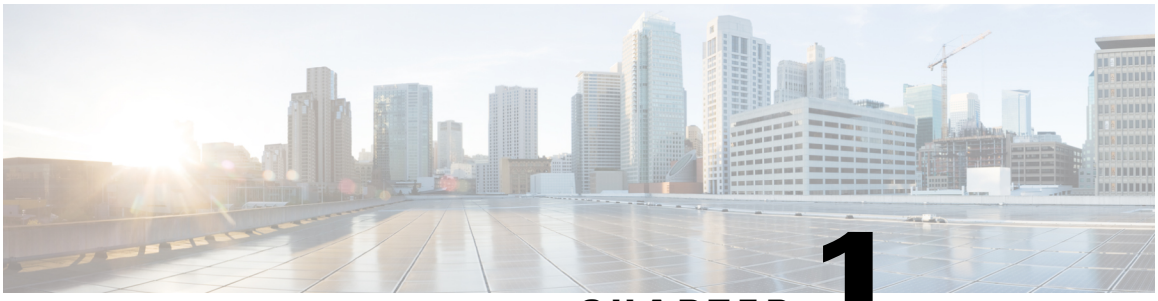
802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE Release 3.3

Last Modified: January 25, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Introduction

This guide introduces IOS XE release 3.3 deployment guide for the Cisco Converged Access CT5760 and Cat3850 products. This guide is designed to help you deploy and monitor new features introduced in the 3.3 release. The features described in this document are only fully supported in 11n capable Gen2 indoor Access Points. The beacon and probe changes are only supported in the indoor 11n capable AP radios.

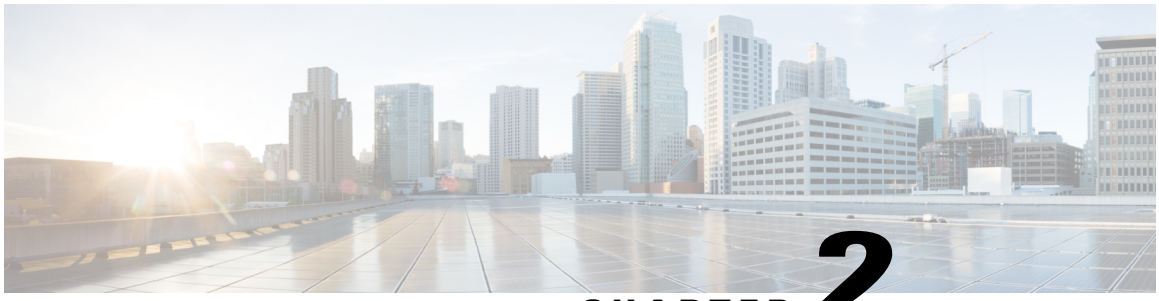
The document builds on previous releases with the assumption that users are familiar with the Converged Access products. Please refer to CT5760 Controller Deployment Guide and Cisco Catalyst 3850 Switch Deployment Guide for released features not covered in this guide.

CT5760 Controller

CT5760 is an innovative UADP ASIC based wireless controller deployed as a centralized controller in the next generation unified wireless architecture. CT5760 controllers are specifically designed to function as the Unified model central wireless controllers. They also support the newer Mobility functionality with Converged Access switches in the wireless architecture.

Figure 1: Cisco WLC 5760

CT5760 is an extensible and high performing wireless controller, which can scale up to 1000 access points and 12000 clients. The controller has 6 to 10 Gbps data ports. As a component of the Cisco Unified Wireless Network, the CT5760 series works in conjunction with Cisco Aironet access points, the Cisco Prime infrastructure, and the Cisco Mobility Services Engine to support business-critical wireless data, voice, and video applications.



CHAPTER 2

802.11r Fast Transition Roaming

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 re-association request or response exchange with the 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. 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 such as voice and video and is the key requirement for voice over Wi-Fi.

This chapter includes the following topics:

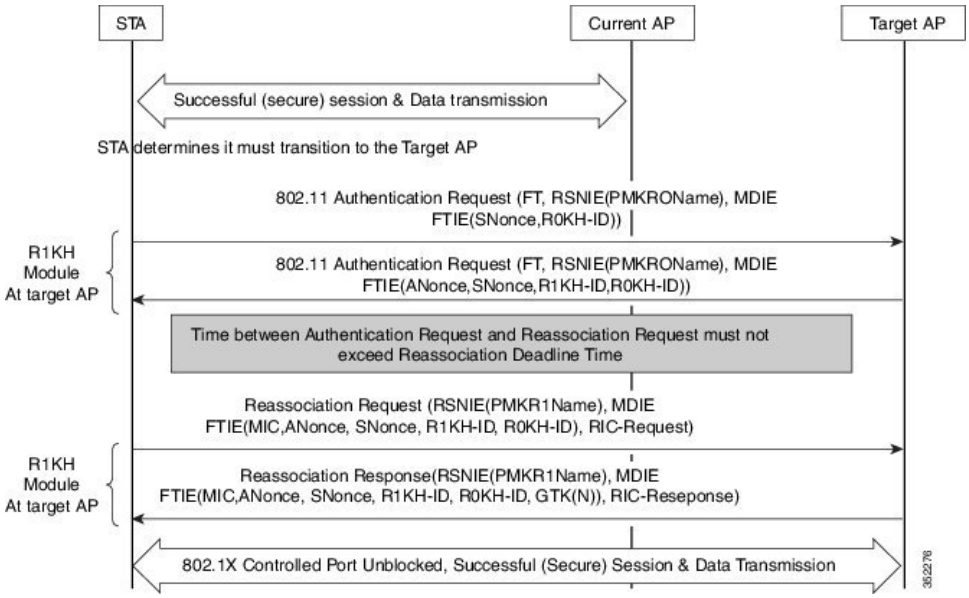
How a Client Roams

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

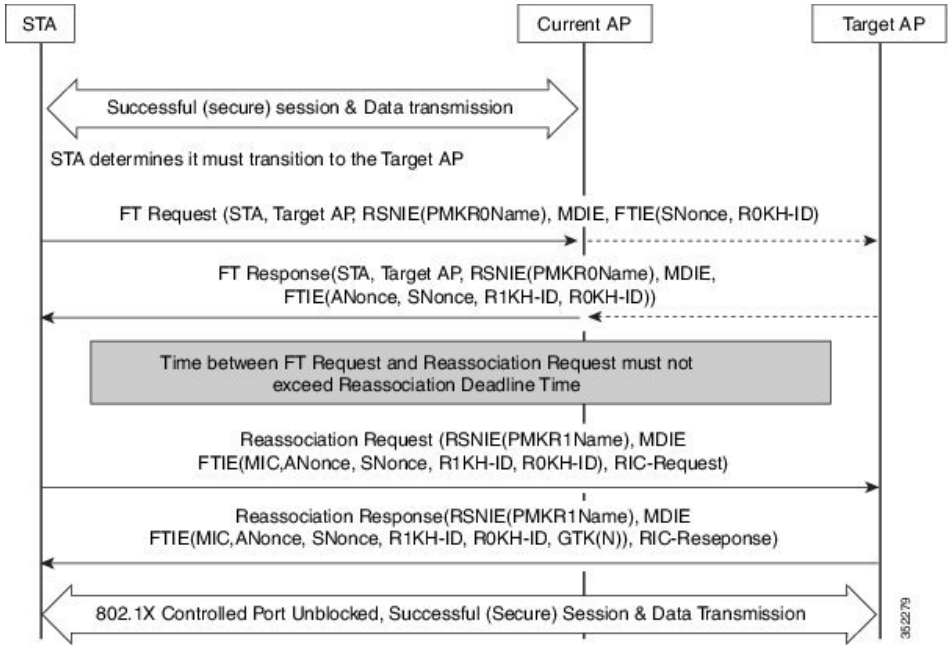
- Over-the-Air: The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.

Figure 2: Fast BSS Transition Over-the-Air in RSN



- 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.

Figure 3: Fast BSS Transition Over the DS in RSN

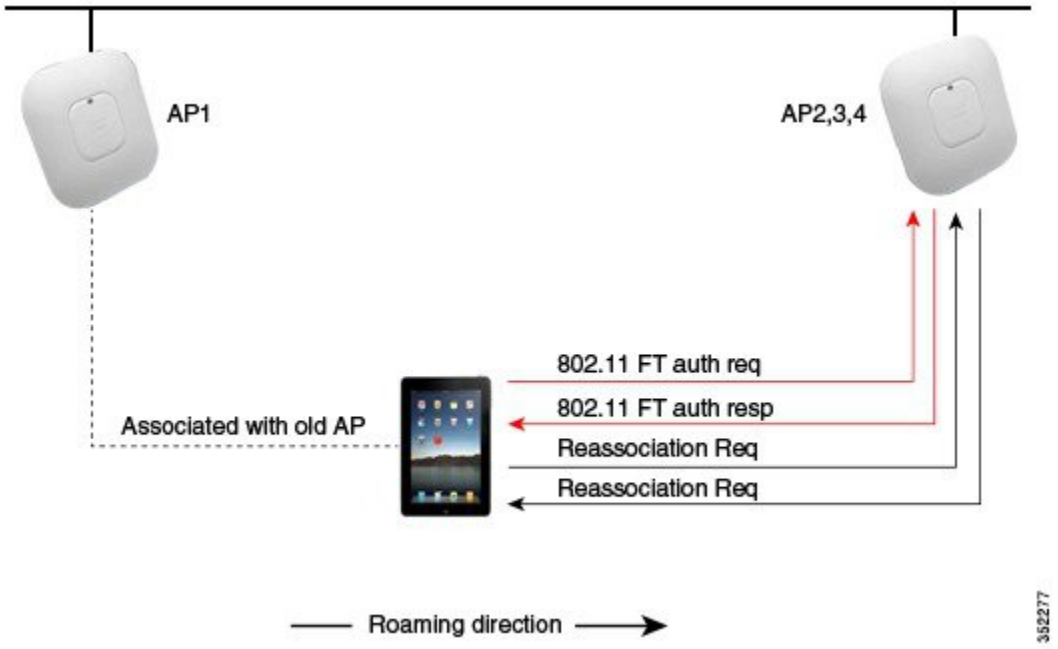


Over the Air Intra Controller Roam

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

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.

Figure 4: Over the Air Intra Controller Roam



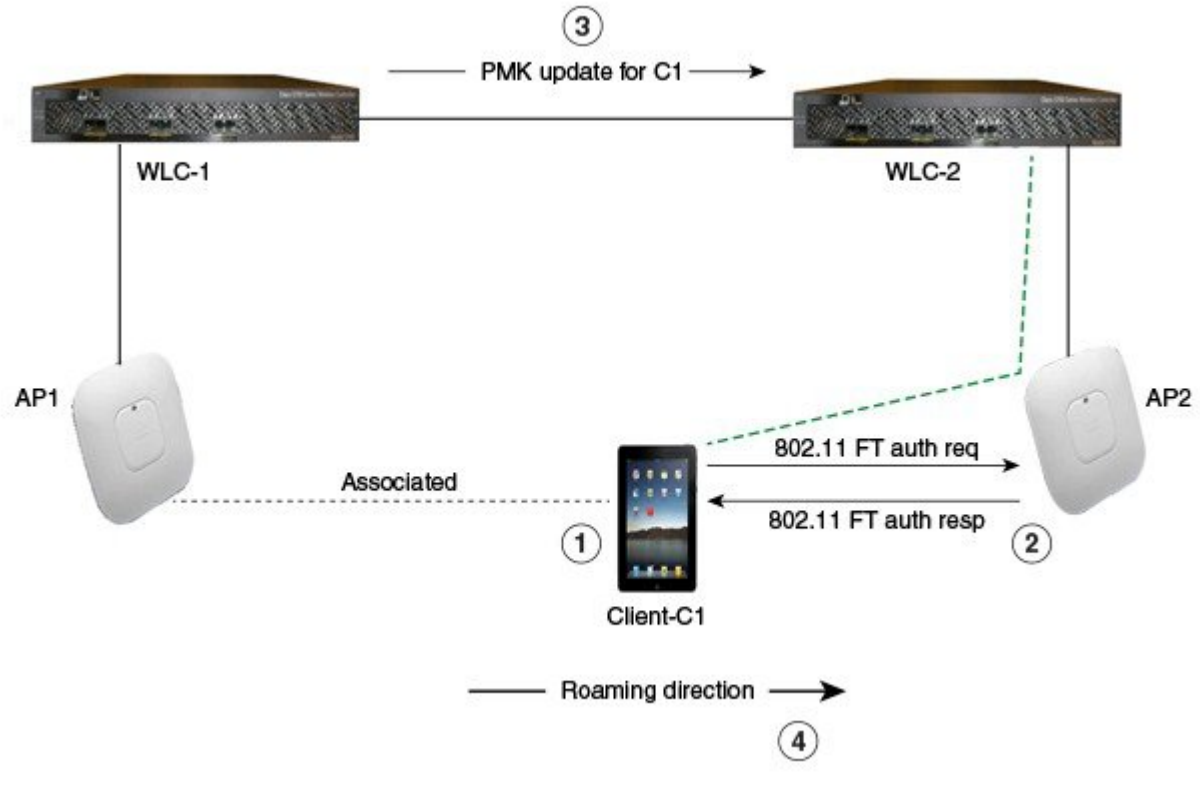
Over the Air Inter Controller Roam

The following steps describe the message exchange in the case where a client is roaming between APs, AP1, and AP2, connected to different controllers, WLC1 and WLC2 respectively, within a mobility group:

1. Client is associated with AP1 and wants to roam to AP2.
2. Client sends FT Authentication Request to AP2 and receives FT Authentication Response from AP2.
3. Pairwise Master Key (PMK) is sent from WLC-1 to WLC-2. WLC-1 sends a mobility message to WLC-2 about the roaming client using the mobility infrastructure.

4 Client completes its roam from AP1 to AP2.

Figure 5: Over the Air Inter Controller Roam



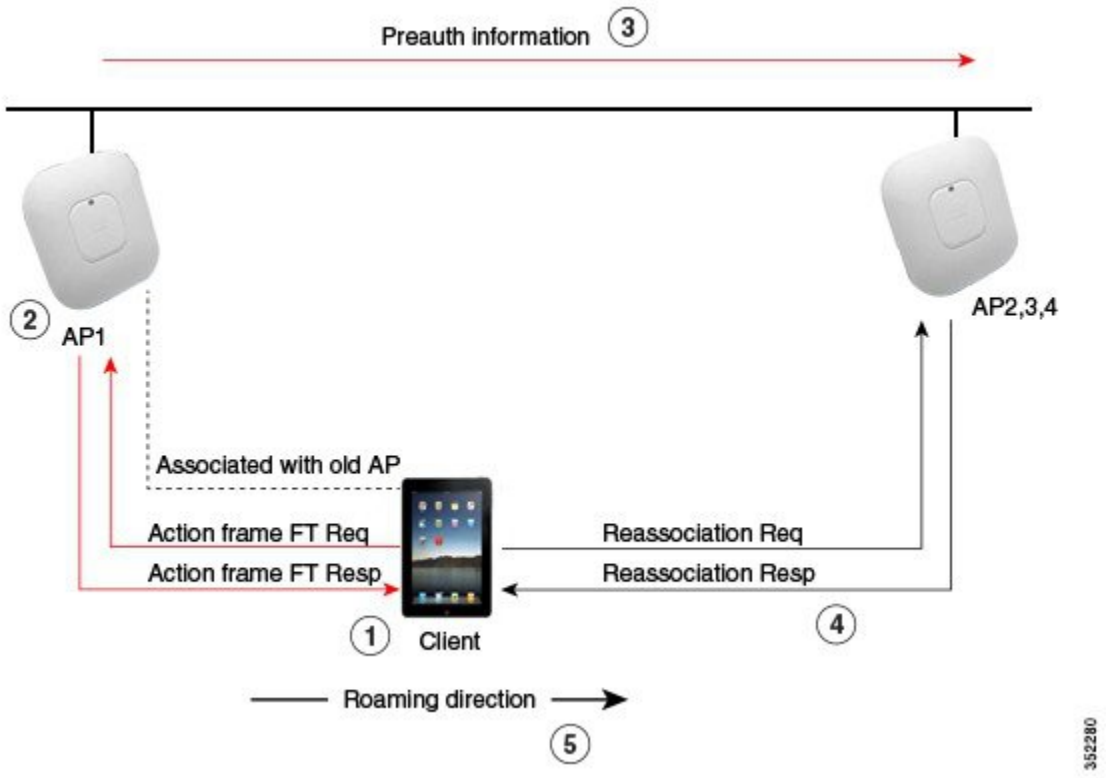
Over-the-DS Intra Controller Roam

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

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 controller, hence the pre-Authentication information 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.

Figure 6: Over the DS Intra Controller Roam



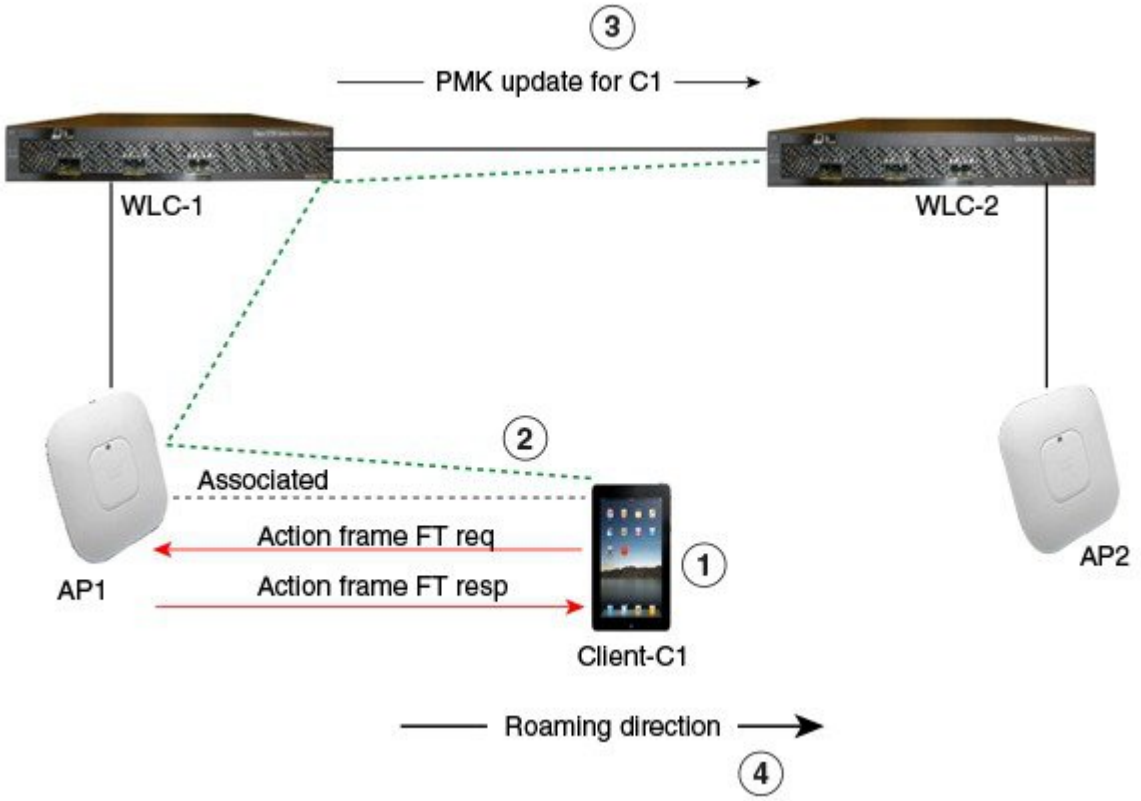
Over-the-DS Inter Controller Roam

The following steps describe the message exchange in the case where a client is roaming between APs, AP1, and AP2, connected to different controllers, WLC1 and WLC2 respectively, within a mobility group:

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 PMK is sent from WLC-1 to WLC-2 . Controller WLC-1 sends a mobility message to WLC-2 about the roaming client.

4 Client completes its roam from AP1 to AP2.

Figure 7: Over the DS Inter Controller Roam



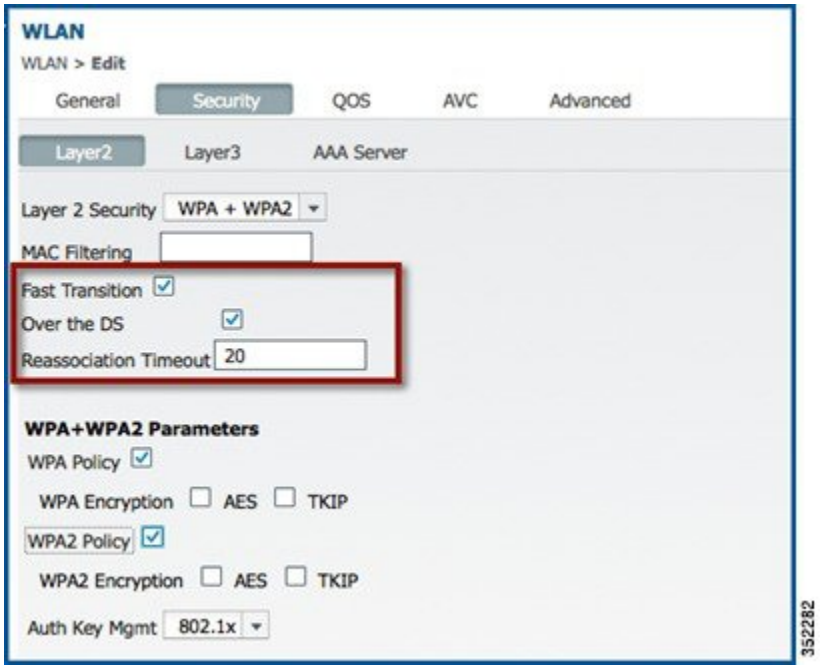
Web UI Configuration for Fast Transition Roaming

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

1 Choose **WLAN > Security > Layer2**. Make sure that **Layer 2 Security** is WPA+WPA2 or Open.
2 Check the **Fast Transition** checkbox. This will enable Over the Air FT for the WLAN.
3 To enable Over the DS FT, check the **Over the DS** checkbox.

4 **Reassociation Timeout** can be configured between 1-100 seconds, the default being 20 seconds. The time between FT Authentication Request and Re-association Request must not exceed the Re-association Timeout.

Figure 8: 802.11r Web UI Configuration



CLI Configuration for Fast Transition Roaming

The following command is available under the WLAN configuration to configure Fast Transition Roaming:

`security ft [ over-the-ds | reassociation-timeout timeout-in-seconds]`
Example:
`Controller(config-wlan)# security ft reassociation-timeout 23`
	• over-the-ds: Enables 802.11r fast transition parameters over a distributed system.
	• reassociation-timeout: Enables 802.11r fast transition reassociation timeout. The range is 1 to 100 seconds.

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

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

Monitoring 802.11r

`show wlan name wlan-name`	Displays the WLAN parameters on the WLAN. The FT parameters are displayed.
	Example:
	`FT Support :Enabled`
	`FT Reassociation Timeout :10`
	`FT Over-The-DS mode :Enabled`

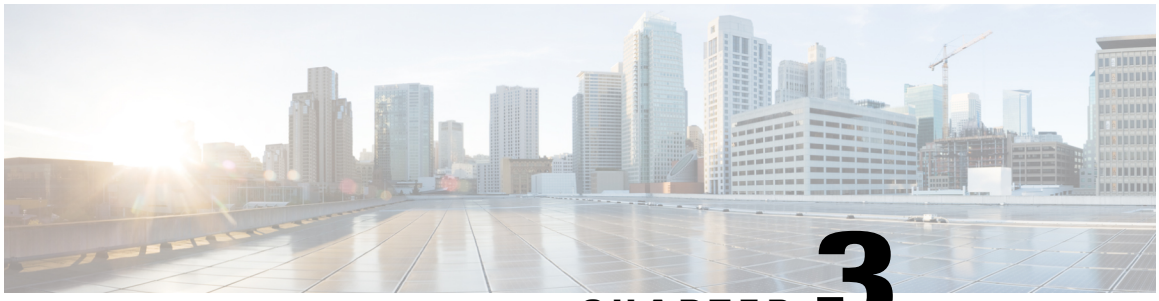
Troubleshooting Support

```
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.
- Non 802.11r client cannot associate to WLAN which has 802.11r enabled.
- This feature will not be supported with LEAP because 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.
- FT Resource request protocol will not be supported in this release because clients also do not have this support.
- Each controller will allow a maximum of 3 FT handshakes with different APs under its control.



CHAPTER 3

802.11k Assisted Roaming

The main goal of introducing this feature in IOS XE 3.3 release is to deliver an intelligent and optimized **Neighbor List Element** to 802.11k supported (Apple) clients to optimize their channel scanning, roaming, and battery usage. 802.11k allows 11k capable clients to request for 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 a request for a list of neighbor APs. The request is in the form of an 802.11 management frame known as an action packet. The AP responds with a list of neighbor APs on the same WLAN with their Wi-Fi channel numbers. The AP response is also an action packet. From the response frame, the client knows which APs are candidates for the next roam. The use of 802.11k radio resource management (RRM) processes allows the client to roam efficiently and quickly.

With the neighbor list information, the 11k capable client does not need to probe all of the 2.4 GHz and 5 GHz channels to find an AP it can roam to. Not having to probe all of the channels reduces channel utilization on all channels, thereby increasing bandwidth on all channels. It also reduces roam time and improves the decisions made by the client. Additionally, it increases battery life of the device because it is neither changing the radio configuration for each channel nor sending probe requests on each channel. It avoids the device having to process all of the probe response frames.

This chapter includes the following topics:

Assisted Roaming with 802.11k

The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points 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 switch. The 802.11k neighbor list is based on the location of the clients without requiring the mobility services engine

(MSE). Two clients on the same switch 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 associating with the APs that advertise the RRM 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 switch receives a request for an 802.11k neighbor list, the following occurs:

1. The switch searches the RRM neighbor table for a list of neighbors on the same band as the AP with which the client is currently associated.
2. The switch checks the neighbors according to the RSSI (Received Signal Strength Indication) 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 switch 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)

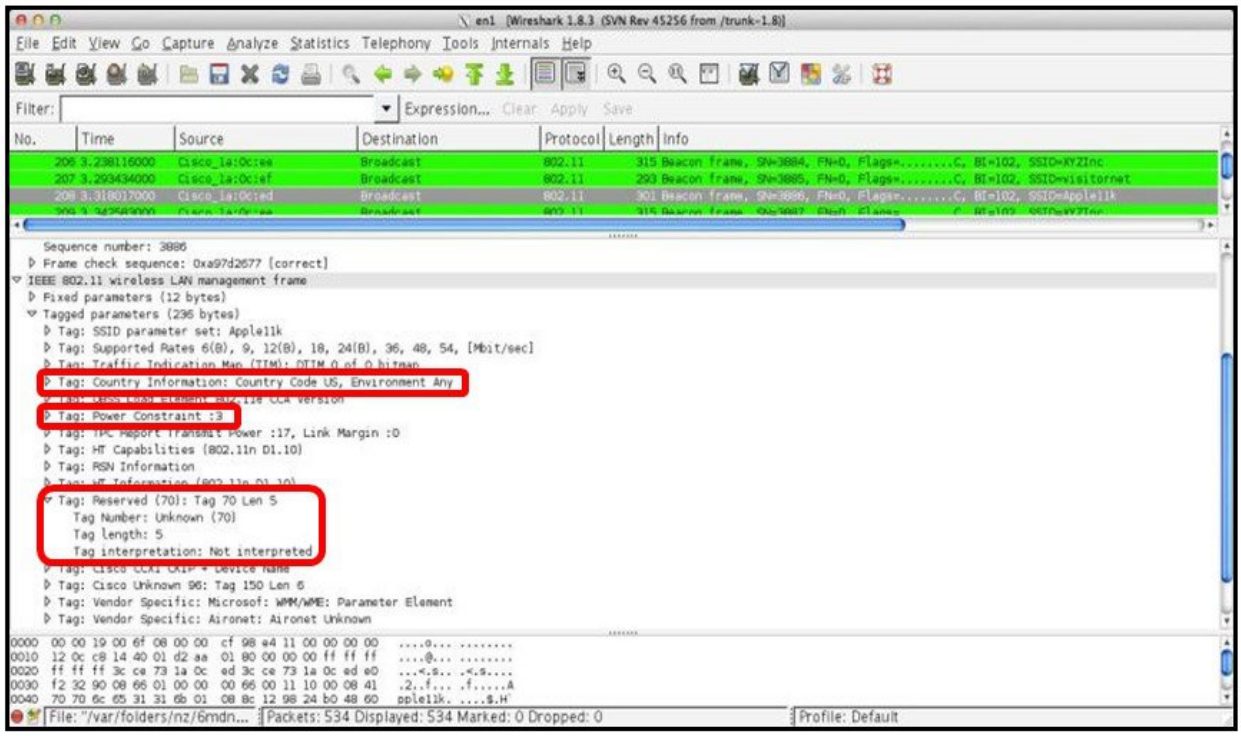
Clients send requests for neighbor lists only after associating with the APs that advertise the RRM capability information element (IE) in the beacon.

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
- RRM enabled Capabilities Element: The RRM Capabilities element is 5 octets long and when included in a beacon or probe response uses bit 1 to signal 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, a neighbor list is sent based on the request from the client and not on the neighbor list capability of the client in the IE. The following Wireshark capture points out these information elements.

Figure 9: 802.11k Information Elements



CLI Configuration for Assisted Roaming

`wireless assisted-roaming floor-bias` *dBm* Example: `Controller(config)# wireless assisted-roaming floor-bias 20`	Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.

`assisted-roaming neighbor-list`
Example:
`Controller(wlan)# assisted-roaming neighbor-list`
	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.

`assisted-roaming dual-list`
Example:
`Controller(wlan)# assisted-roaming dual-list`
	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.

Note The WLC does not have a GUI configuration for 802.11k. 802.11k assisted roaming is enabled by default.

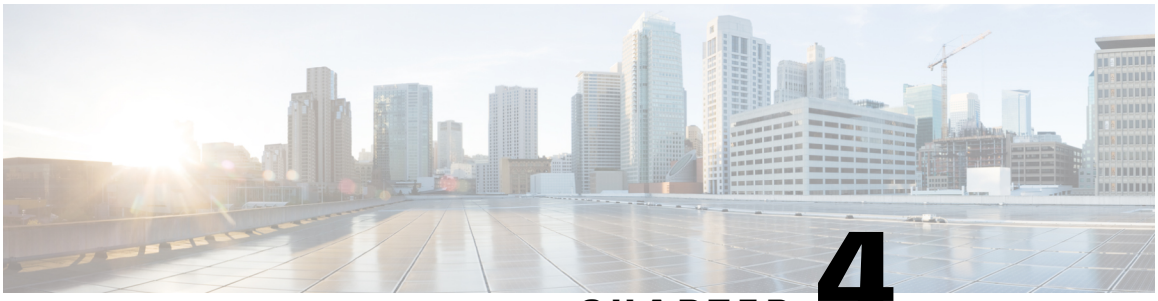
Configuration Example

This example shows how to configure Neighbor floor label bias:

```
Controller# configure terminal
Controller(config)# wireless assisted-roaming floor-bias 10
```

This example shows how to enable 802.11k on a specific WLAN:

```
Controller(config)# wlan test
Controller(config (wlan)# assisted-roaming neighbor-list
```



CHAPTER 4

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

It is also possible to optimize roaming for non-802.11k clients. You can generate a prediction neighbor list for each client without the client requiring to send an 802.11k neighbor list request. When this is enabled on a WLAN, after each successful client association/re-association, the same neighbor list optimization is applied on the non-802.11k client to generate the neighbor list and store the 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 different neighbors. Because clients usually probe before any association or re-association, this list is constructed with the most updated probe data and predicts the next AP that the client is likely to roam to.

We discourage 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.

Similar to aggressive load balancing, there is a switch to turn on the assisted roaming feature both on a per-WLAN basis and globally. The following options are available:

- 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 be activated.

CLI Configuration for Prediction Based Roaming

`assisted-roaming prediction`
Example:
`Controller(wlan)# assisted-roaming prediction`
	Configures assisted roaming prediction list feature 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.

`wireless assisted-roaming prediction-minimum` *`count`* Example: `Controller# wireless assisted-roaming prediction-minimum`	Configures the minimum number of predicted APs required for the prediction list feature to be activated. The default value is 3. **Note** If the number of the APs in the prediction assigned to the client is less than the number that you specify, the assisted roaming feature will not apply on this roam.
`wireless assisted-roaming denial-maximum` *`count`* Example: `Controller# wireless assisted-roaming denial-maximum 8`	Configures the maximum number of times a client can be denied association if the association request is sent to an AP that does not match any AP on the prediction. The valid range is from 1 to 10, and the default value is 5.
`wireless assisted-roaming prediction-minimum` *`count`* Example: `Controller# wireless assisted-roaming prediction-minimum`	Configures the minimum number of predicted APs required for the prediction list feature to be activated. The default value is 3. **Note** If the number of the APs in the prediction assigned to the client is less than the number that you specify, the assisted roaming feature will not apply on this roam.

Configuration Example

This example shows how to configure the prediction list on a specific WLAN:

```
Controller# configure terminal
Controller(config)# wlan test
Controller(config)(wlan)# assisted-roaming prediction
```

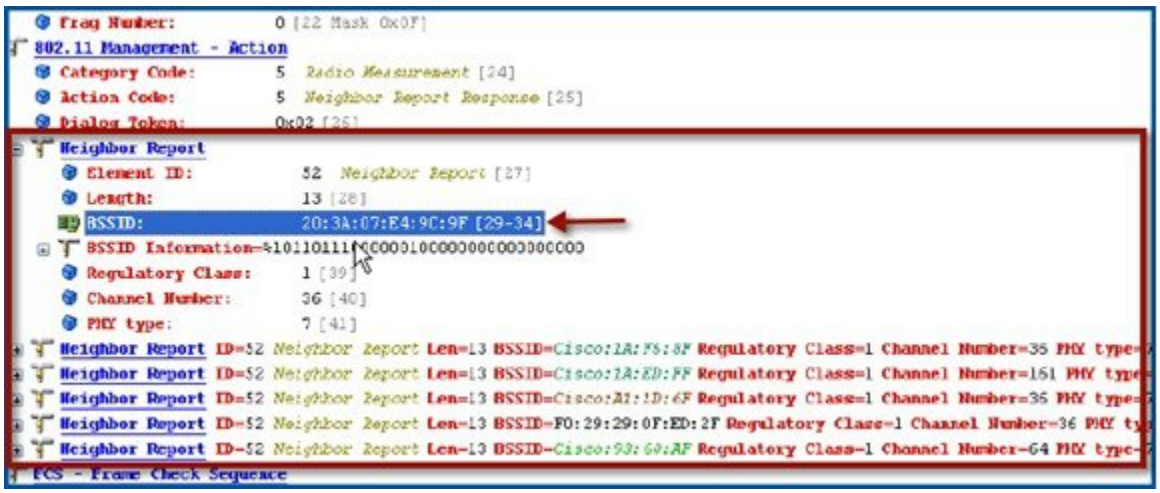
This example shows how to configure the prediction list based on assisted roaming prediction threshold and maximum denial count on a specific WLAN:

```
Controller(config)# wireless assisted-roaming prediction-minimum 3
Controller(config)# wireless assisted-roaming denial-maximum 3
```

Neighbor List Response

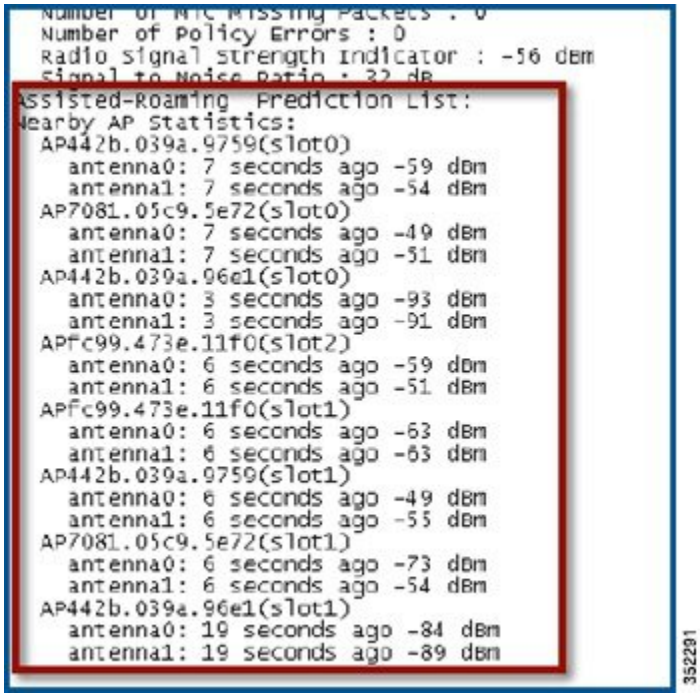
The neighbor list includes information about BSSID, channel and operation details of the neighboring radios as shown in the Wireshark capture below:

Figure 10: 802.11k Neighbor Report



The 802.11k Neighbor list per client can be seen by running the command
`show wireless client mac-address <> detail`

Figure 11: Nearby AP Statistics CLI Output



Limitations

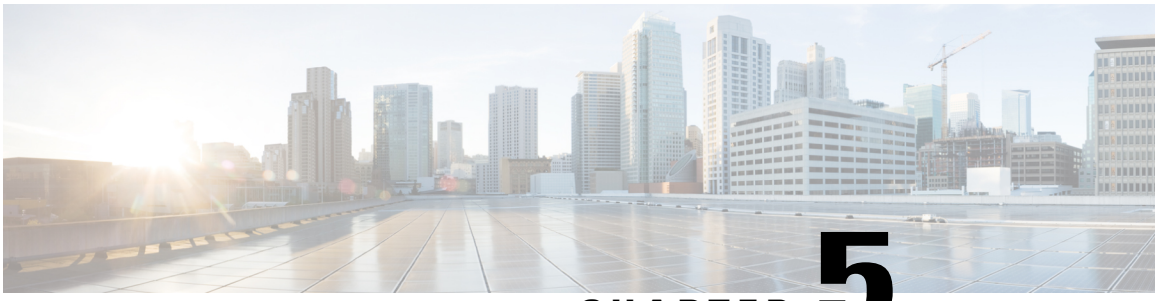
- In this release the following features are not supported:
  - TSF Offset
  - TPC request/response
  - Beacon request/response
  - Quiet element with hardware beacon
  - 11v Location Tracking
- No GUI configuration support
- Since both load balancing and prediction based roaming are designed to influence the AP that a client associates with, it is not possible to enable both the options at the same time on a WLAN.

Troubleshooting Support

The following debug and trace commands can be used to troubleshoot this feature:

```
Controller# debug dot11 dot11k ?
  all           all
  detail        802.11k detail
  errors        802.11k errors
  events        802.11k events
  optimization  802.11k optimization
  simulation    802.11k simulation

Controller# set trace dot11 dot11k ?
  detail        Dot11k Detailed debugging
  errors        Dot11k Errors debugging
  events        Dot11k Events debugging
  filter        Trace Adapted Flag Filter
  history       Dot11k History debugging
  level         Trace Level
  optimization  Dot11k Optimization debugging
  simulation    Dot11k Simulation debugging
```



CHAPTER 5

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 tear down 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.

Management frames that are considered as robust action and therefore protected are the following:

- 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 occur:

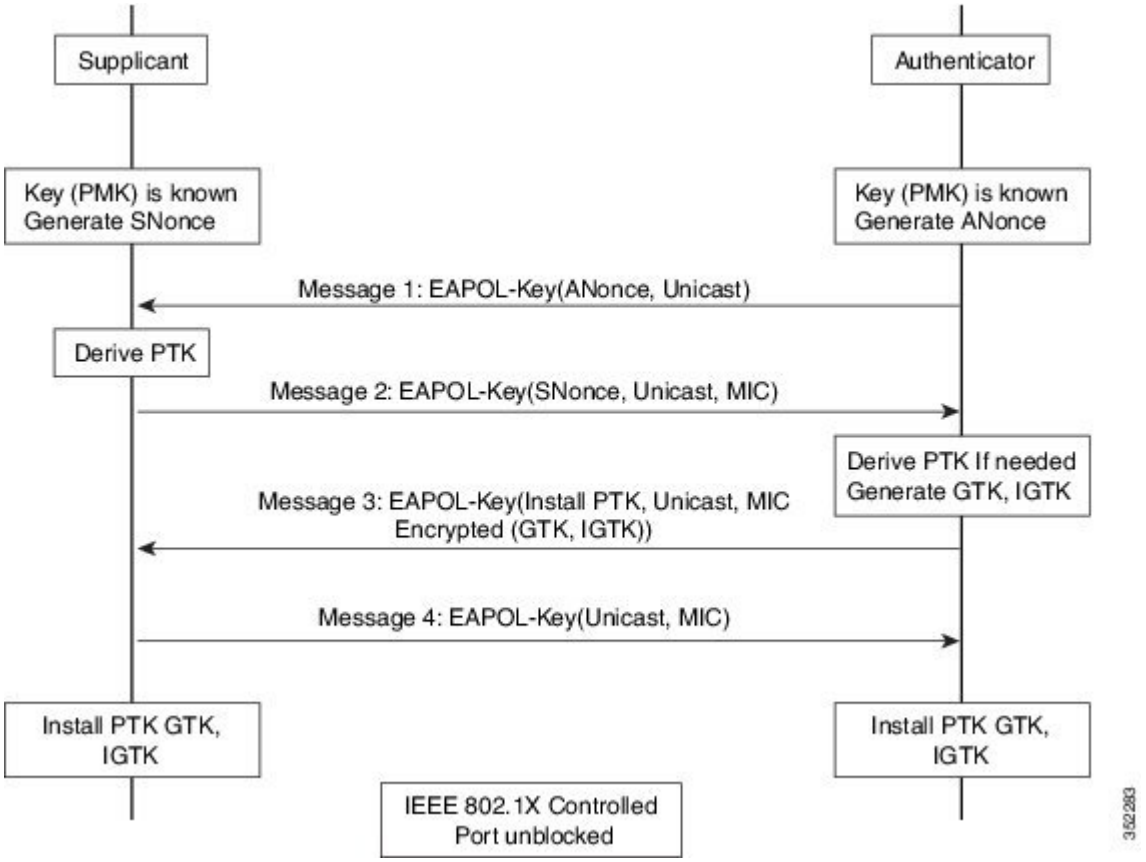
- Client protection is added by the AP adding cryptographic protection to de-authentication and dissociation frames preventing them from being spoofed in a DOS attack.
- Infrastructure protection is added by adding a Security Association (SA) tear down protection mechanism consisting of an Association 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 used to protect MAC management protocol data units (MMPDUs) from that source STA.

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 12: IGTK Exchange in 4-way Handshake

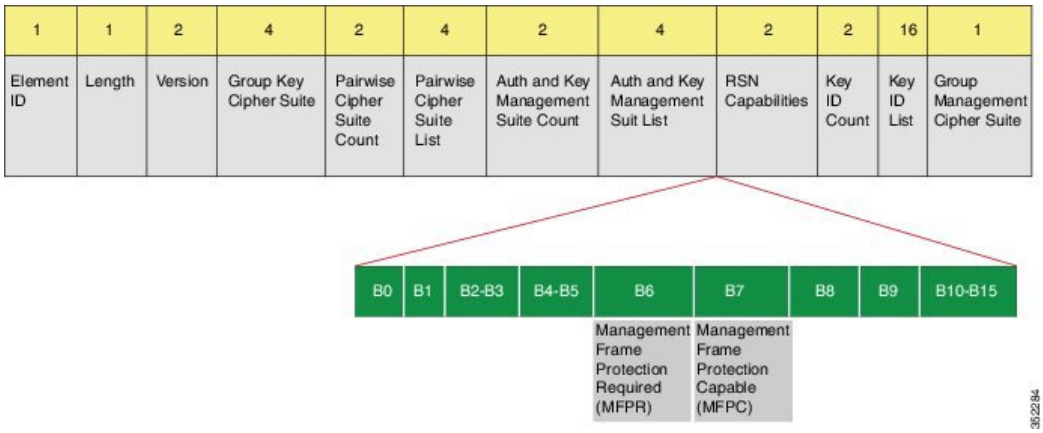


- If the AP later changes the GTK, it sends the new GTK and IGTK to the client using the Group Key Handshake .

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 13: 802.11w Information Elements

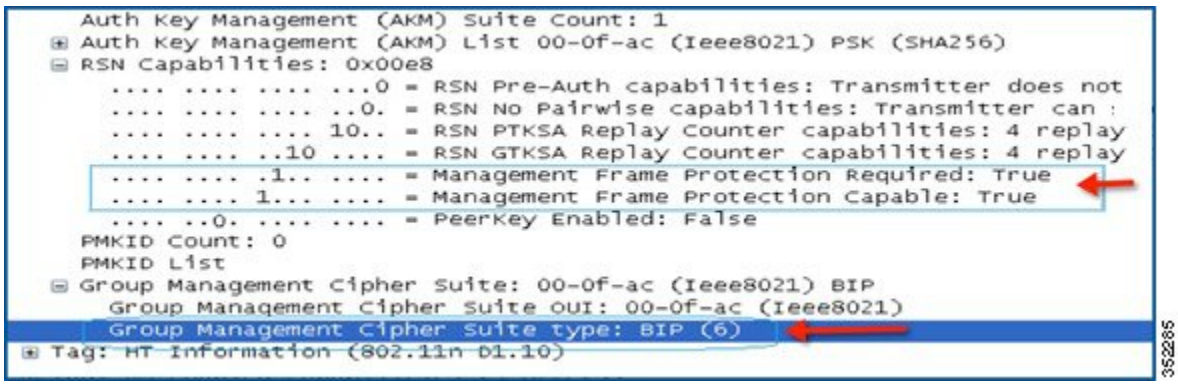


1 Modifications made in the RSN capabilities field of RSNIE.
   a Bit 6: Management Frame Protection Required (MFPR)
   b Bit 7: Management Frame Protection Capable (MFPC)
2 Two new AKM Suites, 5 and 6 are added for AKM Suite Selectors.
3 New Cipher Suite with type 6 is added to accommodate BIP.

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

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

Figure 14: 802.11w Information Elements



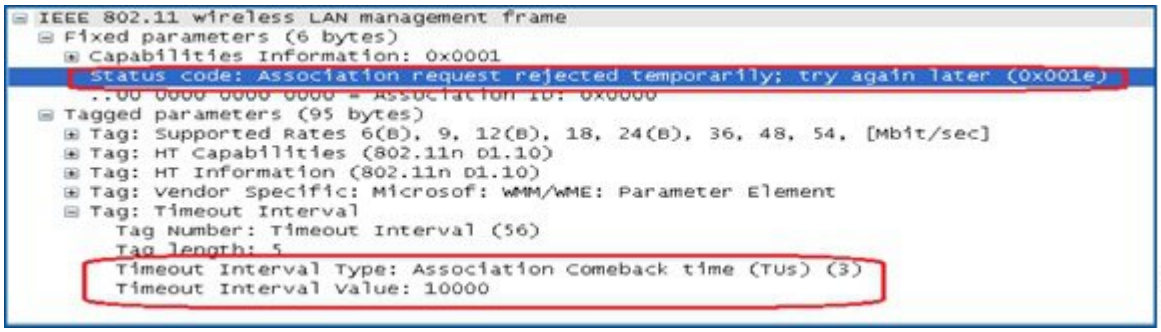
Security Association (SA) Teardown Protection

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 stands for "Association request rejected temporarily; Try again later". The AP should not tear down or otherwise modify the state of the existing association until the SA-Query procedure determines that 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 would be ready to accept an association with this client.

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

Figure 15: Association Reject with Comeback Time



Following this, 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 a SA QUERY response with a matching transaction identifier within the time period, the AP shall allow the association process to be started without starting additional SA Query procedures.

CLI Configuration for Protected Management Frames

`security pmf [ association-comeback` *`association-comeback-time-in-seconds`* `| mandatory | optional | saquery` *`saquery-time-interval-milliseconds`* `]`
 	
Example:
`Controller(config-wlan)#security pmf saquery-retry-time 200`
	Configures the PMF parameters with the following options:
	• association-comeback—Configures the 802.11w association. The range is from 1 through 20 seconds.
	• mandatory—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 is milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.

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

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

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

Note The WLC does not have a GUI configuration for 802.11w.

Monitoring 802.11w

`show wlan name wlan-name`	Displays the WLAN parameters on the WLAN. The PMF parameters are displayed. Here is an example:
	`PMF Support :Disabled`
	`PMF Association Comeback Timeout : 1`
	`PMF SA Query Time : 200`

Configuration Example

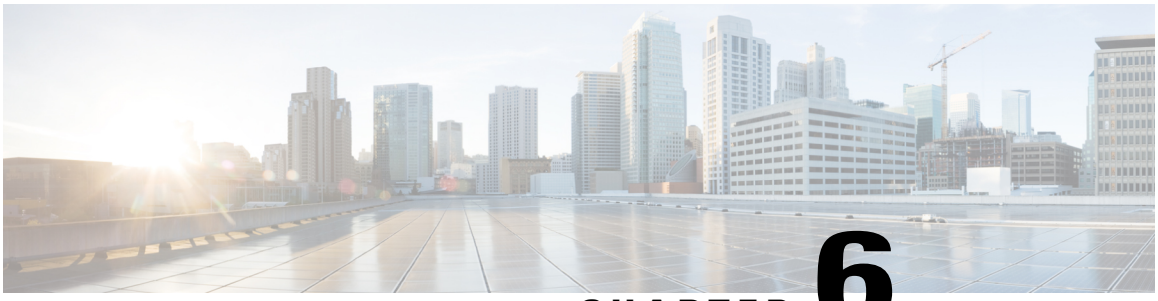
```
wlan 11w-psk 6 11w-psk
 client vlan 49
 security wpa akm psk set-key ascii 0 ciscocisco
 security wpa akm pmf psk
 security pmf association-comeback 10
 security pmf mandatory
 security pmf saquery-retry-time 100
 no shutdown
```

Troubleshooting Support

The following debug and Trace commands can be used to troubleshooting this feature:

```
Controller#debug pmf ?
  all     debug Protected Management Frame all
  events  Protected Management Frame events
  keys    Protected Management Frame keys

Controller#set trace pmf ?
  events  PMF events debugging
  filter  Trace Adapted Flag Filter
  keys    PMF keys debugging
  level   Trace Level
```



CHAPTER 6

References

- 802.11r support is included as part of Voice-Enterprise certification, 802.11k support is included as part of WMM Voice-Enterprise and WMM-AC certification and 802.11w support in included as part of the Protected Management Frame certification: http://www.wi-fi.org/certified-products-advanced-search
- 802.11r and 802.11k support on Apple devices running iOS 6.0 and higher: http://support.apple.com/kb/HT5535
- Enterprise Best Practices for Apple Mobile Devices on Cisco Wireless LANs: http://www.cisco.com/en/US/docs/wireless/technology/vowlan/bestpractices/EntBP-AppMobDevs-on-Wlans.pdf