# Feature of Fast Roaming on EWS AP

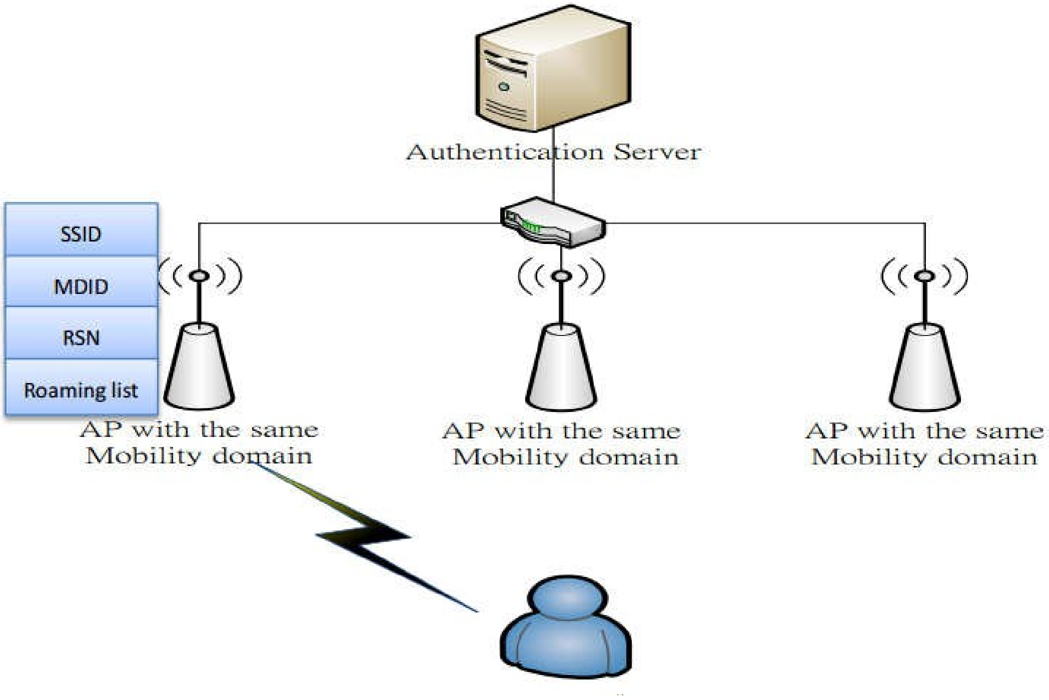
## Table of Contents

# 1. Introduction:

Unlike cellular network where mobility is put into consideration from the design stage on base station and clients, the client handoff in original 802.11 WLAN is to let mobile device decide when to hand off and to which AP it wishes to hand off. Therefore, the deployment of APs to make sure effective coverage plays an important role to let users stay connected with WLAN.

However, as new features such as security (802.11i) and quality of service (802.11e) added into WLAN, number of related messages is also increased; before these messages finish the exchange process, users' traffics cannot proceed and delay-sensitive applications will experience jitters or loss-of-data during handoff.

To address the extra time needed for message exchange during handoff, newer technique as 802.11r is introduced to eliminate related overheads based on the same architecture for client roaming; with assistance from 802.11k, it will further facilitate roaming and lower impact from mobility for delay-sensitive applications.


Authentication Server
SSID
MDID
RSN
Roaming list
AP with the same Mobility domain
AP with the same Mobility domain
AP with the same Mobility domain

# 2. Feature Highlight

To lower extra burden from security and QoS during handoff process, 802.11r introduces a method called “Fast Transition” (FT) to allow a roaming client to initialize a handshake with new AP before it roams to the target AP. The core idea behind this is to use FT key hierarchy to allow clients to make fast BSS transitions between APs within the same ESS and mobility domain without re-authentication required at every AP.

In addition, 802.11k is designed to allow clients to quickly identify nearby AP that are available for roaming. When a client senses the signal strength getting weaker from current AP and needs to prepare hand-off to another AP, this mechanism allows the client to know best candidate AP to roam from surrounding APs.

EnGenius  EWS AP has enclosed 802.11k/r mechanisms to allow 802.11k/r-compliant clients to enjoy less time needed during fast handoff. The following will further explain related WLAN operations by EnGenius  EWS AP to accommodate this fast roaming feature:

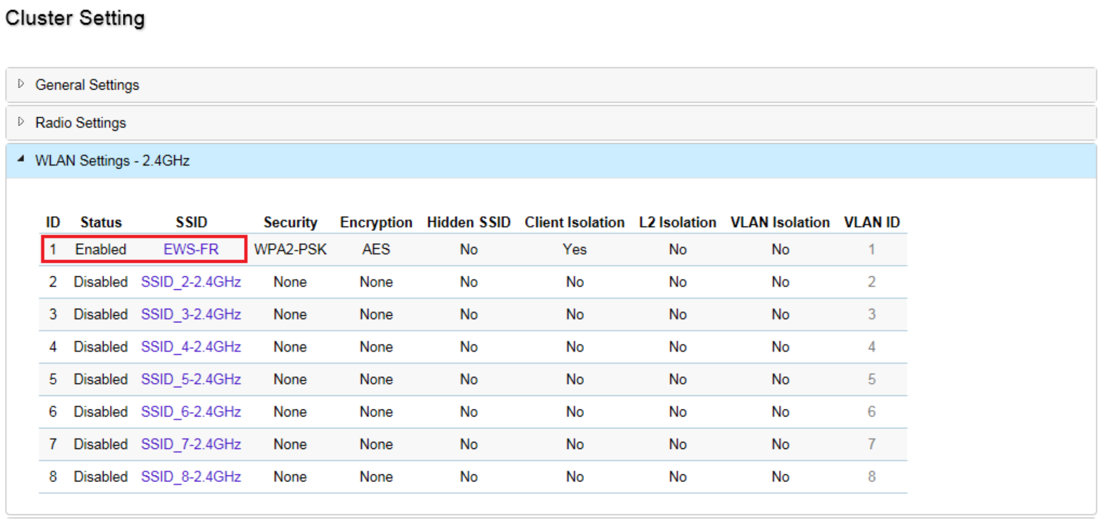
## *2.1 Fast Roaming is Enabled*

Fast roaming feature is supported for the first SSID profile per radio with security types: WPA2/WPA-Mixed PSK and WPA2/WPA-Mixed Enterprise; to make UI simple and hide the complexity behind the scene, when the feature is checked, related mechanisms such as PMKSA caching*, 802.11r Fast Transition, and 802.11k-assisted roaming will be enabled to facilitate client roaming.

*Please refer to the following table for applicable security types.

| **PMKSA Caching** | **802.11k/r** | **Auth Server** |
|---|---|---|
| WPA2-Enterprise | WPA2-Enterprise | RADIUS |
| WPA-Mixed Enterprise | WPA-Mixed Enterprise | |
| | WPA2/ WPA-Mixed -PSK | RADIUS not needed |

The following lists a cluster setting as an example for Fast Roaming:



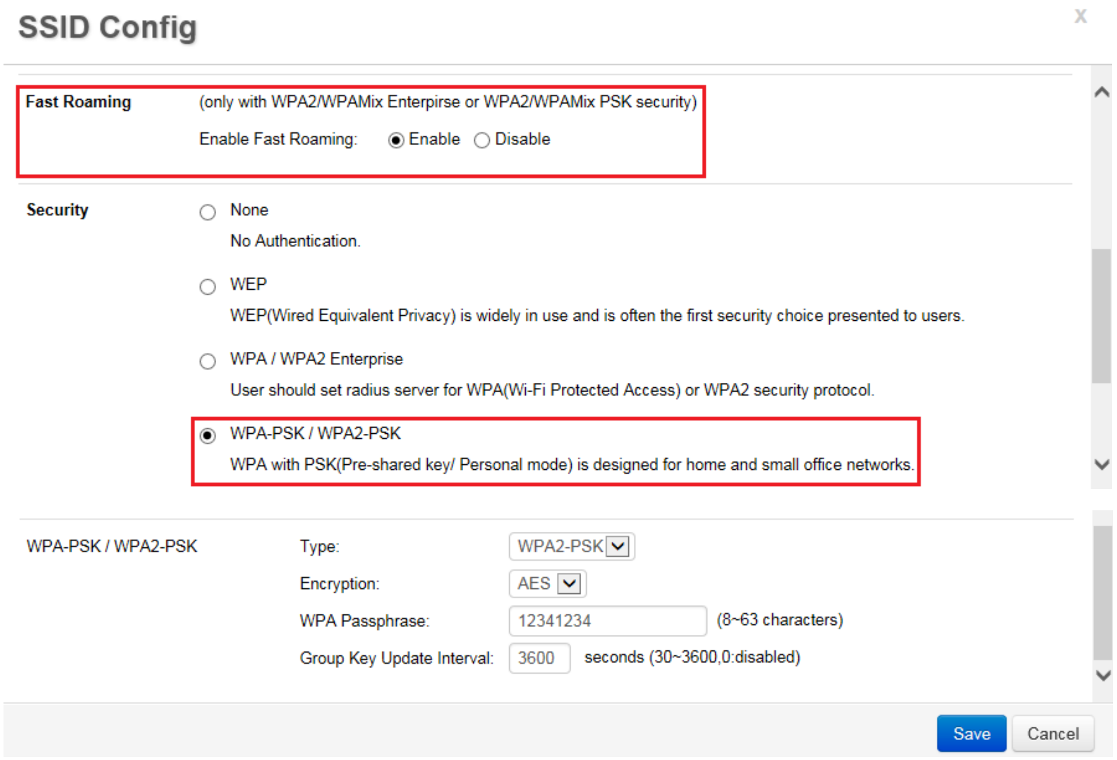
Cluster Setting

▷ General Settings

▷ Radio Settings

◢ WLAN Settings - 2.4GHz

| ID | Status | SSID | Security | Encryption | Hidden SSID | Client Isolation | L2 Isolation | VLAN Isolation | VLAN ID |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Enabled | EWS-FR | WPA2-PSK | AES | No | Yes | No | No | 1 |
| 2 | Disabled | SSID_2-2.4GHz | None | None | No | No | No | No | 2 |
| 3 | Disabled | SSID_3-2.4GHz | None | None | No | No | No | No | 3 |
| 4 | Disabled | SSID_4-2.4GHz | None | None | No | No | No | No | 4 |
| 5 | Disabled | SSID_5-2.4GHz | None | None | No | No | No | No | 5 |
| 6 | Disabled | SSID_6-2.4GHz | None | None | No | No | No | No | 6 |
| 7 | Disabled | SSID_7-2.4GHz | None | None | No | No | No | No | 7 |
| 8 | Disabled | SSID_8-2.4GHz | None | None | No | No | No | No | 8 |



SSID Config

**Fast Roaming** (only with WPA2/WPAMix Enterpirse or WPA2/WPAMix PSK security)

Enable Fast Roaming: ● Enable ○ Disable

**Security**

○ None
No Authentication.

○ WEP
WEP(Wired Equivalent Privacy) is widely in use and is often the first security choice presented to users.

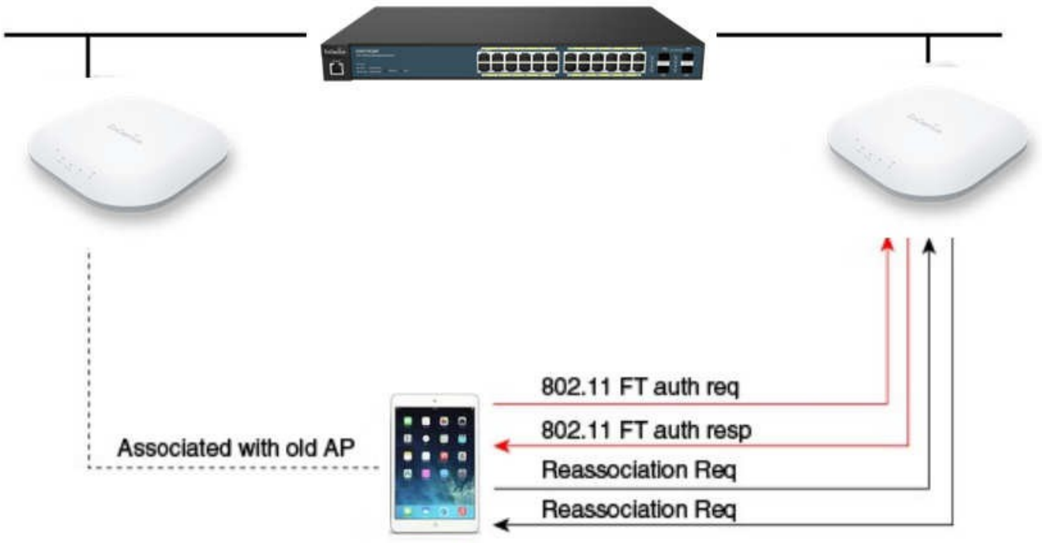
○ WPA / WPA2 Enterprise
User should set radius server for WPA(Wi-Fi Protected Access) or WPA2 security protocol.

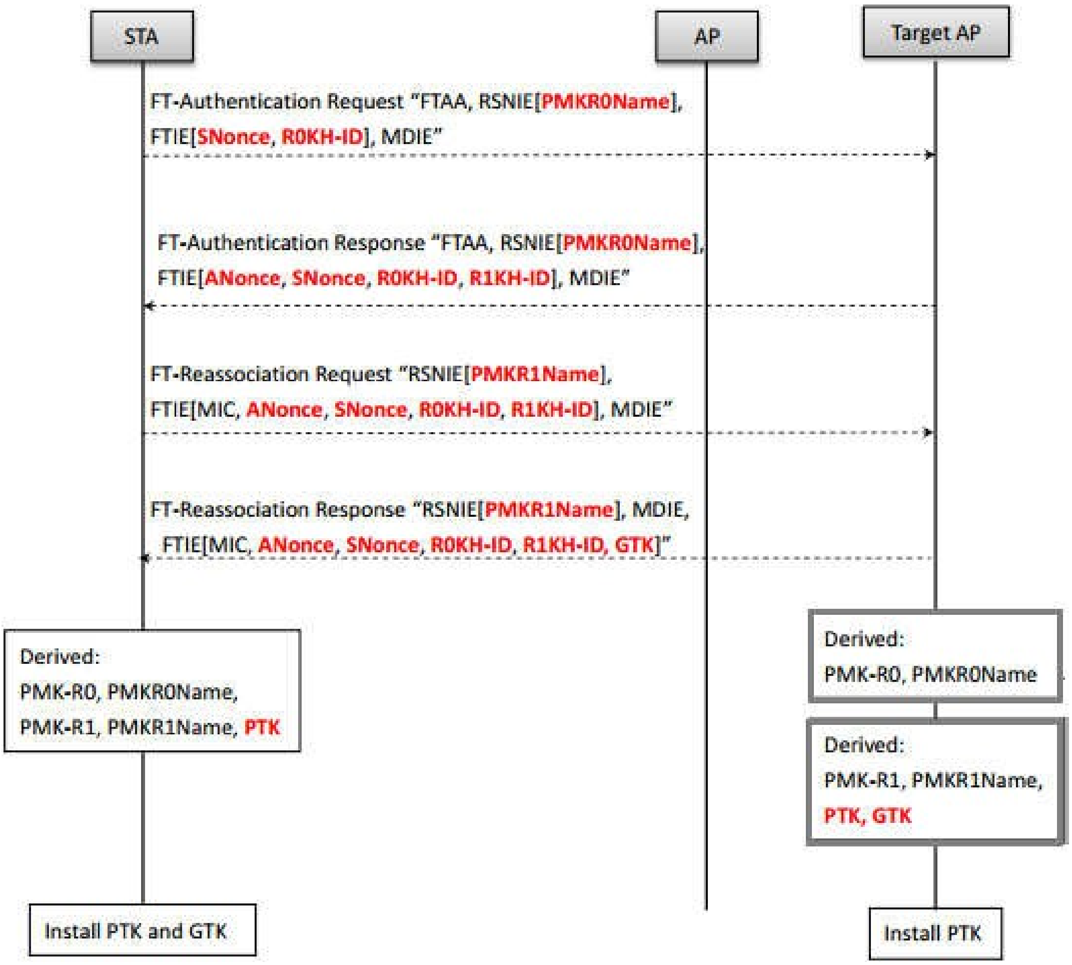
● WPA-PSK / WPA2-PSK
WPA with PSK(Pre-shared key/ Personal mode) is designed for home and small office networks.

WPA-PSK / WPA2-PSK

| | |
|---|---|
| Type: | WPA2-PSK |
| Encryption: | AES |
| WPA Passphrase: | 12341234 (8~63 characters) |
| Group Key Update Interval: | 3600 seconds (30~3600,0:disabled) |

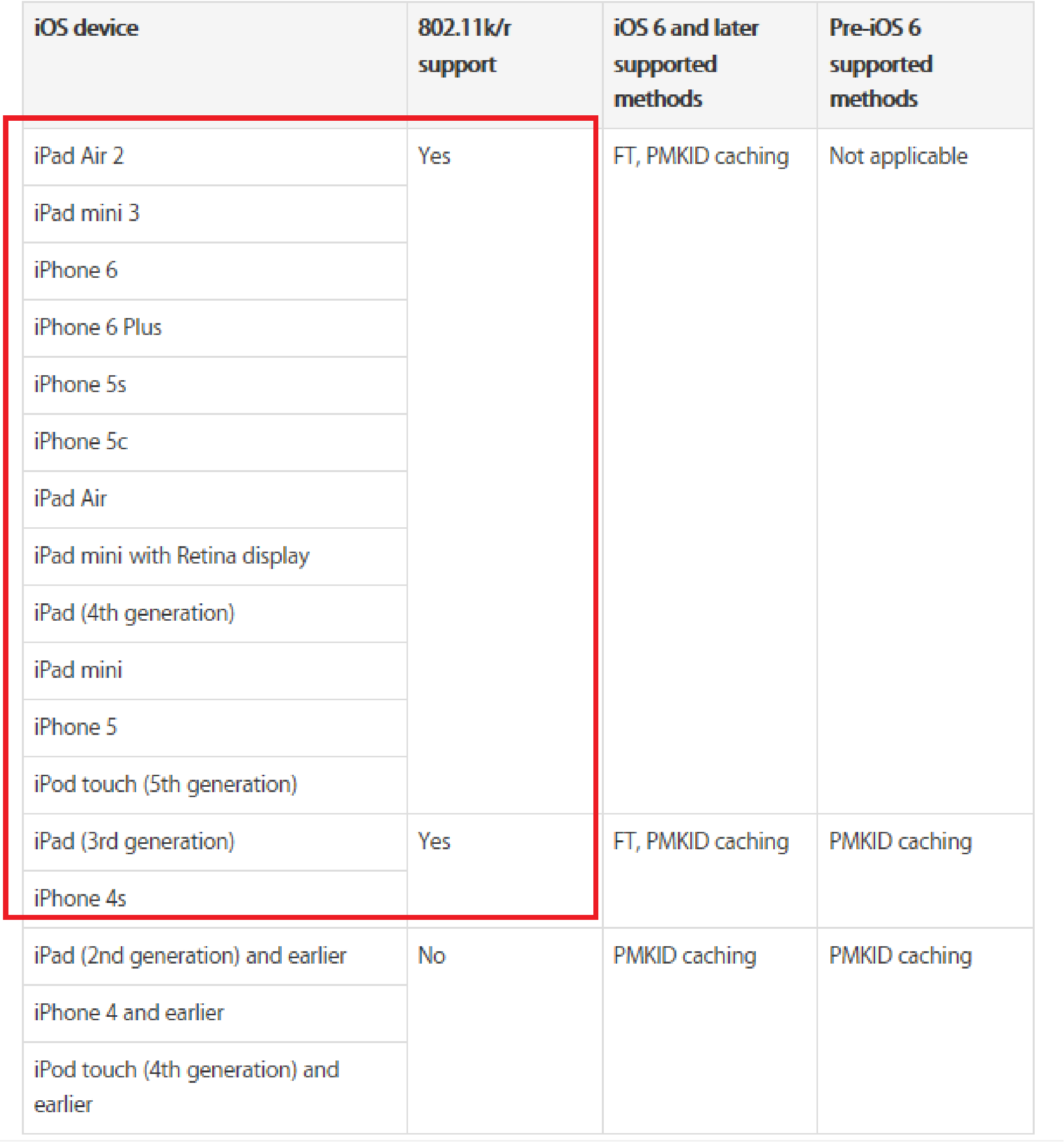
## 2.1.1 802.11k/r-compliant Client Roaming




STA
AP
Target AP
FT-Authentication Request "FTAA, RSNIE[PMKR0Name], FTIE[SNonce, R0KH-ID], MDIE"
FT-Authentication Response "FTAA, RSNIE[PMKR0Name], FTIE[ANonce, SNonce, R0KH-ID, R1KH-ID], MDIE"
FT-Reassociation Request "RSNIE[PMKR1Name], FTIE[MIC, ANonce, SNonce, R0KH-ID, R1KH-ID], MDIE"
FT-Reassociation Response "RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R0KH-ID, R1KH-ID, GTK]"
Derived: PMK-R0, PMKR0Name, PMK-R1, PMKR1Name, PTK
Derived: PMK-R0, PMKR0Name
Derived: PMK-R1, PMKR1Name, PTK, GTK
Install PTK and GTK
Install PTK

Before actual handoff taking place, the client has known the best candidate AP as new AP for roaming; once the new AP is identified, the FT operations will then allow client to perform handshake with selected new AP. The whole process will be completed before client roaming into another AP so re-authentication can be saved from new AP.

The follow table lists some well-known 802.11k/r client types as of this writing:



| iOS device | 802.11k/r support | iOS 6 and later supported methods | Pre-iOS 6 supported methods |
|---|---|---|---|
| iPad Air 2 | Yes | FT, PMKID caching | Not applicable |
| iPad mini 3 | | | |
| iPhone 6 | | | |
| iPhone 6 Plus | | | |
| iPhone 5s | | | |
| iPhone 5c | | | |
| iPad Air | | | |
| iPad mini with Retina display | | | |
| iPad (4th generation) | | | |
| iPad mini | | | |
| iPhone 5 | | | |
| iPod touch (5th generation) | | | |
| iPad (3rd generation) | Yes | FT, PMKID caching | PMKID caching |
| iPhone 4s | | | |
| iPad (2nd generation) and earlier | No | PMKID caching | PMKID caching |
| iPhone 4 and earlier | | | |
| iPod touch (4th generation) and earlier | | | |

## 2.1.2 Non-802.11k/r Client Roaming

When WPA2-Enterprise is selected for wireless security, EnGenius enterprise AP also supports 802.11i-based PMKSA caching method for fast roaming. Under this scenario, non-802.11k/r compliant client can hand off to adjacent new AP within the same ESS without re-authentication.

Upon client completing authentication with RADIUS server through current AP, PMKSA is created for such binding and if fast roaming is enabled, this binding info will be distributed through its LAN to adjacent APs. When a client prepares to roam, its surrounding APs have obtained corresponding PMKSA caching so authentication will not be required again.

## *2.2 Fast Roaming is Disabled (Default)*

Under this circumstance, client roaming will follow the existing method without PMKSA caching, FT mechanisms, and 802.11k info sharing for best candidate AP to roam. It will solely depend on client's decision when to roam and to which AP it should connect. If RADIUS server is used for wireless security, authentication will be required again upon roaming.