# 802.11r or Fast Transition (FT) for fast secure Roaming

Karthickeyan Prabanandhan is a Senior Test Engineer (CCNP, CWNP) in Wireless Engineering Team currently preparing for his CCIE Wireless lab. In this video series Karthick will explain "How to configure a 11r WLAN using CLI and GUI and show us the 11r roaming " on Converged Access (Cisco 5760 WLC and Cisco Catalyst 3850).

## 802.11r Introduction

802.11r is also known, as Fast Transition (FT) is the IEEE standard for fast secure roaming. It introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP. The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and AP after the client does the re-association request or response exchange with new target AP.
The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring re-authentication at every AP. The summary of the key hierarchy is given below. 802.11r eliminates much of the handshaking overhead while roaming thus reducing the handoff times between APs while providing security and QoS. This is useful for client devices that have delay-sensitive applications like voice and video and is key requirement for voice over Wi-Fi.

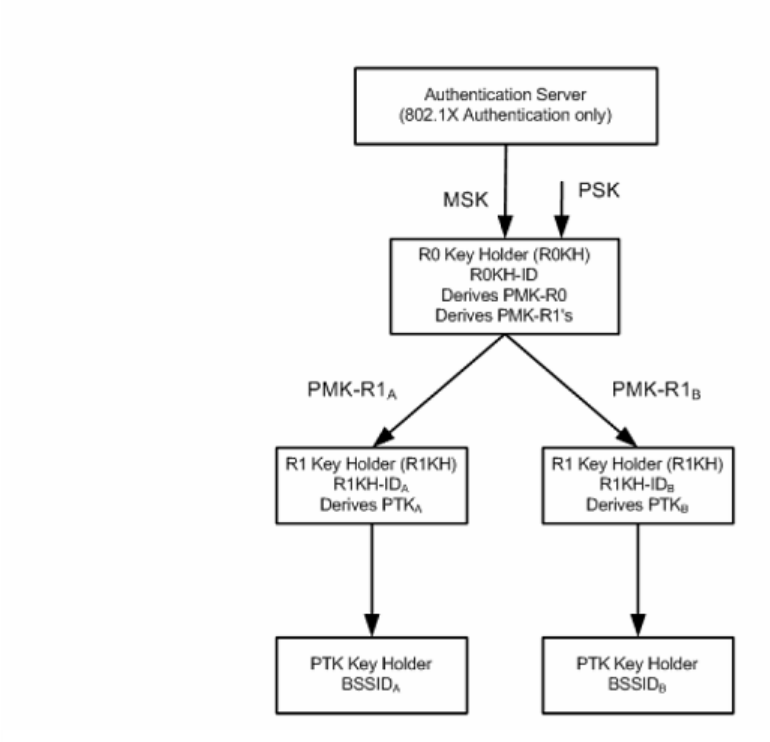
**Summary of the key hierarchy:**

1. An MSK is still derived on the client supplicant and the Authentication Server from the initial 802.1X/EAP authentication phase (transferred from the Authentication Server to the Authenticator (WLC) once the authentication is successful). This MSK, like in the other methods, is used as the seed for the FT key hierarchy. When you use WPA2−PSK instead of an EAP authentication method, the PSK is basically this MSK.

2. A Pairwise Master Key R0 (PMK−R0) is derived from the MSK, which is the first−level key of the FT key hierarchy. The key holders for this PMK−R0 are the WLC and the client.

3. A second−level key, called a Pairwise Master Key R1 (PMK−R1), is derived from the PMK−R0, and the key holders are the client and the APs managed by the WLC that holds the PMK−R0.

4. The third and final level key of the FT key hierarchy is the PTK, which is the final key used in order to encrypt the 802.11 unicast data frames (similar to the other methods that use WPA/TKIP or WPA2/AES). This PTK is derived on FT from the PMK−R1, and the key holders are the client and the APs managed by the WLC.




**802.11r Initial Association**

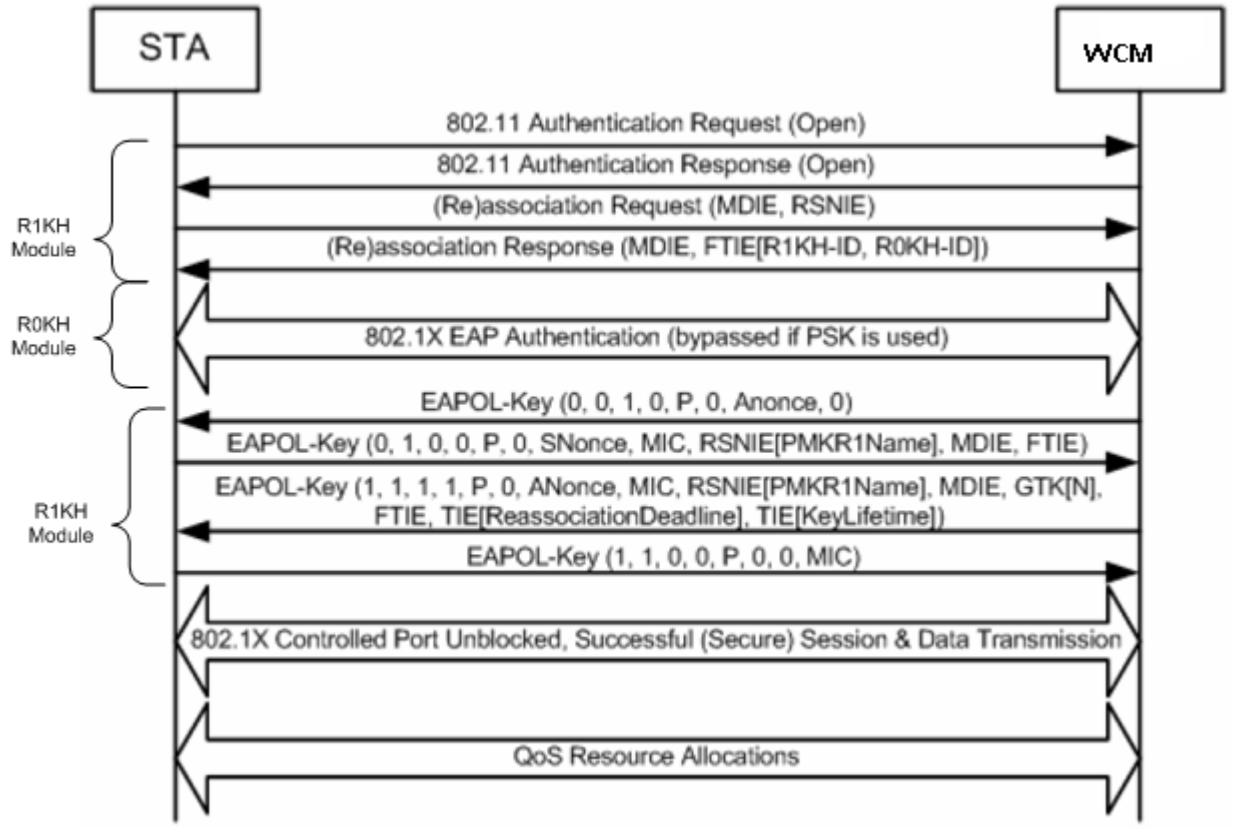
The Client initiates the FT initial mobility domain association procedures by performing an IEEE 802.11 authentication using the Open System authentication algorithm.

Client → NGWC : Authentication-Request (Open System authentication algorithm)
WCM → NGWC : Authentication-Response (Open System authentication algorithm, Status)

Upon successful IEEE 802.11 Open System authentication, the Client will send a (Re)Association Request frame to the controller that includes the MDIE. The contents of the MDIE will be the values advertised by the AP in its Beacon or Probe Response frames. Additionally, the Client includes its security capabilities in the RSNIE.

Client →NGWC: (Re)Association Request (MDIE, RSNIE)
NGWC→ Client: (Re)Association Response (MDIE, FTIE[R1KH-ID, R0KH-ID])

The above steps are explained in the below diagram




**FT Initial Mobility domain Association in RSN**

**802.11r Roaming methods:**

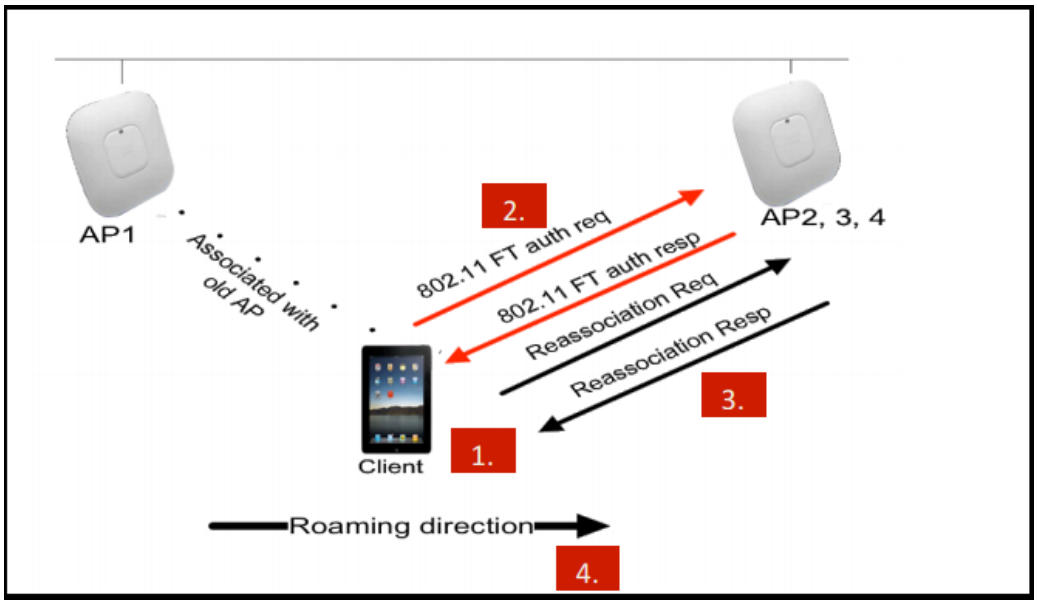
For a client to move from its current AP to a target AP using 802.11r, the message exchanges are performed using one of the following two methods:

- Over-the-Air Roaming
- Over-the-DS (Distribution System) Roaming
- Over-the-Air

**802.11r roaming - over the air**

The client communicates directly with the target AP using IEEE 802.11 authentication with the FT Authentication algorithm.

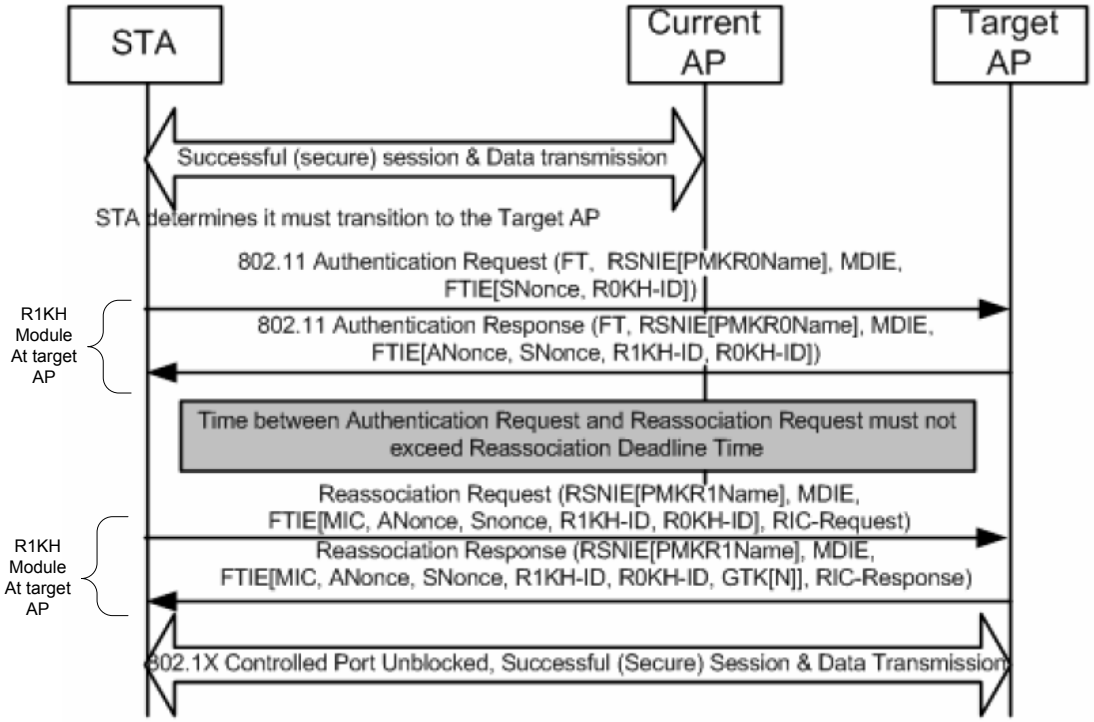
The flow diagram for over-the-air client roaming which explains the sequence of messages that will be exchanged between the client, current AP and target AP is given below




The following steps describe the message exchange in the case where a client is roaming between APs, AP1 and AP2, connected to the NGWC

1. Client is associated with AP1 and wants to roam to AP2
2. Client sends an FT Authentication Request to AP2 and receives FT Authentication Response from AP2
3. Clients sends a Reassociation Request to AP2 and receives a Reassociation Response from AP2
4. Client completes its roam from AP1 to AP2

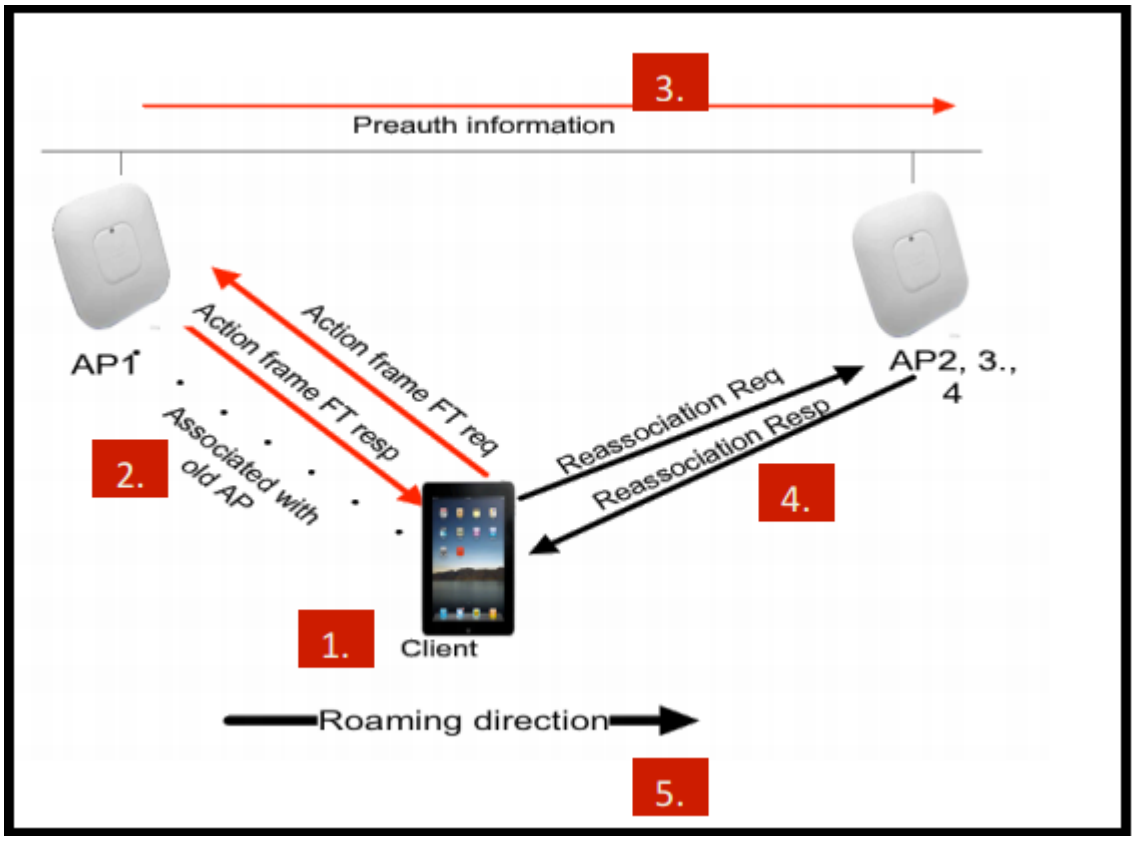
The 802.11 message exchanges are given in the diagram below




**802.11r roaming - over the DS (Distribution System)**

The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the controller

The flow diagram for over-the-ds client roaming which explains the sequence of messages that will be exchanged between the client, current AP and target AP is given below




The following steps describe the message exchange in the case where a client is roaming between APs, AP1 and AP2, connected to the NGWC.

1. Client is associated with AP1 and wants to roam to AP2
2. Client sends FT Authentication Request to AP1 and receives FT Authentication Response from AP1
3. The APs are connected to same NGWC, hence the pre-Authentication info is sent from the controller to AP2
4. Client sends a Reassociation Request to AP2 and receives a Reassociation Response from AP2
5. Client completes its roam from AP1 to AP2

**The 802.11 message exchanges are given in the diagram below**

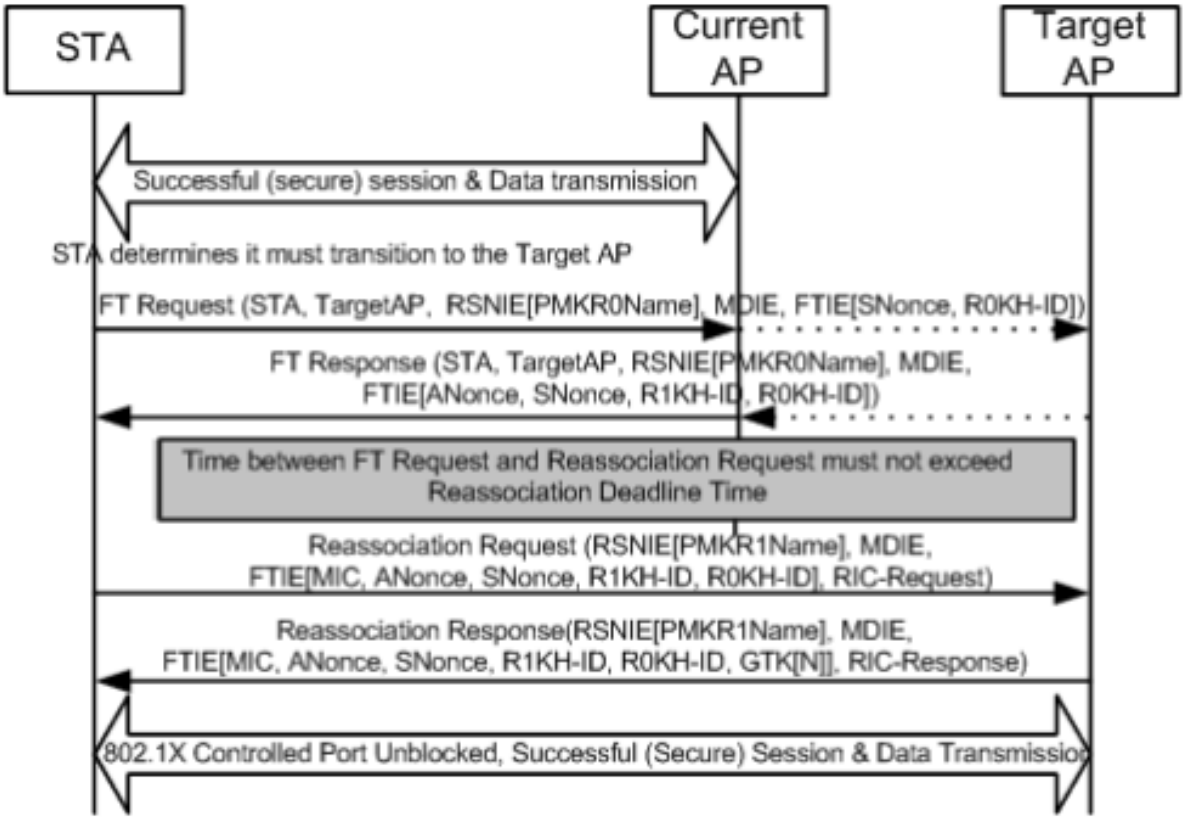



**Figure 7: Fast BSS Transition over-the-ds in an RSN**

**Web UI Configuration for Fast Transition Roaming**

802.11r fast transition roaming can be configured using the GUI under the WLAN.

1. Click on WLAN->Security->Layer2. Make sure that Layer 2 Security is WPA+WPA2 or Open.
2. Enable check box Fast Transition. This will enable Over the Air FT for the WLAN.
3. To enable Over the DS FT, click on check box Over the DS
4. Reassociation Timeout can be configured between 1-100 seconds, the default being 20 sec. The time between FT Authentication Request and Re-association Request must not exceed Re-association Timeout

**Config / Debug commands**

```
Controller(config-wlan)#security wpa akm ft ?
 dot1x          Configures 802.1x support
 psk            Configures PSK support

Controller#debug dot11 dot11r ?
 all            all
 events         802.11r event
```

| | |
|---|---|
| keys | 802.11r keys |

Controller#set trace dot11 dot11r ?

| | |
|---|---|
| event | 802.11r event debugging |
| filter | Trace Adapted Flag Filter |
| keys | 802.11r keys debugging |
| level | Trace Level |

**Limitations**

• Supported only on OPEN and WPA2 WLANs
• This feature will not be supported with LEAP since LEAP only comes up with a 32 byte MSK and other EAP types come up with a 64 byte MSK.
• The domain of 802.11r is confined to the Mobility Group which means all 11r roaming will be supported between clients within the same mobility group.
• FT Resource request protocol will not be supported in this release since clients also do not have this support.
• Each controller will allow a maximum of 3 FT handshake with different APs under its control.