



802.11r, 802.11k, 802.11v, 802.11w Fast Transition Roaming

802.11r Fast Transition Roaming

The 802.11r Fast Transition (FT) Roaming is an amendment to the 802.11 IEEE standards. It is a new concept for roaming. The initial handshake with the new Access Point (AP) occurs before client roams to the target AP, called as Fast Transition (FT).

Initial handshake allows the client and APs to do Pairwise Master Key (PMK) calculation in advance. Once the client performs the re-association request or response exchange with the new AP, the PMK keys are applied to the client and AP. The FT key hierarchy allows clients to make fast Base Station Subsystem (BSS) transitions between APs without the need for re-authentication at every AP. 802.11r eliminates the handshake overhead while roaming and thereby reduces the hand off times between APs, which provides security and QoS. It is useful for client devices with delay-sensitive applications, such as, voice and video over Wi-Fi.

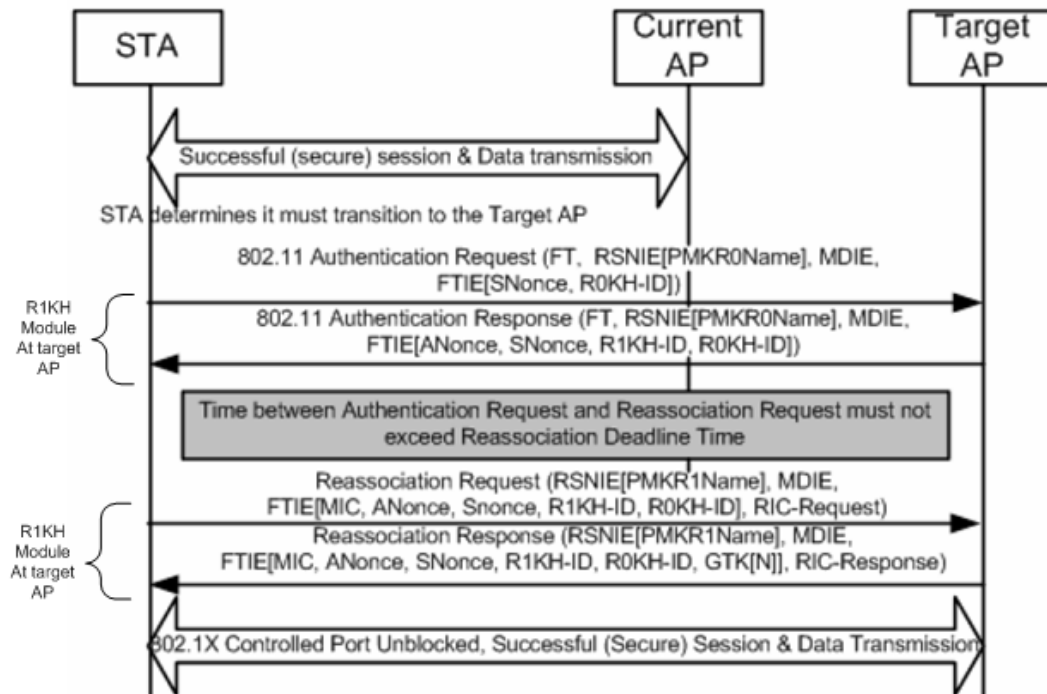
Methods of Client Roaming

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

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

Over-the-Air Fast Transition Roaming

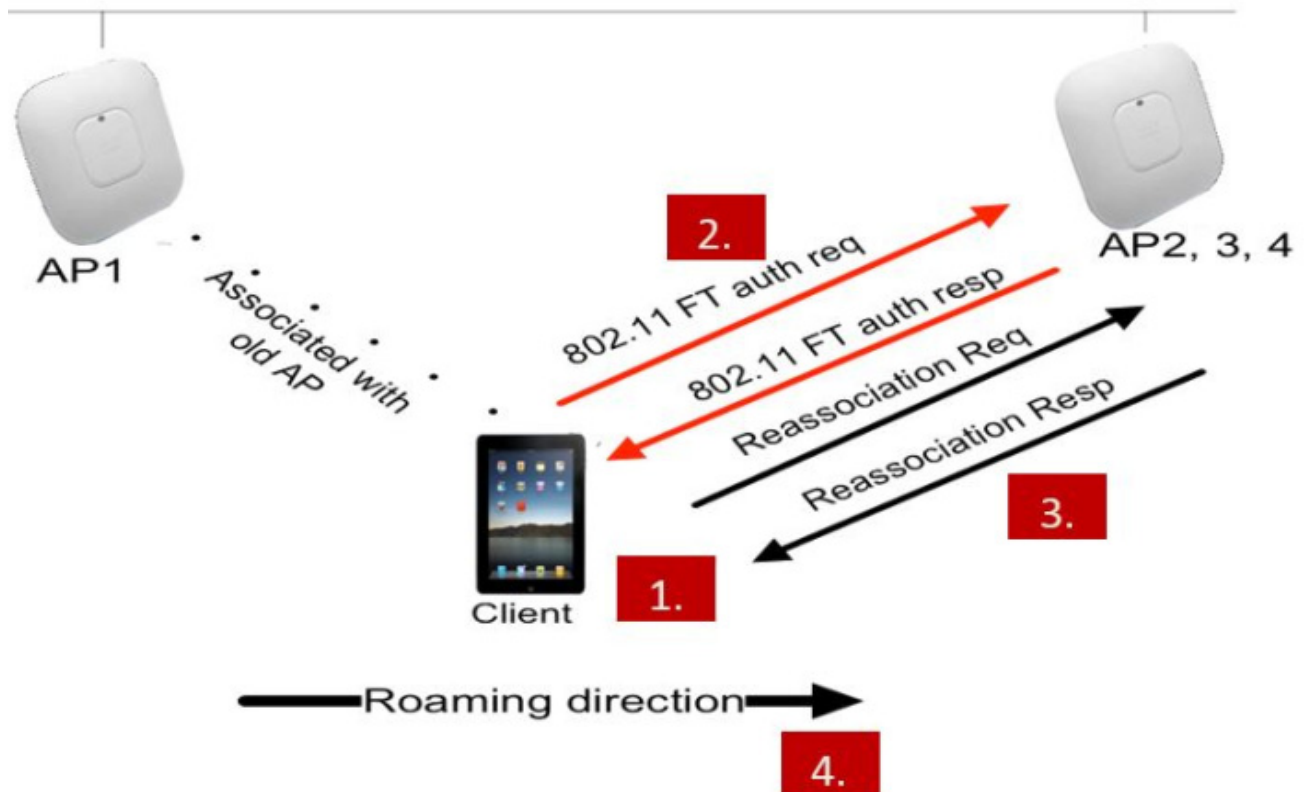
The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.

Figure 11-1 Fast BSS Transition over-the Air in RSN**Roaming Over-the-Air Intra Controller**

When a client is roaming between AP1 and AP2 that are connected to the same controller, the following steps take place by default:

-
- Step 1** Client associates with AP1 and requests to roam with AP2.
 - Step 2** Client sends a FT Authentication Request to AP2 and receives a FT Authentication Response from AP2.
 - Step 3** Client sends a FT Re-association Request to AP2 and receives a FT Re-association Response from AP2.
 - Step 4** Client completes its roam from AP1 to AP2.
-

Figure 11-2 Over-the-Air Intra Controller Roam

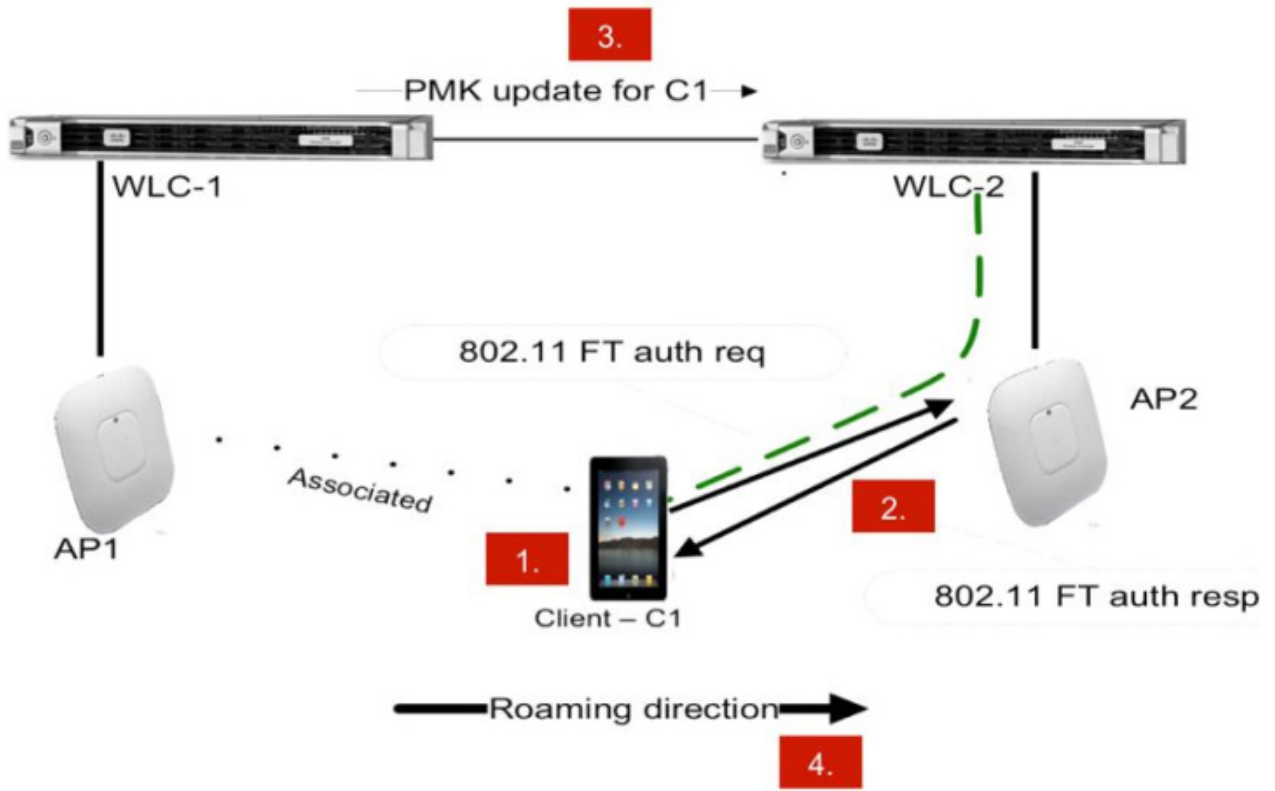


Roaming Over the Air Inter Controller

When a client is roaming between AP1 and AP2 which are connected to different controllers such as WLC1 and WLC2, respectively, within mobility group, the following steps take place by default:

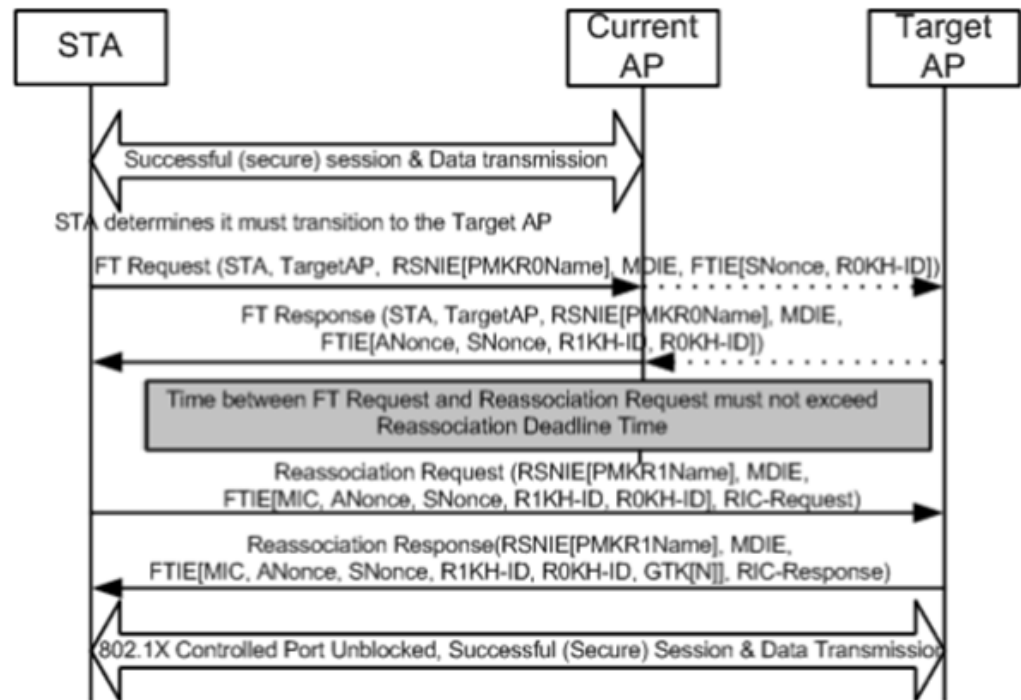
-
- Step 1** Client associates with AP1 and requests to roam with AP2.
 - Step 2** Client sends a FT Authentication Request to AP2 and receives a FT Authentication Response from AP2.
 - Step 3** WLC-1 sends PMK and mobility message to WLC-2 about the roaming client that uses mobility infrastructure.
 - Step 4** Client completes its roam from AP1 to AP2.
-

Figure 11-3 Over-the-Air Inter Controller Roam



Over-the-Distribution System Fast Transition Roaming

In roaming over the DS, the client communicates with the target AP through the current AP. The communication is in FT action frames between the client and the current AP through the controller.

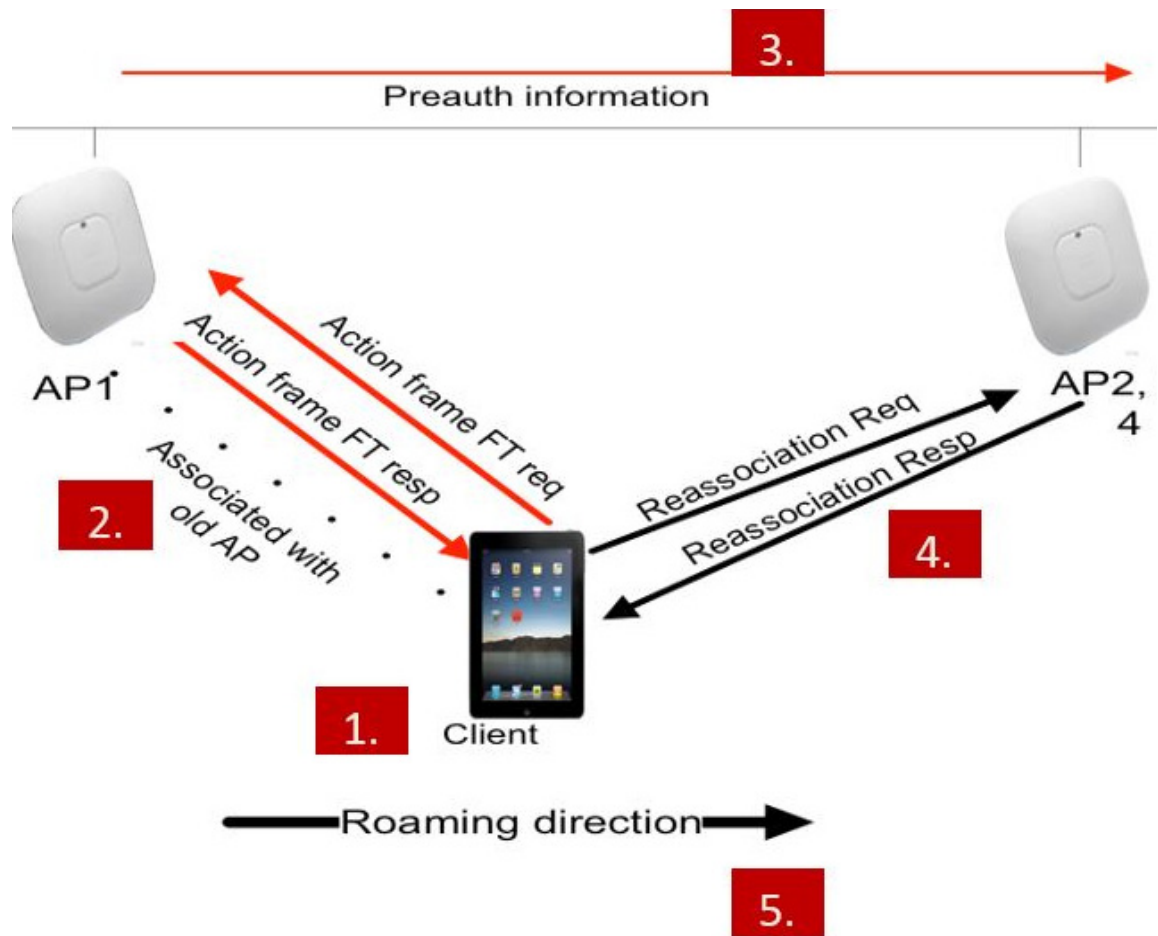
Figure 11-4 **Roaming Over the DS**

Roaming Over the DS Intra Controller

When a client is roaming between AP1 and AP2 that are connected to the same controller, the following steps take place by default:

-
- Step 1** Client associates with AP1 and requests to roam with AP2.
 - Step 2** Client sends a FT Authentication Request to AP1 and receives a FT Authentication Response from AP1.
 - Step 3** The controller sends the pre-authentication information to AP2 as the APs are connected to the same controller.
 - Step 4** Client sends a FT Re-association Request to AP2 and receives a FT Re-association Response from AP2.
 - Step 5** Client completes its roam from AP1 to AP2.
-

Figure 11-5 Over the DS intra controller roam

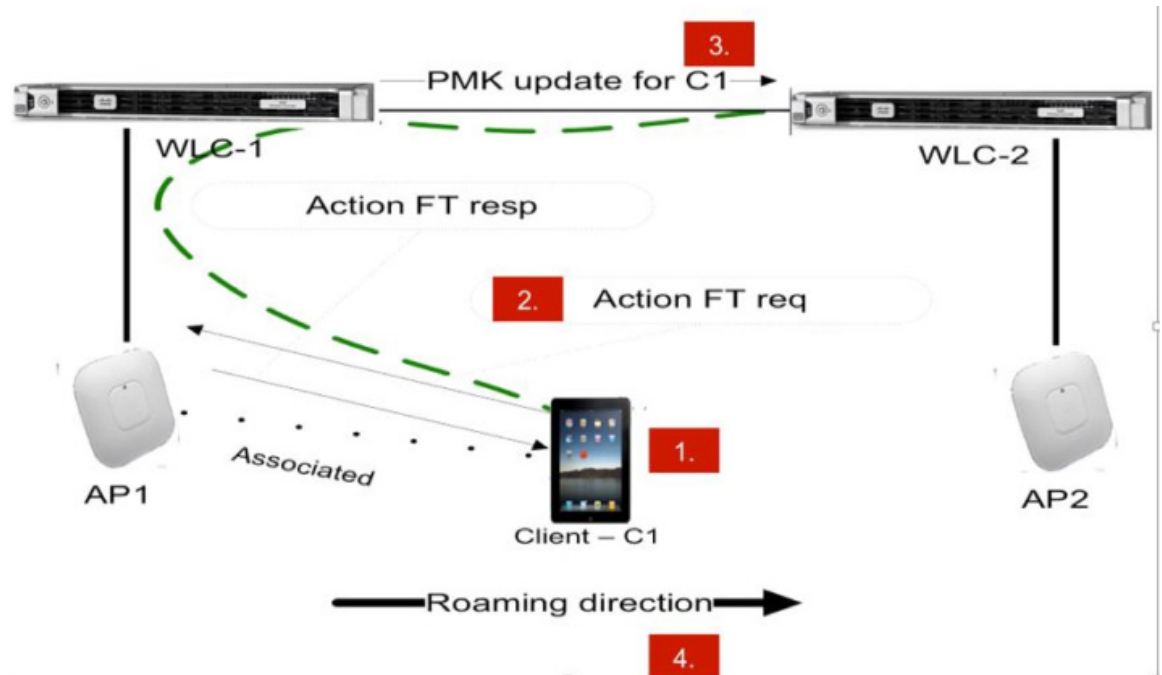


Roaming Over the DS Inter Controller

When a client is roaming between AP1 and AP2 that are connected to the different controllers such as WLC1 and WLC2 respectively within a mobility group, the following steps take place by default:

-
- Step 1** Client associates with AP1 and requests to roam with AP2.
 - Step 2** Client sends a FT Authentication Request to AP1 and receives a FT Authentication Response from AP1.
 - Step 3** WLC-1 sends Pairwise Master Key (PMK) and mobility message to WLC-2 about the roaming client.
 - Step 4** Client completes its roam from AP1 to AP2.
-

Figure 11-6 Over the DS Inter Controller Roam



Configuring Fast Transition Roaming using GUI

To configure FT Roaming using GUI, perform the following steps:

- Step 1** Click **WLANS**.
- Step 2** Choose **WLAN ID > Edit page**.
- Step 3** Choose **Security > Layer 2** tab.
- Step 4** Choose **WPA+WPA2** from the drop-down list.
The Authentication Key Management parameter for FT appears.
- Step 5** Check the **Fast Transition** check box to enable FT.
- Step 6** Check the **Over the DS** check box to enable FT over a DS.



Note The **Over the DS** check box gets enabled only when you enable FT.

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



Note The **Reassociation Timeout** field gets enabled only when you enable FT.

Figure 11-7 Setting up Reassociation Timeout

The screenshot shows the configuration interface for a wireless network. The 'Security' tab is selected, and the 'Layer 3' sub-tab is active. Under 'Layer 2 Security', 'WPA+WPA2' is selected. 'MAC Filtering' is disabled. In the 'Fast Transition' section, 'Fast Transition' is checked, 'Over the DS' is checked, and 'Reassociation Timeout' is set to 20 seconds. The 'Protected Management Frame' section shows 'PMF' as 'Disabled'. The 'WPA+WPA2 Parameters' section shows 'WPA Policy' unchecked, 'WPA2 Policy' checked, and 'WPA2 Encryption' set to 'AES'. The 'Authentication Key Management' section shows '802.1X' unchecked.

- Step 8** Under **Authentication Key Management**, check the **Enable** check box of either **FT 802.1X** or **FT PSK** to enable the key. To disable the key, uncheck the **Enable** check box.



Note If you check the **FT PSK** check box, from the **PSK Format** drop-down list, choose **ASCII** or **Hex** and enter the key value.

- Step 9** Choose **Enable** or **Disable** from the **WPA gtk-randomize State** drop-down list, to configure the WPA Group Temporal Key (GTK) to randomize state.

Figure 11-8 Security - Layer 2 - FT PSK

General **Security** **QoS** **Policy-Mapping** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☒

WPA2 Encryption ☒ AES ☐ TKIP

Authentication Key Management [19](#)

802.1X ☐ Enable

CCKM ☐ Enable

PSK ☐ Enable

FT 802.1X ☐ Enable

FT PSK ☒ Enable

PSK Format

WPA gtk-randomize State [14](#)

Step 10 Click **Apply**.

Configuring Fast Transition Roaming using CLI

To configure FT Roaming, enter the following commands:

config wlan security ft {enable disable} wlan-id	Enable or disable 802.11r fast transition parameters.
config wlan security ft over-the-ds {enable disable} wlan-id	Enable or disable 802.11r fast transition parameters over a distributed system. This is disabled, by default.
config wlan security ft reassociation-timeout timeout-in-seconds wlan-id	Enables 802.11r fast transition reassociation timeout. The range is between 1 to 100 seconds.

The WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

```
config wlan security wpa akm ft-psk {enable | disable} wlan-id
config wlan security wpa akm ft-802.1X {enable | disable} wlan-id
```

Enable or disable the AKM for FT over a DS, enter the following command:

```
config wlan security wpa akm ft over-the-ds {enable | disable} wlan-id
```

To view the WLAN and FT parameters on the WLAN, enter the following command:

```
show wlan wlan-id
```

Troubleshooting Support

- Enable or disable debugging of FT events, using the following command:
`debug ft events {enable | disable}`
- Enable or disable debugging of key generation for FT, using the following command:
`debug ft keys {enable | disable}`

Restrictions for 802.11r Fast Transition

- 802.11r FT feature does not support Mesh APs.
- 802.11r FT feature is not supported on Linux-based APs such as Cisco 600 Series OfficeExtend APs.
- 802.11r fast roaming is not supported on FlexConnect APs in standalone mode.
- 802.11r fast roaming between local authentication and central authentication WLAN is not supported with FlexConnect APs.
- 802.11r fast roaming is not supported if the client uses Over-the-DS pre-authentication in standalone mode on FlexConnect access points.
- The EAP LEAP method is not supported. The WAN link latency prevents association time to a maximum of 2 seconds.
- When a FlexConnect AP moves to standalone mode, existing clients connects until the session timer expires. A new 11r client does not accept while the AP is in standalone mode.
- 802.11r fast roaming does not support Traffic Specification (TSPEC). Therefore, it does not support RIC IE handling.
- If the WAN link latency exists for FlexConnect APs, fast roaming delays. Verify the voice or data maximum latency. The controller handles 802.11r FT authentication request during roaming for both Over-the-Air and Over-the-DS methods.
- The 802.11r FT feature supports only on open and WPA2 configured WLANs.
- Few 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 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).
- 802.11r does not support FT resource request protocol because there are no clients to implement FT resource request protocol. Also, the resource request protocol is optional in the 802.11r amendment.
- To avoid any Denial of Service (DoS) attack, each controller allows a maximum of three FT handshakes with different APs.

802.11k Assisted Roaming

The 802.11k allows 11k capable clients to request a neighbor report containing information about known neighbor APs that are candidates for roaming.

To facilitate roaming, an 11k capable client associated with an AP sends request to a list of neighbor APs. The request is send in the form of an 802.11 management frame, known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with their Wi-Fi channel numbers. The response is also an action frame. The client identifies the APs candidates for the next roam from the response frame. The use of 802.11k radio resource management (RRM) process allows the client to roam efficiently and quickly.

To find an AP to roam from the neighbor list information, the 11k capable client does not probe all of the 2.4 GHz and 5 GHz channels. Client does not probe all the channels to reduce channel utilization, thereby, it increases bandwidth on all channels. It reduces roam time and improves the decisions taken by the client. Additionally, it increases battery life of the device as it neither changes the radio configuration for each channel nor sends probe requests on each channel. It avoids the device to process all the probe response frames.

Assisted Roaming with 802.11k

The 802.11k standard allows clients to request neighbor reports containing information about known neighbor APs that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning.

The assisted roaming feature is based on an intelligent and client optimized neighbor list. The 802.11k neighbor list is generated dynamically on-demand and is not maintained on the controller. Two clients on the same controller but different APs can have different neighbor lists delivered depending on their individual relationship with the surrounding APs.

By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, the dual-list configuration allows 802.11k to return neighbors in both bands.

Clients send requests for neighbor lists only after they associate with the APs that advertise the Radio Management (RM) capability Information Element (IE) in the beacon. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios.

Assembling and Optimizing the Neighbor List

When the controller receives a request for an 802.11k neighbor list, the following occurs:

1. The controller searches the RM neighbor table for a list of neighbors on the same band as AP, with which the client is currently associated.
2. The controller checks the neighbors according to the Received Signal Strength Indication (RSSI) between the APs, the current location of the present AP, the floor information of the neighboring AP from Cisco Prime Infrastructure, and roaming history information on the controller to reduce the list of neighbors to six per band. The list is optimized for APs on the same floor.

802.11k Information Elements (IEs)

Clients send requests for neighbor lists only after they associate with the APs that advertise the RM capability Information Element (IE) in the beacon.

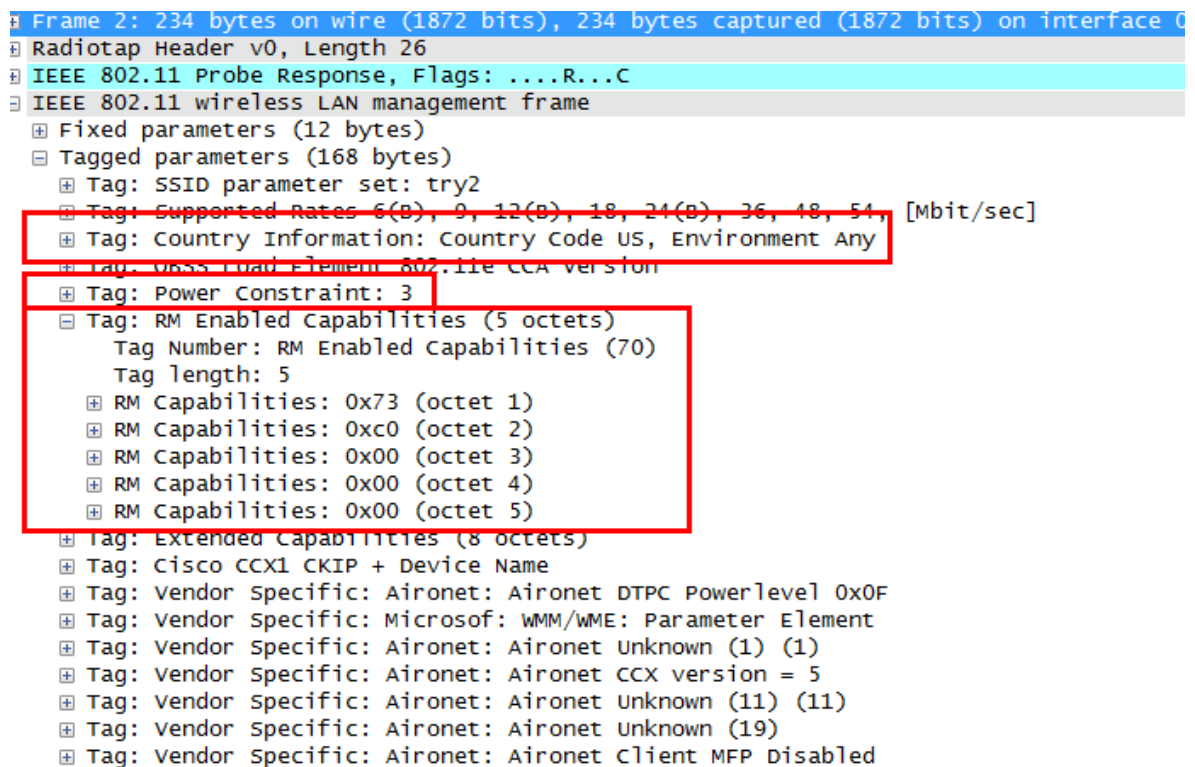
The following elements are implemented in the beacon and probe response on the AP to ensure smooth integration with Apple handheld devices:

- *Country Element*—The Country Information Element contains the information required to allow a station to identify the regulatory domain in which the station is located and to configure its PHY for operation in that regulatory domain.
- *Power Constraint Element*—The power constraint element contains the information necessary to allow a client to determine the local maximum transmit power in the current channel.
- *RM Enable Capabilities Element*—The RM Capabilities element is five octets long. When this element is included in a beacon or probe response, it uses bit 1 to signal so that the AP can provide neighbor list. When used in an association request, bit 1 signifies the client's request for a neighbor list.

The presence of all three of these IEs signifies that this SSID is configured to provide a neighbor list on request. For this release we send neighbor list based on the request from the client and not on the neighbor list capability of the client in the IE.

The following Wireshark capture displays these information elements:

Figure 11-9 802.11k information elements



Configuring Assisted Roaming using GUI

To configure Fast Transition Roaming using GUI, perform the following steps:

- Step 1** Click WLANs.

- Step 2** Choose **WLAN ID > Edit** page.
- Step 3** Click **Advanced** tab.
- Step 4** In the **11k** area, check the **Neighbor List** and **Neighbor List Dual Band** check box.

Figure 11-10 Advanced Tab - Neighbor List

The screenshot displays the 'Advanced' configuration tab for a WLAN. It features several sections: 'General' (Vlan based Central Switching, Central DHCP Processing, Override DNS, NAT-PAT, Central Assoc), 'Lync' (Lync Server), and '11k' (Assisted Roaming Prediction Optimization, Neighbor List, Neighbor List Dual Band). The '11k' section is highlighted with a red rectangular box. Within this box, the 'Assisted Roaming Prediction Optimization' checkbox is checked and labeled 'Enabled'. Below it, the 'Neighbor List' checkbox is checked and labeled 'Enabled', and the 'Neighbor List Dual Band' checkbox is also checked and labeled 'Enabled'.

Configuring Assisted Roaming using CLI

To configure Assisted Roaming enter the following commands:

config wlan assisted-roaming neighbor-list enable <i>wlan-id</i>	Configures an 802.11k neighbor list for a WLAN. By default, assisted roaming is enabled on the neighbor list when you create a WLAN. The no form of the command disables assisted roaming neighbor list.
config wlan assisted-roaming dual-list enable <i>wlan-id</i>	Configures a dual-band 802.11k dual list for a WLAN. By default, assisted roaming is enabled on the dual list when you create a WLAN. The no form of the command disables assisted roaming dual list.
config wireless assisted-roaming floor-bias <i>dBm</i>	Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.

Prediction Based Roaming-Assisted Roaming for Non-802.11k Clients

You can optimize roaming for non-802.11k clients by generating a prediction neighbor list for each client without sending an 802.11k neighbor list request. When prediction based roaming enables a WLAN, after each successful client association/re-association, the same neighbor list optimization applies on the non-802.11k client to generate and store the neighbor list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by the different neighbors as the clients usually probe before any association or re-association. This list is created with the most updated probe data and predicts the next AP that the client is likely to roam to.

The wireless infrastructure discourages clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

- **Denial count**—Maximum number of times a client is refused association.
- **Prediction threshold**—Minimum number of entries required in the prediction list for the assisted roaming feature to activate.

Configuring Prediction Based Roaming using GUI

To configure Prediction Based Roaming using GUI, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Click WLANs . |
| Step 2 | Choose WLAN ID > Edit page. |
| Step 3 | Click Advanced tab. |
| Step 4 | In the 11k area, check the Assisted Roaming Prediction Optimization check box. |

Figure 11-11 Advanced Tab - Assisted Roaming Prediction Optimization

The screenshot shows the 'Advanced' tab in a configuration interface. It contains several sections: 'General' with options like 'Vlan based Central Switching', 'Central DHCP Processing', 'Override DNS', 'NAT-PAT', and 'Central Assoc', all with 'Enabled' checkboxes. A 'Lync' section has a 'Lync Server' dropdown set to 'Disabled'. An '11k' section contains 'Assisted Roaming Prediction Optimization' (checked and highlighted with a red box), 'Neighbor List' (checked), and 'Neighbor List Dual Band' (checked).

Configuring Prediction Based Roaming using CLI

To configure Prediction Based Roaming enter the following commands:


```
config wlan
assisted-roaming prediction
{enable | disable} wlan-id
```

Configures assisted roaming prediction list for a WLAN. By default, the assisted roaming prediction list is disabled.



Note

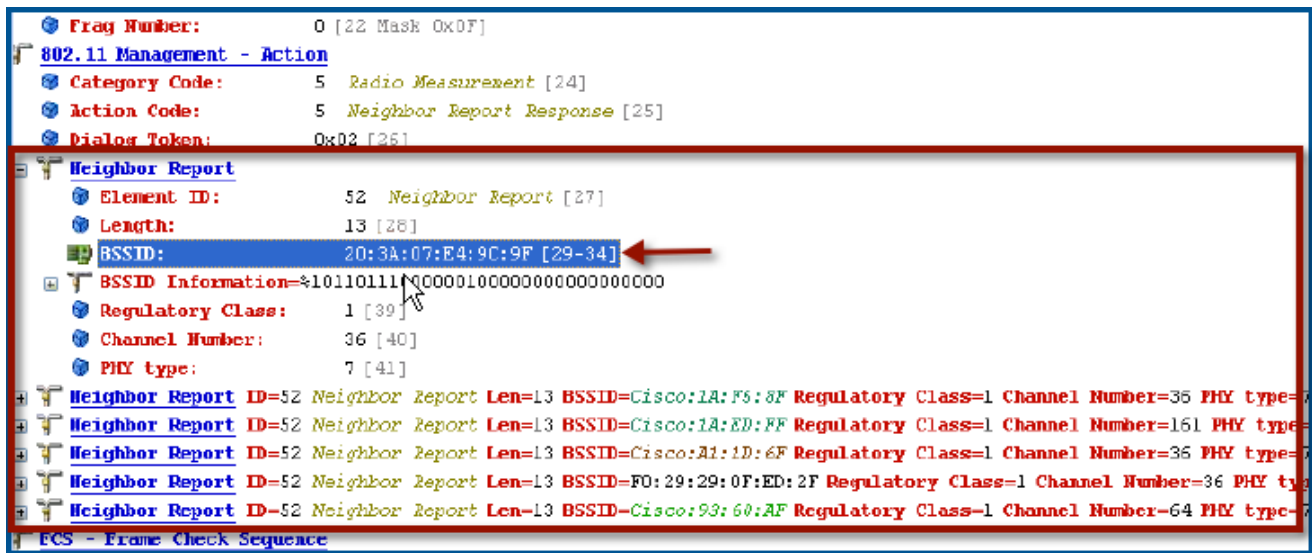
A warning message is displayed and load balancing is disabled for the WLAN, if load balancing is already enabled for the WLAN.

config assisted-roaming denial-maximum <i>count</i>	Configures the maximum number of times a client can deny association if the association request is sent to an AP which does not match any AP on the prediction. The valid range is from 1 to 10, and the default value is 5.
config assisted-roaming prediction-minimum <i>count</i>	Configures the minimum number of predicted APs required for the prediction list to activate. The default value is 3.
	
Note	If the number of AP in the prediction assigned to the client is less than the number that you specify, the assisted roaming does not apply on this roam.

Neighbor List Response

The neighbor list includes information about BSSID, channel and operation details of the neighboring radios as shown in the Wireshark capture below:

Figure 11-12 802.11k Neighbor Report



Troubleshooting Support

- Debug a client for assisted roaming, using the following command:
`debug mac addr client-mac-addr`
- Configure the debugging of all of the 802.11k events, using the following command:
`debug 11k all {enable | disable}`
- Configure the debugging of neighbor details, using the following command:
`debug 11k detail {enable | disable}`

- Configure the debugging of 802.11k errors, using the following command:
`debug 11k errors {enable | disable}`
- Verify the neighbor requests that are received, using the following command:
`debug 11k events {enable | disable}`
- Configure the debugging of the client roaming history, using the following command:
`debug 11k history {enable | disable}`
- Configure the debugging of 802.11k optimizations, using the following command:
`debug 11k optimization {enable | disable}`
- Get details of client roaming parameters that are to be imported for offline simulation, using the following command:
`debug 11k simulation {enable | disable}`

802.11v Max Idle Period, Directed Multicast Service

From Release 8.0, controller supports 802.11v amendment for wireless networks, which describes enhancements to wireless network management, such as:

- Network assisted Power Savings—Helps clients to improve battery life by enabling them to sleep longer. For example, mobile devices use a certain amount of idle period to ensure that they remain connected to access points and therefore consume more power when performing the following tasks in a wireless network.
- Network assisted Roaming—Enables the WLAN to send messages to associated clients, for better APs to associate with clients. This is useful for both load balancing and in directing poorly connected clients.

Enabling 802.11v Network Assisted Power Savings

Wireless devices consume battery to maintain their connection to the clients, in several ways:

- By waking up at regular intervals to listen to the access point beacons containing a DTIM, which indicates buffered broadcast or multicast traffic that the AP will deliver to the clients.
- By sending null frames to the access points, in the form of keep alive messages to maintain connection with APs.
- Devices also periodically listen to beacons (even in the absence of DTIM fields) to synchronize their clock to that of the corresponding AP.
- All these processes consume battery and this consumption impacts some devices (such as Apple), because these devices use conservative session timeout estimation, and therefore, wake up often to send keep alive messages. The 802.11 standard, without 802.11v, does not include any mechanism for the controller or the access points to communicate to the wireless clients about the session timeout for the local client.

To save the power of clients, the following features in the 802.11v standard are used:

- Directed Multicast Service (DMS)
- Base Station Subsystem (BSS) Maximum Idle Period

Directed Multicast Service

The client requests the access point to transmit the required multicast packet as unicast frames. This allows the client to receive the multicast packets that are ignored in sleep mode and also ensures Layer 2 reliability. The unicast frame is transmitted to the client at a potentially higher wireless link rate, which enables the client to receive the packet quickly by enabling the radio for a shorter duration, thus saves battery power. Since the wireless client does not wake up at each DTIM interval to receive multicast traffic, thus allows longer sleeping intervals.

Base Station Subsystem Maximum Idle Period

The BSS Max Idle period is the time frame during which an AP does not disassociate a client due to non-receipt of frames from the connected client. This ensures that the client device does not send keep alive messages frequently. The idle period timer value is transmitted using the association and re-association response frame from the AP to the client. The idle time value indicates the maximum time a client can remain idle without transmitting any frame to an AP. As a result, the clients remain in sleep mode for a longer duration without transmitting the keep alive messages. This in turn saves battery power.

Configuring 802.11v Network Assisted Power Savings using CLI

- Configure the value of BSS Max Idle period, using the following commands:

```
config wlan usertimeout wlan-id
config wlan bssmaxidle {enable | disable} wlan-id
```

- Configure the DMS, using the following command:

```
config wlan dms {enable | disable} wlan-id
```

Monitoring 802.11v Network Assisted Power Savings

- Display the DMS information on each radio slot on an AP, using the following command:

```
show controller d1/d0 | begin DMS
```

- Track the DMS requests processed by the controller, using the following commands:

```
debug 11v all {enable | disable}
debug 11v errors {enable | disable}
debug 11v detail {enable | disable}
```

Troubleshooting Support

- Enable or disable 802.11v debug, using the following command on the WLC:

```
debug 11v detail
```

- Track the DMS requests processed by an access point, using the following command on the AP:

```
debug dot11 dot11v
```

Managing 802.11v BSS Transition

802.11v BSS Transition is applied to the following three scenarios:

- **Solicited request**—Client can send an 802.11v BSS Transition Management Query before roaming for a better option of AP to re-associate with a client.
- **Unsolicited Load Balancing request**—If an AP is heavily loaded, it sends out an 802.11v BSS Transition Management Request to an associated client.
- **Unsolicited Optimized Roaming request**—If a client's RSSI and rate do not meet the requirement, AP sends out an 802.11v BSS Transition Management Request to this client.

802.11v BSS Transition Management Request is a suggestion given to client. Client can make its own decision whether to follow the suggestion or not. To force disassociating a client, you can turn on the disassociation-imminent function. This function is to disassociate the client after a period of time if the client does not re-associate to another AP.

Optimized Roaming + 802.11v

Disassociation function

Optimized Roaming behavior: Check client stats every 90 seconds(or less), if RSSI fails & data rate fails, disassociate the client.

Optimized Roaming + 802.11v behavior: If client is BSS Transition capable, instead of disassociating the client, send the client BSS Transition Request

Association RSSI check

Optimized Roaming behavior: During client association, check client RSSI. If RSSI check fails, don't allow the client to associate.

Optimized Roaming + 802.11v behavior: If client is BSS Transition capable, allow the client to associate, but also send the client BSS Transition Request

Load Balancing + 802.11v

Similar to Optimized roaming, If we just reject the client when Load Balancing fails then client might not have a clear sense of which AP to associate to and would most likely retry the same loaded AP over and over again.

With 11v BSS Transition, the client will not try the loaded AP but has the opportunity to pick an AP from the provided list to join.

Configuring 802.11v BSS Transition Management using GUI

To configure 802.11v BSS Transition Management using GUI, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Click WLANS . |
| Step 2 | Choose WLAN ID > Edit page . |

Step 3 Click **Advanced** tab.

Step 4 In the **11v BSS Transition Support** area, enter the values in the **Disassociation Time** and **Optimized Roaming Disassociation Timer** fields.

Figure 11-13 Advanced Tab - 11v BSS Transition Support

PMIP Mobility Type ☐

PMIP NAI Type Hexadecimal

PMIP Profile None

PMIP Realm

Universal AP Admin Support

Universal AP Admin ☐

11v BSS Transition Support

BSS Transition ☐

Disassociation Imminent ☐

Disassociation Timer(0 to 3000 TBTT) 200

Optimized Roaming Disassociation Timer(0 to 40 TBTT) 40

Tunneling

Tunnel Profile None

mDNS

mDNS Snooping ☐ Enabled

Configuring 802.11v BSS Transition Management using CLI

To enable 802.11v BSS transition management on a controller, enter the following commands:

config wlan bss-transition enable <i>wlan-id</i>	Enables 802.11v BSS transition.
config wlan disassociation-imminent enable <i>wlan-id</i>	Disassociates the STA.
config wlan bss-transition disassociation-imminent oproam-timer <i><timer> <WLAN id></i>	For Unsolicited Optimized Roaming Requests (TBTT = beacon intervals).
config wlan bss-transition disassociation-imminent timer <i><timer> <WLAN id></i>	For solicited and unsolicited requests.

Troubleshooting 11v BSS transition

To troubleshoot 802.11v BSS transition, enter the following command:

```
debug 11v all
```

Restrictions

Client needs to support 802.11v BSS transition.

802.11w Protected Management Frames

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Management frames such as authentication, de-authentication, association, dissociation, beacons, and probes are used by wireless clients to initiate and teardown sessions for network services. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to attack a client associated with the AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, De-authentication, and Robust Action frames.

The following management frames are considered as robust action and therefore protected:

- Spectrum Management
- QoS
- DLS
- Block Ack
- Radio Measurement
- Fast BSS Transition
- SA Query
- Protected Dual of Public Action
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following actions occur:

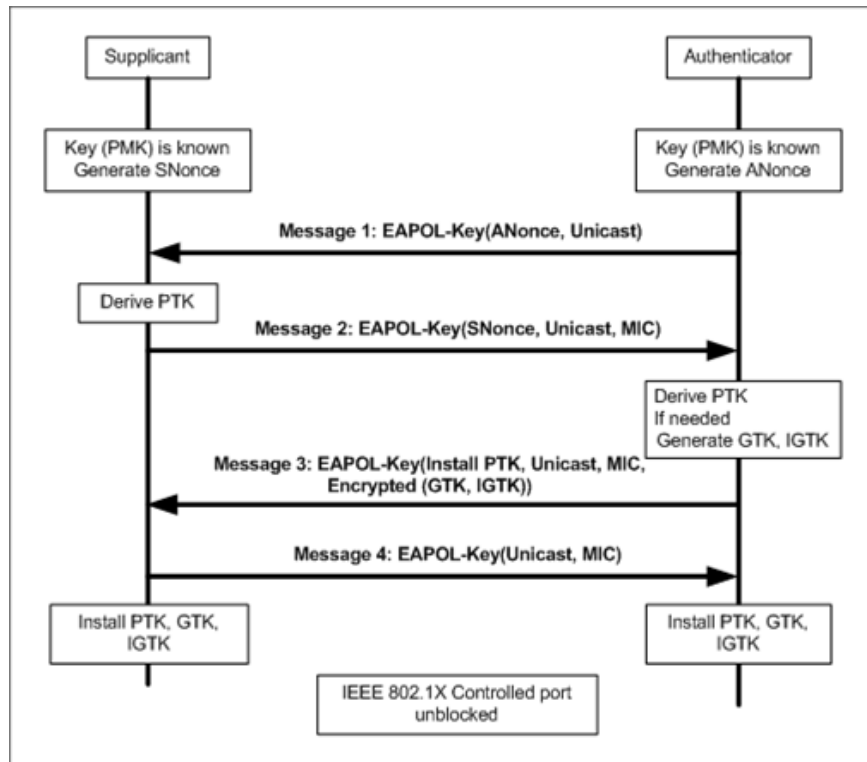
- **Client protection** is achieved by the AP, by adding cryptographic protection for de-authentication and dissociation frames thus prevents them from spoofing in a DOS attack.
- **Infrastructure protection** is achieved by adding a Security Association (SA) teardown protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

802.11w has introduced a new IGTK Key, which is used to protect broadcast/multicast robust management frames.

- **IGTK** is a random value, assigned by the authenticator STA (WLC) and transmitted to the AP. It is used to protect MAC management protocol data units (MMPDUs) from that AP.

When Management Frame Protection is negotiated, the AP encrypts the GTK and IGTK values in the EAPOL-Key frame, which is delivered in message 3 of 4-way handshake.

Figure 11-14 IGTK exchange in 4-way handshake

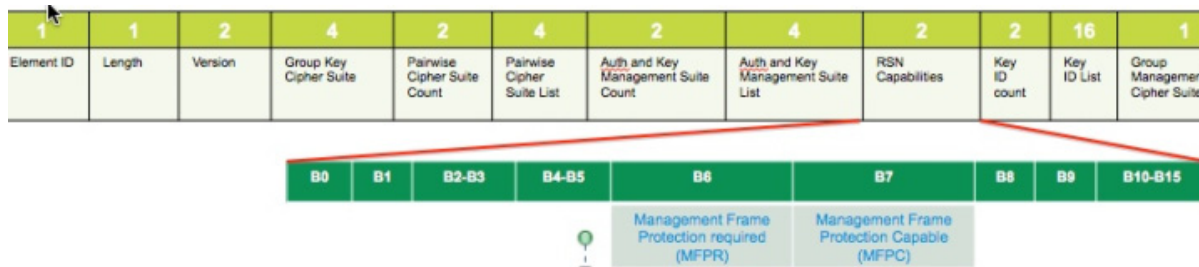


If the AP later changes the GTK, it sends the new GTK and IGTK to the client using the Group Key Handshake.

802.11w defines a new Broadcast/Multicast Integrity Protocol (BIP) that provides data integrity and replay protection for broadcast/multicast robust management frames after successful establishment of an IGTKSA. It adds a MIC that is calculated using the shared IGTK key.

802.11w Information Elements (IEs)

Figure 11-15 802.11w IEs



1. Modifications are performed in the RSN capabilities field of RSNIE.

- Bit 6: Management Frame Protection Required (MFPR)
 - Bit 7: Management Frame Protection Capable (MFPC)
2. Two new AKM Suites 5 and 6 are added for AKM Suite Selectors.
 3. New Cipher Suite with type 6 is added to accommodate BIP.

The WLC adds the modified RSNIE in association and re-association responses. The APs add the modified RSNIE in beacons and probe responses.

The following Wireshark captures shows the RSNIE capabilities and the Group Management Cipher Suite elements:

Figure 11-16 802.11w information elements

```

Auth Key Management (AKM) Suite Count: 1
+ Auth Key Management (AKM) List 00-0f-ac (Ieee8021) PSK (SHA256)
  RSN Capabilities: 0x00e8
    ....0 = RSN Pre-Auth capabilities: Transmitter does no
    ....0 = RSN No Pairwise capabilities: Transmitter can
    ....10.. = RSN PTKSA Replay Counter capabilities: 4 repla
    ....10.... = RSN GTKSA Replay Counter capabilities: 4 repla
    ....1... = Management Frame Protection Required: True
    ....1... = Management Frame Protection Capable: True
    ....0. .... = PeerKey Enabled: False
  PMKID Count: 0
  PMKID List
+ Group Management Cipher suite: 00-0f-ac (Ieee8021) BIP
  Group Management Cipher Suite OUI: 00-0f-ac (Ieee8021)
  Group Management Cipher Suite type: BIP (6)
Tag: HT Information (802.11n D1.10)
Tag: RM Enabled Capabilities (5 octets)
  
```

Security Association Teardown Protection

The Security Association (SA) teardown protection is a mechanism to prevent replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and an SA-Query procedure preventing spoofed association requests from disconnecting an already connected client.

If a client has a valid security association, and has negotiated 802.11w, the AP shall reject another Association Request with status code 30. This status code means "Association request rejected temporarily; Try again later". The AP must not tear down or modify the state of the existing association until the SA-Query procedure determines the original SA is invalid and shall include in the Association Response an Association Comeback Time information element, specifying a comeback time when the AP is ready to accept an association with this client.

The following figure shows the Association Reject message with status code 0x1e (30) and the Association comeback time set to 10 seconds.

Figure 11-17 Association reject with Comeback time

```

IEEE 802.11 wireless LAN management frame
  Fixed parameters (6 bytes)
    Capabilities Information: 0x0001
    Status code: Association request rejected temporarily; try again later (0x001e)
    ..00 0000 0000 0000 = Association ID: 0x0000
  Tagged parameters (95 bytes)
    Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: HT Capabilities (802.11n D1.10)
    Tag: HT Information (802.11n D1.10)
    Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    Tag: Timeout Interval
      Tag Number: Timeout Interval (56)
      Tag length: 5
      Timeout Interval Type: Association Comeback time (TUS) (3)
      Timeout Interval Value: 10000

```

If the AP is not already engaged in an SA query with the client, the AP shall issue an SA query until a matching SA query response is received or the Association Comeback time expires. An AP may interpret reception of a valid protected frame as an indication of a successfully completed SA query. If an SA query response with a matching transaction identifier is not received within the time period, the AP shall allow the association process to start without additional SA Query procedures.

Configuring Protected Management Frames using GUI

To configure Protected Management Frames using GUI, perform the following steps:

- Step 1** Click **WLANs**.
- Step 2** Choose **WLAN ID > Edit page**.
- Step 3** Choose **Security > Layer 2** tab.
- Step 4** Choose **WPA+WPA2** from the drop-down list.



Note The 802.11w IGTK key is derived using the 4-way handshake. The key can only be used on WLANs that are configured for WPA2 security at layer 2.

Figure 11-18 Security - Layer 2 - Protected Management Frame 1

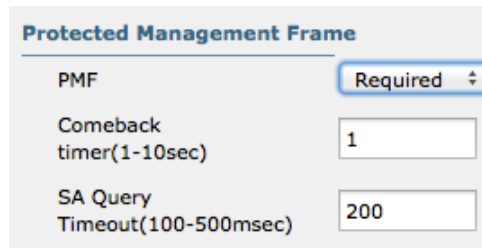
The screenshot shows the configuration page for Layer 2 Security. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'MAC Filtering' checkbox is unchecked. Under 'Fast Transition', 'Fast Transition Over the DS' is checked, and 'Reassociation Timeout' is set to 20 seconds. The 'Protected Management Frame' section shows the 'PMF' dropdown menu open, with options 'Disabled', 'Optional', and 'Required'. A red arrow points to the 'Protected Management Frame' section. Below this, 'WPA+WPA2 Parameters' are shown: 'WPA Policy' is unchecked, 'WPA2 Policy' is checked, and 'WPA2 Encryption' has 'AES' checked and 'TKIP' unchecked. The 'Authentication Key Management' section shows '802.1X' with an 'Enable' checkbox.

Step 5 In the **Protected Management Frame** area, choose the **PMF** state from the drop-down list. The following options are available:

- **Disabled**— Disables 802.11w MFP protection on a WLAN.
- **Optional**— To be used if the client supports 802.11w.
- **Required**— Ensures that the clients that do not support 802.11w cannot associate with the WLAN.

Step 6 If you choose the PMF state as either **Optional** or **Required**, perform the following:

- In the **Comeback timer** field, enter the association comeback interval in milliseconds. The comeback interval is the time within which the access point re-associates with the client after a valid security association.
- In the **SA Query Timeout** field, enter the maximum time before a Security Association (SA) query times out.

Figure 11-19 Security - Layer 2 - Protected Management Frame 2


Protected Management Frame

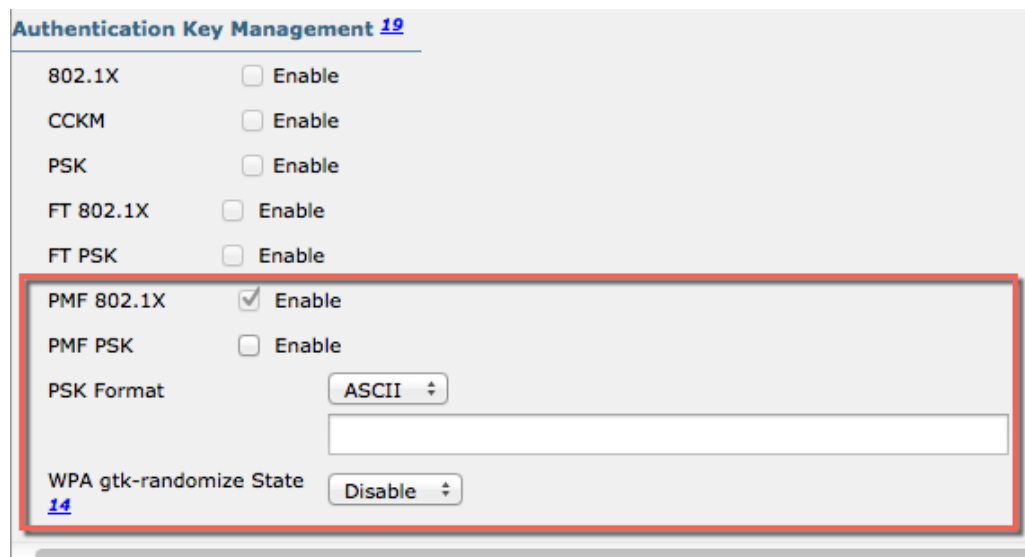
PMF	Required ▾
Comeback timer(1-10sec)	1
SA Query Timeout(100-500msec)	200

Step 7 In the **Authentication Key Management** area, perform the following:

- Check or uncheck the **PMF 802.1X** check box to configure the 802.1X authentication for the protection of management frames.
- Check or uncheck the **PMF PSK** check box to configure the pre-shared keys for PMF.
- From the PSK Format drop-down list, choose ASCII or Hexadecimal and enter the PSK value.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Figure 11-20 Authentication Key Management


Authentication Key Management [19](#)

802.1X	<input type="checkbox"/> Enable
CCKM	<input type="checkbox"/> Enable
PSK	<input type="checkbox"/> Enable
FT 802.1X	<input type="checkbox"/> Enable
FT PSK	<input type="checkbox"/> Enable
PMF 802.1X	<input checked="" type="checkbox"/> Enable
PMF PSK	<input type="checkbox"/> Enable
PSK Format	ASCII ▾ <input type="text"/>
WPA gtk-randomize State	14 Disable ▾

Configuring Protected Management Frames using CLI

To configure Protected Management Frames, enter the following commands:

Config wlan security pmf {disable optional required} wlan-id	Configure the PMF parameters with the following options: <ul style="list-style-type: none"> • Association-comeback—Configures the 802.11w association. The range is from 1 to 20 seconds. • Required— Requires clients to negotiate 802.11w MFP protection on a WLAN. • Optional— Enables 802.11w MFP protection on a WLAN. • Saquery-retry-time— Time interval identified in milliseconds in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the controller. The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.
Config wlan security pmf association-comeback <i>timeout-in-seconds wlan-id</i>	
Config wlan security pmf saquery-retrytimeout <i>timeout-in-milliseconds wlan-id</i>	

WLAN configuration contains a new Authenticated Key Management (AKM) type called Protected Management Frames (PMF).

- Configure the 802.1X authentication for PMF, using the following command:

```
config wlan security wpa akm pmf 802.1x {enable | disable} wlan-id
```

- Configure the pre-shared key support for PMF, using the command:

```
config wlan security wpa akm pmf psk {enable | disable} wlan-id
```

- Configure a pre-shared key for a WLAN, using the following command:

```
config wlan security wpa akm psk set-key {ascii | hex} psk wlan-id
```



Note

802.11w cannot be enabled on WLANs of None, WEP-40, WEP-104, and WPA (AES or TKIP) encryption.

Monitoring 802.11w

To display the WLAN and PMF parameters on the WLAN, enter the following command:

```
show wlan wlan-id
```

Troubleshooting Support

To configure the debugging of PMF, enter the following command:

```
debug pmf events {enable | disable}
```