802.11k/v/r – Multi-Band Operation

2021/12/27

Nishank

Version History

Version	Date	Author (Optional)	Description
0.1	2021-8-23	Nishank	Initial draft
1.0	2021-12-27	Micheal Su	Official release

Outline

- 802.11v Introduction
- 802.11k Introduction
- 802.11k Functional test setup
- 802.11r Introduction
- 802.11r Introduction to SPEC
- 802.11r Mediatek implementation
- 802.11r Functional test setup
- 802.11r Test Without EasyMesh
- 802.11r Frame format

802.11v Introduction

Motivation of 802.11v

- Wireless Network Management(WNM) enables STAs to exchange information for the purpose of improving the overall performance of the wireless network
- STAs use WNM protocols to exchange operational data so that each STA is aware of the network conditions, allowing STAs to be more cognizant of the topology and state of the network
- WNM protocols provide a means for STAs to be aware of the presence of collocated interference, and enable STAs to manage RF parameters based on network conditions

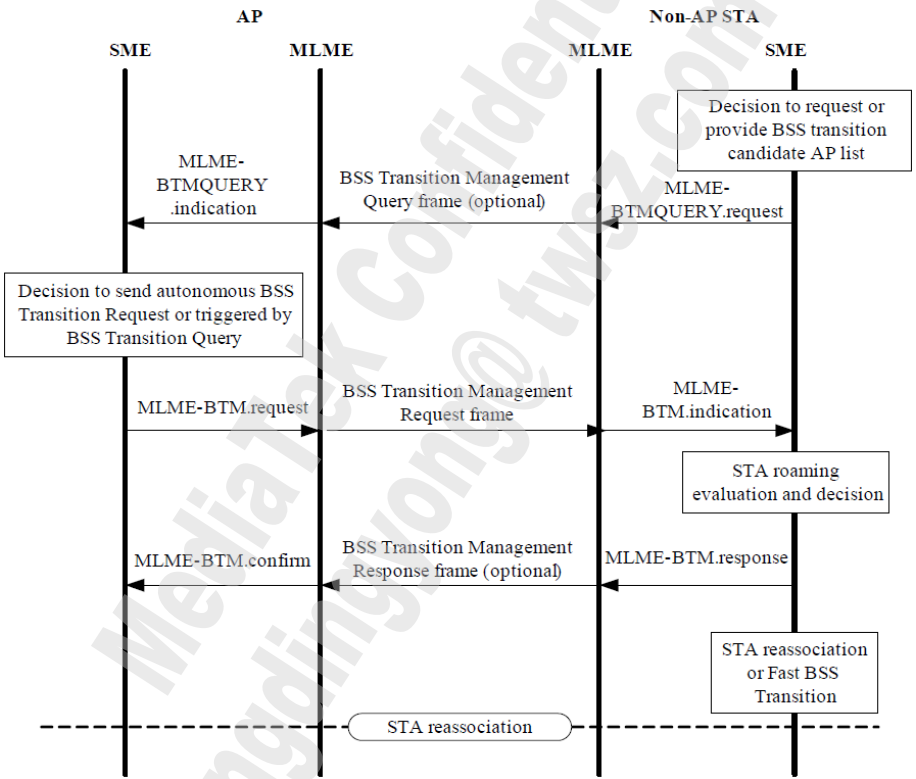
Overview

- The WNM service includes:
  - BSS Max idle period management
  - BSS transition management(BTM)
  - Channel usage
  - Collocated interference reporting, Diagnostic reporting, Event reporting, Multicast diagnostic reporting
  - DMS (Directed Multicast Service)
  - FMS (Flexible Multicast Service)
  - Location services
  - Multiple BSSID capability
  - Proxy ARP
  - QoS traffic capability
  - SSID list
  - Triggered TA statistics
  - TIM broadcast
  - Timing measurement
  - Traffic filtering service
  - WNM-Sleep mode

BSS Transition Management

- BSS transition management enables an AP to request non-AP STAs to transition to a specific AP, or to indicate to a non-AP STA a set of preferred APs, due to network load balancing or BSS Termination
- BSS Transition Management Query
  - uses the action frame body format
  - is transmitted by a STA requesting or providing information on BSS transition candidate AP
- BSS Transition Management Request
  - uses the action frame body format
  - is transmitted by an AP in response to a BSS Transition Management Query frame, or autonomously
- BSS Transition Management Response
  - uses the action frame body format
  - is optionally transmitted by a STA in response to a BSS Transition Management Request frame

BSS Transition Management Procedures



Beacon with BTM Support Sent from APUT

```
⊞ Frame 1: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits)
⊞ 802.11 radio information
⊞ IEEE 802.11 Beacon frame, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (195 bytes)
    ⊞ Tag: SSID parameter set: Rorscha-2G
    ⊞ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    ⊞ Tag: DS Parameter set: Current Channel: 11
    ⊞ Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
    ⊞ Tag: AP Channel Report: Operating Class 32, Channel List : 1, 2, 3, 4, 5, 6, 7,
    ⊞ Tag: AP Channel Report: Operating Class 33, Channel List : 5, 6, 7, 8, 9, 10, 11,
    ⊞ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ⊞ Tag: RSN Information
    ⊞ Tag: ERP Information
    ⊞ Tag: HT Capabilities (802.11n D1.10)
    ⊞ Tag: HT Information (802.11n D1.10)
    ⊟ Tag: Extended Capabilities (8 octets)
        Tag Number: Extended Capabilities (127)
        Tag length: 8
      ⊞ Extended Capabilities: 0x01 (octet 1)
      ⊞ Extended Capabilities: 0x00 (octet 2)
      ⊟ Extended Capabilities: 0x08 (octet 3)
          .... ...0 = TFS: Not supported
          .... ..0. = WNM-Sleep Mode: Not supported
          .... .0.. = TIM Broadcast: Not supported
          .... 1... = BSS Transition: Supported
          ...0 .... = QoS Traffic Capability: Not supported
          ..0. .... = AC Station Count: Not supported
          .0.. .... = Multiple BSSID: Not supported
          0... .... = Timing Measurement: Not supported
      ⊞ Extended Capabilities: 0x00 (octet 4)
      ⊞ Extended Capabilities: 0x00 (octet 5)
      ⊞ Extended Capabilities: 0x00 (octet 6)
      ⊞ Extended Capabilities: 0x00 (octet 7)
      ⊞ Extended Capabilities: 0x00 (octet 8)
    ⊞ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ⊞ Tag: QBSS Load Element 802.11e CCA Version
    ⊞ Tag: Vendor Specific: RalinkTe
    ⊞ Tag: Vendor Specific: Mediatek
```

Association Request with BTM Support Sent from iPhone6/6S

```
⊞ Frame 1: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits)
⊞ 802.11 radio information
⊞ IEEE 802.11 Association Request, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (4 bytes)
  ⊟ Tagged parameters (111 bytes)
    ⊞ Tag: SSID parameter set: Rorscha-2G
    ⊞ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ⊞ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ⊞ Tag: Power Capability Min: 2, Max :18
    ⊞ Tag: Supported Channels
    ⊞ Tag: RSN Information
    ⊞ Tag: HT Capabilities (802.11n D1.10)
    ⊟ Tag: Extended Capabilities (3 octets)
        Tag Number: Extended Capabilities (127)
        Tag length: 3
      ⊞ Extended Capabilities: 0x00 (octet 1)
      ⊞ Extended Capabilities: 0x00 (octet 2)
      ⊟ Extended Capabilities: 0x08 (octet 3)
          .... ...0 = TFS: Not supported
          .... ..0. = WNM-Sleep Mode: Not supported
          .... .0.. = TIM Broadcast: Not supported
          .... 1... = BSS Transition: Supported
          ...0 .... = QoS Traffic Capability: Not supported
          ..0. .... = AC Station Count: Not supported
          .0.. .... = Multiple BSSID: Not supported
          0... .... = Timing Measurement: Not supported
    ⊞ Tag: Vendor Specific: Broadcom
    ⊞ Tag: Vendor Specific: Microsof: WMM/WME: Information Element
```

Association Response with BTM Support Sent from APUT

```
⊞ Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)
⊞ 802.11 radio information
⊞ IEEE 802.11 Association Response, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (6 bytes)
  ⊟ Tagged parameters (182 bytes)
    ⊞ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    ⊞ Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
    ⊞ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ⊞ Tag: HT Capabilities (802.11n D1.10)
    ⊞ Tag: HT Information (802.11n D1.10)
    ⊞ Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
    ⊞ Tag: Vendor Specific: Epigram: HT Additional Capabilities (802.11n D1.00)
    ⊟ Tag: Extended Capabilities (8 octets)
        Tag Number: Extended Capabilities (127)
        Tag length: 8
      ⊞ Extended Capabilities: 0x01 (octet 1)
      ⊞ Extended Capabilities: 0x00 (octet 2)
      ⊟ Extended Capabilities: 0x08 (octet 3)
          .... ...0 = TFS: Not supported
          .... ..0. = WNM-Sleep Mode: Not supported
          .... .0.. = TIM Broadcast: Not supported
          .... 1... = BSS Transition: Supported
          ...0 .... = QoS Traffic Capability: Not supported
          ..0. .... = AC Station Count: Not supported
          .0.. .... = Multiple BSSID: Not supported
          0... .... = Timing Measurement: Not supported
      ⊞ Extended Capabilities: 0x00 (octet 4)
      ⊞ Extended Capabilities: 0x00 (octet 5)
      ⊞ Extended Capabilities: 0x00 (octet 6)
      ⊞ Extended Capabilities: 0x00 (octet 7)
      ⊞ Extended Capabilities: 0x00 (octet 8)
    ⊞ Tag: Vendor Specific: RalinkTe
    ⊞ Tag: Vendor Specific: Mediatek
```

BTM Request Sent from APUT

```
⊞ Frame 1: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
⊞ 802.11 radio information
⊟ IEEE 802.11 Action, Flags: ........C
    Type/Subtype: Action (0x000d)
  ⊞ Frame Control Field: 0xd000
    .000 0001 0011 0000 = Duration: 304 microseconds
    Receiver address: Apple_8a:48:84 (6c:72:e7:8a:48:84)
    Destination address: Apple_8a:48:84 (6c:72:e7:8a:48:84)
    Transmitter address: RalinkTe_76:20:f0 (00:0c:43:76:20:f0)
    Source address: RalinkTe_76:20:f0 (00:0c:43:76:20:f0)
    BSS Id: RalinkTe_76:20:f0 (00:0c:43:76:20:f0)
    Fragment number: 0
    Sequence number: 3653
  ⊞ Frame check sequence: 0x11e80aa6 [correct]
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters
      Category code: WNM (10)
      Action code: BSS Transition Management Request (7)
      Dialog token: 0x01
      .... ...0 = Preferred Candidate List Included: 0
      .... ..0. = Abridged: 0
      .... .1.. = Disassociation Imminent: 1
      .... 0... = BSS Termination Included: 0
      ...1 .... = ESS Disassociation Imminent: 1
      Disassociation Timer: 600
      Validity Interval: 200
      Session Information URL Length: 33
      Session Information URL: http://we.mediatek.inc/Home/Index
```

BTM Request with BSS Transition Candidate List Entries Sent from APUT

```
802.11 Management - Action
    Category Code:          10  WNM [24]
    Action Code:            7  BSS Transition Management Request [25]
    Dialog Token:           1 [26]
    Request mode:           %00010101 [27]
        Reserved:               %000 [27 Mask 0xE0]
        ESS Disassociation Imminent:%1 [27 Mask 0x10]
        BSS Termination Included:%0 [27 Mask 0x08]
        Disassociation Imminent:%1 [27 Mask 0x04]
        Abridged:               %0 [27 Mask 0x02]
        Preferred Candidate List Included:%1 [27 Mask 0x01]
    Disassociation Timer: 22530 [28-29]
    Validity Interval:      200 [30]
    URL Length:             33 [31]
    URL:                    0x687474703A2F2F77652E6D6564696174656B2E696E632F486F6D652F496E646578 [32-64]
    Neighbor Report
        Element ID:             52  Neighbor Report [65]
        Length:                 13 [66]
        BSSID:                  00:0C:43:26:60:E0  RalinkTech:26:60:E0 [67-72]
        BSSID Information:      %00000011000010000000000000000000 [73-80]
            High Throughput:        %0 [75 Mask 0x08]
            Mobility Domain:        %0 [75 Mask 0x04]
            Capabilities=%000000 Immediate Block Ack=%0 Delayed Block Ack=%0 Radio Measurement=%0 APSD=%0 QoS=%0 Spectrum Management=%0
            Key Scope:              %0  distinct authenticator or the information is not available [76 Mask 0x80]
            Security:               %0 [76 Mask 0x40]
            AP Reachability:        0  Reserved [76 Mask 0x30]
        Regulatory Class:       0 [76]
        Channel Number:         0 [77]
        PHY Type:               36 [78]
    Extra bytes (Padding):(1 bytes) [79 Mask 0xFFFF]
FCS - Frame Check Sequence
    FCS:                    0x25C93E2D [80-83]
```

BTM Response Sent from iPhone6/6S

```
⊞ Frame 1: 33 bytes on wire (264 bits), 33 bytes captured (264 bits)
⊞ 802.11 radio information
⊟ IEEE 802.11 Action  Flags: ........C
    Type/Subtype: Action (0x000d)
  ⊞ Frame Control Field: 0xd000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: RalinkTe_76:20:f0 (00:0c:43:76:20:f0)
    Destination address: RalinkTe_76:20:f0 (00:0c:43:76:20:f0)
    Transmitter address: Apple_8a:48:84 (6c:72:e7:8a:48:84)
    Source address: Apple_8a:48:84 (6c:72:e7:8a:48:84)
    BSS Id: RalinkTe_76:20:f0 (00:0c:43:76:20:f0)
    Fragment number: 0
    Sequence number: 3011
  ⊞ Frame check sequence: 0x6967f404 [correct]
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters
      Category code: WNM (10)
      Action code: BSS Transition Management Response (8)
  ⊞ Tagged parameters (3 bytes)
```

BTM Response Sent from iPhone6/6S (cont.)

- **No matter APUT sends BTM Request with or without BSS Transition Candidate List Entries, iPhone6/6S always sends BTM Response with status code 1**
  - **iPhone6/6S intends to retain association with the current BSS and replies the "Reject" status code by an unspecified reject reason**

```
802.11 Management - Action
    Category Code:          10  WNM [24]
    Action Code:            8   BSS Transition Management Response [25]
    Dialog Token:           1 [26]
    Status code:            1 [27]
    BSS Termination Delay:0 [28]
FCS - Frame Check Sequence
    FCS:                    0x36D0989B [29-32]
```

Status Code	Status code description
0	Accept
1	Reject—Unspecified reject reason.
2	Reject—Insufficient Beacon or Probe Response frames received from all candidates.
3	Reject—Insufficient available capacity from all candidates.
4	Reject—BSS Termination undesired.
5	Reject—BSS Termination delay requested.
6	Reject—STA BSS Transition Candidate List provided.
7	Reject—No suitable BSS transition candidates.
8	Reject—Leaving ESS.
9–255	Reserved

Disassociation Sent from APUT

- **Even though iPhone6/6S replies BTM Response with the "Reject" status code, APUT still can send disassociation to iPhone6/6S and terminate the connection**

```
802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %00  Management [0 Mask 0x0C]
    Subtype:                %1010  Disassociation [0 Mask 0xF0]
    Frame Control Flags:    %00000000 [1]
        0... .... Non-strict order
        .0.. .... Non-Protected Frame
        ..0. .... No More Data
        ...0 .... Power Management - active mode
        .... 0... This is not a Re-Transmission
        .... .0.. Last or Unfragmented Frame
        .... ..0. Not an Exit from the Distribution System
        .... ...0 Not to the Distribution System
    Duration:               314  Microseconds [2-3]
    Destination:            6C:72:E7:8A:48:84 [4-9]
    Source:                 00:0C:43:26:60:28  RalinkTech:26:60:28 [10-15]
    BSSID:                  00:0C:43:26:60:28  RalinkTech:26:60:28 [16-21]
    Seq Number:             82 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
802.11 Management
    Disassociation Reason Code:   4  Disassociated due to inactivity [24-25]
FCS - Frame Check Sequence
    FCS:                    0x59D1F387 [26-29]
```

BTM-related Commands

- Trigger BTM Request :
  - wappctrl ra0/rai0 mbo send_btm_req [peer_mac]-> Send BTM Request to Station.
  - E.g : wappctrl rai0 mbo send_btm_req 0a:0c:43:49:76:f6
- Request Mode Setting :
  - wappctrl ra0 mbo disassoc_imnt 1; → set MBO disassociation imminent bit of BTM
  - wappctrl ra0 mbo disassoc_timer 10; → set how long before AP sending disassociation
  - wappctrl ra0 mbo bss_term_onoff 1; → set MBO BSS termination flag
  - wappctrl ra0 mbo bss_term_duration 2; → set how long the BSS will be down (minute)
  - wappctrl ra0 mbo bss_term_tsf 5; → set how long before BSS shutdown (TSF)
- Add BSS Transition Candidate List :
  - wappctrl ra0 mbo nebor_bssid 00:0C:43:48:50:14;
  - wappctrl ra0 mbo nebor_op_class 81;
  - wappctrl ra0 mbo nebor_op_ch 1;
  - wappctrl ra0 mbo nebor_pref 254;
  - wappctrl ra0 mbo add_test_nr 254;

Indicate Neighbor Report List to Daemon

- mbo_nr.sh [num of entries]
  - mbo_nr.sh 3
  - AP's own bss will be the 1st to append , so you'll only see it appends NO.0~2 in log if indicated 3 entries.
- Show neighbor list
  - wappctrl ra0 mbo nrlist

```
# wappctrl ra0 mbo nrlist
[wapp_cli_cmd_ext]#(cmd(interface=ra0
cmd=mbo nrlist ) len=29)#
 mbo_cmd_show_nrlist, wapp->daemon_nr_list.CurrListNum 3
 No.0 00:0C:43:48:50:14  Pref 255 BssidInfo 0x887  ChNum 6 OpClass 83 PhyType 7
 No.1 60:A4:4C:46:AC:40  Pref 255 BssidInfo 0x807  ChNum 1 OpClass 83 PhyType 7
 No.2 00:0C:43:26:60:20  Pref 255 BssidInfo 0x1807  ChNum 6 OpClass 83 PhyType 7
```

How To Support 802.11v BTM

- Enable ***Passpoint Release-2 Support*** while configuring

```
    EEPROM Type of 1st Card (FLASH)  --->
    EEPROM Type of 2nd Card (EFUSE)  --->
-*- Basic Functions
[*] WSC(WiFi Simple Config)
[*] WSC V2(WiFi Simple Config Version 2.0)
[ ] WSC out-of-band(NFC)
[*] 802.11n Draft3
[*] 802.11ac
-*- PMF Support
[*] Passpoint Release-2 Support
```

- **rlt_wifi_ap or mt_wifi_ap**

- **Kconfig**

```
config PASSPOINT_R2
    bool "Passpoint Release-2 Support"
    depends on WIFI_DRIVER
    select DOT11W_PMF_SUPPORT
    default n
```

- **Makefile**

```
ifeq ($(CONFIG_PASSPOINT_R2),y)
    EXTRA_CFLAGS += -DCONFIG_DOT11U_INTERWORKING -DCONFIG_DOT11V_WNM
                    -DCONFIG_HOTSPOT -DCONFIG_HOTSPOT_R2

  spec_objs += $(RT_WIFI_DIR)/common/wnm.o\
               $(RT_WIFI_DIR)/common/gas.o\
               $(RT_WIFI_DIR)/common/hotspot.o
endif
```

How To Support 802.11v BTM (cont.)

- Input “wapp –d1 –v2” in console to start the Wapp daemon
- Check if wapp is still working well:
  - ps →

```
1848 admin     1344 S    wapp -d1 -v2
1849 admin     1336 S    wapp -d1 -v2
```

  → two lines of wapp exist
- If wapp crash:
  - killall wapp; wapp –d1 –v2

How To Support 802.11v BTM (cont.)

- **If need to support the optional feature to <u>add BSS Transition Candidate List Entries in BTM Request</u>, please enable *802.11k Radio Resource Management* while configuring**

```
<*> Main Mode (AP)  --->
-*- Ralink RT2860 802.11n AP support
[ ]   WDS
[*]   MBSSID
[*]   AP-Client Support
[*]     AP-Client TGn Cert Support
[*]     MAC Repeater Support
[ ] 802.11r Fast BSS Transition
[*] 802.11k Radio Resource Management
```

Extended Capabilities Information Element

Bit(s)	Information	Notes
19	BSS Transition	The STA sets the BSS Transition field to 1 when the MIB attribute dot11MgmtOptionBSSTransitionActivated is true, and sets it to 0 otherwise. See 11.22.6.

WNM Action Details

- **Several Action frame formats are defined for Wireless Network Management (WNM) purposes**
- **WNM Action fields:**

Action field value	Description
6	BSS Transition Management Query
7	BSS Transition Management Request
8	BSS Transition Management Response

BSS Transition Management Query Frame Format

- The BSS Transition Management Query frame uses the Action frame body format and is transmitted by a STA requesting or providing information on BSS transition candidate APs

	Category	Action	Dialog Token	BSS Transition Query Reason	BSS Transition Candidate List Entries (Optional)
Octets:	1	1	1	1	variable

  - Dialog Token: a nonzero value chosen by the STA sending the BSS Transition Management Query to identify the query/request/response transaction
  - BSS Transition Query Reason: contains the reason code for a BSS transition management query
  - BSS Transition Candidate List Entries: contains zero or more Neighbor Report elements

BSS Transition Management Request Frame Format

- **The BSS Transition Management Request frame uses the Action frame body format and is transmitted by an AP STA in response to a BSS Transition Management Query frame, or autonomously**

	Category	Action	Dialog Token	Request mode	Disassociation Timer
Octets:	1	1	1	1	2

	Validity Interval	BSS Termination Duration (optional)	Session Information URL (optional)	BSS Transition Candidate List Entries
Octets:	1	0 or 12	variable	variable

  - **Dialog Token: the nonzero value received in the BSS Transition Management Query frame if the BSS Transition Management Request frame is being transmitted in response to a BSS Transition Management Query frame; If the BSS Transition Management Request frame is being transmitted other than in response to a BSS Transition Management Query frame, then the Dialog Token field is a nonzero value chosen by the AP STA sending the BSS Transition Management Request frame to identify the request/response transaction**

BSS Transition Management Request Frame Format (cont.)

- Disassociation Timer: the time after which the AP will issue a Disassociation frame to this STA. A value of 0 indicates that the AP has not determined when it will send a Disassociation frame to this STA
- Validity Interval: the number of beacon transmission times (TBTTs) until the BSS transition candidate list is no longer valid
- BSS Termination Duration: contains the BSS Termination Duration subelement for the current BSS and is present only when the BSS Termination Included field is 1 in the Request mode field
- Session Information URL(optional): is present when the ESS Disassociation Imminent field is 1
- BSS Transition Candidate List Entries: contains one or more Neighbor Report elements

BSS Transition Management Request Frame Format (cont.)

octet number	1	2	3	4	5-6	7	0 or 12 [8-19]	variable	variable
function	Category	Action	Dialog Token	Request Mode	Disassociation Timer	Validity Interval	BSS Termination Duration	Session Information URL	BSS Transition Candidate List Entries

Bit number	0	1	2	3	4	5-7
function	Preferred Candidate List Included	Abridged	Disassociation Imminent	BSS Termination Included	ESS Disassociation Imminent	Reserved

Neighbor Report Information Elements

octet number	1	2	3-8	9-12	13	14	15	16-
function	Element ID	Length	BSSID	BSSID Information	Regulatory Class	Channel Number	PHY Type	Optional sub-elements

bit number	0-1	2	3	4-9	10	11	12-31
function	AP Reachability	Security	Key Scope	Capabilities	Mobility Domain	High Throughput	Reserved

BSS Transition Management Response Frame Format

- The BSS Transition Management Response frame uses the Action frame body format and is optionally transmitted by a STA in response to a BSS Transition Management Request frame

	Category	Action	Dialog Token	Status code	BSS Ter-mination Delay	Target BSSID (Optional)	BSS Transi-tion Candi-date List Entries (Optional)
Octets:	1	1	1	1	1	0 or 6	variable

  - Dialog Token: the value in the corresponding BSS Transition Management Request frame
  - Status code: the status code in response to a BSS Transition Management Request frame. If the STA will transition to another BSS, then the status code is 0 (i.e.,Accept). If the STA intends to retain the association with the current BSS, the status code is one of the “Reject” status codes.
  - BSS Termination Delay: the number of minutes that the responding STA requests the BSS to delay termination
  - Target BSSID: the BSSID of the BSS that the non-AP STA transitions to
  - BSS Transition Candidate List Entries: contains zero or more Neighbor Report elements

802.11k Introduction

IEEE 802.11k

- Radio Resource Management (RRM)
- RRM defines and exposes radio and network information to facilitate the management and maintenance of a mobile WLAN
- Simply speaking, it just provides information for STA to discover the best available AP

MTK 802.11k Implementation

- **Mediatek does not have full 11k amendment implemented and actually the following items are what we have**
  - **Action frame**
    - Neighbor Report
    - AP Channel Report Capability
  - **IE**
    - Beacon Report

Mediatek RRM IE

- **Neighbor Report**
- **Beacon Report**
- **AP Channel Report**

```
◢ Tag: RM Enabled Capabilities (5 octets)
    Tag Number: RM Enabled Capabilities (70)
    Tag length: 5
  ◢ RM Capabilities: 0xf3 (octet 1)
      .... ...1 = Link Measurement: Enabled
      .... ..1. = Neighbor Report: Enabled
      .... .0.. = Parallel Measurements: Disabled
      .... 0... = Repeated Measurements: Disabled
      ...1 .... = Beacon Passive Measurement: Enabled
      ..1. .... = Beacon Active Measurement: Enabled
      .1.. .... = Beacon Table Measurement: Supported
      1... .... = Beacon Measurement Reporting Conditions: Enabled
  ◢ RM Capabilities: 0xc0 (octet 2)
      .... ...0 = Frame Measurement: Disabled
      .... ..0. = Channel Load Measurement: Disabled
      .... .0.. = Noise Histogram Measurement: Disabled
      .... 0... = Statistics Measurement: Disabled
      ...0 .... = LCI Measurement: Disabled
      ..0. .... = LCI Azimuth capability: Disabled
      .1.. .... = Transmit Stream/Category Measurement: Supported
      1... .... = Triggered Transmit Stream/Category Measurement: Enabled
  ◢ RM Capabilities: 0x01 (octet 3)
      .... ...1 = AP Channel Report capability: Enabled
      .... ..0. = RM MIB capability: Disabled
      ...0 00.. = Operating Channel Max Measurement Duration: 0
      000. .... = Nonoperating Channel Max Measurement Duration: 0
  ▷ RM Capabilities: 0x00 (octet 4)
  ▷ RM Capabilities: 0x00 (octet 5)
```

Kernel Configuration

- **DOT11K_RRM_SUPPORT**

```
config DOT11K_RRM_SUPPORT
        bool "802.11k Radio Resource Management"
        depends on MT_AP_SUPPORT
        default n
```

```
#RRM
ifeq ($(CONFIG_DOT11K_RRM_SUPPORT),y)
    EXTRA_CFLAGS += -DDOT11K_RRM_SUPPORT -DAP_SCAN_SUPPORT -DSCAN_SUPPORT -DAPPLE_11K_IOT
    spec_objs += $(SRC_EMBEDDED_DIR)/common/rrm_tlv.o \
                 $(SRC_EMBEDDED_DIR)/common/rrm.o \
                 $(SRC_EMBEDDED_DIR)/common/rrm_sanity.o
endif
```

Profile Settings

- How to turn on/off RRM
  - RRMEnable=1: ON
  - RRMEnable=0: OFF

iwpriv Command

- **How to show RRM information**
  - **iwpriv rai0 show rrminfo**

For E.g :

```
root@OpenWrt:/# iwpriv rai0 show rrminfo
[69298.812000] 0: bDot11kRRMEnable=1
[69298.820000] Regulator Class=115
[69298.824000] 1: bDot11kRRMEnable=1
[69298.832000] Regulator Class=128
[69298.840000] 2: bDot11kRRMEnable=1
[69298.844000] Regulator Class=128
[69298.852000] 3: bDot11kRRMEnable=1
[69298.856000] Regulator Class=128
[69298.864000] Country Code=US
[69298.872000] Power Constraint=0
[69298.876000] Regulator TxPowerPercentage=100
```

802.11k
Functional test setup

Our Purpose

- **Copy the packet exchange behavior of Apple router with iPhone**
  - **Apple router has only two bits ON**
  - **Mediatek only covers this two capabilities**
    - Neighbor Report (Nego. by Action Frame)
    - AP Channel Report Capability (Static IE)

Apple Router RRM Capability

- **Apple router RRM IE**
  - **Neighbor Report**
  - **AP Channel Report**

```
⊟ Tag: RM Enabled Capabilities (5 octets)
    Tag Number: RM Enabled Capabilities (70)
    Tag length: 5
  ⊟ RM Capabilities: 0x02 (octet 1)
        .....0 = Link Measurement: Disabled
        .....1. = Neighbor Report: Enabled
        ....0... = Parallel Measurements: Disabled
        ....0... = Repeated Measurements: Disabled
        ...0 .... = Beacon Passive Measurement: Disabled
        ..0. .... = Beacon Active Measurement: Disabled
        .0.. .... = Beacon Table Measurement: Not supported
        0... .... = Beacon Measurement Reporting Conditions: Disabled
  ⊟ RM Capabilities: 0x00 (octet 2)
        .... ...0 = Frame Measurement: Disabled
        .... ..0. = Channel Load Measurement: Disabled
        .... .0.. = Noise Histogram Measurement: Disabled
        .... 0... = Statistics Measurement: Disabled
        ...0 .... = LCI Measurement: Disabled
        ..0. .... = LCI Azimuth capability: Disabled
        .0.. .... = Transmit Stream/Category Measurement: Not supported
        0... .... = Triggered Transmit Stream/Category Measurement: Disabled
  ⊟ RM Capabilities: 0x01 (octet 3)
        .... ...1 = AP Channel Report capability: Enabled
        .... ..0. = RM MIB capability: Disabled
        ...0 00.. = Operating Channel Max Measurement Duration: 0
        000. .... = Nonoperating Channel Max Measurement Duration: 0
  ⊟ RM Capabilities: 0x00 (octet 4)
        .... .000 = Measurement Pilotcapability: 0
        .... 0... = Measurement Pilot Transmission Information: Disabled
        ...0 .... = Neighbor Report TSF Offset: Disabled
        ..0. .... = RCPI Measurement capability: Disabled
        .0.. .... = RSNI Measurement capability: Not supported
        0... .... = BSS Average Access Delay capability: Disabled
  ⊟ RM Capabilities: 0x00 (octet 5)
        .... ...0 = BSS Available Admission Capacity capability: Disabled
        .... ..0. = Antenna capability: Disabled
        0000 00.. = Reserved: 0x00
```

Neighbor Report Testing Steps

1. AP1 power on with RRMEnable=1 (SSID=AAA)
2. AP2 power on (SSID=AAA)
   - SSID of AP2 MUST be exactly the same with that of AP1 (MTK proprietary design)
   - Channel is not necessarily the same with AP1, but MUST be in the same band and in the range of AP1's channel list
   - AP2 does not need to turn on RRM
   - Security is not necessarily the same with AP1
3. AP1 needs to do "iwpriv ra0 set SiteSurvey=" before iPhone connects to AP1. This is to make sure that AP2 would be in the current scan list of AP1. SiteSurvey should be triggered by user manually, because it is not an original feature of 11k itself
4. iPhone 6 or other 11k-supported (Neighbor Report) STAs connect to AP1

MT7615 + iPhone 6 (Neighbor Report Request)

MT7615_RRM_ON_IPHONE6_OPNE_NONE.pkt [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Channel	RATE	RSSI	Protocol	Length	Sequence number	Info
410	34.911569800	RalinkTe_26:60:a8	Broadcast		6.0	94%	802.11	263	1839	Beacon frame, SN=1839, FN=0, Flags=.
411	35.013934800	RalinkTe_26:60:a8	Broadcast		6.0	94%	802.11	263	1840	Beacon frame, SN=1840, FN=0, Flags=.
412	35.116313800	RalinkTe_26:60:a8	Broadcast		6.0	94%	802.11	263	1841	Beacon frame, SN=1841, FN=0, Flags=.
413	35.218684800	RalinkTe_26:60:a8	Broadcast		6.0	94%	802.11	263	1842	Beacon frame, SN=1842, FN=0, Flags=.
414	35.321315800	RalinkTe_26:60:a8	Broadcast		6.0	94%	802.11	263	1843	Beacon frame, SN=1843, FN=0, Flags=.
415	35.423556800	RalinkTe_26:60:a8	Broadcast		6.0	99%	802.11	263	1844	Beacon frame, SN=1844, FN=0, Flags=.
416	35.525933800	RalinkTe_26:60:a8	Broadcast		6.0	94%	802.11	263	1845	Beacon frame, SN=1845, FN=0, Flags=.
417	35.540183800	Apple_1c:46:9c	RalinkTe_26:60:a8		6.0	73%	802.11	55	1815	Authentication, SN=1815, FN=0, Flags
418	35.559060800	RalinkTe_26:60:a8	Apple_1c:46:9c		6.0	94%	802.11	34	0	Authentication, SN=0, FN=0, Flags=..
419	35.559061800		RalinkTe_26:60:a8 (R		6.0	73%	802.11	14		Acknowledgement, Flags=.....
420	35.559800800	Apple_1c:46:9c	RalinkTe_26:60:a8		6.0	73%	802.11	155	1816	Association Request, SN=1816, FN=0,
421	35.560427800	RalinkTe_26:60:a8	Apple_1c:46:9c		6.0	94%	802.11	264	1	Association Response, SN=1, FN=0, Fl
422	35.560429800		RalinkTe_26:60:a8 (R		6.0	73%	802.11	14		Acknowledgement, Flags=.....
423	35.561677800	Apple_1c:46:9c	RalinkTe_26:60:a8		6.0	73%	802.11	49	1817	Action, SN=1817, FN=0, Flags=.....
424	35.561679800	Apple_1c:46:9c	RalinkTe_26:60:a8		24.0	73%	802.11	28	1818	Null function (No data), SN=1818, FN
425	35.575181800	Apple_1c:46:9c	RalinkTe_26:60:a8		24.0	73%	802.11	28	1819	Null function (No data), SN=1819, FN
426	35.577683800	RalinkTe_26:60:a8	Apple_1c:46:9c		6.0	94%	802.11	46	2	Action, SN=2, FN=0, Flags=.....
427	35.577686800		RalinkTe_26:60:a8 (R		6.0	73%	802.11	14		Acknowledgement, Flags=.....
428	35.578055800	RalinkTe_26:60:a8	Apple_1c:46:9c		6.0	94%	802.11	37	3	Action, SN=3, FN=0, Flags=.....
429	35.578057800		RalinkTe_26:60:a8 (R		6.0	73%	802.11	14		Acknowledgement, Flags=.....
430	35.578058800	Apple_1c:46:9c	RalinkTe_26:60:a8		6.0	73%	802.11	37	1820	Action, SN=1820, FN=0, Flags=.....
431	35.578307800	RalinkTe_26:60:a8 (TA)	Apple_1c:46:9c (RA)		6.0	94%	802.11	48		802.11 Block Ack Req, Flags=.....

```
⊞ Frame 423: 49 bytes on wire (392 bits), 49 bytes captured (392 bits)
⊞ 802.11 radio information
⊞ IEEE 802.11 Action, Flags: .........
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Neighbor Report Request (4)
      Dialog token: 1
  ⊟ Tagged parameters (18 bytes)
    ⊟ Tag: SSID parameter set: MT7615_YIWEI_RRM
        Tag Number: SSID parameter set (0)
        Tag length: 16
        SSID: MT7615_YIWEI_RRM
```

MT7615 + iPhone 6 (Neighbor Report Response)

MT7615_RRM_ON_IPHONE6_OPNE_NONE.pkt [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Channel	RATE	RSSI	Protocol	Length	Sequence number	Info
426	35.577683800	RalinkTe_26:60:a8	Apple_1c:46:9c		6.0	94%	802.11	46	2	Action, SN=2, FN=0, Flags=.....
427	35.577686800		RalinkTe_26:60:a8 (R		6.0	73%	802.11	14		Acknowledgement, Flags=.....
428	35.578055800	RalinkTe_26:60:a8	Apple_1c:46:9c		6.0	94%	802.11	37	3	Action, SN=3, FN=0, Flags=.....
429	35.578057800		RalinkTe_26:60:a8 (R		6.0	73%	802.11	14		Acknowledgement, Flags=.....
430	35.578058800	Apple_1c:46:9c	RalinkTe_26:60:a8		6.0	73%	802.11	37	1820	Action, SN=1820, FN=0, Flags=.....
431	35.578307800	RalinkTe_26:60:a8 (TA)	Apple_1c:46:9c (RA)		6.0	94%	802.11	48		802.11 Block Ack Req, Flags=.....
432	35.578310800	Apple_1c:46:9c	RalinkTe_26:60:a8		1.0	0%	802.11	28	0	Association Request, SN=0, FN=0, F

```
⊞ Frame 426: 46 bytes on wire (368 bits), 46 bytes captured (368 bits)
⊞ 802.11 radio information
⊞ IEEE 802.11 Action, Flags: .........
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Neighbor Report Response (5)
      Dialog token: 1
  ⊟ Tagged parameters (15 bytes)
    ⊟ Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 13
        BSSID: RalinkTe_44:08:6a (00:0c:43:44:08:6a)
      ⊟ BSSID Information: 0x00000003
          .... .... .... .... .... .... .... ..11 = AP Reachability: Reachable (0x00000003)
          .... .... .... .... .... .... .... .0.. = Security: False
          .... .... .... .... .... .... .... 0... = Key Scope: False
        ⊞ .... .... .... .... .... .... ..00 0000 .... = Capability: 0x00000000
          .... .... .... .... .... .0.. .... .... = Mobility Domain: False
          .... .... .... .... .... 0... .... .... = High Throughput Control (+HTC): False
          0000 0000 0000 0000 0000 .... .... .... = Reserved: 0x00000000
        Operating Class: 0
        Channel Number: 36 (iterative measurements on that Channel Number)
        PHY Type: 0x00
```

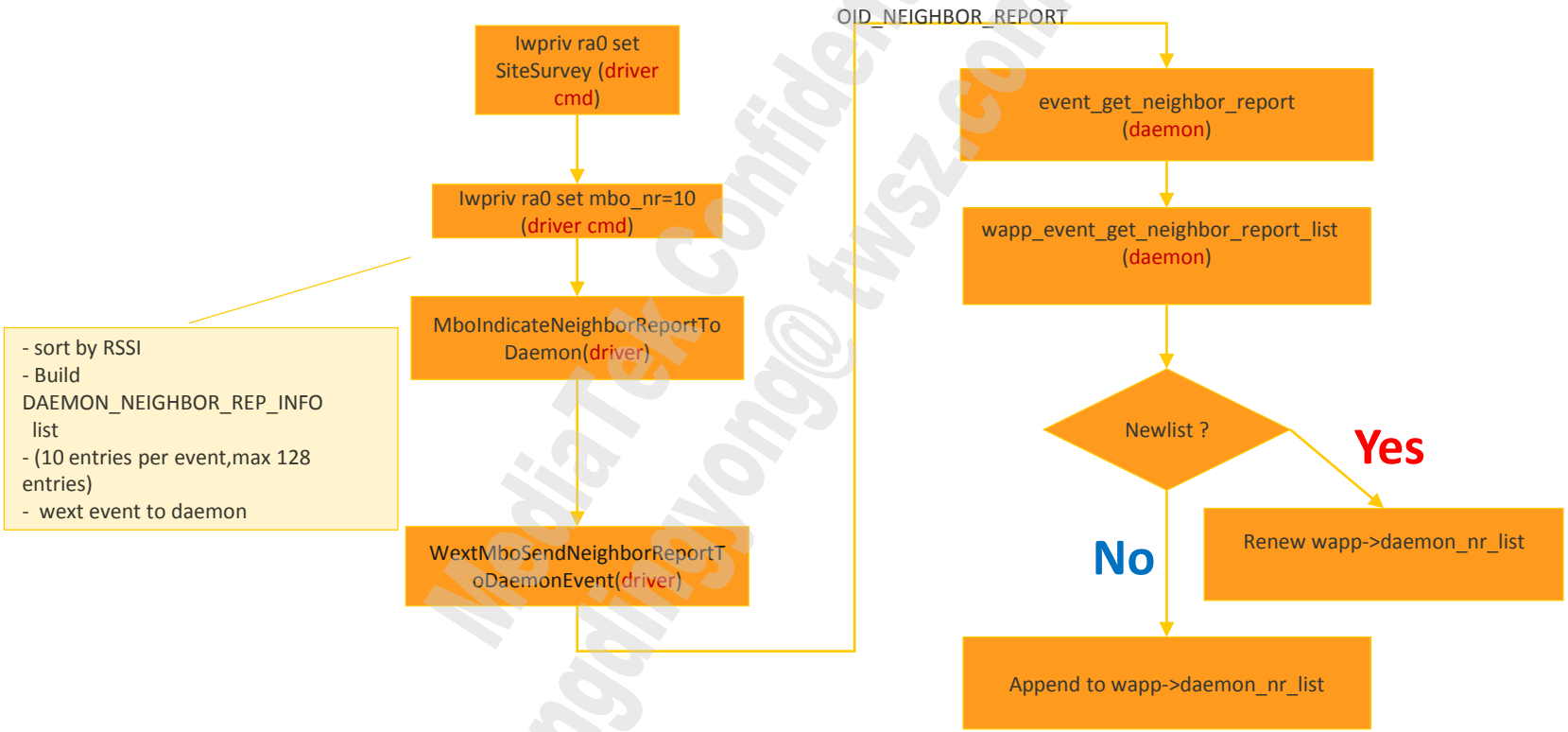
Neighbor Report

- **IEEE Std. 802.11-2012**

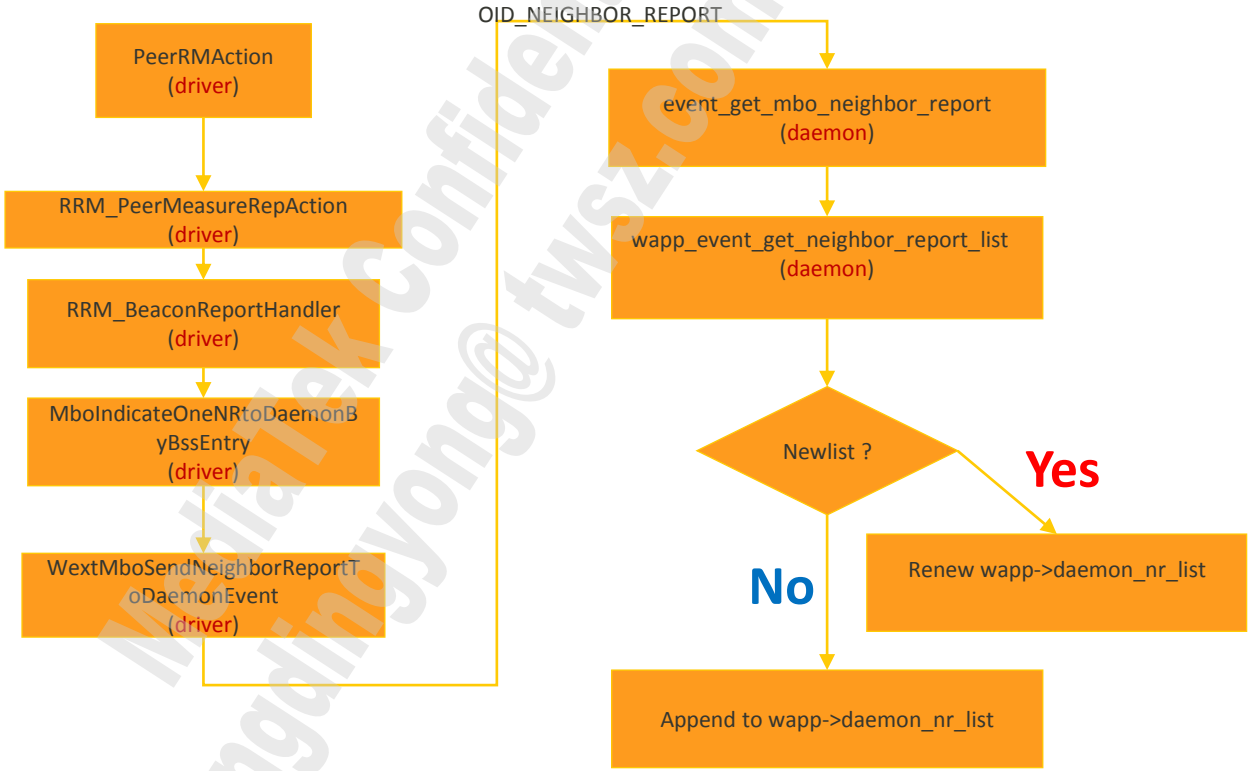
4.3.8.10 Neighbor report

The neighbor report request is sent to an AP, which returns a neighbor report containing information about known neighbor APs that are candidates for a service set transition. Neighbor reports contain information from the table dot11RMNeighborReportTable in the MIB concerning neighbor APs. This request/report pair enables a STA to gain information about the neighbors of the associated AP to be used as potential roaming candidates.

[BTM/ANQP] Neighbor Report List Indicate to Daemon – mbo_nr.sh



[Beacon Report Response] Neighbor Report List Indicate to Daemon



802.11r Introduction

IEEE 802.11R

- Fast BSS Transition (FT)
- FT permits continuous connectivity aboard wireless devices in motion with fast and secure handoffs in a seamless manner
- Simply speaking, it redefines the security key negotiation protocol, allowing both the negotiation and request for wireless resources to occur in parallel

802.11r
Introduction to SPEC

Outline

- Introduction
- Terminology
- FT protocol & method
- FT messages
- FT key hierarchy
- FT key distribution (IAPP)

IEEE 802.11r

- A.K.A. Fast BSS Transition (FT)
- FT seeks to reduce the length of time that connectivity is lost between a STA and the DS during a BSS transition
  - Up to 100ms transition time might be saved

IEEE 802.11r

- FT redefines the security key negotiation protocol, allowing both the key negotiation and request for wireless resources to occur in parallel
- Simply speaking, the 4-way key handshake is saved in a FT process

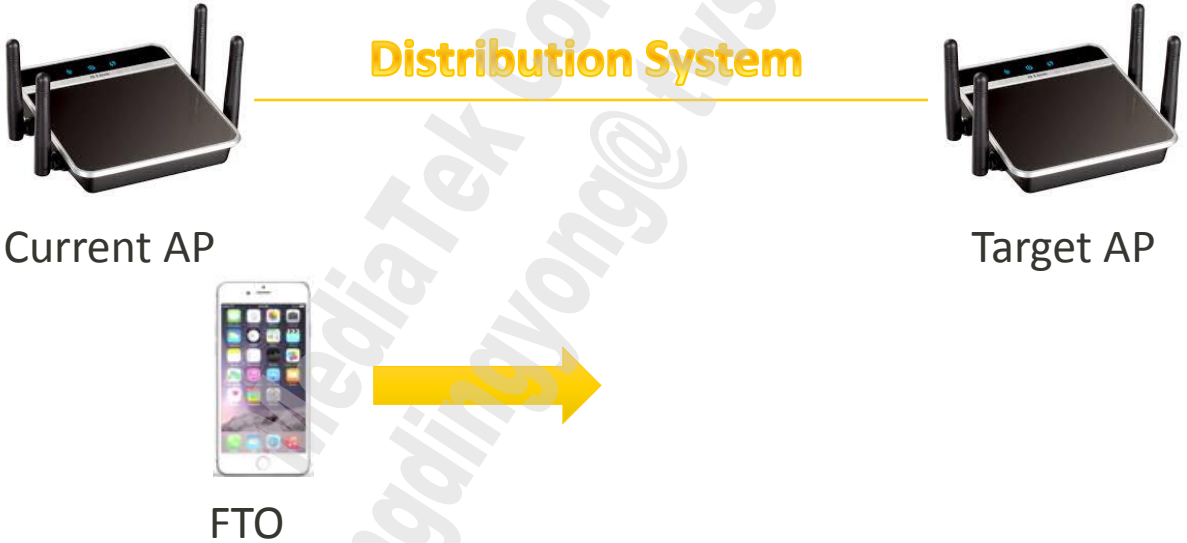
4-Way Key Handshake Saved

- Auth (open)
- Auth (open)
- Assoc Request
- Assoc Response
- 4-way msg-1
- 4-way msg-2
- 4-way msg-3
- 4-way msg-4

- Auth (FT request)
- Auth (FT response)
- Reassoc Request
- Reassoc Response

FT Terminology

- **FT Originator**
- **Current AP**
- **Target AP**



FT Protocols

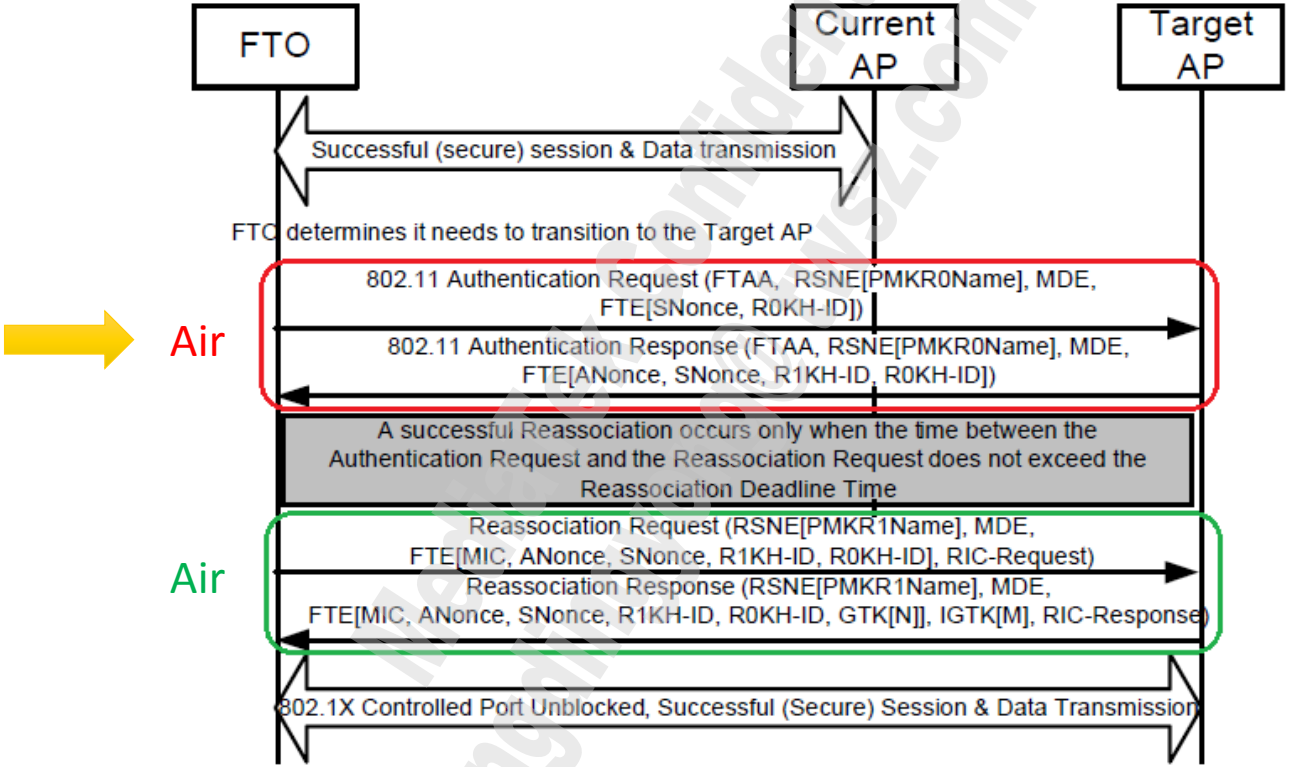
- FT Protocol
  - FTO makes a transition to a target AP and does NOT require a resource request prior to its transition
  - Total 4 messages required
- FT Resource Request Protocol
  - FTO requires a resource request prior to its transition
  - Total 6 messages required
  - Not implemented

FT Methods

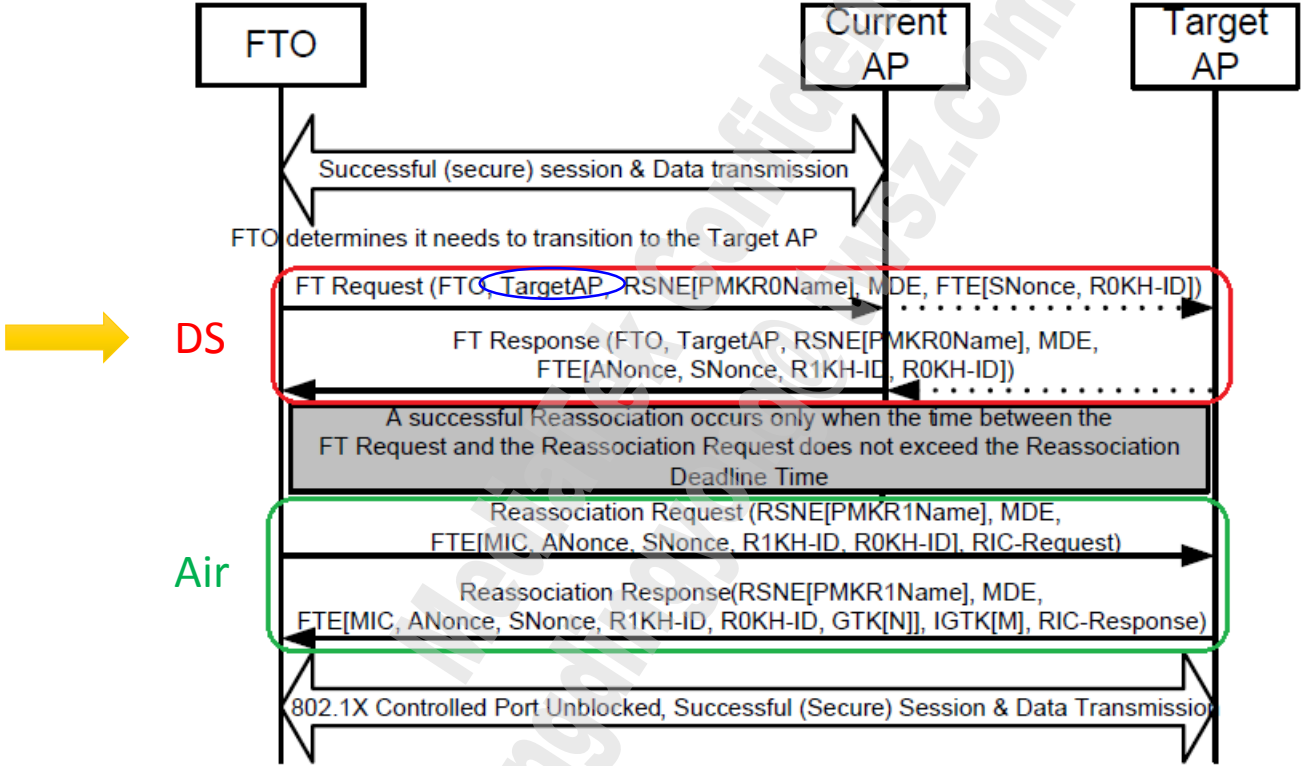
- **Over-The-Air (OTA)**
  - The FTO communicates directly with the target AP using **FT authentication algorithm**
- **Over-The-DS (OTD)**
  - The FTO communicates with the target AP via the current AP using **FT Action frames**
  - Optional

```
◢ Tag: Mobility Domain
    Tag Number: Mobility Domain (54)
    Tag length: 3
    Mobility Domain Identifier: 0x5452
    FT Capability and Policy: 0x03
    .... ...1 = Fast BSS Transition over DS: 0x1
    .... ..1. = Resource Request Protocol Capability: 0x1
```

Over-The-Air



Over-The-DS



How FT Works

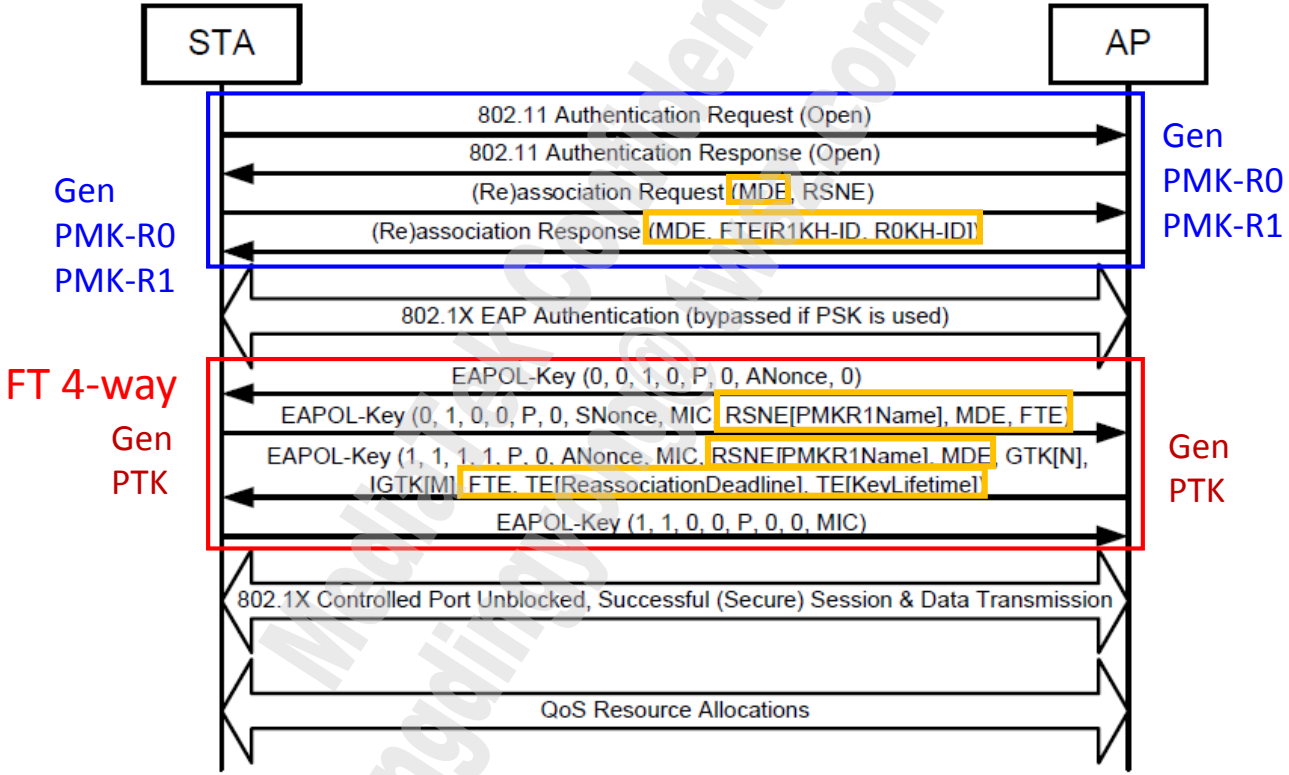
- The contents of 4-way key handshake are distributed evenly to the following four frames
  - FT Request (Auth/Action)
  - FT Response (Auth/Action)
  - Reassociation Request
  - Reassociation Response

38:48:4C:68:F1:1E	RalinkTech:26:60:F0	RalinkTech:26:60:F0	802.11 Auth	FC=.....,SN= 647,FN= 0,Algorithm=2,ATSN=1,Status=0
RalinkTech:26:60:F0	38:48:4C:68:F1:1E	RalinkTech:26:60:F0	802.11 Auth	FC=.....,SN= 0,FN= 0,Algorithm=2,ATSN=2,Status=0
38:48:4C:68:F1:1E	RalinkTech:26:60:F0	RalinkTech:26:60:F0	802.11 Reassoc Req	FC=.....,SN= 648,FN= 0,Listen=20,AP=RalinkTech:47:02:C8
RalinkTech:26:60:F0	38:48:4C:68:F1:1E	RalinkTech:26:60:F0	802.11 Reassoc Rsp	FC=.....,SN= 0,FN= 0,Status=0,AID=1

FT Key Distribution

- The distribution of keys from R0KH (Current AP) to the R1KHs (Target APs) is outside the scope of 802.11r
- Mediatek implementation of IAPP is wappd
  - The distribution of keys happens when a FTO first connects (FT initial mobility domain association) to the current AP which would be termed R0KH

FT Initial Mobility Domain Association



802.11r
Mediatek implementation

Kernel Configuration

- **DOT11R_FT_SUPPORT**

```
config DOT11R_FT_SUPPORT
        bool "802.11r Fast BSS Transition"
        depends on MT_AP_SUPPORT
        default n
```

```
# FT
ifeq ($(CONFIG_DOT11R_FT_SUPPORT),y)
EXTRA_CFLAGS += -DDOT11R_FT_SUPPORT
dot11_ft_objs += $(SRC_EMBEDDED_DIR)/common/ft.o\
                 $(SRC_EMBEDDED_DIR)/common/ft_tlv.o\
                 $(SRC_EMBEDDED_DIR)/common/ft_iocl.o\
                 $(SRC_EMBEDDED_DIR)/common/ft_rc.o\
                 $(SRC_EMBEDDED_DIR)/ap/ap_ftkd.o
endif
```

Profile Settings

- How to turn on FT
  - FtSupport=1
- How to turn off FT
  - FtSupport=0

iwpriv Command

- How to show FT information
  - iwpriv ra0 show ftinfo

```
root@OpenWrt:/# iwpriv ra0 show ftinfo
[ 6891.904000] MDID=RT
[ 6891.908000] R0KHID=Ralink:11:b4:58:2a:f3:5d, Len=24
[ 6891.916000] FT Enable=1
[ 6891.924000] FT RIC=0
[ 6891.928000] FT OTD=1
[ 6891.932000]
[ 6891.932000] PMKID Cache INFO: (now: 1647983)
[ 6891.944000]
[ 6891.944000] FT_R1KH_ENTRY Cache INFO:
[ 6891.952000] R0KHID(bin)=
```

IAPP Daemon

- Mediatek has its own Inter-Access Point Protocol (IAPP) daemon which defines the communication protocol between APs to exchange messages
- MTK IAPP daemon has no inter-operability with IAPP daemons from other vendors

User Configuration

- ralinkiappd (Deprecated)
  - source/user/ralinkiappd
  - Old version
  - Support one interface only
- mtkiappd
  - source/user/mtkiappd
  - Old version
  - Support multiple interfaces
  - Included only after SDK v5.0.2.0
    - MediaTek_APSoC_SDK5020_20160630.tar.bz2
- wapp (EasyMesh)
  - build_dir/target-mipsel_24kec+dsp_uClibc-0.9.33.2/wappd/iapp
  - New version
  - Support multiple interfaces

How to Launch the Daemon

- **# wapp –d1 –c ra0 –c rax0**

```
USAGE:     wapp <-d debug level> <-c wireless_if_name>

Default:   wapp -d1 -cra0 -crax0
```

  – ***Note: All APs must be within the same subnet***

```
# mtkiappd -d 3
iapp> -e=br0, -w=br0, -wi=ra0, IfNameWlanCount = 1
iapp> (ver.v1.1.0) task start...
iapp> own address (10.10.10.252)
iapp> broadcast address (10.10.10.255)
iapp> network Mask address (255.255.255.0)
# iapp> (FlgIsMsgReady is TRUE)
iapp> Register ethernet interface as (br0)
iapp> mt_iapp_get_wifi_iface_mac - IfName[0]: ra0
MAC: 0x4171b8, len = 6
0x0000 : 00 0c 43 26 60 0a
iapp> Process ID = 0x10ee (0 0)
iapp>[ra0]IOCTL Flags = 0x8404!
iapp>[ra0]IOCTL Flags = 0x840b!
```

Limitation

- Mediatek 11r has NO inter-operability with other vendors since no specific definition and test plan for IAPP
- PMF should be disabled if you want your device to support both iPhone and Android STAs
- Only two wireless interfaces are supported

802.11r
Functional test setup

Outline

- How to test
  - With EasyMesh
  - Without EasyMesh

EasyMesh Scenarios

- Scenario 1
  - STA roaming from Controller to Agent
- Scenario 2
  - STA roaming from Agent to Controller

How-To

- **Configure "FtSupport=1" in profile to enable FT function**

```
(7615D)
# nvram_set 2860 FtSupport "1;1;1;1"
# nvram_set rtdev FtSupport "1;1;1;1"
# nvram_set 2860 FtOtd "1;1;1;1"        //Optional
# nvram_set rtdev FtOtd "1;1;1;1"       //Optional
# reboot
```

- **Check whether wapp has 11r related parameters**

```
root@OpenWrt:/# ps
  PID USER       VSZ STAT COMMAND
 2917 root      1436 S    wapp -d1 -v2 -cra0 -crax0
 2918 root      1400 S    wapp -d1 -v2 -cra0 -crax0
```

- **Run Wi-Fi onboarding at both Controller and Agent**

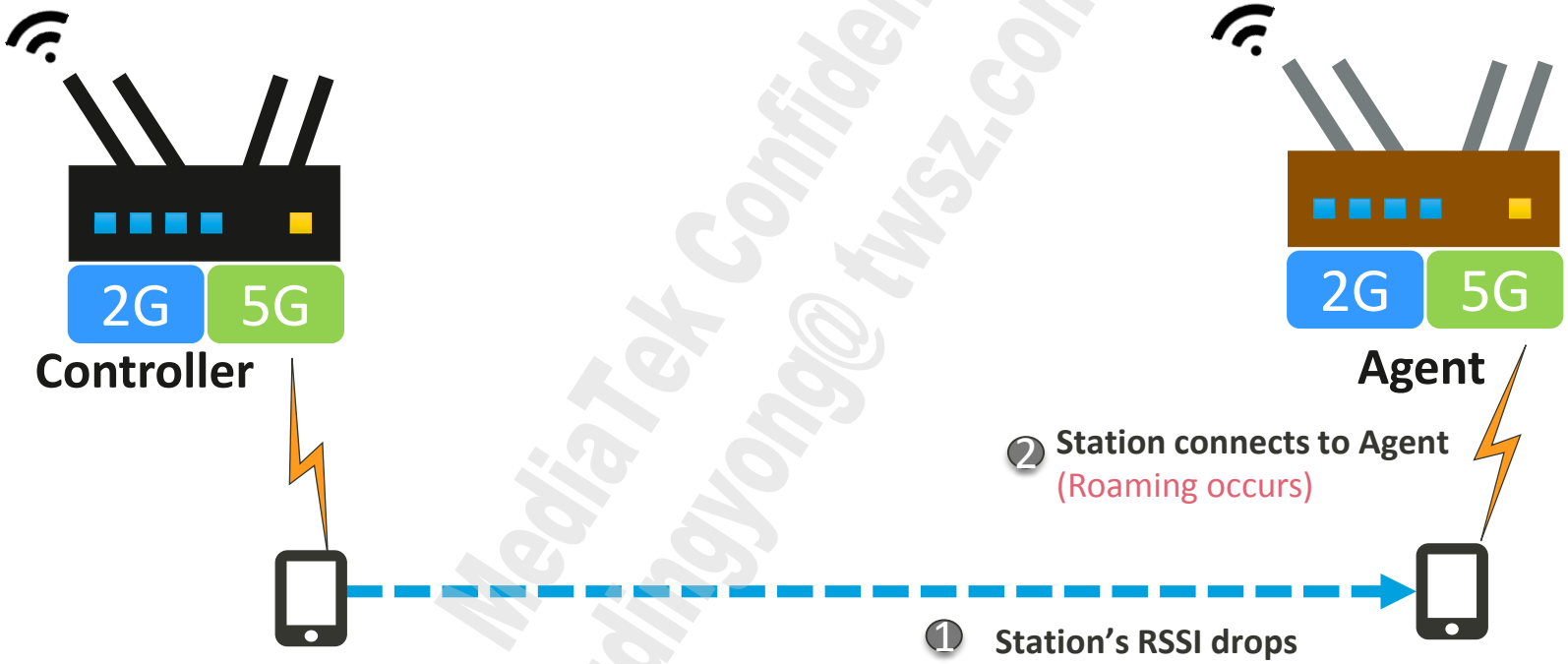
```
# wappctrl ra0 wps_pbc
```

Scenario 1

- Scenario 1
  - Controller and Agent are located at different places
  - iPhone XR first connects to 5LG-1 of Controller whose BSSID is 00:11:22:33:44:90
  - iPhone XR moves from Controller to Agent

- Result: When the RSSI of iPhone XR is about -65 dBm, the iPhone XR will roam to 5LG-1 of the Agent

Scenario 1



Packets

- **Authentication packets with Fast BSS Transition algorithm**

No.	Time	Source	Destination	Protocol	Length	Info
14	17:30:11.08…	Apple_98:18:70	Cimsys_33:44:a8	802.11	213	Authentication, SN=418,
15	17:30:11.09…	Cimsys_33:44:a8	Apple_98:18:70	802.11	201	Authentication, SN=0, F
16	17:30:11.10…	Apple_98:18:70	Cimsys_33:44:a8	802.11	342	Reassociation Request,
17	17:30:11.18…	Cimsys_33:44:a8	Apple_98:18:70	802.11	477	Reassociation Response,

```
▷ Frame 14: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits)
▷ IEEE 802.11 Authentication, Flags: ........
◢ IEEE 802.11 wireless LAN
  ◢ Fixed parameters (6 bytes)
      Authentication Algorithm: Fast BSS Transition (2)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
  ◢ Tagged parameters (183 bytes)
    ▷ Tag: RSN Information
    ▷ Tag: Mobility Domain
    ▷ Tag: Fast BSS Transition
```

```
▷ Frame 15: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)
▷ IEEE 802.11 Authentication, Flags: ........
◢ IEEE 802.11 wireless LAN
  ◢ Fixed parameters (6 bytes)
      Authentication Algorithm: Fast BSS Transition (2)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
  ◢ Tagged parameters (171 bytes)
    ▷ Tag: Mobility Domain
    ▷ Tag: Fast BSS Transition
    ▷ Tag: RSN Information
```

Packets

- **New handshake packets for 802.11r**
  - **Auth-Req/Auth-Rsp/Reassoc-Req/Reassoc-Rsp**
- **No more 4-way handshake packets**

No.	Time	Source	Destination	Protocol	Length	Info
8	17:30:08.04…	Cimsys_33:44:a8	Apple_98:18:70	802.11	368	Probe Response, SN=3300, FN=0, Flags=....., BI=100, SSID=Miga-Multi-AP-5LG-1[Pac
9	17:30:08.93…	Apple_98:18:70	Cimsys_33:44:90	802.11	34	Action, SN=380, FN=0, Flags=...P....[Malformed Packet]
10	17:30:08.94…	Apple_98:18:70	Cimsys_33:44:90	802.11	37	Action, SN=382, FN=0, Flags=.....[Malformed Packet]
11	17:30:10.77…	Apple_98:18:70	Cimsys_33:44:90	802.11	197	Action, SN=415, FN=0, Flags=.....
12	17:30:10.92…	Apple_98:18:70	Cimsys_33:44:90	802.11	34	Action, SN=416, FN=0, Flags=.....
13	17:30:10.94…	Apple_98:18:70	Cimsys_33:44:90	802.11	37	Action, SN=417, FN=0, Flags=.....[Packet size limited during capture]
14	17:30:11.08…	Apple_98:18:70	Cimsys_33:44:a8	802.11	213	Authentication, SN=418, FN=0, Flags=.....[Malformed Packet]
15	17:30:11.09…	Cimsys_33:44:a8	Apple_98:18:70	802.11	201	Authentication, SN=0, FN=0, Flags=.....[Malformed Packet]
16	17:30:11.10…	Apple_98:18:70	Cimsys_33:44:a8	802.11	342	Reassociation Request, SN=419, FN=0, Flags=....., SSID=Miga-Multi-AP-5LG-1
17	17:30:11.18…	Cimsys_33:44:a8	Apple_98:18:70	802.11	477	Reassociation Response, SN=1, FN=0, Flags=.....[Malformed Packet]
18	17:30:11.18…	Apple_98:18:70	Cimsys_33:44:a8	802.11	52	Action, SN=420, FN=0, Flags=....., SSID=Miga-Multi-AP-5LG-1[Malformed Packet]
19	17:30:11.19…	Apple_98:18:70	Cimsys_33:44:90	802.11	30	Deauthentication, SN=421, FN=0, Flags=.....[Packet size limited during capture]
20	17:30:11.19…	Apple_98:18:70	Cimsys_33:44:90	802.11	30	Deauthentication, SN=422, FN=0, Flags=.....[Malformed Packet]
21	17:30:11.19…	Apple_98:18:70	Cimsys_33:44:90	802.11	30	Deauthentication, SN=423, FN=0, Flags=.....[Packet size limited during capture]
22	17:30:11.19…	Apple_98:18:70	Cimsys_33:44:90	802.11	30	Deauthentication, SN=424, FN=0, Flags=.....[Malformed Packet]
23	17:30:11.21…	Cimsys_33:44:a8	Apple_98:18:70	802.11	46	Action, SN=2, FN=0, Flags=.....
24	17:30:11.21…	Cimsys_33:44:a8	Apple_98:18:70	802.11	37	Action, SN=3, FN=0, Flags=.....
25	17:30:11.21…	Apple_98:18:70	Cimsys_33:44:a8	802.11	37	Action, SN=425, FN=0, Flags=.....[Malformed Packet]
26	17:30:11.56…	Apple_98:18:70	Cimsys_33:44:a8	802.11	37	Action, SN=428, FN=0, Flags=.....[Malformed Packet]

Current AP

FT handshake packets

Target AP

Packets

- **The interval between the two packets is 1.279 sec.**

The last packet of the current AP

```
10622 17:30:11.162000    Elecom_e8:f6:73    Apple_98:18:70    802.11    234 QoS Data, SN=1837, FN=0, Flags=.p..R.F.

Frame 10622: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)
IEEE 802.11 QoS Data, Flags: .p..R.F.
  Type/Subtype: QoS Data (0x0028)
  ▷ Frame Control Field: 0x884a
  .000 0000 0011 1100 = Duration: 60 microseconds
  Receiver address: Apple_98:18:70 (74:b5:87:98:18:70)
  Transmitter address: Cimsys_33:44:90 (00:11:22:33:44:90)
  Destination address: Apple_98:18:70 (74:b5:87:98:18:70)
  Source address: Elecom_e8:f6:73 (bc:5c:4c:e8:f6:73)
  BSS Id: Cimsys_33:44:90 (00:11:22:33:44:90)
  STA address: Apple_98:18:70 (74:b5:87:98:18:70)
```

The first packet of the target AP

```
10744 17:30:12.441104    Elecom_e8:f6:73    Apple_98:18:70    802.11    82 QoS Data, SN=44, FN=0, Flags=.p.

Frame 10744: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
IEEE 802.11 QoS Data, Flags: .p....F.
  Type/Subtype: QoS Data (0x0028)
  ▷ Frame Control Field: 0x8842
  .000 0000 0011 1100 = Duration: 60 microseconds
  Receiver address: Apple_98:18:70 (74:b5:87:98:18:70)
  Transmitter address: Cimsys_33:44:a8 (00:11:22:33:44:a8)
  Destination address: Apple_98:18:70 (74:b5:87:98:18:70)
  Source address: Elecom_e8:f6:73 (bc:5c:4c:e8:f6:73)
  BSS Id: Cimsys_33:44:a8 (00:11:22:33:44:a8)
  STA address: Apple_98:18:70 (74:b5:87:98:18:70)
```

Roaming record

- iPhone ping 192.168.1.1 (Controller) continuously to check
- The Roaming record shows that the iPhone occurs roaming from 00:11:22:33:44:90 to 00:11:22:33:44:a8

```
【发生漫游】
漫游前:00:11:22:33:44:90
漫游后:00:11:22:33:44:a8
漫游切换间隔: 0ms
64 bytes from 192.168.1.1: icmp_seq=22 ttl=64
time=7.000ms
64 bytes from 192.168.1.1: icmp_seq=23 ttl=64
time=5.000ms
64 bytes from 192.168.1.1: icmp_seq=24 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=25 ttl=64
time=6.000ms
64 bytes from 192.168.1.1: icmp_seq=26 ttl=64
time=5.000ms
64 bytes from 192.168.1.1: icmp_seq=27 ttl=64
time=10.000ms
64 bytes from 192.168.1.1: icmp_seq=28 ttl=64
time=5.000ms
64 bytes from 192.168.1.1: icmp_seq=29 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=30 ttl=64
time=5.000ms
```

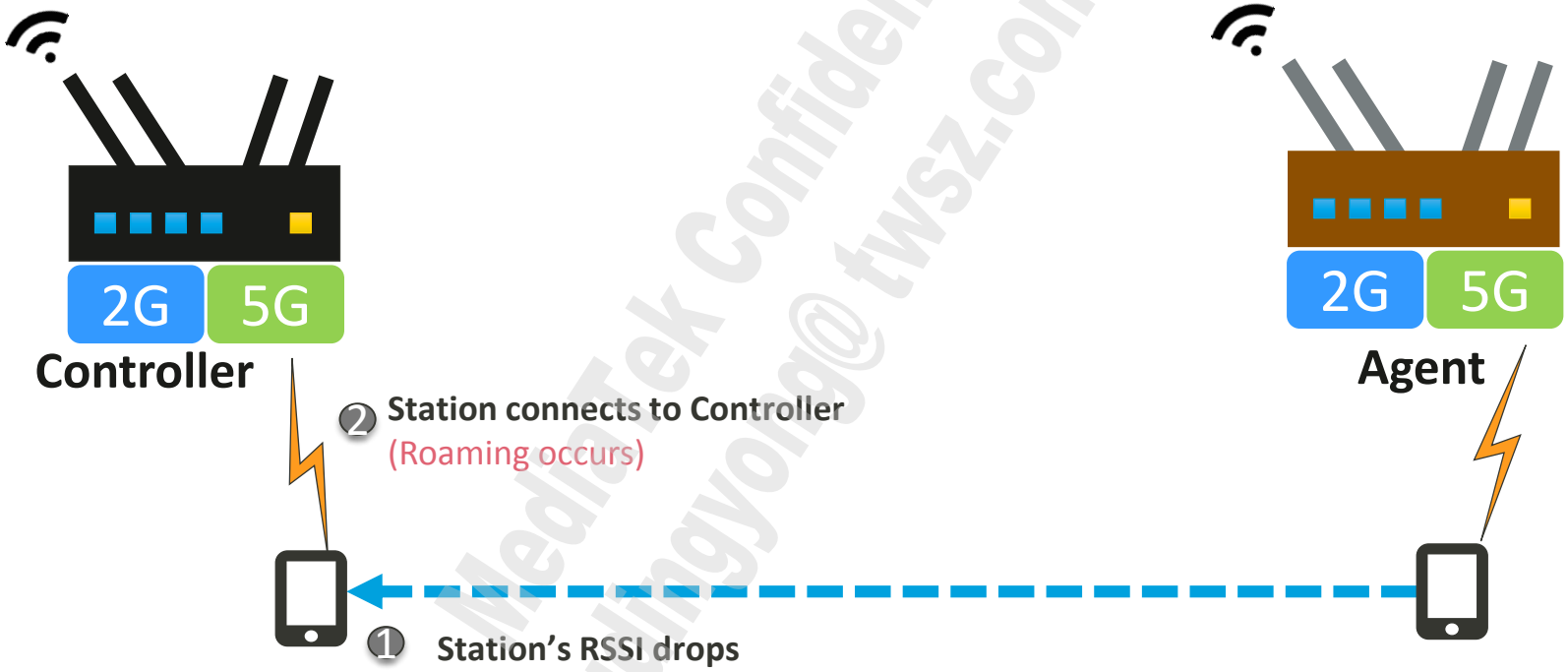
Controller Agent

WiFi魔盒

Scenario 2

- Scenario 2
  - After iPhone XR roams to Agent, we move it from Agent to Controller.
- Result: The Agent will send BTM request first, then the sniffer log shows that iPhone accept this request. But, iPhone still send the FT packets to target AP.

Scenario 2



Packets

- **The Agent will send BTM request first, then the sniffer log shows that iPhone accept this request.**
  But, iPhone still send the FT packets to target AP

iPhone Accept BTM steering

```
▷ Frame 2715: 39 bytes on wire (312 bits), 39 bytes captured (312 bits)
▷ IEEE 802.11 Action, Flags: ...P....
◢ IEEE 802.11 wireless LAN
  ◢ Fixed parameters
      Category code: WNM (10)
      Action code: BSS Transition Management Response (8)
      Dialog token: 0x01
      BSS Transition Status Code: 0
      BSS Termination Delay: 0
      BSS Transition Target BSS: Cimsys_33:44:90 (00:11:22:33:44:90)
      BSS Transition Candidate List Entries: 802eb627
  ▷ Tag: Agere Proprietary
```

2616	19:46:04.652556	Cimsys_33:44:a8	Apple_98:18:70	802.11	82	Action, SN=24, FN=0, Flags=.....[Malformed Packet]
2622	19:46:04.747150	Apple_98:18:70	Cimsys_33:44:a8	802.11	122	Action, SN=1940, FN=0, Flags=....., SSID=Wildcard (Broadcast)[Malformed Pac
2627	19:46:04.958039	Cimsys_33:44:a8	Apple_98:18:70	802.11	54	BSS Transition Management Request[Malformed Packet]
2715	19:46:07.732791	Apple_98:18:70	Cimsys_33:44:a8	802.11	39	BSS Transition Management Response
2718	19:46:07.734206	Apple_98:18:70	Cimsys_33:44:a8	802.11	197	Action, SN=2012, FN=0, Flags=.....[Malformed Packet]
2724	19:46:08.047075	Apple_98:18:70	Cimsys_33:44:90	802.11	213	Authentication, SN=2013, FN=0, Flags=.....[Packet size limited during capt
2725	19:46:08.049558	Cimsys_33:44:90	Apple_98:18:70	802.11	201	Authentication, SN=0, FN=0, Flags=.....[Malformed Packet]
2726	19:46:08.051011	Apple_98:18:70	Cimsys_33:44:90	802.11	342	Reassociation Request, SN=2014, FN=0, Flags=....., SSID=Miga-Multi-AP-5LG-
2730	19:46:08.135258	Cimsys_33:44:90	Apple_98:18:70	802.11	477	Reassociation Response, SN=1, FN=0, Flags=.....[Packet size limited during
2731	19:46:08.138229	Apple_98:18:70	Cimsys_33:44:90	802.11	52	Action, SN=2015, FN=0, Flags=....., SSID=Miga-Multi-AP-5LG-1[Packet size li
2732	19:46:08.141569	Cimsys_33:44:a8	Apple_98:18:70	802.11	34	Action, SN=32, FN=0, Flags=.....[Malformed Packet]
2733	19:46:08.141765	Apple_98:18:70	Cimsys_33:44:a8	802.11	30	Deauthentication, SN=2016, FN=0, Flags=.....[Packet size limited during cap
2734	19:46:08.142335	Cimsys_33:44:a8	Apple_98:18:70	802.11	34	Action, SN=33, FN=0, Flags=.....[Packet size limited during capture]
2735	19:46:08.142509	Cimsys_33:44:a8	Apple_98:18:70	802.11	34	Action, SN=34, FN=0, Flags=.....[Malformed Packet]
2736	19:46:08.142639	Cimsys_33:44:a8	Apple_98:18:70	802.11	34	Action, SN=35, FN=0, Flags=.....[Malformed Packet]
2737	19:46:08.143341	Apple_98:18:70	Cimsys_33:44:a8	802.11	30	Deauthentication, SN=2017, FN=0, Flags=.....[Malformed Packet]
2738	19:46:08.143454	Apple_98:18:70	Cimsys_33:44:a8	802.11	30	Deauthentication, SN=2018, FN=0, Flags=.....[Packet size limited during cap
2739	19:46:08.143594	Apple_98:18:70	Cimsys_33:44:a8	802.11	30	Deauthentication, SN=2019, FN=0, Flags=.....[Malformed Packet]
2741	19:46:08.160827	Apple_98:18:70	Cimsys_33:44:90	802.11	37	Action, SN=2020, FN=0, Flags=.....[Malformed Packet]
2743	19:46:08.163496	Cimsys_33:44:90	Apple_98:18:70	802.11	31	Action, SN=2, FN=0, Flags=.....[Malformed Packet]
2744	19:46:08.163631	Cimsys_33:44:90	Apple_98:18:70	802.11	37	Action, SN=3, FN=0, Flags=.....[Malformed Packet]
2745	19:46:08.163866	Apple_98:18:70	Cimsys_33:44:90	802.11	37	Action, SN=2021, FN=0, Flags=.....[Malformed Packet]

BTM steering

FT packets

Target AP

Packets

- The interval between the two packets is **0.15 sec**.

The last packet of the current AP

```
18109 17:30:47.300561    Elecom_df:e0:67    Apple_98:18:70    802.11    158 QoS Data, SN=1837, FN=0, Flags=.p..R.F.

Frame 18109: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)
IEEE 802.11 QoS Data, Flags: .p..R.F.
    Type/Subtype: QoS Data (0x0028)
    Frame Control Field: 0x884a
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: Apple_98:18:70 (74:b5:87:98:18:70)
    Transmitter address: Cimsys_33:44:a8 (00:11:22:33:44:a8)
    Destination address: Apple_98:18:70 (74:b5:87:98:18:70)
    Source address: Elecom_df:e0:67 (bc:5c:4c:df:e0:67)
    BSS Id: Cimsys_33:44:a8 (00:11:22:33:44:a8)
```

The first packet of the target AP

```
18121 17:30:47.450826    Elecom_e8:f6:73    Apple_98:18:70    802.11    1414 QoS Data, SN=0, FN=0, Flags=.p....F.

Frame 18121: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits)
IEEE 802.11 QoS Data, Flags: .p....F.
    Type/Subtype: QoS Data (0x0028)
    Frame Control Field: 0x8842
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Apple_98:18:70 (74:b5:87:98:18:70)
    Transmitter address: Cimsys_33:44:90 (00:11:22:33:44:90)
    Destination address: Apple_98:18:70 (74:b5:87:98:18:70)
    Source address: Elecom_e8:f6:73 (bc:5c:4c:e8:f6:73)
    BSS Id: Cimsys_33:44:90 (00:11:22:33:44:90)
    STA address: Apple_98:18:70 (74:b5:87:98:18:70)
```

Roaming record

- iPhone ping 192.168.1.1 (Controller) continuously to check.
- The Roaming record shows that the iPhone occurs roaming from 00:11:22:33:44:a8 to 00:11:22:33:44:90.

```
64 bytes from 192.168.1.1: icmp_seq=53 ttl=64
time=80.000ms
64 bytes from 192.168.1.1: icmp_seq=54 ttl=64
time=126.000ms

【发生漫游】
漫游前:00:11:22:33:44:a8
漫游后:00:11:22:33:44:90
漫游切换间隔: 0ms
TIMEOUT x1
64 bytes from 192.168.1.1: icmp_seq=56 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=57 ttl=64
time=5.000ms
64 bytes from 192.168.1.1: icmp_seq=58 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=59 ttl=64
time=5.000ms
```

Agent

Controller

TIMEOUT occurs

WiFi魔盒

Conclusion

- **The following pictures are the result of the scenario1 and scenario2. It shows that it only 1 packet lost.**

```
【发生漫游】
漫游前:00:11:22:33:44:90
漫游后:00:11:22:33:44:a8
漫游切换间隔: 0ms
64 bytes from 192.168.1.1: icmp_seq=22 ttl=64
time=7.000ms
64 bytes from 192.168.1.1: icmp_seq=23 ttl=64
time=5.000ms
64 bytes from 192.168.1.1: icmp_seq=24 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=25 ttl=64
time=6.000ms
64 bytes from 192.168.1.1: icmp_seq=26 ttl=64
time=5.000ms
64 bytes from 192.168.1.1: icmp_seq=27 ttl=64
time=10.000ms
64 bytes from 192.168.1.1: icmp_seq=28 ttl=64
time=5.000ms
64 bytes from 192.168.1.1: icmp_seq=29 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=30 ttl=64
time=5.000ms
```

Controller
Agent

From Controller to Agent.

```
64 bytes from 192.168.1.1: icmp_seq=53 ttl=64
time=80.000ms
64 bytes from 192.168.1.1: icmp_seq=54 ttl=64
time=126.000ms

【发生漫游】
漫游前:00:11:22:33:44:a8
漫游后:00:11:22:33:44:90
漫游切换间隔: 0ms
TIMEOUT x1
64 bytes from 192.168.1.1: icmp_seq=56 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=57 ttl=64
time=5.000ms
64 bytes from 192.168.1.1: icmp_seq=58 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=59 ttl=64
time=5.000ms
```

Agent
Controller
TIMEOUT occurs

From Agent to Controller.

```
time=3.000ms
64 bytes from 192.168.1.1: icmp_seq=72 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=73 ttl=64
time=3.000ms
64 bytes from 192.168.1.1: icmp_seq=74 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=75 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=76 ttl=64
time=4.000ms
64 bytes from 192.168.1.1: icmp_seq=77 ttl=64
time=3.000ms
--- 192.168.1.1 ping statistics ---
77 packets transmitted, 76 packets received, 1%
packet loss
round-trip min/avg/max/ = 3.000/12.179/319.000 ms
成功!
```

802.11r
Test Without EasyMesh

How-To

- **Configure "FtSupport=1" in profile to enable FT function**

```
(7615D)
# nvram_set 2860 FtSupport "1;1;1;1"
# nvram_set rtdev FtSupport "1;1;1;1"
# nvram_set 2860 FtOtd "1;1;1;1"        //Optional
# nvram_set rtdev FtOtd "1;1;1;1"       //Optional
# reboot
```

- **Configure the SSID, Security Mode and Pre-Shared Key**
  Note: DUT1 and DUT2 use the same wireless setting

- **DUT1 and DUT2 are connected via Ethernet**

- **Enable the FT daemon by either executing command**

```
# wapp –d1 –c ra0
```

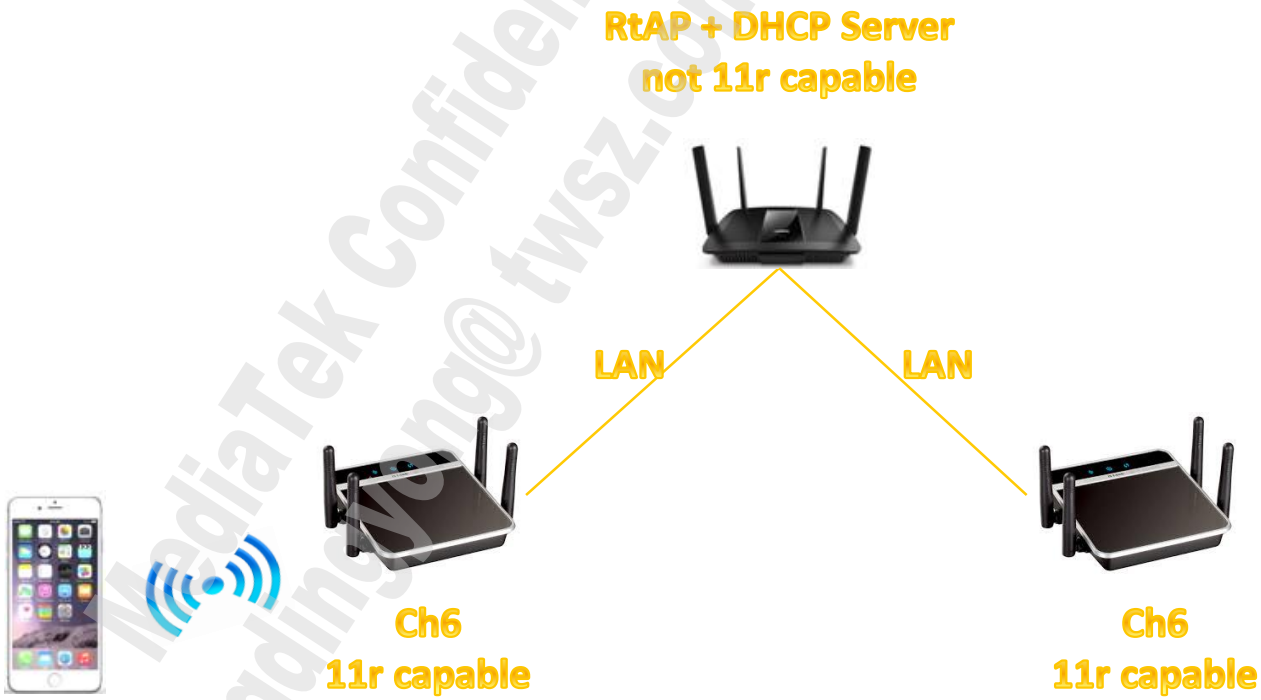
Note: If Dual Band is adopted, you have to specify both interfaces

```
# wapp –d1 –c ra0 –c rax0
```

- **Then, iPhone connects to DUT1. And move iPhone between DUT1 and DUT2** ***(You can refer to p27 or p33)***

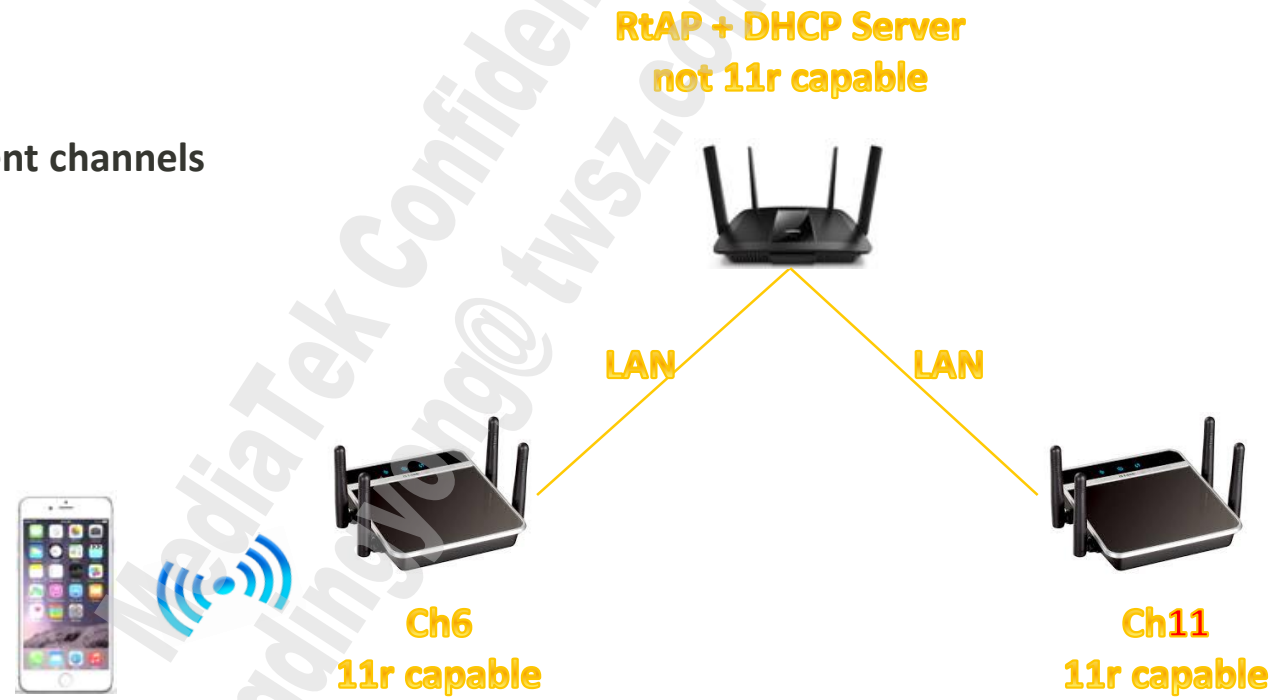
APs + RootAP Scenario (1)

- 11r protocol: OTA
- Client: iPhone



APs + RootAP Scenario (2)

- 11r protocol: OTA
- Client: iPhone
- DUTs are in different channels



APs + RootAP Scenario (3)

- 11r protocol: OTA
- Client: iPhone
- DS is WiFi instead of Ethernet

802.11r
Frame format

Auth Algorithm Definition

Authentication algorithm	Authentication transaction sequence no.	Status code	Presence of fields 4-15
Open System	1	Reserved	Not present
Open System	2	Status	Not present
Shared Key	1	Reserved	Not present
Shared Key	2	Status	The Challenge text element is present
Shared Key	3	Reserved	The Challenge text element is present
Shared Key	4	Status	Not present
FT	1	Reserved	The Mobility Domain element is present. The Fast BSS Transition and RSNEs are present if dot11RSNAActivated is true.
FT	2	Status	The Mobility Domain element is present if Status is 0. The Fast BSS Transition and RSNEs are present if Status is 0 and dot11RSNAActivated is true.
FT	3	Reserved	The Mobility Domain element is present. The Fast BSS Transition and RSNEs are present if dot11RSNAActivated is true. The RIC element is optionally present.
FT	4	Status	The Mobility Domain element is present if Status is 0. The Fast BSS Transition and RSNEs are present if dot11RSNAActivated is true. The RIC element is optionally present if Status is 0. The TIE (reassociation deadline) is present if a RIC element is present.

Element ID

- **IEs added in 802.11r**

Information Element	Element ID	Length (in octets)
Mobility Domain (MDIE)	54	5
Fast BSS Transition (FTIE)	55	84 ~ 257
Timeout Interval	56	7
RIC Data (RDIE)	57	6
RIC Descriptor	75	3 ~ 257

FT-related IEs

- **Mobility Domain**
  - FT attribute and capability advertisement
- **FT**
  - FT key material exchange
- **RSN**
  - A common IE for security capability advertisement
  - AKM suite and PMKID announcement for FT

Mobility Domain Element

- **MD IE format**

	Element ID	Length	MDID	FT Capability and Policy
Octets:	1	1	2	1

	B0	B1	B2	B7
	Fast BSS Transition over DS	Resource Request Protocol Capability	Reserved	
Bits:	1	1	6	

MDID: MTK default Mobility Domain ID is *"RT"*

Fast BSS Transition Element

- **FT IE format**

	Element ID	Length	MIC Control	MIC	ANonce	SNonce	Optional Parameter(s)
Octets:	1	1	2	16	32	32	variable

	Subelement ID	Length	Data
Octets:	1	1	variable

FT Subelement

- **Subelement ID**

Value	Contents of Data field	Length (in octets)
0	Reserved	
1	PMK-R1 key holder identifier (R1KH-ID)	6
2	GTK subelement	35–51
3	PMK-R0 key holder identifier (R0KH-ID)	1–48
4	IGTK	Variable
5–255	Reserved	

MEDIATEK

everyday genius