AN14212

802.11kvr Roaming

Rev. 3.0 — 12 May 2025

Application note

Document information

Information	Content
Keywords	802.11kvr, roaming, bgscan, wpa_supplicant, fast transition, resource management, basic service set transition management, neighbor report, beacon report, wireless network management
Abstract	Explains how to enable fast transition, configure wpa_supplicant, load the driver parameters. And describes different types of fast transition.

1 Introduction

NXP Wi-Fi radios support 802.11kvr roaming standards:

- **802.11k (Radio Resource Measurement):** provides information about the available APs and respective RSSI to help the client choose the best AP.
- **802.11v (Wireless Network Management):** provides information to the client about available APs for roaming, without a full scan.
- **802.11r (Fast Basic Service Set Transition):** eliminates the need for fresh authentication when a client roams to another network.

This document explains how to use 802.11kvr for roaming.

Note: *802.11kvr is supported only in STA mode. Mobile AP mode does not support 802.11k, 802.11v, and 802.11r standards.*

1.1 Supported devices

Refer to the feature list in the release note to check if 802.11kvr is supported in the software release package. The wireless SoCs that support 802.11kvr are:

- 88W8987 ref.[5]
- 88W8997 ref.[6]
- 88Q9098 ref.[7]
- 88W9098 ref.[8]
- AW611 ref.[9]
- AW690 ref.[10]
- AW692 ref.[11]
- AW693 ref.[12]
- IW416 ref.[13]
- IW610 ref.[15]
- IW611 ref.[14]
- IW612 ref.[16]
- IW620 ref.[17]

1.2 Prerequisites

- Open source wpa_supplicant v2.10 or higher ref.[18]
- Open source kernel v4.6 or higher

2 802.11kvr

Figure 1 shows the interaction between 802.11k, 802.11v, and 802.11r for roaming.

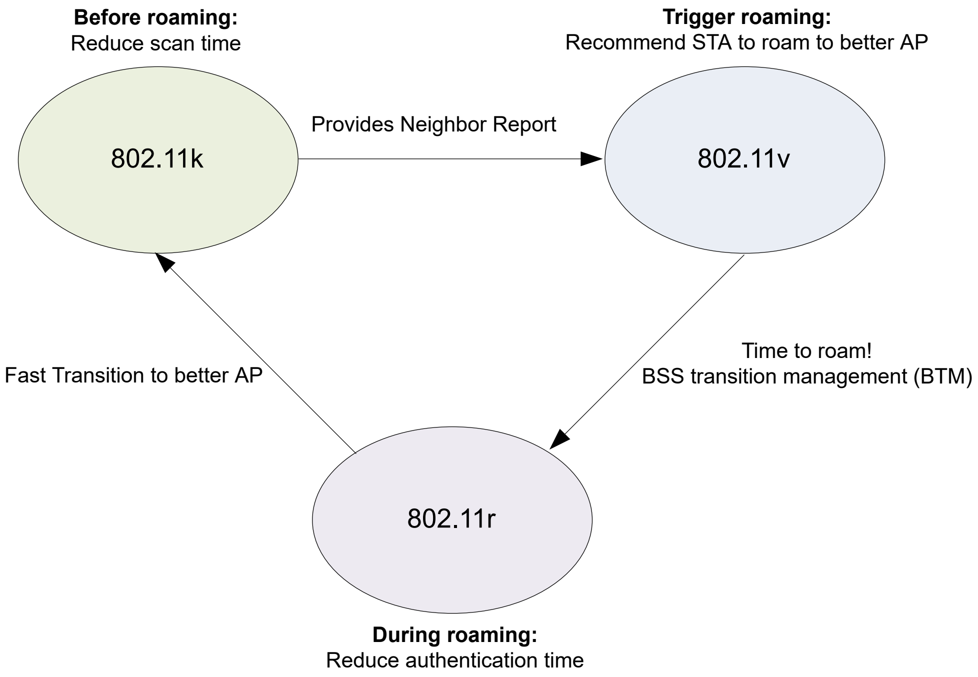


Figure 1. Overview of 802.11kvr

802.11k is a Radio Resource Management (RRM) that provides mechanisms for APs and clients to dynamically measure the available radio resources. APs and clients can send neighbor reports, beacon reports, and link measurement reports to each other.

- Neighbor reports: information about known neighbor APs to help STA better understand its surroundings
- Beacon reports: information about channel configuration, location, coverage/frequency planning, and AP detection
- Link measurement reports: information about a requested link

802.11v is BSS transition management (BTM) with Wireless Network Management (WNM) that allows client devices to exchange information about the network topology. The information includes RF environment, making each client network aware of its surroundings. STA can send a BTM query to the AP and get a list of preferred candidates.

- BTM query: A connected AP suggests the STA to roam to another APs with a better connection with a preferred candidate list.

802.11r is Fast Basic Service Set Transition (FT), which is faster than normal roaming because it avoids a 4-way handshake when transitioning from one AP to another. The two types of FT are over-the-air and over-the-distribution-system (over-the-DS).

3 Configuration

This section explains how to configure 802.11kvr.

3.1 Driver load parameters

To enable 802.11kvr, load the driver with the parameters:

```
host_mlme=1
cfg80211_wext = 0xf (STA mask of CFG80211 and WEXT control)
```

Note: *For more details about the driver load parameters, refer to the README in the software release package.*

Example of driver loading:

```
insmod mlan.ko
insmod moal.ko fw_name=nxp/<fw_name>.bin cfg80211_wext=0xf auto_ds=2 ps_mode=2
 txpwrlimit_cfg=nxp/<power_table>.bin cal_data_cfg=nxp/WlanCalData.conf host_mlme=1
 drvdbg=0x20037
```

Note: *Setting `dvrdbg = 0x20037` is optional and used to log roaming messages on dmesg.*

3.2 wpa_supplicant

wpa_supplicant is the MAC Sublayer Management Entity (MLME) to send/receive RRM action frames, FT action frames, and BTM frames. Refer to */wpa_supplicant/README* for more information.

Note: *Open source wpa_supplicant version v.2.10 or above must be used. wpa_supplicant must be built with the flag, CONFIG_80211R enabled.*

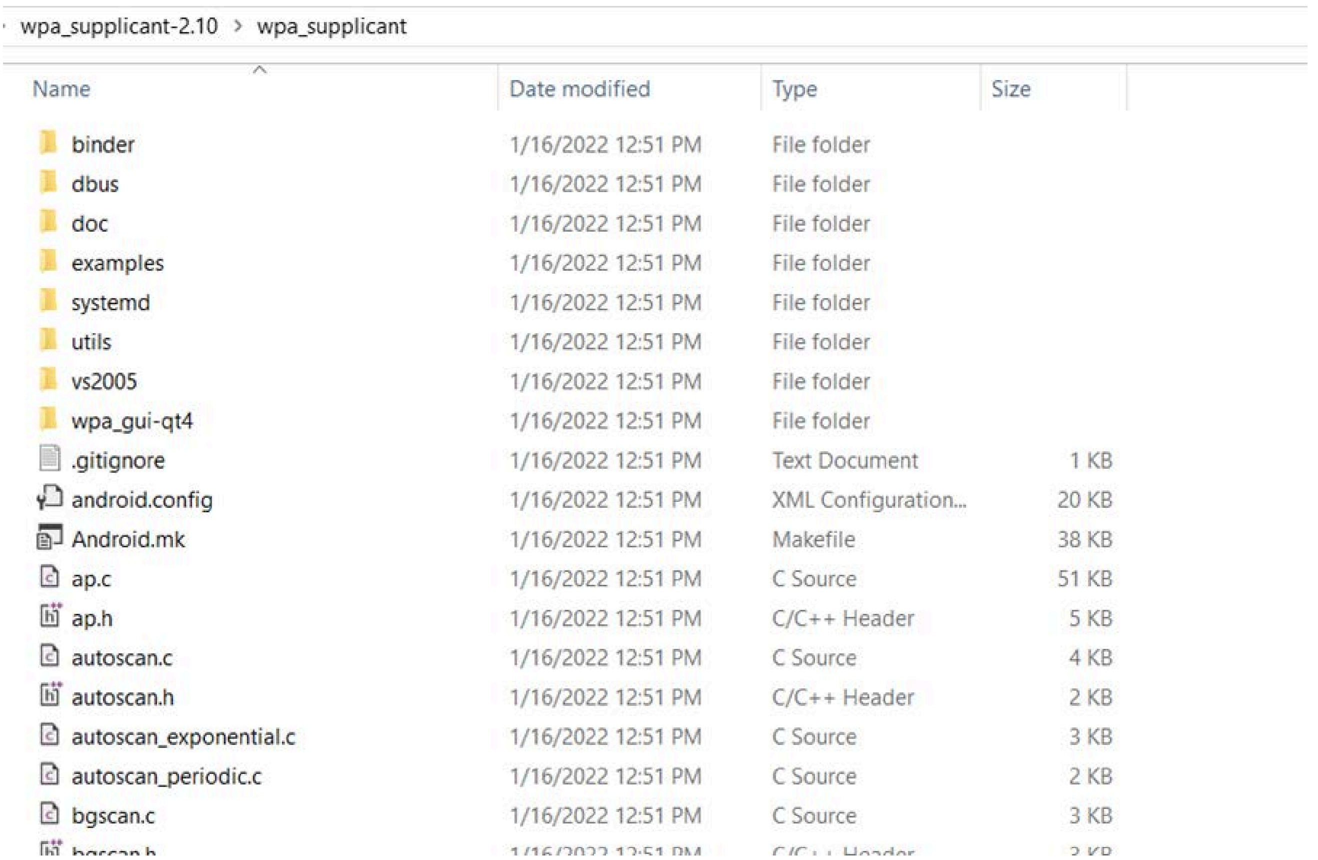
Step 1 – Download wpa_supplicant open source code (*wpa_supplicant-2.10.tar.gz*) (see ref.[18]).

Step 2 – Decompress the file.

```
tar -xvf wpa_supplicant-2.10.tar.gz
```

Step 3 – Move to the *wpa_supplicant* directory. See Figure 2.

```
cd wpa_supplicant
```



Name	Date modified	Type	Size
binder	1/16/2022 12:51 PM	File folder	
dbus	1/16/2022 12:51 PM	File folder	
doc	1/16/2022 12:51 PM	File folder	
examples	1/16/2022 12:51 PM	File folder	
systemd	1/16/2022 12:51 PM	File folder	
utils	1/16/2022 12:51 PM	File folder	
vs2005	1/16/2022 12:51 PM	File folder	
wpa_gui-qt4	1/16/2022 12:51 PM	File folder	
.gitignore	1/16/2022 12:51 PM	Text Document	1 KB
android.config	1/16/2022 12:51 PM	XML Configuration...	20 KB
Android.mk	1/16/2022 12:51 PM	Makefile	38 KB
ap.c	1/16/2022 12:51 PM	C Source	51 KB
ap.h	1/16/2022 12:51 PM	C/C++ Header	5 KB
autoscan.c	1/16/2022 12:51 PM	C Source	4 KB
autoscan.h	1/16/2022 12:51 PM	C/C++ Header	2 KB
autoscan_exponential.c	1/16/2022 12:51 PM	C Source	3 KB
autoscan_periodic.c	1/16/2022 12:51 PM	C Source	2 KB
bgscan.c	1/16/2022 12:51 PM	C Source	3 KB
bgscan.h	1/16/2022 12:51 PM	C/C++ Header	2 KB

Figure 2. wpa_supplicant directory content

Step 4 – Enable the IEE80211R flag in the *.config* file.

```
CONFIG_IEEE80211R=y
```

Step 5 – Build wpa_supplicant.

```
make
```

Example of output:

```
CC ../src/drivers/driver_nl80211.c
CC ../src/drivers/driver_nl80211_capa.c
CC ../src/drivers/driver_nl80211_event.c
CC ../src/drivers/driver_nl80211_monitor.c
…
```

Step 6 – Create the configuration file *wpa_supplicant.conf*.

Example of *wpa_supplicant.conf* content:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
update_config=1
ap_scan=1
network={
 ssid="TEST_NETWORK"
 key_mgmt=FT-PSK                     # Fast Transition Key Management
 proto=RSN
 pairwise=CCMP
 group=CCMP
 psk="1234567890"
 bgscan="simple:30:-75:120"        # Background scan settings
}
```

- Set the key management to FT-PSK or FT-EAP.

```
key_mgmt=FT-PSK
key_mgmt=FT-EAP
```

- Set the background scanning parameters.

```
bgscan=”simple :<short scan interval> : <signal strength threshold> : <long scan
 interval>”
```

Where:

Table 1. Command parameters

Parameter	Description
`short scan interval`	Perform a scan every X seconds when the signal strength is weaker than the threshold
`signal strength threshold`	Signal strength from AP (dBm)
`long scan interval`	Perform a scan every X seconds when the signal strength is higher than the threshold

Example of command:

```
bgscan="simple:30:-75:120"
```

In the example, a scan is performed every 30 seconds when the signal strength from the current AP is below -75dBm. If the signal strength is above -75dBm, the interval is every 120 seconds.

Step 7 – Run `wpa_supplicant`.

```
wpa_supplicant -B  -Dnl80211 -<interface> -c/etc/wpa_supplicant.conf
```

4 wpa_cli

Once 802.11kvr is enabled, wpa_supplicant automatically handles roaming. The command line interface wpa_cli is used to interact with wpa_supplicant and trigger the following actions:

- Neighbor report
- BTM query
- Over-the-Air Fast Transition
- Over-the-DS Fast Transition

5 Setup

The setup to demonstrate 802.11kvr consists of:

- Enterprise Wireless LAN controller
- at least two APs
- at least one STA

Note: *Refer to the user manual of your Enterprise controller and APs to enable 802.11kvr.*

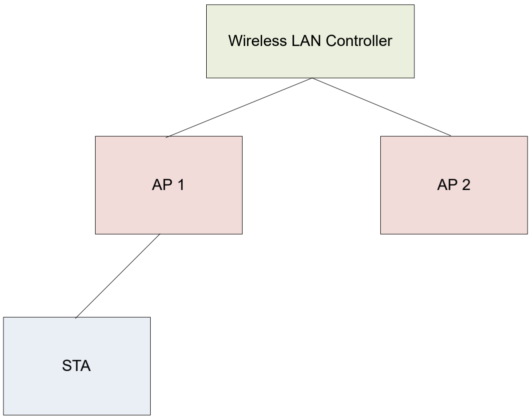
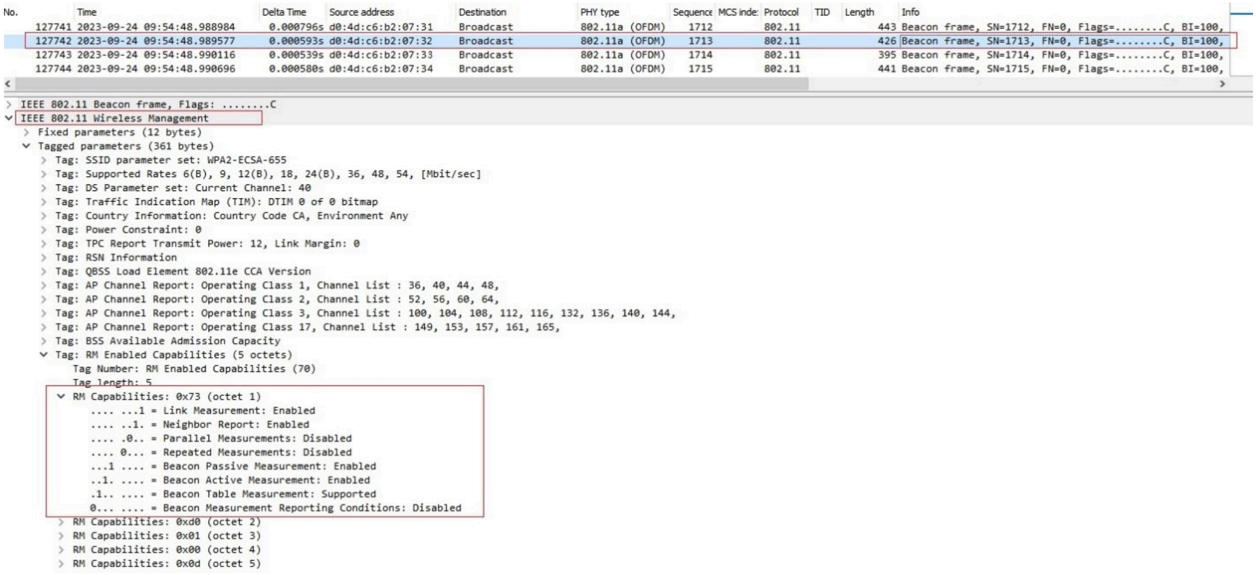


Figure 3. 802.11kvr set up example

Step 1 – Connect the APs to the Wireless LAN controller.

Figure 4 shows the AP enabled with 802.11kvr.

- AP MAC= d0:4d:c6:b2:07:32
- 802.11kvr (Link measurement and Neighbor report) is enabled in the AP.



```
No.     Time                        Delta Time Source address       Destination  PHY type       Sequence MCS inde: Protocol TID Length Info
 127741 2023-09-24 09:54:48.988984  0.000796s d0:4d:c6:b2:07:31  Broadcast    802.11a (OFDM)  1712             802.11          443 Beacon frame, SN=1712, FN=0, Flags=........C, BI=100,
 127742 2023-09-24 09:54:48.989577  0.000593s d0:4d:c6:b2:07:32  Broadcast    802.11a (OFDM)  1713             802.11          426 Beacon frame, SN=1713, FN=0, Flags=........C, BI=100,
 127743 2023-09-24 09:54:48.990116  0.000539s d0:4d:c6:b2:07:33  Broadcast    802.11a (OFDM)  1714             802.11          395 Beacon frame, SN=1714, FN=0, Flags=........C, BI=100,
 127744 2023-09-24 09:54:48.990696  0.000580s d0:4d:c6:b2:07:34  Broadcast    802.11a (OFDM)  1715             802.11          441 Beacon frame, SN=1715, FN=0, Flags=........C, BI=100,
```

```
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (361 bytes)
    > Tag: SSID parameter set: WPA2-ECSA-655
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 40
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    > Tag: Country Information: Country Code CA, Environment Any
    > Tag: Power Constraint: 0
    > Tag: TPC Report Transmit Power: 12, Link Margin: 0
    > Tag: RSN Information
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: AP Channel Report: Operating Class 1, Channel List : 36, 40, 44, 48,
    > Tag: AP Channel Report: Operating Class 2, Channel List : 52, 56, 60, 64,
    > Tag: AP Channel Report: Operating Class 3, Channel List : 100, 104, 108, 112, 116, 132, 136, 140, 144,
    > Tag: AP Channel Report: Operating Class 17, Channel List : 149, 153, 157, 161, 165,
    > Tag: BSS Available Admission Capacity
    v Tag: RM Enabled Capabilities (5 octets)
        Tag Number: RM Enabled Capabilities (70)
        Tag length: 5
      v RM Capabilities: 0x73 (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
          0... .... = Beacon Measurement Reporting Conditions: Disabled
      > RM Capabilities: 0xd0 (octet 2)
      > RM Capabilities: 0x01 (octet 3)
      > RM Capabilities: 0x00 (octet 4)
      > RM Capabilities: 0x0d (octet 5)
```

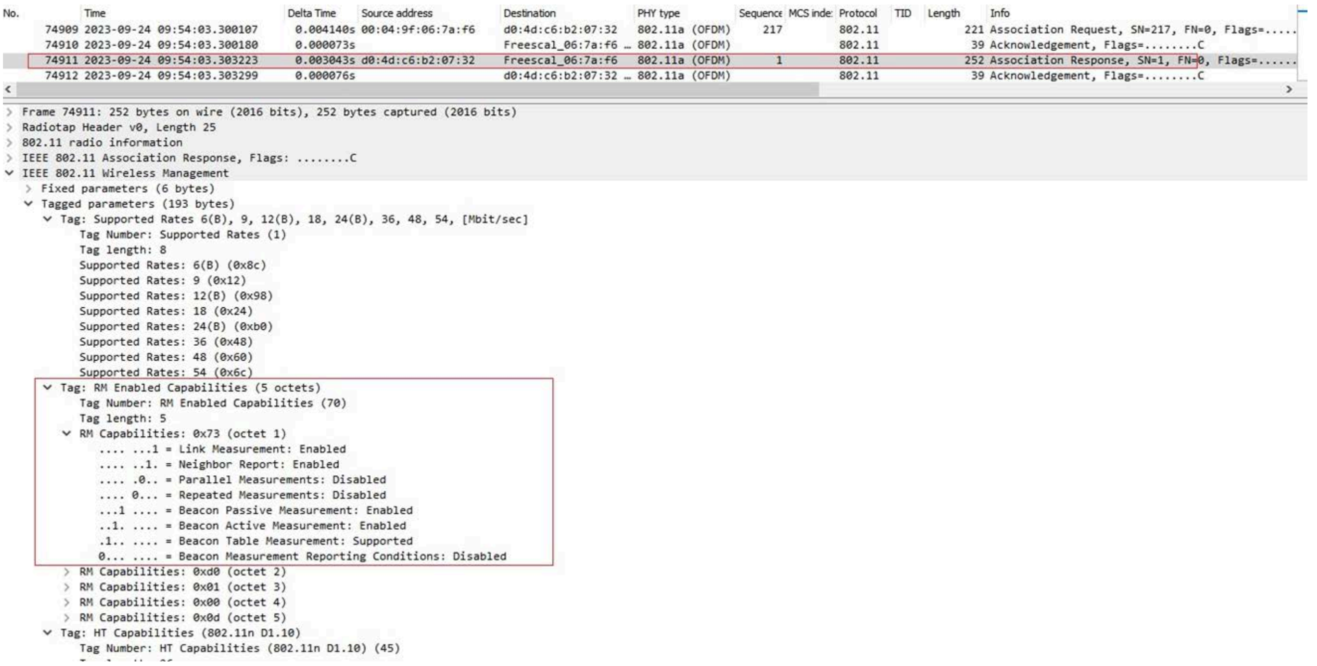
Figure 4. Example of AP enabled with 802.11kvr

Step 2 – Bring up the DUT in STA mode and define the configuration (Section 3).

Step 3 – Connect the STA to the AP.

Figure 5 shows the STA enabled with 802.11kvr.

- AP MAC= d0:4d:c6:b2:07:32
- STA MAC= 00:04:9f:06:7a:f6
- STA and AP exchange association request and responses.
- 802.11kvr (Link measurement and Neighbor report) is enabled in the Wi-Fi environment.



```
No.         Time                         Delta Time Source address    Destination         PHY type       Sequence MCS inde: Protocol TID Length Info
      74909 2023-09-24 09:54:03.300107   0.004140s 00:04:9f:06:7a:f6 d0:4d:c6:b2:07:32   802.11a (OFDM)   217             802.11          221 Association Request, SN=217, FN=0, Flags=.....
      74910 2023-09-24 09:54:03.300180   0.000073s                   Freescal_06:7a:f6 … 802.11a (OFDM)                   802.11           39 Acknowledgement, Flags=........C
      74911 2023-09-24 09:54:03.303223   0.003043s d0:4d:c6:b2:07:32 Freescal_06:7a:f6   802.11a (OFDM)     1             802.11          252 Association Response, SN=1, FN=0, Flags=......
      74912 2023-09-24 09:54:03.303299   0.000076s                   d0:4d:c6:b2:07:32 … 802.11a (OFDM)                   802.11           39 Acknowledgement, Flags=........C

> Frame 74911: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (6 bytes)
  v Tagged parameters (193 bytes)
    v Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
        Tag Number: Supported Rates (1)
        Tag length: 8
        Supported Rates: 6(B) (0x8c)
        Supported Rates: 9 (0x12)
        Supported Rates: 12(B) (0x98)
        Supported Rates: 18 (0x24)
        Supported Rates: 24(B) (0xb0)
        Supported Rates: 36 (0x48)
        Supported Rates: 48 (0x60)
        Supported Rates: 54 (0x6c)
    v Tag: RM Enabled Capabilities (5 octets)
        Tag Number: RM Enabled Capabilities (70)
        Tag length: 5
      v RM Capabilities: 0x73 (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
          0... .... = Beacon Measurement Reporting Conditions: Disabled
      > RM Capabilities: 0xd0 (octet 2)
      > RM Capabilities: 0x01 (octet 3)
      > RM Capabilities: 0x00 (octet 4)
      > RM Capabilities: 0x0d (octet 5)
    v Tag: HT Capabilities (802.11n D1.10)
        Tag Number: HT Capabilities (802.11n D1.10) (45)
```

Figure 5. Example of STA enabled with 802.11kvr

6 802.11k examples

This section provides examples for Neighbor Report, Link measurement, and Beacon report.

6.1 Neighbor report

The example demonstrates a Neighbor report request from the STA. AP 1 responds with a list of neighboring APs on the same Wi-Fi network, including AP 2. If there are no other APs in the environment, the neighbor report is empty.

wpa_supplicant handles the Neighbor reports. A `wpa_cli` command (in step 2) can be used to manually request a neighbor report.

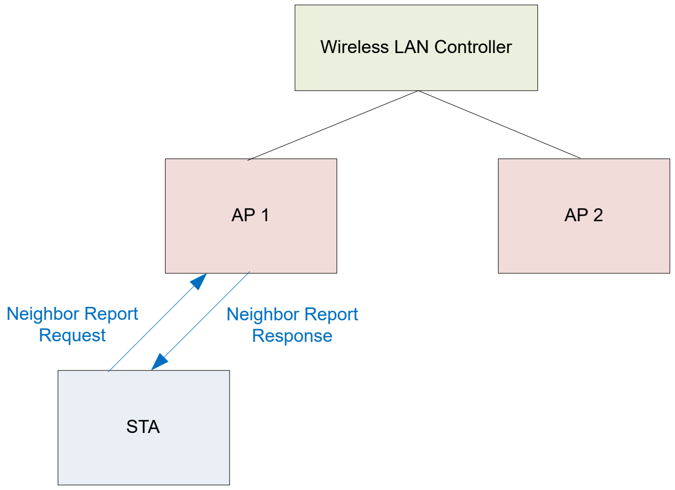


Figure 6. Setup for Neighbor report

Step 1 – Set up the environment (Section 5).

Step 2 – Run the `wpa_cli` command to trigger a Neighbor report request.

```
./wpa_cli neighbor_rep_request
```

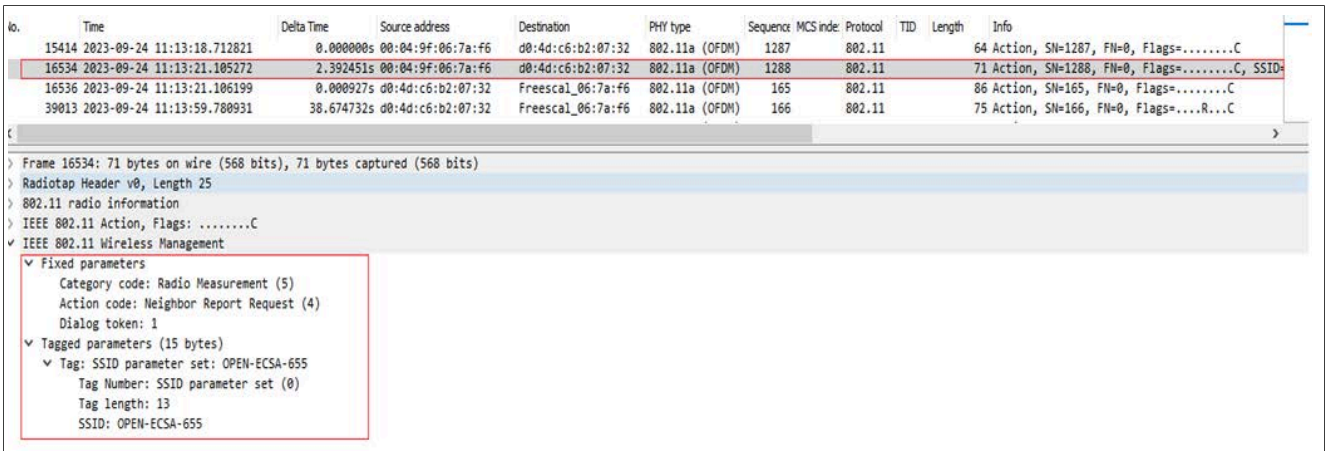
Command output example:

The log shows STA sending “RRM: Neighbor report request” to the AP.

```
RRM: Neighbor report request (for ), token=4
nl80211: Send Action frame (ifindex=3, freq=2422 MHz wait=0 ms no_cck=0 offchanok=1)
nl80211: Drv Event 60 (NL80211_CMD_FRAME_TX_STATUS) received for mlan0
nl80211: Frame TX status event A1=00:11:32:ed:9e:b0 stype=13 cookie=0xf6573dff ack=1
nl80211: Frame TX status: cookie=0xf6573dff (match) (ack=1)
mlan0: Event TX_STATUS (16) received
mlan0: EVENT_TX_STATUS dst=00:11:32:ed:9e:b0 type=0 stype=13
Off-channel: Ignore Action TX status - no pending operation
nl80211: BSS Event 59 (NL80211_CMD_FRAME) received for mlan0
nl80211: RX frame da=c0:95:da:00:e5:38 sa=00:11:32:ed:9e:b0 bssid=00:11:32:ed:9e:b0
 freq=2422 ssi_signal=0 fc=0xd0 seq_ctrl=0x60 stype=13 (WLAN_FC_STYPE_ACTION) len=27
mlan0: Event RX_MGMT (18) received
mlan0: Received Action frame: SA=00:11:32:ed:9e:b0 Category=5 DataLen=2 freq=2422 MHz
```

Figure 7 shows a sniffer capture example of the Neighbor Report Request from the STA to the AP.

- STA MAC= 00:04:9f:06:7a:f6
- AP MAC= d0:4d:c6:b2:07:32



No.	Time	Delta Time	Source address	Destination	PHY type	Sequence	MCS inde:	Protocol	TID	Length	Info
15414	2023-09-24 11:13:18.712821	0.000000s	00:04:9f:06:7a:f6	d0:4d:c6:b2:07:32	802.11a (OFDM)	1287		802.11		64	Action, SN=1287, FN=0, Flags=........C
16534	2023-09-24 11:13:21.105272	2.392451s	00:04:9f:06:7a:f6	d0:4d:c6:b2:07:32	802.11a (OFDM)	1288		802.11		71	Action, SN=1288, FN=0, Flags=........C, SSID=
16536	2023-09-24 11:13:21.106199	0.000927s	d0:4d:c6:b2:07:32	Freescal_06:7a:f6	802.11a (OFDM)	165		802.11		86	Action, SN=165, FN=0, Flags=........C
39013	2023-09-24 11:13:59.780931	38.674732s	d0:4d:c6:b2:07:32	Freescal_06:7a:f6	802.11a (OFDM)	166		802.11		75	Action, SN=166, FN=0, Flags=....R...C

```
> Frame 16534: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Neighbor Report Request (4)
      Dialog token: 1
  v Tagged parameters (15 bytes)
    v Tag: SSID parameter set: OPEN-ECSA-655
        Tag Number: SSID parameter set (0)
        Tag length: 13
        SSID: OPEN-ECSA-655
```

Figure 7. Example of Neighbor report request from STA to AP

Step 3 – Look for AP response (Neighbor report displayed on the console of the STA).

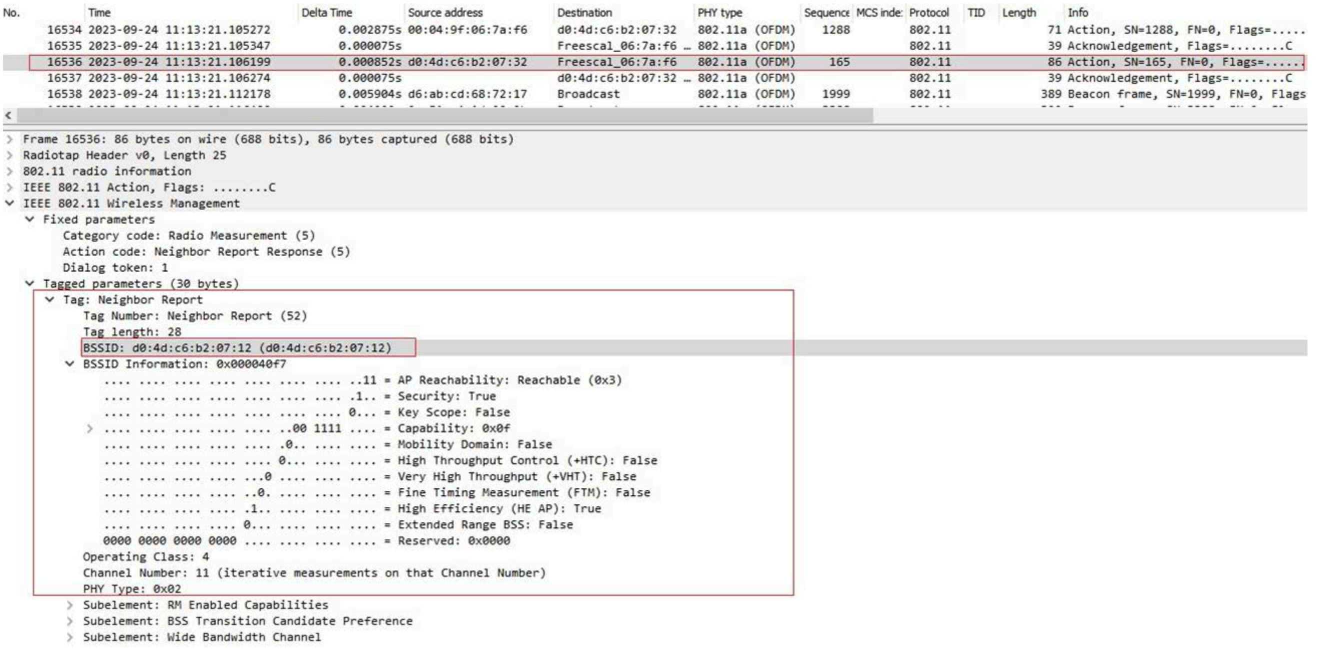
Command output example:

The log shows “RRM: New Neighbor Report”.

```
<3>CTRL-EVENT-SCAN-RESULTS
<3>RRM-NEIGHBOR-REP-RECEIVED bssid=dc:ce:c1:23:9a:4b info=0x2f7 op_class=115 chan=40
 phy_type=7
<3>RRM-NEIGHBOR-REP-RECEIVED bssid=dc:ce:c1:23:9a:44 info=0x2e7 op_class=81 chan=1
 phy_type=7
<3>CTRL-EVENT-SCAN-STARTED
<3>CTRL-EVENT-SCAN-RESULTS
…
RRM: New Neighbor Report - hexdump(len=31): 02 34 0d d0 4d c6 b2 07 32 f7 02 00 00 7d a1
 07 34 d0 4d c6 b2 07 12 e7 02 00 00 51 0b 07
mlan0: RRM: Notifying neighbor report (token = 2)
mlan0: RRM-NEIGHBOR-REP-RECEIVED bssid= d0:4d:c6:b2:07:32 info=0x2f7 op_class=125
 chan=161 phy_type=7
mlan0: RRM-NEIGHBOR-REP-RECEIVED bssid= d0:4d:c6:b2:07:12 info=0x2e7 op_class=81 chan=11
 phy_type=7
```

Figure 8 shows a sniffer capture example of Neighbor report response from the AP.

- AP MAC= d0:4d:c6:b2:07:32
- STA MAC= 00:04:9f:06:7a:f6



```
No.    Time                        Delta Time  Source address     Destination          PHY type        Sequence MCS inde: Protocol TID Length Info
 16534 2023-09-24 11:13:21.105272  0.002875s  00:04:9f:06:7a:f6  d0:4d:c6:b2:07:32    802.11a (OFDM)  1288               802.11         71 Action, SN=1288, FN=0, Flags=.....
 16535 2023-09-24 11:13:21.105347  0.000075s                     Freescal_06:7a:f6 …  802.11a (OFDM)                     802.11         39 Acknowledgement, Flags=........C
 16536 2023-09-24 11:13:21.106199  0.000852s  d0:4d:c6:b2:07:32  Freescal_06:7a:f6    802.11a (OFDM)   165               802.11         86 Action, SN=165, FN=0, Flags=.....
 16537 2023-09-24 11:13:21.106274  0.000075s                     d0:4d:c6:b2:07:32 …  802.11a (OFDM)                     802.11         39 Acknowledgement, Flags=........C
 16538 2023-09-24 11:13:21.112178  0.005904s  d6:ab:cd:68:72:17  Broadcast            802.11a (OFDM)  1999               802.11        389 Beacon frame, SN=1999, FN=0, Flags
```

```
> Frame 16536: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Neighbor Report Response (5)
      Dialog token: 1
  v Tagged parameters (30 bytes)
    v Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 28
        BSSID: d0:4d:c6:b2:07:12 (d0:4d:c6:b2:07:12)
      v BSSID Information: 0x000040f7
          .... .... .... .... .... .... .... ..11 = AP Reachability: Reachable (0x3)
          .... .... .... .... .... .... .... .1.. = Security: True
          .... .... .... .... .... .... .... 0... = Key Scope: False
        > .... .... .... .... .... ..00 1111 .... = Capability: 0x0f
          .... .... .... .... .... .0.. .... .... = Mobility Domain: False
          .... .... .... .... .... 0... .... .... = High Throughput Control (+HTC): False
          .... .... .... .... ...0 .... .... .... = Very High Throughput (+VHT): False
          .... .... .... .... ..0. .... .... .... = Fine Timing Measurement (FTM): False
          .... .... .... .... .1.. .... .... .... = High Efficiency (HE AP): True
          .... .... .... .... 0... .... .... .... = Extended Range BSS: False
          0000 0000 0000 0000 .... .... .... .... = Reserved: 0x0000
        Operating Class: 4
        Channel Number: 11 (iterative measurements on that Channel Number)
        PHY Type: 0x02
      > Subelement: RM Enabled Capabilities
      > Subelement: BSS Transition Candidate Preference
      > Subelement: Wide Bandwidth Channel
```

Figure 8. Neighbor report response from the AP

6.2 Link measurement

wpa_supplicant initiates link measurement requests and responses to and from the AP and STA. In this example, the STA sends a link measurement report to the AP.

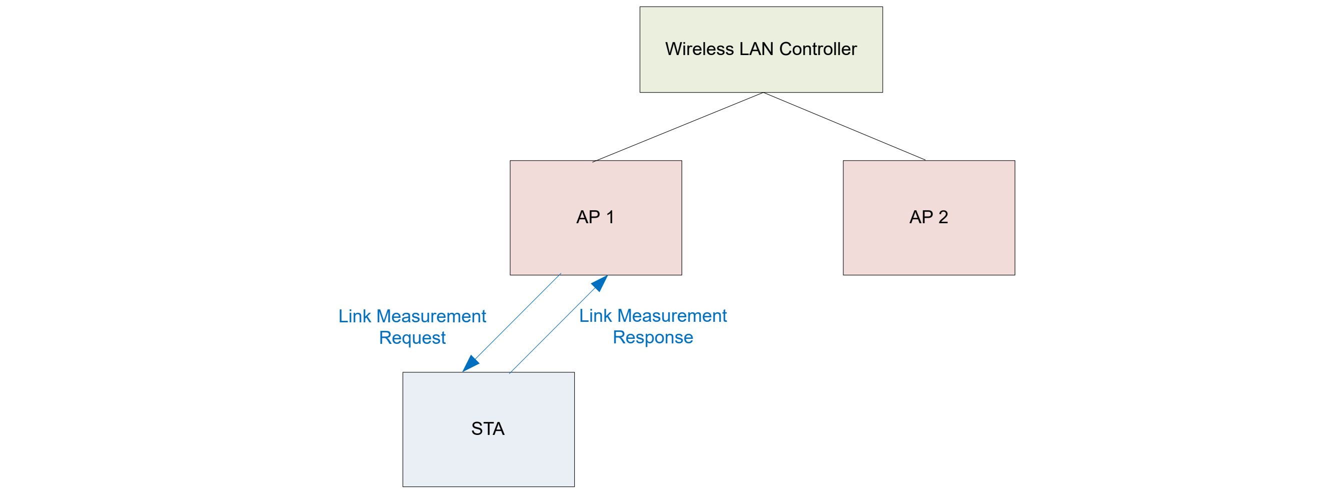


Figure 9. Link measurement setup

Step 1 – Set up the environment (Section 5).

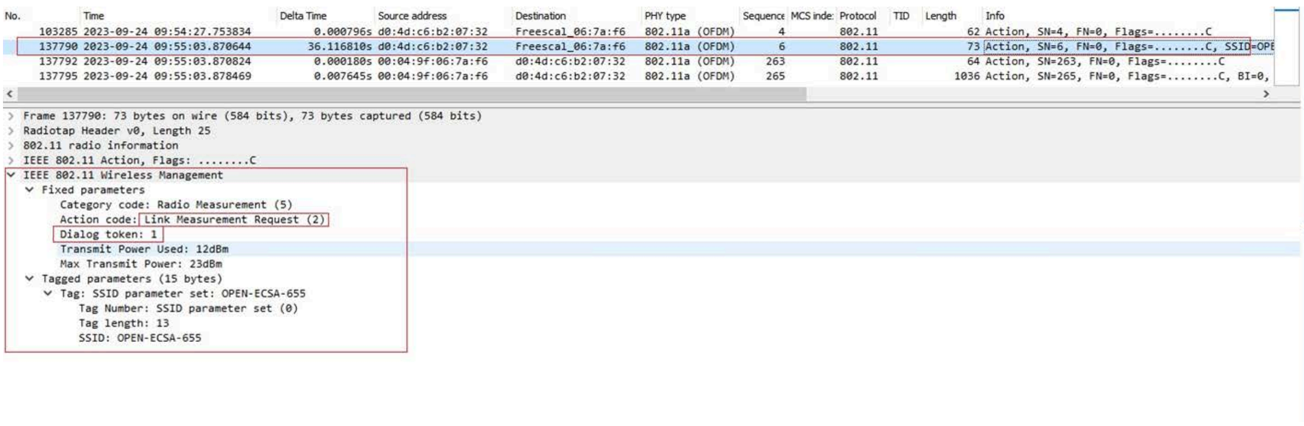
Step 2 – The AP sends a link measurement request to the STA. The request shows on the console of the STA.

Example of output:

```
mlan0: Received Action frame: SA=cc:88:c7:10:d7:11 Category=5 DataLen=31 freq=5805 MHz
Measurement request type 5 token 151
SSID subelement with zero length - wildcard SSID
```

Figure 10 shows an example of the STA receiving a link measurement request from the AP.

- AP MAC= d0:4d:c6:b2:07:32
- STA MAC= 00:04:9f:06:7a:f6



No.	Time	Delta Time	Source address	Destination	PHY type	Sequence	MCS inde:	Protocol	TID	Length	Info
103285	2023-09-24 09:54:27.753834	0.000796s	d0:4d:c6:b2:07:32	Freescal_06:7a:f6	802.11a (OFDM)	4		802.11		62	Action, SN=4, FN=0, Flags=........C
137790	2023-09-24 09:55:03.870644	36.116810s	d0:4d:c6:b2:07:32	Freescal_06:7a:f6	802.11a (OFDM)	6		802.11		73	Action, SN=6, FN=0, Flags=........C, SSID=OPE
137792	2023-09-24 09:55:03.870824	0.000180s	00:04:9f:06:7a:f6	d0:4d:c6:b2:07:32	802.11a (OFDM)	263		802.11		64	Action, SN=263, FN=0, Flags=........C
137795	2023-09-24 09:55:03.878469	0.007645s	00:04:9f:06:7a:f6	d0:4d:c6:b2:07:32	802.11a (OFDM)	265		802.11		1036	Action, SN=265, FN=0, Flags=........C, BI=0,

```
> Frame 137790: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Link Measurement Request (2)
      Dialog token: 1
      Transmit Power Used: 12dBm
      Max Transmit Power: 23dBm
  v Tagged parameters (15 bytes)
    v Tag: SSID parameter set: OPEN-ECSA-655
        Tag Number: SSID parameter set (0)
        Tag length: 13
        SSID: OPEN-ECSA-655
```

Figure 10. Example of STA receiving link measurement request from the AP

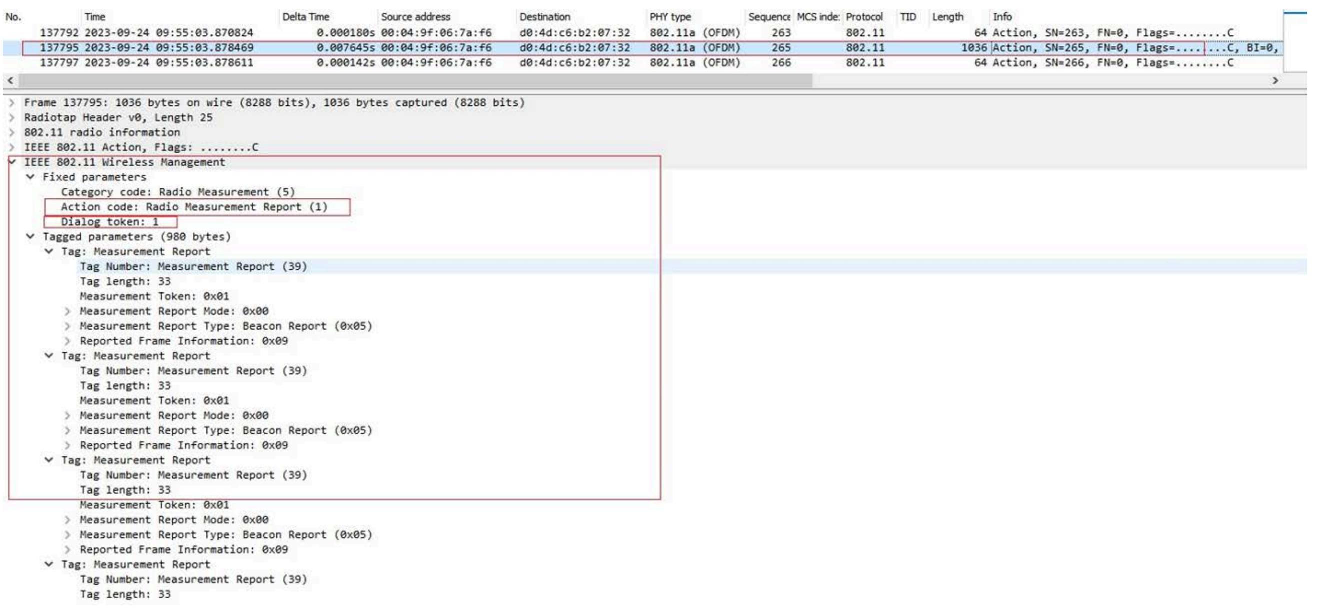
Step 3 – STA responds with a link measurement response on the console.

Command output example:

```
RRM: Radio Measurement report - hexdump(len=35): 27 21 97 00 05 80 a1 00 00 00 00 00 00
 00 00 00 00 09 3e ff cc 88 c7 10 d7 11 00 00 00 00 00 02 02 01 00
nl80211: Send Action frame (ifindex=3, freq=5805 MHz wait=0 ms no_cck=0 offchanok=1)
```

Figure 11 shows an example of link measurement response from STA to AP.

- AP MAC= d0:4d:c6:b2:07:32
- STA MAC= 00:04:9f:06:7a:f6



No.	Time	Delta Time	Source address	Destination	PHY type	Sequence	MCS inde:	Protocol	TID	Length	Info
137792	2023-09-24 09:55:03.870824	0.000180s	00:04:9f:06:7a:f6	d0:4d:c6:b2:07:32	802.11a (OFDM)	263		802.11		64	Action, SN=263, FN=0, Flags=........C
137795	2023-09-24 09:55:03.878469	0.007645s	00:04:9f:06:7a:f6	d0:4d:c6:b2:07:32	802.11a (OFDM)	265		802.11		1036	Action, SN=265, FN=0, Flags=........C, BI=0,
137797	2023-09-24 09:55:03.878611	0.000142s	00:04:9f:06:7a:f6	d0:4d:c6:b2:07:32	802.11a (OFDM)	266		802.11		64	Action, SN=266, FN=0, Flags=........C

```
> Frame 137795: 1036 bytes on wire (8288 bits), 1036 bytes captured (8288 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Radio Measurement Report (1)
      Dialog token: 1
  v Tagged parameters (980 bytes)
    v Tag: Measurement Report
        Tag Number: Measurement Report (39)
        Tag length: 33
        Measurement Token: 0x01
      > Measurement Report Mode: 0x00
      > Measurement Report Type: Beacon Report (0x05)
      > Reported Frame Information: 0x09
    v Tag: Measurement Report
        Tag Number: Measurement Report (39)
        Tag length: 33
        Measurement Token: 0x01
      > Measurement Report Mode: 0x00
      > Measurement Report Type: Beacon Report (0x05)
      > Reported Frame Information: 0x09
    v Tag: Measurement Report
        Tag Number: Measurement Report (39)
        Tag length: 33
        Measurement Token: 0x01
      > Measurement Report Mode: 0x00
      > Measurement Report Type: Beacon Report (0x05)
      > Reported Frame Information: 0x09
    v Tag: Measurement Report
        Tag Number: Measurement Report (39)
        Tag length: 33
```

Figure 11. Example of link measurement response from the STA to the AP

6.3 Beacon report

wpa_supplicant initiates the STA and AP to send beacon reports to each other. In this example, the STA sends a beacon report to the AP.

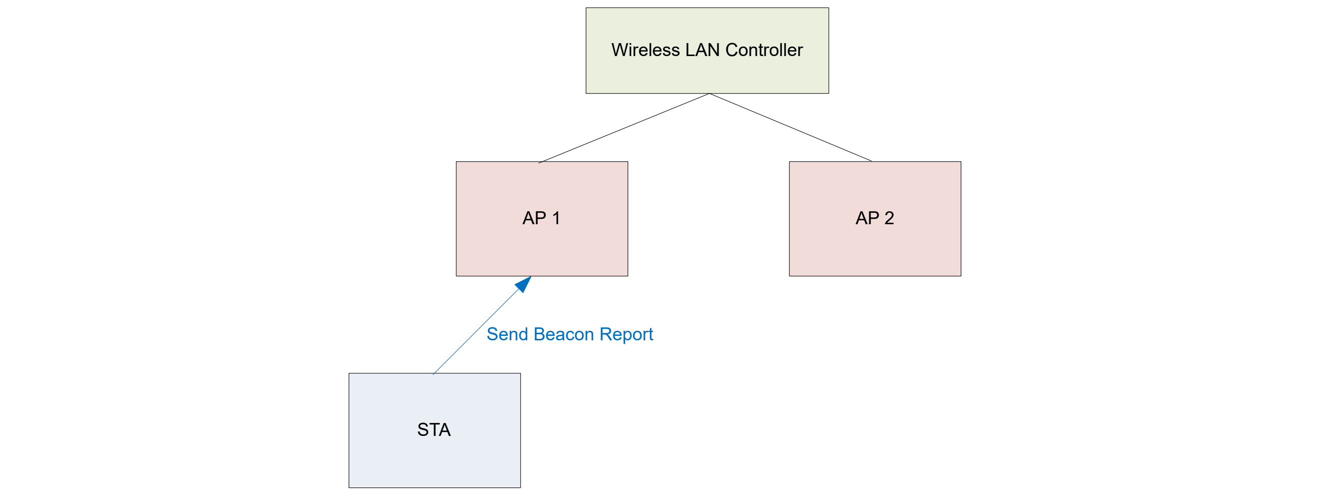


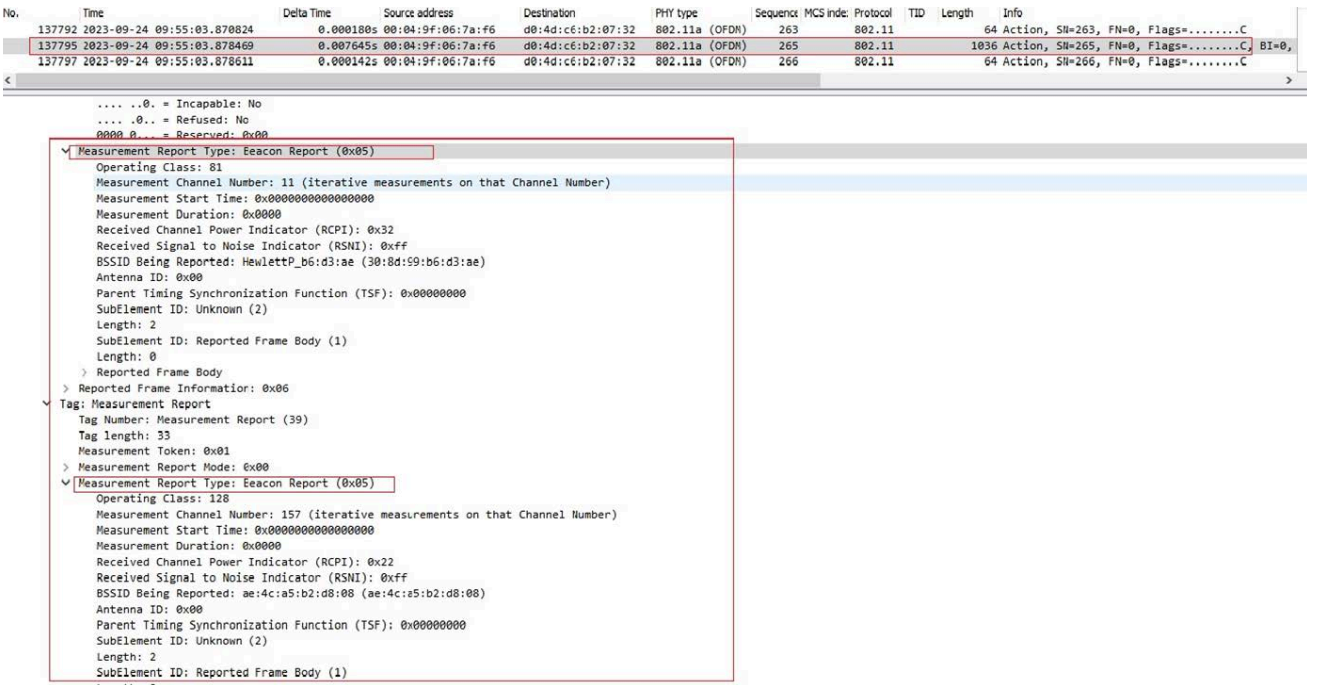
Figure 12. Beacon report setup

Step 1 – Set up the environment (Section 5).

Step 2 – STA sends a beacon report to the AP.

Figure 13 shows a sniffer capture example of the STA sending a Beacon Report to the AP.

- AP MAC= d0:4d:c6:b2:07:32
- STA MAC= 00:04:9f:06:7a:f6



```
No.     Time                        Delta Time  Source address     Destination        PHY type       Sequence MCS inde: Protocol TID Length Info
 137792 2023-09-24 09:55:03.870824   0.000180s 00:04:9f:06:7a:f6  d0:4d:c6:b2:07:32  802.11a (OFDM)  263               802.11          64 Action, SN=263, FN=0, Flags=........C
 137795 2023-09-24 09:55:03.878469   0.007645s 00:04:9f:06:7a:f6  d0:4d:c6:b2:07:32  802.11a (OFDM)  265               802.11        1036 Action, SN=265, FN=0, Flags=........C, BI=0,
 137797 2023-09-24 09:55:03.878611   0.000142s 00:04:9f:06:7a:f6  d0:4d:c6:b2:07:32  802.11a (OFDM)  266               802.11          64 Action, SN=266, FN=0, Flags=........C
```

```
            .... ..0. = Incapable: No
            .... .0.. = Refused: No
            0000 0... = Reserved: 0x00
        Measurement Report Type: Eeacon Report (0x05)
            Operating Class: 81
            Measurement Channel Number: 11 (iterative measurements on that Channel Number)
            Measurement Start Time: 0x0000000000000000
            Measurement Duration: 0x0000
            Received Channel Power Indicator (RCPI): 0x32
            Received Signal to Noise Indicator (RSNI): 0xff
            BSSID Being Reported: HewlettP_b6:d3:ae (30:8d:99:b6:d3:ae)
            Antenna ID: 0x00
            Parent Timing Synchronization Function (TSF): 0x00000000
            SubElement ID: Unknown (2)
            Length: 2
            SubElement ID: Reported Frame Body (1)
            Length: 0
          > Reported Frame Body
        > Reported Frame Informatior: 0x06
    Tag: Measurement Report
        Tag Number: Measurement Report (39)
        Tag length: 33
        Measurement Token: 0x01
      > Measurement Report Mode: 0x00
        Measurement Report Type: Eeacon Report (0x05)
            Operating Class: 128
            Measurement Channel Number: 157 (iterative measurements on that Channel Number)
            Measurement Start Time: 0x0000000000000000
            Measurement Duration: 0x0000
            Received Channel Power Indicator (RCPI): 0x22
            Received Signal to Noise Indicator (RSNI): 0xff
            BSSID Being Reported: ae:4c:a5:b2:d8:08 (ae:4c:a5:b2:d8:08)
            Antenna ID: 0x00
            Parent Timing Synchronization Function (TSF): 0x00000000
            SubElement ID: Unknown (2)
            Length: 2
            SubElement ID: Reported Frame Body (1)
```

Figure 13. Example of the STA sending a beacon report to the AP

7 802.11v example

The example shows a BSS transition management query (BTM) from the STA. The AP responds with a request for the STA to roam based on a preferred candidate list. The request is in a BSS management frame.

If the AP is configured with disassociation imminent function enabled, the STA is forced to roam to a better AP. If disassociation imminent function is disabled, the STA can reject or accept the request. Refer to the user manual of the AP manual for this configuration.

wpa_supplicant handles BTM queries. Issue a wpa_cli command (in step 2) to manually send a BTM query.

Figure 14 shows the BTM query sequence, where:

1. BTM query
2. BTM request
3. BTM response

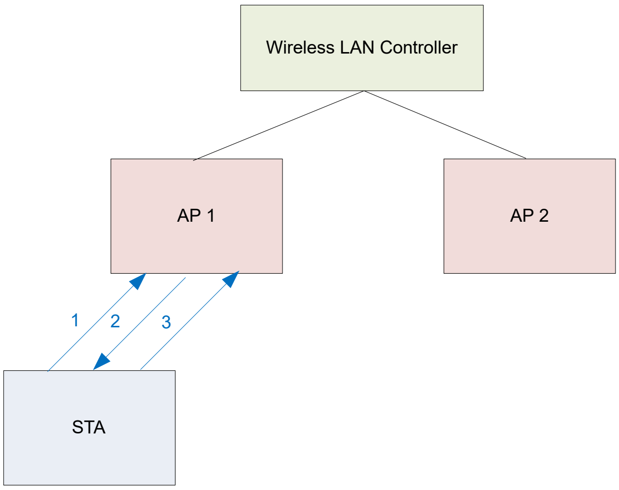


Figure 14. BTM query communication

Step 1 – Set up the environment (Section 5).

Step 2 – Issue a wpa_cli command to trigger a BTM query.

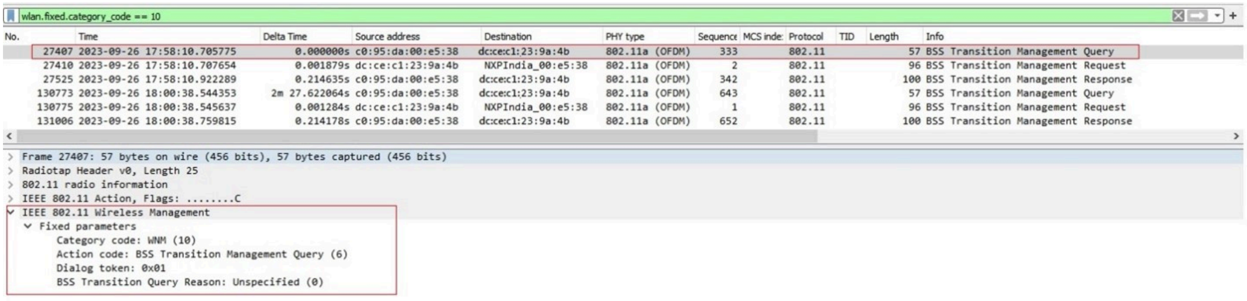
```
./wpa_cli wnm_bss_query 1
```

Command output example:

```
WNM: Send BSS Transition Management Query to 00:11:32:ed:9e:b0 query_reason=1
nl80211: Send[ 3172.437052] wlan: mlan0 START SCAN
Action frame (ifindex=3, freq=2422 MHz wait=0 ms no_cck=0 offchanok=1)
OK
nl80211: Drv Event 60 (NL80211_CMD_FRAME_TX_STATUS) received for mlan0
nl80211: Frame TX status event A1=00:11:32:ed:9e:b0 stype=13 cookie=0x75319743 ack=1
nl80211: Frame TX status: cookie=0x75319743 (match) (ack=1)
mlan0: Event TX_STATUS (16) received
mlan0: EVENT_TX_STATUS dst=00:11:32:ed:9e:b0 type=0 stype=13
Off-channel: Ignore Action TX status - no pending operation
nl80211: BSS Event 59 (NL80211_CMD_FRAME) received for mlan0
nl80211: RX frame da=c0:95:da:00:e5:38 sa=00:11:32:ed:9e:b0 bssid=00:11:32:ed:9e:b0
 freq=2422 ssi_signal=0 fc=0xd0 seq_ctrl=0x90 stype=13 (WLAN_FC_STYPE_ACTION) len=54
mlan0: Event RX_MGMT (18) received
mlan0: Received Action frame: SA=00:11:32:ed:9e:b0 Category=10 DataLen=29 freq=2422 MHz
WNM: RX action 7 from 00:11:32:ed:9e:b0
```

Figure 15 shows the example where the STA sends a BTM query to the AP 1.

- STA MAC= c0:95:da:00:e5:38
- AP MAC= dc:ce:c1:23:9a:4b



wlan.fixed.category_code == 10

No.	Time	Delta Time	Source address	Destination	PHY type	Sequence	MCS inde:	Protocol	TID	Length	Info
27407	2023-09-26 17:58:10.705775	0.000000s	c0:95:da:00:e5:38	dc:ce:c1:23:9a:4b	802.11a (OFDM)	333		802.11		57	BSS Transition Management Query
27410	2023-09-26 17:58:10.707654	0.001879s	dc:ce:c1:23:9a:4b	NXPIndia_00:e5:38	802.11a (OFDM)	2		802.11		96	BSS Transition Management Request
27525	2023-09-26 17:58:10.922289	0.214635s	c0:95:da:00:e5:38	dc:ce:c1:23:9a:4b	802.11a (OFDM)	342		802.11		100	BSS Transition Management Response
130773	2023-09-26 18:00:38.544353	2m 27.622064s	c0:95:da:00:e5:38	dc:ce:c1:23:9a:4b	802.11a (OFDM)	643		802.11		57	BSS Transition Management Query
130775	2023-09-26 18:00:38.545637	0.001284s	dc:ce:c1:23:9a:4b	NXPIndia_00:e5:38	802.11a (OFDM)	1		802.11		96	BSS Transition Management Request
131006	2023-09-26 18:00:38.759815	0.214178s	c0:95:da:00:e5:38	dc:ce:c1:23:9a:4b	802.11a (OFDM)	652		802.11		100	BSS Transition Management Response

```
> Frame 27407: 57 bytes on wire (456 bits), 57 bytes captured (456 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
    v Fixed parameters
        Category code: WNM (10)
        Action code: BSS Transition Management Query (6)
        Dialog token: 0x01
        BSS Transition Query Reason: Unspecified (0)
```

Figure 15. Example of STA sending a BTM query to the AP 1

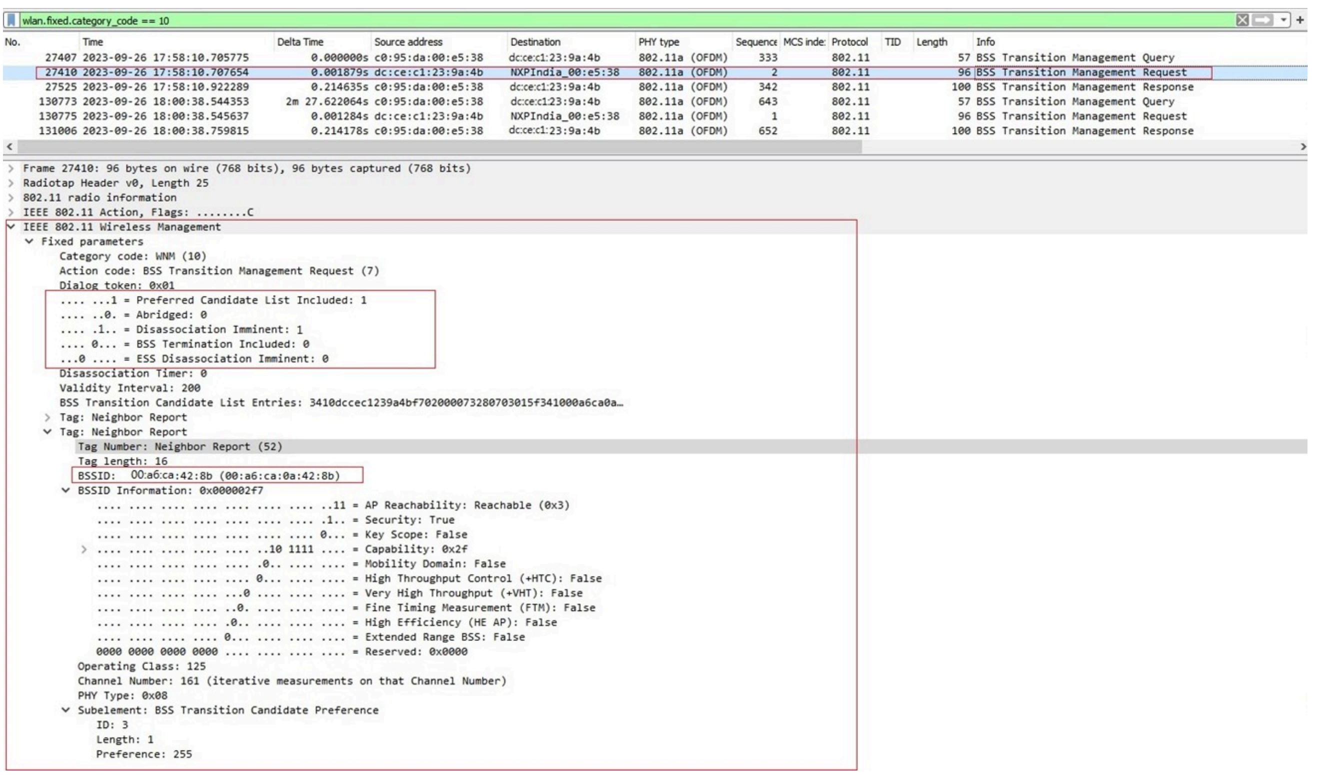
Step 3 – AP 1 sends STA a BTM request with a preferred candidate list. The request is displayed on the console of the STA. The STA decides whether to roam or not based on this information.

dmesg output example:

```
WNM: BSS Transition Management Request: dialog_token=1 request_mode=0x1 disassoc_timer=0
 validity_interval=100
mlan0: WNM: Preferred List Available
WNM: Neighbor report tag 52
WNM: Subelement id=6 le[ 3172.532203] wlan: SCAN COMPLETED: scanned AP count=1
n=3
WNM: Subelement id=3 len=1
…
WNM: BSS Transition Candidate List
0: 00:11:32:ed:9e:b0 info=0x17 op_class=12 chan=3 phy=0 pref=1 freq=2422
WNM: Candidate list valid for 10240 ms
mlan0: WNM: Fetch current scan results from the driver for checking transition candidates
nl80211: Received scan results (1 BSSes)
nl80211: Scan results indicate BSS status with 00:11:32:ed:9e:b0 as associated
mlan0: WNM: No transition candidate matches existing scan results
WNM: Scan 1 frequencies based on transition candidate list
WNM: Scan only for a specific BSSID since there is only a single candidate
 00:11:32:ed:9e:b0
mlan0: Setting scan request: 0.000000 sec
mlan0: Starting AP scan for wildcard SSID
WPS: Building WPS IE for Probe Request
WPS:  * Version (hardcoded 0x10)
WPS:  * Request Type
WPS:  * Config Methods (3108)
WPS:  * UUID-E
WPS:  * Primary Device Type
WPS:  * RF Bands (3)
WPS:  * Association State
WPS:  * Configuration Error (0)
WPS:  * Device Password ID (0)
WPS:  * Manufacturer
WPS:  * Model Name
WPS:  * Model Number
WPS:  * Device Name
WPS:  * Version2 (0x20)
P2P: * P2P IE header
P2P: * Capability dev=25 group=00
P2P: * Listen Channel: Regulatory Class 81 Channel 6
mlan0: Optimize scan based on previously generated frequency list
mlan0: Scan a previously specified BSSID 00:11:32:ed:9e:b0 and SSID synology_wifi_2.4G
mlan0: Add radio work 'scan'@0xaaab1e40e190
mlan0: First radio work item in the queue - schedule start immediately
mlan0: Starting radio work 'scan'@0xaaab1e40e190 after 0.000030 second wait
mlan0: nl80211: scan request
nl80211: Scan for a specific BSSID: 00:11:32:ed:9e:b0
Scan requested (ret=0) - scan timeout 30 seconds
nl80211: Drv Event 33 (NL80211_CMD_TRIGGER_SCAN) received for mlan0
mlan0: nl80211: Scan trigger
```

Figure 16 shows an example of BTM query request from the AP to the STA.

- STA MAC= c0:95:da:00:e5:38
- AP MAC= dc:ce:c1:23:9a:4b
- Preferred candidate list with the AP BSSID = 00:a6:ca:42:8b (AP 2).
- Dissociation Imminent enabled. STA is forced to roam.



wlan.fixed.category_code == 10

```
No.     Time                        Delta Time   Source address     Destination         PHY type       Sequence MCS inde: Protocol TID Length Info
  27407 2023-09-26 17:58:10.705775     0.000000s c0:95:da:00:e5:38  dc:ce:c1:23:9a:4b   802.11a (OFDM)   333              802.11               57 BSS Transition Management Query
  27410 2023-09-26 17:58:10.707654     0.001879s dc:ce:c1:23:9a:4b  NXPIndia_00:e5:38   802.11a (OFDM)     2              802.11               96 BSS Transition Management Request
  27525 2023-09-26 17:58:10.922289     0.214635s c0:95:da:00:e5:38  dc:ce:c1:23:9a:4b   802.11a (OFDM)   342              802.11              100 BSS Transition Management Response
 130773 2023-09-26 18:00:38.544353 2m 27.622064s c0:95:da:00:e5:38  dc:ce:c1:23:9a:4b   802.11a (OFDM)   643              802.11               57 BSS Transition Management Query
 130775 2023-09-26 18:00:38.545637     0.001284s dc:ce:c1:23:9a:4b  NXPIndia_00:e5:38   802.11a (OFDM)     1              802.11               96 BSS Transition Management Request
 131006 2023-09-26 18:00:38.759815     0.214178s c0:95:da:00:e5:38  dc:ce:c1:23:9a:4b   802.11a (OFDM)   652              802.11              100 BSS Transition Management Response
```

```
> Frame 27410: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters
      Category code: WNM (10)
      Action code: BSS Transition Management Request (7)
      Dialog token: 0x01
      .... ...1 = Preferred Candidate List Included: 1
      .... ..0. = Abridged: 0
      .... .1.. = Disassociation Imminent: 1
      .... 0... = BSS Termination Included: 0
      ...0 .... = ESS Disassociation Imminent: 0
      Disassociation Timer: 0
      Validity Interval: 200
      BSS Transition Candidate List Entries: 3410dccec1239a4bf702000073280703015f341000a6ca0a…
    > Tag: Neighbor Report
    v Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 16
        BSSID:  00:a6:ca:42:8b (00:a6:ca:0a:42:8b)
      v BSSID Information: 0x000002f7
           .... .... .... .... .... .... .... ..11 = AP Reachability: Reachable (0x3)
           .... .... .... .... .... .... .... .1.. = Security: True
           .... .... .... .... .... .... .... 0... = Key Scope: False
         > .... .... .... .... .... ..10 1111 .... = Capability: 0x2f
           .... .... .... .... .... .0.. .... .... = Mobility Domain: False
           .... .... .... .... .... 0... .... .... = High Throughput Control (+HTC): False
           .... .... .... .... ...0 .... .... .... = Very High Throughput (+VHT): False
           .... .... .... .... ..0. .... .... .... = Fine Timing Measurement (FTM): False
           .... .... .... .... .0.. .... .... .... = High Efficiency (HE AP): False
           .... .... .... .... 0... .... .... .... = Extended Range BSS: False
           0000 0000 0000 0000 .... .... .... .... = Reserved: 0x0000
        Operating Class: 125
        Channel Number: 161 (iterative measurements on that Channel Number)
        PHY Type: 0x08
      v Subelement: BSS Transition Candidate Preference
           ID: 3
           Length: 1
           Preference: 255
```

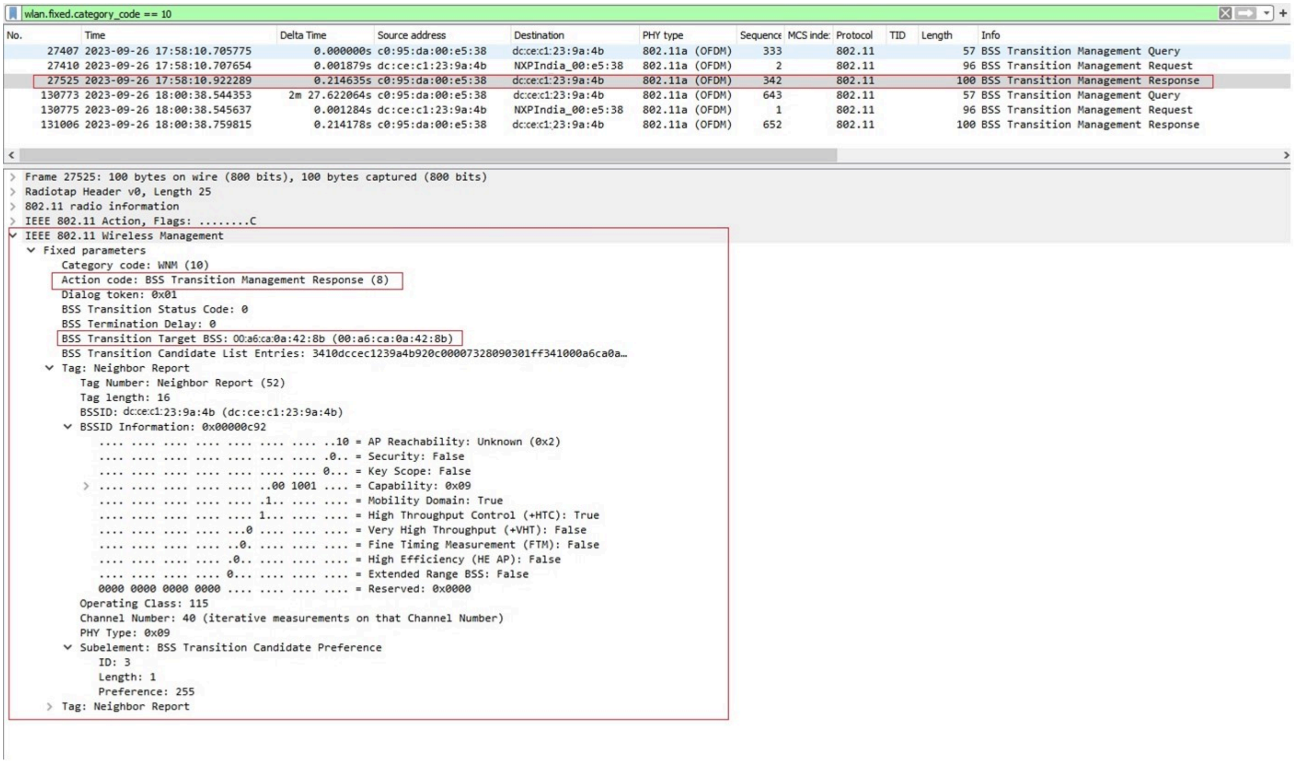
Figure 16. Example of BTM query request from the AP to the STA

Step 4 – STA responds to the request of AP1 to roam to a different AP.

Note: *STA roams using 802.11r. Refer to Section 8.*

Figure 17 shows an example of the STA response to AP 1 with the decision to roam to AP 2.

- STA MAC= c0:95:da:00:e5:38
- AP MAC= dc:ce:c1:23:9a:4b
- BSS Transition Target BSS = 00:a6:ca:42:8b (decides to roam to AP 2)



```
wlan.fixed.category_code == 10

No.    Time                        Delta Time   Source address     Destination        PHY type       Sequence MCS inde: Protocol TID Length Info
 27407 2023-09-26 17:58:10.705775    0.000000s c0:95:da:00:e5:38 dc:ce:c1:23:9a:4b   802.11a (OFDM)  333              802.11            57 BSS Transition Management Query
 27410 2023-09-26 17:58:10.707654    0.001879s dc:ce:c1:23:9a:4b NXPIndia_00:e5:38   802.11a (OFDM)    2              802.11            96 BSS Transition Management Request
 27525 2023-09-26 17:58:10.922289    0.214635s c0:95:da:00:e5:38 dc:ce:c1:23:9a:4b   802.11a (OFDM)  342              802.11           100 BSS Transition Management Response
130773 2023-09-26 18:00:38.544353 2m 27.622064s c0:95:da:00:e5:38 dc:ce:c1:23:9a:4b   802.11a (OFDM)  643              802.11            57 BSS Transition Management Query
130775 2023-09-26 18:00:38.545637    0.001284s dc:ce:c1:23:9a:4b NXPIndia_00:e5:38   802.11a (OFDM)    1              802.11            96 BSS Transition Management Request
131006 2023-09-26 18:00:38.759815    0.214178s c0:95:da:00:e5:38 dc:ce:c1:23:9a:4b   802.11a (OFDM)  652              802.11           100 BSS Transition Management Response
```

```
> Frame 27525: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
  v 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: 00:a6:ca:0a:42:8b (00:a6:ca:0a:42:8b)
      BSS Transition Candidate List Entries: 3410dccec1239a4b920c00007328090301ff341000a6ca0a…
    v Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 16
        BSSID: dc:ce:c1:23:9a:4b (dc:ce:c1:23:9a:4b)
      v BSSID Information: 0x00000c92
          .... .... .... .... .... .... .... ..10 = AP Reachability: Unknown (0x2)
          .... .... .... .... .... .... .... .0.. = Security: False
          .... .... .... .... .... .... .... 0... = Key Scope: False
        > .... .... .... .... .... ..00 1001 .... = Capability: 0x09
          .... .... .... .... .... .1.. .... .... = Mobility Domain: True
          .... .... .... .... .... 1... .... .... = High Throughput Control (+HTC): True
          .... .... .... .... ...0 .... .... .... = Very High Throughput (+VHT): False
          .... .... .... .... ..0. .... .... .... = Fine Timing Measurement (FTM): False
          .... .... .... .... .0.. .... .... .... = High Efficiency (HE AP): False
          .... .... .... .... 0... .... .... .... = Extended Range BSS: False
          0000 0000 0000 0000 .... .... .... .... = Reserved: 0x0000
        Operating Class: 115
        Channel Number: 40 (iterative measurements on that Channel Number)
        PHY Type: 0x09
      v Subelement: BSS Transition Candidate Preference
          ID: 3
          Length: 1
          Preference: 255
    > Tag: Neighbor Report
```

Figure 17. Example of the STA response to AP 1

8 802.11r examples

This section provides an example for over-the-air and over-the-distribution-system (over-the-DS) Fast Transition. A EAPoL key 4-way handshake is not required for FT.

8.1 Over-the-air fast transition (FT)

In Over-the-Air FT, the STA directly communicates with the target AP using IEEE 802.11 FT-Auth and FT-(Re)Association during the FT association flow. The capability for FT is advertised in the Beacon Mobility Domain Information Element of the AP.

In this example, the wireless LAN controller is configured for over-the-air FT. The STA is connected to AP1 at location A. As the STA moves closer to AP2 at location B, the received signal strength from AP1 drops below the set signal threshold. The STA automatically switches to AP2.

wpa_supplicant handles Over-the-Air FT. The following wpa_cli command can also be used to manually trigger Over-the-Air FT.

```
./wpa_cli -i mlan0 ROAM  <MACaddress of Target AP >
```

Figure 18 shows Over-the-Air FT communication. The arrows represent the Over-the-Air FT sequence:

1. Authentication
2. Authentication
3. Reassociation Request
4. Reassociation Response

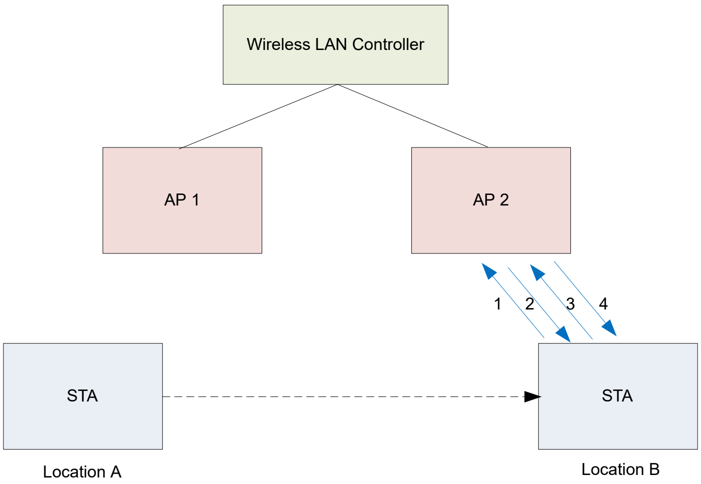


Figure 18. Over-the-air FT communication

Step 1 – Set up the environment (Section 5).

Step 2 – Move STA closer to AP 2 until the signal strength from AP1 is less than the threshold.

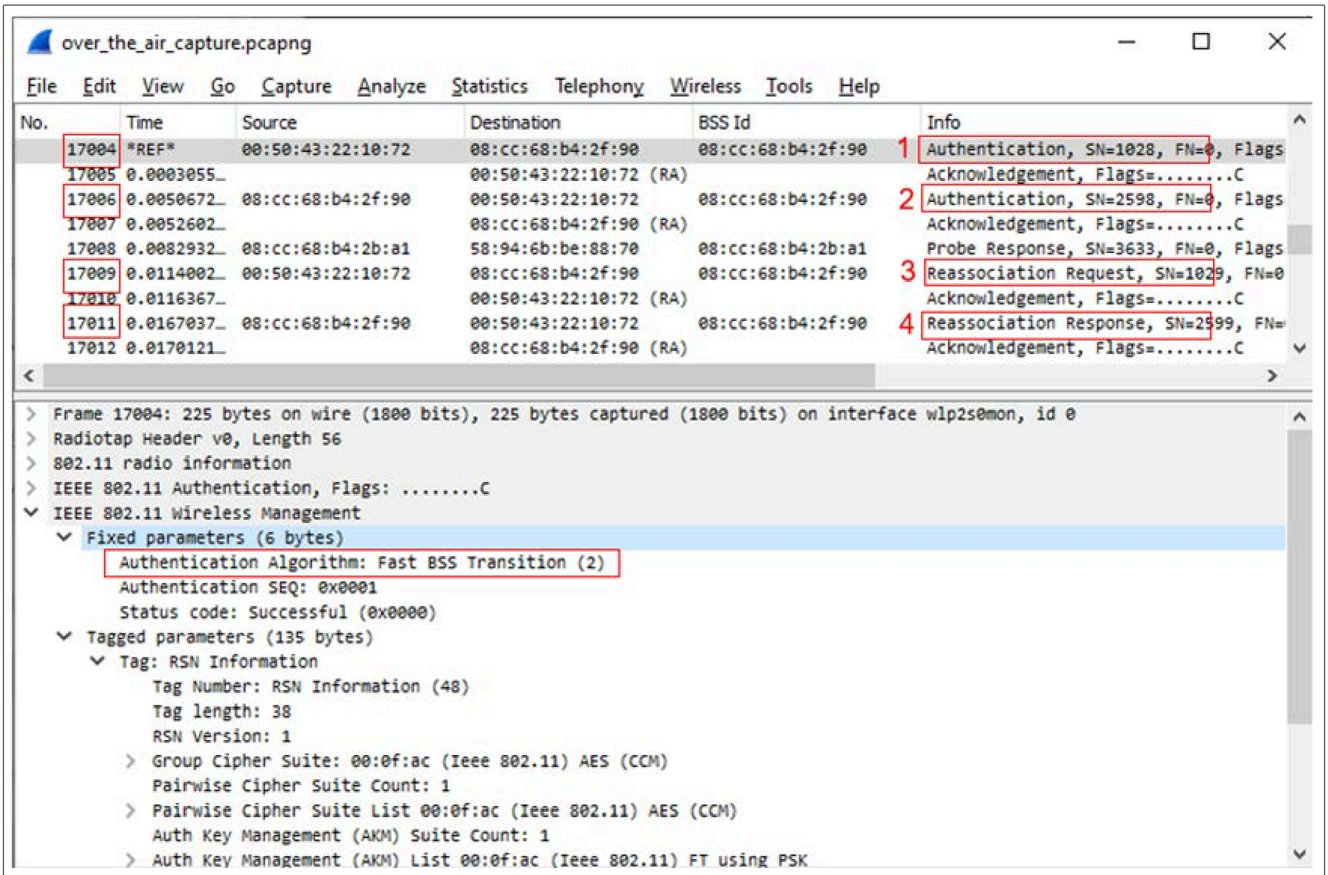
Step 3 – STA roams from AP 1 to AP 2, which is also shown on the console.

Command output example:

```
wlan: send out FT auth,wait for auth response
wlan : FT response  target AP 08:XX:XX:XX:2f:90
wlan: FT auth received
Fast BSS Transition use ft-over-air
wlan: Fast Bss transition to bssid 08:XX:XX:XX:2f:90 successfully
```

Figure 19 shows a sniffer capture example of Over-the-Air FT.

- AP 1 MAC= `08:cc:68:b4:2b:a0`
- STA MAC= `00:50:43:22:10:72`
- AP 2 MAC= `08:cc:68:b4:2f:90`
- Over-the-Air Transition sequence of Authentication, Authentication, Reassociation Request, and Reassociation Response.


over_the_air_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
1
2
3
4

No.	Time	Source	Destination	BSS Id	Info
17004	*REF*	00:50:43:22:10:72	08:cc:68:b4:2f:90	08:cc:68:b4:2f:90	Authentication, SN=1028, FN=0, Flags
17005	0.0003055…		00:50:43:22:10:72 (RA)		Acknowledgement, Flags=........C
17006	0.0050672…	08:cc:68:b4:2f:90	00:50:43:22:10:72	08:cc:68:b4:2f:90	Authentication, SN=2598, FN=0, Flags
17007	0.0052602…		08:cc:68:b4:2f:90 (RA)		Acknowledgement, Flags=........C
17008	0.0082932…	08:cc:68:b4:2b:a1	58:94:6b:be:88:70	08:cc:68:b4:2b:a1	Probe Response, SN=3633, FN=0, Flags
17009	0.0114002…	00:50:43:22:10:72	08:cc:68:b4:2f:90	08:cc:68:b4:2f:90	Reassociation Request, SN=1029, FN=0
17010	0.0116367…		00:50:43:22:10:72 (RA)		Acknowledgement, Flags=........C
17011	0.0167037…	08:cc:68:b4:2f:90	00:50:43:22:10:72	08:cc:68:b4:2f:90	Reassociation Response, SN=2599, FN=
17012	0.0170121…		08:cc:68:b4:2f:90 (RA)		Acknowledgement, Flags=........C

```
> Frame 17004: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface wlp2s0mon, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: ........C
v IEEE 802.11 Wireless Management
    v Fixed parameters (6 bytes)
          Authentication Algorithm: Fast BSS Transition (2)
          Authentication SEQ: 0x0001
          Status code: Successful (0x0000)
    v Tagged parameters (135 bytes)
        v Tag: RSN Information
              Tag Number: RSN Information (48)
              Tag length: 38
              RSN Version: 1
            > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
              Pairwise Cipher Suite Count: 1
            > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
              Auth Key Management (AKM) Suite Count: 1
            > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT using PSK
```

Figure 19. Sniffer capture example of Over-the-Air FT

8.1.1 Over-the-Air FT flow

The Figure 20 shows the interaction between the wpa_supplicant, Wi-Fi driver, and firmware.

The wpa_supplicant commands (in uppercase) are defined in *hostap/src/drivers/nl80211_copy.h*.

For more details about the driver to firmware APIs, see ref.[1], ref.[2], ref.[3], and ref.[4].

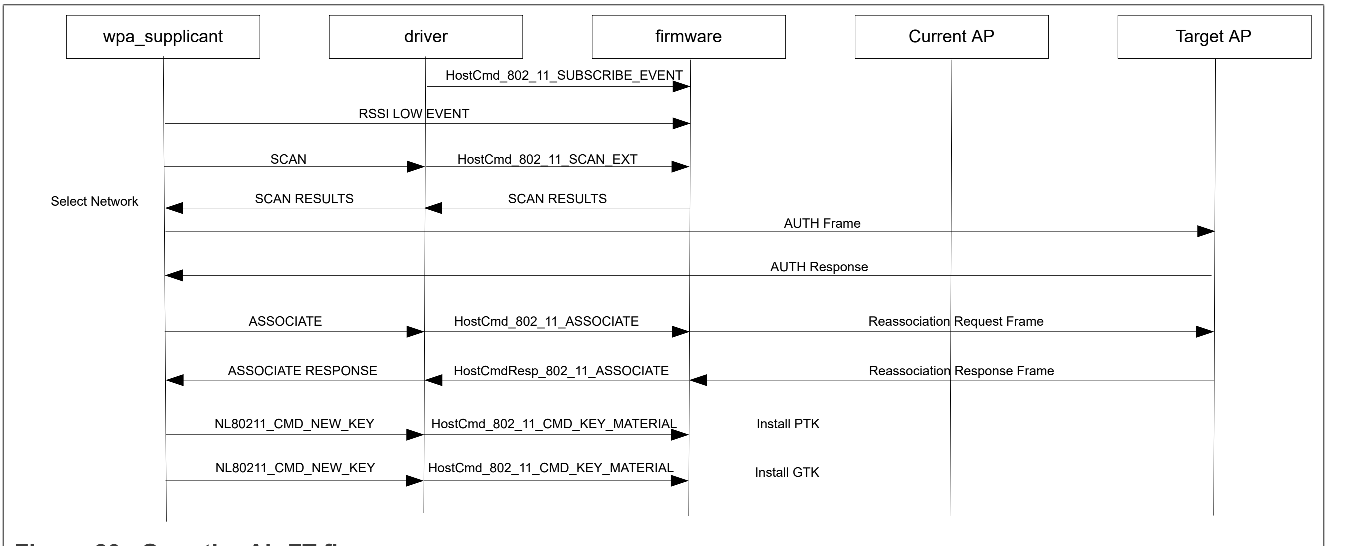


Figure 20. Over-the-Air FT flow

8.2 Over-the-DS fast transition (FT)

In over-the-DS FT, the STA communicates with the target AP through the current AP. STA sends IEEE 802.11 FT action frames to the current AP, which forwards the frames to the target. The capability for FT is advertised in the Beacon Mobility Domain Information Element of the AP.

In this example, the wireless LAN controller is configured for Over-the-DS FT. The STA is connected to AP1 at location A. When the STA moves closer to AP2 at location B, the received signal strength from AP1 drops below the set signal threshold. The STA is triggered to roam to AP 2 when the wpa_supplicant command is issued.

Note: *Open source wpa_supplicant does not support automatic roaming Over-the-DS.*

The command to manually trigger Over-the-DS FT is:

```
./wpa_cli -i mlan0 FT_DS  <MACaddress of Target AP >
```

Figure 21 shows Over-the-DS FT communication. The arrows represent the FT Over-the-DS sequence:

1. Action Frame (Fast Transfer Request)
2. Action Frame (Fast Transfer Response)
3. Reassociation Request
4. Reassociation Response

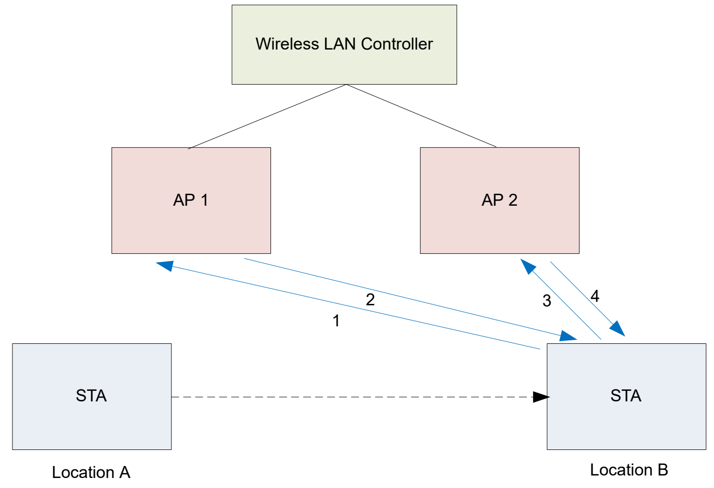


Figure 21. Over-the-DS FT communication

Step 1 – Set up the environment (Section 5).

Step 2 – Move STA closer to AP 2, where the signal strength from AP 1 will be less than the threshold.

Step 3 – Run the `wpa_cli` command to trigger Over-the-DS FT.

```
./wpa_cli -i mlan0 FT_DS  <MACaddress of Target AP >
```

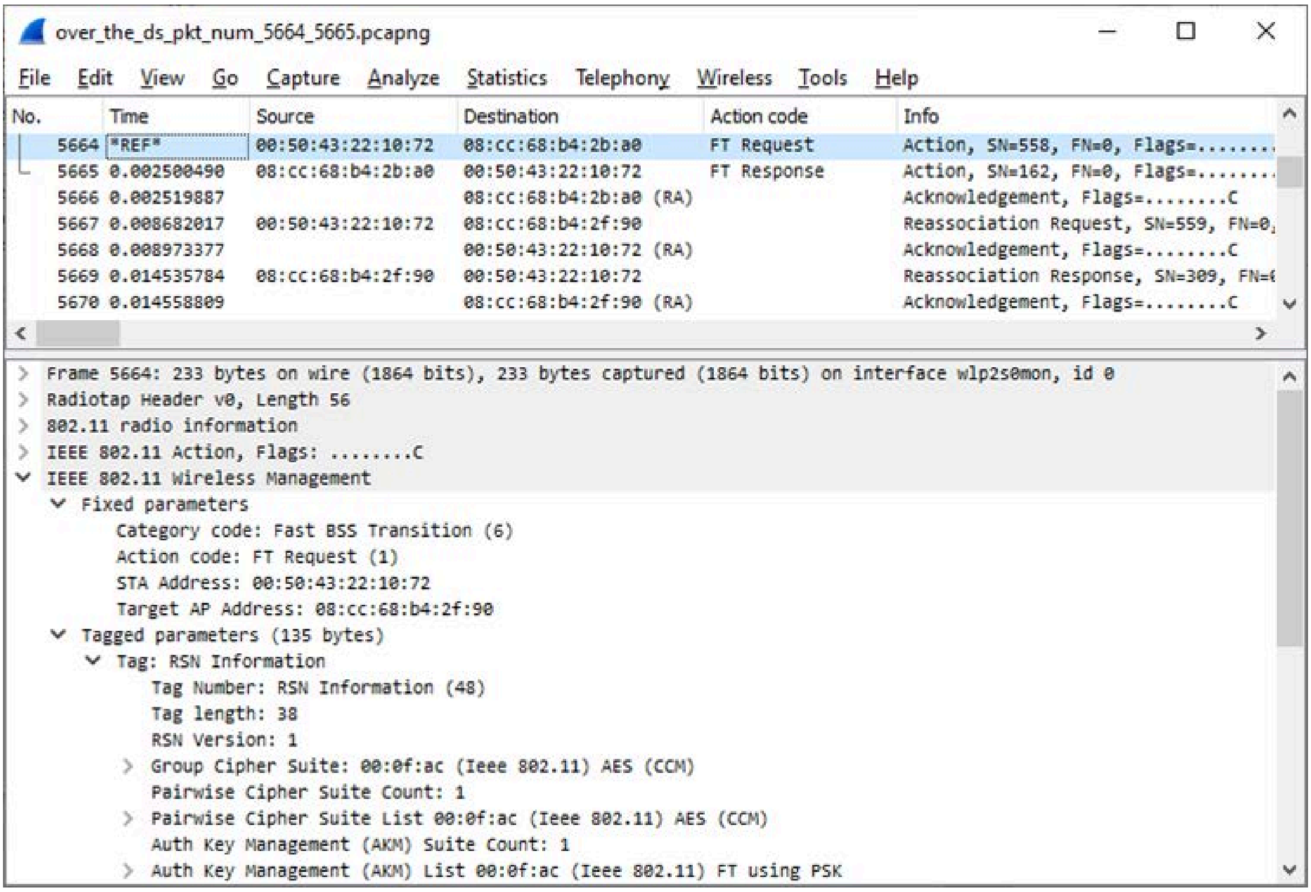
Step 4 – The STA roams from AP 2 to AP 1 (also shown on the console).

Output example:

```
wlan: send out FT request,wait for FT response
wlan : FT response  target AP 08:XX:XX:XX:2f:90
wlan: received FT response
Fast BSS transition to bssid 08:XX:XX:XX:2f:90 successfully
```

Figure 22 shows a sniffer capture example of Over-the-DS FT.

- AP 1 MAC= 08:cc:68:b4:2b:a0
- STA MAC= 00:50:43:22:10:72
- AP 2 MAC= 08:cc:68:b4:2f:90
- Over-the-DS FT sequence of Action, Action, Reassociation Request, and Reassociation Response.


over_the_ds_pkt_num_5664_5665.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Action code	Info
5664	*REF*	00:50:43:22:10:72	08:cc:68:b4:2b:a0	FT Request	Action, SN=558, FN=0, Flags=.......
5665	0.002500490	08:cc:68:b4:2b:a0	00:50:43:22:10:72	FT Response	Action, SN=162, FN=0, Flags=.......
5666	0.002519887		08:cc:68:b4:2b:a0 (RA)		Acknowledgement, Flags=........C
5667	0.008682017	00:50:43:22:10:72	08:cc:68:b4:2f:90		Reassociation Request, SN=559, FN=0,
5668	0.008973377		00:50:43:22:10:72 (RA)		Acknowledgement, Flags=........C
5669	0.014535784	08:cc:68:b4:2f:90	00:50:43:22:10:72		Reassociation Response, SN=309, FN=
5670	0.014558809		08:cc:68:b4:2f:90 (RA)		Acknowledgement, Flags=........C

```
> Frame 5664: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface wlp2s0mon, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
    v Fixed parameters
          Category code: Fast BSS Transition (6)
          Action code: FT Request (1)
          STA Address: 00:50:43:22:10:72
          Target AP Address: 08:cc:68:b4:2f:90
    v Tagged parameters (135 bytes)
        v Tag: RSN Information
              Tag Number: RSN Information (48)
              Tag length: 38
              RSN Version: 1
            > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
              Pairwise Cipher Suite Count: 1
            > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
              Auth Key Management (AKM) Suite Count: 1
            > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT using PSK
```

Figure 22. Sniffer capture example of Over-the-DS FT

8.2.1 Over-the-DS FT flow

Figure 23 shows the interaction between the wpa_supplicant, Wi-Fi driver, and firmware.

The wpa_supplicant commands (in uppercase) are defined in *hostap/src/drivers/nl80211_copy.h*.

For more details about the driver to firmware APIs, see ref.[1], ref.[2], ref.[3], and ref.[4].

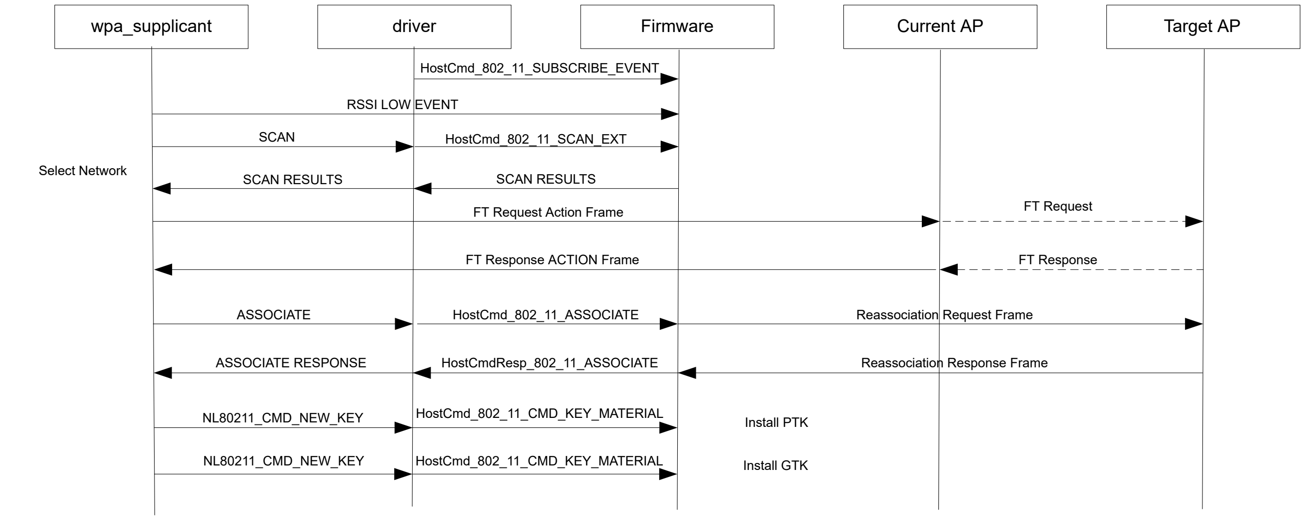


Figure 23. Over-the-DS FT flow

9 Abbreviations

Table 2. Abbreviations

Abbreviation	Description
AP	Access point
bgscan	Background scan
BSS	Basic service set
BTM	BSS transition management
DS	Distribution system
DUT	Device under test
ESS	Extended service set
FT	Fast transition
MLME	MAC sublayer management entity
RRM	Radio resource management
RSSI	Receive signal strength indication
STA	Station
WNM	Wireless network management
wpa_cli	Command line interface for wpa_supplicant

10 References

[1] Application note – AN13296: Embedded Wi-Fi Subsystem API Specification V16 (link)

[2] Application note – AN13297: Embedded Wi-Fi Subsystem API Specification V17 (link)

[3] Application note – AN13538: Embedded Wi-Fi Subsystem API Specification V18 (link)

[4] Application note – AN14314: Embedded Wi-Fi Subsystem API Specification for AW692/AW693 (link)

[5] Webpage – 88W8987: 2.4/5 GHz Dual-Band 1x1 Wi-Fi® 5 (802.11ac) + Bluetooth® Solution (link)

[6] Webpage – 88W8997: 2.4/5 GHz Dual-Band 2x2 Wi-Fi® 5 (802.11ac) + Bluetooth® Solution (link)

[7] Webpage – 88Q9098: 2.4/5 GHz Dual-Band 2x2 Wi-Fi® 6 (802.11ax) + Bluetooth® Automotive Solution (link)

[8] Webpage – 88W9098: 2.4/5 GHz Dual-Band 2x2 Wi-Fi® 6 (802.11ax) + Bluetooth® (link)

[9] Webpage – AW611: 2.4/5 GHz Dual-band 1x1 Wi-Fi® 6 (802.11ax) + Bluetooth® Automotive Solution (link)

[10] Webpage – AW690: Wi-Fi® 6 1x1 Concurrent Dual Wi-Fi (CDW) and Bluetooth® Combo SoC (link)

[11] Webpage – AW692: 2x2 Single-band (5 GHz) Concurrent Dual Wi-Fi® 6, 1x1 (2.4 GHz) Wi-Fi 6, and Bluetooth® Combo Solution (link)

[12] Webpage – AW693: 2x2 Dual-band (5-7 GHz), 1x1 (2.4 GHz) Concurrent Dual Wi-Fi 6/6E and Bluetooth Combo Solution (link)

[13] Webpage – IW416: 2.4/5 GHz Dual-Band 1x1 Wi-Fi® 4 (802.11n) + Bluetooth® Solution (link)

[14] Webpage – IW611: 2.4/5 GHz Dual-band 1x1 Wi-Fi® 6 (802.11ax) + Bluetooth® Solution (link)

[15] Webpage – IW610: 2.4/5 GHz Dual-band 1x1 Wi-Fi® 6 + Bluetooth Low Energy + 802.15.4 Tri-Radio Solution link

[16] Webpage – IW612: 2.4/5 GHz Dual-Band 1x1 Wi-Fi® 6 (802.11ax) + Bluetooth® + 802.15.4 Tri-radio Solution (link)

[17] Webpage – IW620: 2.4/5 GHz Dual-Band 2x2 Wi-Fi® 6 (802.11ax) + Bluetooth® Solution (link)

[18] Webpage – Linux WPA/WPA2/WPA3/IEEE 802.1X Supplicant (link)

11 Note about the source code in the document

The example code shown in this document has the following copyright and BSD-3-Clause license:

12 Revision history

Table 3. Revision history

Document ID	Release date	Description
AN14212 v.3.0	12 May 2025	• Section 1.1 "Supported devices": added IW610. • Section 10 "References": updated.
AN14212 v.2.0	13 January 2025	• Changed the access of the document to public. • Supersedes AN13888 – 802.11r and fast transition (FT).
AN14212 v.1.0	22 August 2024	• Initial version

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Suitability for use in automotive applications — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Bluetooth — the Bluetooth wordmark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by NXP Semiconductors is under license.

Tables

Figures

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.