Mediatek Wi-Fi AP Software Programming Guide

Version: 4.12
Release date: 2022-04-21

Document Revision History

Revision	Date	Author	Description
4.5	2015/03/25	Money Wang	Update ● WPS ● PMF ● IEEE802.11h ● Authenticator Add • ACL
4.6	2015/08/25	Money Wang	Update ACS-related parameters ACS stands for Automatic Channel Selection Add maximum support rate parameters Update CountryRegionABand to support Ch144 Update MBSSID chapter Remove iNIC
4.7	2015/12/18	White Pai	Update TX/RX Stream Update DFS Add beamforming Update Fixed Rate
4.8	2016/03/25	Money Wang	Update FAQ Fix some typos Fix incorrect flow described in MAC Repeater Update for MT7615
4.9	2017/01/23	Money Wang	Rewrite • Profile and iwpriv • WSC • IEEE802.11h • IOCTL Add • Intrusion Detection System • Protection Mechanism Update • MBSSID • WscConfMethods/ApCliWscSsid • 7615 FixedRate • AP-Client fixed rate • FAQ Remove • WAPI • SNMP MIB
4.10	2017/11/21	Money Wang	Some minor updates
4.11.1	2019/08/13	Mike Tseng	Update 802.11ax related items
4.11.2	2019/09/09	Bruce Huang	Update profile description for TxPower
4.11.3	2019/09/10	William Dai	Update IEEE802.11h
4.11.4	2019/10/04	Mike Tseng	Update FixedRate for MT7915
4.12	2022/04/21	Miller Shen	Add 11BE and 6G config Update • CountryRegionABand • WirelessMode • VHT_BW • Debug (for wifi7 logan driver) Add 21. HE 6G connect

Table of Contents

1 Introduction

This document is a software programming guide for Mediatek Wi-Fi SoftAP driver and it teaches you how to configure your own settings. We do provide two kinds of configuration method, profile and iwpriv. Later we show you the profile parameter list, the iwpriv command list, and some OID examples to demonstrate how to fully utilize the WLAN driver.

2 WLAN SoftAP Driver Profile

2.1 Sample Profile

You can find a sample profile in the driver tarball. Also, you can use the reference GUI with pre-built-by-MTK image to create a profile and use it in your project.

2.2 Basic Profile Parameter

In this section, all the common profile parameters would be introduced and they obey the following syntax of assignment.

[Syntax]

Parameter=Value

The WLAN driver needs to be restarted after modifing the profile. Otherwise, settings would not take effect and an interface down/up cycle could help.

ifconfig ra0 down
ifconfig ra0 up

2.2.1 CountryRegion

Description: Country region for WLAN radio 2.4 GHz regulation (G band)
Value:

CountryRegion=5

Region	Channels
0	1-11
1	1-13
2	10-11
3	10-13
4	14
5	1-14 all active scan
6	3-9
7	5-13
31	1-11 active scan, 12-14 passive scan
32	1-11 active scan, 12-14 passive scan
33	1-14 all active scan, 14 b mode only

2.2.2 CountryRegionABand

Description: Country region for WLAN radio 5/6 GHz regulation (A band)
Value:

CountryRegionABand=7

5GHz Region index list

Region	Channels
0	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
1	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
2	36, 40, 44, 48, 52, 56, 60, 64
3	52, 56, 60, 64, 149, 153, 157, 161
4	149, 153, 157, 161, 165
5	149, 153, 157, 161
6	36, 40, 44, 48
7	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165
8	52, 56, 60, 64
9	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165
10	36, 40, 44, 48, 149, 153, 157, 161, 165
11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 149, 153, 157, 161
12	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144
13	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165
14	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 144, 149, 153, 157, 161, 165

6GHz Region index list

Region	Channels
0	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 113, 117, 121, 125, 129, 133, 137, 141, 145, 149, 153, 157, 161, 165, 169, 173, 177, 181, 185, 189, 193, 197, 201, 205, 209, 213, 217, 221, 225, 229, 233
1	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97
2	101, 105, 109, 113, 117
3	121, 125, 129, 133, 137, 141, 145, 149, 153, 157, 161, 165, 169, 173, 177, 181, 185
4	189, 193, 197, 201, 205, 209, 213, 217, 221, 225, 229, 233
5	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97
6	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97
7	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109

2.2.3 CountryCode

Description: County code for WLAN radio regulation
Value:

CountryCode=

Note:
Default is empy.
2 characters, like TW for Taiwan.
Please refer to the following link for ISO3166 code list for other countries.
http://www.iso.org/iso/prods-services/iso3166ma/02iso-3166-code-lists/country_names_and_code_elements
This parameter can also be configured in EEPROM or eFuse.
Configuration in EEPROM or eFuse has higher priority than that in WLAN Profile.

2.2.4 SSID

Description: Configure AP SSID
Value:

SSID=Mediatek-AP

0~z, 1~32 ASCII characters

2.2.5 WirelessMode

Description: Wireless mode configuration
Value:

WirelessMode=9

0: legacy 11b/g mixed
1: legacy 11b only
2: legacy 11a only
4: legacy 11g only
6: 11n only in 2.4g band
7: 11gn mixed
8: 11an mixed
9: 11bgn mixed
11: 11n only in 5g band
14: 11A/AN/AC mixed 5G band only
15: 11AN/AC mixed 5G band only
16: 11bgn/AX mixed 2.4G band only
17: 11A/AN/AC/AX mixed 5G band only
18: 11AX 6G band only
19: 11AX 2.4G/6G band
20: 11AX 5G/6G band
21: 11AX 2.4G/5G/6G band
22: 11BE 2.4G band
23: 11BE 5G band
24: 11BE 6G band
25: 11BE 2.4G/6G band
26: 11BE 5G/6G band
27: 11BE 2.4G/5G/6G band

2.2.6 Channel

Description: WLAN primary channel configuration (2.4G or 5G band or 6G band)
Value:

Channel=0

Note:
The range of configurable values depends on CountryRegion or CountryRegionABand.
Its default value is zero and the driver automatically selects a random working channel.

2.2.7 VHT_Sec80_Channel

Description: WLAN primary channel configuration for the 2nd VHT80 group (5G band only)

Value:

VHT_Sec80_Channel=0

Note: Same as Channel

2.2.8 HT_BW

Description: HT channel bandwidth configuration
Value:

HT_BW=1

0: 20 MHz
1: 20/40 MHz

2.2.9 VHT_BW

Description: 11ac channel bandwidth configuration
Value:

VHT_BW=1

0: disable
1: 80M
2: 160M
3: 80M+80M
4: 320M

2.2.10 HT_GI

Description: HT guard interval configuration
Value:

HT_GI=1

0: Long GI
1: Short GI

2.2.11 VHT_SGI

Description: 11ac guard interval configuration
Value:

VHT_SGI=1

0: Long GI
1: Short GI

2.2.12 HT_MCS

Description: Modulation and Coding Scheme (MCS) configuration
Value:

HT_MCS=33

0 ~15, 32: Fix MCS rate for HT rate
33: Auto Rate Adaption, recommended

2.2.13 HT_RDG

Description: Enable or disable Reverse Direction Grant
Value:

HT_RDG=1

0: disable
1: enable

2.2.14 HT_EXTCHA

Description: Locate the 40MHz extension channel in combination with the main channel
Value:

HT_EXTCHA=0

0: Below
1: Above

2.2.15 HT_AMSDU

Description: Enable or disable A-MSDU transmission
Value:

HT_AMSDU=1

0: disable
1: enable

2.2.16 AMSDU_NUM

Description: Set supported A-MSDU number when transmission
Value:

AMSDU_NUM=4

1~4 : means supported AMSDU number.

2.2.17 HT_AutoBA

Description: Enable or disable automatically building Block Ack session with the peer
Value:

HT_AutoBA=1

0: disable
1: enable

2.2.18 HT_BADecline

Description: Configure whether always declining Block Ack Request sent from the peer
Value:

HT_BADecline=0

0: disable
1: enable

2.2.19 HT_DisallowTKIP

Description: Enable or disable 11N rate with 11N AP when cipher is TKIP or WEP
Value:

HT_DisallowTKIP=1

0: disable
1: enable

2.2.20 HT_STBC

Description: Enable or disable HT STBC
Value:

HT_STBC=0

0: disable
1: enable

2.2.21 VHT_STBC

Description: Enable or disable 11ac STBC
Value:

VHT_STBC=1

0: disable

1: enable

2.2.22 HT_LDPC

Description: Enable or disable HT LDPC
Value:

HT_LDPC=0

0: disable
1: enable

Note: MT76x2E/MT7615 only

2.2.23 VHT_LDPC

Description: Enable or disable 11ac LDPC
Value:

VHT_LDPC=1

0: disable
1: enable

Note: MT76x2E/MT7615 only

2.2.24 G_BAND_256QAM

Description: Enable or disable 256-QAM support for MT7615 2.4g
Value:

G_BAND_256QAM=1

0: disable
1: enable

2.2.25 VHT_BW_SIGNAL

Description: Enable or disable 11ac bandwidth signaling
Value:

VHT_BW_SIGNAL=0

0: disable
1: static
2: dynamic

2.2.26 HT_TxStream

Description: Configure the number of spatial streams for transmission
Value:

HT_TxStream=2

1~2: valid spatial streams

Note: 4ss is MT7615 only
The TX path settings in E2P offset 0x34 [7:4] has higher priority than HT_TxStream.

2.2.27 HT_RxStream

Description: Configure the number of spatial streams for reception
Value:

HT_RxStream=2

1~2: valid spatial streams

Note: 4ss is MT7615 only
The RX path settings in E2P offset 0x34 [3:0] has higher priority than HT_RxStream.

2.2.28 E2pAccessMode

Description: Configure the storage of EEPROM
Value:

E2pAccessMode=2

0: NONE
1: EFUSE mode
2: FLASH mode
~~3: EEPROM mode~~
4: BIN FILE mode

2.3 Advanced Profile Parameter

2.3.1 BeaconPeriod

Description: Beacon period (ms) configuration
Value:

BeaconPeriod=100

20 ~ 1024 (unit is in milli-seconds)

2.3.2 DtimPeriod

Description: DTIM period configuration and it stands for Delivery Traffic Indication Map
Value:

DtimPeriod=1

1~255 (unit is Beacon count)

2.3.3 FragThreshold

Description: Fragment threshold configuration
Value:

FragThreshold=2346

256~2346

2.3.4 RTSThreshold

Description: RTS threshold configuration
Value:

RTSThreshold=2347

1~2347

2.3.5 TxPower

Description: Configure transmission power in percentage
Value:

TxPower=100

1~100 (%)

Note: PERCENTAGEenable=1 is also required when using this function in MT7615, MT7915

91 ~ 100%, treat as 100% in terms of mW	
61 ~ 90%, treat as 75% in terms of mW	-1dBm
31 ~ 60%, treat as 50% in terms of mW	-3dBm
16 ~ 30%, treat as 25% in terms of mW	-6dBm
10 ~ 15%, treat as 12.5% in terms of mW	-9dBm
1 ~ 9 %, treat as MIN(~3%) in terms of mW	-12dBm

2.3.6 TxPreamble

Description: Tx preamble configuration
Value:

TxPreamble=1

0: Long preamble
1: Short preamble
2: Auto

2.3.7 TxBurst

Description: Enable or disable Tx Burst (Mediatek-proprietary acceleration method)
Value:

TxBurst=1

0: disable
1: enable

2.3.8 PktAggregate

Description: Enable or disable piggyback packet aggregation (Mediatek proprietary)
Value:

PktAggregate=0

0: disable
1: enable

2.3.9 ShortSlot

Description: Enable or disable short slot time (9us) for backward-compatibility with 11b
Value:

ShortSlot=1

0: disable
1: enable

2.3.10 MaxStaNum

Description: Configure the maximum number of station that could connect with this AP
Value:

Not support on MT7615/MT7915

2.3.11 MbssMaxStaNum

Description: Configure the maximum number of station that could connect with this AP (MT7615/MT7915)
Value:

MbssMaxStaNum=255

0: disable
1~255

2.3.12 AutoChannelSelect

Description: Configure Automatic Channel Selection Algorithm
Value:

AutoChannelSelect=1

0: Disable
1: Old CSA (AP count)
2: New CSA (CCA)
3: MT7615/MT7915 CSA (Busy time)

2.3.13 AutoChannelSkipList

Description: Configure channels you want to skip when Auto Channel Selection is enabled
Value:

AutoChannelSkipList=<channel_list>

Example:

<channel_list>=2;3;4;5;7;8;10;

2.3.14 ACSCheckTime

Description: Configuration of periodic check time for automatic channel selection
Value:

ACSCheckTime=1

0: Disable

Note: Unit is hour

2.3.15 HT_LinkAdapt

Decription: Enable or disable HT Link Adaptation Control
Value:

HT_LinkAdapt=0

0: disable
1: enable

2.3.16 HT_OpMode

Description: HT operation mode configuration
Value:

HT_OpMode=0

0: Mixed mode (MM)
1: Greenfield mode (GF)

2.3.17 HT_MpduDensity

Description: Minimum separation of MPDUs in an A-MPDU
Value:

HT_MpduDensity=4

0: no restriction
1: 1/4 µs
2: 1/2 µs
3: 1 µs
4: 2 µs
5: 4 µs
6: 8 µs
7: 16 µs

2.3.18 HT_BAWinSize

Description: Block Ack window size configuration
Value:

HT_BAWinSize=64

1~256

2.3.19 HT_MIMOPSMode

Description: Spatial Multiplexing (SM) power save mode configuration
Value:

HT_MIMOPSMode=3

0: Static
1: Dynamic

2: Reserved
3: Disable (AP behaves according to the capability announced by STA)

Note:
Please use HT_MIMOPSMode=3 to pass the TGn 4.2.28 Spatial Multiplexing Power Save Operation.

2.3.20 VHT_DisallowNonVHT

Description: Enable or disable the function of rejecting connection attempt from non-VHT STA
Value:

VHT_DisallowNonVHT=0

0: disable
1: enable

2.3.21 NoForwarding

Description: Enable or disable No-Packet-Forwarding within a BSSID
Value:

NoForwarding=0

0: disable
1: enable

2.3.22 NoForwardingBTNBSSID

Description: Enable or disable No-Packet-Forwarding between each BSSID
Value:

NoForwardingBTNBSSID=0

0: disable
1: enable

2.3.23 NoForwardingMBCast

Description: Enable or disable No-MC-BC-Packet-Forwarding within a BSSID
Value:

NoForwardingMBCast=0

0: disable
1: enable

2.3.24 HideSSID

Description: Enable or disable configuring an empty SSID
Value:

HideSSID=0

0: disable
1: enable

2.3.25 StationKeepAlive

Description: Enable or disable auto detection of aliveness of connected stations periodically
Value:

StationKeepAlive=0

0: disable
1~65535 seconds

2.3.26 VLANID

Description: VLAN ID configuration
Value:

VLANID=0

0: Disable

2.3.27 VLANPriority

Description: VLAN priority configuration
Value:

VLANPriority=0

0: Disable

2.3.28 EntryLifeCheck

Description: Configure how many consecutive failed Tx packets sent to a STA can be ignored before AP sends Deauth to it
Value:

EntryLifeCheck=20

1 ~ 65535

2.3.29 EtherTrafficBand

Description: Configure Ethernet packets binding with specific RF band
Value:

EtherTrafficBand=2G

2G: Ethernet packets bind with 2.4GHz
5G: Ethernet packets bind with 5GHz

Note: Forwarding Module should be also enabled

2.3.30 WirelessEvent

Description: Enable or disable sending wireless event to the system log
Value:

WirelessEvent=0

0: disable
1: enable

3 WLAN SoftAP Driver iwpriv Command

3.1 Set

[Syntax]
iwpriv ra0 set [parameters]=[Value]

Note: Execute one iwpriv/set command at a time.

3.1.1 All 1-to-1 command

You can check the definition of all commands listed here in the Profile section since they have one-to-one mapping and the terminology is completely identical.

3.1.1.1 SSID

3.1.1.2 WirelessMode

3.1.1.3 Channel

3.1.1.4 BeaconPeriod

3.1.1.5 DtimPeriod

3.1.1.6 FragThreshold

3.1.1.7 RTSThreshold

3.1.1.8 TxPower

3.1.1.9 TxPreamble

3.1.1.10 TxBurst

3.1.1.11 PktAggregate

3.1.1.12 ShortSlot

3.1.1.13 NoForwarding

3.1.1.14 NoForwardingBTNBSSID

3.1.1.15 NoForwardingMBCast

3.1.1.16 HideSSID

3.1.2 Debug

Description: Configure the printing level of debug message
Value:

iwpriv ra0 set Debug=5

0~5
0: OFF
1: ERROR
2: WARN
3: NOTICE
4: INFO
5: DEBUG

Value	Level	Description
0	OFF	Means disable the log and can't be used for log printing. Notes: Use MTWF_PRINT() to print the result of the iwpriv command.
1	ERROR	Error conditions. This is a fatal error. If not resolved, it will affect the normal operation of the function or system.
2	WARN	Warning conditions. This is a minor error. If not resolved, it will not affect the normal operation of the function or system.
3	**NOTICE**	Normal but significant condition. Output some important information. Such as station connection, channel switching and so on. However, these logs can't affect performance, can't print too frequently and too much. **NOTICE is the default level.**
4	INFO	Normal but not significant condition. Used for informational messages. Output some less important information.
5	DEBUG	Debug-level messages. Output some detailed information.

Note:

```
iwpriv ra0 set debug=?
        usage and current state:
          0:MISC(L3)      1:INIT(L3)       2:HW(L3)       3:FW(L3)
          4:HIF(L3)       5:FPGA(L3)       6:TEST(L3)     7:RA(L3)
          8:AP(L3)        9:CLIENT(L3)   10:TX(L3)        11:RX(L3)
        12:CFG(L3)      13:MLME(L3)    14:PROTO(L3)   15:SEC(L3)
        16:PS(L3)       17:POWER(L3)   18:COEX(L3)    19:P2P(L3)
        20:TOKEN(L3)  21:CMW(L3)       22:BF(L3)      23:CFG80211(L3)
        24:MLO(L3)

iwpriv ra0 set debug=3  =>  all CAT set NOTICE Level
```

iwpriv ra0 set debug=<dbg_lvl>:<cat>:<sub_cat>

- Ex: set SER log to DEBUG(5)
  iwpriv ra0 set debug=5:2:2

  Debug(5)
  DBG_CAT_HW(2)
  DBG_SUBCAT_SER(2)
  ※ define at include/common/debug.h

3.1.3 ResetCounter

Description: Reset all statistics counters
Value:

iwpriv ra0 set ResetCounter=1

3.1.4 PartialScan

Description: Configure scanning behavior of site survey
Value:

iwpriv ra0 set PartialScan=1

0: Full scan (scan would finish at once)
1: Partial scan (scan would be divided into multiple sub-scan)

3.1.5 SiteSurvey

Description: Manually trigger a site survey to scan all available channels
Value:

iwpriv ra0 set SiteSurvey=

Note:
Passive scan: “iwpriv ra0 set SiteSurvey=”
Active scan: “iwpriv ra0 set SiteSurvey=Target_SSID”

3.1.6 HtBw

Description: HT channel bandwidth configuration
Value:

iwpriv ra0 set HtBw=1

0: 20 MHz
1: 20/40 MHz

3.1.7 VhtBw

Description: 11ac channel bandwidth configuration
Value:

iwpriv ra0 set VhtBw=1

0: disable
1: 80M
2: 160M
3: 80M+80M

3.1.8 HtMcs

Description: Modulation and Coding Scheme (MCS) configuration
Value:

iwpriv ra0 set HtMcs=33

0 ~15, 32: Fix MCS rate for HT rate
33: Auto Rate Adaption, recommended

3.1.9 HtGi

Description: HT guard interval configuration
Value:

iwpriv ra0 set HtGi=1

0: Long GI
1: Short GI

3.1.10 HtStbc

Description: Enable or disable HT STBC
Value:

iwpriv ra0 set HtStbc=1

0: disable
1: enable

3.1.11 VhtStbc

Description: Enable or disable 11ac STBC
Value:

iwpriv ra0 set VhtStbc=1

0: disable

1: enable

3.1.12 HtOpMode

Description: HT operation mode configuration
Value:

iwpriv ra0 set HtOpMode=0

0: Mixed mode (MM)
1: Greenfield mode (GF)

3.1.13 HtExtcha

Description: Locate the 40MHz extension channel in combination with the main channel
Value:

iwpriv ra0 set HtExtcha=0

0: Below
1: Above

3.1.14 HtMpduDensity

Description: Minimum separation of MPDUs in an A-MPDU
Value:

iwpriv ra0 set HtMpduDensity=4

0: no restriction
1: 1/4 µs
2: 1/2 µs
3: 1 µs
4: 2 µs
5: 4 µs
6: 8 µs
7: 16 µs

3.1.15 HtRdg

Description: Enable or disable HT Reverse Direction Grant
Value:

iwpriv ra0 set HtRdg=1

0: disable
1: enable

3.1.16 HtAutoBa

Description: Enable or disable automatically building Block Ack session with the peer
Value:

iwpriv ra0 set HtAutoBa=1

0: disable
1: enable

3.1.17 BADecline

Description: Configure whether always declining Block Ack Request sent from the peer
Value:

iwpriv ra0 set BADecline=0

0: disable
1: enable

3.1.18 BASetup

Description: Add an Originator BA entry into the BA table manually
Value:

iwpriv ra0 set BASetup=00:0c:43:01:02:03-0

→ The six 2-digit hex-decimal numbers composes the STA MAC address
→ The seventh decimal number is the TID value

3.1.19 BAOriTearDown

Description: Remove an Originator BA entry from the BA table manually
Value:

iwpriv ra0 set BAOriTearDown=00:0c:43:01:02:03-0

→ The six 2-digit hex-decimal numbers composes the STA MAC address
→ The seventh decimal number is the TID value

3.1.20 BARecTearDown

Description: Remove an Recipient BA entry from the BA table manually
Value:

iwpriv ra0 set BARecTearDown=00:0c:43:01:02:03-0

→ The six 2-digit hex-decimal numbers composes the STA MAC address

→ The seventh decimal number is the TID value

3.1.21 HtAmsdu

Description: Enable or disable A-MSDU transmission
Value:

iwpriv ra0 set HtAmsdu=0

0: disable
1: enable

3.1.22 HtDisallowTKIP

Description: Enable or disable 11N rate with 11N AP when cipher is TKIP or WEP
Value:

iwpriv ra0 set HtDisallowTKIP=0

0: disable
1: enable

3.1.23 VhtBwSignal

Description: Enable or disable 11ac bandwidth signaling
Value:

iwpriv ra0 set VhtBwSignal=1

0: disable
1: static
2: dynamic

3.1.24 DisConnectSta

Description: Disconnect one specific connected STA
Value:

iwpriv ra0 set DisConnectSta=00:11:22:33:44:55

[MAC address]

3.1.25 DisConnectAllSta

Description: Disconnect all connected STAs
Value:

iwpriv ra0 set DisConnectAllSta=1

1: disconnect all STAs

3.1.26 CountryString

Description: Country string configuration
Value:

iwpriv ra0 set CountryString=TAIWAN

32 characters, ex:Taiwan, case insensitive

Note: Please refer to ISO3166 code list for other countries and can be found at http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html#sz

Item	Country Number	ISO Name	Country Name (CountryString)	Support 802.11A	802.11A Country Region	Support 802.11G	802.11G Country Region
	0	DB	Debug	Yes	A_BAND_REGION_7	Yes	G_BAND_REGION_5
	8	AL	ALBANIA	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	12	DZ	ALGERIA	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	32	AR	ARGENTINA	Yes	A_BAND_REGION_3	Yes	G_BAND_REGION_1
	51	AM	ARMENIA	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	36	AU	AUSTRALIA	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	40	AT	AUSTRIA	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	31	AZ	AZERBAIJAN	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	48	BH	BAHRAIN	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	112	BY	BELARUS	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	56	BE	BELGIUM	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	84	BZ	BELIZE	Yes	A_BAND_REGION_4	Yes	G_BAND_REGION_1
	68	BO	BOLIVIA	Yes	A_BAND_REGION_4	Yes	G_BAND_REGION_1
	76	BR	BRAZIL	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	96	BN	BRUNEI DARUSSALAM	Yes	A_BAND_REGION_4	Yes	G_BAND_REGION_1
	100	BG	BULGARIA	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	124	CA	CANADA	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_0
	152	CL	CHILE	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	156	CN	CHINA	Yes	A_BAND_REGION_4	Yes	G_BAND_REGION_1
	170	CO	COLOMBIA	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_0
	188	CR	COSTA RICA	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	191	HR	CROATIA	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	196	CY	CYPRUS	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	203	CZ	CZECH REPUBLIC	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	208	DK	DENMARK	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	214	DO	DOMINICAN REPUBLIC	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_0
	218	EC	ECUADOR	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	818	EG	EGYPT	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	222	SV	EL SALVADOR	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	233	EE	ESTONIA	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	246	FI	FINLAND	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	250	FR	FRANCE	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	268	GE	GEORGIA	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	276	DE	GERMANY	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	300	GR	GREECE	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	320	GT	GUATEMALA	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_0
	340	HN	HONDURAS	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	344	HK	HONG KONG	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	348	HU	HUNGARY	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	352	IS	ICELAND	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	356	IN	INDIA	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1

	360	ID	INDONESIA	Yes	A_BAND_REGION_4	Yes	G_BAND_REGION_1
	364	IR	IRAN	Yes	A_BAND_REGION_4	Yes	G_BAND_REGION_1
	372	IE	IRELAND	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	376	IL	ISRAEL	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	380	IT	ITALY	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	392	JP	JAPAN	Yes	A_BAND_REGION_9	Yes	G_BAND_REGION_1
	400	JO	JORDAN	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	398	KZ	KAZAKHSTAN	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	408	KP	KOREA DEMOCRATIC	Yes	A_BAND_REGION_5	Yes	G_BAND_REGION_1
	410	KR	KOREA REPUBLIC OF	Yes	A_BAND_REGION_5	Yes	G_BAND_REGION_1
	414	KW	KUWAIT	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	428	LV	LATVIA	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	422	LB	LEBANON	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	438	LI	LIECHTENSTEIN	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	440	LT	LITHUANIA	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	442	LU	LUXEMBOURG	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	446	MO	MACAU	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	807	MK	MACEDONIA	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	458	MY	MALAYSIA	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	484	MX	MEXICO	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_0
	492	MC	MONACO	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	504	MA	MOROCCO	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	528	NL	NETHERLANDS	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	554	NZ	NEW ZEALAND	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	578	NO	NORWAY	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_0
	512	OM	OMAN	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	586	PK	PAKISTAN	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	591	PA	PANAMA	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_0
	604	PE	PERU	Yes	A_BAND_REGION_4	Yes	G_BAND_REGION_1
	608	PH	PHILIPPINES	Yes	A_BAND_REGION_4	Yes	G_BAND_REGION_1
	616	PL	POLAND	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	620	PT	PORTUGAL	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	630	PR	PUERTO RICO	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_0
	634	QA	QATAR	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	642	RO	ROMANIA	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	643	RU	RUSSIA FEDERATION	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	682	SA	SAUDI ARABIA	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	702	SG	SINGAPORE	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	703	SK	SLOVAKIA	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	705	SI	SLOVENIA	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	710	ZA	SOUTH AFRICA	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	724	ES	SPAIN	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	752	SE	SWEDEN	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	756	CH	SWITZERLAND	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	760	SY	SYRIAN ARAB REPUBLIC	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	158	TW	TAIWAN	Yes	A_BAND_REGION_3	Yes	G_BAND_REGION_0
	764	TH	THAILAND	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	780	TT	TRINIDAD AND TOBAGO	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	788	TN	TUNISIA	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	792	TR	TURKEY	Yes	A_BAND_REGION_2	Yes	G_BAND_REGION_1
	804	UA	UKRAINE	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	784	AE	UNITED ARAB EMIRATES	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	826	GB	UNITED KINGDOM	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_1
	840	US	UNITED STATES	Yes	A_BAND_REGION_0	Yes	G_BAND_REGION_0
	858	UY	URUGUAY	Yes	A_BAND_REGION_5	Yes	G_BAND_REGION_1
	860	UZ	UZBEKISTAN	Yes	A_BAND_REGION_1	Yes	G_BAND_REGION_0
	862	VE	VENEZUELA	Yes	A_BAND_REGION_5	Yes	G_BAND_REGION_1
	704	VN	VIET NAM	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1
	887	YE	YEMEN	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1

	716	ZW	ZIMBABWE	No	A_BAND_REGION_0	Yes	G_BAND_REGION_1

3.1.27 AutoChannelSel

Description: Configure Automatic Channel Selection Algorithm
Value:

iwpriv ra0 set AutoChannelSel=3

0: Disable
1: Old CSA (AP count)
2: New CSA (CCA)
3: MT7615/MT7915 CSA (Busy time)

3.1.28 KickStaRssiLow

Description: Configure the weakest signal threshold that AP would disconnect the STA
Value:

iwpriv ra0 set KickStaRssiLow=0

0: Disable
0 ~ -100

3.1.29 AssocReqRssiThres

Description: Configure the weakest signal threshold that AP would reject the Association Request
Value:

iwpriv ra0 set AssocReqRssiThres=0

0: Disable
0 ~ -100

3.2 Show

You could use iwpriv ra0 show command to display general or specific information. As to specific information, you have to turn on the corresponding function in driver config.

[Format]
iwpriv ra0 show [parameter]

[Parameter list]
1. driverinfo - show driver version
2. stat - show statistics counter

3. stainfo - show MAC address of associated STAs
4. stacountinfo - show TRx byte count of associated STAs
5. stasecinfo - show security information of associated STAs
6. bainfo - show BlockAck information
7. connStatus - show AP-Client connection status
8. reptinfo - show MAC Repeater information
9. wdsinfo - show WDS link list
10. igmpinfo - show all entries in the IGMP Snooping Table
11. mbss - show MBSS PHY mode information
12. blockch - show DFS blocked channel list

[Example]
iwpriv ra0 show driverinfo
Driver version: 2.7.1.6

3.3 Others

3.3.1 stat

Description: Show WLAN statistics
Value:
iwpriv ra0 stat

Note:
You can use "iwpriv ra0 set ResetCounter=1" to reset statistics
Also, you can use the following command line shell script to get per-second statistics.
 # while [1]; do iwpriv ra0 set ResetCounter=1; sleep 1; iwpriv ra0 stat; done;

3.3.2 get_site_survey

Description: Show site survey result
Value:
iwpriv ra0 get_site_survey

Note: You need to use "iwpriv ra0 set SiteSurvey=" to collect information first

3.3.3 get_mac_table

Description: Show MAC addresses of connected stations
Value:
iwpriv ra0 get_mac_table

3.3.4 get_ba_table

Description: Show raw data of the BlockAck table
Value:

iwpriv ra0 get_ba_table

3.3.5 get_wsc_profile

Description: Show WPS profile information
Value:

iwpriv ra0 get_wsc_profile

3.3.6 e2p

Description: Read/Write EEPROM content
Value:

// Read
iwpriv ra0 e2p offset
//Read rage (the maximum displayed range is 1K bytes)
iwpriv ra0 e2p start:end
// Write
iwpriv ra0 e2p offset=value

Note:

offset = hexidecimal address
value = hexidecimal value (4 hexs)

Example:

```
# iwpriv ra0 e2p 0=7622
ra0      e2p:
[0x00]:7622
# iwpriv ra0 e2p 0
ra0      e2p:
[0x0000]:0x7622
iwpriv ra0 e2p 400:416
   [0x0400]:0000  [0x0402]:0000  [0x0404]:0000  [0x0406]:0000
   [0x0408]:0000  [0x040A]:0000  [0x040C]:0000  [0x040E]:0000
   [0x0410]:0000  [0x0412]:0000  [0x0414]:0000
```

4 MBSSID

The Multiple BSSID (MBSSID) function is a feature providing additional virtual WLANs which look like real WLANs to users. Its common application is to create one Main and several Guest Networks simultaneously. You may configure each BSSID with different settings.

4.1 How to Enable

Please turn on MBSS_SUPPORT in driver config.

We also suggest turn on NEW_MBSSID_MODE which changes how the driver creates extended MAC addresses for these virtual BSSID.

4.2 Profile Parameter

4.2.1 BssidNum

Description: Multiple BSSID number configuration
Value:

BssidNum=1

1~16

Note:
1. It depends on MBSS_SUPPORT
2. It should be placed before other configuration in the profile
3. 16-BSSID is supported only in new products (MT7612 & MT7615)

4.2.2 MacAddress

Description: Direct assignment of MAC address
Value:

MacAddress=00:0c:43:11:22:33

Note:
This is only supported in MT7615 and you have to take care of the address confliction problem on your own if using this parameter to assign a MAC address to your device. As to other BSSID, you can use MacAddress1 ~ MacAddress15 to configure the MAC address assignment.

Example: BssidNum=4
If you want to do the following assignment,

ra0 00:0c:43:11:22:33
ra1 00:0c:43:11:22:34
ra2 00:0c:43:11:22:35
ra3 00:0c:43:11:22:36

then you can use the following configuration in your profile.

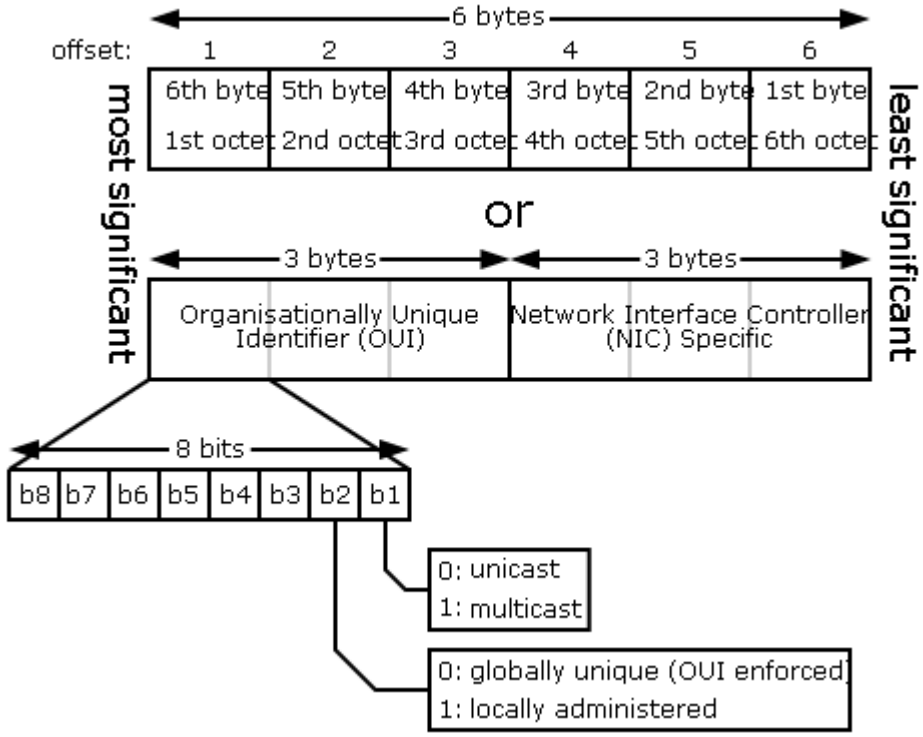
MacAddress=00:0c:43:11:22:33
MacAddress1=00:0c:43:11:22:34
MacAddress2=00:0c:43:11:22:35
MacAddress3=00:0c:43:11:22:36

MT7615 would use Enhanced New MBSSID Mode by default if you do not want to use MacAddress.

4.3 Important Note

4.3.1 MAC Address Format

The following MAC address format figure is from http://en.wikipedia.org/wiki/MAC_address and all subsequent discussion is based on this format.



4.3.2 Old MBSSID Mode

As to main BSSID, **the 1st byte** of its MAC address should be:

- Multiple of 2 for 2-BSSID
- Multiple of 4 for 4-BSSID
- Multiple of 8 for 8-BSSID

Taking BssidNum=4 for example, address extension would be done on 1st byte.

- ra0: 00:0c:43:00:00:0**0** 00 is multiple of 4
- ra1: 00:0c:43:00:00:0**1** 01 comes from (1st byte 0x00) + 0x01
- ra2: 00:0c:43:00:00:0**2** 02 comes from (1st byte 0x00) + 0x02
- ra3: 00:0c:43:00:00:0**3** 03 comes from (1st byte 0x00) + 0x03

Other possible address extension:

Multiple of 4	1st BSSID	2nd BSSID	3rd BSSID	4th BSSID
0x00	00-0C-43-DD-EE-F0	00-0C-43-DD-EE-F1	00-0C-43-DD-EE-F2	00-0C-43-DD-EE-F3
0x04	00-0C-43-DD-EE-F4	00-0C-43-DD-EE-F5	00-0C-43-DD-EE-F6	00-0C-43-DD-EE-F7
0x08	00-0C-43-DD-EE-F8	00-0C-43-DD-EE-F9	00-0C-43-DD-EE-FA	00-0C-43-DD-EE-FB
0x0C	00-0C-43-DD-EE-FC	00-0C-43-DD-EE-FD	00-0C-43-DD-EE-FE	00-0C-43-DD-EE-FF

Please be noted that all these MAC addresses should be reserved because they are global MAC addresses.

4.3.3 New MBSSID Mode

Since there is a MAC address reservation problem in the old MBSSID mode, we provide the new MBSSID mode which will utilize **b2 of 6th byte** of a virtual MAC address to claim it as locally administered. Address extension would be done on 6th byte. This is supported in 5-series products.

Taking BssidNum=4 for example:

- ra0: 0**0**:0c:43:00:00:00
- ra1: 0**2**:0c:43:00:00:00 0**2** comes from (6th byte 0x00 | b'000000**1**0)
- ra2: 0**6**:0c:43:00:00:00 0**6** comes from (6th byte 0x00 | b'0000**01**10)
- ra3: 0**a**:0c:43:00:00:00 0**a** comes from (6th byte 0x00 | b'0000**10**10)

4.3.4 Enhanced New MBSSID Mode

The enhanced new MBSSID mode removes the restriction of using the 6th byte since OUI (Consists of 6th, 5th, 4th bytes) is not controllable. Local Administration bit would be turned on and address extension would be done on 3rd byte. The extension algorithm is **(3rd Byte & MacMSK) + (idx)**. BssidNum will affect MacMSK. This is supported only in new 7-series products and will be turned on by default.

```
if (BssidNum <= 2)          { MacMSK  = b'1111111 0;}
else if (BssidNum <= 4)          { MacMSK  = b'111111 00;}
else if (BssidNum <= 8)          { MacMSK  = b'111110 00;}
```

else if (BssidNum <= 16) { MacMSK = b'11110000;}

Taking BssidNum=4 for example:

- ra0: 00:0c:43:0**0**:00:00
- ra1: 02:0c:43:0**0**:00:00 00 comes from (3rd byte 0x00 & 0xfc) + 0x00
- ra2: 02:0c:43:0**1**:00:00 01 comes from (3rd byte 0x00 & 0xfc) + 0x01
- ra3: 02:0c:43:0**2**:00:00 02 comes from (3rd byte 0x00 & 0xfc) + 0x02

MT7603, MT7628 and MT7615 make a different policy which uses **first 4 bits** of 3rd byte to do address extension. The extension algorithm is **(3rd Byte & MacMSK) + (idx << 4)**.

if (BssidNum <= 2) { MacMSK = b'11101111;}
else if (BssidNum <= 4) { MacMSK = b'11001111;}
else if (BssidNum <= 8) { MacMSK = b'10001111;}
else if (BssidNum <= 16) { MacMSK = b'00001111;}

Taking BssidNum=4 for example:

- ra0: 00:0c:43:**0**0:00:00
- ra1: 02:0c:43:**1**0:00:00 10 comes from (3rd byte 0x00 & 0xcf) + (0x01 << 4)
- ra2: 02:0c:43:**2**0:00:00 20 comes from (3rd byte 0x00 & 0xcf) + (0x02 << 4)
- ra3: 02:0c:43:**3**0:00:00 30 comes from (3rd byte 0x00 & 0xcf) + (0x03 << 4)

4.3.5 Address Confliction Problem

In this section, we'll explain the address conflication problem.
Suppose we have four DUTs with the following global MAC addresses.

DUT-A: 00:0c:43:10:22:33
DUT-B: 00:0c:43:11:22:33
DUT-C: 00:0c:43:12:22:33
DUT-D: 00:0c:43:13:22:33

Each DUT turns on MBSSID and configures its BssidNum=4. As a result, you will get the following total 16 MAC addresses.

	1st BSSID	2nd BSSID	3rd BSSID	4th BSSID
DUT-A	00:0c:43:10:22:33	02:0c:43:11:22:33	02:0c:43:12:22:33	02:0c:43:13:22:33
DUT-B	00:0c:43:11:22:33	02:0c:43:11:22:33	02:0c:43:12:22:33	02:0c:43:13:22:33
DUT-C	00:0c:43:12:22:33	02:0c:43:11:22:33	02:0c:43:12:22:33	02:0c:43:13:22:33
DUT-D	00:0c:43:13:22:33	02:0c:43:11:22:33	02:0c:43:12:22:33	02:0c:43:13:22:33

The 2nd, 3rd and 4th BSSID are exactly identical for these DUTs. So, the address conflict problem does exist but the conflicting rate is extremely low. Using local MAC address as BSSID, this problem is inevitable.

4.4 Configuration

BssidNum can be configured only through profile and you must restart the interface to make it to work. Other parameters can be configured dynamically through iwpriv command per interface. MBSSID-supported parameters are SSID, AuthMode, EncrypType, WPAPSK, etc.

4.4.1 Example

BssidNum=4
SSID=SSID_A;SSID_B;SSID_C;SSID_D
AuthMode=OPEN;SHARED;WPAPSK;WPA2PSK
EncrypType=NONE;WEP;TKIP;AES

5 WPS

Wi-Fi Protected Setup (WPS) also known as Wi-Fi Simple Configuration (WSC) is a standard feature which simplifies the process of setting up protected connections for the various Wi-Fi devices connecting to APs. Without WPS, a user should manually configure SSID and security to create a WLAN. Unfortunately, most users do not know how it works and the configuration process becomes nightmare to them.

5.1 WPS Scenarios

There are two kinds of WPS scenarios. One is to set up a new WLAN and the other is to add new member devices to an existed WLAN. **Initial WLAN Setup** is that a user must do after buying a new AP device. After finishing initial WLAN setup, AP is ready to accept connection requests from client devices and here comes **Adding Member Devices**. The following list decribes all the possible scenarios when using WPS. The terminology used here would be introduced in the next section.

- Initial WLAN Setup
  - Standalone AP with a built-in Registrar
    - WPS is not needed in this case
  - AP and an External Registrar
    - EAP-based setup of External Wireless Registrar
      - [AP as Enrollee] --- EAP --- [Wireless Registrar]
    - UPnP-based setup of External Wired Registrar
      - [AP as Enrollee] --- UPnP --- [Wired Registrar]

- Adding Member Devices
  - In-band setup using a standalone AP/Registrar
    - [STA Enrollee] --- EAP --- [AP/Registrar]
  - In-band setup using an External Registrar
    - UPnP-based setup of External Wireless Registrar
      - [STA Enrollee] --- EAP --- [AP] --- UPnP --- [Wireless Registrar]
    - UPnP-based setup of External Wired Registrar
      - [STA Enrollee] --- EAP --- [AP] --- UPnP --- [Wired Registrar]

*EAP stands for Extensible Authentication Protcol
https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
*UPnP stands for Universal Plug and Play
https://en.wikipedia.org/wiki/Universal_Plug_and_Play

5.2 Architectural Overview

This section presents high-level description of the Wi-Fi Simple Configuration architecture. Most material is taken directly from the WSC specification. In the following figure, you can see that there are three logical components involved in WSC: the Registrar, the access point (AP), and the Enrollee.

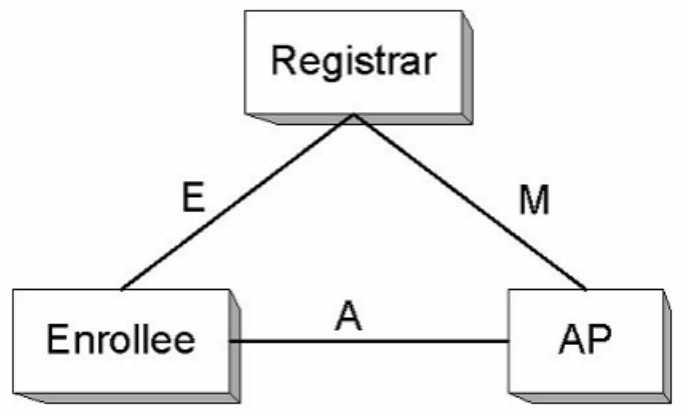


Figure 1: Components and Interfaces

[Component]

The **Enrollee** is a device seeking to join a WLAN domain. Once an Enrollee obtains a valid credential, it becomes a member.

The **Registrar** is an entity with the authority to issue and revoke domain credentials. A registrar may be integrated into an AP, or it may be separate from the AP.

The **AP** is an infrastructure mode 802.11 Access Point. We also call it **Proxy**.

[Interface]

Interface E is logically located between the Enrollee and the Registrar and its purpose is to enable the Registrar to discover and issue WLAN credentials to the Enrollee.

Interface M is between the AP and the Registrar and it enables an external Registrar to manage a WSC AP.

Interface A is between the Enrollee and the AP and it enables discovery of the WSC WLAN and communication between the Enrollee and IP-only Registrars.

5.3 Profile Parameter

5.3.1 WscConfMode

Description: Configure WPS role (bitwise OR)
Value:

WscConfMode=7

b'000: 0 Disable
b'001: 1 Enrollee
b'010: 2 Proxy
b'100: 4 Registrar

5.3.2 WscConfStatus

Description: Configure WPS state
Value:

WscConfStatus=1

1: AP is unconfigured
2: AP is configured

5.3.3 WscConfMethods

Description: Configure the configuration methods which Enrollee or Registrar supports
Value:

WscConfMethods=238c

Note:

Hexadecimal value only.
0x238c = 0x2008 | 0x0280 | 0x0100 | 0x0004 //Bitwise-OR all values which DUT supports
Virtual Display PIN + Virtual Push Button + Keypad + Label PIN

Config Method	Value
Label PIN	0x0004
External NFC Token	0x0010
Integrated NFC Token	0x0020
NFC Interface	0x0040
Keypad	0x0100
Virtual Push Button	0x0280
Physical Push Button	0x0480
Virtual Display PIN	0x2008
Physical Display PIN	0x4008

5.3.4 WscKeyASCII

Description: Choose the format/length of a generated key for an un-configured AP (internal registrar)
Value:

WscKeyASCII=0

0: Hex (64-bytes)
1: ASCII (Random length)
8 ~ 63: ASCII length

5.3.5 WscSecurityMode

Description: Configure the security mode which AP would use when being configured
Value:

WscSecurityMode=0

0: WPA2PSK AES
1: WPA2PSK TKIP
2: WPAPSK AES
3: WPAPSK TKIP

5.3.6 Wsc4digitPinCode

Description: Configure whether to use 4-digit PIN code
Value:

Wsc4digitPinCode=1

0: 8-digit PIN code
1: 4-digit PIN code

5.3.7 WscVendorPinCode

Description: Configure a fixed PIN code which AP would use as an Enrollee
Value:

WscVendorPinCode=[xxxx|yyyyyyyy]

xxxx is a 4-digit PIN code
yyyyyyyy is a 8-digit PIN code

5.3.8 WscDefaultSSID0

Description: Configure the SSID which AP would use after being configured
Value:

WscDefaultSSID0=SSID

1~32 characters

5.3.9 WscV2Support

Description: Enable or disable WPS v2.0 support
Value:

WscV2Support=1

0: disable
1: enable

5.3.10 WscManufacturer

Description: WPS manufacturer string
Value:

WscManufacturer=

Less than 64 characters

5.3.11 WscModelName

Description: WPS model name string
Value:

WscModelName=

Less than 32 characters

5.3.12 WscDeviceName

Description: WPS device name string
Value:

WscDeviceName=

Less than 32 characters

5.3.13 WscModelNumber

Description: WPS model number string
Value:

WscModelNumber=

Less than 32 characters

5.3.14 WscSerialNumber

Description: WPS serial number string
Value:

WscSerialNumber=

Less than 32 characters

5.4 iwpriv Command

5.4.1 WscConfMode

Description: Configure WPS role (bitwise OR)
Value:

iwpriv ra0 set WscConfMode=7

b’000: 0 Disable
b’001: 1 Enrollee
b’010: 2 Proxy
b’100: 4 Registrar

5.4.2 WscConfStatus

Description: Configure WPS state
Value:

iwpriv ra0 set WscConfStatus=1

1: AP is unconfigured
2: AP is configured

5.4.3 WscMode

Description: Configure WPS mode
Value:

iwpriv ra0 set WscMode=1

1: PIN Mode
2: PBC Mode

5.4.4 WscGetConf

Description: Trigger WPS action
Value:

iwpriv ra0 set WscGetConf=1

5.4.5 WscStop

Description: Stop WPS process
Value:

iwpriv ra0 set WscStop=1

5.4.6 WscPinCode

Description: Enter Enrollee's PIN code which AP with built-in Registrar would use
Value:

iwpriv ra0 WscPinCode=[xxxx|yyyyyyyy]

xxxx is a 4-digit PIN code
yyyyyyyy is a 8-digit PIN code

5.4.7 WscGenPinCode

Description: Generate a random PIN code for DUT as an Enrollee
Value:

iwpriv ra0 set WscGenPinCode=1

Note:

PIN code can be either 4-digit or 8-digit depending on Wsc4digitPinCode
One of the digits in the 8-digit PIN code is used as a checksum

5.4.8 WscVendorPinCode

Description: Configure an assigned PIN code for DUT as an Enrollee
Value:

iwpriv ra0 set WscVendorPinCode=[xxxx|yyyyyyyy]

xxxx is a 4-digit PIN code
yyyyyyyy is a 8-digit PIN code

5.4.9 WscSecurityMode

Description: Configure the security mode which AP would use when being configured
Value:

iwpriv ra0 set WscSecurityMode=0

0: WPA2PSK AES

1: WPA2PSK TKIP
2: WPAPSK AES
3: WPAPSK TKIP

5.4.10 WscOOB

Description: Reset WPS AP to the OOB (out-of-box) state
Value:

iwpriv ra0 set WscOOB=1

Note:

<OOB settings>
SSID MediatekInitailAP**xxxxxx** (last 3 bytes of ra0 MAC 00:0c:43:**xx:xx:xx**)
AuthMode WPA2PSK
EncrypType AES
WPAPSK MediatekInitialAPxx1234
WscConfStatus 1 (AP is unconfigured)

5.4.11 WscStatus

Description: Get current WPS status
Value:

iwpriv ra0 set WscStatus=0

0: Not Used
1: Idle
2: WSC Process Fail
3: Start WSC Process
4: Received EAPOL-Start
5: Sending EAP-Req (ID)
6: Received EAP-Rsp (ID)
7: Received EAP-Req with wrong WSC SMI Vendor ID
8: Received EAP-Req with wrong WSC Vendor Type
9: Sending EAP-Req (WSC_START)
10: Sending M1
11: Received M1
12: Sending M2
13: Received M2
14: Received M2D
15: Sending M3
16: Received M3
17: Sending M4
18: Received M4
19: Sending M5

20: Received M5
21: Sending M6
22: Received M6
23: Sending M7
24: Received M7
25: Sending M8
26: Received M8
27: Processing EAP Response (ACK)
28: Processing EAP Request (Done)
29: Processing EAP Response (Done)
30: Sending EAP-Fail
31: WSC_ERROR_HASH_FAIL
32: WSC_ERROR_HMAC_FAIL
33: WSC_ERROR_DEV_PWD_AUTH_FAIL
34: WSC configured

5.4.12 WscMultiByteCheck

Description: Enable or disable multi-byte check
Value:

iwpriv ra0 set WscMultiByteCheck=0

0: disable
1: enable

5.4.13 WscVersion

Description: Set WPS support version
Value:

iwpriv ra0 set WscVersion=10

0x10: Hexadecimal

5.4.14 WscVersion2

Description: Set WPS version of V2 support
Value:

iwpriv ra0 set WscVersion2=20

0x20: Hexadecimal

5.4.15 WscV2Support

Description: Enable or disable WPS V2.0 support
Value:

iwpriv ra0 WscV2Support=1

0: disable
1: enable

5.4.16 WscFragment

Description: Enable or disable WPS fragmentation
Value:

iwpriv ra0 WscFragment=0

0: disable
1: enable

5.4.17 WscFragmentSize

Description: Configure the size of WPS fragmentation
Value:

iwpriv ra0 set WscFragmentSize=128

128~300

5.4.18 WscSetupLock

Description: Enable or disable WPS setup lock
Value:

iwpriv ra0 set WscSetupLock=1

0: disable
1: enable

5.4.19 WscSetupLockTime

Description: Configure WPS setup lock time
Value:

iwpriv ra0 set WscSetupLockTime=0

0: lock forever
Unit: minute

5.4.20 WscMaxPinAttack

Description: Configure WPS PIN attack MAX time
Value:

iwpirv ra0 set WscMaxPinAttack=10

0: disable
1-10

5.4.21 WscExtraTlvTag

Description: Add extra TLV tag to Beacon, probe response and WSC EAP messages
Value:

iwpriv ra0 set WscExtraTlvTag=1088

Hex value: 0000 ~ FFFF
Example: 1088

5.4.22 WscExtraTlvType

Description: Define data format of extra TLV value
Value:

iwpriv ra0 set WscExtraTlvType=1

0: ASCII string
1: Hex string

5.4.23 WscExtraTlvData

Description: Add extra TLV data to Beacon, probe response and WSC EAP messages
Value:

iwpriv ra0 set WscExtraTlvData=

ASCII string or Hex string

5.5 WPS Scenario in Practice

5.5.1 Initial WLAN setup with an External Registrar

[Unconfigured AP] ← EAP → [Wireless Registrar]
[Unconfigured AP] ← UPnP → [Wired Registrar]

Please make sure that the UPnP deamon has been lanuched in AP since UPnP is the protocol used to communicate with Wired Registrar. After WPS registration succeeds, the AP turns into Configured state and will work as a Proxy forwarding EAP and UPnP messages between Enrolle and Registrar.

- **AP Enrollee** command sequence

- PIN
  - iwpriv ra0 set WscConfMode=1
  - iwpriv ra0 set WscConfStatus=1
  - iwpriv ra0 set WscMode=1
  - iwpriv ra0 set WscGenPinCode=1 (Optional if PIN code is fixed)
  - iwpriv ra0 set WscGetConf=1
- PBC
  - iwpriv ra0 set WscConfMode=1
  - iwpriv ra0 set WscConfStatus=1
  - iwpriv ra0 set WscMode=2
  - iwpriv ra0 set WscGetConf=1

5.5.2 Adding a member device using a standalone AP/Registrar

[STA] ← EAP → [AP/Registrar]

In this case, AP within a builtin Registrar could directly respond to the STA Enrollee.

- **AP Registrar** command sequence
  - PIN
    - iwpriv ra0 set WscConfMode=7
    - iwpriv ra0 set WscPinCode=xxxxxxxx (Mandatory, xxxxxxxx is Enrollee's PIN code)
    - iwpriv ra0 set WscMode=1
    - iwpriv ra0 set WscGetConf=1
  - PBC
    - iwpriv ra0 set WscConfMode=7
    - iwpriv ra0 set WscMode=2
    - iwpriv ra0 set WscGetConf=1

5.5.3 Adding a member device using an External Wired Registrar

[STA] ← EAP → [AP] ← UPnP → [External Registrar]

In this case, AP just plays as a Proxy and almost does nothing.

- PIN
  - Registrar side
    - When prompted for the enrollee's PIN, enter it
    - The registration process will begin, and the application will display the result of the process on completion
  - Enrollee side
    - Trigger PIN process
    - The application will display the result of the process on completion
- PBC

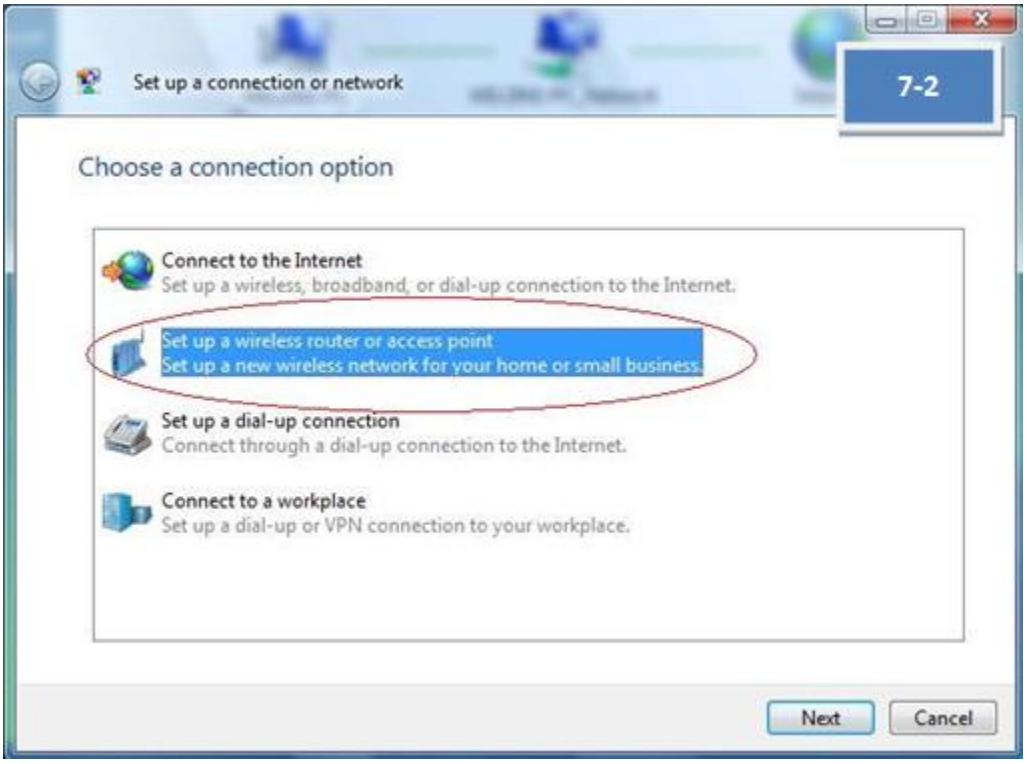
- Registrar side
  - Select "push-button"
  - The registration process will begin, and the application will display the result of the process on completion
- Enrollee side
  - Trigger PBC process
  - The application will display the result of the process on completion

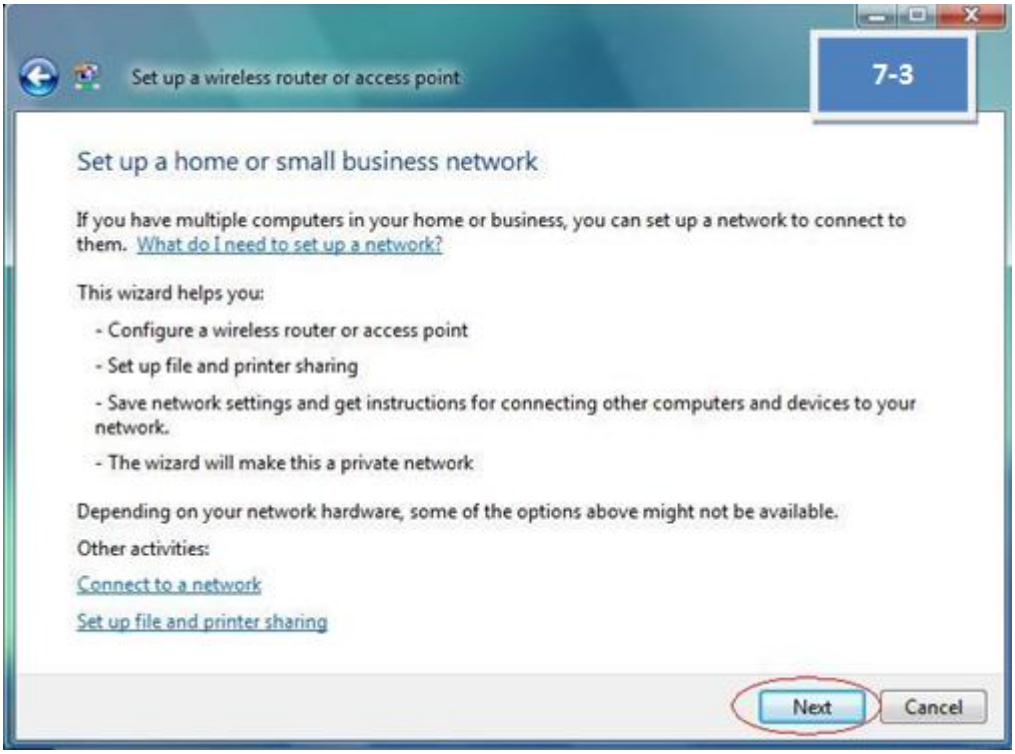
5.6 A Real Example

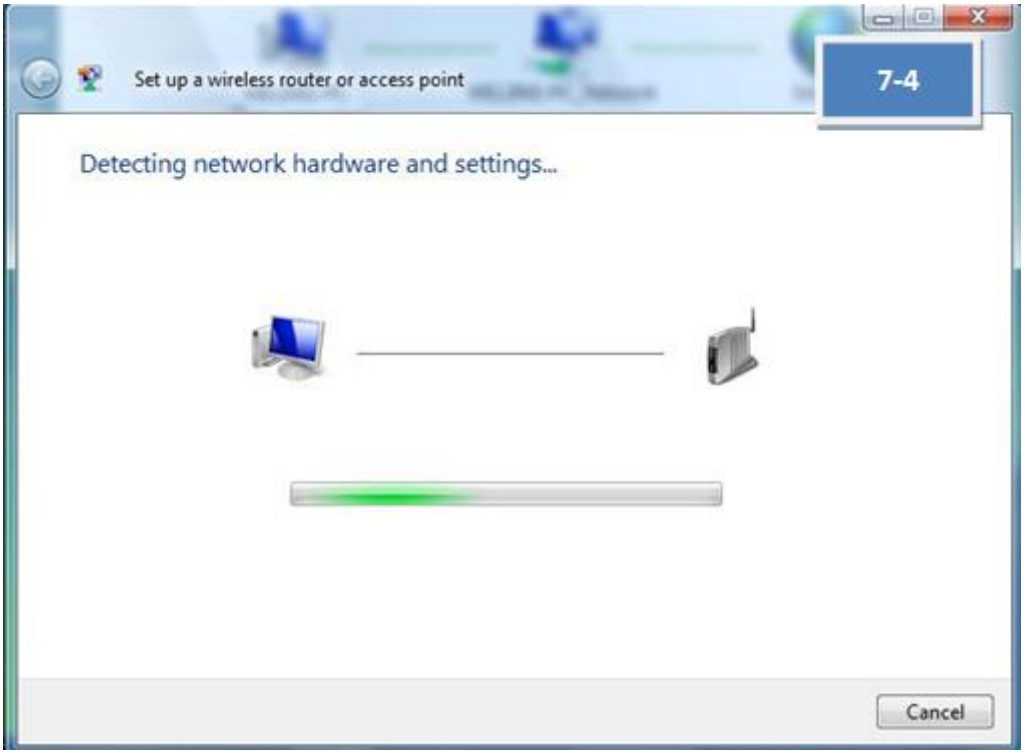
5.6.1 Initial WLAN setup with a wired external Registrar in PIN mode

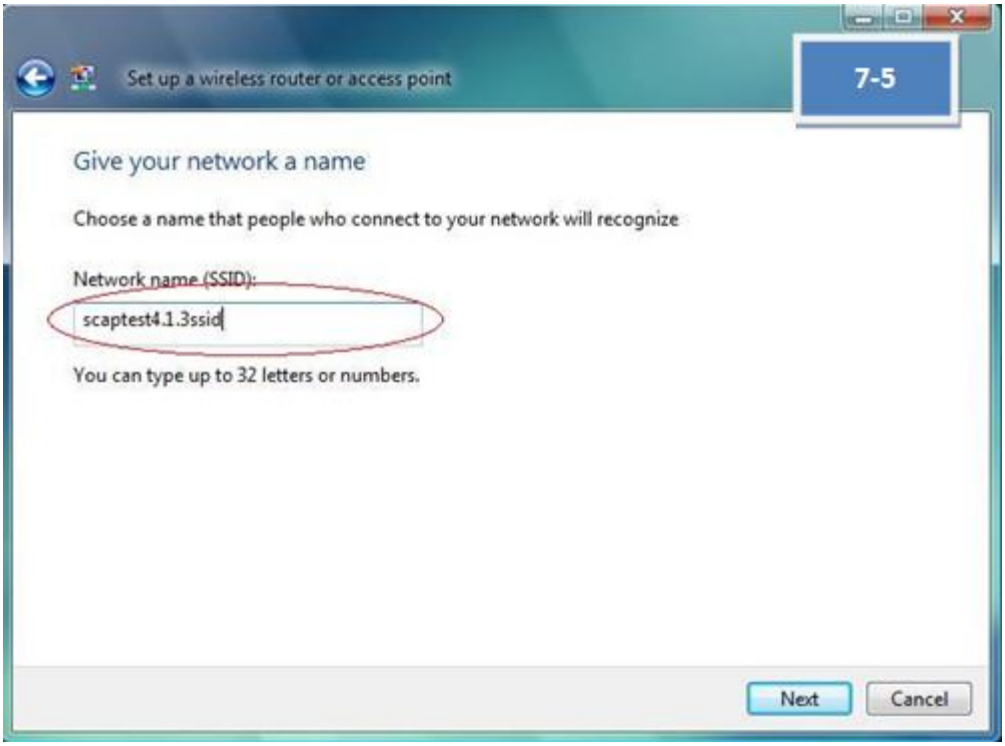
1. [AP] – Power on
2. [AP] – Connect the Ethernet cable between AP and external Registrar (Windows) and make sure you can ping AP from external Registrar first!
3. [AP] – Execute "**iwpriv ra0 set WscConfMode=1**" to configure AP as an Enrollee
4. [AP] – Execute "**iwpriv ra0 set WscConfStatus=1**" to configured AP to un-configured state
5. [AP] – Execute "**iwpriv ra0 set WscMode=1**" to run in PIN mode
6. [AP] – Execute "**iwpriv ra0 set WscGetConf=1**" to trigger WPS process
7. [ER] – The external Registrar on Microsoft STA will be configured with the new parameters (SSID = "scaptest4.1.3ssid" and WPA2PSK="scaptest4.1.3psk")
8. [ER] – Read AP PIN code from console and enter it at the ER on Microsoft STA
9. [STA] – Manually configure a STA with the new credential parameters (SSID="scaptest4.1.3ssid" and WPA2PSK passphrase="scaptest4.1.3psk")
10. [STA] – Check whether ping can reach the AP

As to details of step-7, please refer to the following figures from [7-1] to [7-6].

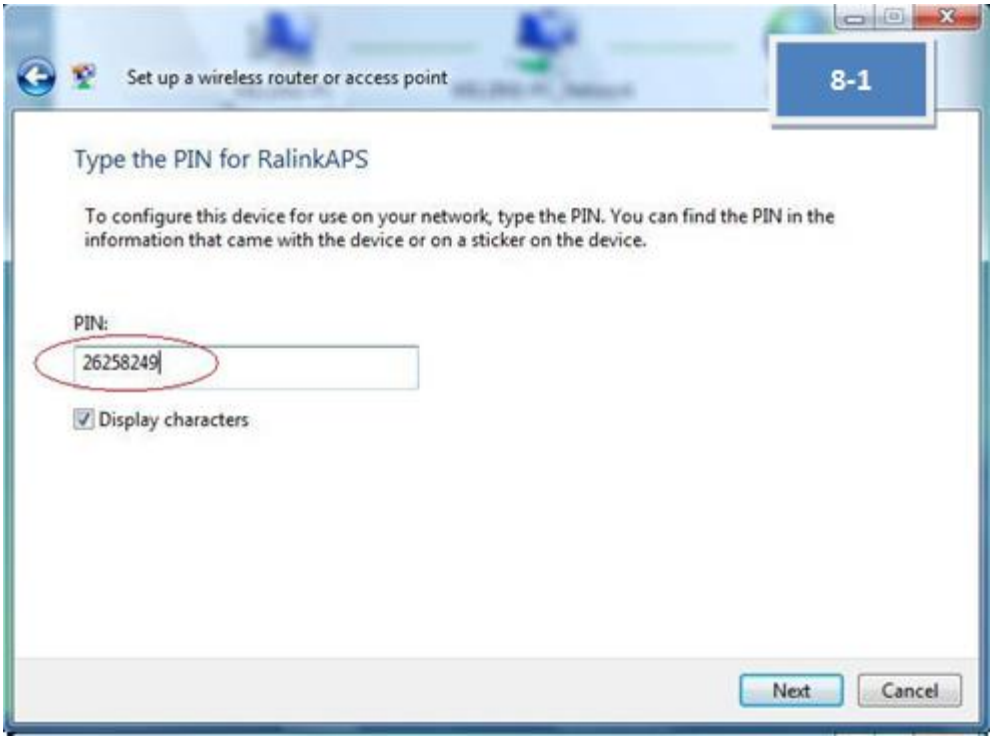


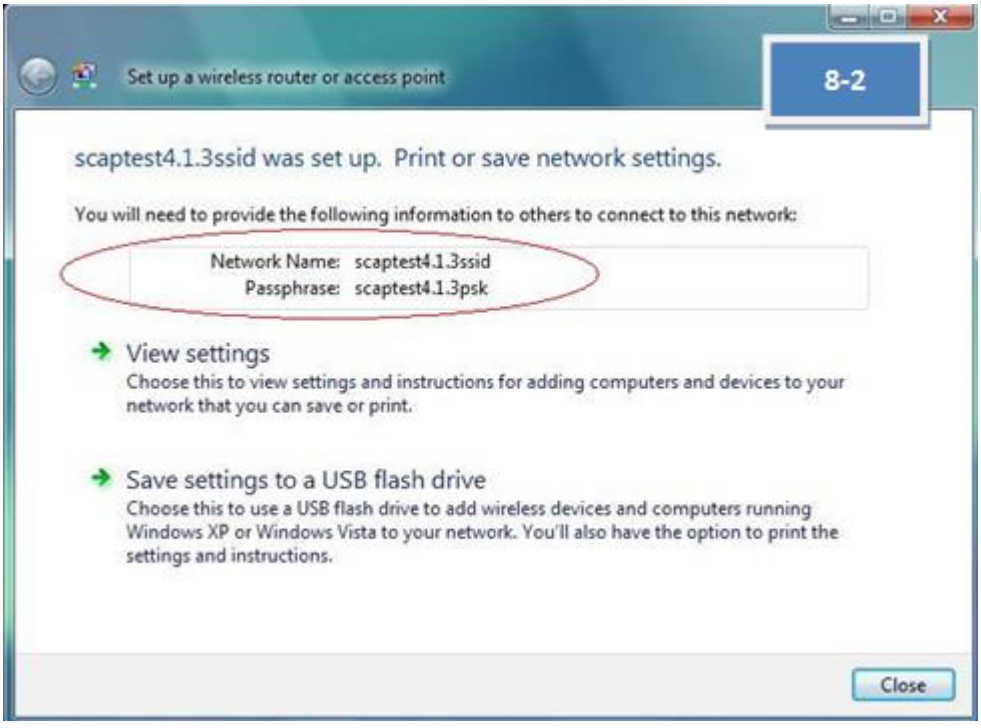






As to details of step-8, please refer to the following figures from [8-1] to [8-2].



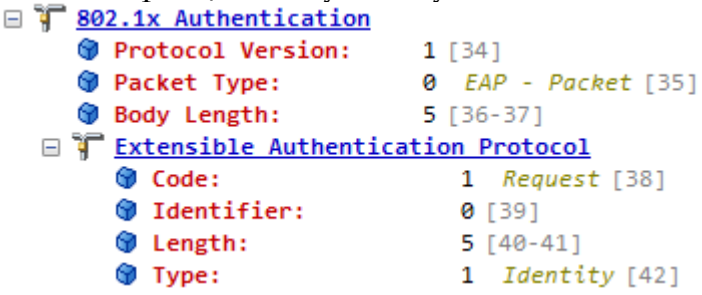


5.7 Notes for WPS

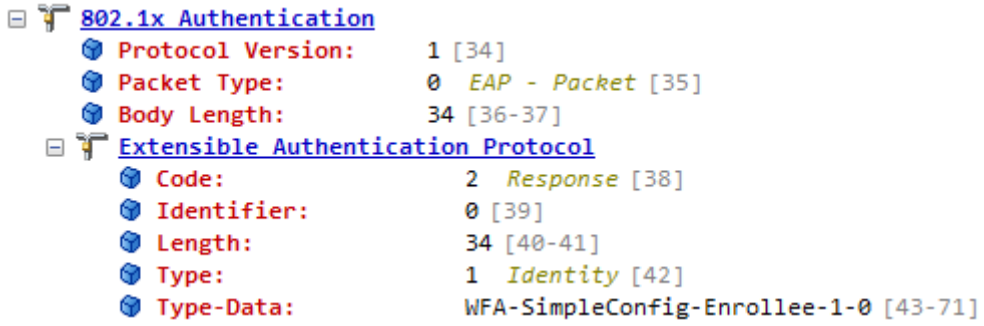
5.7.1 How to know WPS AP serves as Registrar, Enrollee or Proxy

It depends on the content of EAP-Response/Identity sent from WPS STA. You can check this in the packet trace recorded by a wireless sniffer. The following snapshots provide an example.

<EAP-Request/Identity sent by WPS AP>



<EAP-Response/Identity sent by WPS STA>



- When WPS STA responds with identity being "WFA-SimpleConfig-**Enrollee**-1-0" WPS AP serves as Registrar. If AP does not trigger WPS, WPS AP serves as proxy only.

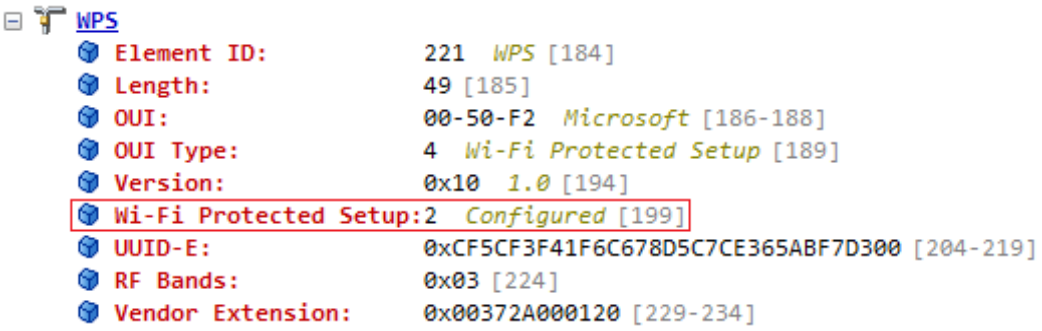
- When WPS STA responds with identity being "WFA-SimpleConfig-**Registrar**-1-0"
  WPS AP serves as Enrollee.

5.7.2 How to Know WPS AP PIN Code

You can use IOCTL to make a query with OID **RT_OID_WSC_PIN_CODE** to retrieve AP PIN Code directly. In case of MT7615, you can use "**iwpriv ra0 show WscPin**" to dump the PIN code.

5.7.3 WPS Configuration Status

The WPS attribute "Simple Configuration (SC) State" in WPS IEs (contained in beacon and probe response) indicates whether an AP DUT is configured.



If an AP is shipped from the factory in an un-configured state (SC State is 0x01), then the AP must change to the configured state (SC State is 0x02) if any of the following occurs.

1. Automatic configuration via WPS by an external Registrar

   The AP sends the WSC_Done message in the External Registrar configuration process.

2. Automatic configuration via WPS by an internal Registrar

   The AP receives the WSC_Done response in the Enrollee Registration Process from the first Enrollee. The internal registrar waits until successful completion of the protocol before applying the automatically generated credentials to avoid an accidental transition from un-configured to configured one in the case that a neighbouring device tries to run WSC before the real enrollee, but fails. A failed attempt does not change the configuration of the AP, nor the Simple Config State.

3. Manual configuration by an user

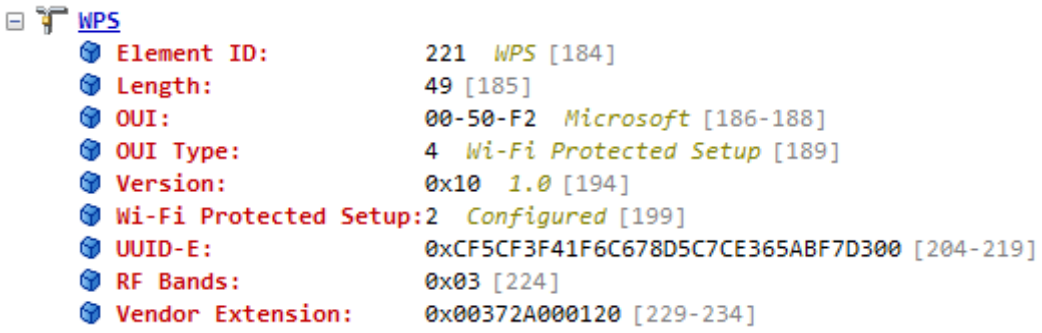
   One user manually configures the AP using whatever interface(s) it provides to modify any one of the followings:
   - SSID
   - Encryption method
   - Authentication method
   - Any key or pass phrase

If an AP is shipped from the factory in an un-configured state (SC State 0x01), then a Factory Reset must revert the Simple Config State to be un-configured. If an AP is shipped from the factory pre-configured with WPA2PSK and a randomly generated key, the SC State must be 'Configured' (0x02) so as to prevent an external Registrar from overwriting the default factory settings. A factory reset must restore the DUT to the same configuration as what it was when shipped.

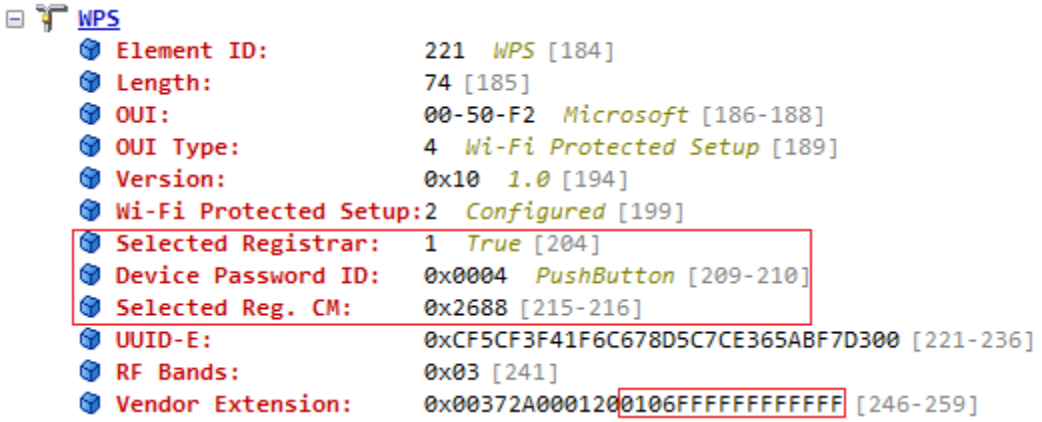
5.7.4 How to Know WPS process has been triggered

You can check the WPS IE in beacons sent by the AP to differentiate whether a WPS process is ongoing.

<Normal>



<Ongoing> The key is that Selected Registrar should be TRUE.



5.8 UPnP Daemon HowTo

In our reference design, we use miniupnpd to work as a daemon for WPS proxy function. The path in our SDK is **source/user/miniupnpd-1.6**. You can study the "**miniupnpd.sh**" inside to write your own startup script. If you want to run it with MBSSID, you have to launch multiple miniupnpds for each BSSID.

[Example]
miniupnpd -m 1 -I ra0 -P /var/run/miniupnpd.ra0 -i $WAN_IF -a $LAN_IPADDR -n 7777
miniupnpd -m 1 -I rai0 -P /var/run/miniupnpd.rai0 -i $WAN_IF -a $LAN_IPADDR -n 8888

6 Protection Mechanism

Protection in Wi-Fi is one kind of backward-compatibile mechanism to make sure that the operation of old devices would not be affected by new devices and vice versa. Since the Wi-Fi technology evolves from the legacy CCK to the VHT, protection mechanism becomes complex and mandatory.

BG protection means that an 11g station should be aware that a legacy 11b station would exist and send frames with protection, like RTS/CTS or CTS-to-Self, enabled to prevent interference from happening. Mediatek provides a parameter named BGProtection to configure the above-mentioned behavior. When configuring BGProtection=0 and DisableOLBC=0, AP would automatically turn on the protection when either an 11b station connected to it or receiving Beacon/Probe Response frames from an 11b AP working nearby. When there is no 11b device around, AP would automatically turn off the protection. This protection mechanism applies to 2.4G only.

HT protection means that a HT station should be aware that a legacy 11bg station would exist and adopt necessary protection if necessary. In the SPEC IEEE Std 802.11-2012, there are four modes for HT protection.

Encoding	Mode	Scenario
B'00	No protection	No non-HT station exists at all
B'01	Nonmember protection	At least one non-HT station exists in a different BSS
B'10	20MHz protection	All HT stations but at least one HT20 station exists
B'11	Non-HT mixed	Otherwise

This protection mechanism would be tested in the WFA TGn Test Plan 4.2.26 Basic Association in 802.11n Environment.

20/40 MHz BSS Coexistence is a mechanism to avoid interference when using 40MHz in the crowded 2.4g band. In fact, using 40MHz is not recommended in 2.4g since multiple unrelated BSSs might easily be overlapped in the same channel and are close enough. This protection mechanism would be tested in the WFA TGn Test Plan 4.2.41 AP 20/40 MHz Coexistence. In the test case, there are 3 scenarios which would make APUT to drops to 20 MHz.
APUT is

- not starting a 40 MHz BSS in presence of an 802.11g BSS.
- appropriately switching from 40 MHz to 20 MHz in presence of 40 MHz intolerant STA.
- appropriately switching from 40 MHz to 20 MHz when receiving frames disallowing the use of 40 MHz channel width.

6.1 Profile Parameter

6.1.1 BGProtection

Description: 11bg protection configuration
Value:

BGProtection=0

0: Auto
1: Always On
2: Always Off

6.1.2 DisableOLBC

Description: Enable or disable detection of OLBC (Overlapping Legacy BSS Condition)
Value:

DisableOLBC=0

0: enable
1: disable

6.1.3 HT_PROTECT

Description: Enable or disable 802.11n protection mechanism
Value:

HT_PROTECT=1

0: disable
1: enable

6.1.4 HT_BSSCoexistence

Description: Enable or disable HT BSS coexistence support in 2.4G
Value:

HT_BSSCoexistence=1

0: disable
1: enable

6.2 iwpriv Command

6.2.1 BGProtection

Description: 11bg protection configuration
Value:

iwpriv ra0 set BGProtection=0

0: Auto
1: Always On
2: Always Off

6.2.2 DisableOLBC

Description: Enable or disable detection of OLBC (Overlapping Legacy BSS Condition)
Value:

iwpriv ra0 set DisableOLBC=0

0: enable
1: disable

6.2.3 HtProtect

Description: Enable or disable 802.11n protection mechanism
Value:

iwpriv ra0 set HtProtect=0

0: disable
1: enable

6.2.4 HtBssCoex

Description: Enable or disable HT BSS coexistence support in 2.4G
Value:

iwpriv ra0 set HtBssCoex=0

0: disable
1: enable

6.2.5 AP2040Rescan

Description: Trigger a scan to recheck HT20/40 coexistence
Value:

iwpriv ra0 set AP2040Rescan=1

7 WMM

7.1 Introduction

IEEE 802.11e amendment is to provide basic QoS features to 802.11 network and Wi-Fi Multimedia (WMM) is a WFA interoperability certification based on the IEEE 802.11e standard. WMM prioritizes wireless traffic according to four Access Categories, including Voice (VO), Video (VI), Best Effort (BE) and Background (BK).

7.2 iwpriv Command

7.2.1 WmmCapable

Description: Enable or disable WMM QoS function
Value:

iwpriv ra0 set WmmCapable=1

0: disable
1: enable

7.3 Profile Parameter

7.3.1 WmmCapable

Description: Enable or disable WMM QoS function
Value:

WmmCapable=1

0: disable
1: enable

Note: Only WmmCapable has iwpriv command support

7.3.2 APSDCapable

Description: WMM Automatic Power Save Delivery (APSD) function configuration
Value:

APSDCapable=0

0: disable
1: enable

7.3.3 APAifsn

Description: AP arbitration interframe space number configuration
Value:

APAifsn=3;7;1;1

AC_BE;AC_BK;AC_VI;AC_VO

7.3.4 APCwmin

Description: AP contention window minimum (exponent) configuration
Value:

APCwmin=4;4;3;2

AC_BE;AC_BK;AC_VI;AC_VO

7.3.5 APCwmax

Description: AP contention window maximum (exponent) configuration
Value:

APCwmax=6;10;4;3

AC_BE;AC_BK;AC_VI;AC_VO

7.3.6 APTxop

Description: AP Transmit Opportunity configuration (unit: 32μs)
Value:

APTxop=0;0;94;47

AC_BE;AC_BK;AC_VI;AC_VO

7.3.7 APACM

Description: AP Admission Control Mandatory configuration
Value:

APACM=0;0;0;0

AC_BE;AC_BK;AC_VI;AC_VO

7.3.8 BSSAifsn

Description: STA arbitration interframe space number configuration
Value:

BSSAifsn=3;7;2;2

AC_BE;AC_BK;AC_VI;AC_VO

7.3.9 BSSCwmin

Description: STA contention window minimum (exponent) configuration
Value:

BSSCwmin=4;4;3;2

AC_BE;AC_BK;AC_VI;AC_VO

7.3.10 BSSCwmax

Description: STA contention window maximum (exponent) configuration
Value:

BSSCwmax=10;10;4;3

AC_BE;AC_BK;AC_VI;AC_VO

7.3.11 BSSTxop

Description: STA Transmit Opportunity configuration (unit: 32μs)
Value:

BSSTxop=0;0;94;47

AC_BE;AC_BK;AC_VI;AC_VO

7.3.12 BSSACM

Description: STA Admission Control Mandatory configuration
Value:

BSSACM=0;0;0;0

AC_BE;AC_BK;AC_VI;AC_VO

7.3.13 AckPolicy

Description: Acknowledgement policy configuration
Value:

AckPolicy=0;0;0;0

0: Normal Ack or Implicit Block Ack Request
1: No Ack
2: No explicit acknowledgement

3: Block Ack

AC_BE;AC_BK;AC_VI;AC_VO

7.4 How to Run WMM test

1. WmmCapable=1
2. TxBurst=**0**
3. HT_RDG=0
4. Parameters for AP
   APAifsn=3;7;1;1 // AC_BE;AC_BK;AC_VI;AC_VO
   APCwmin=4;4;3;2 // AC_BE;AC_BK;AC_VI;AC_VO
   APCwmax=6;10;4;3 // AC_BE;AC_BK;AC_VI;AC_VO
   APTxop=0;0;94;47 // AC_BE;AC_BK;AC_VI;AC_VO
   APACM=0;0;0;0 // AC_BE;AC_BK;AC_VI;AC_VO
5. Parameters for all STAs
   BSSAifsn=3;7;2;2 // AC_BE;AC_BK;AC_VI;AC_VO
   BSSCwmin=4;4;3;2 // AC_BE;AC_BK;AC_VI;AC_VO
   BSSCwmax=10;10;4;3 // AC_BE;AC_BK;AC_VI;AC_VO
   BSSTxop=0;0;94;47 // AC_BE;AC_BK;AC_VI;AC_VO
   BSSACM=0;0;0;0 // AC_BE;AC_BK;AC_VI;AC_VO
6. Ack policy
   AckPolicy=0;0;0;0 // AC_BE;AC_BK;AC_VI;AC_VO;

All default values comply with the Wi-Fi specification.

8 IEEE802.11h

8.1 TPC

We do not support Transmission Power Control (TPC) and we provide a more flexible feature named Single SKU for fulfillment of the similar request. You can also consider TxPower to manually change the power in run-time.

8.2 DFS

DFS stands for Dynamic Frequency Selection and this function is only applicable in 5G band. We just list the basic settings for DFS here. You can check *DFS Debug Guideline* for further information.

8.2.1 Profile Parameter

8.2.1.1 IEEE80211H

Description: Enable or disable IEEE 802.11h support (DFS)
Value:

IEEE80211H=1

0: disable
1: enable

8.2.1.2 DfsEnable

Description: Enable or disable DFS
Value:

DfsEnable=1

0: disable
1: enable

Note: MT7615/MT7915 only
To turn on DFS, you must have IEEE80211H=1 and DfsEnable=1.

8.2.1.3 RDRegion

Description: Configure the area/type of DFS regulation
Value:

RDRegion=JAP

CE/FCC/JAP

8.2.1.4 DfsDedicatedZeroWait

Description: Enable dedicated path for DFS function
Value:

DfsDedicatedZeroWait=1

0: disable
1: enable

Note: MT7915 only

8.2.1.5 DfsZeroWaitDefault

Description: Enable default zero wait DFS flow
Value:

DfsZeroWaitDefault=1

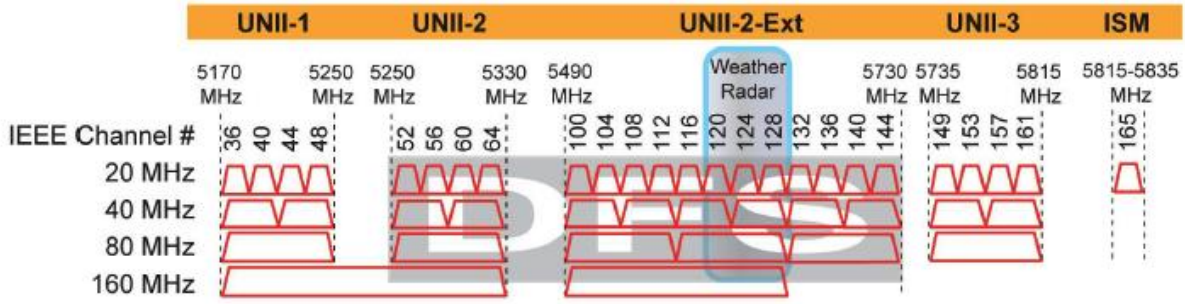
0: disable
1: enable

To turn on zero-wait DFS, you must have DfsDedicatedZeroWait =1 and DfsZeroWaitDefault =1.
Note: MT7915 only

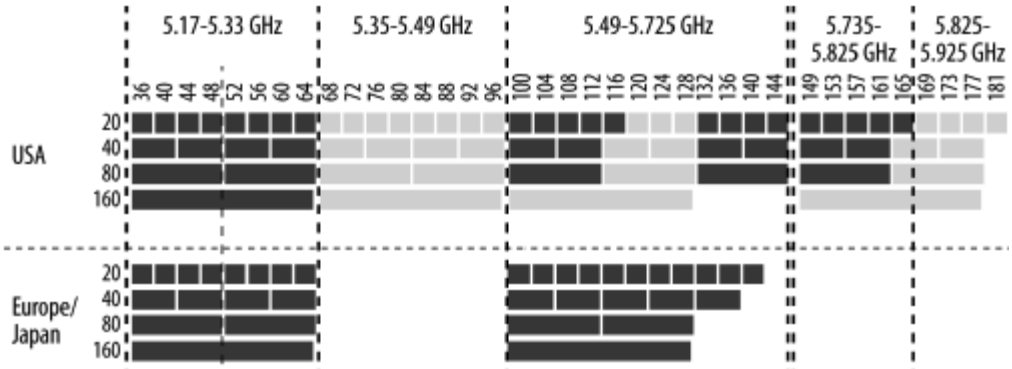
8.2.2 Profile configuration for DFS test

(1) **IEEE80211H=1**
(2) **DfsEnable=1** (MT7615 only)
(3) **RDRegion=CE / FCC / JAP**
   i. CE is for Europe
   ii. FCC is for USA
   iii. JAP is for Japan
(4) **Channel** is set to a DFS channel
   i. Band 2/W53: Ch52 - Ch64
   ii. Band 3/W56: Ch100 - Ch144

From http://wifinigel.blogspot.tw/2014/05/80211ac-5ghz-emperors-new-clothes-part-2.html



From
https://community.aerohive.com/aerohive/topics/effect_of_dfs_on_802_11ac
Matthew Gast's book, "*802.11ac: A Survival Guide*".



9 SECURITY

9.1 All possible combinations of security policy

Type I. Without Radius (IEEE8021X has to be **False**)

	OPEN	SHARED	WEPAUTO
NONE	V	X	X
WEP	V	V	V
802.1x daemon	Off	Off	Off

Type II. With Radius (Non-WiFi standard) (IEEE8021X has to be **True**)

	OPEN
NONE	V
WEP	V
802.1x daemon	On

Type III. With WFA WPA/WPA2 (IEEE8021X has to be **False**)

	WPAPSK	WPA2PSK	WPAPSK WPA2PSK	WPA	WPA2	WPA WPA2
TKIP	V	V	V	V	V	V
AES	V	V	V	V	V	V
TKIPAES	V	V	V	V	V	V
802.1x daemon	Off	Off	Off	**On**	**On**	**On**

9.2 iwpriv Command

9.2.1 AuthMode

Description: WLAN security authentication mode
Value:

iwpriv ra0 set AuthMode=OPEN

OPEN	Open system
SHARED	Shared key system
WEPAUTO	Auto switch between OPEN and SHARED
OWE	Enhanced Open
WPAPSK	WPA Pre-Shared Key (Infra)
WPA2PSK	WPA2 Pre-Shared Key (Infra)

WPA3PSK WPA3 SAE (Infra)
WPAPSKWPA2PSK WPAPSK/WPA2PSK mixed mode (Infra)
WPA2PSKWPA3PSK WPA2PSK/WPA3PSK mixed mode (Infra)
WPA WPA Enterprise mode
WPA2 WPA2 Enterprise mode
WPA3 WPA3 Enterprise mode
WPA3-192 WPA3 Suite B 192 bit Enterprise mode
WPA1WPA2 WPA/WPA2 mixed mode

Noted: Make sure WPA3 is supported on your using driver version before you setup WPA3 related settings.

9.2.2 EncrypType

Description: WLAN security encryption type
Value:

iwpriv ra0 set EncrypType=NONE

NONE	No encryption
WEP	Wired Equivalent Privacy
TKIP	Temporal Key Integrity Protocol
AES	Advanced Encryption Standard
TKIPAES	Mixed cipher
GCMP256	Galois/Counter Mode Protocol – 256 bit

9.2.3 DefaultKeyID

Description: Default key ID (WEP only)
Value:

iwpriv ra0 set DefaultKeyID=1

The ID range is 1~4

9.2.4 Key1

Description: Key 1 string (WEP only)
Value:

iwpriv ra0 set Key1=aaaaa

10 or 26 hexadecimal characters
5 or 13 ASCII characters

9.2.5 Key2

Description: Key 2 string (WEP only)
Value:

iwpriv ra0 set Key2=aaaaa

10 or 26 hexadecimal characters
5 or 13 ASCII characters

9.2.6 Key3

Description: Key 3 string (WEP only)
Value:

iwpriv ra0 set Key3=aaaaa

10 or 26 hexadecimal characters
5 or 13 ASCII characters

9.2.7 Key4

Description: Key 4 string (WEP only)
Value:

iwpriv ra0 set Key4=aaaaa

10 or 26 hexadecimal characters
5 or 13 ASCII characters

9.2.8 WPAPSK

Description: WLAN security password for TKIP/AES/GCMP256
Value:

iwpriv ra0 set WPAPSK=12345678

8~63 ASCII characters
64 hexadecimal characters

9.2.9 WpaMixPairCipher

Description: Providing more flexible combination of cipher suite (NOT recommended)
Value:

iwpriv ra0 set WpaMixPairCipher=WPA_TKIP_WPA2_AES

WPA_AES_WPA2_TKIPAES
WPA_AES_WPA2_TKIP
WPA_TKIP_WPA2_AES
WPA_TKIP_WPA2_TKIPAES
WPA_TKIPAES_WPA2_AES
WPA_TKIPAES_WPA2_TKIPAES

WPA_TKIPAES_WPA2_TKIP

9.3 Profile Parameter

9.3.1 AuthMode

Description: WLAN security authentication mode
Value:

AuthMode=OPEN

OPEN	Open system
SHARED	Shared key system
WEPAUTO	Auto switch between OPEN and SHARED
OWE	Enhanced Open
WPAPSK	WPA Pre-Shared Key (Infra)
WPA2PSK	WPA2 Pre-Shared Key (Infra)
WPA3PSK	WPA3 SAE (Infra)
WPAPSKWPA2PSK	WPAPSK/WPA2PSK mixed mode (Infra)
WPA2PSKWPA3PSK	WPA2PSK/WPA3PSK mixed mode (Infra)
WPA	WPA Enterprise mode
WPA2	WPA2 Enterprise mode
WPA3	WPA3 Enterprise mode
WPA3-192	WPA3 Suite B 192 bit Enterprise mode
WPA1WPA2	WPA/WPA2 mixed mode

Noted: Make sure WPA3 is supported on your using driver version before you setup WPA3 related settings.

9.3.2 EncrypType

Description: WLAN security encryption type
Value:

EncrypType=NONE

NONE	No encryption
WEP	Wired Equivalent Privacy
TKIP	Temporal Key Integrity Protocol
AES	Advanced Encryption Standard
TKIPAES	Mixed cipher
GCMP256	Galois/Counter Mode Protocol – 256 bit

9.3.3 RekeyMethod

Description: Configuration of rekey method for WPA/WPA2
Value:

RekeyMethod=DISABLE

TIME: Time rekey
PKT: Packet rekey
DISABLE: Disable rekey

9.3.4 RekeyInterval

Description: Rekey interval configuration for WPA/WPA2
Value:

RekeyInterval=0

The value range is 0 ~ 0x3FFFFF. (Unit: 1 second or 1000 packets)
Use 0 to disable rekey

9.3.5 PMKCachePeriod

Description: PMK cache life time configuration for WPA/WPA2
Value:

PMKCachePeriod=10

The value range is 0 ~ 65535. (Unit: minute)

9.3.6 WPAPSK

Description: WLAN security password for TKIP/AES/GCMP256
Value:

WPAPSK=01234567

8~63 ASCII characters
64 hexadecimal characters

9.3.7 DefaultKeyID

Description: Default key ID (WEP only)
Value:

DefaultKeyID=1

The ID range is 1~4

9.3.8 Key1Type

Description: Key 1 type
Value:

Key1Type=0

0: Hexadecimal
1: ASCII

9.3.9 Key1Str

Description: Key 1 string
Value:

Key1Str=

10 or 26 hexadecimal characters
5 or 13 ASCII characters

9.3.10 Key2Type

Description: Key 2 type
Value:

Key2Type=0

0: Hexadecimal
1: ASCII

9.3.11 Key2Str

Description: Key 2 string
Value:

Key2Str=

10 or 26 hexadecimal characters
5 or 13 ASCII characters

9.3.12 Key3Type

Description: Key 3 type
Value:

Key3Type=0

0: Hexadecimal
1: ASCII

9.3.13 Key3Str

Description: Key 3 string
Value:

Key3Str=

10 or 26 hexadecimal characters
5 or 13 ASCII characters

9.3.14 Key4Type

Description: Key 4 type
Value:

Key4Type=0

0: Hexadecimal
1: ASCII

9.3.15 Key4Str

Description: Key 4 string
Value:

Key4Str=

10 or 26 hexadecimal characters
5 or 13 ASCII characters

9.3.16 WpaMixPairCipher

Description: Providing more flexible combination of cipher suite
Value:

WpaMixPairCipher=WPA_TKIP_WPA2_AES

WPA_AES_WPA2_TKIPAES
WPA_AES_WPA2_TKIP
WPA_TKIP_WPA2_AES
WPA_TKIP_WPA2_TKIPAES
WPA_TKIPAES_WPA2_AES
WPA_TKIPAES_WPA2_TKIPAES
WPA_TKIPAES_WPA2_TKIP

9.4 New WFA Security Rules

		2013/12/31	2014/1/1
Personal			
WPA-PSK Only	TKIP	V	X
	AES	△	X
WPA2-PSK Only	TKIP	△	X
	AES	V	V
WPA-PSK/WPA2-PSK Mixed			
WPA-PSK	TKIP	V	V
	AES	△	X
WPA2-PSK	TKIP	△	X
	AES	V	V
Enterprise			
WPA Only	TKIP	V	X
	AES	△	X
WPA2 Only	TKIP	△	X
	AES	V	V
WPA/WPA2 Mixed			
WPA	TKIP	V	V
	AES	△	X
WPA2	TKIP	△	X
	AES	V	V

V = Allowed by WFA
X = Prohibited by WFA
△ = It was not prohibited by WFA, but no test case use it.

Note: Please check 9.5.5 for the correct settings of mixed mode.

9.5 iwpriv command examples

Please specify SSID at last step to trigger the AP restart procedure which would reload new security settings.

9.5.1 OPEN/NONE

1. iwpriv ra0 set AuthMode=OPEN
2. iwpriv ra0 set EncrypType=NONE
3. iwpriv ra0 set IEEE8021X=0
4. iwpriv ra0 set SSID=myownssid

9.5.2 SHARED/WEP

1. iwpriv ra0 set AuthMode=SHARED
2. iwpriv ra0 set EncrypType=WEP
3. iwpriv ra0 set Key1=0123456789
4. iwpriv ra0 set DefaultKeyID=1

5. iwpriv ra0 set IEEE8021X=0
6. iwpriv ra0 set SSID=myownssid

9.5.3 WPAPSK/TKIP

1. iwpriv ra0 set AuthMode=WPAPSK
2. iwpriv ra0 set EncrypType=TKIP
3. ~~iwpriv ra0 set SSID=myownssid~~
4. iwpriv ra0 set WPAPSK=myownpresharedkey
5. iwpriv ra0 set SSID=myownssid

Note: Deprecated by WFA since 2014.01.01

9.5.4 WPA2PSK/AES

1. iwpriv ra0 set AuthMode=WPA2PSK
2. iwpriv ra0 set EncrypType=AES
3. ~~iwpriv ra0 set SSID=MySsid~~
4. iwpriv ra0 set WPAPSK=MyPassword
5. iwpriv ra0 set SSID=MySsid

9.5.5 WPAPSKWPA2PSK/TKIPAES

1. iwpriv ra0 set AuthMode=WPAPSKWPA2PSK
2. iwpriv ra0 set EncrypType=TKIPAES
3. ~~iwpriv ra0 set SSID=MySsid~~
4. ~~iwpriv ra0 set WpaMixPairCipher=**WPA_TKIP_WPA2_AES**~~
5. iwpriv ra0 set WPAPSK=MyPassword
6. iwpriv ra0 set SSID=MySsid

9.5.6 WPA3PSK/AES

1. iwpriv ra0 set AuthMode=WPA3PSK
2. iwpriv ra0 set EncrypType=AES
3. iwpriv ra0 set WPAPSK=MyPassword
4. iwpriv ra0 set SSID=MySsid

9.5.7 WPA2PSKWPA3PSK/AES

5. iwpriv ra0 set AuthMode= WPA2PSKWPA3PSK
6. iwpriv ra0 set EncrypType=AES
7. iwpriv ra0 set WPAPSK=MyPassword
8. iwpriv ra0 set SSID=MySsid

10 Authenticator

IEEE Std. 802.1X-2001 is a standard for port-based network access control. It introduces an extensible mechanism for authenticating and authorizing users. There are 3 major components which includes **Supplicant**, **Authenticator** and **Authentication Server** (AS).

The following material is from http://tldp.org/HOWTO/html_single/8021X-HOWTO/.

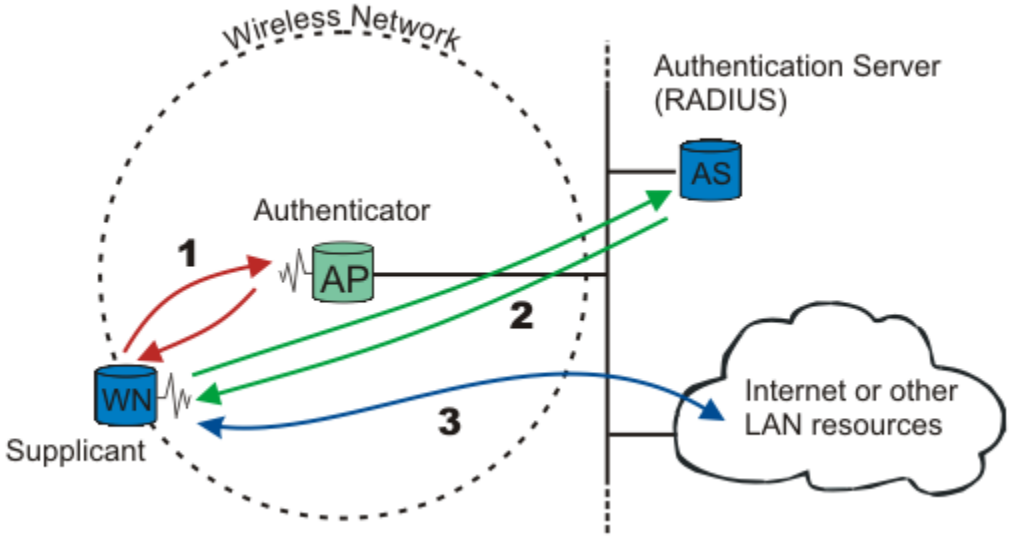


Figure: *A wireless node must be authenticated before it can gain access to other LAN resources.*

When a new wireless node (WN) requests access to a LAN resource, the access point (AP) asks for the WN's identity. No other traffic than EAP is allowed before the WN is authenticated.

The wireless node that requests authentication is often called **Supplicant**, although it is more correct to say that the wireless node contains a Supplicant. The Supplicant is responsible for responding to Authenticator data that will establish its credentials. The same goes for the access point; the access point contains an **Authenticator**. The Authenticator does not even need to be in the access point; it can be an external component.

After the identity has been sent, the authentication process begins.The protocol used between the Supplicant and the Authenticator is EAP, or more correctly, EAP encapsulation over LAN (**EAPoL**). The **Authenticator** re-encapsulates the EAP messages to Radius format, and passes them to the **Authentication Server**.

During authentication, the **Authenticator** just relays packets between the **Supplicant** and the **Authentication Server**. When the authentication process finishes, the Authentication Server sends a success message (or failure message if the

authentication failed). The Authenticator then opens the “port” for the Supplicant. After a successful authentication, the Supplicant is granted access to other LAN resources or Internet.

10.1 Profile Parameter

10.1.1 IEEE8021X

Description: Enable or disable 802.1X-WEP/802.1X-NONE mode
Value:

IEEE8021X=0

0: disable
1: enable

Note: It is enabled only when using Radius-WEP or Radius-NONE.

10.1.2 RADIUS_Server

Description: RADIUS server IP address configuration
Value:

RADIUS_Server=10.10.10.253

Note: IPv4 only

10.1.3 RADIUS_Port

Description: RADIUS server port number configuration
Value:

RADIUS_Port=1812

10.1.4 RADIUS_Key

Description: RADIUS key configuration
Value:

RADIUS_Key=password

10.1.5 own_ip_addr

Descripion: Configure SoftAP its own IP address
Value:

own_ip_addr=10.10.10.254

10.1.6 session_timeout_interval

Descripion: Configure the timeout interval for re-authentication
Value:

session_timeout_interval=120 (unit: second)

Note:

0: Disable re-authentication service
It must be larger than 60. Every session would be re-authenticated for a regular interval defined by this parameter.

10.1.7 PMKCachePeriod

Description: PMK Cache period configuration
Value:

PMKCachePeriod=10 (unit: minutes)

Note:

Default is 10 minutes.

10.1.8 EAPifname

Description: EAPifname is assigned as the binding interface for EAP negotiation
Value:

EAPifname=

Example:

EAPifname=br0

Note:

Its default value is "br0". However, if the wireless interface is not attached to the bridge interface or the name of the bridge interface is not "br0", please modify it.

10.1.9 PreAuth

Description: Enable or disable **WPA2** pre-authentication mode
Value:

PreAuth=0

0: disable
1: enable

10.1.10 PreAuthifname

Description: PreAuthifname is assigned as the binding interface for **WPA2** pre-authentication
Value:

PreAuthifname=

Example:

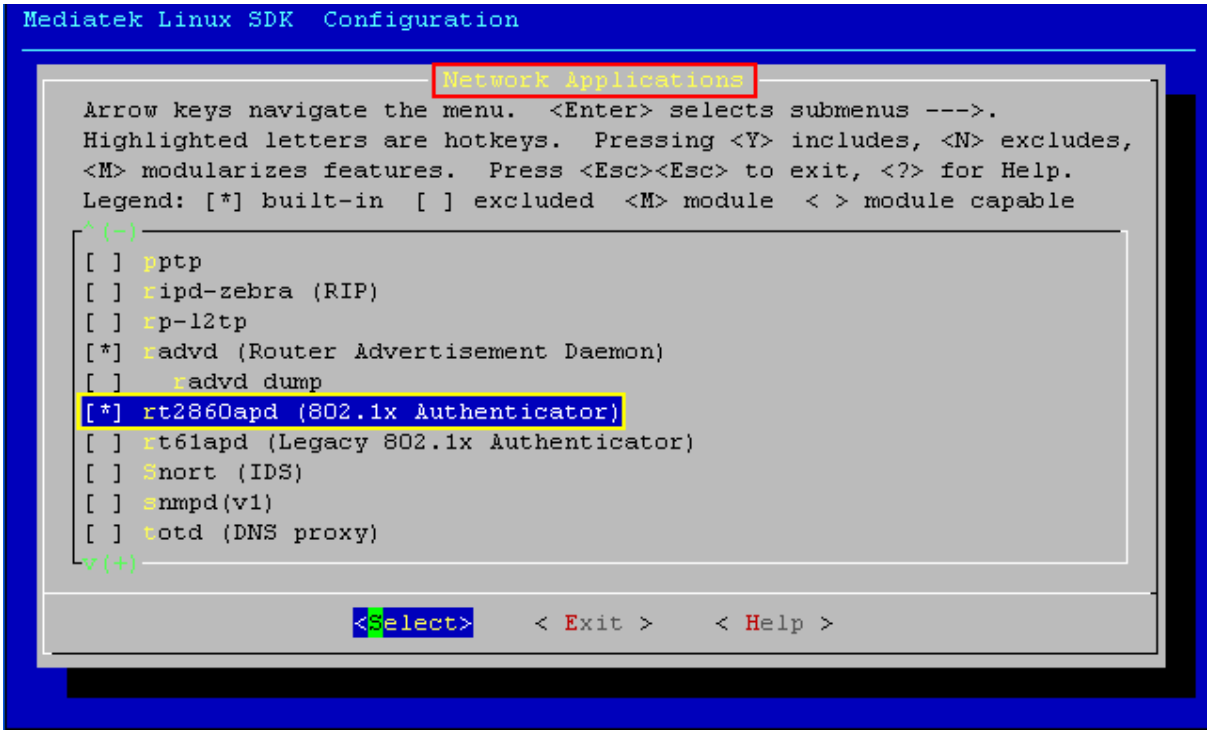
PreAuthifname=br0

10.2 rt2860apd

rt2860apd - IEEE 802.1X Authenticator (user space utility)
Source folder in reference SDK: **RT288x_SDK/source/user/802.1x**
Binary location in reference image: **/bin/rt2860apd**

rt2860apd implements part of IEEE 802.1X which helps the Authentication Server (AS) authorizing the Supplicant and also prove itself a valid Authenticator to AS. Please be noted that rt2860apd does not include the state machine for Key Management. Instead, the Key Management function is included in the wireless driver. Actually, rt2860apd relays EAP frames between the Supplicant and the AS. The port control entity is also implemented in the wireless driver.

10.2.1 How to turn on rt2860apd



10.2.2 How to configure rt2860apd

When rt2860apd starts, it will read settings from the driver profile. For any changes to make, you need to edit the configuration file, and then restart both the wireless interface and rt2860apd. Actually, the command “iwpriv ra0 set SSID=XXXX” would do the job.

The following four parameters in the configuration file are mandatory for rt2860apd. You should configure them correctly according to your own setup.

- RADIUS_Server='10.10.10.253'
- RADIUS_Port='1812'
- RADIUS_Key='password'
- own_ip_addr='10.10.10.254'

10.3 Multiple RADIUS Servers Support

As to MBSSID, you can use “;” to separate the settings for each BSSID. Example is as follows.
RADIUS_Server=192.168.2.1;192.168.2.2;192.168.2.3;192.168.2.4
RADIUS_Port=1811;1812;1813;1814
RADIUS_Key=ralink_1;ralink_2;ralink_3;ralink_4

This implies,
The RADIUS server IP for ra0 is 192.168.2.1, its port is 1811 and its secret key is ralink_1.
The RADIUS server IP for ra1 is 192.168.2.2, its port is 1812 and its secret key is ralink_2.
The RADIUS server IP for ra2 is 192.168.2.3, its port is 1813 and its secret key is ralink_3.
The RADIUS server IP for ra3 is 192.168.2.4, its port is 1814 and its secret key is ralink_4.

Also, we have **Failover** mechanism and it means you can have a backup Radius server for each BSSID. Example is as follows. Both of them are written in the same profile.

<Default>
RADIUS_Server=192.168.2.1;192.168.2.2;192.168.2.3;192.168.2.4
RADIUS_Port=1811;1812;1813;1814
RADIUS_Key=ralink_1;ralink_2;ralink_3;ralink_4

<Failover>
RADIUS_Server=10.10.10.1; 10.10.10.2; 10.10.10.3; 10.10.10.4
RADIUS_Port=1812;1812;1812;1812
RADIUS_Key=ralink_5;ralink_6;ralink_7;ralink_8

You may use iwpriv command to do the same thing for each BSSID.
iwpriv ra0 set RADIUS_Server="192.168.1.1;192.168.1.2"
iwpriv ra0 set RADIUS_Port="1812;1813"
iwpriv ra0 set RADIUS_Key="mediatek123;mediatek456"

For backward compatibility, "RADIUS_Key" and "RADIUS_Key%d" are both accepted by the driver for key configuration. You may use either one of them but the paramter "RADIUS_Key" has higher priority.

<Default>
RADIUS_Key1=ralink_1 // ra0
RADIUS_Key2=ralink_2 // ra1
RADIUS_Key3=ralink_3 // ra2
RADIUS_Key4=ralink_4 // ra3

<Failover>
RADIUS_Key1=ralink_5
RADIUS_Key2=ralink_6
RADIUS_Key3=ralink_7
RADIUS_Key4=ralink_8

10.4 Enhanced Dynamic WEP Keying

In **Radius-WEP**, the authentication process also generates keys for both broadcast and unicast. The unicast key is unique for every individual client so it is always generated randomly by 802.1X daemon. However, the broadcast key is shared among all associated clients and it can be manually configured by User or still generated randomly by 802.1X daemon just like the unicast key does.

802.1X daemon would use the following parameters in the profile as material to "manually" generate the broadcast key.

- DefaultKeyID
- Key0Type, Key1Type, Key2Type, Key3Type
- Key0Str, Key1Str, Key2Str, Key3Str

The 802.1X daemon needs to read the profile to decide whether the broadcast key is generated randomly or not, but if the Key%dStr is empty or incorrectly configured, the broadcast key would be generated randomly by 802.1X daemon instead.

10.5 Examples

In the following examples, we all assume that DUT has IP address 192.168.1.138 and the Authentication Server has IP address 192.168.1.1. Also, we assume that Radius secret is "myownkey".

10.5.1 Radius-None

RADIUS_Server=192.168.1.1
RADIUS_Port=1812
RADIUS_Key=myownkey
own_ip_addr=192.168.1.138
AuthMode=OPEN
EncrypType=NONE
IEEE8021X=1

10.5.2 Radius-WEP

RADIUS_Server=192.168.1.1
RADIUS_Port=1812
RADIUS_Key=myownkey
own_ip_addr=192.168.1.138
AuthMode=OPEN
EncrypType=WEP
IEEE8021X=1

10.5.3 WPA-TKIP

RADIUS_Server=192.168.1.1
RADIUS_Port=1812
RADIUS_Key=myownkey
own_ip_addr=192.168.1.138
AuthMode=WPA
EncrypType=TKIP
IEEE8021X=0

Note: Deprecated by WFA since 2014.01.01

10.5.4 WPA2-AES

RADIUS_Server=192.168.1.1
RADIUS_Port=1812
RADIUS_Key=myownkey
own_ip_addr=192.168.1.138
AuthMode=WPA2
EncrypType=AES
IEEE8021X=0

10.5.5 WPA1WPA2-TKIPAES

RADIUS_Server=192.168.1.1

RADIUS_Port=1812
RADIUS_Key=myownkey
own_ip_addr=192.168.1.138
AuthMode=WPA1WPA2
EncrypType=TKIPAES
~~WpaMixPairCipher=WPA_TKIP_WPA2_AES~~
IEEE8021X=0

10.5.6 WPA3-AES

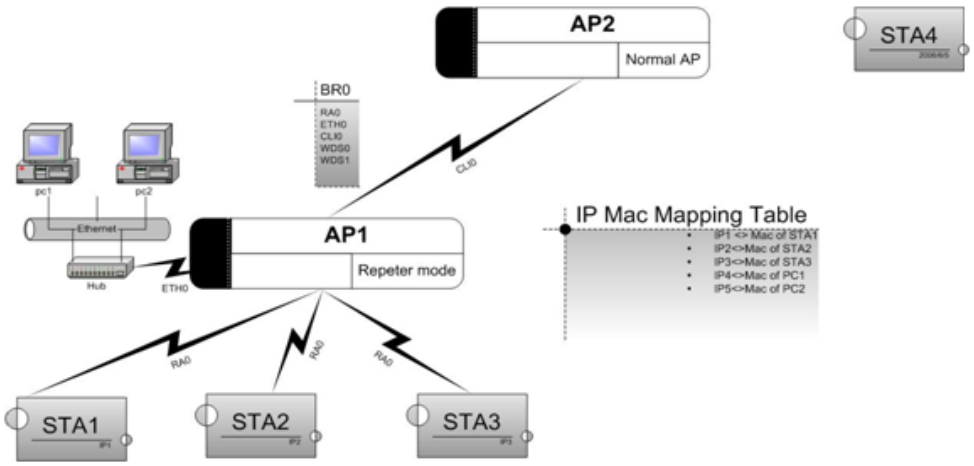
RADIUS_Server=192.168.1.1
RADIUS_Port=1812
RADIUS_Key=myownkey
own_ip_addr=192.168.1.138
AuthMode=WPA3
EncrypType=AES
IEEE8021X=0

10.5.7 WPA3-192-GCMP256

RADIUS_Server=192.168.1.1
RADIUS_Port=1812
RADIUS_Key=myownkey
own_ip_addr=192.168.1.138
AuthMode=WPA3-192
EncrypType=GCMP256
IEEE8021X=0

11 AP-CLIENT

The AP-Client function provides a simulated and virtual STA interface while the original AP interface is working simultaneously. Its application is usually a wireless repeater or a wireless extender. AP-Client mainly provides a 1-to-N MAC address mapping mechanism such that multiple stations connected to the AP can transparently communicate with another AP, which we usually call RootAP. When AP-Client function is enabled, besides the original AP interface named ra0, a virtual interface named apcli0 will be created. In a repeater application, the software bridge, like br0, is used to relay packets between these two interfaces.The following figure shows the common network topology and operation module of our AP-Client function.



AP1 is an Access Point which enabled AP-Client and therefore has two wireless interfaces, ra0 and apcli0, providing the AP and station function respectively. AP2 is just a tranditional Access Point that provides normal AP function. In the figure, you can see that STA1 associated to AP1 and STA4 associated to AP2. In the old days, if STA1 wants to communicate with STA4, AP1 and AP2 must have some kind of connection between them to relay traffic, like Ethernet LAN (wired) or WDS (wireless). Now with the new AP-Client feature, AP1 can use the simulated STA interface apcli0 to connect to AP2, thus creating the link, and then STA1 can communicate with STA4 transparently and wired stations connected to AP1 through Ethernet could also communicate with STA4.

Here are some reminders for you before using AP-Client.

- AP-Client only supports the following protocols due to the limitation of 1-to-N MAC address mapping mechanism
  - All IP-based network applications
  - ARP
  - DHCP
  - PPPoE

11.1 AP-Client Setup

- Turn on **APCLI_SUPPORT** in driver config
- Use "**ifconfig apcli0 up**" to bring up your AP-Client interface
- In a repeater application, you may use the following commands to bridge ra0 and apcli0
  - **brctl addif br0 ra0**
  - **brctl addif br0 apcli0**
- The security policy support for AP-Client include
  - OPEN
  - SHARED (WEP)
  - WPAPSK (TKIP, AES)
  - WPA2PSK (TKIP, AES)
- Please be noted that AP-Client is also a virtual interface. When you use AP-Client and MBSSID simultaneously, AP-Client will consume one slot for MBSSID and the parameter "BssidNum" should be larger than 1 and less than 7 (1 < BssidNum < 7)
  [Note for MT7915] Yellow mark part could be ignored since it is for old project <= 7621
- Use "**iwpriv apcli0 show connStatus**" to display connection status with RootAP

11.2 Profile Parameter

11.2.1 ApCliEnable

Description: Enable or disable AP-Client function
Value:

ApCliEnable=1

0: disable
1: enable

11.2.2 ApCliSsid

Description: Configure the target/RootAP SSID which AP-Client wants to connect with
Value:

ApCliSsid=target_ssid

target_ssid: 1~32 characters

11.2.3 ApCliBssid

Description: Configure the target BSSID which AP-Client wants to join
Value:

ApCliBssid=00:11:22:33:44:55

Note: It is an optional command. Users can use this command to indicate the desired BSSID. Otherwise, AP-Client would get correct BSSID according to configured SSID automatically.

11.2.4 ApCliAuthMode

Description: AP-Client authentication mode configuration
Value:

ApCliAuthMode=OPEN

OPEN
SHARED
WPAPSK
WPA2PSK

11.2.5 ApCliEncrypType

Description: AP-Client encryption type configuration
Value:

ApCliEncrypType=NONE

NONE
WEP
TKIP
AES

11.2.6 ApCliWPAPSK

Description: WPA/WPA2 Pre-Shared Key configuration
Value:

ApCliWPAPSK=12345678

8~63 ASCII characters
64 hexadecimal characters

11.2.7 ApCliDefaultKeyID

Description: Default key index configuration
Value:

ApCliDefaultKeyID=1

The ID range is 1~4

11.2.8 ApCliKey1Type

Descripion: Set the WEP key type of AP-Client for key index 1
Value:

ApCliKey1Type=0

0: Hexadecimal
1: ASCII

11.2.9 ApCliKey1Str

Description: Set the WEP key string of AP-Client for key 1
Value:

ApcliKey1Str=012345678

10 or 26 hexadecimal characters
5 or 13 ASCII characters

11.2.10 ApCliKey2Type

Descripion: Set the WEP key type of AP-Client for key index 2
Value:

ApCliKey2Type=0

0: Hexadecimal
1: ASCII

11.2.11 ApCliKey2Str

Description: Set the WEP key string of AP-Client for key 2
Value:

ApcliKey2Str=012345678

10 or 26 hexadecimal characters
5 or 13 ASCII characters

11.2.12 ApCliKey3Type

Descripion: Set the WEP key type of AP-Client for key index 3
Value:

ApCliKey3Type=0

0: Hexadecimal
1: ASCII

11.2.13 ApCliKey3Str

Description: Set the WEP key string of AP-Client for key 3
Value:

ApcliKey3Str=012345678

10 or 26 hexadecimal characters
5 or 13 ASCII characters

11.2.14 ApCliKey4Type

Descripion: Set the WEP key type of AP-Client for key index 4
Value:

ApCliKey4Type=0

0: Hexadecimal
1: ASCII

11.2.15 ApCliKey4Str

Description: Set the WEP key string of AP-Client for key 4
Value:

ApcliKey4Str=012345678

10 or 26 hexadecimal characters
5 or 13 ASCII characters

11.2.16 ApCliTxMode

[Note for MT7915] Discussed with Chien-hao Hsu/Money Wang, 11.2.16/11.2.17 can be merged and use “iwpriv ra0 set FixedRate=[WCID]-[Mode]-[BW]-[MCS]-[VhtNss]-[SGI]-[Preamble]-[STBC]-[LDPC]-[SPE_EN], 填apcli wcid即可” to replace
Description: Fixed transmission mode configuration
Value:

ApCliTxMode=HT

cck | CCK,
ofdm | OFDM,
ht | HT

11.2.17 ApCliTxMcs

[Note for MT7915] Discussed with Chien-hao Hsu/Money Wang, 11.2.16/11.2.17 can be merged and use “iwpriv ra0 set FixedRate=[WCID]-[Mode]-[BW]-[MCS]-[VhtNss]-[SGI]-[Preamble]-[STBC]-[LDPC]-[SPE_EN], 填apcli wcid即可” to replace

Description: AP-Client Tx MCS configuration
Value:

ApCliTxMcs=33

0~15, 32: Fixed MCS
33: Auto MCS

11.2.18 ApCliWscSsid

Description: Configure the SSID which AP-Client wants to do WPS negotiation
Value:

ApCliWscSsid=target_ssid

targer_ssid: 1~32 characters

Note: This must be configured in PIN mode and PIN mode only since there is no overlapping check in PIN mode. User may have to collect the potential WPS registrar list in user space (through site survey) and try the SSID in the list one by one

11.3 iwpriv Command

11.3.1 ApCliEnable

Description: Enable or disable AP-Client function
Value:

iwpriv apcli0 set ApCliEnable=0

0: disable
1: enable

11.3.2 ApCliSsid

Description: Configure the target/RootAP SSID which AP-Client wants to connect with
Value:

iwpriv apcli0 set ApCliSsid=target_ssid

target_ssid: 1~32 characters

11.3.3 ApCliBssid

Description: Configure the target BSSID which AP-Client wants to join
Value:

iwpriv apcli0 set ApCliBssid=00:11:22:33:44:55

Note: It is an optional command. Users can use this command to indicate the desired BSSID. Otherwise, AP-Client would get correct BSSID according to configured SSID automatically.

11.3.4 ApCliAuthMode

Description: AP-Client authentication mode configuration
Value:

iwpriv apcli0 set ApCliAuthMode=OPEN

OPEN
SHARED
WPAPSK
WPA2PSK

11.3.5 ApCliEncrypType

Description: AP-Client encryption type configuration
Value:

iwpriv apcli0 set ApCliEncrypType=NONE

NONE
WEP
TKIP
AES

11.3.6 ApCliWPAPSK

Description: WPA/WPA2 Pre-Shared Key configuration
Value:

iwpriv apcli0 set ApCliWPAPSK=12345678

8~63 ASCII characters
64 hexadecimal characters

11.3.7 ApCliDefaultKeyID

Description: Default key index configuration
Value:

iwpriv apcli0 set ApCliDefaultKeyID=1

The ID range is 1~4

11.3.8 ApCliKey1

Description: Set the WEP key string of AP-Client for key 1
Value:

iwpriv apcli0 set ApcliKey1=012345678

10 or 26 hexadecimal characters
5 or 13 ASCII characters

11.3.9 ApCliKey2

Description: Set the WEP key string of AP-Client for key 2
Value:

iwpriv apcli0 set ApcliKey2=012345678

10 or 26 hexadecimal characters
5 or 13 ASCII characters

11.3.10 ApCliKey3

Description: Set the WEP key string of AP-Client for key 3
Value:

iwpriv apcli0 set ApcliKey3=012345678

10 or 26 hexadecimal characters
5 or 13 ASCII characters

11.3.11 ApCliKey4

Description: Set the WEP key string of AP-Client for key 4
Value:

iwpriv apcli0 set ApcliKey4=012345678

10 or 26 hexadecimal characters
5 or 13 ASCII characters

11.3.12 ApCliTxMode

[Note for MT7915] Discussed with Chien-hao Hsu/Money Wang, 11.3.12 can be removed.
Description: Fixed transmission mode configuration
Value:

iwpriv apcli0 set ApCliTxMode=HT

CCK

OFDM
HT

11.3.13 ApCliTxMcs

[Note for MT7915] Discussed with Chien-hao Hsu/Money Wang, 11.3.13 can be removed.
Description: Fixed Tx MCS configuration
Value:

iwpriv apcli0 set ApCliTxMcs=33

0~15, 32: Fixed MCS
33: Auto MCS

11.3.14 ApCliWscSsid

Description: Configure the SSID which AP-Client wants to do PIN mode WPS negotiation
Value:

iwpriv apcli0 set ApCliWscSsid=target_ssid

targer_ssid: 1~32 characters

Note: This must be configured in PIN mode and PIN mode only since there is no overlapping check in PIN mode. User may have to collect the potential WPS registrar list in user space (through site survey) and try the SSID in the list one by one

11.3.15 ApCliAutoConnect

Description: Enable or disable the auto-connection function to find the configured SSID
Value:

iwpriv apcli0 set ApCliAutoConnect=1

0: disable
1: enable

Note: APCLI_AUTO_CONNECT_SUPPORT must be turned on

11.4 AP-Client normal connection examples

11.4.1 OPEN/NONE

iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliAuthMode=OPEN
iwpriv apcli0 set ApCliEncrypType=NONE
iwpriv apcli0 set ApCliSsid=ROOTAP_SSID
iwpriv apcli0 set ApCliEnable=1

11.4.2 OPEN/WEP

iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliAuthMode=OPEN
iwpriv apcli0 set ApCliEncrypType=WEP
iwpriv apcli0 set ApCliDefaultKeyID=1
iwpriv apcli0 set ApCliKey1=1234567890
iwpriv apcli0 set ApCliSsid=ROOTAP_SSID
iwpriv apcli0 set ApCliEnable=1

11.4.3 WPAPSK/TKIP

iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliAuthMode=WPAPSK
iwpriv apcli0 set ApCliEncrypType=TKIP
iwpriv apcli0 set ApCliSsid=ROOTAP_SSID
iwpriv apcli0 set ApCliWPAPSK=12345678
iwpriv apcli0 set ApCliSsid=ROOTAP_SSID
iwpriv apcli0 set ApCliEnable=1

11.4.4 WPA2PSK/AES

iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliAuthMode=WPA2PSK
iwpriv apcli0 set ApCliEncrypType=AES
iwpriv apcli0 set ApCliSsid=ROOTAP_SSID
iwpriv apcli0 set ApCliWPAPSK=12345678
iwpriv apcli0 set ApCliSsid=ROOTAP_SSID → [Note for MT7915] can be removed
iwpriv apcli0 set ApCliEnable=1

11.5 AP-Client WPS connection examples

11.5.1 PIN mode

iwpriv apcli0 set Debug=3

```
iwpriv apcli0 set WscGenPinCode=1              // Generate PIN code
iwpriv apcli0 set Debug=0

iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set WscConfMode=1                // Enrollee
iwpriv apcli0 set WscMode=1                    // PIN mode
iwpriv apcli0 set ApCliEnable=1
iwpriv apcli0 set ApCliWscSsid=<target_AP>     // SSID of the target WPS AP (must)
iwpriv apcli0 set WscGetConf=1                 // Trigger
```

*Input the generated PIN code in the Registrar
*You have to collect all PIN WPS Registrar in advance and try each of them as <target_AP> one by one

11.5.2 PBC Mode

```
iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set WscConfMode=1                // Enrollee
iwpriv apcli0 set WscMode=2                    // PBC mode
iwpriv apcli0 set ApCliEnable=1
iwpriv apcli0 set WscGetConf=1                 // Trigger
```

12 WDS

A Wireless Distribution System is a system enabling the wireless interconnection of acess points. Each WDS AP needs to be in the same channel, using the same encryption type. Actually, there is no official specification and test plan to ensure the inter-operability of all WDS products from different Vendors. Therefore, the WDS link could be only created between two peers using identical solution.

Mediatek's implementation provides two modes of AP-to-AP connectivity. One is **Bridge mode**, in which WDS APs communicate only with each other and do not allow wireless stations to access them. The other is **Repeater mode**, in which WDS APs communicate with each other and also accepts connection requests from wireless stations.

In case you want to have an auto-learning WDS peer, we also provide the **Lazy mode** in which you do not need to thoroughly configure the WDS settings. However, please be noted that you cannot configure all APs to be in Lazy mode, otherwise no 4-address frame will be transmitted at all and auto-learning would be impossible. This means that there should be at least one AP being configured in Bridge mode or Repeater mode.

12.1 How to Steup WDS

1. Edit the driver profile in each WDS peer
   WDS Peer-A with the MAC address 00:0C:43:aa:bb:cc
   - WdsEnable=3
   - WdsPhyMode=HTMIX;
   - WdsList=00:0C:43:11:22:33;
   - WdsEncrypType=NONE;

   WDS Peer-B with the MAC address 00:0C:43:11:22:33
   - WdsEnable=3
   - WdsPhyMode=HTMIX;
   - WdsList=00:0C:43:aa:bb:cc;
   - WdsEncrypType=NONE;

2. Edit your networking script file, like bridge_setup.sh, according to the number of WDS link. Add "**brctl addif br0 wds0**" and "**ifconfig wds0 0.0.0.0**" to relative places

3. Use "**iwpriv ra0 show wdsinfo**" to display WDS link information

12.2 WDS Security

WDS security is **PSK-only**, and it does not support mixed mode, like WPAPSKWPA2PSK.

When WDS is in Lazy mode, all WDS links (wds0 ~ wds3) shall share the same encryption type and key material (referring to wds0 settings). Otherwise, each WDS link has its own security settings. No matter what WDS mode you use, it has nothing to do with the encryption of the main BSSID (ra0).

WdsKey:
It is used for all WDS interfaces and supports only AES and TKIP configuration. If you want to use WEP, key settings will be retrieved from the main BSSID.

Wds0Key/Wds1Key/Wds2Key/Wds3Key:
They are used to configure key settings for each WDS interface.

The following example is to create one WDS link (wds0) with AES encryption.

```
WdsEnable=3
WdsPhyMode=HTMIX;HTMIX;HTMIX;HTMIX
WdsList=00:0c:43:12:34:56;
WdsEncrypType=AES;NONE;NONE;NONE
Wds0Key=12345678
Wds1Key=
Wds2Key=
Wds3Key=
```

12.3 Profile Parameter

12.3.1 WdsEnable

Description: WDS function configuration
Value:

WdsEnable=0

0: **Disable** - Disable WDS function.
1: Restrict mode - Same as Repeater mode.
2: **Bridge mode** - Enable WDS and work like a bridge.
The MAC address of peer WDS APs should be configured in the

"WdsList" field.

In this mode, AP is just a bridge and will not send any beacon and will not respond to any probe request packet. Therefore STA will not be able to connect with it.

3: **Repeater mode** - Enable WDS and work like a repeater.

The MAC address of peer WDS APs should be configured in the "WdsList" field.

4: **Lazy mode** - Enable WDS function.

It automatically learns from 4-address format frames sent by the WDS peer and you do not have to configure WdsList manually.

12.3.2 WdsList

Description: WDS peer MAC address configuration
Value:

WdsList=00:10:20:30:40:50;

The maximum WDS link number is 4.
wds0;wds1;wds2;wds3

12.3.3 WdsEncrypType

Description: WDS encryption configuration
Value:

WdsEncrypType=NONE;

The option includes NONE, WEP, TKIP and AES.

Example:

WdsEncrypType=NONE;WEP;TKIP;AES

The encrptytion of wds0 is NONE
The encrptytion of wds1 is WEP
The encrptytion of wds2 is TKIP
The encrptytion of wds3 is AES

12.3.4 WdsKey

Description: WDS key configuration
Value:

WdsKey=12345678

8 ~ 63 ASCII characters (eg: 12345678) for TKIP or AES
64 hexadecimal characters for TKIP or AES

WdsKey is kept for backward-compatibility and it only supports TKIP and AES.

You can use either WdsKey or Wds[0-4]Key but not both.

Note: Combinations of WDS security mode

EncrypType	WdsEncrypType	WdsEncrypType of the WDS peer	Note
NONE	NONE	NONE	
WEP	WEP	WEP	Using legacy key setting method
TKIP	TKIP	TKIP	WDS's key is from WdsKey
TKIP	AES	AES	WDS's key is from WdsKey
AES	TKIP	TKIP	WDS's key is from WdsKey
AES	AES	AES	WDS's key is from WdsKey
TKIPAES	TKIP	TKIP	WDS's key is from WdsKey
TKIPAES	AES	AES	WDS's key is from WdsKey

12.3.5 Wds0Key

Description: WDS key for Link-0
Value:

Wds0Key=12345678

10 or 26 hexadecimal characters (eg: 1234567890) for WEP
5 or 13 ASCII characters (eg: 12345) for WEP
8 ~ 63 ASCII characters (eg: 12345678) for TKIP or AES
64 hexadecimal characters for TKIP or AES

12.3.6 Wds1Key

Description: WDS key for Link-1
Value:

Wds1Key=12345678

12.3.7 Wds2Key

Description: WDS key for Link-2
Value:

Wds2Key=12345678

12.3.8 Wds3Key

Description: WDS key for Link-3
Value:

Wds3Key=12345678

12.3.9 WdsPhyMode

Description: WDS link physical mode configuration
Value:

WdsPhyMode=HTMIX;

The option includes CCK, OFDM, HTMIX and VHT.

Example:

WdsPhyMode=CCK;OFDM;HTMIX;VHT

The PHY mode of wds0 is CCK
The PHY mode of wds1 is OFDM
The PHY mode of wds2 is HTMIX
The PHY mode of wds3 is VHT

13 IGMP SNOOPING

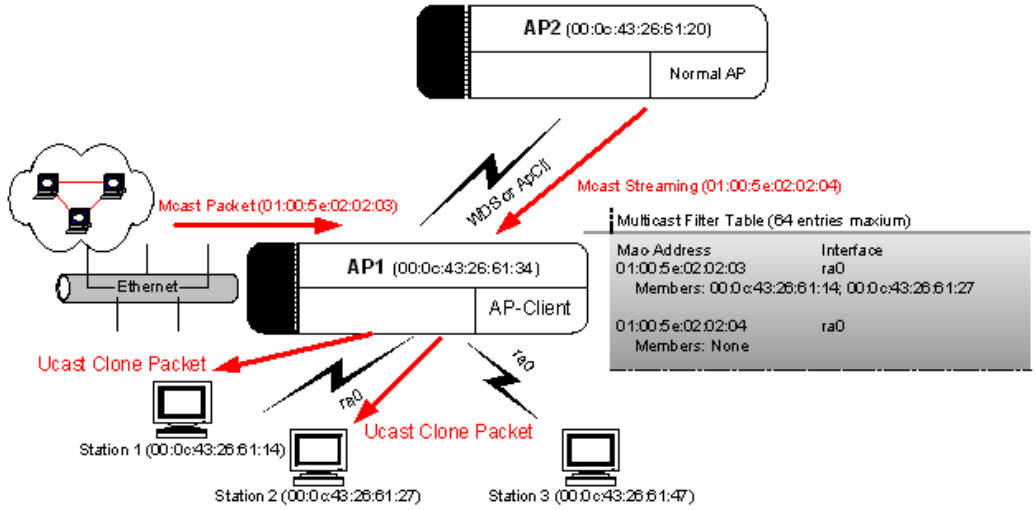
13.1 Basic

Please check the following two Wiki links.

- http://en.wikipedia.org/wiki/Multicast_address
- http://en.wikipedia.org/wiki/Internet_Group_Management_Protocol

IGMP Snooping provides a mechanism converting multicast traffic into unicast traffic. When AP receives incoming multicast traffic, the conversion would be done based on an IGMP Snooping table (Multicast Filter Table).

13.2 Introduction to IGMP Snooping Table



An IGMP Snooping table (a.k.a. Multicast Filter Table) entry consists of 3 components, Group-ID (Multicast MAC Address), Network-Interface and Member-List. Taking above figure for example, you can see that Multicast Filter Table of AP1 has two table entries. One is “01:00:5e:02:02:03” with two members on interface ra0 and the other is “01:00:5e:02:02:04” without any member on interface ra0.

In our implementation, AP will automatically maintain the Multicast Filter Table through packet snooping. The IGMP-Membership-Report packets sent from connected stations would be checked and parsed. You can also manually add and delete an entry through iwpriv command.

13.3 Multicast Packet Parsing Process

When AP receives multicast packets, it will check whether the multicast destination address matches any Group-ID in the Multicast Filter Table. AP will drop the packet if no match found. Otherwise, there are two cases how AP handles a multicast

packet. The first one is that Member-List of the matching entry is empty and then AP just forwards multicast packets to all stations connected to the Network-Interface. In the second case, there are members in the Member-List and AP will do the MC-to-UC conversion based on the membership.

Taking the previous figure for example, AP1 received an Ethernet multicast packet with Group-ID being 01:00:5e:02:02:03. Firstly AP1 checked the Multicast Filter Table and found the first entry matched. Therefore, AP1 cloned every multicast packet into two unicast packets destined to Station 1 and Station 2 respectively.

In the same figure, a multicast streaming sent from AP2 to AP1 with Group-ID 01:00:5e:02:02:04 was forwarded to all stations connected to AP1 (ra0) since the matching entry had no member at all.

<Multicast Filter Table Example>

Group-ID	Network-Interface	Member-List
01:00:5e:02:02:03	ra0	00:0c:43:26:61:14 (Station 1) 00:0c:43:26:61:27 (Station 2)
01:00:5e:02:02:04	ra0	

13.4 Profile Parameter

13.4.1 IgmpSnEnable

Description: Enable or disable IGMP Snooping function
Value:

IgmpSnEnable=1

0: disable
1: enable

Note: Please make sure that IGMP_SNOOP_SUPPORT is turned on in driver config

13.5 iwpriv Command

13.5.1 IgmpSnEnable

Description: Enable or disable IGMP Snooping function
Value:

iwpriv ra0 set IgmpSnEnable=1

0: disable

1: enable

13.5.2 IgmpAdd

Description: Create a new group or add a new member to the existing group
Format:

// Create a new group <Group-ID> which can be a MAC address or an IP address

iwpriv ra0 set IgmpAdd=<Group-ID>

// Add a new member to the existing group. [Member] can only be a MAC address

iwpriv ra0 set IgmpAdd=<Group-ID-[Member]-...>

Value:

// Create a new group via either IP or MAC address
iwpriv ra0 set IgmpAdd=**226.2.2.3**
iwpriv ra0 set IgmpAdd=**01:00:5e:02:02:03**

// Add a new member to the existing group
iwpriv ra0 set IgmpAdd=**226.2.2.3**-**00:0c:43:26:61:11**
// Add 2 new members to the existing group
iwpriv ra0 set IgmpAdd=**01:00:5e:02:02:03**-**00:0c:43:26:61:27**-**00:0c:43:26:61:28**

13.5.3 IgmpDel

Description: Delete a group or remove a member from the existing group
Format:

// Delete a group <Group-ID> which can be a MAC address or an IP address

iwpriv ra0 set IgmpDel=<Group-ID>

// Remove a member from the existing group. [Member] can only be a MAC address

iwpriv ra0 set IgmpDel=<Group-ID-[Member]-...>

Value:

// Delete a new group via either IP or MAC address
iwpriv ra0 set IgmpDel=**226.2.2.3**
iwpriv ra0 set IgmpDel=**01:00:5e:02:02:03**

// Remove a member from the existing group
iwpriv ra0 set IgmpDel=**226.2.2.3**-**00:0c:43:26:61:11**

// Remove members from the existing group
iwpriv ra0 set IgmpDel=**01:00:5e:02:02:03**-**00:0c:43:26:61:27**-**00:0c:43:26:61:28**

14 MAC Repeater

The MAC Repeater is a variation of the original AP-Client funcation and it acts as a wireless proxy for its clients. The repeater will create a corresponding upstream connection to the RootAP for each downstream client connected to it. An upstream connection is created according to its own wireless capability and security mode. When a client disconnects from the repeater, the repeater must also disconnect its corresponding upstream connection with the RootAP. All communication between downstream clients and upstream RootAP utilizes one "AP-Client" interface on the repeater.

For example, if there are 3 clients connected to the repeater, 3 upstream connections will be created accordingly. Besides these "proxy connection", the repeater itself would also create a connection with RootAP. Therefore, in this case there would be totally 3 downstream and 4 upstream connections.

Please be noted that MAC Repeater has the following limitation.

- Roaming of STAs between different BSSs is not supported
- WPA2-Enterprise Security is not supported
- Supported protocols: IPv4 / ARP / DHCP
- The MAC Repeater supports up to 16 clients → [Note for MT7915] support 32 clients per band
- Impact CPU utilization due to parsing all received packets from the STA and all multicast and broadcast packets

14.1 iwpriv Command

14.1.1 MACRepeaterEn

Description: Enable or disable MAC Repeater function
Value:

iwpriv ra0 set MACRepeaterEn=1

0: disable
1: enable

14.1.2 Example

- **iwpriv ra0 set MACRepeaterEn=1**
- ifconfig apcli0 up
- brctl addif br0 apcli0
- iwpriv apcli0 set ApCliEnable=0
- iwpriv apcli0 set ApCliAuthMode=OPEN
- iwpriv apcli0 set ApCliEncrypType=NONE

- iwpriv apcli0 set ApCliSsid=RootAP_SSID
- iwpriv apcli0 set ApCliEnable=1

14.2 Profile Parameter

14.2.1 MACRepeaterEn

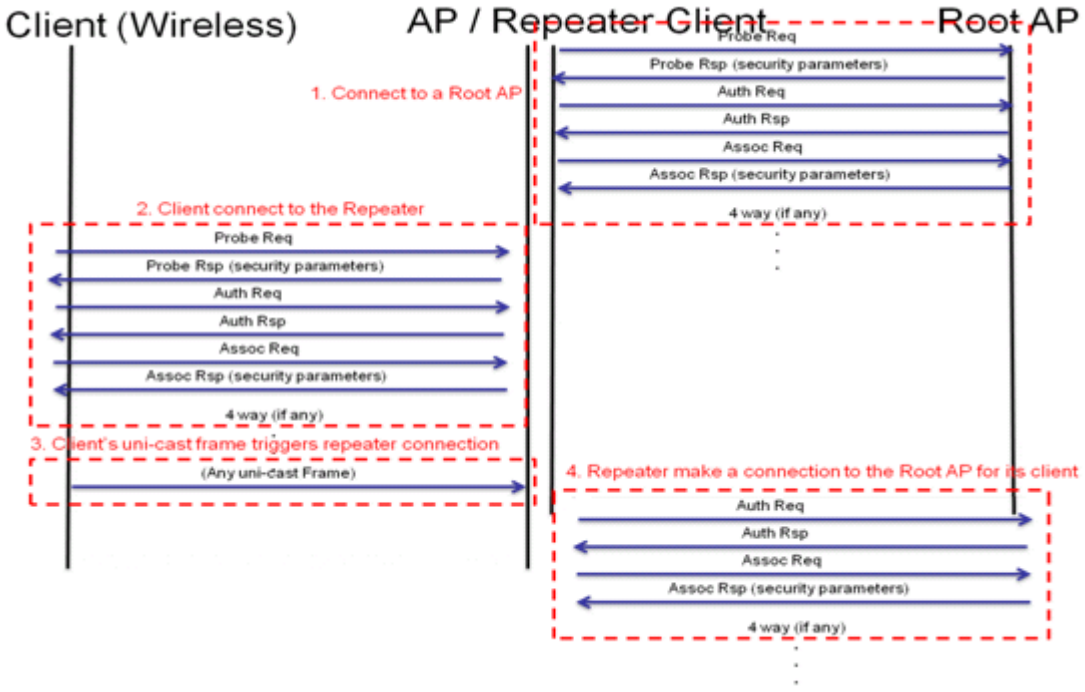
Description: Enable or disable the MAC Repeater function.
Value:

MACRepeaterEn=0

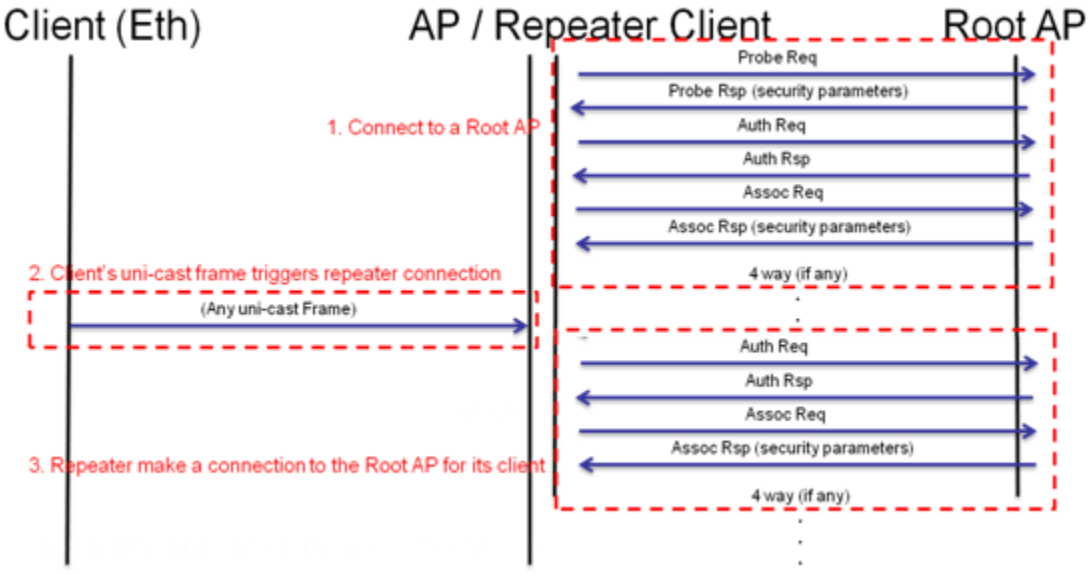
0: disable
1: enable

14.3 Management Frame Flow

14.3.1 Wireless client

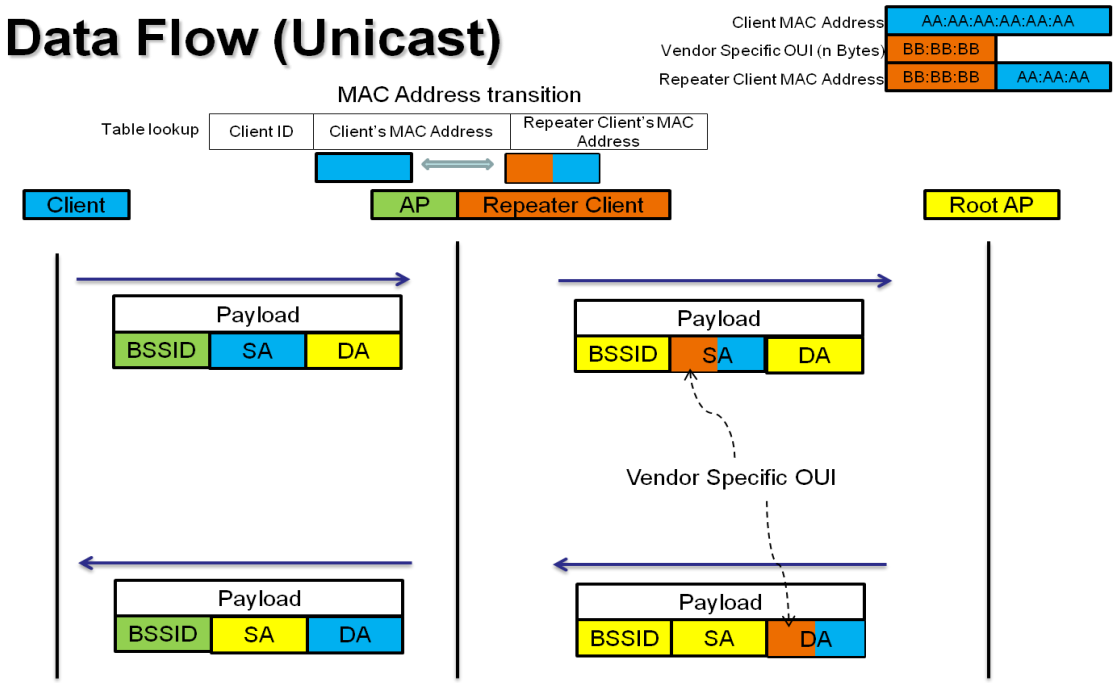


14.3.2 Ethernet client

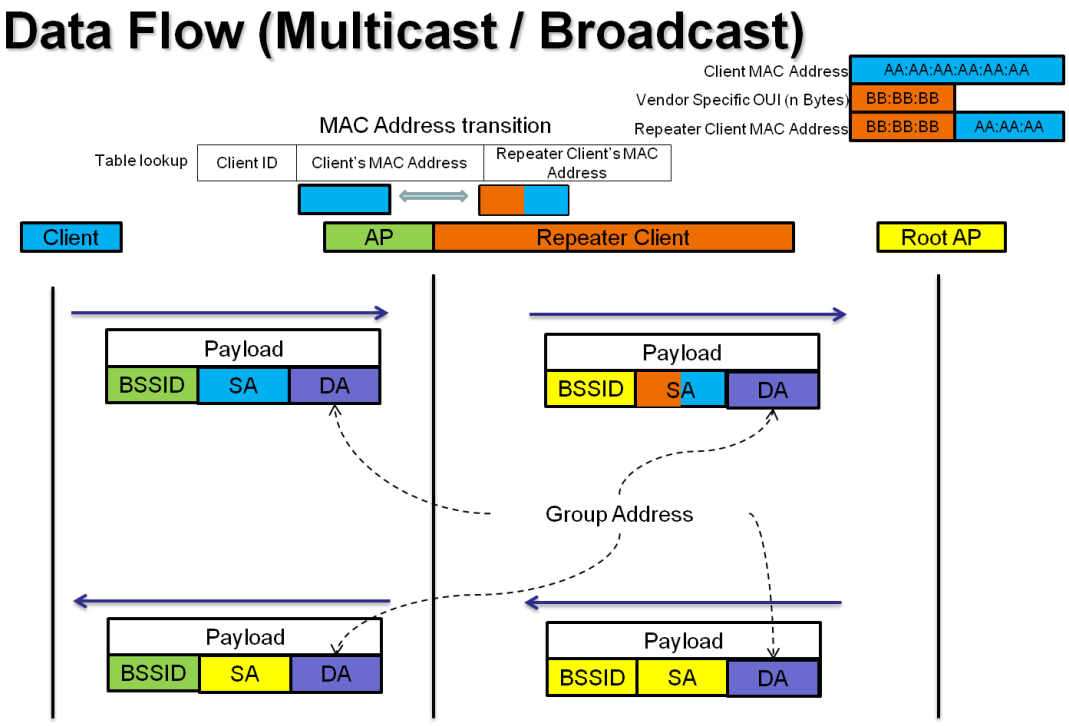


14.4 Data Frame Flow

14.4.1 Unicast



14.4.2 Multicast / Broadcast



15 PMF

PMF stands for Protected Management Frame and IEEE 802.11w is the PMF standard. Its objective is to increase the security of 802.11 management frames.

~~Note: Currently supported chips are MT7602E, MT7612E, MT7603E, MT7628.~~
Note: PMF parameter is useless for new WPA3 security mode due to PMF is default on

15.1 iwpriv Command

15.1.1 PMFMFPC

Description: Enable or disable Protection Management Frame Capable
Value:

iwpriv ra0 set PMFMFPC=1

0: disable
1: enable

15.1.2 PMFMFPR

Description: Enable or disable Protection Management Frame Required
Value:

iwpriv ra0 set PMFMFPR=1

0: disable
1: enable

15.1.3 PMFSHA256

Description: Enable or disable use SHA256 for Encryption
Value:

iwpriv ra0 set PMFSHA256=1

0: disable
1: enable

Note: SHA stands for Secure Hash Algorithm

15.2 Profile Parameter

15.2.1 PMFMFPC

Description: Disable or enable Protection Management Frame Capable
Value:

PMFMFPC=0

0: Disable
1: Enable

15.2.2 PMFMFPR

Description: Disable or enable Protection Management Frame Required
Value:

PMFMFPR=0

0: Disable
1: Enable

15.2.3 PMFSHA256

Description: Disable or enable use SHA256 for Encryption
Value:

PMFSHA256=0

0: Disable
1: Enable

15.3 Wi-Fi PMF Testing Note

15.3.1 DUT Requirement

PMF is a mandatory testing item to TGac but an optional one to TGn. Actually you can refer to the following table for the correct combination in a dual band AP.

<11ac dual band AP>

Combination	11ac 5GHz	11n 2.4GHz
Correct	PMF supported	PMF supported
Not acceptable	PMF supported	PMF Not Available
Not acceptable	PMF Not Available	PMF supported
Not acceptable	PMF Not Available	PMF Not Available

<11n dual band AP>

Combination	11n 5GHz	11n 2.4GHz
Correct	PMF supported	PMF supported
Not acceptable	PMF supported	PMF Not Available
Not acceptable	PMF Not Available	PMF supported
Correct	PMF Not Available	PMF Not Available

15.3.2 PMF Test Section 4.3.3.3

Verification of CCMP to protect transmitted unicast deauthentication/disassociation frames

- iwpriv ra0 set PMFMFPC=1
- iwpriv ra0 set PMFMFPR=0
- iwpriv ra0 set PMFSHA256=0
- iwpriv ra0 set SSID=PMF-4.3.3.3
- iwpriv ra0 set **DisConnectSta=00:0C:43:35:93:00**

15.3.3 PMF Test Section 4.4

Verify use of BIP (Broadcast Integrity Protocol) to protect broadcast management frames

- iwpriv ra0 set PMFMFPC=1
- iwpriv ra0 set PMFMFPR=0
- iwpriv ra0 set PMFSHA256=0
- iwpriv ra0 set SSID=PMF-4.4
- iwpriv ra0 set **DisConnectAllSta=2**

16 Transmit Beamforming

Beamforming is a signal process technique for directional signal transmission and reception. There are two kinds of beamforming, one is **explicit** and the other is **implicit**. The difference between them is that Beamformer requires **explicit** feedback from Beamformee through some protocol packet echange. You could find well-explained details in the following website.
http://chimera.labs.oreilly.com/books/1234000001739/ch04.html

MT7915 supports both explicit and implicit beamforming.

16.1 Profile Parameter

16.1.1 ETxBfEnCond

Description: Enable or disable explicit TX beamforming
Value:

ETxBfEnCond=1

0: Disable
1: Enable

16.1.2 ITxBfEn

Description: Enable or disable implicit TX beamforming
Value:

ITxBfEn=0

0: Disable
1: Enable

Note:
Please be noted that iBF requires further phase calibration procedure. Also, you can turn on both eBF and iBF but eBF has higher priority than iBF if the connected client supports eBF.

17 Fixed Rate

17.1 Profile Parameter

17.1.1 FixedTxMode

Description: Fix Tx Mode for testing fixed rate
Value:

FixedTxMode=CCK

CCK
OFDM
HT

17.1.2 BasicRate

Description: Basic rate support
Value:

BasicRate=15

0~4095

Note:
We use a bitmap to configure basic support rate
1: Basic rate-1Mbps
2: Basic rate-2Mbps
3: Basic rate-1Mbps, 2Mbps
4: Basic rate-5.5Mbps
15: Basic rate-1Mbps, 2Mbps, 5.5Mbps, 11Mbps

Examples:

Basic Rate Bitmap												
Bit	11	10	9	8	7	6	5	4	3	2	1	0
Rate	54	48	36	24	18	12	9	6	11	5.5	2	1
Set	0	1	0	1	0	1	0	1	1	1	1	1
Hex	5				5				F			
Decimal	1375											

17.1.3 SupportRate

Description: Maximum support rate configuration for 11bg
Value:

SupportRate=0xFFF

Basic Rate Bitmap												
Bit	11	10	9	8	7	6	5	4	3	2	1	0
Rate	54	48	36	24	18	12	9	6	11	5.5	2	1
Set	1	1	1	1	1	1	1	1	1	1	1	1
Hex	F				F				F			

Note:
Unlike BasicRate, the SupportRate bitmap must be composed of consecutive 1s.
For example, if SupportRate=0x7F, it means the maximum support rate is OFDM 12M.
Also, this settings will be applied globally which means no per-SSID configuration is allowed.
Only RT5x92 supports this. Its macro is DYNAMIC_RX_RATE_ADJ.

17.1.4 SupportHTRate

Description: Maximum support rate configuration for 11n
Value:

SupportHTRate=0xFFFF

HT Rate Bitmap																
Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
MCS	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Set	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Hex	F				F				F				F			

Note:
Unlike BasicRate, the SupportHTRate bitmap must be composed of consecutive 1s.
For example, if SupportHTRate=0x7F, it means the maximum support rate is MCS 6.
Also, this settings will be applied globally which means no per-SSID configuration is allowed.
Only RT5x92 supports this. Its macro is DYNAMIC_RX_RATE_ADJ.

17.2 iwpriv Command

17.2.1 FixedTxMode

Description: Fix Tx Mode for testing fixed rate
Value:

iwpriv ra0 set FixedTxMode=CCK

CCK
OFDM
HT

17.2.2 BasicRate

Description: configure basic rate
Value:

iwpriv ra0 set BasicRate=15

0~4095

17.3 802.11n Data Rate Table

MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
16	3	BPSK	1/2	19.50	21.70	40.50	45.00
17	3	QPSK	1/2	39.00	43.30	81.00	90.00
18	3	QPSK	3/4	58.50	65.00	121.50	135.00
19	3	16-QAM	1/2	78.00	86.70	162.00	180.00
20	3	16-QAM	3/4	117.00	130.00	243.00	270.00
21	3	64-QAM	2/3	156.00	173.30	324.00	360.00
22	3	64-QAM	3/4	175.50	195.00	364.50	405.00
23	3	64-QAM	5/6	195.00	216.70	405.00	450.00
24	4	BPSK	1/2	26.00	28.80	54.00	60.00
25	4	QPSK	1/2	52.00	57.60	108.00	120.00
26	4	QPSK	3/4	78.00	86.80	162.00	180.00
27	4	16-QAM	1/2	104.00	115.60	216.00	240.00
28	4	16-QAM	3/4	156.00	173.20	324.00	360.00
29	4	64-QAM	2/3	208.00	231.20	432.00	480.00
30	4	64-QAM	3/4	234.00	260.00	486.00	540.00
31	4	64-QAM	5/6	260.00	288.80	540.00	600.00

17.4 2.4g

17.4.1 B only

iwpriv ra0 set FixedTxMode=CCK
iwpriv ra0 set WirelessMode=1 // 11b only
iwpriv ra0 set BasicRate=3 // 1, 2 Mbps

```
iwpriv ra0 set HtMcs=0                  // Please check Note-11b
iwpriv ra0 set SSID=11B_only_AP         // Restart AP
```

Note-11b:

HtMcs	0	1	2	3
Rate	1 Mbps	2 Mbps	5.5 Mbps	11 Mbps

17.4.2 G only

```
iwpriv ra0 set FixedTxMode=OFDM
iwpriv ra0 set WirelessMode=4           // 11g only
iwpriv ra0 set BasicRate=351            // 1, 2, 5.5, 11, 6, 12, 24 Mbps
iwpriv ra0 set HtMcs=0                  // Please check Note-11g
iwpriv ra0 set SSID=11G_only_AP         // Restart AP
```

Note-11g:

HtMcs	0	1	2	3	4	5	6	7
Rate	6 Mbps	9 Mbps	12 Mbps	18 Mbps	24 Mbps	36 Mbps	48 Mbps	54 Mbps

17.4.3 N only

```
iwpriv ra0 set FixedTxMode=HT
iwpriv ra0 set WirelessMode=6           // 2.4g 11n only
iwpriv ra0 set BasicRate=15             // 1, 2, 5.5, 11 Mbps
iwpriv ra0 set HtMcs=0                  // Please check Note-11n
iwpriv ra0 set HtGi=0
iwpriv ra0 set HtBw=0
iwpriv ra0 set SSID=11GN_only_AP        // Restart AP
```

Note-11n:
HtMcs=<0-15> + HtGi=<0-1> + HtBw=<0-1>
Please check all possible combination of above set in the frist section.

17.4.4 B/G/N mixed

```
iwpriv ra0 set FixedTxMode=HT
iwpriv ra0 set WirelessMode=9           // 11bgn mixed
iwpriv ra0 set BasicRate=15             // 1, 2, 5.5, 11 Mbps
iwpriv ra0 set HtMcs=0                  // Please check Note-11n
iwpriv ra0 set HtGi=0
iwpriv ra0 set HtBw=0
iwpriv ra0 set SSID=11BGN_mixed_AP      // Restart AP
```

Note-11n:

HtMcs=<0-15> + HtGi=<0-1> + HtBw=<0-1>
Please check all possible combination of above set in the first section.

17.5 5g

17.5.1 A only

iwpriv ra0 set FixedTxMode=**OFDM**
iwpriv ra0 set WirelessMode=**2** // 11a only
iwpriv ra0 set BasicRate=336 // 6, 12, 24 Mbps
iwpriv ra0 set HtMcs=0 // Please check Note-11a
iwpriv ra0 set SSID=11A_only_AP // Restart AP

Note-11a:

HtMcs	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Rate	6 Mbps	9 Mbps	12 Mbps	18 Mbps	24 Mbps	36 Mbps	48 Mbps	54 Mbps

17.5.2 N only

iwpriv ra0 set FixedTxMode=**HT**
iwpriv ra0 set WirelessMode=**11** // 5g 11n only
iwpriv ra0 set BasicRate=336 // 6, 12, 24 Mbps
iwpriv ra0 set HtMcs=0
iwpriv ra0 set HtGi=0
iwpriv ra0 set HtBw=0
iwpriv ra0 set SSID=11AN_only_AP // Restart AP

Note-11n:
HtMcs=<0-15> + HtGi=<0-1> + HtBw=<0-1>
Please check all possible combination of above set in the first section.

17.6 AP-Client

iwpriv apcli0 set ApCliTxMode=**HT**
iwpriv apcli0 set ApCliHtMcs=0
iwpriv ra0 set HtGi=0
iwpriv ra0 set HtBw=0
iwpriv ra0 set SSID=11N_only_AP // Restart AP

Note-11n:
ApCliHtMcs=<0-15> + HtGi=<0-1> + HtBw=<0-1>
Please check all possible combination of above set in the first section.

17.7 11ac

17.7.1 VHT Fixed Rate iwpriv command

17.7.1.1 fpga_on

Description: Turn on or off VHT fixed rate
Value:

iwpriv rai0 set fpga_on=6

0: Disable
6: Enable

17.7.1.2 dataphy

Description: PHY mode configuration
Value:

iwpriv rai0 set dataphy=4

0 = CCK
1 = OFDM
2 = HT-MM
3 = HT-GF
4 = VHT

17.7.1.3 databw

Description: Bandwidth configuration
Value:

iwpriv rai0 set databw=2

0 = 20M
1 = 40M
2 = 80M

17.7.1.4 datamcs

Description: MCS configuration
Value:

iwpriv rai0 set datamcs=24

Note
bit[3:0] stands for Modulation Coding Scheme (MCS)

Range: 0 - 9

bit[6:4] stands for Number of Spatial Stream (NSS)

0: 1SS

1: 2SS

Example:
datamcs=24 → 2SS MCS8
24 (dec) = 0x18 = b'0001,1000
bit[6:4] = b'001 = 1 (dec) → 2SS
bit[3:0] = b'1000 = 8 (dec) → MCS8

1SS & 2SS MCS Rate mapping table:

1SS

MCS Index	Modulation	Value (Dec)
0	BPSK	0
1	QPSK	1
2	QPSK	2
3	16-QAM	3
4	16-QAM	4
5	64-QAM	5
6	64-QAM	6
7	64-QAM	7
8	256-QAM	8
9	256-QAM	9

2SS

MCS Index	Modulation	Value (Dec)
0	BPSK	16
1	QPSK	17
2	QPSK	18
3	16-QAM	19
4	16-QAM	20
5	64-QAM	21
6	64-QAM	22
7	64-QAM	23
8	256-QAM	24
9	256-QAM	25

17.7.1.5 datagi

Description: Guard Interval configuration
Value:

iwpriv rai0 set datagi=0

0 = Long GI
1 = Short GI

17.7.2 VHT Fixed Rate example

```
iwpriv rai0 set WirelessMode=14
iwpriv rai0 set fpga_on=6  // Enable VHT fixed rate
iwpriv rai0 set dataphy=4  // VHT
iwpriv rai0 set databw=2          // 80MHz
iwpriv rai0 set datagi=0          // SGI
iwpriv rai0 set datamcs=25// 2SS MCS9
```

The following 802.11ac rate table is from http://www.revolutionwifi.net/.

802.11ac OFDM Data Rates

MCS	Modulation	Bits per Symbol	Coding Ratio	20-MHz		40-MHz		80-MHz	
				800ns	400ns	800ns	400ns	800ns	400ns
1 Spatial Stream				Data Rate (Mbps)					
MCS 0	BPSK	1	1/2	6.5	7.2	13.5	15.0	29.3	32.5
MCS 1	QPSK	2	1/2	13.0	14.4	27.0	30.0	58.5	65.0
MCS 2	QPSK	2	3/4	19.5	21.7	40.5	45.0	87.8	97.5
MCS 3	16-QAM	4	1/2	26.0	28.9	54.0	60.0	117.0	130.0
MCS 4	16-QAM	4	3/4	39.0	43.3	81.0	90.0	175.5	195.0
MCS 5	64-QAM	6	2/3	52.0	57.8	108.0	120.0	234.0	260.0
MCS 6	64-QAM	6	3/4	58.5	65.0	121.5	135.0	263.3	292.5
MCS 7	64-QAM	6	5/6	65.0	72.2	135.0	150.0	292.5	325.0
MCS 8	256-QAM	8	3/4	78.0	86.7	162.0	180.0	351.0	390.0
MCS 9	256-QAM	8	5/6	N/A	N/A	180.0	200.0	390.0	433.3
2 Spatial Streams				Data Rate (Mbps)					
MCS 0	BPSK	1	1/2	13.0	14.4	27.0	30.0	58.5	65.0
MCS 1	QPSK	2	1/2	26.0	28.9	54.0	60.0	117.0	130.0
MCS 2	QPSK	2	3/4	39.0	43.3	81.0	90.0	175.5	195.0
MCS 3	16-QAM	4	1/2	52.0	57.8	108.0	120.0	234.0	260.0
MCS 4	16-QAM	4	3/4	78.0	86.7	162.0	180.0	351.0	390.0
MCS 5	64-QAM	6	2/3	104.0	115.6	216.0	240.0	468.0	520.0
MCS 6	64-QAM	6	3/4	117.0	130.0	243.0	270.0	526.5	585.0
MCS 7	64-QAM	6	5/6	130.0	144.4	270.0	300.0	585.0	650.0
MCS 8	256-QAM	8	3/4	156.0	173.3	324.0	360.0	702.0	780.0
MCS 9	256-QAM	8	5/6	N/A	N/A	360.0	400.0	780.0	866.7

17.8 Fixed Rate for MT7615

17.8.1 FixedRate

Description: MT7615 fixed rate without auto fallback

iwpriv ra0 set FixedRate=
[WCID]-[Mode]-[BW]-[MCS]-[VhtNss]-[SGI]-[Preamble]-[STBC]-[LDPC]-[SPE_EN]

<Total 10 fields>
[WCID] Wireless Client ID
[Mode] CCK=0, OFDM=1, HT=2, GF=3, VHT=4
[BW] 20M=0, 40M=1, 80M=2, 160M=3
[MCS] CCK=0~3, OFDM=0~7, HT=0~32, VHT=0~9
[VhtNss] Nss=1~4
[SGI] Long=0, Short=1
[Preamble] Long=0, Short=1
[STBC] disable=0, enable=1
[LDPC] disable=0, enable=1
[SPE_EN] disable=0, enable=1

Example:
iwpriv ra0 set FixedRate=1-2-1-21-4-0-0-0-0-0

17.8.2 FixedRateFallback

Description: MT7615 fixed rate with auto fallback

iwpriv ra0 set FixedRateFallback=
[WCID]-[Mode]-[BW]-[MCS]-[VhtNss]-[SGI]-[Preamble]-[STBC]-[LDPC]-[SPE_EN]-[is5G]

<Total 11 fields>
[WCID] Wireless Client ID
[Mode] CCK=0, OFDM=1, HT=2, GF=3, VHT=4
[BW] 20M=0, 40M=1, 80M=2, 160M=3
[MCS] CCK=0~3, OFDM=0~7, HT=0~32, VHT=0~9
[VhtNss] Nss=1~4
[SGI] Long=0, Short=1
[Preamble] Long=0, Short=1
[STBC] disable=0, enable=1
[LDPC] disable=0, enable=1
[SPE_EN] disable=0, enable=1
[is5G] 2G=0, 5G=1

Example:
iwpriv ra0 set FixedRateFallback=1-2-1-21-4-0-0-0-0-0-0

Note:
You can use “iwpriv ra0 show stainfo” to get WCID (AID) assigned to the connected STA.

17.9 Fixed Rate for MT7915

17.9.1 Fixed Rate command

Iwpriv ra0 set FixedRate=
[WCID]-[Mode]-[BW]-[MCS]-[VhtNss]-[SGI]-[Preamble]-[STBC]-[LDPC]-[SPE-EN]

<Total 10 Fields>:
[WCID] Wireless Client ID
[Mode] CCK=0, OFDM=1, HT=2, GF=3, VHT=4, HE_SU=8, HE_ER=9
[BW] 20M=0, 40M=1, 80M=2, 160M=3

[MCS] CCK=0~3, OFDM=0~7, HT=0~32, VHT=0~9, HE_SU=0~11,
HE_ER=0~2(0~2 for 242-RU, 0 for 106-RU)
[VhtNss/HeNss] Nss=1~4 , HeNss=1~4, others=ignore
[VhtGI/HeGI] SGI=15, LGI=0 for VhtGI/ SGI=0, MGI=85, LGI=170 for HeGI
[Preamble] Long=0, Short=1 (for mode OFDM)
[STBC] disable=0, enable=1
[LDPC] disable=0, enable=7 (should be "enable" for BW>20MHz)
[SPE_EN] disable=0, enable=1

Examples:
iwpriv ra0 set FixedRate=1-8-2-11-1-0-0-0-7-0 (HE_SU MCS11 with 1nss and SGI)
iwpriv ra0 set FixedRate=1-8-2-11-2-85-0-0-7-0 (HE_SU MCS11 with 2nss and MGI)
iwpriv ra0 set FixedRate=1-4-2-9-2-15-0-0-7-0 (VHT MCS9 with 2nss)

17.9.2 Auto Rate Command

iwpriv ra0 set AutoRate=[WCID]:1
Example:
iwpriv ra0 set AutoRate=1:1

Note: Available on MT7915.

18 ACL

Access Control List (ACL) provides a way to accomplish MAC address filtering. You can use this feature to implement White List or Black List.

18.1 Profile Parameter

18.1.1 AccessPolicy0

Description: ACL access policy configuration for BSSID-0
Value:

AccessPolicy0=0

0: Disable
1: Allow all entries in the ACL table (white list)
2: Reject all entries in the ACL table (black list)

18.1.2 AccessControlList0

Description: ACL table entry configuration for BSSID-0
Value:

AccessControlList0=

[Mac Address];[Mac Address];...

Example:

00:10:20:30:40:50;0A:0b:0c:0D:0e:0f;1a:2b:3c:4d:5e:6f

Note: Maximum entry number is 64

18.1.3 AccessPolicy1

Description: ACL access policy configuration for BSSID-1
Value:

AccessPolicy1=0

0: Disable
1: Allow all entries in the ACL table (white list)
2: Reject all entries in the ACL table (black list)

18.1.4 AccessControlList1

Description: ACL table entry configuration for BSSID-1

Value:

AccessControlList1=

[Mac Address];[Mac Address];...

Example:

00:10:20:30:40:50;0A:0b:0c:0D:0e:0f;1a:2b:3c:4d:5e:6f

Note: Maximum entry number is 64

18.1.5 AccessPolicy2

Description: ACL access policy configuration for BSSID-2
Value:

AccessPolicy2=0

0: Disable
1: Allow all entries in the ACL table (white list)
2: Reject all entries in the ACL table (black list)

18.1.6 AccessControlList2

Description: ACL table entry configuration for BSSID-2
Value:

AccessControlList2=

[Mac Address];[Mac Address];...

Example:

00:10:20:30:40:50;0A:0b:0c:0D:0e:0f;1a:2b:3c:4d:5e:6f

Note: Maximum entry number is 64

18.1.7 AccessPolicy3

Description: ACL access policy configuration for BSSID-3
Value:

AccessPolicy3=0

0: Disable
1: Allow all entries in the ACL table (white list)
2: Reject all entries in the ACL table (black list)

18.1.8 AccessControlList3

Description: ACL table entry configuration for BSSID-3
Value:

AccessControlList3=

[Mac Address];[Mac Address];...

Example:

00:10:20:30:40:50;0A:0b:0c:0D:0e:0f;1a:2b:3c:4d:5e:6f

Note: Maximum entry number is 64

18.2 iwpriv Command

18.2.1 AccessPolicy

Description: ACL access policy configuration
Value:

iwpriv ra0 set AccessPolicy=0

0: Disable
1: Allow all entries in the ACL table (white list)
2: Reject all entries in the ACL table (black list)

18.2.2 ACLAddEntry

Description: Add new entry (MAC address) into ACL table
Value:

iwpriv ra0 set ACLAddEntry="xx:xx:xx:xx:xx:xx;yy:yy:yy:yy:yy:yy"

[MAC address];[MAC address];...;[MAC address]"

Note: Maximum entry number is 64

18.2.3 ACLDelEntry

Description: Remove old entry (MAC address) from ACL table
Value:

iwpriv ra0 set ACLDelEntry="xx:xx:xx:xx:xx:xx;yy:yy:yy:yy:yy:yy"

[MAC address];[MAC address];...;[MAC address]"

18.2.4 ACLClearAll

Description: Remove all entries from ACL table
Value:

iwpriv ra0 set ACLClearAll=1

18.2.5 ACLShowAll

Description: Dump all entries in ACL table
Value:

iwpriv ra0 set ACLShowAll=1

18.3 ACL example

18.3.1 White List

iwpriv ra0 set AccessPolicy=1
iwpriv ra0 set ACLAddEntry="00:0c:43:28:aa:12;00:0c:43:28:aa:11;00:0c:43:28:aa:10"
iwpriv ra0 set ACLShowAll=1

18.3.2 Black List

iwpriv ra0 set AccessPolicy=2
iwpriv ra0 set ACLAddEntry="00:0c:43:28:aa:12;00:0c:43:28:aa:11;00:0c:43:28:aa:10"
iwpriv ra0 set ACLShowAll=1

19 Intrusion Detection System

Intrusion Detection System (IDS) provides a way to protect your Wi-Fi device from some flooding attack. You have to turn on the macro IDS_SUPPORT to use this function.

19.1 Profile Parameter

19.1.1 IdsEnable

Description: Enable or disable Intrusion Detection System
Value:

IdsEnable=0

0: disable
1: enable

19.1.2 AuthFloodThreshold

Description: Authentication frame flooding threshold configuration
Value:

AuthFloodThreshold=32

0: disable
1~65535 (default=32)

19.1.3 AssocReqFloodThreshold

Description: Assocation request frame flooding threshold configuration
Value:

AssocReqFloodThreshold=32

0: disable
1~65535 (default=32)

19.1.4 ReassocReqFloodThreshold

Description: Reassocation request frame flooding threshold configuration
Value:

ReassocReqFloodThreshold=32

0: disable
1~65535 (default=32)

19.1.5 ProbeReqFloodThreshold

Description: Probe request frame flooding threshold configuration
Value:

ProbeReqFloodThreshold=32

0: disable
1~65535 (default=32)

19.1.6 DisassocFloodThreshold

Description: Disassocation frame flooding threshold configuration
Value:

DisassocFloodThreshold=32

0: disable
1~65535 (default=32)

19.1.7 DeauthFloodThreshold

Description: Deauthentication frame flooding threshold configuration
Value:

DeauthFloodThreshold=32

0: disable
1~65535 (default=32)

19.1.8 EapReqFloodThreshold

Description: EAP request frame flooding threshold configuration
Value:

EapReqFloodThreshold=32

0: disable
1~65535 (default=32)

20 IOCTL I/O Control Interface

20.1 Introduction

IOCTL is one way for a user space application to access the data declaimed and used in a kernel space driver. In case of WiFi, the most common application is to retrieve site survey data in the form of a structure array. It is much easier to manipulate the data retrieved via IOCTL than to parse the output printed by “iwpriv ra0 get_site_survey”. One thing you should pay attention to when using IOTCL is that the definition of exchanged data structures must be aligned. We usually copy the definition in driver to the user space application directly.

20.2 IOCTL in iwpriv

Parameters:

```
int     socket_id;
char    name[25];                   // interface name
char    data[255];                  // command string
struct  iwreq wrq;                  // defined in <linux/wireless.h>
```

Default values:

```
wrq.ifr_name = name = “ra0”;            // interface name
wrq.u.data.pointer = data;          // data buffer of command string
wrq.u.data.length = strlen(data);       // length of command string
wrq.u.data.flags = 0;
```

20.2.1 SET

Set Data		
Function Type	Command	IOCTL

RTPRIV_IOCTL_SET	iwpriv ra0 set SSID=RT2800AP	sprintf(name, "ra0");
		strcpy(data, "SSID=RT2800AP”);
		strcpy(wrq.ifr_name, name);
		wrq.u.data.length = strlen(data);
		wrq.u.data.pointer = data;
		wrq.u.data.flags = 0;
		ioctl(socket_id, RTPRIV_IOCTL_SET, &wrq);

20.2.2 GET

Get Data		
Function Type	Command	IOCTL

RTPRIV_IOCTL_STATISTICS	iwpriv ra0 stat	sprintf(name, "ra0");
		strcpy(data, "stat”);
		strcpy(wrq.ifr_name, name);
		wrq.u.data.length = strlen(data);
		wrq.u.data.pointer = data;

		wrq.u.data.flags = 0; ioctl(socket_id,RTPRIV_IOCTL_STATISTICS, &wrq);

RTPRIV_IOCTL_GSITESURVEY	iwpriv ra0 get_site_survey	sprintf(name, "ra0");
		strcpy(data, "get_site_survey");
		strcpy(wrq.ifr_name, name);
		wrq.u.data.length = strlen(data);
		wrq.u.data.pointer = data;
		wrq.u.data.flags = 0;
		ioctl(socket_id,RTPRIV_IOCTL_GSITESURVEY, &wrq);

RTPRIV_IOCTL_SHOW	iwpriv ra0 show	sprintf(name, "ra0");
		strcpy(data, "show wdsinfo");
		strcpy(wrq.ifr_name, name);
		wrq.u.data.length = strlen(data);
		wrq.u.data.pointer = data;
		wrq.u.data.flags = 0;
		ioctl(socket_id,RTPRIV_IOCTL_SHOW, &wrq);

20.3 Sample User Space Application

```
//==========================================================================
//
// rtuser:
//          1. User space application to demo how to use IOCTL function.
//          2. Use sscanf to get the raw data back from string message.
//          3. The command format "parameter=value" is same as iwpriv command format.
//          4. Remember to insert driver module and bring interface up prior execute rtuser.
//
// Make:
//                    cc -Wall -ortuser rtuser.c
// Run:
//                    ./rtuser
//
//==========================================================================

#include <stdio.h>
#include <string.h>
#include <sys/socket.h>
#include <sys/ioctl.h>
#include <unistd.h>
#include <linux/wireless.h>

#if WIRELESS_EXT <= 11
#ifndef SIOCDEVPRIVATE
#define SIOCDEVPRIVATE                          0x8BE0
#endif
#define SIOCIWFIRSTPRIV                         SIOCDEVPRIVATE
#endif

#define RT_PRIV_IOCTL                           (SIOCIWFIRSTPRIV + 0x01)
#define RTPRIV_IOCTL_SET                        (SIOCIWFIRSTPRIV + 0x02)
#define RTPRIV_IOCTL_BBP                        (SIOCIWFIRSTPRIV + 0x03)
#define RTPRIV_IOCTL_MAC                        (SIOCIWFIRSTPRIV + 0x05)
#define RTPRIV_IOCTL_E2P                        (SIOCIWFIRSTPRIV + 0x07)
#define RTPRIV_IOCTL_STATISTICS         (SIOCIWFIRSTPRIV + 0x09)
#define RTPRIV_IOCTL_ADD_PMKID_CACHE    (SIOCIWFIRSTPRIV + 0x0A)
```

```
#define RTPRIV_IOCTL_RADIUS_DATA                (SIOCIWFIRSTPRIV + 0x0C)
#define RTPRIV_IOCTL_GSITESURVEY        (SIOCIWFIRSTPRIV + 0x0D)
#define RTPRIV_IOCTL_ADD_WPA_KEY                (SIOCIWFIRSTPRIV + 0x0E)
#define RTPRIV_IOCTL_GET_MAC_TABLE(SIOCIWFIRSTPRIV + 0x0F)

#ifndef   TRUE
#define  TRUE    1
#endif
#ifndef   FALSE
#define  FALSE   0
#endif

#define MAC_ADDR_LEN                                    6
#define ETH_LENGTH_OF_ADDRESS                           6

typedef  struct _SITE_SURVEY {
        unsigned char           channel;
        unsigned short          rssi;
        unsigned char           ssid[33];
        unsigned char           bssid[6];
        unsigned char           security[9];
} SITE_SURVEY;

SITE_SURVEY             SiteSurvey[100];
char                    data[4096];

int main( int argc, char ** argv )
{
        char            name[25];
        int             socket_id;
        struct          iwreq wrq;
        int             ret;

        // open socket based on address family: AF_INET
        socket_id = socket(AF_INET, SOCK_DGRAM, 0);
        if (socket_id < 0)
        {
                printf("\nrtuser::error::Open socket error!\n\n");
                return -1;
        }

        // interface name as "ra0"
        sprintf(name, "ra0");

        // get wireless name
        strcpy(wrq.ifr_name, name);
        wrq.u.data.length = 255;
        memset(data, 0x00, 255);
        wrq.u.data.pointer = data;
        wrq.u.data.flags = 0;
        ret = ioctl(socket_id, SIOCGIWNAME, &wrq);
        if(ret != 0)
        {
                printf("\nrtuser::error::get wireless name\n\n");
                goto rtuser_exit;
        }

        printf("\nrtuser[%s]:%s\n", name, wrq.u.pointer);

        // iwpriv ra0 set WPAPSK=11223344
        memset(data, 0x00, 255);
        strcpy(data, "WPAPSK=11223344");
```

```
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = strlen(data)+1;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = 0;
	ret = ioctl(socket_id, RTPRIV_IOCTL_SET, &wrq);
	if(ret != 0)
	{
		printf("\nrtuser::error::set wpapsk\n\n");
		goto rtuser_exit;
	}

#if 0
	//iwpriv ra0 set SiteSurvey=1
	memset(data, 0x00, 255);
	strcpy(data, "SiteSurvey=1");
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = strlen(data)+1;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = 0;
	ret = ioctl(socket_id, RTPRIV_IOCTL_SET, &wrq);
	sleep(10);
#endif

	// iwpriv ra0 get_site_survey
	memset(data, 0x00, 4096);
	strcpy(data, "");
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = 4096;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = 0;
	ret = ioctl(socket_id, RTPRIV_IOCTL_GSITESURVEY, &wrq);
	if (ret != 0)
	{
		printf("\nrtuser::error::get site survey\n\n");
		goto rtuser_exit;
	}

	printf("\n========== Get Site Survey AP List ==========");
	if (wrq.u.data.length > 0)
	{
		printf("%s\n", wrq.u.data.pointer);
		// You can parse the string here and store the data to the SITE_SURVEY data structure
	}

	// iwpriv ra0 set SSID=rtuser
	memset(data, 0x00, 255);
	strcpy(data, "SSID=rtuser");
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = strlen(data)+1;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = 0;
	ret = ioctl(socket_id, RTPRIV_IOCTL_SET, &wrq);
	if (ret != 0)
	{
		printf("\nrtuser::error::set SSID\n\n");
		goto rtuser_exit;
	}

rtuser_exit:
	if (socket_id >= 0)
		close(socket_id);
```

```
	if (ret)
		return ret;
	else
		return 0;
}
```

21 HE 6G Connect

21.1 Configure 6G AP and APCLI by editing profile

Profile (6G) :

- WirelessMode=18 // 16: (HE_2G) / 17: (HE_5G) / 18: (HE_6G)
- Channel=37 // 1~14: (2G) / 36~165: (5G) / 1~233: (6G)
- SSID1=[SSID]
- VHT_BW=1 // 0: (BW40) / 1: (BW80) 2: (BW160)
- Country
  - CountryCode=US
  - CountryRegion=5
  - CountryRegionABand=0
- AuthMode=WPA3PSK
- EncrypType=AES
- WPAPSK=12345678
- PweMethod=2 // Add if parameter "PweMethod" not exist

21.2 Check APCLI's site survey result

iwpriv ra0 get_site_survey result

```
root@OpenWrt:/# iwpriv ra0 get_site_survey
ra0       get_site_survey:
Total=3
No  Ch  SSID                            BSSID             Security          Siganl(%)W-Mode  ExtCH      NT SSID_
Len WPS DPID BcnRept   MDId FToverDS RsrReqCap
0   37  BW_6G_YIWEI                     00:0c:43:aa:bb:00 WPA3PSK/AES       100      a/n/ac/ax   NONE    In 11
     NO      NO
1   37  MTK_MT7986_AP_AX8400_6G         c2:0c:43:59:a6:f9 WPA3PSK/AES       100      a/n/ac/ax   NONE    In 23
     NO      NO
2   37  asus_ss7_6G                     7c:10:c9:61:a0:b8 WPA3PSK/AES       100      a/n/ac/ax   NONE    In 11
     NO      NO

root@OpenWrt:/#
```

21.3 Check APCLI's site survey result

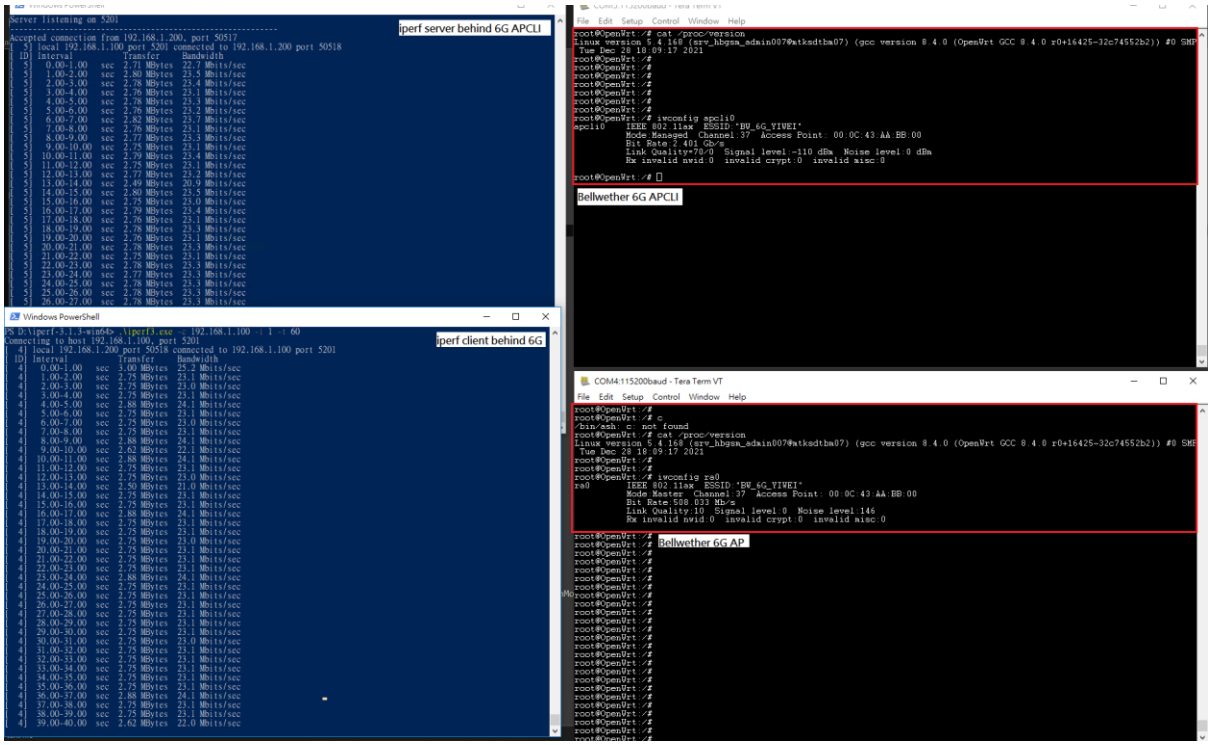
ifconfig apcli0 up
brctl addif br-lan apcli0

iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliAuthMode=WPA3PSK
iwpriv apcli0 set ApCliEncrypType=AES
iwpriv apcli0 set ApCliSsid=BW_6G_YIWEI
iwpriv apcli0 set ApCliWPAPSK=12345678
iwpriv apcli0 set ApCliEnable=1

21.4 Check AP and APCLI status

AP Status	APCLI Status
root@OpenWrt:/# iwconfig ra0 ra0 IEEE 802.11ax ESSID:"BW_6(Mode:Master Channel:37 Ac Bit Rate:508.033 Mb/s Link Quality:10 Signal lev Rx invalid nwid:0 invalid root@OpenWrt:/#	root@OpenWrt:/# iwconfig apcli0 apcli0 IEEE 802.11ax ESSID:"BW_6G_ Mode:Managed Channel:37 Ac Bit Rate:2.401 Gb/s Link Quality=70/0 Signal le Rx invalid nwid:0 invalid c root@OpenWrt:/#

21.5 Verify AP and APCLI connection by ping or iperf



22 Q&A

22.1 Why does WPAPSK not work?

Please make sure the parameter **"DefaultKeyID" is set to 2** in the configuration file.

22.2 How to switch driver to operate in 5G band?

Please make sure the IC supports 5G band.
Also, please configure the WirelessMode and Channel correctly.

22.3 How do I check my channel list?

Please check CountryRegion or CountryRegionABand.

22.4 How can I know the version of current WLAN Driver?

Please use the following command.
 # iwpriv ra0 show driverinfo

22.5 Can SoftAP support Antenna diversity?

No, SoftAP do not support antenna diversity even EEPROM has set antenna enabled.

22.6 TX & RX performance is always unbalance

When encounter TX & RX performance unbalance issue during Wi-Fi performance test, please check the TxBurst option is off or on. When TxBurst is on, the TX packets will have higher priority than RX packets. In the result, the WLAN TX performance will be higher than RX. This problem usual appears in Fast Ethernet + WLAN solution. GiGaBit Ethernet + WLAN solution doesn't have such problem.

How to turn off TxBurst?
By profile:
TxBurst=0
By iwpriv command:
iwpriv ra0 set TxBurst=0

22.7 Why can't I configure a SSID containing comma ","?

Please modify your code as follows.

```
==========
INT RTMPAPPrivIoctlSet(
	IN RTMP_ADAPTER *pAd,
	IN RTMP_IOCTL_INPUT_STRUCT *ploctlCmdStr)
{
	PSTRING this_char;
	PSTRING value;
	INT Status = NDIS_STATUS_SUCCESS;

	while ((this_char = strsep((char **)&ploctlCmdStr->u.data.pointer, "\0")) != NULL)
	{
		if (!*this_char)
			continue;

		if ((value = strchr(this_char, '=')) != NULL)
			*value++ = 0;
```

22.8 Why throughput is low when using 1SS to send traffic with legacy rate or MCS0-7?

Using 2SS to send traffic with legacy rate and MCS0-7 is our design by default. If you intend to change from 2SS to 1SS, please use TC instead of TSSI.

22.9 TGn 4.2.10 failed. Why does DUT not send MC traffic?

4.2.10 Group traffic with WPA2-PSK Only Mode and WPA/WPA2-PSK Mixed Mode
If this item fails, please turn off IGMP Snooping first.

22.10 TGn 4.2.29 failed. Why the performance cannot reach the criteria?

Please make sure that the following items are correctly configured.
<Profile>
TxPreamble=1
PktAggregate=0

<Driver Config>
-CONFIG_RA_NETWORK_WORKQUEUE_BH=y
+CONFIG_RA_NETWORK_TASKLET_BH=y

<Kernel Config>
Please check items in Networking Option & Core Netfilter in your kernel config. Remove those you do not use or know.

22.11 How to modify a profile with sed?

If vi/vim does not exist in your configuration, you can use sed to modify profile as well. The following is an example for your reference. We change HT_LDPC=1 to HT_LDPC=0.

sed -i 's/HT_LDPC=0/HT_LDPC=1/g' RT2860AP.dat

22.12 Do you have suggested kernel version for each chipset?

The following mapping has been fully verified by MTK and please develop your project according to this mapping.

22.13 Why does debug message not show up?

If "iwpriv ra0 set Debug=3" shows nothing, you may have to change the default kmsg printing level and please try to execute "dmesg -n 7" to manually adjust the level.