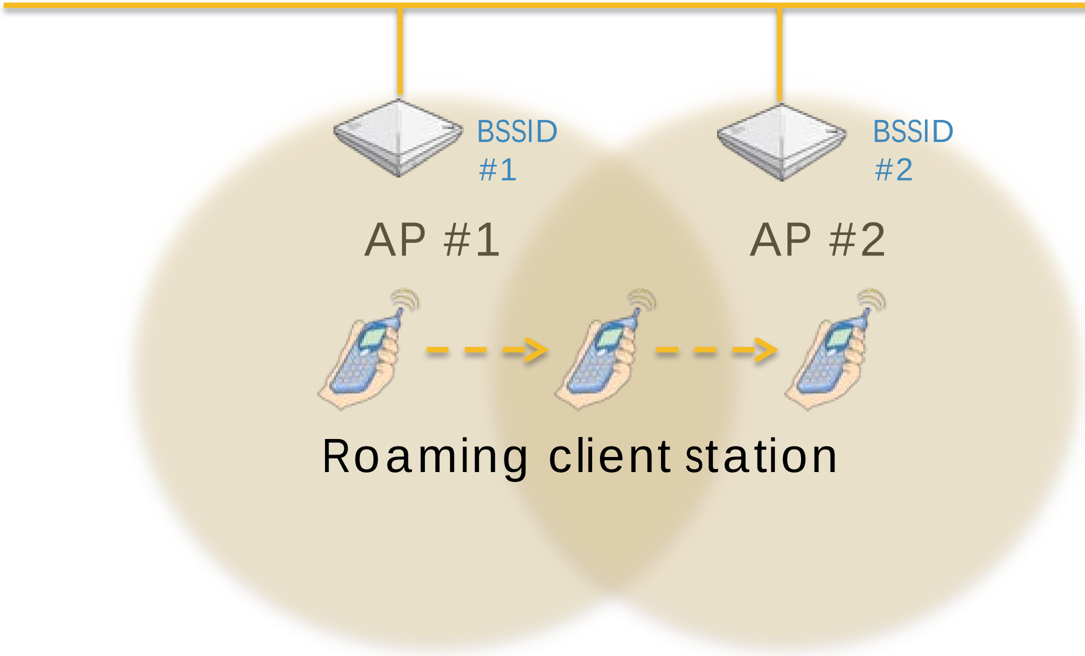
Covers 100% of exam objectives, including Wireless Network Attacks and Threat Assessment, Security Policy, Wireless LAN Security Design and Architecture, and Monitoring and Management

Includes interactive learning environment and study tools with:

- 2 complete online practice exams
- 150 electronic flashcards
- Electronic glossary

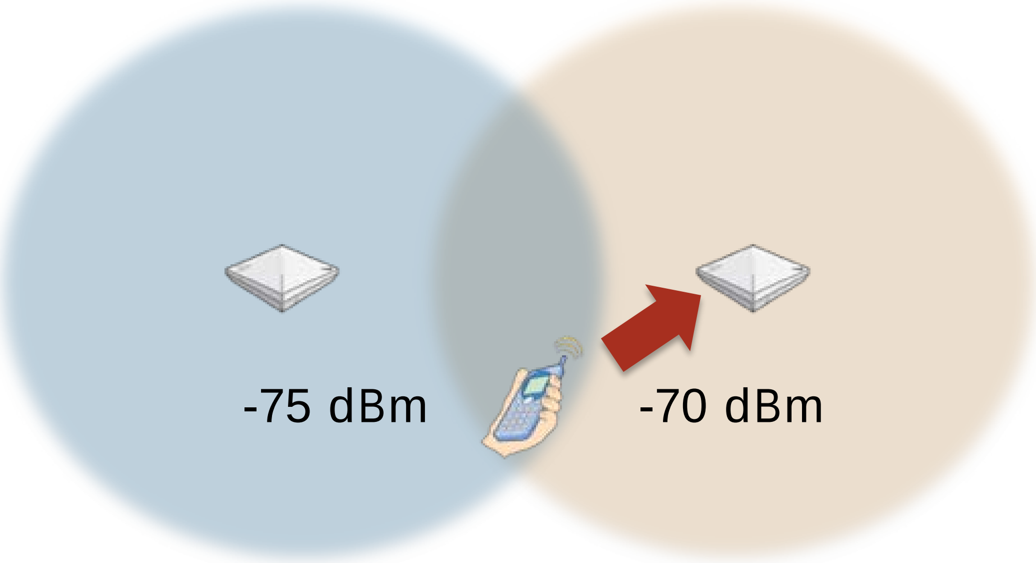
SYBEX

Layer 2: Roaming



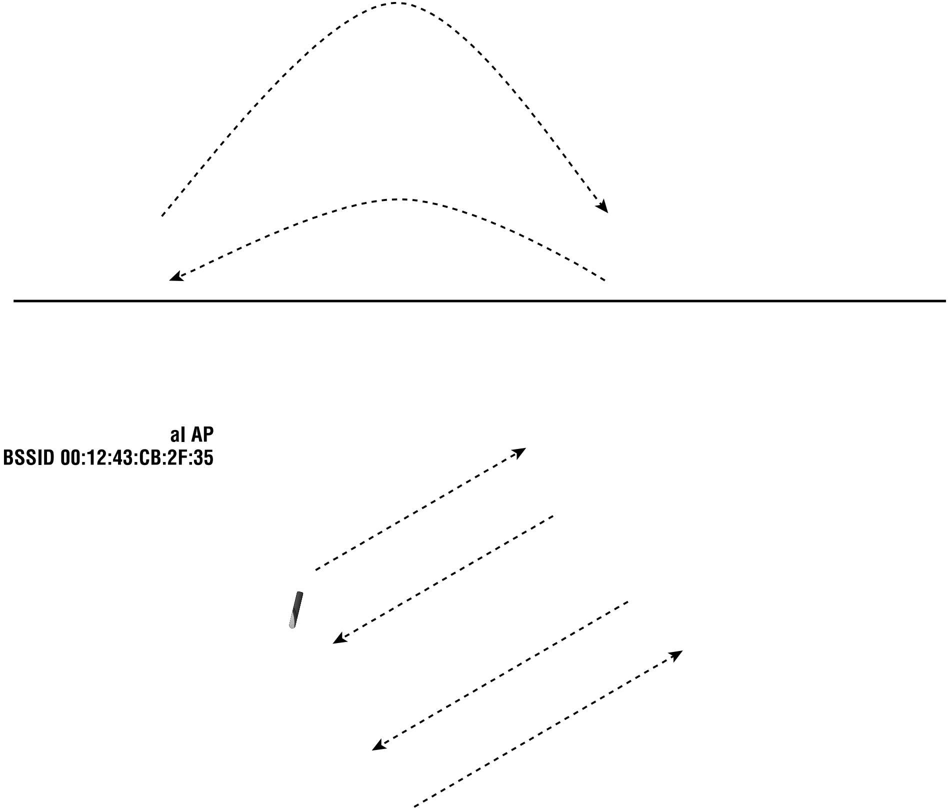
- Clients make the roaming decision

Client to AP handoff



- Clients make the roaming decision
- Based on factors such as RSSI or SNR
- The client sends a frame called the reassociation request frame, to start the roaming procedure.

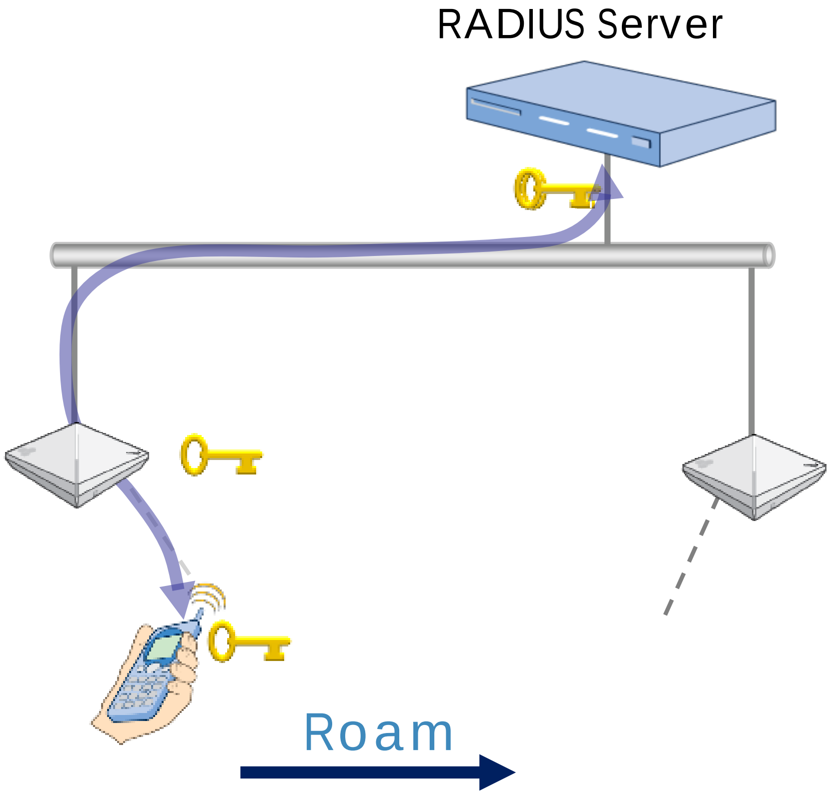
AP to AP handoff



The AP-to-AP handoff communications involves two primary tasks:

- The target AP informs the original AP that the client station is roaming.
- The target AP requests the client’s buffered packets from the original AP.

Fast Secure Roaming



- PMK caching
- Preauthentication
- Opportunistic Key Caching
- Fast BSS Transition

Overview

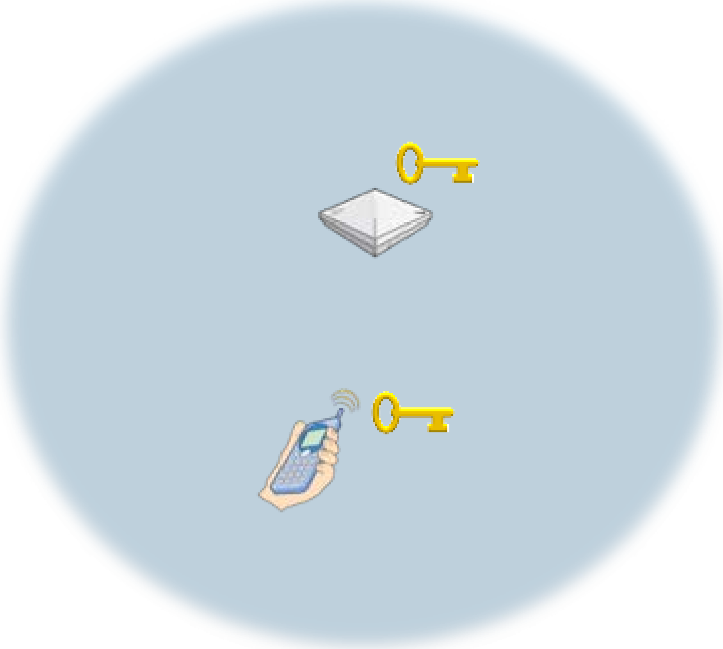
- There is a *symbiotic relationship* between PSK/802.1X authentication and the generation of dynamic encryption keys.

- An outstanding by-product of 802.1X/EAP can be the generation and distribution of dynamic encryption keys.

- Dynamic encryption keys can also be generated as a by-product of PSK authentication.

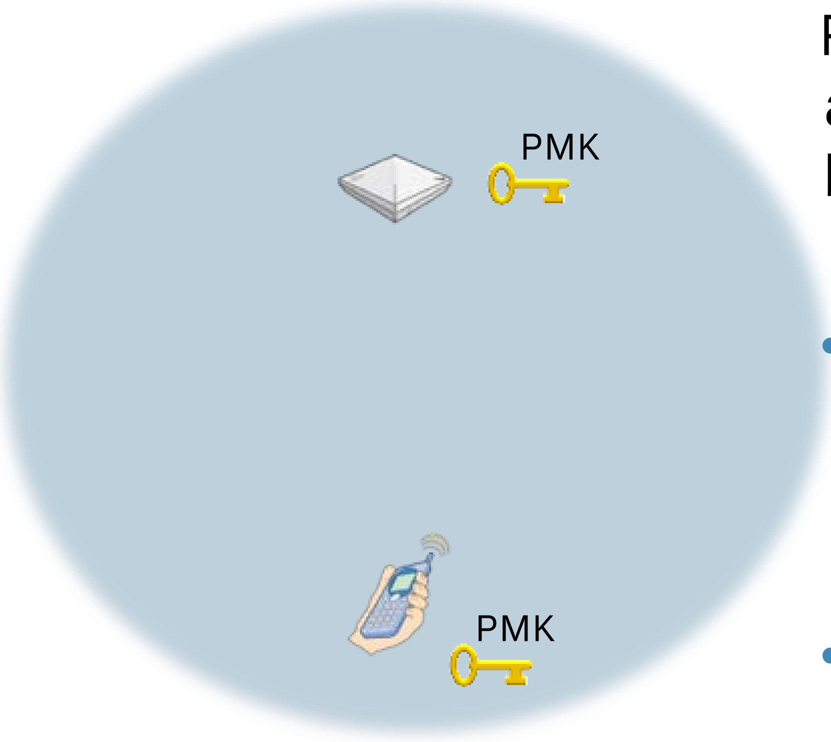
- Encryption and authentication are tied to each other in a Robust Secure Network Association (RSNA).

RSNA



A robust security network association (RSNA) requires two 802.11 stations (STAs) to establish procedures to authenticate and associate with each other as well as create dynamic encryption keys through the 4-Way Handshake process.

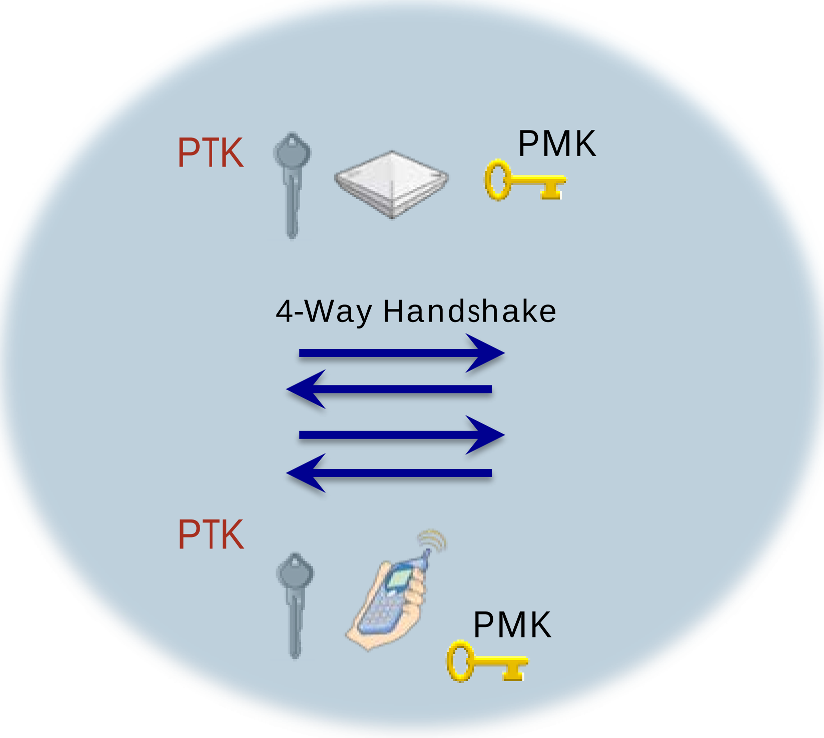
PMKSA



Robust security network associations (RSNAs) can be broken down into several subtypes.

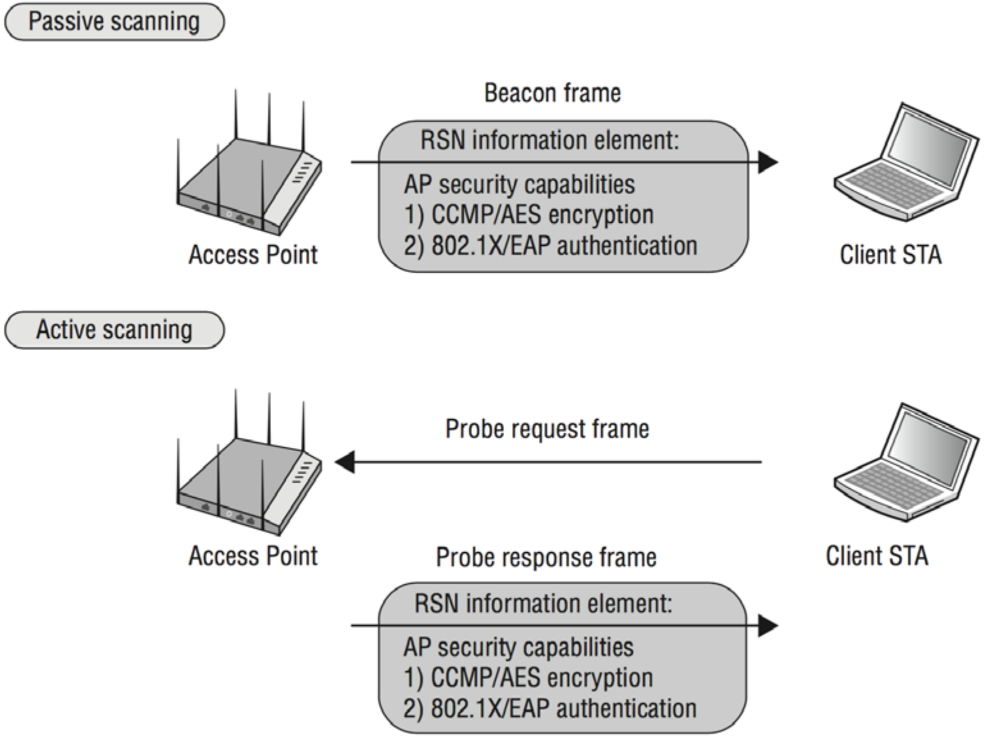
- 802.1X/EAP or PSK authentication process is needed to produce the pairwise master key (PMK)
- This is known as a pairwise master key security association (PMKSA)

PTKSA



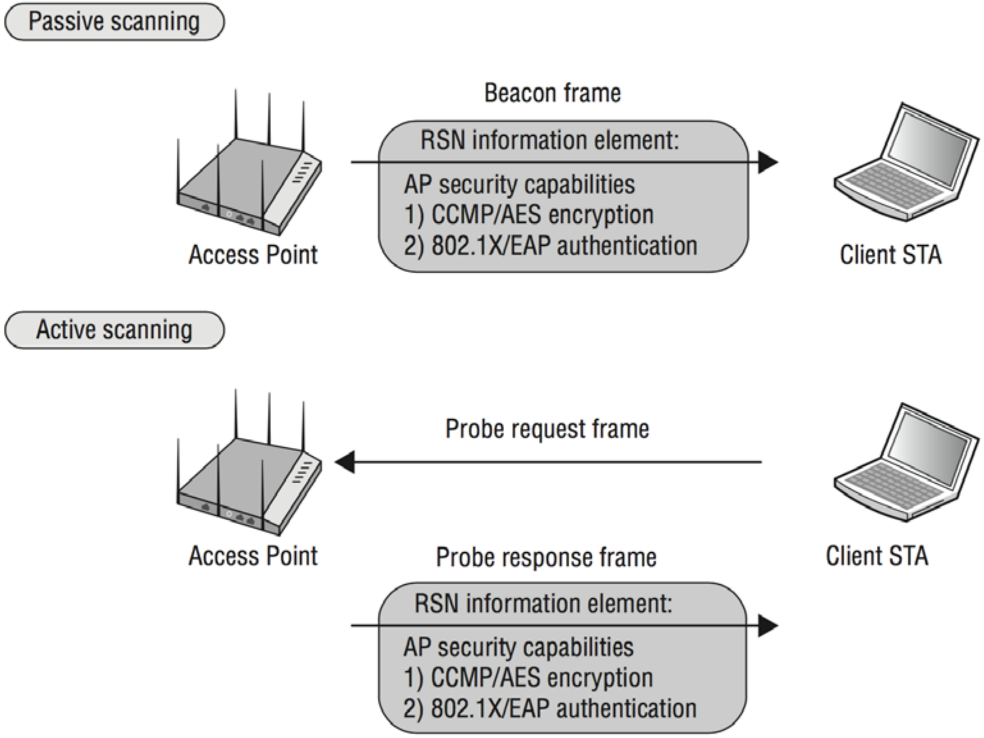
- The PMK is the seeding material for the 4-Way Handshake.
- The handshake creates the pairwise transient key (PTK)which is used for encryption and decryption of unicast traffic.
- This is known as a pairwise transient key security association (PTKSA)

RSN Information Element (RSNIE)



- RSN security can be identified by a field found in certain 802.11 management frames.
- This field is known as the robust security network information element (RSNIE) and is often referred to simply as the RSN information element.

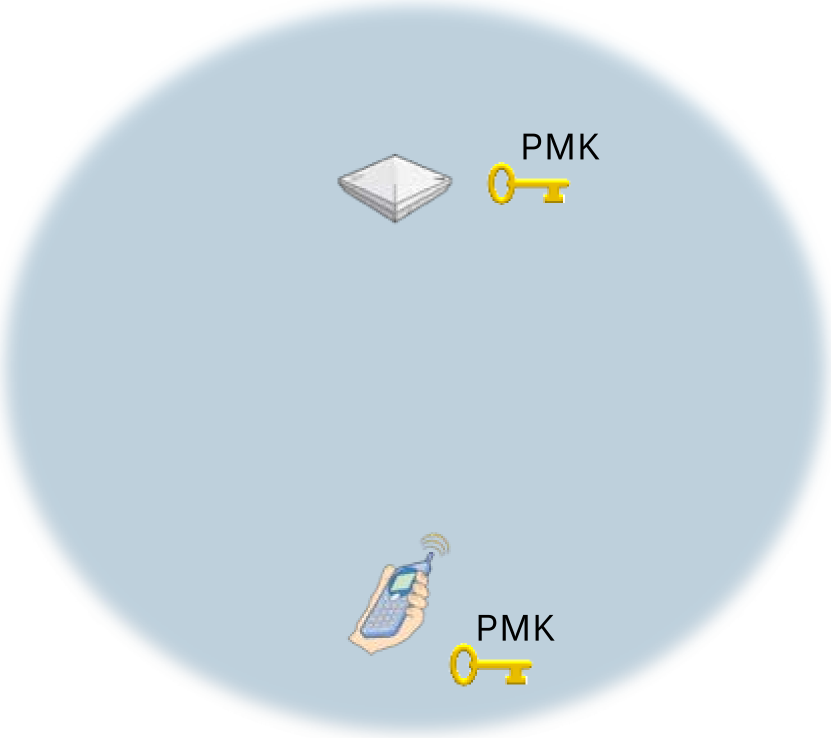
RSN Information Element (RSNIE)



- The RSN information element field is always found in four different 802.11 management frames:
  - beacon management frames
  - probe response frames
    association request frames
  - reassociation request frames

- The RSNIE can also be found in reassociation response frames if 802.11r mechanisms are enabled.

PMKID



- A unique identifier is created for each PMKSA that has been established between the authenticator and the supplicant.

- The pairwise master key identifier (PMKID) is a unique identifier that refers to a PMKSA.

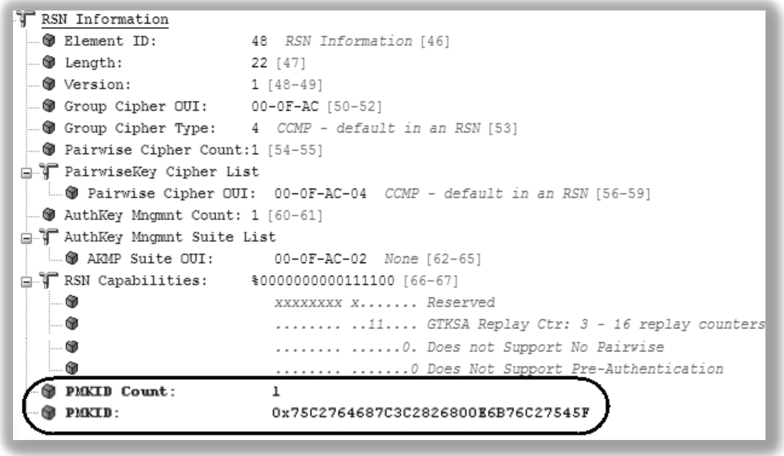
PMKID

Element ID	Length	Version	Group Cipher Suite	Pairwise Cipher Suite Count	Pairwise Cipher Suite List	AKM Suite Count	AKM Suite List	RSN Capabili-ties	PMKID Count	PMKID List

- The pairwise master key identifier (PMKID) is found in the RSN information element in association request frames and reassociation request frames that are sent from a client station to an AP.

- The PMKID is also found in FT Action frames.

PMKID

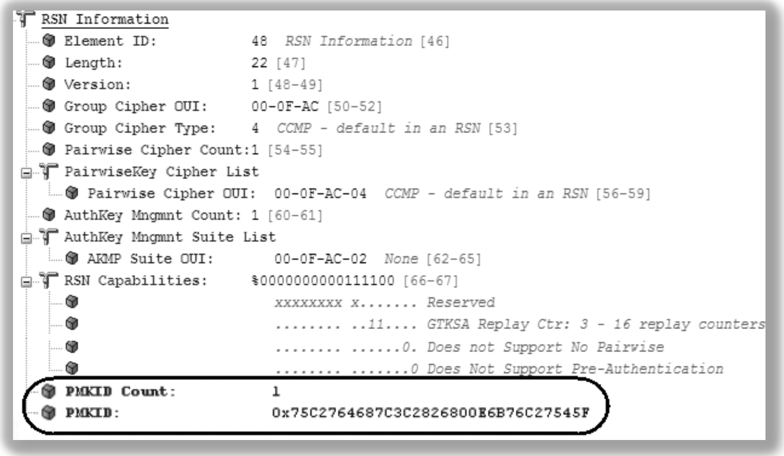


```
RSN Information
    Element ID:             48  RSN Information [46]
    Length:                 22 [47]
    Version:                1 [48-49]
    Group Cipher OUI:       00-0F-AC [50-52]
    Group Cipher Type:      4  CCMP - default in an RSN [53]
    Pairwise Cipher Count:1 [54-55]
    PairwiseKey Cipher List
        Pairwise Cipher OUI:  00-0F-AC-04  CCMP - default in an RSN [56-59]
    AuthKey Mngmnt Count: 1 [60-61]
    AuthKey Mngmnt Suite List
        AKMP Suite OUI:       00-0F-AC-02  None [62-65]
    RSN Capabilities:       %0000000000111100 [66-67]
                              xxxxxxxx x....... Reserved
                              ........ ..11.... GTKSA Replay Ctr: 3 - 16 replay counters
                              ........ ......0. Does not Support No Pairwise
                              ........ .......0 Does Not Support Pre-Authentication
    PMKID Count:              1
    PMKID:                    0x75C2764687C3C2826800E6B76C27545F
```

The PMKID can reference the following types of pairwise master key security associations:

- PMKSA derived from a PSK for the target AP
- Cached PMKSA from an 802.1X/EAP or SAE authentication
- Cached PMKSA that has been obtained through preauthentication with the target AP

PMKID

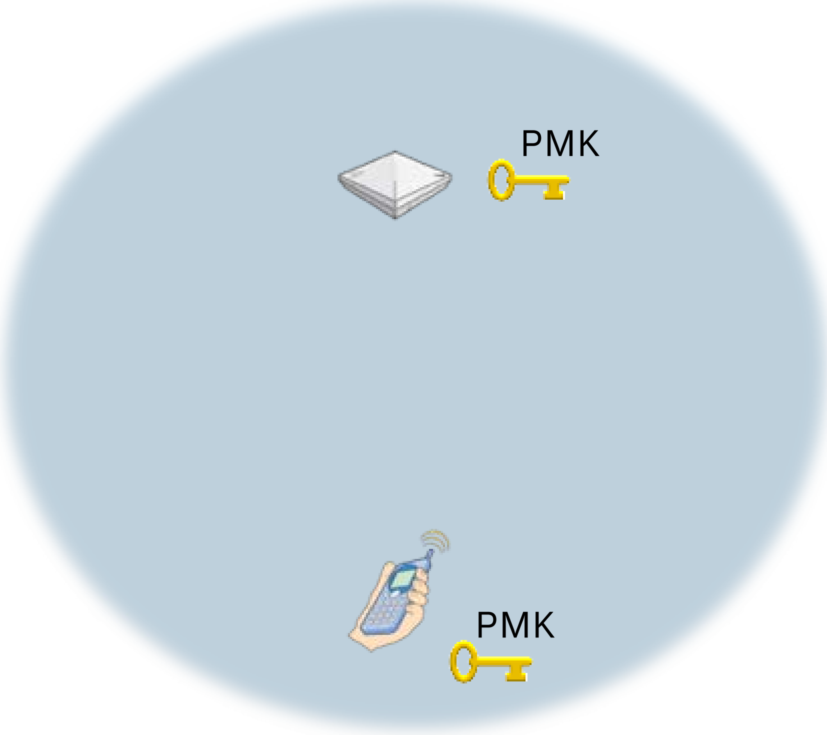


```
RSN Information
  Element ID:             48  RSN Information [46]
  Length:                 22 [47]
  Version:                1 [48-49]
  Group Cipher OUI:       00-0F-AC [50-52]
  Group Cipher Type:      4  CCMP - default in an RSN [53]
  Pairwise Cipher Count:1 [54-55]
  PairwiseKey Cipher List
    Pairwise Cipher OUI:  00-0F-AC-04  CCMP - default in an RSN [56-59]
  AuthKey Mngmnt Count: 1 [60-61]
  AuthKey Mngmnt Suite List
    AKMP Suite OUI:       00-0F-AC-02  None [62-65]
  RSN Capabilities:       %0000000000111100 [66-67]
                          xxxxxxxx x....... Reserved
                          ........ ..11.... GTKSA Replay Ctr: 3 - 16 replay counters
                          ........ ......0. Does not Support No Pairwise
                          ........ .......0 Does Not Support Pre-Authentication
  PMKID Count:            1
  PMKID:                  0x75C2764687C3C2826800E6B76C27545F
```

The PMKID can reference the following types of pairwise master key security associations:

- PMK-R0 security association derived as part of an FT initial mobility domain association
- PMK-R1 security association derived as part of an FT initial mobility domain association or as part of a fast BSS transition

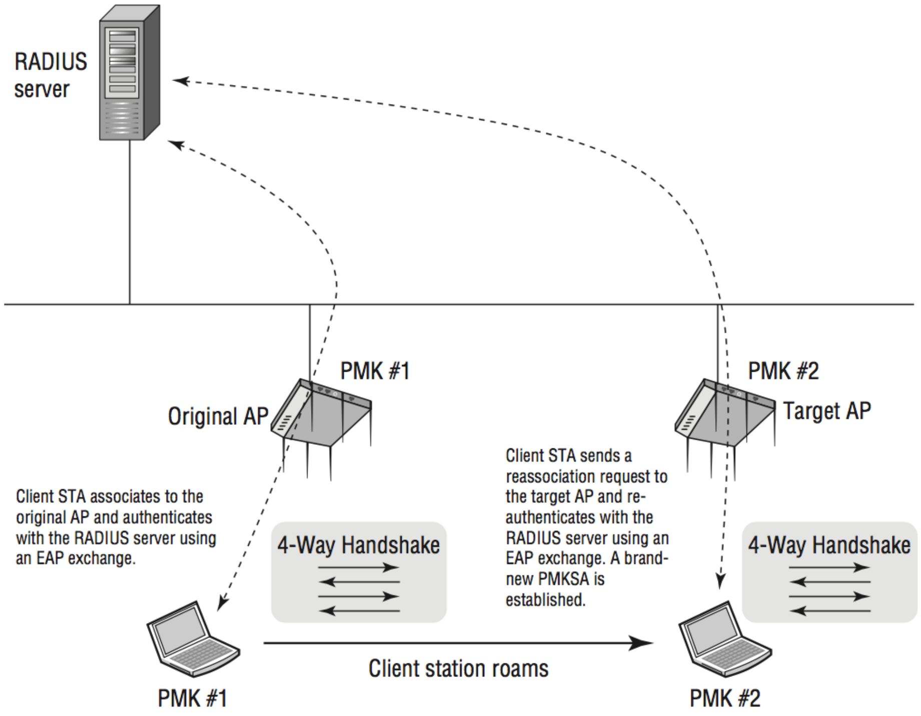
PMKSA



The components of a PMKSA include:

- PMK - he created Pairwise Master Key.
- PMKID - The unique identifier of the association.
- Authenticator MAC - Layer 2 address of the authenticator.
- Lifetime - The key lifetime is not otherwise specified, then the PMK lifetime is infinite.
- AKMP - The authentication and key management protocol.
- Authorization parameters - Anything specified by the authentication server or supplicant. Example: Authorized SSID

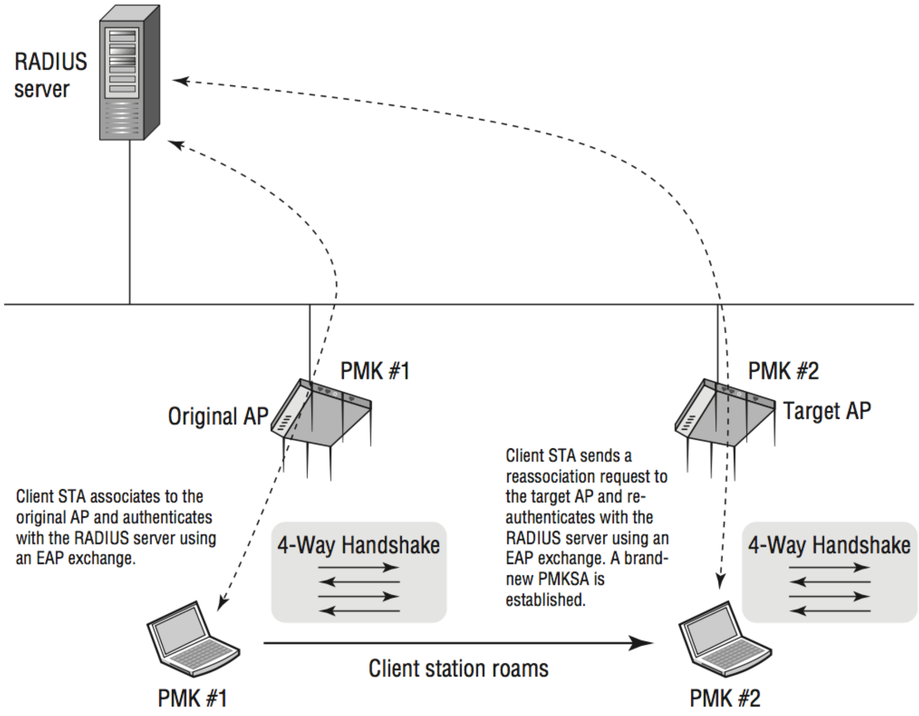
PMKSA – 802.1X/EAP


RADIUS server
PMK #1
Original AP
PMK #2
Target AP
Client STA associates to the original AP and authenticates with the RADIUS server using an EAP exchange.
4-Way Handshake
Client STA sends a reassociation request to the target AP and re-authenticates with the RADIUS server using an EAP exchange. A brand-new PMKSA is established.
4-Way Handshake
Client station roams
PMK #1
PMK #2

Without any type of fast secure roaming mechanism

- Every time a client roams, the client will re-authenticate.
- Therefore, every time time a client roams a new PMKSA is established.

PMKSA – 802.1X/EAP



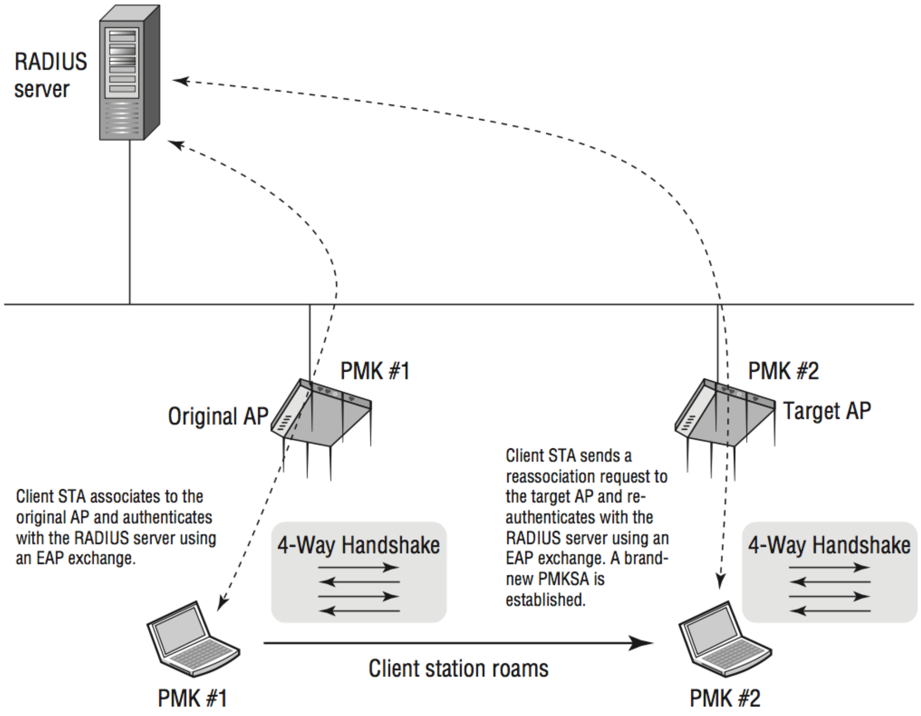
Client STA associates to the original AP and authenticates with the RADIUS server using an EAP exchange.

Client STA sends a reassociation request to the target AP and re-authenticates with the RADIUS server using an EAP exchange. A brand-new PMKSA is established.

- 802.1X/EAP authentication can take 700 milliseconds (ms) or longer for the client to authenticate.

- VoWiFi requires a handoff of 150 ms or less to avoid a degradation of the quality of the call or even worse, a loss of connection.

PMKSA – 802.1X/EAP

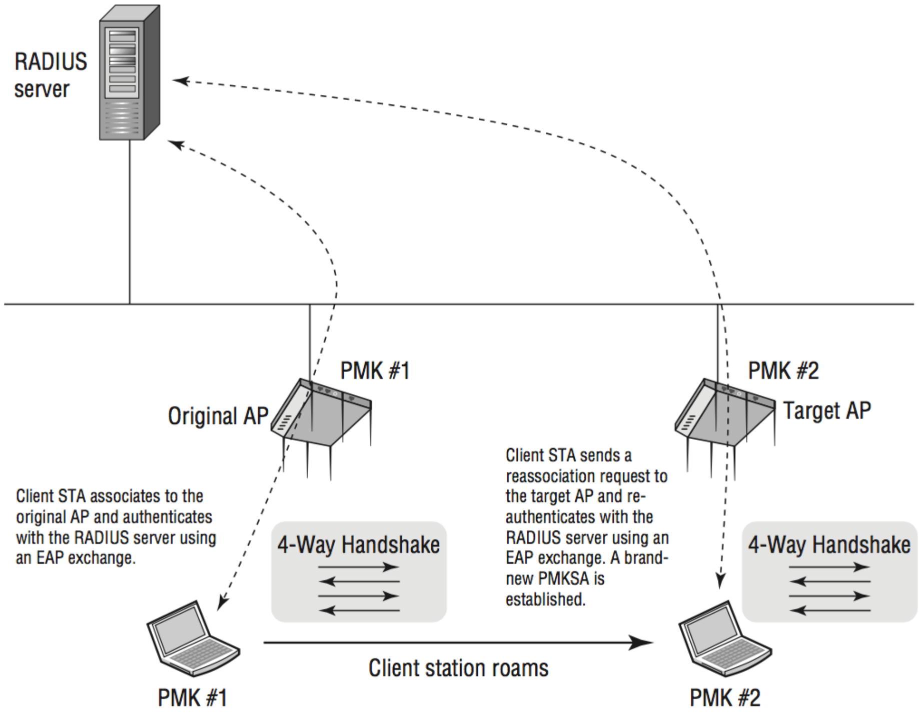


Client STA associates to the original AP and authenticates with the RADIUS server using an EAP exchange.

Client STA sends a reassociation request to the target AP and re-authenticates with the RADIUS server using an EAP exchange. A brand-new PMKSA is established.

- 802.1X/EAP authentication can take 700 milliseconds (ms) or longer for the client to authenticate.
- VoWiFi requires a handoff of 150 ms to avoid a degradation of the quality of the call or even worse, a loss of connection. A 50 ms or less handoff is ideal.

PMKSA – 802.1X/EAP

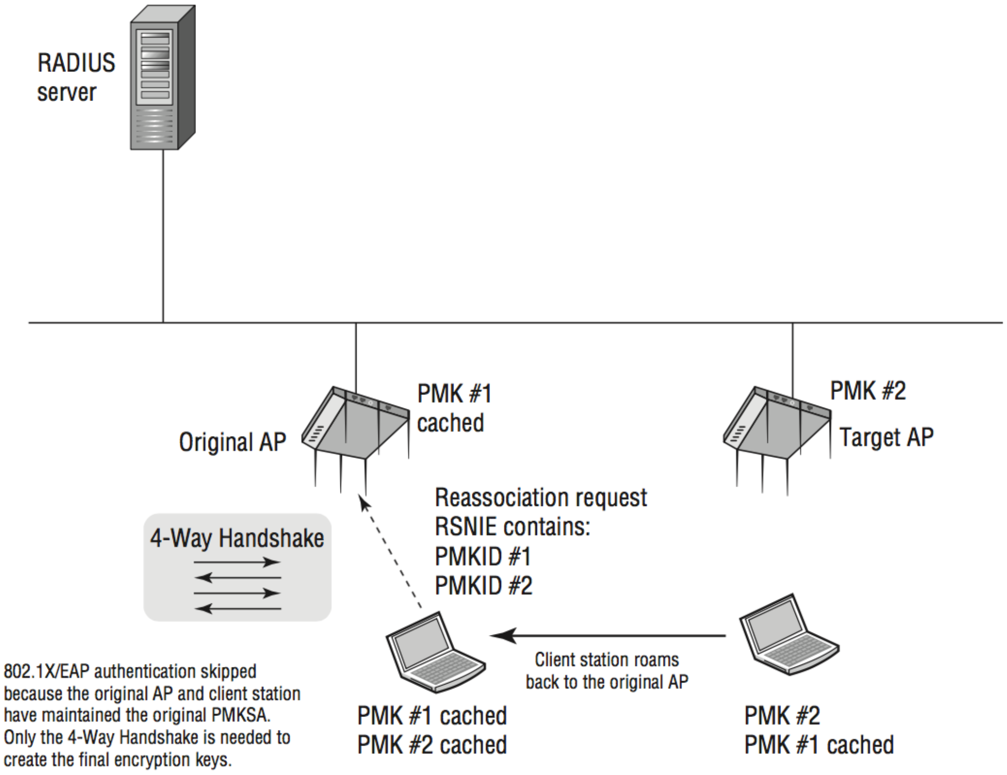


Client STA associates to the original AP and authenticates with the RADIUS server using an EAP exchange.

Client STA sends a reassociation request to the target AP and re-authenticates with the RADIUS server using an EAP exchange. A brand-new PMKSA is established.

- The normal delay will disrupt the communications of time-sensitive applications such as voice and video.
- Therefore, the 802.11-2012 standard defines three fast secure roaming mechanisms:
    - PMK caching
    - Preauthentication
    - Fast BSS transition

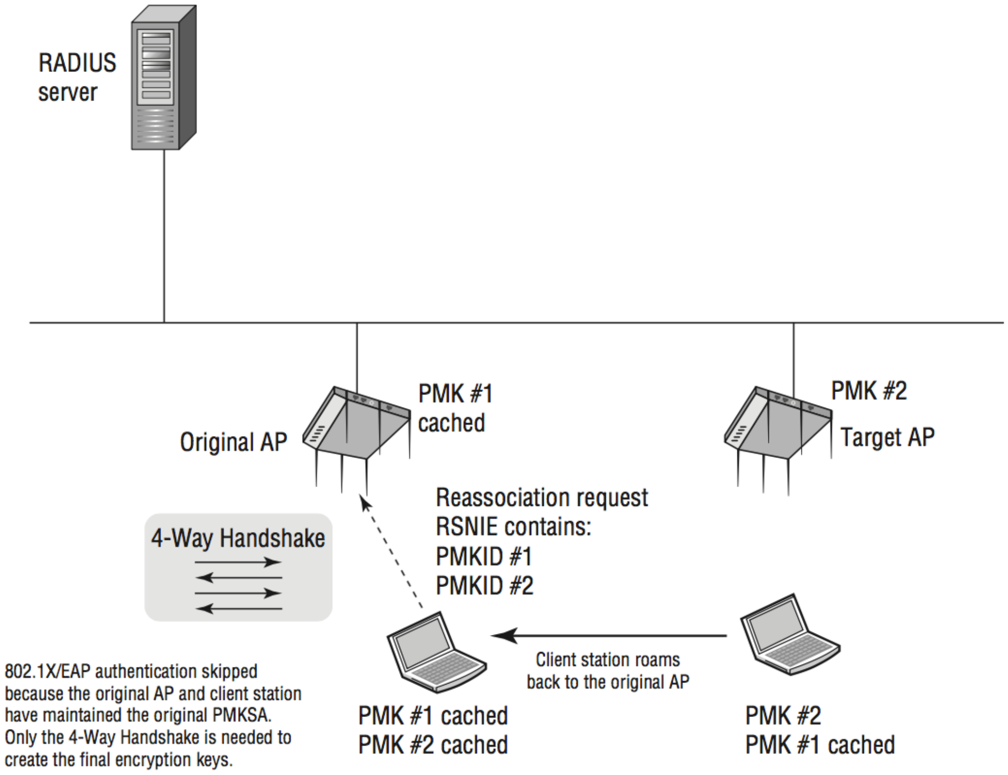
PMK Caching



802.1X/EAP authentication skipped because the original AP and client station have maintained the original PMKSA. Only the 4-Way Handshake is needed to create the final encryption keys.

- The 802.11-2012 standard states *"An AP whose authenticator has retained the PMK for one or more of the PMKIDs can skip the IEEE 802.1X/EAP authentication and proceed with the 4-Way Handshake."*
- In simpler words, when the client roams back to the original AP, both devices still have the original cached PMK #1 and they can skip the 802.1X/EAP exchange.

PMK Caching

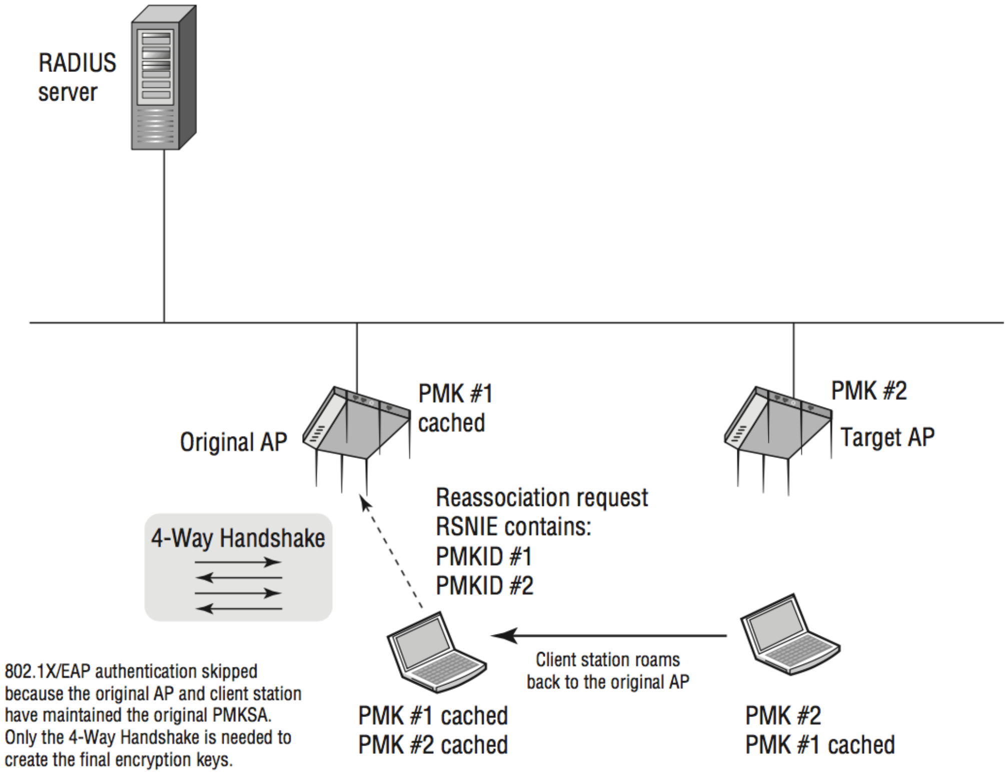


802.1X/EAP authentication skipped because the original AP and client station have maintained the original PMKSA. Only the 4-Way Handshake is needed to create the final encryption keys.

- The client does not need to re-authenticate and create a new PMK because the original PMK still exists.

- The cached original PMK is then used to seed the 4-Way Handshake.

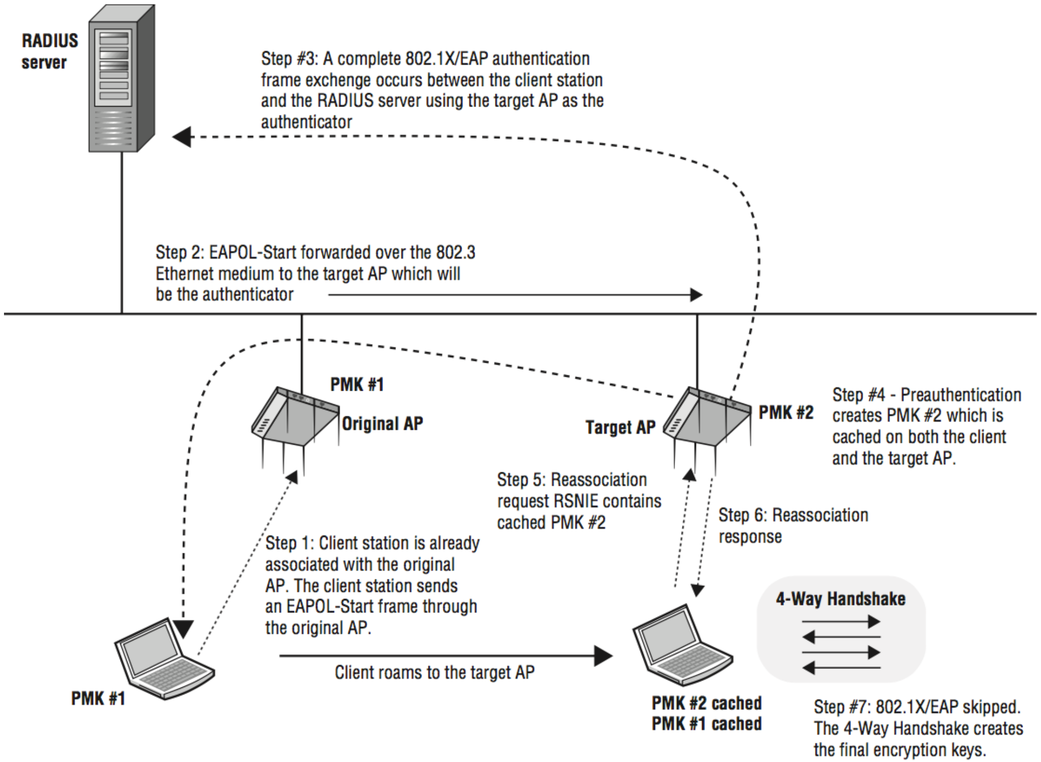
PMK Caching



802.1X/EAP authentication skipped because the original AP and client station have maintained the original PMKSA. Only the 4-Way Handshake is needed to create the final encryption keys.

- PMK caching is sometimes called fast secure roam-back.
- This does not address fast secure roaming when the client roams forward.

Preauthentication

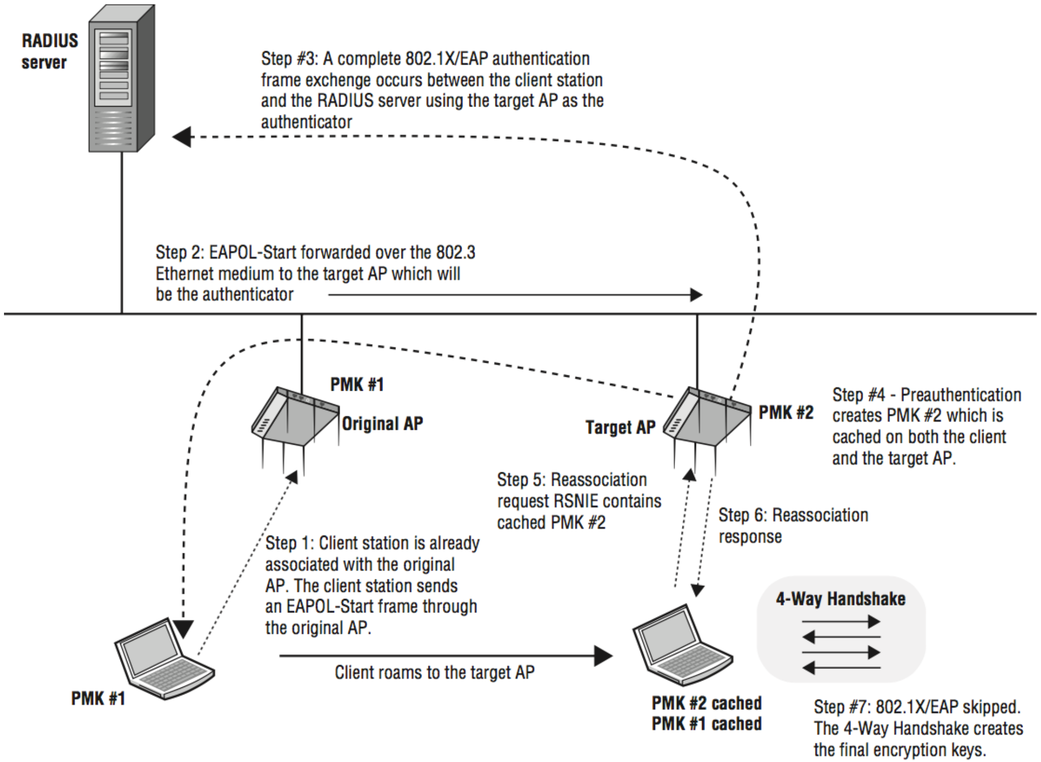


RADIUS server
Step #3: A complete 802.1X/EAP authentication frame exchange occurs between the client station and the RADIUS server using the target AP as the authenticator
Step 2: EAPOL-Start forwarded over the 802.3 Ethernet medium to the target AP which will be the authenticator
PMK #1
Original AP
Target AP
PMK #2
Step #4 - Preauthentication creates PMK #2 which is cached on both the client and the target AP.
Step 5: Reassociation request RSNIE contains cached PMK #2
Step 6: Reassociation response
Step 1: Client station is already associated with the original AP. The client station sends an EAPOL-Start frame through the original AP.
4-Way Handshake
PMK #1
Client roams to the target AP
PMK #2 cached
PMK #1 cached
Step #7: 802.1X/EAP skipped. The 4-Way Handshake creates the final encryption keys.

- A client station can use preauthentication to establish a new PMKSA with an AP prior to roaming to a new target AP.

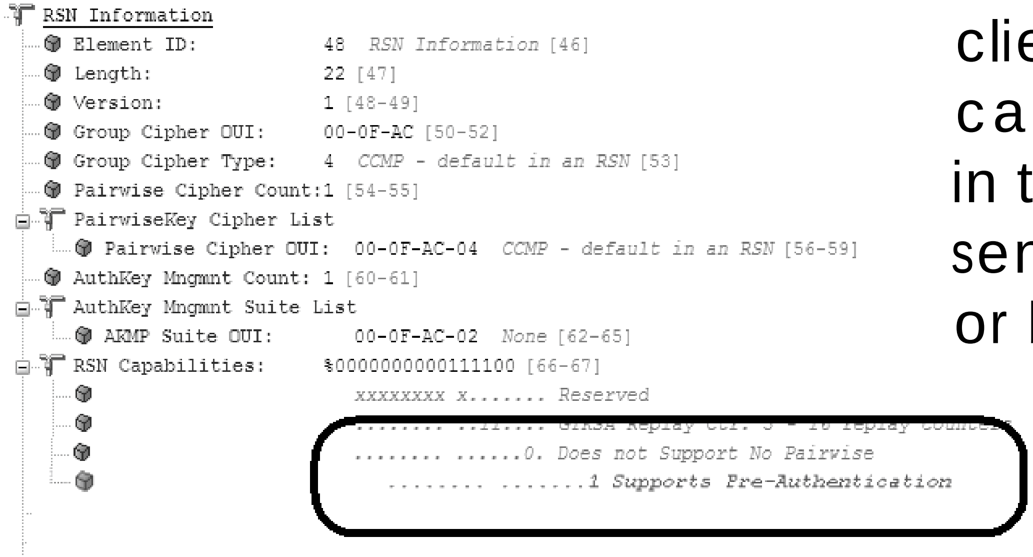
- Preauthentication allows a client station to initiate a new 802.1X/EAP exchange with a RADIUS server while associated with the original AP.

Preauthentication


RADIUS server
Step #3: A complete 802.1X/EAP authentication frame exchange occurs between the client station and the RADIUS server using the target AP as the authenticator
Step 2: EAPOL-Start forwarded over the 802.3 Ethernet medium to the target AP which will be the authenticator
PMK #1
Original AP
Target AP
PMK #2
Step #4 - Preauthentication creates PMK #2 which is cached on both the client and the target AP.
Step 5: Reassociation request RSNIE contains cached PMK #2
Step 6: Reassociation response
Step 1: Client station is already associated with the original AP. The client station sends an EAPOL-Start frame through the original AP.
4-Way Handshake
PMK #1
Client roams to the target AP
PMK #2 cached
PMK #1 cached
Step #7: 802.1X/EAP skipped. The 4-Way Handshake creates the final encryption keys.

- The purpose of the new 802.1X/EAP authentication is to create a new PMKSA relationship with a new target AP where the client might roam.
- The client does not need to re-authenticate and create a new PMK because a precreated cached PMK already exists.

Preauthentication



```
RSN Information
   Element ID:             48  RSN Information [46]
   Length:                 22 [47]
   Version:                1 [48-49]
   Group Cipher OUI:       00-0F-AC [50-52]
   Group Cipher Type:      4  CCMP - default in an RSN [53]
   Pairwise Cipher Count:1 [54-55]
   PairwiseKey Cipher List
      Pairwise Cipher OUI:  00-0F-AC-04  CCMP - default in an RSN [56-59]
   AuthKey Mngmnt Count: 1 [60-61]
   AuthKey Mngmnt Suite List
      AKMP Suite OUI:       00-0F-AC-02  None [62-65]
   RSN Capabilities:       %0000000000111100 [66-67]
                              xxxxxxxx x....... Reserved
                              ........ ..11.... GTKSA Replay Ctr: 3 - 16 replay counters
                              ........ ......0. Does not Support No Pairwise
                                ........ .......1 Supports Pre-Authentication
```

An AP can indicate to the client station that the AP is capable of preauthentication in the RSN information element sent in the AP’s probe response or beacon frames.

PMK Caching and Preauthentication

- Both PMK caching and preauthentication were originally defined in the 802.11i security amendment.
- The intent was to use them together to solve fast secure roaming.
- Neither method scaled very well and preauthentication put a tremendous load on RADIUS servers.
- Instead, vendors began to adopt a non-standard method called opportunistic key caching (OKC).

Opportunistic Key Caching (OKC)

- OKC allows for PMK caching between multiple APs that are under some sort of administrative control.

- Unlike preauthentication, OKC does not mandate how a PMK arrives at the target AP.

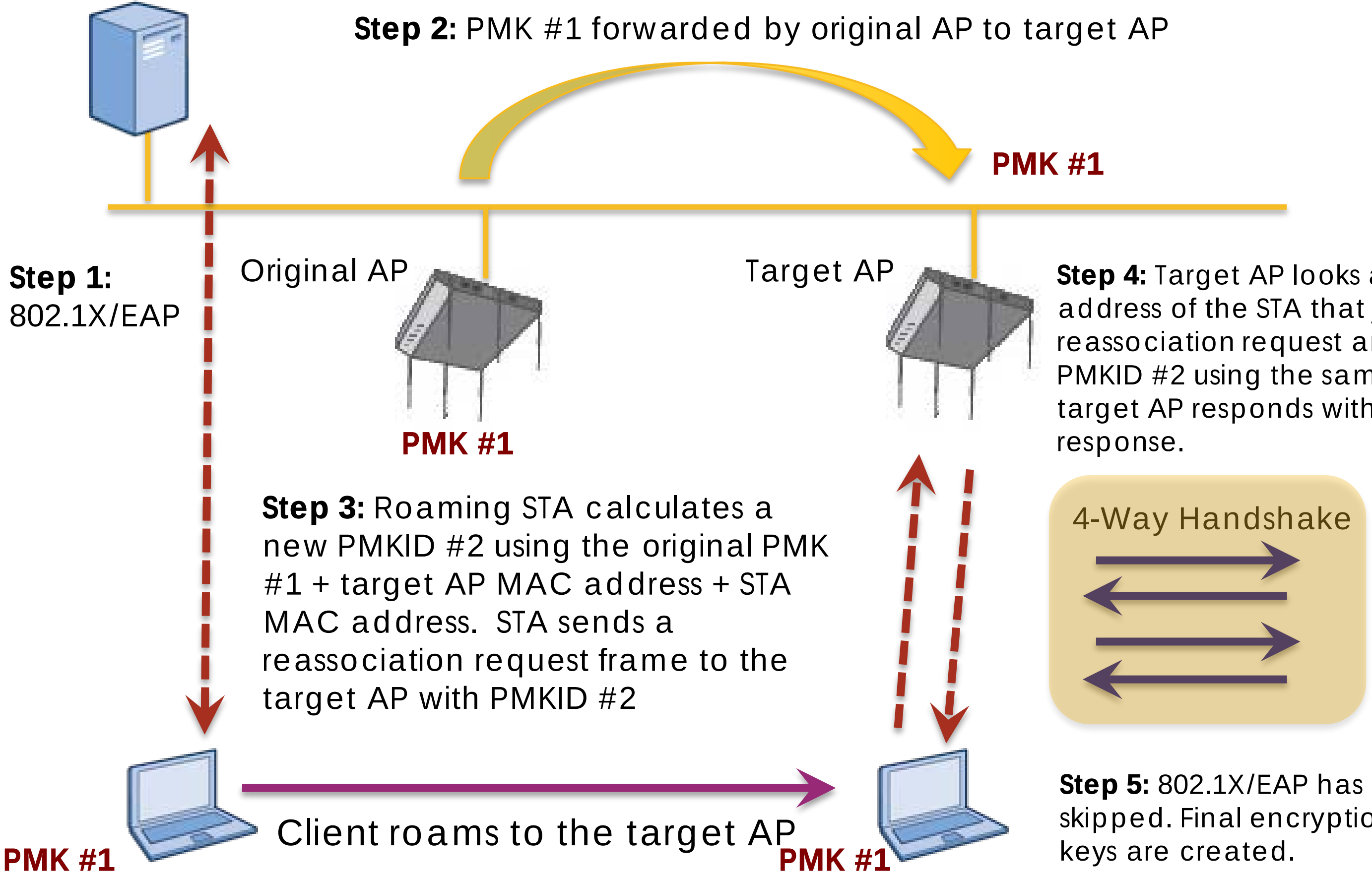
- OKC instead allows a client station the opportunity to take advantage of a single cached PMK shared among multiple access points.

Opportunistic Key Caching (OKC)

- OKC forwards a PMK from an original AP and then distributes it to other APs.
- The PMK distribution between APs is dependent on the WLAN architecture and is usually proprietary.
- In a WLAN controller environment, the PMKs are usually forwarded by the controller to the APs. In a non-controller environment, the PMKs are forwarded by the APs to each other using a proprietary protocol.

Aerohive: AMRP

Opportunistic Key Caching (OKC)



Step 1: 802.1X/EAP

Step 2: PMK #1 forwarded by original AP to target AP

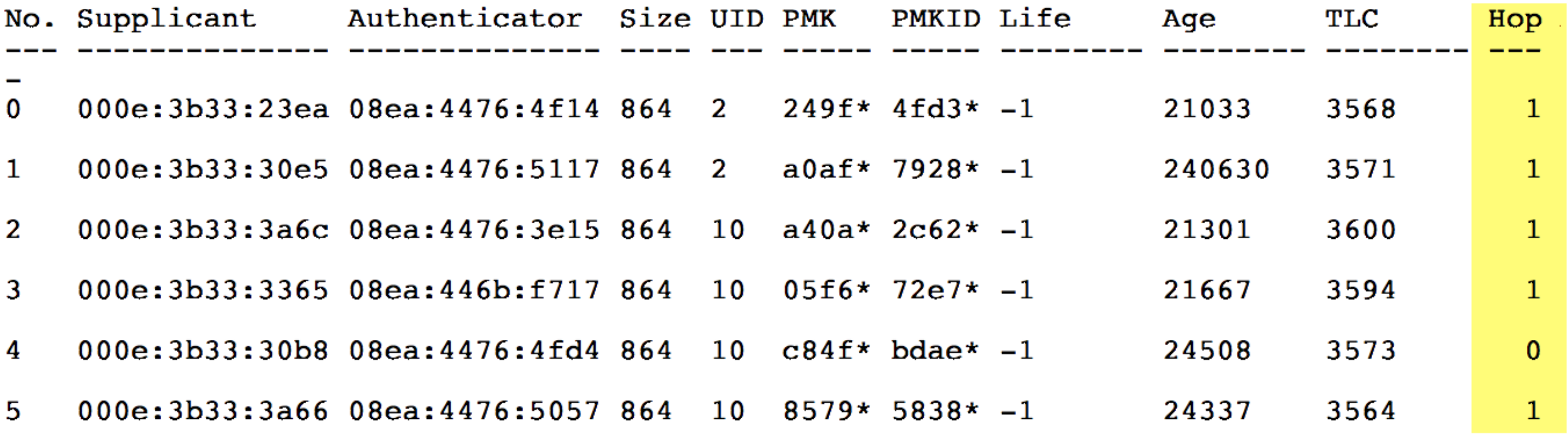
Step 3: Roaming STA calculates a new PMKID #2 using the original PMK #1 + target AP MAC address + STA MAC address. STA sends a reassociation request frame to the target AP with PMKID #2

Client roams to the target AP

Step 4: Target AP looks at the MAC address of the STA that just sent the reassociation request and calculates PMKID #2 using the same formula. The target AP responds with a reassociation response.

Step 5: 802.1X/EAP has been skipped. Final encryption keys are created.

AP roaming cache

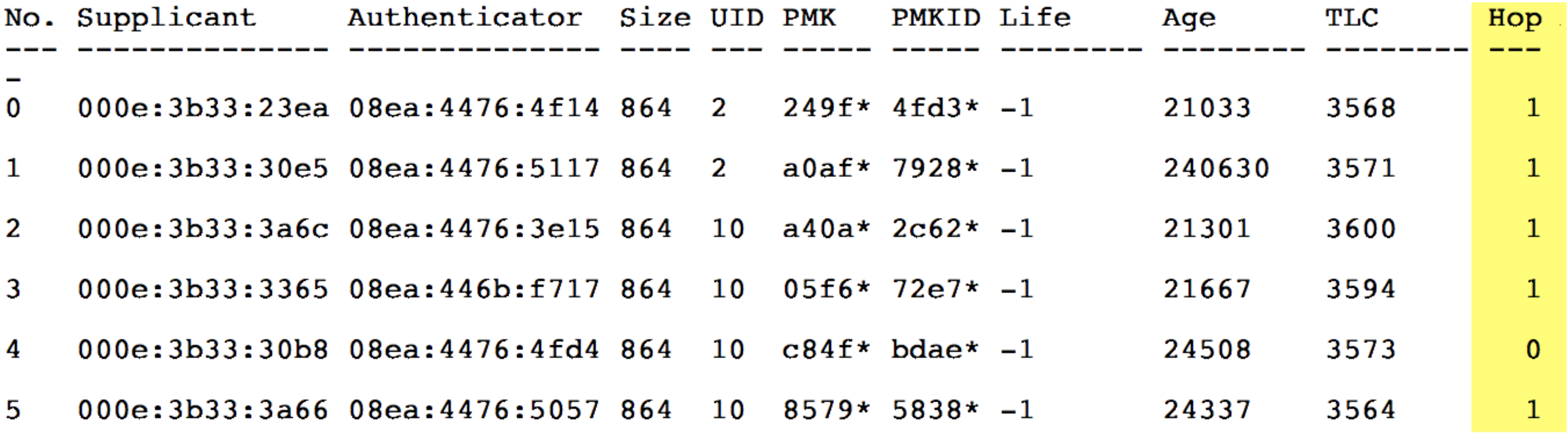


```
No. Supplicant     Authenticator  Size UID PMK   PMKID Life     Age      TLC      Hop
--- -------------- -------------- ---- --- ----- ----- -------- -------- -------- ---
-
0   000e:3b33:23ea 08ea:4476:4f14 864  2   249f* 4fd3* -1       21033    3568       1

1   000e:3b33:30e5 08ea:4476:5117 864  2   a0af* 7928* -1       240630   3571       1

2   000e:3b33:3a6c 08ea:4476:3e15 864  10  a40a* 2c62* -1       21301    3600       1

3   000e:3b33:3365 08ea:446b:f717 864  10  05f6* 72e7* -1       21667    3594       1

4   000e:3b33:30b8 08ea:4476:4fd4 864  10  c84f* bdae* -1       24508    3573       0

5   000e:3b33:3a66 08ea:4476:5057 864  10  8579* 5838* -1       24337    3564       1
```

- Supplicant #4 is a client that is currently associated to the AP.

- The other supplicants are client stations that are one hop away and not associated to the AP.

AP roaming cache

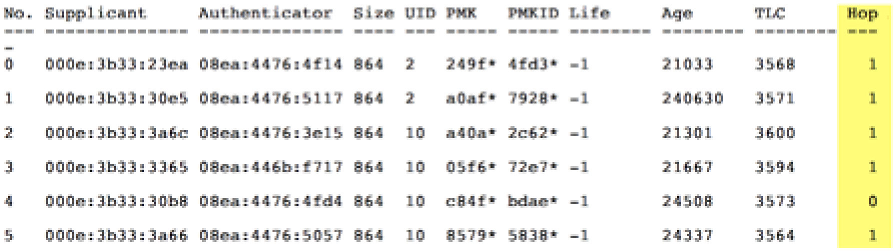


```
No. Supplicant     Authenticator  Size UID PMK   PMKID Life     Age      TLC      Hop
--- -------------- -------------- ---- --- ----- ----- -------- -------- -------- ---
-
0   000e:3b33:23ea 08ea:4476:4f14 864  2   249f* 4fd3* -1       21033    3568       1
1   000e:3b33:30e5 08ea:4476:5117 864  2   a0af* 7928* -1       240630   3571       1
2   000e:3b33:3a6c 08ea:4476:3e15 864  10  a40a* 2c62* -1       21301    3600       1
3   000e:3b33:3365 08ea:446b:f717 864  10  05f6* 72e7* -1       21667    3594       1
4   000e:3b33:30b8 08ea:4476:4fd4 864  10  c84f* bdae* -1       24508    3573       0
5   000e:3b33:3a66 08ea:4476:5057 864  10  8579* 5838* -1       24337    3564       1
```

- The PMKs of the other stations have already been forwarded to this AP and are cached.

- Any client that also supports OKC can use its original PMK when roaming to this new AP

OKC – Is it supported?



```
No. Supplicant     Authenticator  Size UID PMK   PMKID Life     Age      TLC      Hop
--- -------------- -------------- ---- --- ----- ----- -------- -------- --------- ---
-
0   000e:3b33:23ea 08ea:4476:4f14 864  2   249f* 4fd3* -1       21033    3568       1

1   000e:3b33:30e5 08ea:4476:5117 864  2   a0af* 7928* -1       240630   3571       1

2   000e:3b33:3a6c 08ea:4476:3e15 864  10  a40a* 2c62* -1       21301    3600       1

3   000e:3b33:3365 08ea:446b:f717 864  10  05f6* 72e7* -1       21667    3594       1

4   000e:3b33:30b8 08ea:4476:4fd4 864  10  c84f* bdae* -1       24508    3573       0

5   000e:3b33:3a66 08ea:4476:5057 864  10  8579* 5838* -1       24337    3564       1
```

- OKC is not an official fast secure roaming standard.

- Most enterprise WLAN vendors support OKC.

- However, many clients do not support OKC.
  - Example: iOS clients never supported OKC.

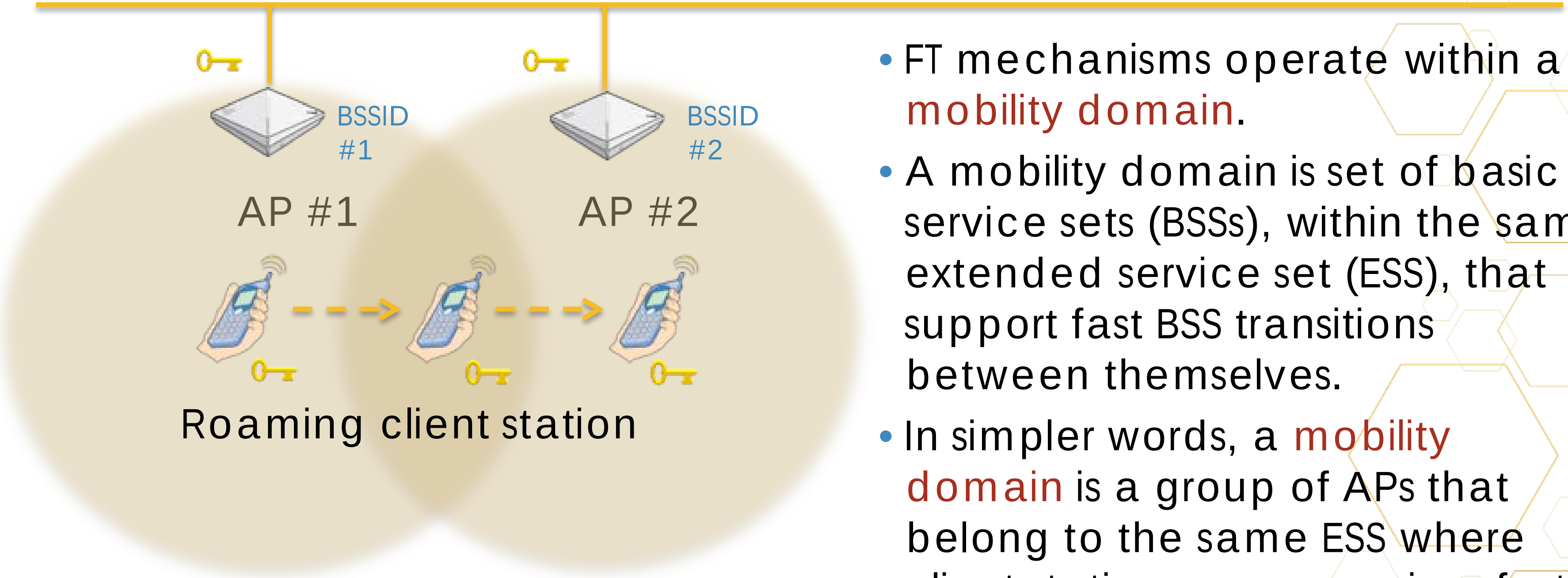
Fast BSS Transition (FT)

- The 802.11r-2008 amendment is known as the fast basic service set transition (FT) amendment.

- The main difference between OKC and FT is that the 802.11r-2008 amendment fully defined the key hierarchy used when creating cached keys.

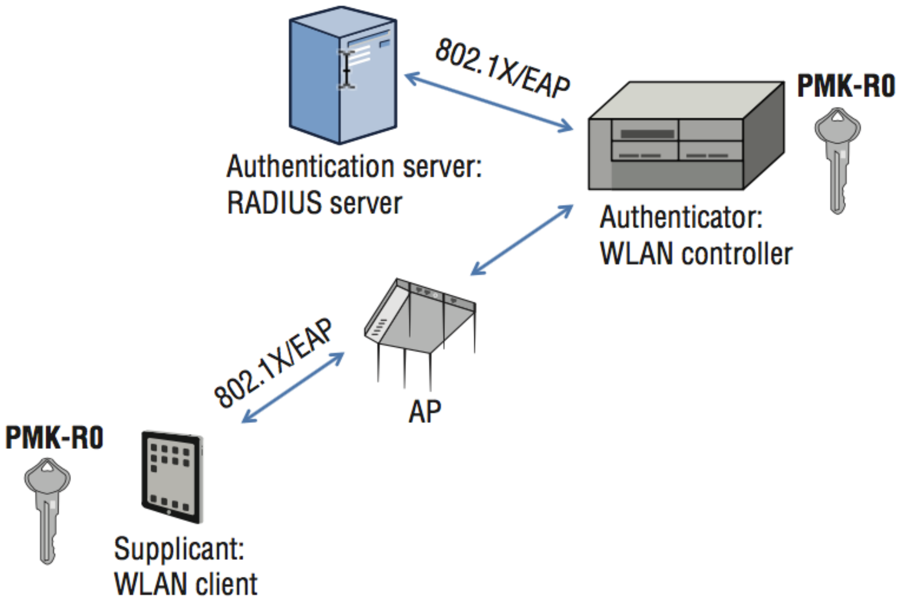
- The fast BSS transition mechanisms originally defined in the 802.11r-2008 amendment are now found in clause 12 of the 802.11-2012 standard.

Fast BSS Transition (FT)



- FT mechanisms operate within a mobility domain.
- A mobility domain is set of basic service sets (BSSs), within the same extended service set (ESS), that support fast BSS transitions between themselves.
- In simpler words, a mobility domain is a group of APs that belong to the same ESS where client stations can roam in a fast and secure manner.

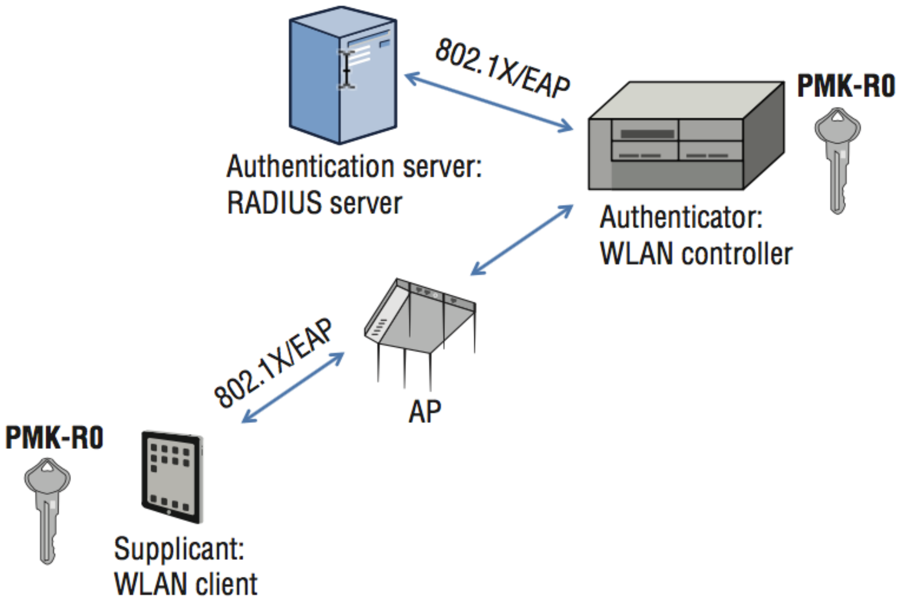
Fast BSS Transition (FT)



- The first time a client station enters a mobility domain, the client will associate with an AP and perform an initial 802.1X/EAP authentication.

- From that point forward, as the client station roams between APs, the client will be using fast BSS transitions.

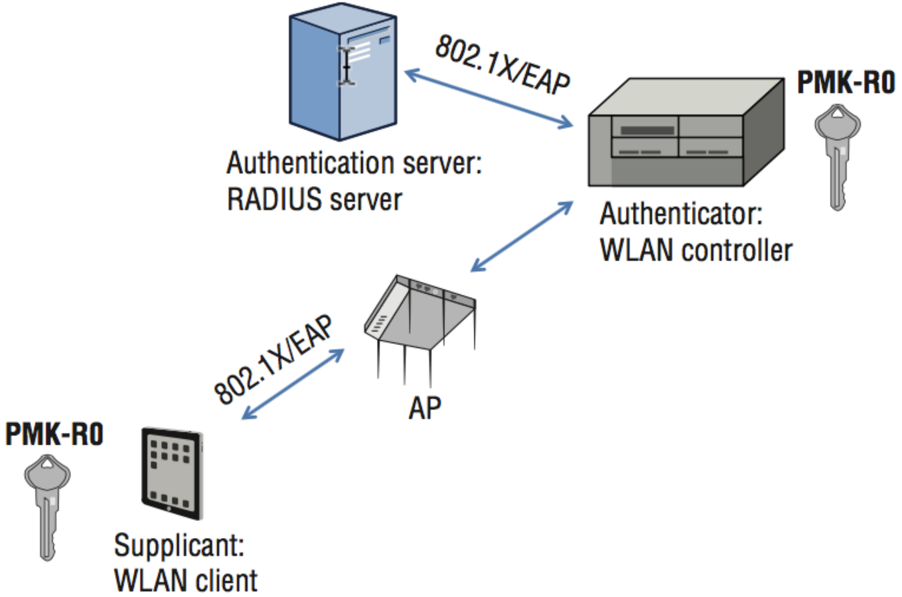
Fast BSS Transition (FT)



- FT uses the 802.1X/EAP exchange to create the master session key which seeds a multi-tiered key management solution.

- After the supplicant and the RADIUS server exchange credentials, a first-level pairwise master is created.

Fast BSS Transition (FT)



- The first-level pairwise master is called the PMK-RO key and is sent to the authenticator and the WLAN client.

- Depending on the WLAN architecture, the 802.1X/EAP authenticator can either be an AP or a WLAN controller.

Fast BSS Transition (FT)

Fast BSS transition uses a three-level key hierarchy:

Pairwise Master Key R0 (PMK-R0) The first-level key of the FT key hierarchy. This key is derived from the master session key (MSK).

Pairwise Master Key R1 (PMK-R1) The second-level key of the FT key hierarchy.

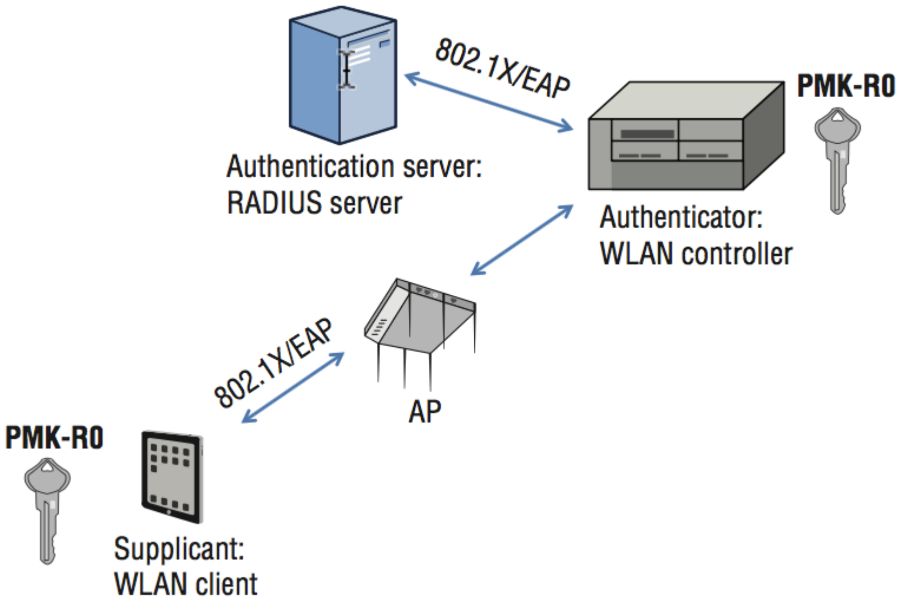
Pairwise Transient Key (PTK) The third-level key of the FT key hierarchy. The PTK is the final key used to encrypt 802.11 data frames.

Fast BSS Transition (FT)

Fast BSS transition also assigns different roles to different devices. Each device is assigned a *key holder* role to manage one or more of the multiple keys used in the FT key hierarchy.

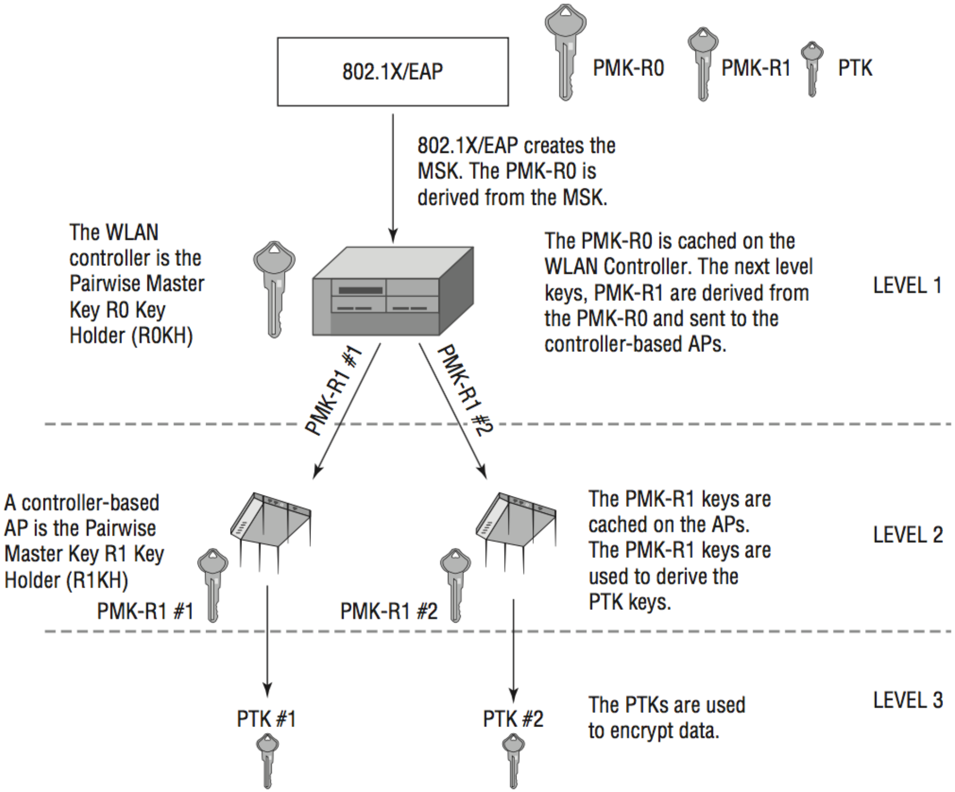
Device	Key holder role
Original AP or WLAN controller	Pairwise master key (PMK) R0 key holder (R0KH)
Access point	Pairwise master key (PMK) R1 key holder (R1KH)
Client station	Pairwise master key (PMK) S0 key holder (S0KH)
Client station	Pairwise master key (PMK) S1 key holder (S1KH)

Fast BSS Transition (FT)



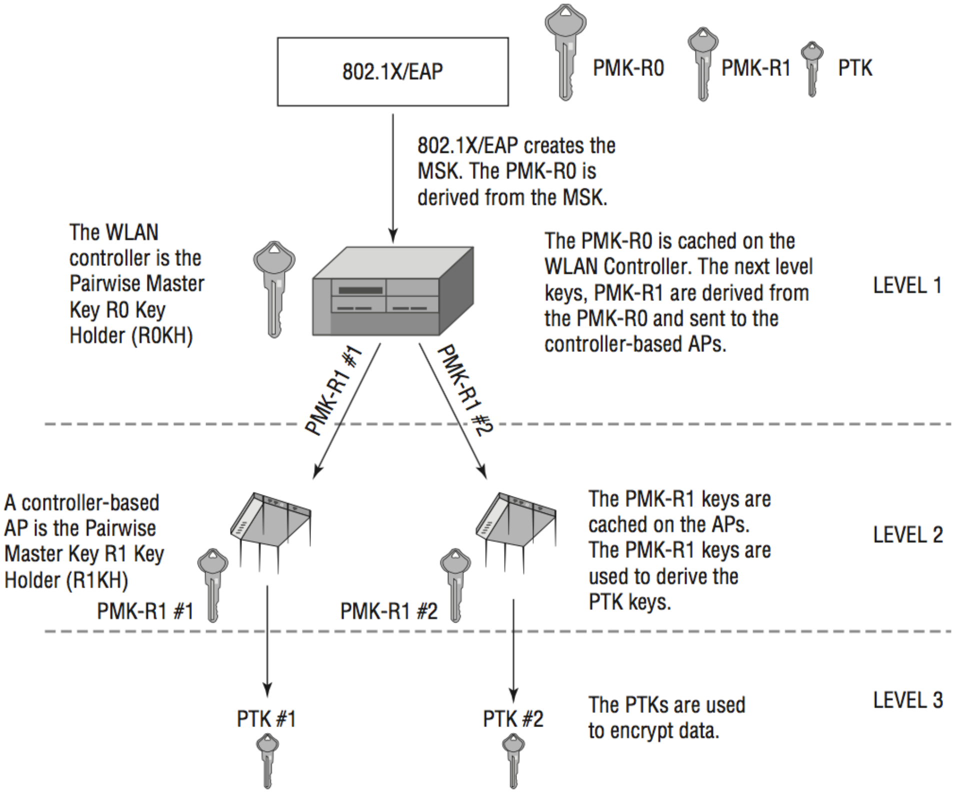
- The various levels of FT keys are derived and stored in different WLAN devices depending on the WLAN architecture that has been deployed.
- For example, in a controller-less environment, the first level PMK-R0 key is created and cached on an access point.
- In an environment where WLAN controllers are deployed, the first level PMK-R0 key is created and cached on a WLAN controller.

FT Key hierarchy


802.1X/EAP
PMK-R0
PMK-R1
PTK
802.1X/EAP creates the MSK. The PMK-R0 is derived from the MSK.
The WLAN controller is the Pairwise Master Key R0 Key Holder (R0KH)
The PMK-R0 is cached on the WLAN Controller. The next level keys, PMK-R1 are derived from the PMK-R0 and sent to the controller-based APs.
LEVEL 1
PMK-R1 #1
PMK-R1 #2
A controller-based AP is the Pairwise Master Key R1 Key Holder (R1KH)
PMK-R1 #1
PMK-R1 #2
The PMK-R1 keys are cached on the APs. The PMK-R1 keys are used to derive the PTK keys.
LEVEL 2
PTK #1
PTK #2
The PTKs are used to encrypt data.
LEVEL 3

- The various levels of FT keys are derived and stored in different WLAN devices depending on the WLAN architecture that has been deployed.
- For example, in a controller-less environment, the first level PMK-R0 key is created and cached on an access point.
- In an environment where WLAN controllers are deployed, the first level PMK-R0 key is created and cached on a WLAN controller.

FT Key hierarchy: WLAN controller infrastructure



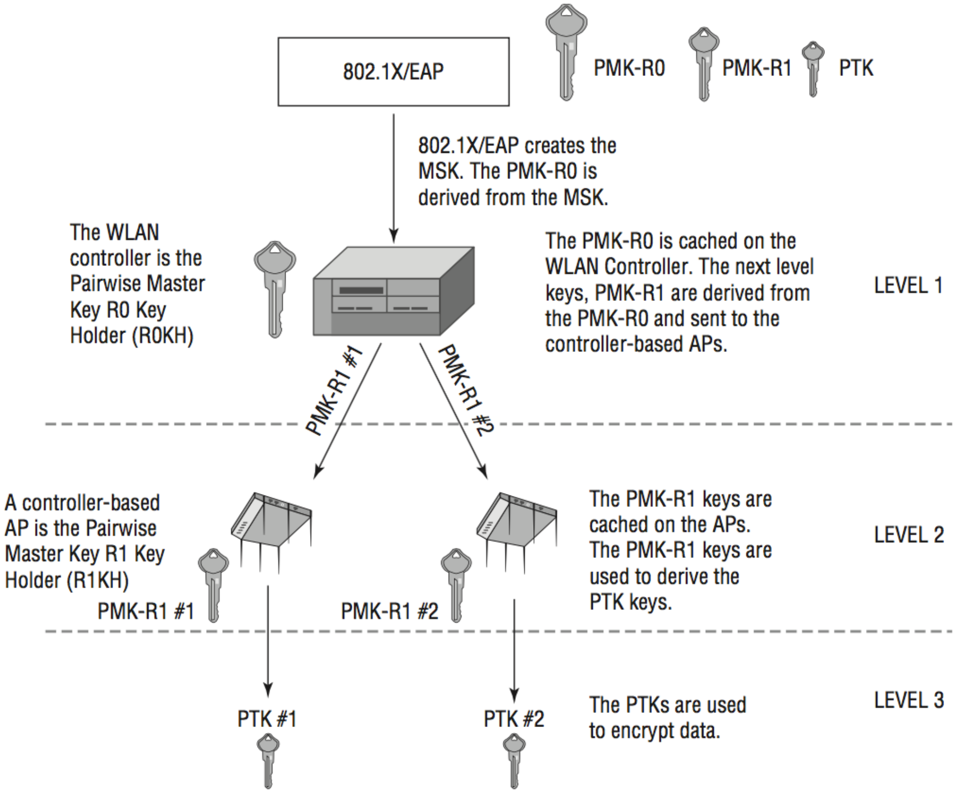
802.1X/EAP
PMK-R0
PMK-R1
PTK
802.1X/EAP creates the MSK. The PMK-R0 is derived from the MSK.
The WLAN controller is the Pairwise Master Key R0 Key Holder (R0KH)
The PMK-R0 is cached on the WLAN Controller. The next level keys, PMK-R1 are derived from the PMK-R0 and sent to the controller-based APs.
LEVEL 1
PMK-R1 #1
PMK-R1 #2
A controller-based AP is the Pairwise Master Key R1 Key Holder (R1KH)
The PMK-R1 keys are cached on the APs. The PMK-R1 keys are used to derive the PTK keys.
LEVEL 2
PMK-R1 #1
PMK-R1 #2
PTK #1
PTK #2
The PTKs are used to encrypt data.
LEVEL 3

- The PMK-R0 is created and cached on the WLAN controller. The WLAN controller is the key holder for the first-level key.

- The second-level PMK-R1 keys are derived from the PMK-R0 and sent from the WLAN controller to the controller-based APs.

- The PMK-R1 keys are cached on the APs.

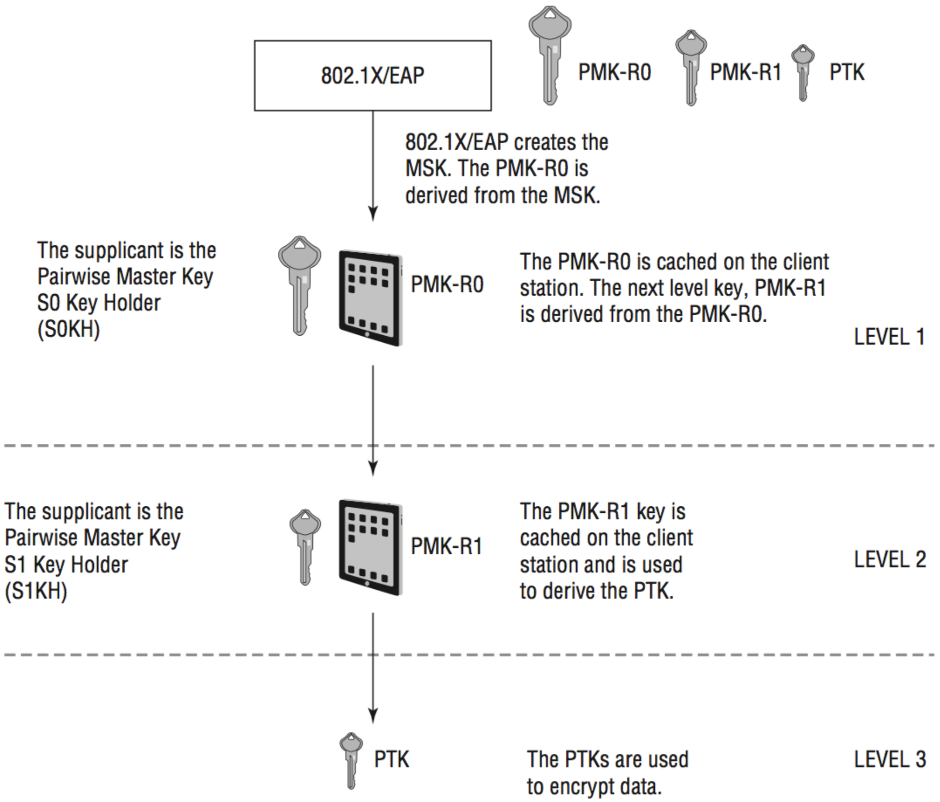
FT Key hierarchy: WLAN controller infrastructure



802.1X/EAP
PMK-R0
PMK-R1
PTK
802.1X/EAP creates the MSK. The PMK-R0 is derived from the MSK.
The WLAN controller is the Pairwise Master Key R0 Key Holder (R0KH)
The PMK-R0 is cached on the WLAN Controller. The next level keys, PMK-R1 are derived from the PMK-R0 and sent to the controller-based APs.
LEVEL 1
PMK-R1 #1
PMK-R1 #2
A controller-based AP is the Pairwise Master Key R1 Key Holder (R1KH)
The PMK-R1 keys are cached on the APs. The PMK-R1 keys are used to derive the PTK keys.
LEVEL 2
PMK-R1 #1
PMK-R1 #2
PTK #1
PTK #2
The PTKs are used to encrypt data.
LEVEL 3

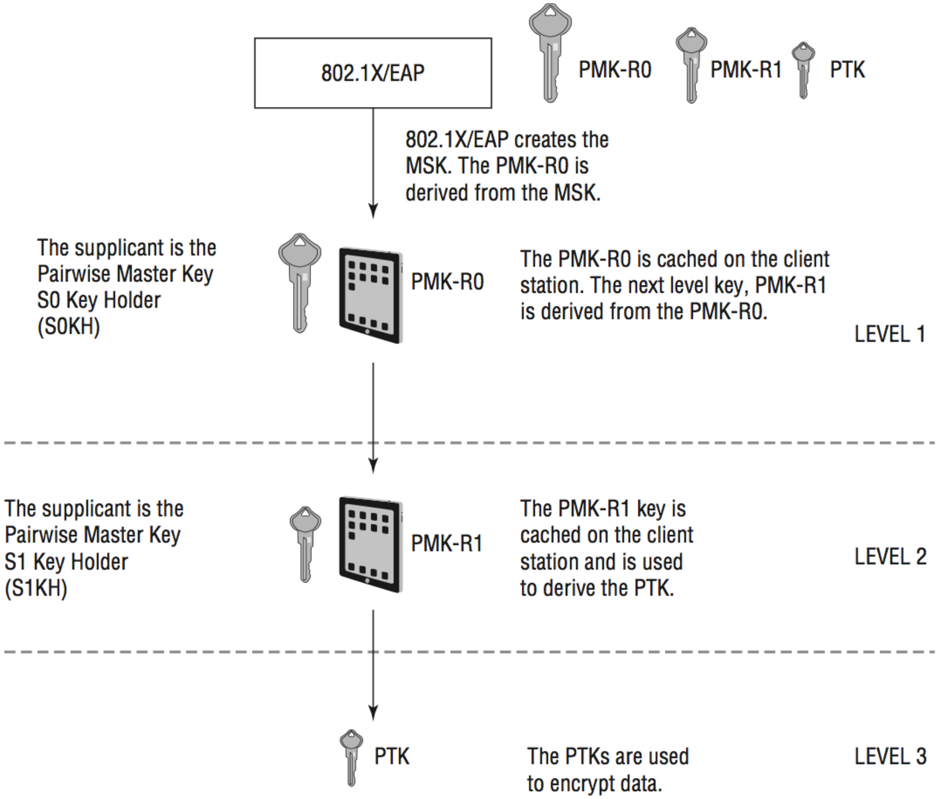
- The access points are the key holders for the PMK-R1 keys.
- The PMK-R1 keys are used to derive the PTKs, which are used to encrypt 802.11 data frames.

FT Key hierarchy: Supplicant


802.1X/EAP
PMK-R0
PMK-R1
PTK
802.1X/EAP creates the MSK. The PMK-R0 is derived from the MSK.
The supplicant is the Pairwise Master Key S0 Key Holder (S0KH)
PMK-R0
The PMK-R0 is cached on the client station. The next level key, PMK-R1 is derived from the PMK-R0.
LEVEL 1
The supplicant is the Pairwise Master Key S1 Key Holder (S1KH)
PMK-R1
The PMK-R1 key is cached on the client station and is used to derive the PTK.
LEVEL 2
PTK
The PTKs are used to encrypt data.
LEVEL 3

- The various levels of FT keys are also derived and stored on the client station.
- The PMK-R0 is cached on the supplicant, which is the client station.
- The client station is the key holder for the first-level key.

FT Key hierarchy: Supplicant



802.1X/EAP

PMK-R0

PMK-R1

PTK

802.1X/EAP creates the MSK. The PMK-R0 is derived from the MSK.

The supplicant is the Pairwise Master Key S0 Key Holder (S0KH)

PMK-R0

The PMK-R0 is cached on the client station. The next level key, PMK-R1 is derived from the PMK-R0.

LEVEL 1

The supplicant is the Pairwise Master Key S1 Key Holder (S1KH)

PMK-R1

The PMK-R1 key is cached on the client station and is used to derive the PTK.

LEVEL 2

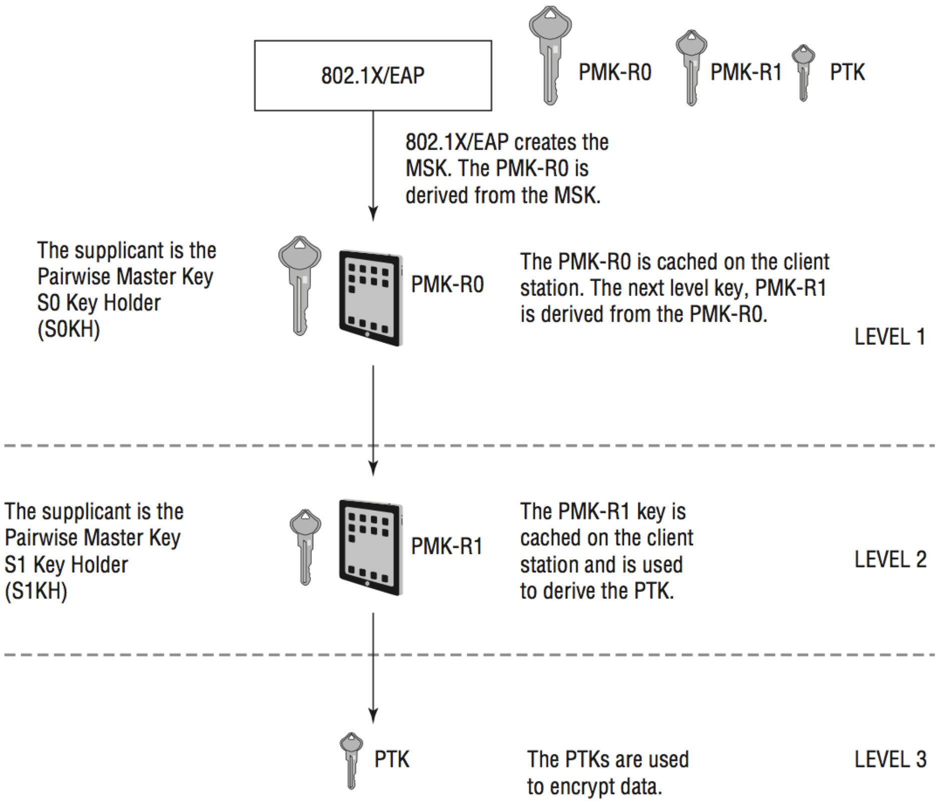
PTK

The PTKs are used to encrypt data.

LEVEL 3

- The client station derives the second-level key, PMK-R1, from the PMK-R0.
- The PMK-R1 key is cached on the client station.
- The supplicants are the key holders for the PMK-R1 keys.

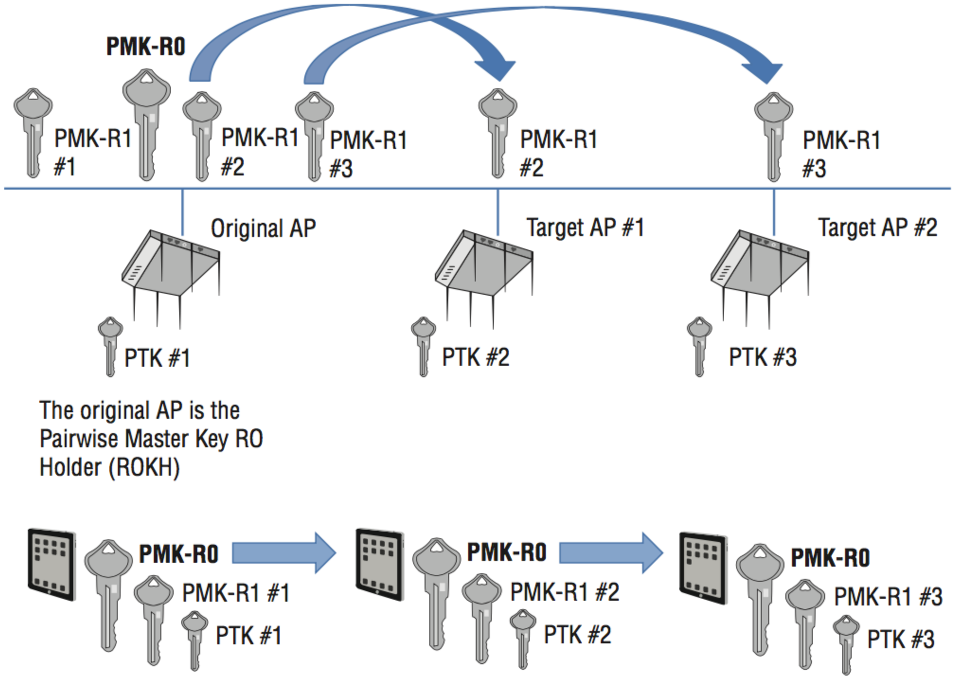
FT Key hierarchy: Supplicant


802.1X/EAP
PMK-R0
PMK-R1
PTK
802.1X/EAP creates the MSK. The PMK-R0 is derived from the MSK.
The supplicant is the Pairwise Master Key S0 Key Holder (S0KH)
PMK-R0
The PMK-R0 is cached on the client station. The next level key, PMK-R1 is derived from the PMK-R0.
LEVEL 1
The supplicant is the Pairwise Master Key S1 Key Holder (S1KH)
PMK-R1
The PMK-R1 key is cached on the client station and is used to derive the PTK.
LEVEL 2
PTK
The PTKs are used to encrypt data.
LEVEL 3

- The PMK-R1 key is cached on the client station.

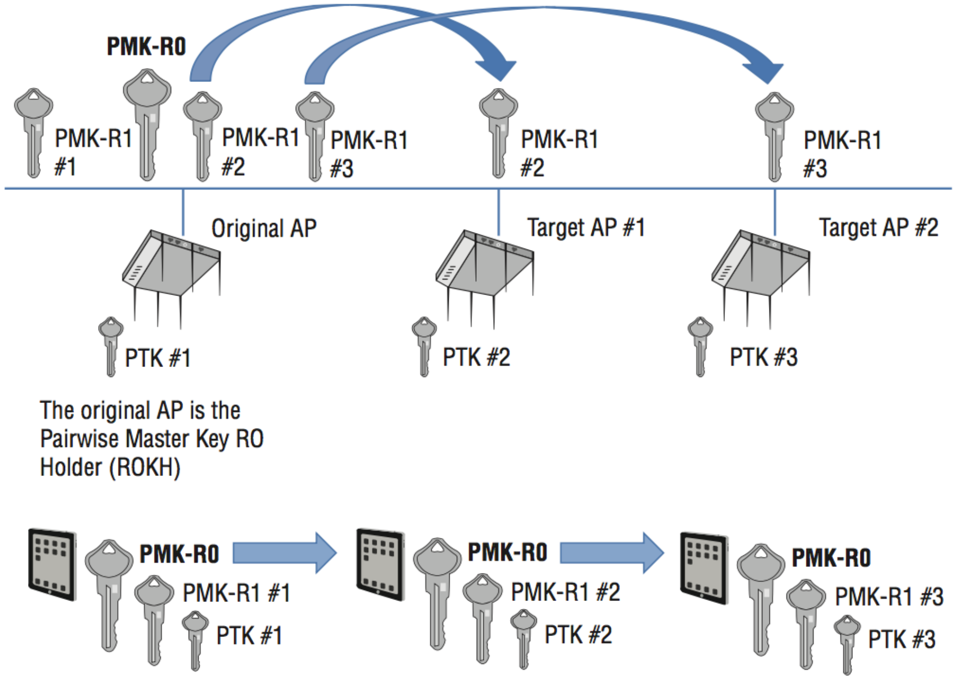
- The PMK-R1 keys are used to derive the PTKs, which are used to encrypt unicast 802.11 data frames.

FT Key hierarchy: Distributed AP architecture



- The 802.1X/EAP exchange creates the master session key (MSK). The MSK is used to create the first-level master key, PMK-R0.
- The PMK-R0 is created and cached on an AP where the client first associates.
- The original AP is the key holder for the first-level key.

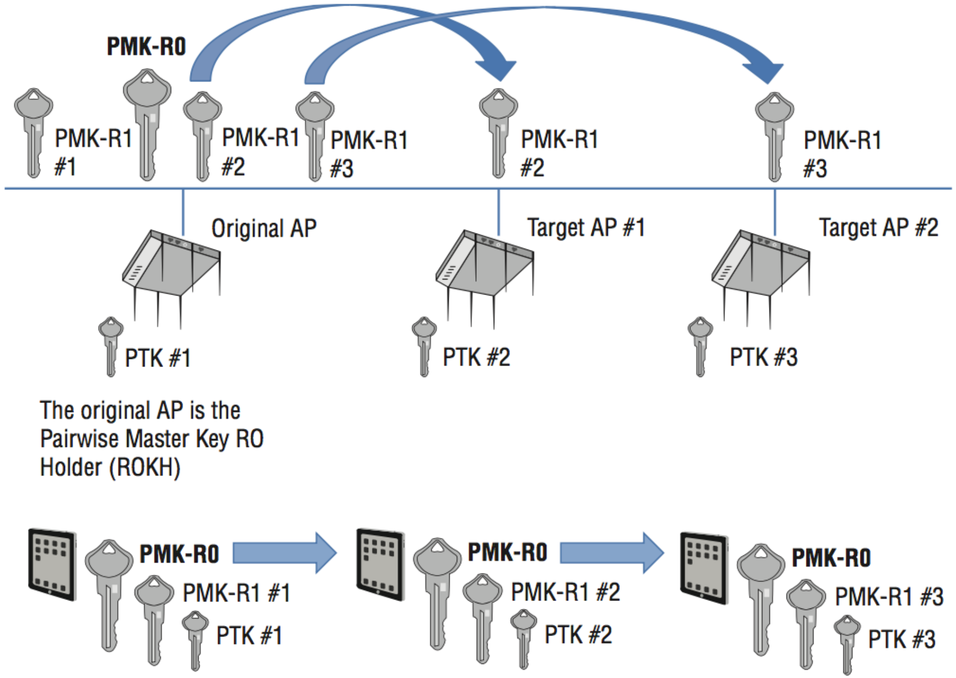
FT Key hierarchy: Distributed AP architecture



- The second-level PMK-R1 keys are derived from the PMK-R0 and sent from the original AP to other target APs over a secure channel.

- How the PMK-R1 keys are securely distributed is outside of the scope of the 802.11-2012 standard.

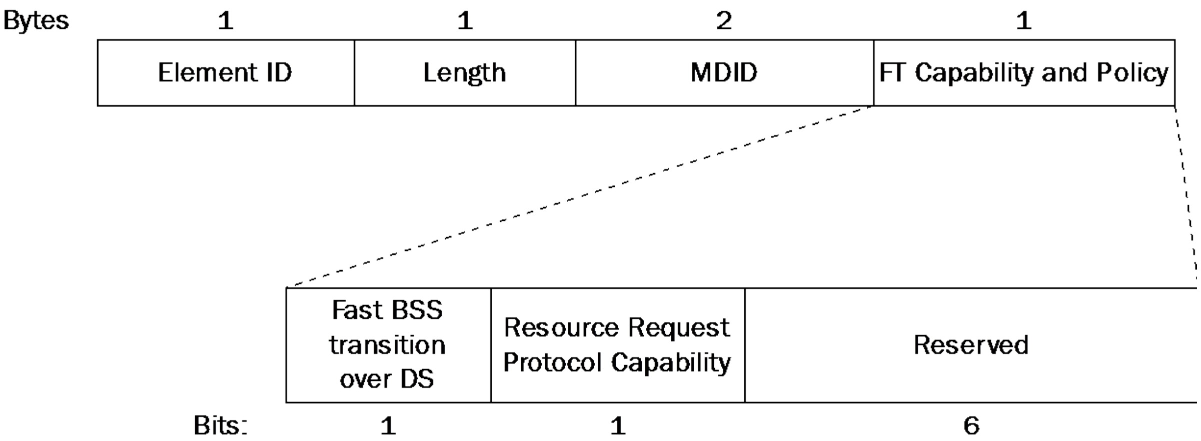
FT Key hierarchy: Distributed AP architecture



The original AP is the Pairwise Master Key R0 Holder (R0KH)

- The PMK-R1 keys are cached on the target APs, which are the key holders for the PMK-R1 keys.
- The PMK-R1 keys are used to derive the PTKs, which are used to encrypt unicast 802.11 data frames.

Mobility Domain Information Element

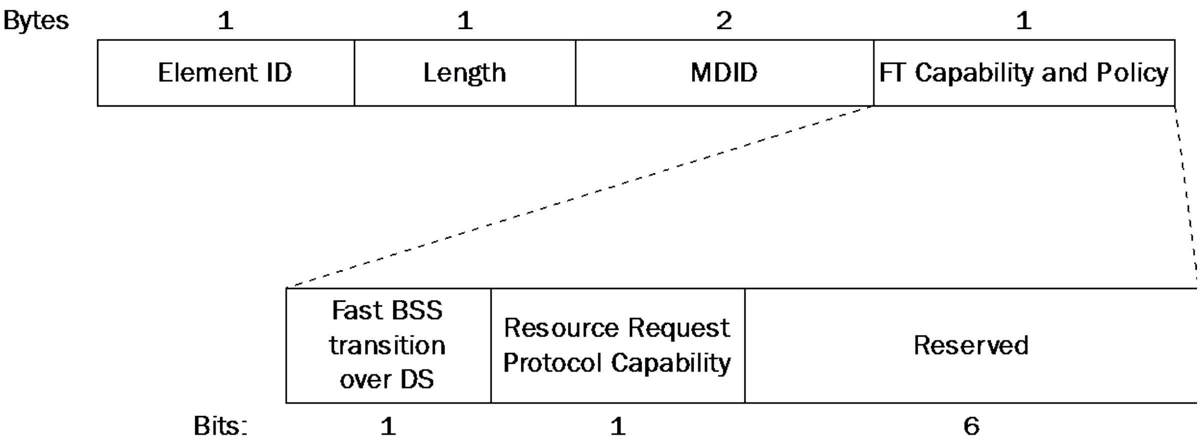


Bytes	1	1	2	1
	Element ID	Length	MDID	FT Capability and Policy

	Fast BSS transition over DS	Resource Request Protocol Capability	Reserved
Bits:	1	1	6

- The mobility domain information element (MDIE) is used to indicate the existence of a mobility domain as well as the method of fast BSS transition.
- The mobility domain identifier (MDID) field is the unique identifier of the group of APs that constitute a mobility domain.

Mobility Domain Information Element



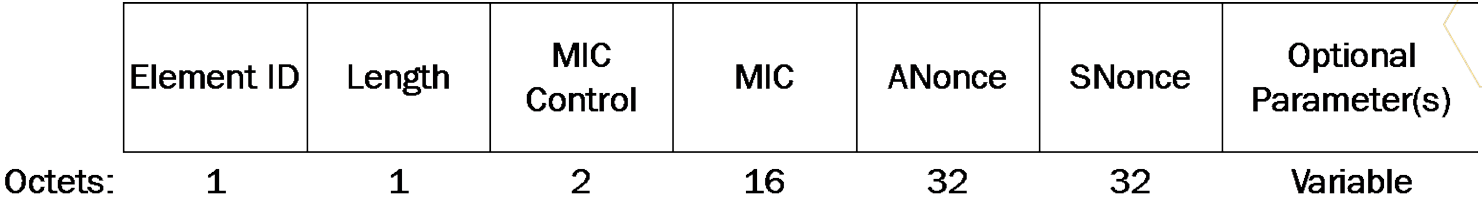
Bytes	1	1	2	1
	Element ID	Length	MDID	FT Capability and Policy

	Fast BSS transition over DS	Resource Request Protocol Capability	Reserved
Bits:	1	1	6

- The FT capability and Policy field is used to indicate whether over-the-air or over-the-DS fast BSS transition is to be performed.

- We will discuss the difference between over-the-air and over-the-DS fast BSS transition later in this module.

Fast BSS Transition Information Element

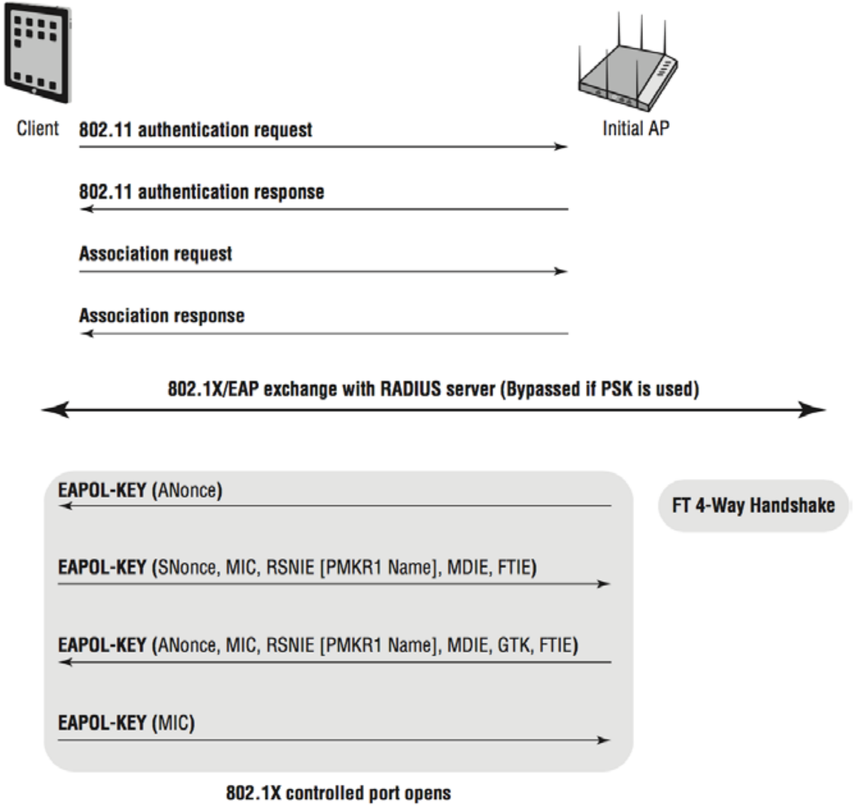


	Element ID	Length	MIC Control	MIC	ANonce	SNonce	Optional Parameter(s)
Octets:	1	1	2	16	32	32	Variable

- The fast BSS transition information element (FTIE) includes information needed to perform the FT authentication sequence during a fast BSS transition.

- Notice that some of the fields look very similar to the information used during a typical 4-Way Handshake exchange.

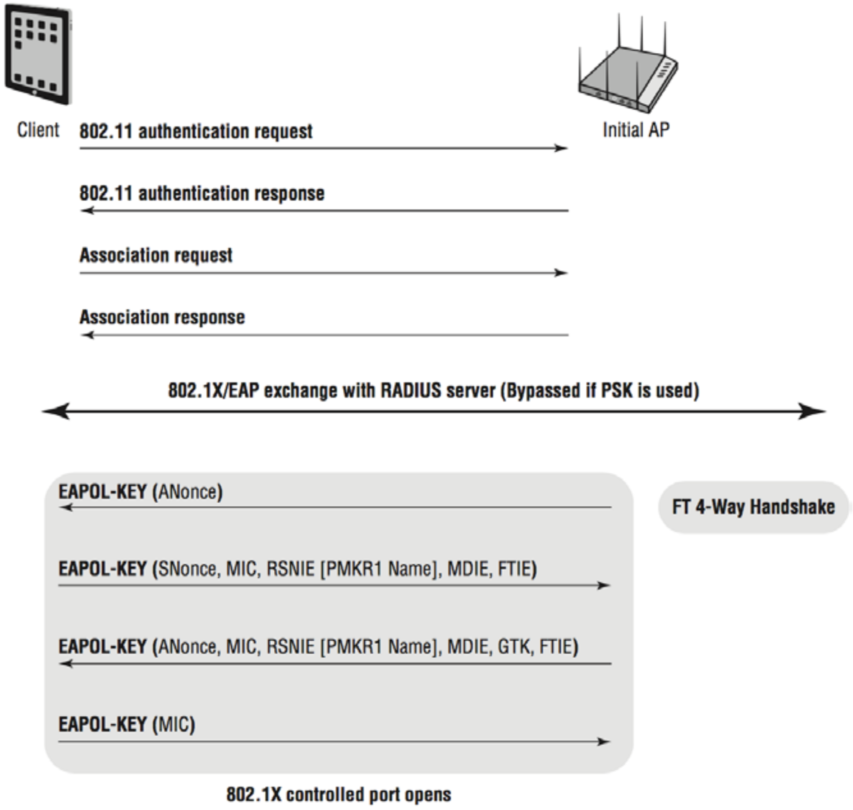
FT Initial Mobility Domain Association



Client
Initial AP
802.11 authentication request
802.11 authentication response
Association request
Association response
802.1X/EAP exchange with RADIUS server (Bypassed if PSK is used)
EAPOL-KEY (ANonce)
FT 4-Way Handshake
EAPOL-KEY (SNonce, MIC, RSNIE [PMKR1 Name], MDIE, FTIE)
EAPOL-KEY (ANonce, MIC, RSNIE [PMKR1 Name], MDIE, GTK, FTIE)
EAPOL-KEY (MIC)
802.1X controlled port opens

- The FT initial mobility domain association is the first association in the mobility domain.
- Open System authentication request/response frames with the first AP.
- The client station and AP then use the MDIE and FTIE information in the association request/response frames to indicate future use of the FT procedures.

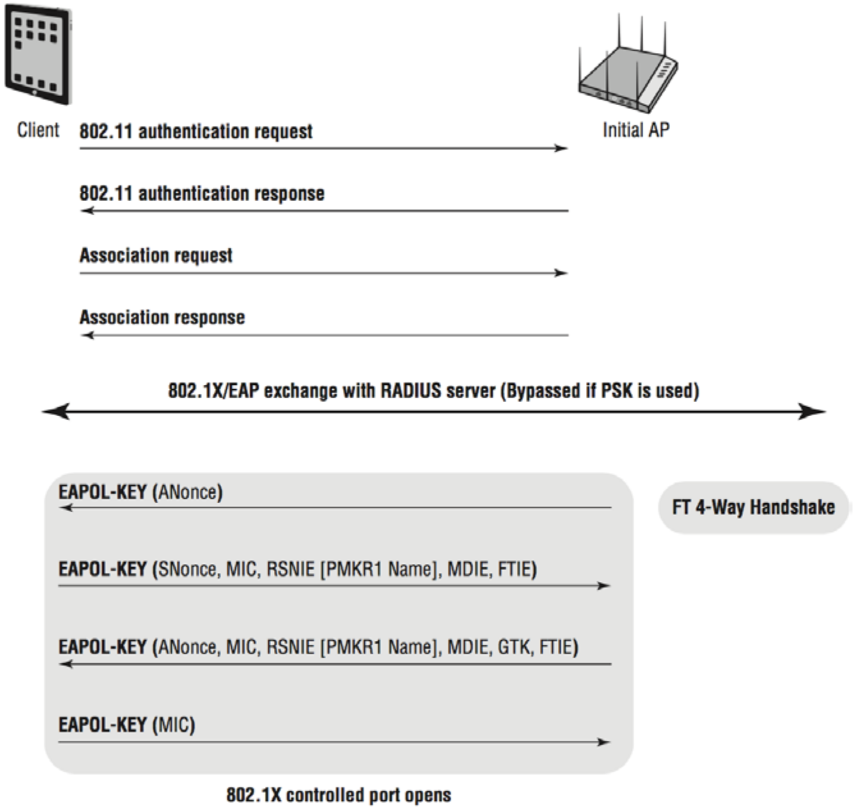
FT Initial Mobility Domain Association



Client
Initial AP
802.11 authentication request
802.11 authentication response
Association request
Association response
802.1X/EAP exchange with RADIUS server (Bypassed if PSK is used)
EAPOL-KEY (ANonce)
EAPOL-KEY (SNonce, MIC, RSNIE [PMKR1 Name], MDIE, FTIE)
EAPOL-KEY (ANonce, MIC, RSNIE [PMKR1 Name], MDIE, GTK, FTIE)
EAPOL-KEY (MIC)
FT 4-Way Handshake
802.1X controlled port opens

- The PTK and GTK encryption keys are created during the FT 4-Way Handshake and the 802.1X/EAP controlled port is unblocked.
- The original 802.1X/EAP exchange also creates the master session key (MSK) that is used for the FT key hierarchy.

FT Initial Mobility Domain Association

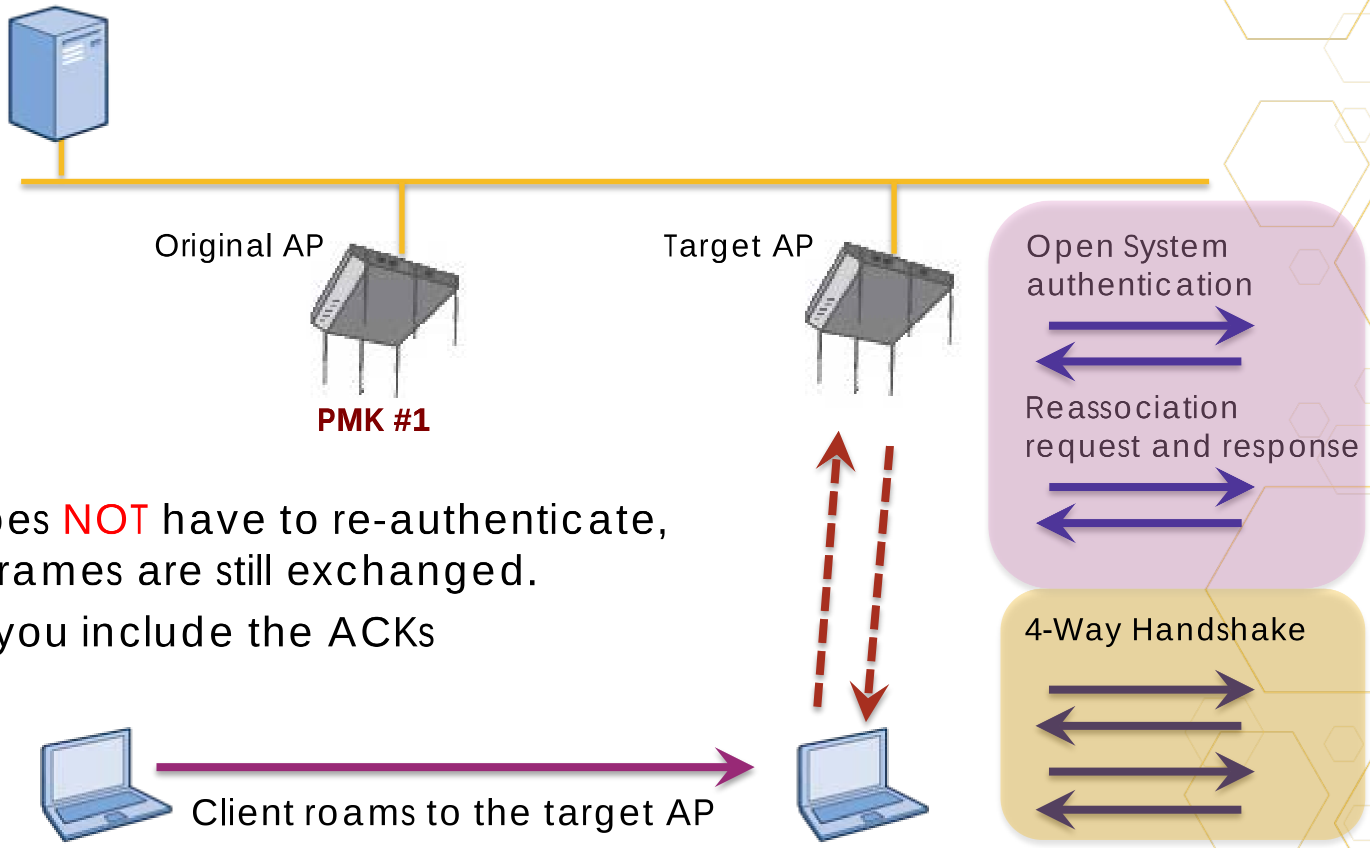


Client
Initial AP
802.11 authentication request
802.11 authentication response
Association request
Association response
802.1X/EAP exchange with RADIUS server (Bypassed if PSK is used)
EAPOL-KEY (ANonce)
EAPOL-KEY (SNonce, MIC, RSNIE [PMKR1 Name], MDIE, FTIE)
EAPOL-KEY (ANonce, MIC, RSNIE [PMKR1 Name], MDIE, GTK, FTIE)
EAPOL-KEY (MIC)
FT 4-Way Handshake
802.1X controlled port opens

- The FT initial mobility domain association is not much different than any initial association used by clients that do not support fast BSS transition.

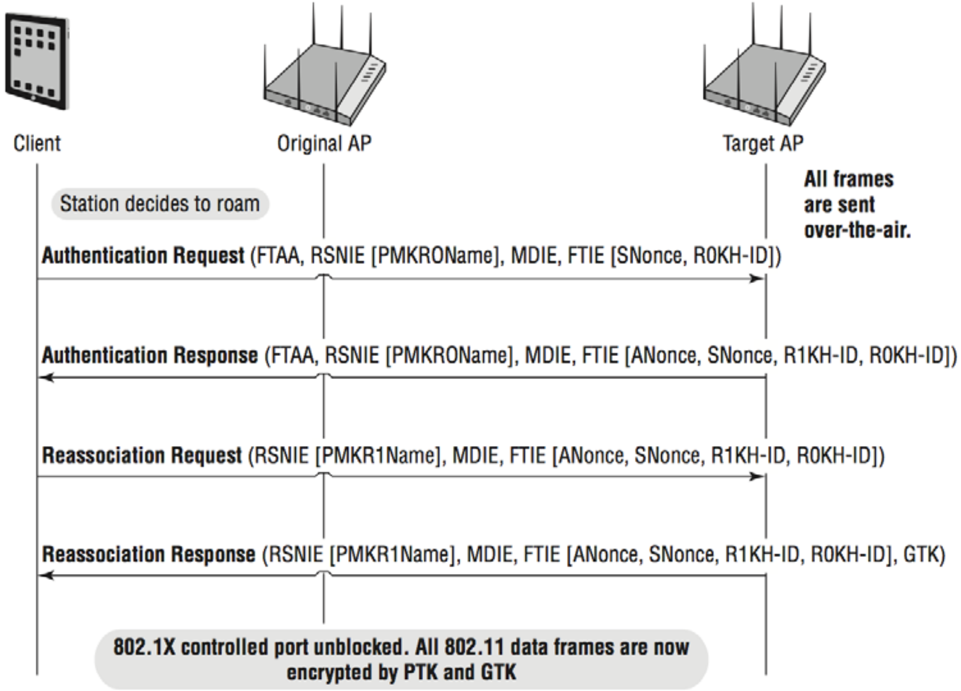
- The main difference is that extra information, such as the MDIE and FTIE, is communicated during an FT initial mobility domain association.

Non-FT roaming


Original AP
PMK #1
Target AP
Open System authentication
Reassociation request and response
4-Way Handshake
Client roams to the target AP

- If a client does NOT have to re-authenticate, a total of 8 frames are still exchanged.
- 16 frames if you include the ACKs

Over-the-Air Fast BSS Transition



Authentication Request (FTAA, RSNIE [PMKR0Name], MDIE, FTIE [SNonce, R0KH-ID])

Authentication Response (FTAA, RSNIE [PMKR0Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])

Reassociation Request (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])

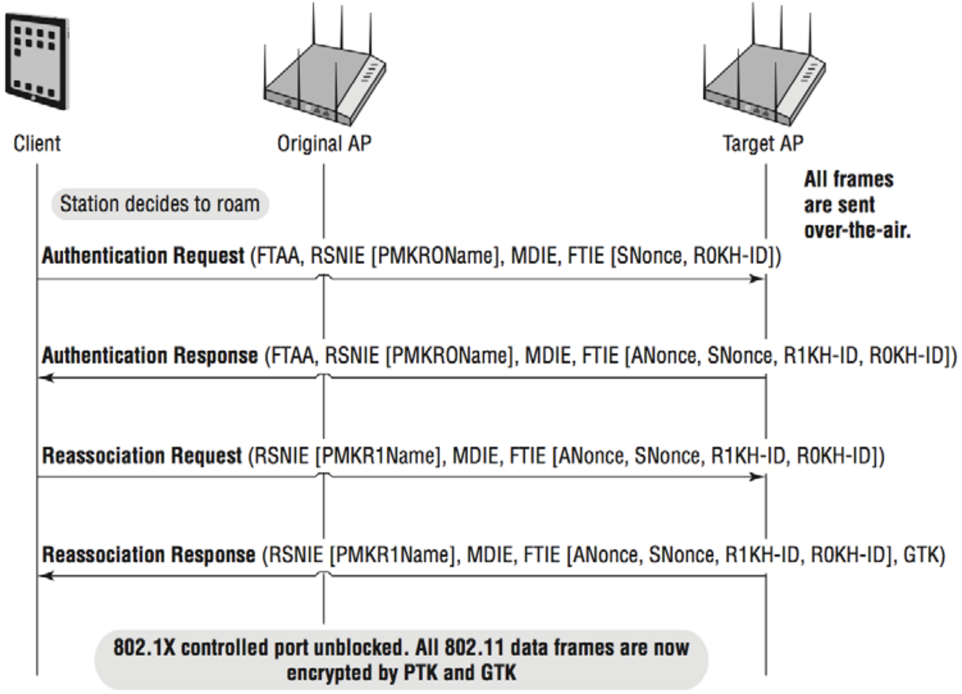
Reassociation Response (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID], GTK)

802.1X controlled port unblocked. All 802.11 data frames are now encrypted by PTK and GTK

- The FT process defines a more efficient method that effectively combines the initial Open System authentication and reassociation frames with the 4-Way Handshake frames.

- In other words, four fewer frames are needed when a client roams, thus speeding up the roaming process.

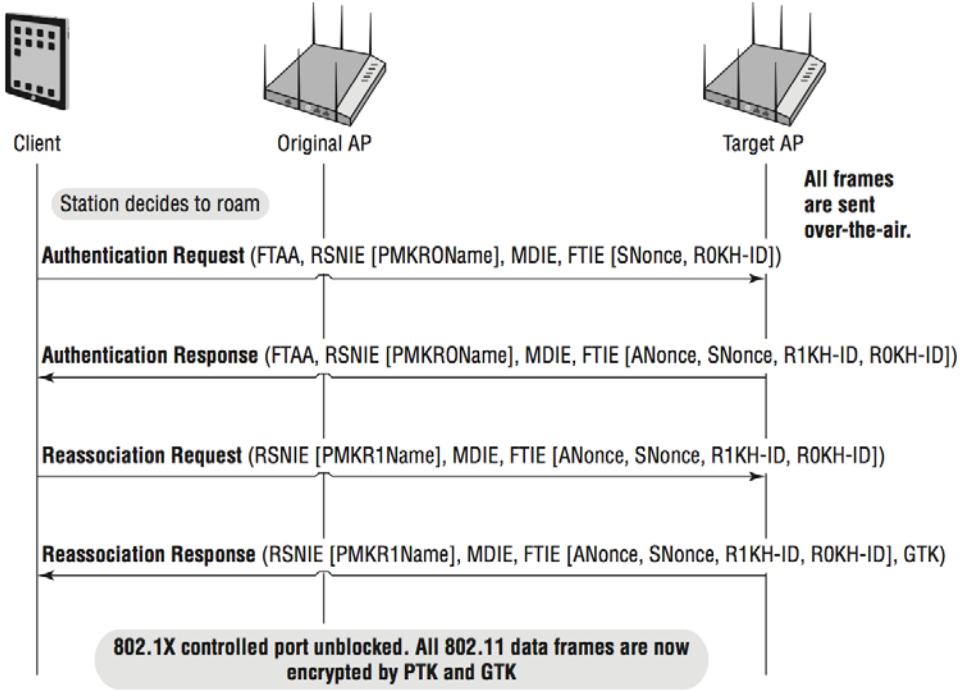
Over-the-Air Fast BSS Transition


Client
Original AP
Target AP
All frames are sent over-the-air.
Station decides to roam
Authentication Request (FTAA, RSNIE [PMKR0Name], MDIE, FTIE [SNonce, R0KH-ID])
Authentication Response (FTAA, RSNIE [PMKR0Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])
Reassociation Request (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])
Reassociation Response (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID], GTK)
802.1X controlled port unblocked. All 802.11 data frames are now encrypted by PTK and GTK

- An FT protocol frame exchange is used to initiate the roaming exchange *and* create dynamic encryption keys.

- Note that the authentication request/response frames and reassociation request/response frames carry an FT authentication algorithm(FTAA) along with nonces and other information needed to create the final dynamic keys.

Over-the-Air Fast BSS Transition



Client

Original AP

Target AP

All frames are sent over-the-air.

Station decides to roam

Authentication Request (FTAA, RSNIE [PMKROName], MDIE, FTIE [SNonce, R0KH-ID])

Authentication Response (FTAA, RSNIE [PMKROName], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])

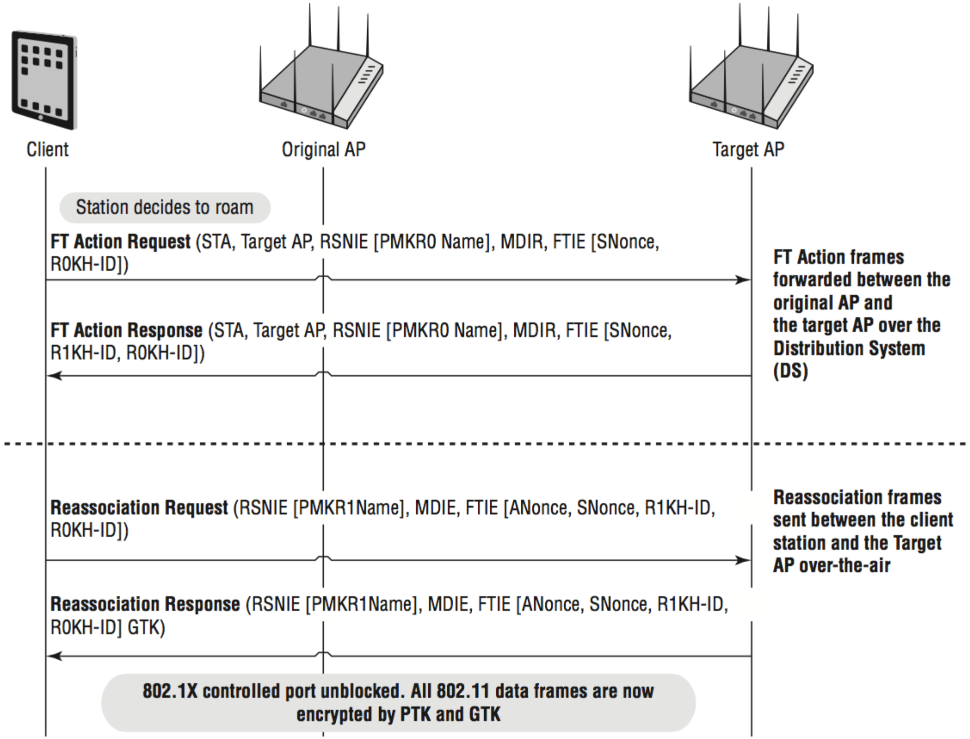
Reassociation Request (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])

Reassociation Response (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID], GTK)

802.1X controlled port unblocked. All 802.11 data frames are now encrypted by PTK and GTK

- This process is known as over-the-air fast BSS transition.
- The client station communicates directly with the target AP using standard 802.11 authentication with the FT authentication algorithm.
- The PMK-R1 key is the seeding material for the over-the-air fast BSS transition process that creates the final pairwise transient key (PTK).

Over-the-DS Fast BSS Transition



Client

Original AP

Target AP

Station decides to roam

FT Action Request (STA, Target AP, RSNIE [PMKR0 Name], MDIR, FTIE [SNonce, R0KH-ID])

FT Action Response (STA, Target AP, RSNIE [PMKR0 Name], MDIR, FTIE [SNonce, R1KH-ID, R0KH-ID])

FT Action frames forwarded between the original AP and the target AP over the Distribution System (DS)

Reassociation Request (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])

Reassociation Response (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID] GTK)

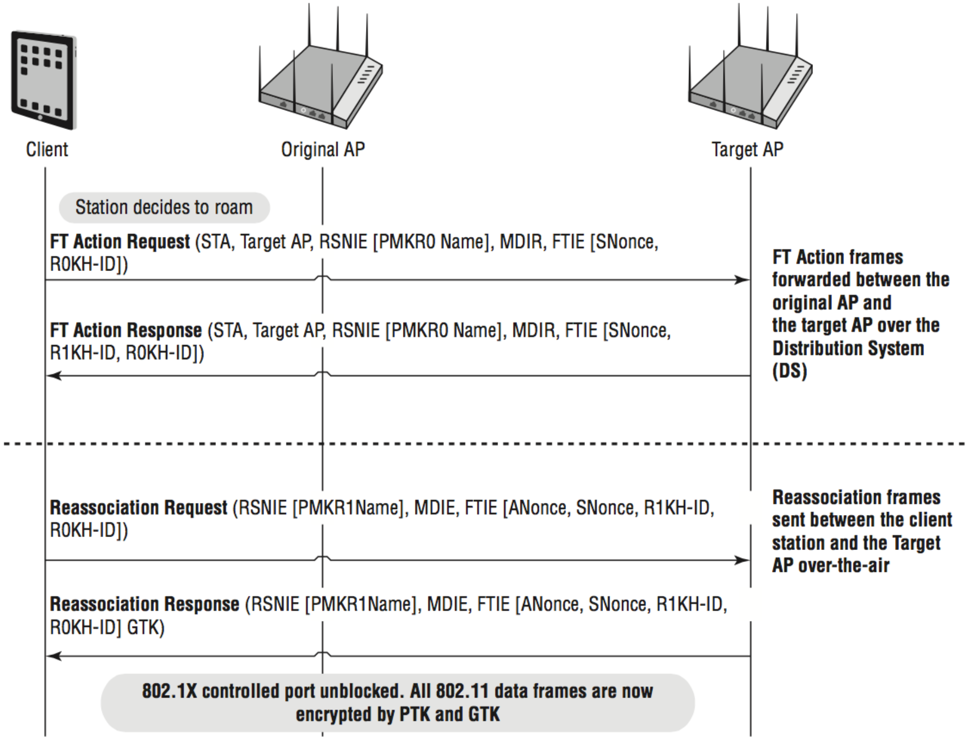
Reassociation frames sent between the client station and the Target AP over-the-air

802.1X controlled port unblocked. All 802.11 data frames are now encrypted by PTK and GTK

- An alternative to the FT method is over-the-DS fast BSS transition, which requires the use of FT Action frames to complete the PTK creation process.

- The over-the-DS process uses the FT Action frames over the wired 802.3 infrastructure.

Over-the-DS Fast BSS Transition



Station decides to roam

FT Action Request (STA, Target AP, RSNIE [PMKR0 Name], MDIR, FTIE [SNonce, R0KH-ID])

FT Action Response (STA, Target AP, RSNIE [PMKR0 Name], MDIR, FTIE [SNonce, R1KH-ID, R0KH-ID])

FT Action frames forwarded between the original AP and the target AP over the Distribution System (DS)

Reassociation Request (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])

Reassociation Response (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID] GTK)

Reassociation frames sent between the client station and the Target AP over-the-air

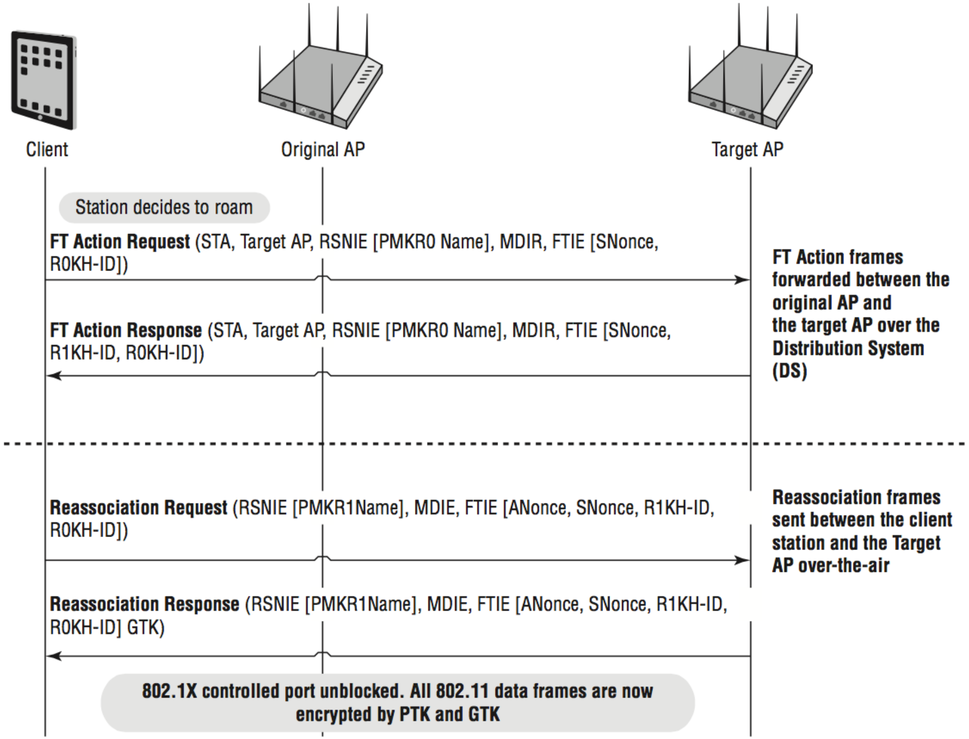
802.1X controlled port unblocked. All 802.11 data frames are now encrypted by PTK and GTK

- The client station sends an FT Action request frame to the target AP via the original AP.

- The FT Action request frame frame is forwarded over the distribution system (DS), which is the wired infrastructure.

- The target AP responds back to the client station over the DS with an FT Action response frame.

Over-the-DS Fast BSS Transition



Station decides to roam

FT Action Request (STA, Target AP, RSNIE [PMKR0 Name], MDIR, FTIE [SNonce, R0KH-ID])

FT Action Response (STA, Target AP, RSNIE [PMKR0 Name], MDIR, FTIE [SNonce, R1KH-ID, R0KH-ID])

FT Action frames forwarded between the original AP and the target AP over the Distribution System (DS)

Reassociation Request (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])

Reassociation Response (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID] GTK)

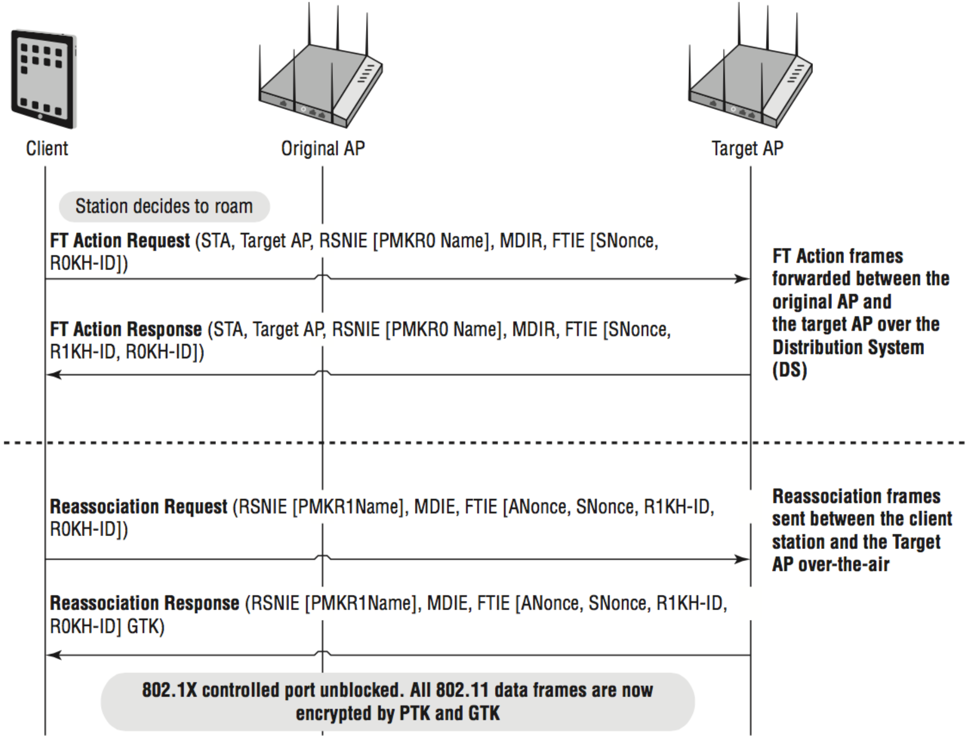
Reassociation frames sent between the client station and the Target AP over-the-air

802.1X controlled port unblocked. All 802.11 data frames are now encrypted by PTK and GTK

- The reassociation request and response frames are then sent from the client station to the target AP over the air.

- The PMK-R1 key is the seeding material for the over-the-DS fast BSS transition exchange that creates the final pairwise transient key (PTK).

Over-the-DS Fast BSS Transition



FT Action Request (STA, Target AP, RSNIE [PMKR0 Name], MDIR, FTIE [SNonce, R0KH-ID])

FT Action Response (STA, Target AP, RSNIE [PMKR0 Name], MDIR, FTIE [SNonce, R1KH-ID, R0KH-ID])

FT Action frames forwarded between the original AP and the target AP over the Distribution System (DS)

Reassociation Request (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID])

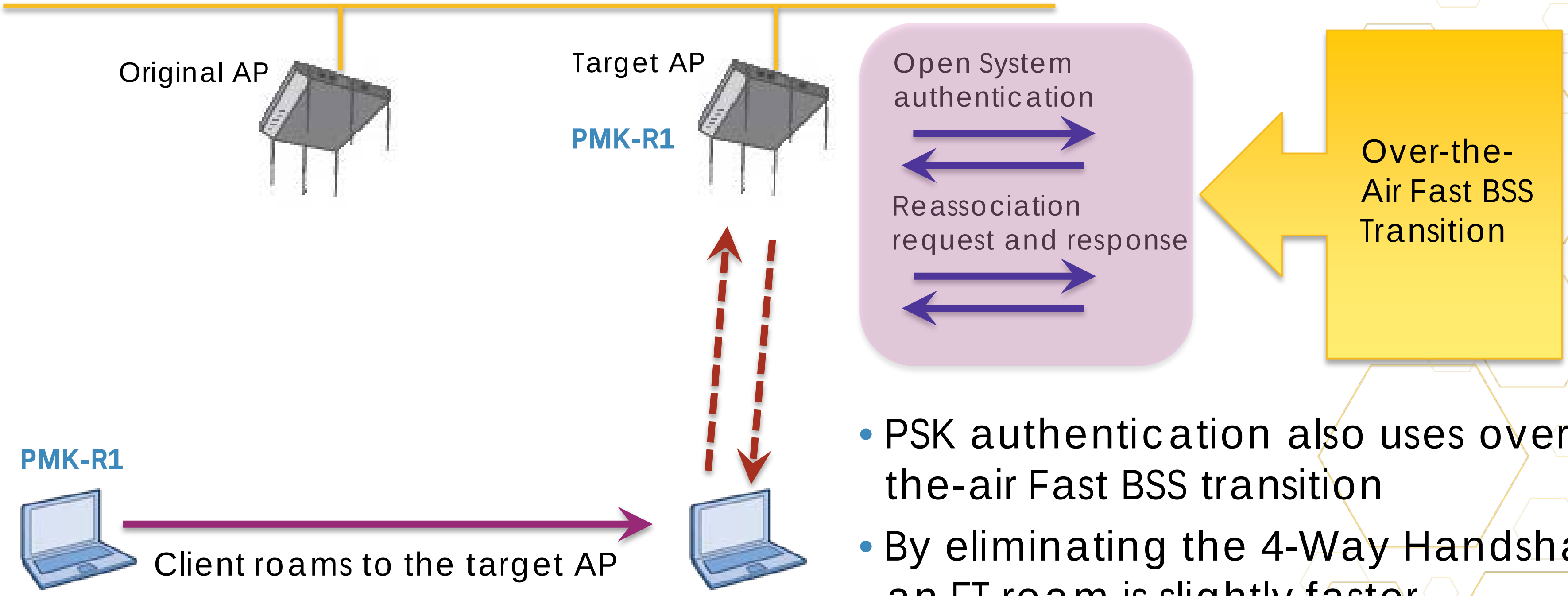
Reassociation Response (RSNIE [PMKR1Name], MDIE, FTIE [ANonce, SNonce, R1KH-ID, R0KH-ID] GTK)

Reassociation frames sent between the client station and the Target AP over-the-air

802.1X controlled port unblocked. All 802.11 data frames are now encrypted by PTK and GTK

- Over-the-DS fast BSS transition is considered to be an *optional* method that may be supported by a few WLAN vendors.

Fast BSS Transition and PSK authentication



Original AP

Target AP

PMK-R1

Open System authentication

Reassociation request and response

Over-the-Air Fast BSS Transition

PMK-R1

Client roams to the target AP

- PSK authentication also uses over-the-air Fast BSS transition
- By eliminating the 4-Way Handshake, an FT roam is slightly faster.

Fast BSS Transition

The RSN information element found in WLAN management frames includes three authentication and key management (AKM) suites:

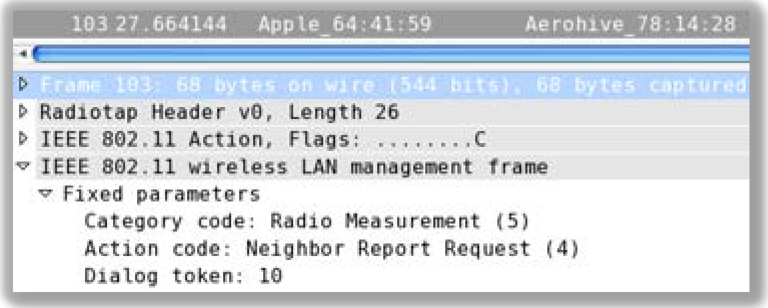
- FT authentication using IEEE 802.1X, with FT key management
- FT authentication using PSK, with FT key management
- FT authentication over SAE with SHA-256, with FT key management

802.11k

- The 802.11k-2008 amendment, in conjunction with the ratified 802.11r-2008 amendment, together have the potential to improve roaming performance within secure 802.11 WLANs.

- 802.11k defines radio resource measurement (RRM) mechanisms that enable 802.11k-compliant radios to better understand the RF environment in which they exist.

802.11k

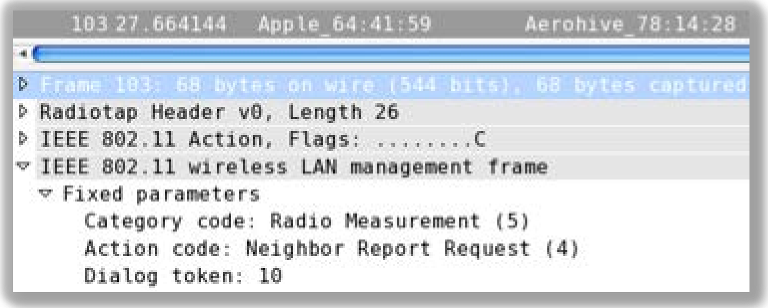


```
103 27.664144   Apple_64:41:59          Aerohive_78:14:28
▷ Frame 103: 68 bytes on wire (544 bits), 68 bytes captured
▷ Radiotap Header v0, Length 26
▷ IEEE 802.11 Action, Flags: ........C
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Neighbor Report Request (4)
      Dialog token: 10
```

- A key component of RRM is the neighbor report, which is used by client stations to gain information from the associated AP about potential roaming neighbors.

- The neighbor report information assists the fast roaming process by providing a method for the client to request from the associated AP a report about neighboring APs available within the same mobility domain.

802.11k



```
103 27.664144   Apple_64:41:59          Aerohive_78:14:28
▷ Frame 103: 68 bytes on wire (544 bits), 68 bytes captured
▷ Radiotap Header v0, Length 26
▷ IEEE 802.11 Action, Flags: ........C
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Neighbor Report Request (4)
      Dialog token: 10
```

- This can speed up the client scanning process by informing the client device of nearby APs to which it may roam.

- The neighbor report information is typically delivered through a request/report frame exchange inside 802.11 Action frames.

802.11v

- The IEEE 802.11v-2011 amendment defined wireless network management (WNM) as information about network resources that is exchanged between the client devices and an AP.

- The intended goal is to enhance overall performance of the wireless network.

- Whereas 802.11k provides exchange of information about the RF environment, 802.11v exchanges WNM information about surrounding existing network conditions.

Voice Enterprise

- In 2012, the Wi-Fi Alliance debuted a vendor-interoperability certification called Voice Enterprise that defines enhanced support for voice applications in the enterprise environment.

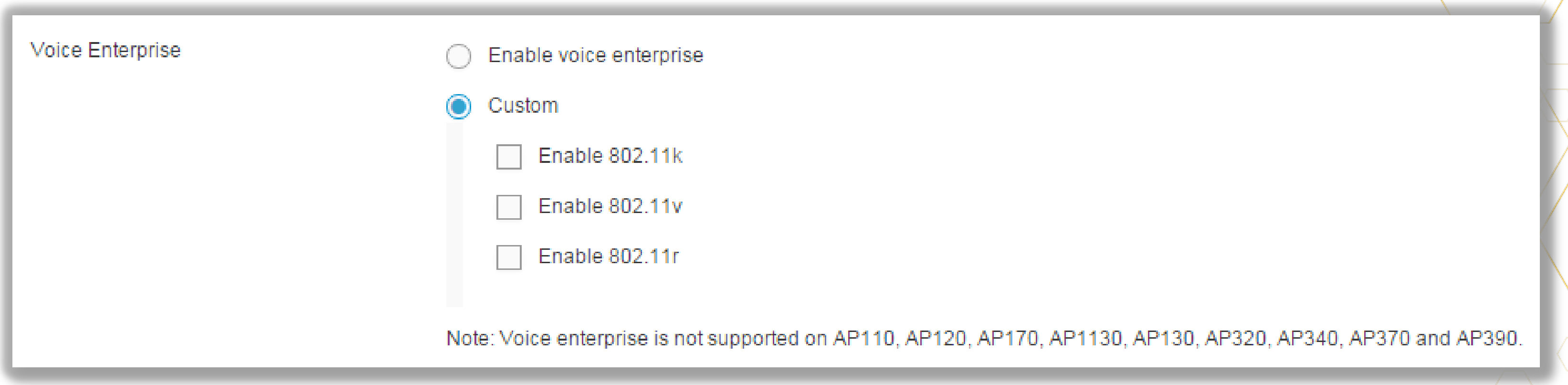
- Many aspects of the 802.11r, 802.11k, and 802.11v amendments are tested for Voice Enterprise certification.

Voice Enterprise

Performance of equipment submitted for Wi-Fi Alliance Voice Enterprise certification has to meet the following thresholds to ensure that the Wi-Fi network preserves good voice call quality:

- Latency (One way delay < 50 ms)
- Jitter (< 50 ms)

Voice Enterprise SSID



Voice Enterprise

○ Enable voice enterprise

● Custom

□ Enable 802.11k

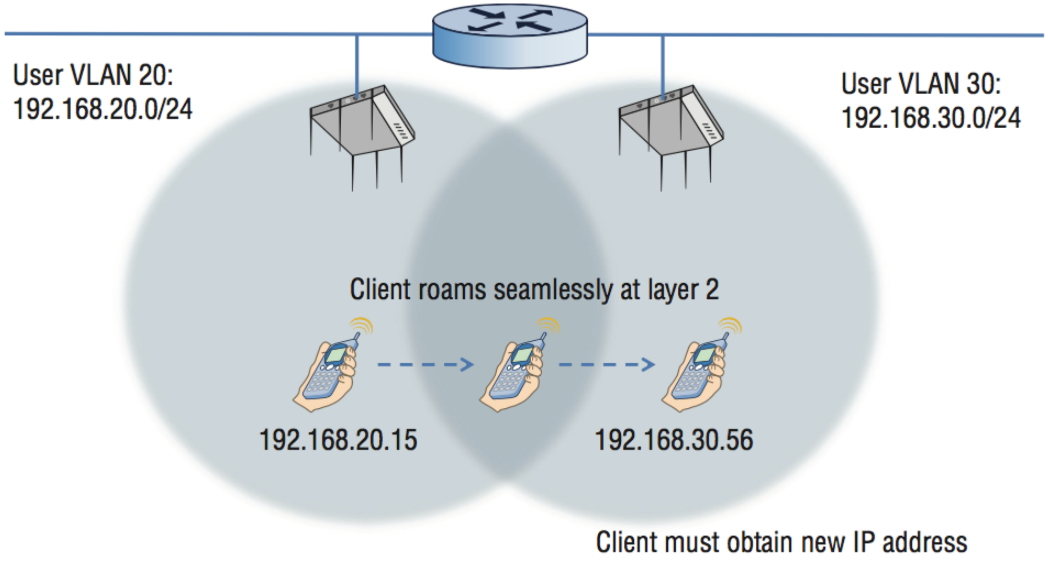
□ Enable 802.11v

□ Enable 802.11r

Note: Voice enterprise is not supported on AP110, AP120, AP170, AP1130, AP130, AP320, AP340, AP370 and AP390.

- Voice Enterprise settings may cause connectivity issues with legacy clients.
- The drivers of the legacy clients may not be able to handle the 802.11k/r/v information elements.
- Separate SSID may be needed.

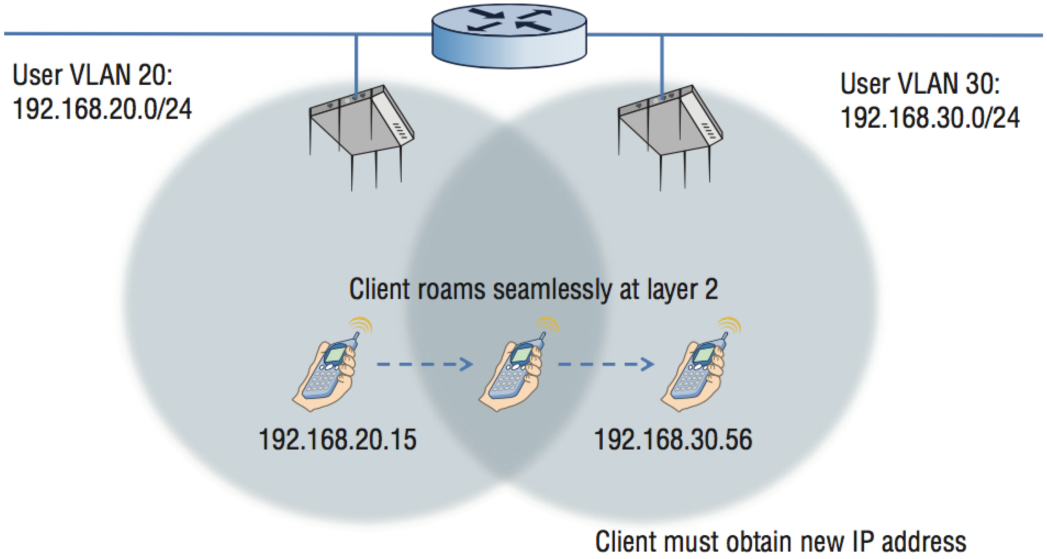
Layer 3 roaming boundaries



- One major consideration when designing a WLAN is what happens when client stations roam across Layer 3 boundaries.

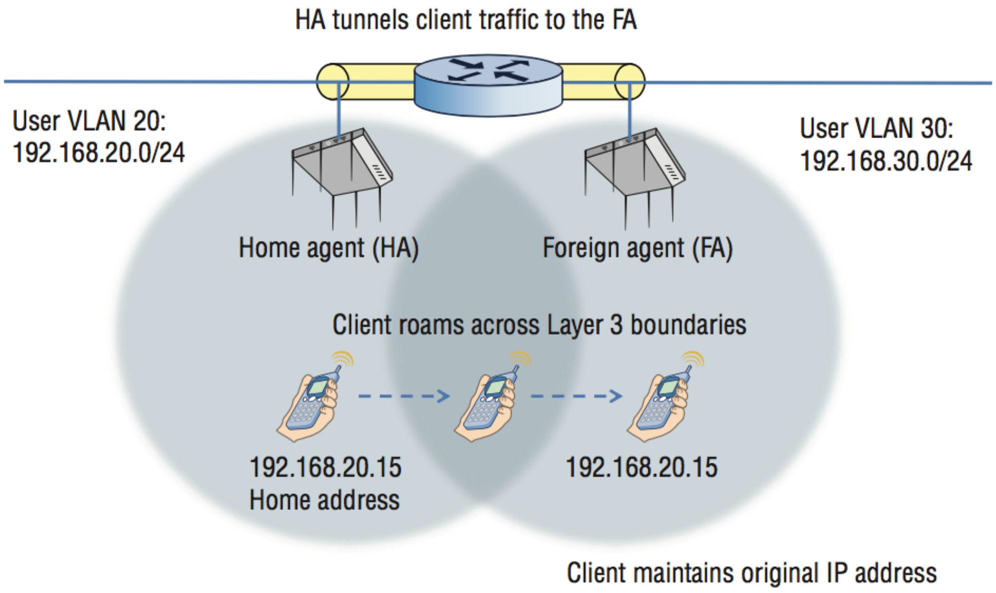
- Client stations will lose Layer 3 connectivity and must acquire a new IP address.

Layer 3 roaming boundaries



- Any connection-oriented applications that are running when the client reestablishes Layer 3 connectivity will have to be restarted.
- For example, a VoIP phone conversation would disconnect in this scenario, and the call would have to be reestablished.

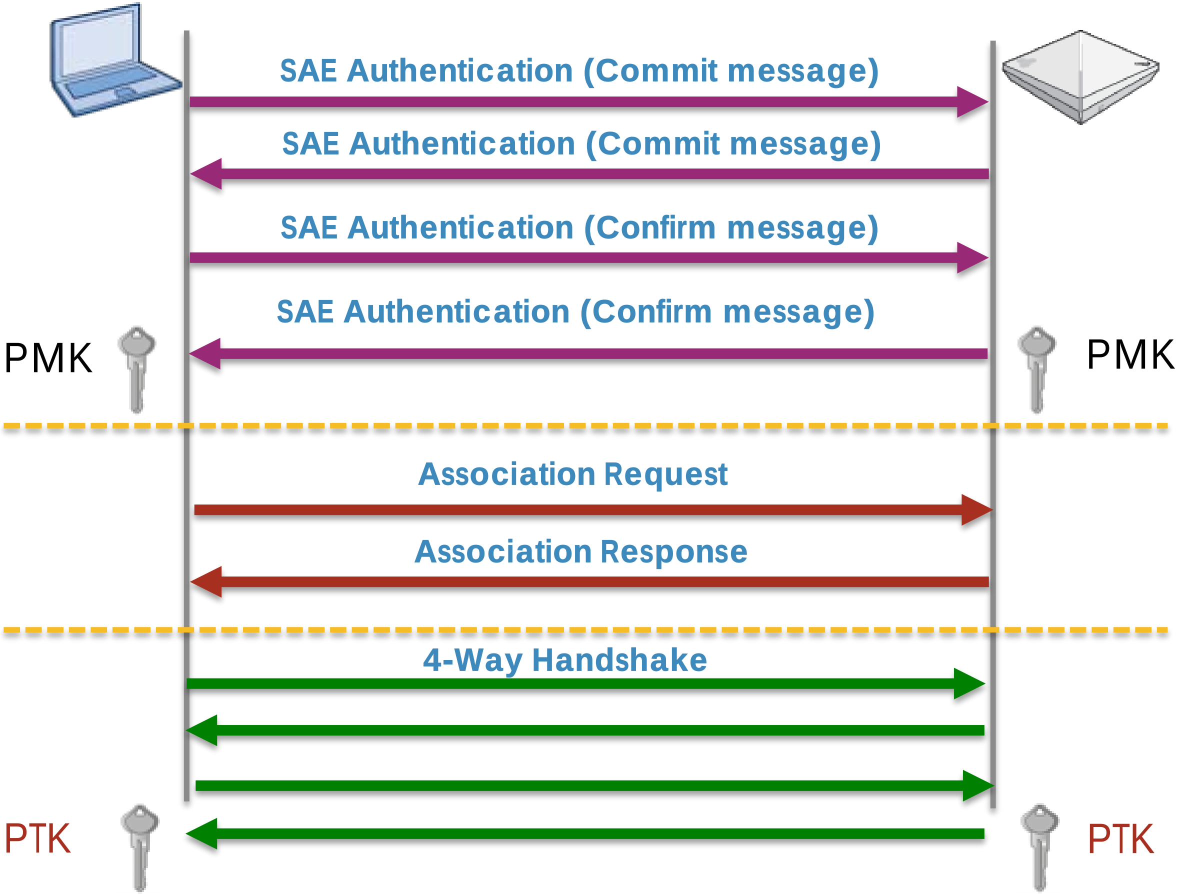
Mobile IP



- The only way to maintain upper-layer communications when crossing Layer 3 subnets is to provide a Layer 3 roaming solution that is based on the Mobile IP standard.

- Mobile IP uses an IP tunneling method and IP header encapsulation to allow packets to traverse between separate Layer 3 domains.

Secure Authentication of Equals



SAE Authentication (Commit message)
SAE Authentication (Commit message)
SAE Authentication (Confirm message)
SAE Authentication (Confirm message)
PMK
PMK
Association Request
Association Response
4-Way Handshake
PTK
PTK

- Once the PMK is created and the association process completes, the AP and the client can then commence a 4-Way Handshake to create a pairwise transient key (PTK).

Aerohive NETWORKS

SAE Roaming

Once the PMK is created and the association process completes, the AP and the What about roaming when using SAE authentication?

There are two potential methods:

- Option 1 A client station could roam to a new AP with the following sequence of frame exchanges: Probe Request/Response frame exchange, SAE authentication frame exchange, reassociation frame exchange, and then a 4-Way Handshake.

SAE Roaming

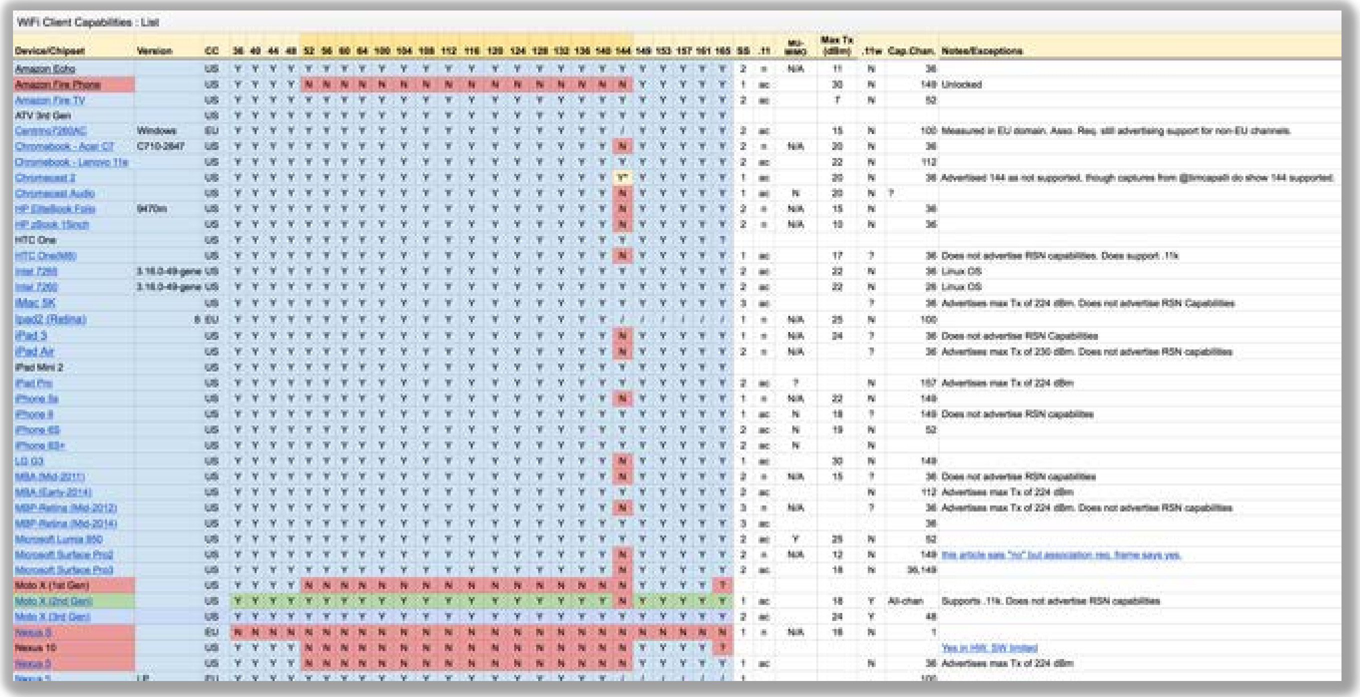
- Option 2 A client station can be SAE authenticated to many APs simultaneously by completing the SAE protocol with any number of APs while still being associated to another AP.

- In other words, a client could perform an SAE commit and confirm exchange with a potential roaming target prior to roaming to the target AP. This creates a PMK on neighboring APs.

- When the client roams, the PMK is already on the target AP and all the client has to do is a reassociation frame exchange and a 4-Way Handshake when it actually

Upgrade your clients first

clients.mikealbano.com



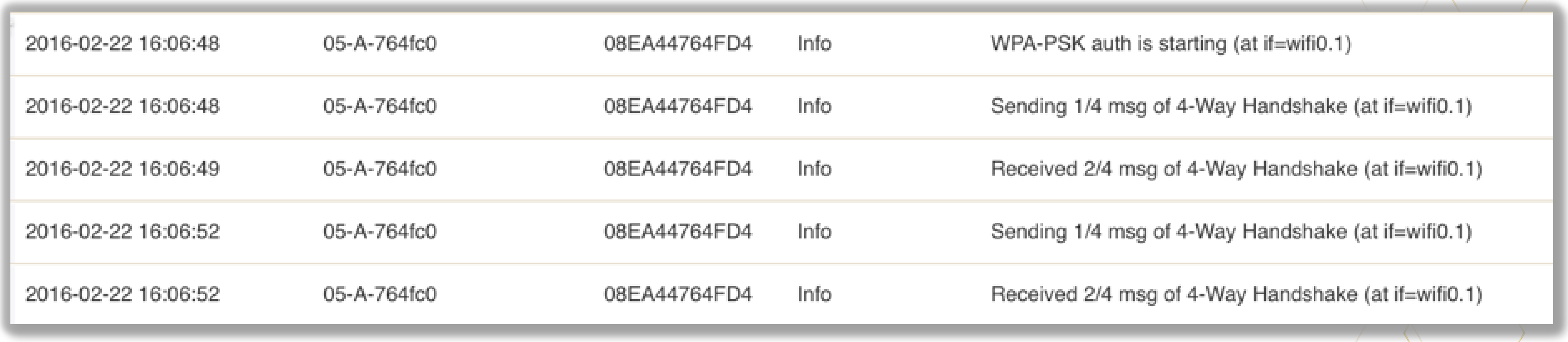
WiFi Client Capabilities : List

Device/Chipset	Version	CC	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165	SS	.11	MU-MIMO	Max Tx (dBm)	.11w	Cap.Chan.	Notes/Exceptions
Amazon Echo		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	n	N/A	11	N	36	
Amazon Fire Phone		US	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	1	ac		30	N	149	Unlocked
Amazon Fire TV		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac		7	N	52	
ATV 3rd Gen		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							
Centrino7260AC	Windows	EU	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	/	Y	Y	Y	Y	Y	2	ac		15	N	100	Measured in EU domain. Asso. Req. still advertising support for non-EU channels.
Chromebook - Acer C7	C710-2847	US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	2	n	N/A	20	N	36	
Chromebook - Lenovo 11e		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac		22	N	112	
Chromecast 2		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y*	Y	Y	Y	Y	Y	1	ac		20	N	36	Advertised 144 as not supported, though captures from @timcapati do show 144 supported.
Chromecast Audio		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	1	ac	N	20	N	?	
HP EliteBook Folio	9470m	US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	2	n	N/A	15	N	36	
HP zBook 15inch		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	2	n	N/A	10	N	36	
HTC One		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	?							
HTC One(M8)		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	1	ac		17	?	36	Does not advertise RSN capabilities. Does support .11k
Intel 7265	3.16.0-49-gene	US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac		22	N	36	Linux OS
Intel 7260	3.16.0-49-gene	US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac		22	N	36	Linux OS
iMac 5K		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	3	ac			?	36	Advertises max Tx of 224 dBm. Does not advertise RSN Capabilities
Ipad2 (Retina)	8	EU	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	/	/	/	/	/	/	1	n	N/A	25	N	100	
iPad 3		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	1	n	N/A	24	?	36	Does not advertise RSN Capabilities
iPad Air		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	2	n	N/A		?	36	Advertises max Tx of 230 dBm. Does not advertise RSN capabilities
iPad Mini 2		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							
iPad Pro		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac	?		N	157	Advertises max Tx of 224 dBm
iPhone 5s		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	1	n	N/A	22	N	149	
iPhone 6		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	1	ac	N	18	?	149	Does not advertise RSN capabilities
iPhone 6S		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac	N	19	N	52	
iPhone 6S+		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac	N		N		
LG G3		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	1	ac		30	N	149	
MBA (Mid-2011)		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	2	n	N/A	15	?	36	Does not advertise RSN capabilities
MBA (Early-2014)		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac			N	112	Advertises max Tx of 224 dBm
MBP-Retina (Mid-2012)		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	3	n	N/A		?	36	Advertises max Tx of 224 dBm. Does not advertise RSN capabilities
MBP-Retina (Mid-2014)		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	3	ac				36	
Microsoft Lumia 950		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac	Y	25	N	52	
Microsoft Surface Pro2		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	2	n	N/A	12	N	149	this article says "no" but association req. frame says yes.
Microsoft Surface Pro3		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	2	ac		18	N	36,149	
Moto X (1st Gen)		US	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	?							
Moto X (2nd Gen)		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	1	ac		18	Y	All-chan	Supports .11k. Does not advertise RSN capabilities
Moto X (3rd Gen)		US	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	ac		24	Y	48	
Nexus 5		EU	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	1	n	N/A	18	N	1	
Nexus 10		US	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	?							Yes in HW, SW limited
Nexus 6		US	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	1	ac			N	36	Advertises max Tx of 224 dBm
Nexus 5	LP	EU	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	/	/	/	/	/	/	1					100	

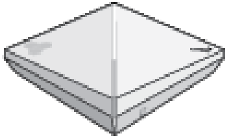
Blame

Your Wi-Fi sucks!

Layer 2: PSK Authentication Troubleshooting

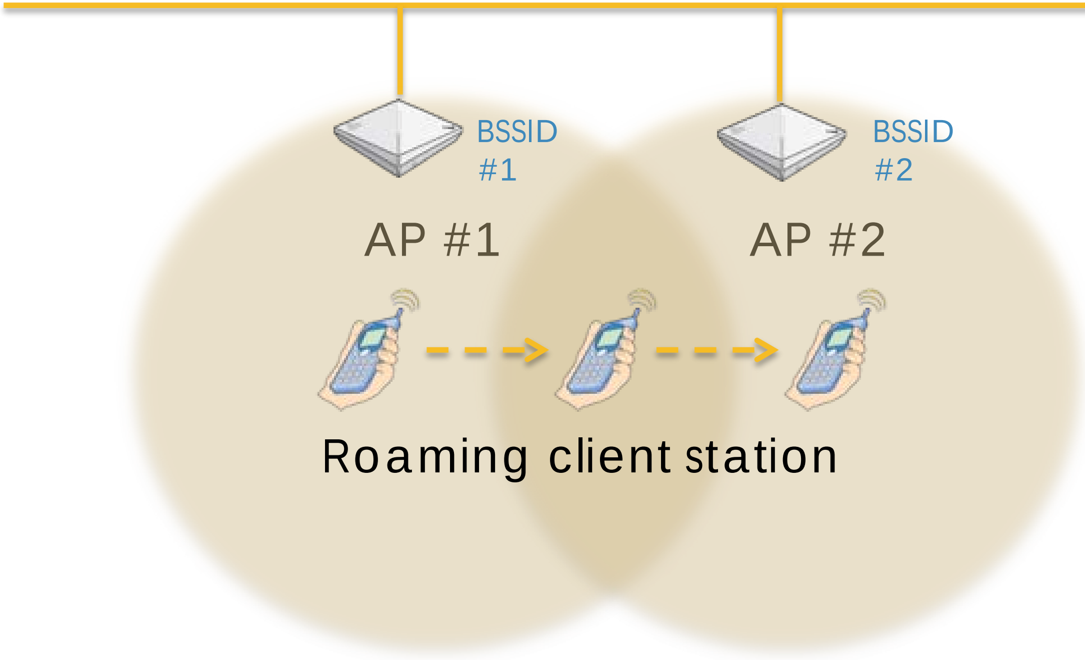


```
2016-02-22 16:06:48    05-A-764fc0    08EA44764FD4    Info    WPA-PSK auth is starting (at if=wifi0.1)
2016-02-22 16:06:48    05-A-764fc0    08EA44764FD4    Info    Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
2016-02-22 16:06:49    05-A-764fc0    08EA44764FD4    Info    Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
2016-02-22 16:06:52    05-A-764fc0    08EA44764FD4    Info    Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
2016-02-22 16:06:52    05-A-764fc0    08EA44764FD4    Info    Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
```



- Passphrase mismatch
- PMKs never properly created
- 4-Way Handshake fails

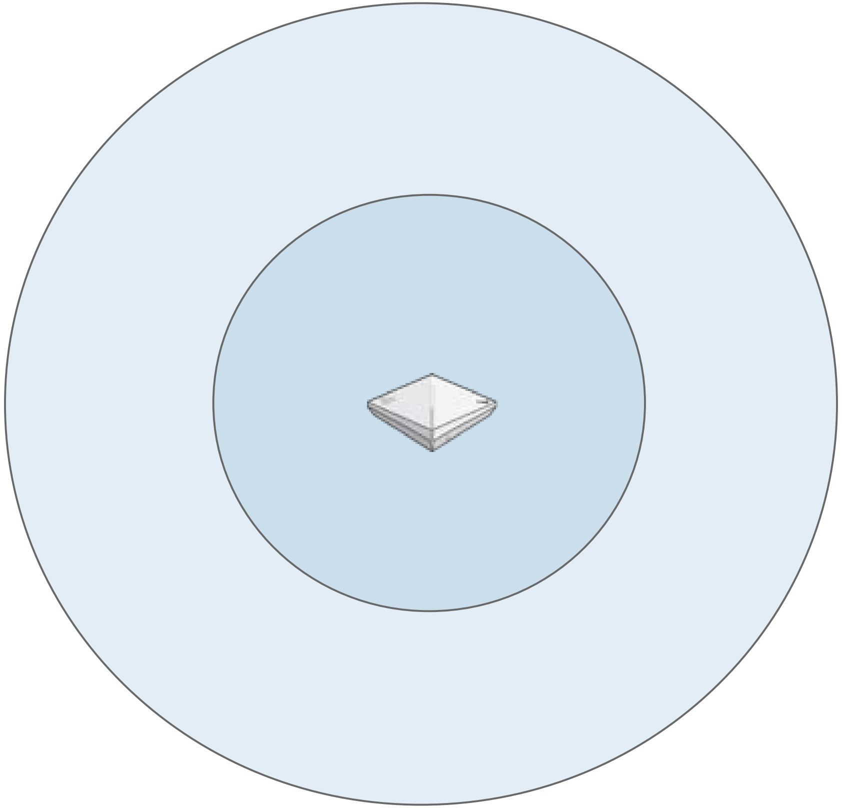
Layer 2: Roaming Problems



- Drivers (client problem)
- Sticky Problems (bad design)
- Layer 3 roaming

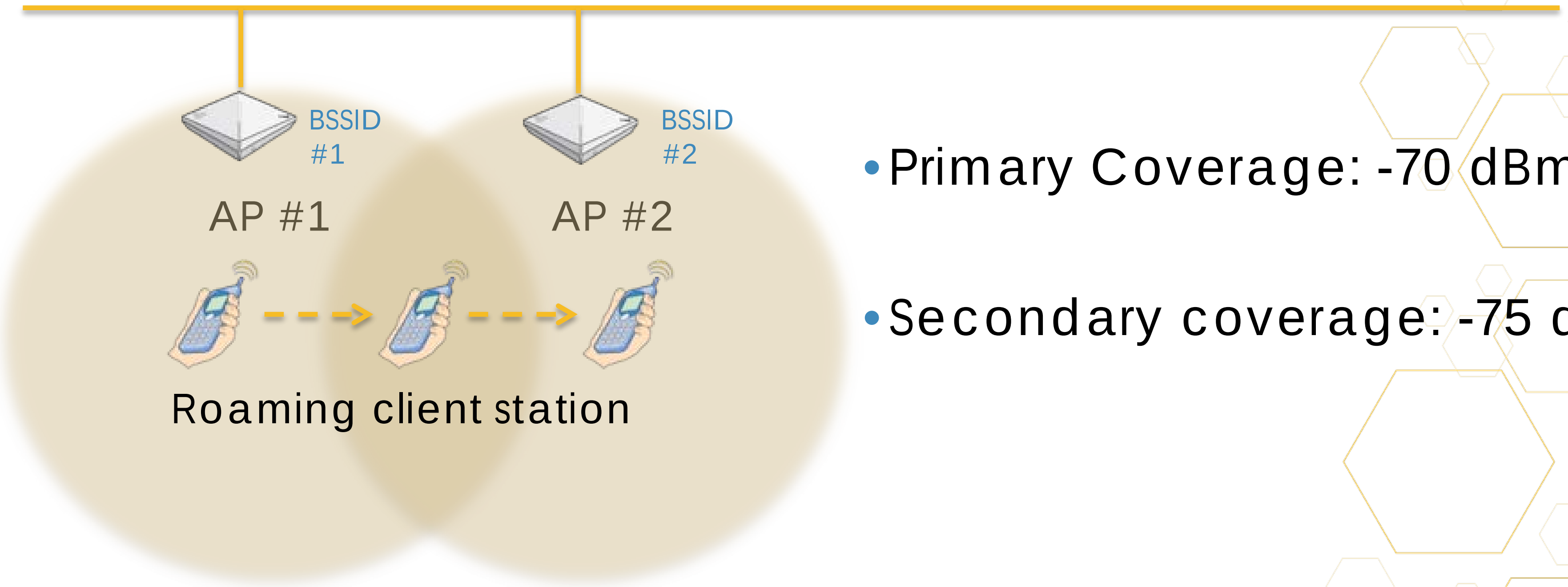
High Power is BAD

Low Power is Good



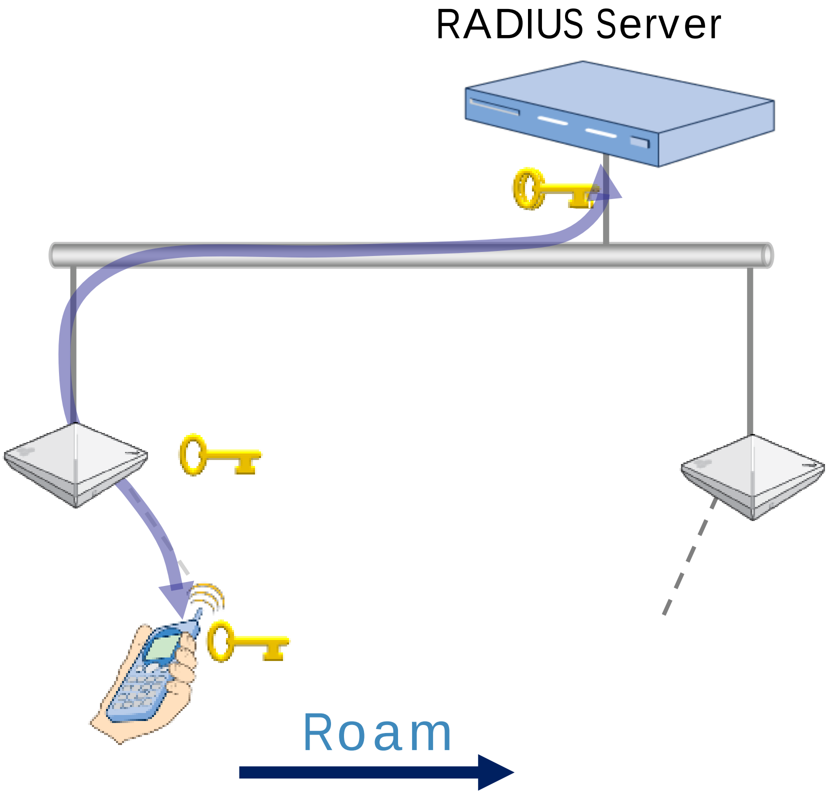
- Capacity Problems
- Increase CCI
- Hidden Node
- Mismatch power between clients and AP
- Roaming – Sticky problems
- Turn down the power!

How do you measure cell overlap?



- Primary Coverage: -70 dBm
- Secondary coverage: -75 dBm
- Clients make the roaming decision

Layer 2: Fast Secure Roaming



- Do clients support Opportunistic Key Caching (OKC)?
- Do clients support 802.11r and 802.11k mechanisms?

But… it’s backward compatible!

- Legacy client devices often cannot connect when new 802.11 technology is introduced
- Client drivers do not know how to handle new Information Elements in Beacons
- Example: Fast BSS Transition IE

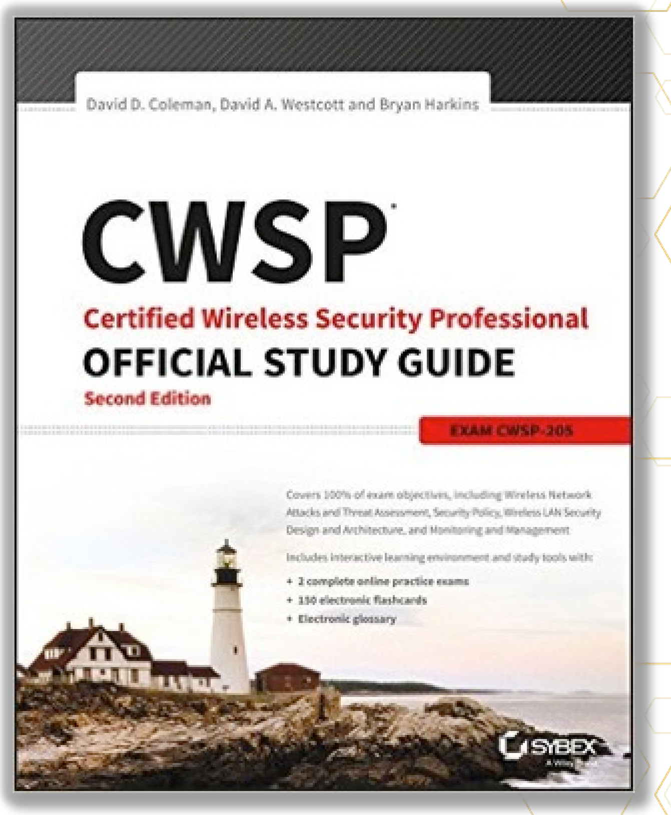
Who am I?

Available now:

Sybex CWSP Study Guide
2nd Edition

ISBN: 978-1119211082

Amazon:
http://amzn.com/1119211085



David D. Coleman, David A. Westcott and Bryan Harkins

CWSP®

Certified Wireless Security Professional

OFFICIAL STUDY GUIDE

Second Edition

EXAM CWSP-205

Covers 100% of exam objectives, including Wireless Network Attacks and Threat Assessment, Security Policy, Wireless LAN Security Design and Architecture, and Monitoring and Management

Includes interactive learning environment and study tools with:

- 2 complete online practice exams
- 150 electronic flashcards
- Electronic glossary

SYBEX A Wiley Brand

Aerohive NETWORKS

Questions

Thank you