802.11r BSS Fast Transition Deployment Guide

First Published: 2016-07-06

802.11r BSS Fast Transition

Information About 802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, 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, which is called Fast Transition (FT). 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 reassociation request or response exchange with new target AP.

802.11r provides two methods of roaming:

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

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

From Release 8.0, you can create an 802.11r WLAN that is also an WPAv2 WLAN. In earlier releases, you had to create separate WLANs for 802.11r and for normal security. Non-802.11r clients can now join 802.11r-enabled WLANs as the 802.11r WLANs can accept non-802.11r associations. If clients do not support mixed mode or 802.11r join, they can join non-802.11r WLANS. When you configure FT PSK and later define PSK, clients that can join only PSK can now join the WLAN in mixed mode.

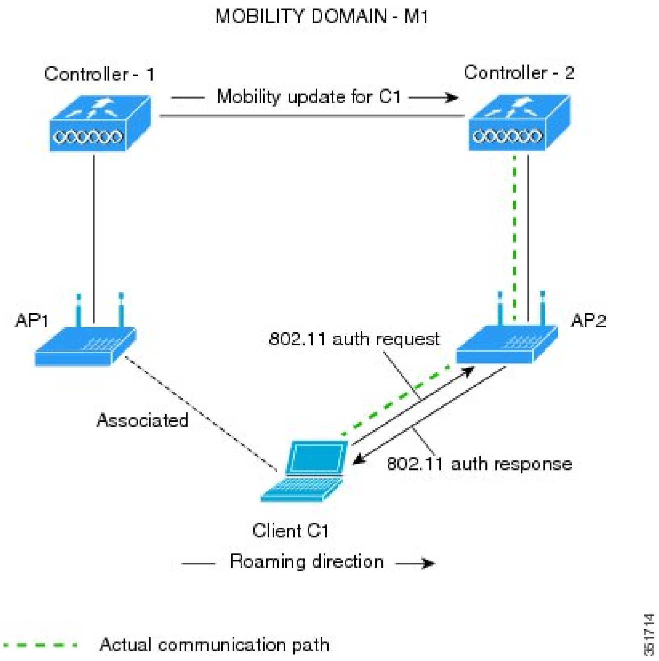
How a Client Roams

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

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-DS—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.

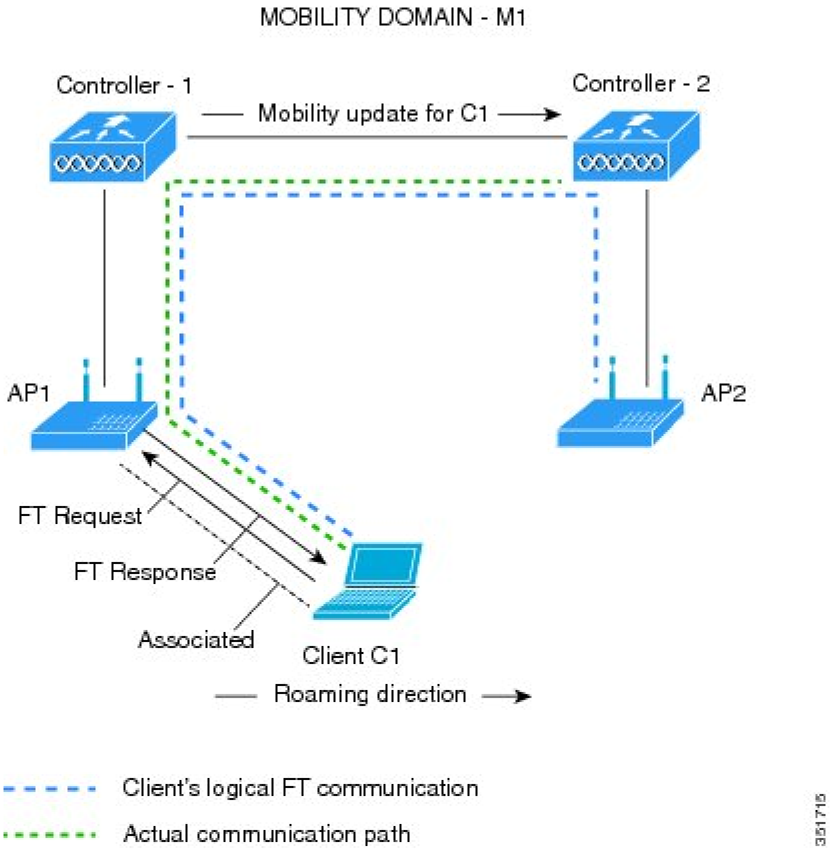
This figure shows the sequence of message exchanges that occur when Over the Air client roaming is configured.

Figure 1: Message Exchanges when Over the Air client roaming is configured



This figure shows the sequence of message exchanges that occur when Over the DS client roaming is configured.

Figure 2: Message Exchanges when Over the DS client roaming is configured



Restrictions for 802.11r Fast Transition

- This feature is not supported on mesh access points.
- In 8.1 and earlier releases, this feature is not supported on access points in FlexConnect mode. In Release 8.2, this restriction is removed.
- For access points in FlexConnect mode:
    - 802.11r Fast Transition is supported in central and locally switched WLANs.
    - This feature is not supported for the WLANs enabled for local authentication.
    - 802.11r client association is not supported on access points in standalone mode.
    - 802.11r fast roaming is not supported on access points in standalone mode.
    - 802.11r fast roaming between local authentication and central authentication WLAN is not supported.
    - 802.11r fast roaming works only if the APs are in the same FlexConnect group.

- 802.11r fast roaming is not supported if the client uses Over-the-DS preauthentication in standalone mode.
- EAP LEAP method is not supported. WAN link latency prevents association time to a maximum of 2 seconds.
- The service from standalone AP to client is only supported until the session timer expires.
- TSpec is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.
- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The Cisco WLC handles 802.11r Fast Transition authentication request during roaming for both Over-the-Air and Over-the-DS methods.
- This feature is supported on open and WPA2 configured WLANs.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

  The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r enabled WLANs.

  Another workaround is to have two SSIDs with the same name but with different security settings (FT and non-FT).
- Fast Transition resource request protocol is not supported because clients do not support this protocol. Also, the resource request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each Cisco WLC allows a maximum of three Fast Transition handshakes with different APs.
- Non-802.11r capable devices will not be able to associate with FT-enabled WLAN.
- 802.11r FT + PMF is not recommended.
- 802.11r FT Over-the-Air roaming is recommended for FlexConnect deployments.
- In a default FlexGroup scenario, fast roaming is not supported.

Configuring 802.11r Fast Transition (GUI)

Step 1 Choose **WLANs** to open the **WLANs** window.

Step 2 Click a WLAN ID to open the **WLANs > Edit** window.

Step 3 Choose **Security** > **Layer 2** tab.

Step 4 From the **Layer 2 Security** drop-down list, choose **WPA+WPA2**.
The Authentication Key Management parameters for Fast Transition are displayed.

Step 5 From the **Fast Transition** drop-down list, choose Fast Transition on the WLAN.

Step 6 Check or uncheck the **Over the DS** check box to enable or disable Fast Transition over a distributed system.

This option is available only if you enable Fast Transition or if Fast Transition is adaptive.

To use 802.11r Fast Transition over-the-air and over-the-ds must be disabled.

Step 7 In the **Reassociation Timeout** field, enter the number of seconds after which the reassociation attempt of a client to an AP should time out. The valid range is 1 to 100 seconds.

Note This option is available only if you enable Fast Transition.

Step 8 Under Authentication Key Management, choose **FT 802.1X** or **FT PSK**. Check or uncheck the corresponding check boxes to enable or disable the keys. If you check the **FT PSK** check box, from the PSK Format drop-down list, choose **ASCII** or **Hex** and enter the key value.

Note When Fast Transition adaptive is enabled, you can use only **802.1X** and **PSK AKM.**.

Step 9 From the **WPA gtk-randomize State** drop-down list, choose **Enable** or **Disable** to configure the Wi-Fi Protected Access (WPA) group temporal key (GTK) randomize state.

Step 10 Click **Apply** to save your settings.

Configuring 802.11r Fast Transition (CLI)

Step 1 To enable or disable 802.11r fast transition parameters, use the **config wlan security ft** {**enable** | **disable**} *wlan-id* command.

Step 2 To enable or disable 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** {**enable** | **disable**} *wlan-id* command.
The Client devices normally prefer fast transition over-the-ds if the capability is advertised in the WLAN. To force a client to perform fast transition over-the-air, disable fast transition over-the-ds.

Step 3 To enable or disable the authentication key management for fast transition using preshared keys (PSK), use the **config wlan security wpa akm ft psk** {**enable** | **disable**} *wlan-id* command.
By default, the authentication key management using PSK is disabled.

Step 4 To enable or disable authentication key management for adaptive using PSK, use the **config wlan security wpa akm psk** {**enable** | **disable**} *wlan-id* command.

Step 5 To enable or disable authentication key management for fast transition using 802.1X, use the **config wlan security wpa akm ft-802.1X** {**enable** | **disable**} *wlan-id* command.
By default, authentication key management using 802.1X is enabled.

Step 6 To enable or disable authentication key management for adaptive using 802.1x, use the **config wlan security wpa akm 802.1x** {**enable** | **disable**} *wlan-id* command.

Note When Fast Transition adaptive is enabled, you can use only 802.1X and PSK AKM.

Step 7 To enable or disable 802.11r fast transition reassociation timeout, use the **config wlan security ft reassociation-timeout** *timeout-in-seconds wlan-id* command.
The valid range is 1 to 100 seconds. The default value of reassociation timeout is 20 seconds.

Step 8 To view the fast transition configuration on a WLAN, use the **show wlan** *wlan-id* command.

Step 9 To view the fast transition configuration on a client, use the **show client detail** *client-mac* command.

Note This command is relevant only for a connected or connecting client station (STA).

Step 10 To enable or disable debugging of fast transition events, use the **debug ft events** {**enable** | **disable**} command.

Troubleshooting 802.11r BSS Fast Transition

Symptom	Resolution
Non-802.11r legacy clients are no longer connecting.	Check if the WLAN has FT enabled. If so, non-FT WLAN will need to be created.
When configuring WLAN, the FT setup options are not shown.	Check if WPA2 is being used (802.1x / PSK). FT is supported only on WPA2 and OPEN SSIDs.
802.11r clients appear to reauthenticate when they do a Layer 2 roam to a new controller.	Check if the reassociation timeout has been lowered from the default of 20 by navigating to **WLANs** > *WLAN Name* > **Security** > **Layer 2** on the controller GUI.

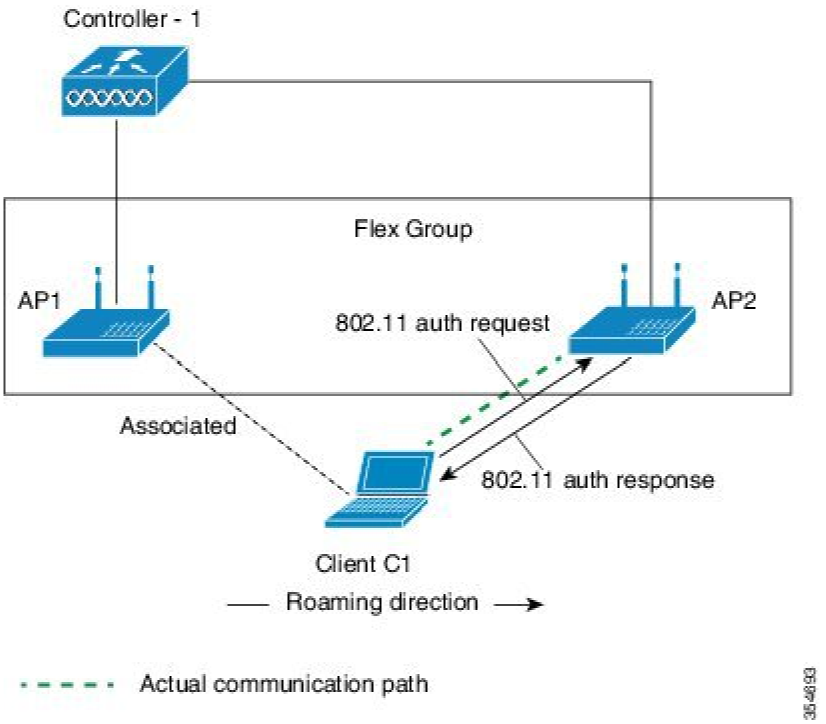
802.11r BSS Fast Transition on FlexConnect Deployment

In a FlexConnect Deployment scenario, 802.11r BSS FT roaming is supported between APs within the same FlexConnect group. To enable seamless roaming, the 802.11r Key Cache is distributed to all the APs in the same FlexConnect Group. The Key Cache distribution is done by the Cisco WLC after the client device does the initial FT association through Central Authentication.

The Flex deployment supports both Over-the-Air and Over-the-DS roaming. Both the roaming scenarios are illustrated below:

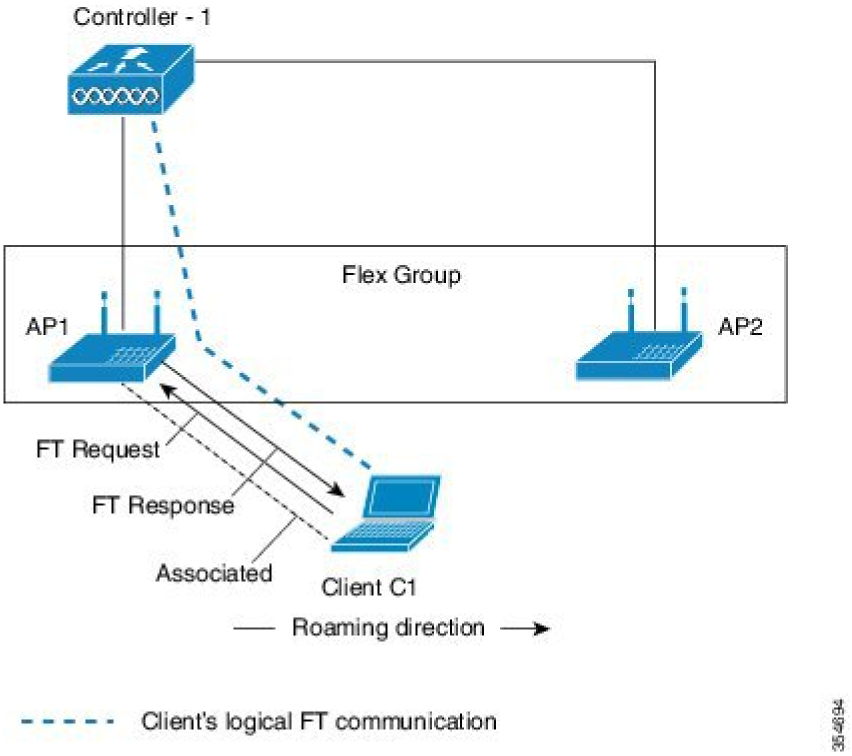
Over-the-Air Roaming

Figure 3: Over-the-Air Roaming Scenario



Over-the-DS Roaming

Figure 4: Over-the-DS Roaming Scenario



Optimizations for FlexConnect Deployment

The 802.11r Fast Transition (FT) feature for FlexConnect mode APs is optimized such that the FT authentication request process and validation occur at Cisco AP itself and the Cisco AP itself sends FT authentication response. There is no change in the key derivation system.

Note This new design is applicable only to FlexConnect central authentication topology. In a FlexConnect local authentication scenario, 802.11r BSS Fast Transition is not supported.

Authentication Request

1. The Cisco AP forwards the FT authentication request to Cisco WLC as well for processing.
2. Upon receiving the FT authentication response from Cisco WLC, the Cisco AP checks if it is a success:
   - If successful, the Cisco AP consumes the packet.
   - If unsuccessful, the Cisco AP sends the deauthentication notification to the client.
3. ANonce is derived at Cisco AP and sent to Cisco WLC by piggybacking the FT authentication request's ANonce field.

Note ANonce used for key derivation at Cisco WLC and Cisco AP is the same.

Authentication and Association Request

1. FT authentication request and association request are sent in parallel to Cisco WLC to validate and process.
2. Cisco AP intercepts the FT auth response and reassociation response from Cisco WLC and checks if it is successful:
    - If successful, Cisco AP consumes success response as it has already been sent by the Cisco AP.
    - If unsuccessful, Cisco AP sends deauthentication to client.

Note The key derivation occurs at both Cisco AP and Cisco WLC.