MTK Wi-Fi SoftAP Software Programming Guide

Version:	2.4
Release date:	2013-04-23

© 2008 - 2013 MediaTek Inc.
This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Specifications are subject to change without notice.

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

Document Revision History

Revision	Date	Author	Description
1.0	2012/11/08	Pan Liu	Initial Version
1.1	2012/11/13	Pan Liu	Update iwpriv command
1.2	2012/12/11	Pan Liu	Add NoForwardingMBCast
1.3	2013/01/04	Pan Liu	Add VHT_BW and VhtBW
1.4	2013/1/14	Pan Liu	Update Apclient WPS command sample
1.5	2013/1/22	Pan Liu	Add FAQ- FixTxMode iwpriv command sample
1.6	2013/1/23	Pan Liu	Add new DAT item VHT_DisallowNonVHT and SingleSKU.dat sample.
1.7	2013/3/6	Pan Liu	Add MAC Repeater section
1.8	2013/3/8	Pan Liu	Add command and profile, DFS debug example
1.9	2013/3/13	Pan Liu	Add Singlesku.dat 5G and 2.4G sample profile and DFS example update
2.0	2013/3/15	Pan Liu	Add IgmpAdd1, WPS command and NEW BSSID Mode MAC address limitation. Update BGProtection
2.1	2013/3/27	Pan Liu	Add EfuseUploadToHost
2.2	2013/3/28	Pan Liu	Add FAQ for TX/RX unbalance issue.
2.3	2013/4/23	Pan Liu	Add iNIC system address configuration for WLAN profile support
2.4	2013/4/23	Pan Liu	Add iwpriv command AP2040Rescan, WLAN profile updates

MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Table of Contents

MEDIATEK CONFIDENTIAL
FOR wangjian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL
FOR wangxiao@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

FOR wangxian@ cynchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL
FOR wangxiang@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

1 Introduction

This document is the Software programming guide for Mediatek Wi-Fi SoftAP driver. The Software Programming guide covers profile setting, command list, and OID examples to demonstrate how to programming the WLAN driver.

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2 Wi-Fi SoftAP driver Profile Default Setting

```
#The word of "Default" must not be removed
Default
CountryRegion=5
CountryRegionABand=7
CountryCode=TW
BssidNum=1
SSID=RT2860AP
WirelessMode=9
TxRate=0
Channel=11
BasicRate=15
BeaconPeriod=100
DtimPeriod=1
TxPower=100
DisableOLBC=0
BGProtection=0
TxAntenna=
RxAntenna=
TxPreamble=0
RTSThreshold=2347
FragThreshold=2346
TxBurst=1
PktAggregate=0
TurboRate=0
WmmCapable=0
APSDCapable=0
DLSCapable=0
APAifsn=3;7;1;1
APCwmin=4;4;3;2
APCwmax=6;10;4;3
APTxop=0;0;94;47
APACM=0;0;0;0
BSSAifsn=3;7;2;2
BSSCwmin=4;4;3;2
BSSCwmax=10;10;4;3
BSSTxop=0;0;94;47
BSSACM=0;0;0;0
AckPolicy=0;0;0;0
NoForwarding=0
NoForwardingBTNBSSID=0
HideSSID=0
StationKeepAlive=0
ShortSlot=1
AutoChannelSelect=0
IEEE8021X=0
IEEE80211H=0
CSPeriod=10
WirelessEvent=0
IdsEnable=0
```

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxian@cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
AuthFloodThreshold=32
AssocReqFloodThreshold=32
ReassocReqFloodThreshold=32
ProbeReqFloodThreshold=32
DisassocFloodThreshold=32
DeauthFloodThreshold=32
EapReqFooldThreshold=32
PreAuth=0
AuthMode=OPEN
EncrypType=NONE
RekeyInterval=0
RekeyMethod=DISABLE
PMKCachePeriod=10
WPAPSK=
DefaultKeyID=1
Key1Type=0
Key1Str=
Key2Type=0
Key2Str=
Key3Type=0
Key3Str=
Key4Type=0
Key4Str=
AccessPolicy0=0
AccessControlList0=
AccessPolicy1=0
AccessControlList1=
AccessPolicy2=0
AccessControlList2=
AccessPolicy3=0
AccessControlList3=
WdsEnable=0
WdsEncrypType=NONE
WdsList=
WdsKey=
RADIUS_Server=192.168.2.3
RADIUS_Port=1812
RADIUS_Key=ralink
own_ip_addr=192.168.5.234
EAPifname=br0
PreAuthifname=br0
HT_HTC=0
HT_RDG=0
HT_EXTCHA=0
HT_LinkAdapt=0
HT_OpMode=0
HT_MpduDensity=5
HT_BW=1
VHT_BW=0
HT_AutoBA=1
HT_AMSDU=0
HT_BAWinSize=64
HT_GI=1
```

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxian@cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
HT_MCS=33
WscManufacturer=
WscModelName=
WscDeviceName=
WscModelNumber=
WscSerialNumber=
RadioOn=1
```

2.1 WLAN Profile Description

Syntax is 'Param'='Value' and describes below.

SectionNumber **Param**
Value

. . .
. . .
. . .

The WLAN driver needs to be restart, after WLAN profile has been modified.
Otherwise settings will not take any effect.

A interface down/ up could do that.
EX:

```
ifconfig ra0 down
ifconfig ra0 up
```

2.1.1 CountryRegion

Description: Country region for WLAN radio 2.4G HZ regulation.
Value:

CountryRegion=5

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

MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.2 CountryRegionForABand

Description: Country region for WLAN radio 5G HZ regulation.
Value:

CountryRegionABand=7

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

2.1.3 CountryCode

Description: County Code for WLAN radio regulation.
Value: (Default is empty)

CountryCode=

2 characters, like TW for Taiwan.
Please refer to ISO3166 code list for other countries and can be found at
http://www.iso.org/iso/prods-services/iso3166ma/02iso-3166-code-lists/country_names_and_code_elements

Note:

1. This parameter can be set from EEPRM or EFUSE.
2. EEPROM/EFUSE has higher priority than the WLAN Profile.

2.1.4 ChannelGeography

Description: For Channel list builder
Value:

ChannelGeography=1
0: Outdoor
1: Indoor
2: Both

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangjian@cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.5 BssidNum

Description: multiple BSSID number
Value:

BssidNum=1

1/2/4/8/16

Note:

1. MAC Address alignment on MBSSID.
    1.1. Main BSSID have to insure MAC address is multiple of 2s on 2-BSSIDs' application.
    1.2. Main BSSID have to insure MAC address is multiple of 4s on 4-BSSIDs' application.
    1.3. Main BSSID have to insure MAC address is multiple of 8s on 8-BSSIDs' application.
2. Example 4 BSSIDs:

Align	1st	2nd	3rd	4th
0x00	AA-BB-CC-DD-EE-F0	AA-BB-CC-DD-EE-F1	AA-BB-CC-DD-EE-F2	AA-BB-CC-DD-EE-F3
0x04	AA-BB-CC-DD-EE-F4	AA-BB-CC-DD-EE-F5	AA-BB-CC-DD-EE-F6	AA-BB-CC-DD-EE-F7
0x08	AA-BB-CC-DD-EE-F8	AA-BB-CC-DD-EE-F9	AA-BB-CC-DD-EE-FA	AA-BB-CC-DD-EE-FB
0x0C	AA-BB-CC-DD-EE-FC	AA-BB-CC-DD-EE-FD	AA-BB-CC-DD-EE-FE	AA-BB-CC-DD-EE-FF

3. 16 BSSID support only on RT55XX serie chipset and after.

2.1.6 SSID

Description: The target BSSID string name
Value:

SSID=11n-AP

0~z, 1~32 ASCII characters.

2.1.7 SSID1

Description: The target BSSID string name
Value:

SSID1=11n-AP1

0~z, 1~32 ASCII characters.

2.1.8 SSID2

Description: The target BSSID string name
Value:

SSID2=11n-AP2

0~z, 1~32 ASCII characters.

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

2.1.9 SSID3

Description: The target BSSID string name
Value:

SSID3=11n-AP3

0~z, 1~32 ASCII characters.

2.1.10 SSID4

Description: The target BSSID string name
Value:

SSID4=11n-AP4

0~z, 1~32 ASCII characters.

2.1.11 WirelessMode

Description: Wireless Mode
Value:

WirelessMode=9

0: legacy 11b/g mixed
1: legacy 11B only
2: legacy 11A only
3: legacy 11a/b/g mixed
4: legacy 11G only
5: 11ABGN mixed
6: 11N only
7: 11GN mixed
8: 11AN mixed
9: 11BGN mixed
10: 11AGN mixed
11: 11N only in 5G band only
14: 11A/AN/AC mixed 5G band only (Only 11AC chipset support)

2.1.12 Channel

Description: WLAN Radio channel (2.4G Band or 5G band)
Value:

Channel=0

Depends on CountryRegion or CountryRegionForABand.
Default value = 0, the driver scan BSSID's channel automatically.

2.1.13 BasicRate

Description: Basic rate support

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Value:

BasicRate=15

0~4095

Note:

A bitmap represent basic support rate (A mode not support)
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 Bit Map (max. 12-bit, represent max. 12 basic rates)												
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											

Note:

Set correct basic rates set before changing wireless mode.

11B/G Mixed, 11B/G/N Mixed, and 11N Only:
iwpriv ra0 set BasicRate=15 ➔ (0x0F: 1, 2, 5.5, 11 Mbps)
11B:
iwpriv ra0 set BasicRate=3 ➔ (0x03: 1, 2 Mbps)
11G-Only and 11G/N Mixed:
iwpriv ra0 set BasicRate=351 ➔ (0x15F: 1, 2, 5.5, 11, 6, 12, 24 Mbps)

2.1.14 BeaconPeriod

Description: Beacon period setting (It is SoftAP only)

Value:

BeaconPeriod=100

2.1.15 DtimPeriod

Description: DTIM period

Value:

DtimPeriod=1

1~255

2.1.16 TxPower

Description: WLAN Radio Transmit Power setting in percentage

Value:

TxPower=100

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

0~100

2.1.17 DisableOLBC

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

DisableOLBC=0

0: disable
1: enable

2.1.18 BGProtection

Description: Enable/disable WLAN 11B or 11G protection
Value:

BGProtection=0

0: AUTO
1: On
2: Off

2.1.19 MaxStaNum

Description: Configure Maximun numbder of station that could connect with this SoftAP
Value:

MaxStaNum=0

0: disable
1~32

2.1.20 TxAntenna

Description: Configure Tx antenna number
Value:

TxAntenna=1

1: 1Tx1R
2: 2Tx2R
3: 3Tx3R

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.21 RxAntenna

Description: Configure Rx antenna number
Value:

RxAntenna=1

1: 1Tx1R
2: 2Tx2R
3: 3Tx3R

2.1.22 TxPreamble

Description: Enable or disable Tx preamble
Value:

TxPreamble=0

0: disable
1: enable

2.1.23 RTSThreshold

Description: Set RTS Threshold
Value:

RTSThreshold=2347

1~2347

2.1.24 FragThreshold

Description: Set Fragment threshold
Value:

FragThreshold=2346

256~2346

2.1.25 TxBurst

Description: Enable or disable Tx burst
Value:

TxBurst=1

0: disable
1: enable

FOR MEDIATEK CONFIDENTIAL wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.26 PktAggregate

Description: Enable or disable Tx Aggregate
Value:

PktAggregate=0

0: disable
1: enable

2.1.27 WmmCapable

Description: Enable or disable WMM QOS function
Value:

WmmCapable=1

0: disable
1: enable

2.1.28 APSDCapable

Description: Enable or disable WMM APSD function
Value:

APSDCapable=0

0: disable
1: enable

2.1.29 DLSCapable

Description: Enable or disable DLS function (Ralink proprietary function, Ralink 11n STA support only)
Value:

DLSCapable=0

0: disable
1: enable

2.1.30 APAifsn

Description: WMM parameter for AP
Value:

APAifsn=3;7;1;1

AC_BE;AC_BK;AC_VI;AC_VO

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

MEDIATEK CONFIDENTIAL FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.31 APCwmin

Description: WMM parameter for AP
Value:

```
APCwmin=4;4;3;2

AC_BE;AC_BK;AC_VI;AC_VO
```

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.32 APCwmax

Description: WMM parameter for AP
Value:

```
APCwmax=6;10;4;3

AC_BE;AC_BK;AC_VI;AC_VO
```

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.33 APTxop

Description: WMM parameter for AP
Value:

```
APTxop=0;0;94;47

AC_BE;AC_BK;AC_VI;AC_VO
```

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.34 APACM

Description: WMM parameter for AP
Value:

```
APACM=0;0;0;0

AC_BE;AC_BK;AC_VI;AC_VO
```

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.35 BSSAifsn

Description: WMM parameter for station
Value:

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

BSSAifsn=3;7;2;2

AC_BE;AC_BK;AC_VI;AC_VO

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.36 BSSCwmin

Description: WMM parameter for station
Value:

BSSCwmin=4;4;3;2

AC_BE;AC_BK;AC_VI;AC_VO

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.37 BSSCwmax

Description: WMM parameter for station
Value:

BSSCwmax=10;10;4;3

AC_BE;AC_BK;AC_VI;AC_VO

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.38 BSSTxop

Description: WMM parameter for station
Value:

BSSTxop=0;0;94;47

AC_BE;AC_BK;AC_VI;AC_VO

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.39 BSSACM

Description: WMM parameter for station
Value:

BSSACM=0;0;0;0

MEDIATEK CONFIDENTIAL
FOR wangxian@cwnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

AC_BE;AC_BK;AC_VI;AC_VO

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.40 AckPolicy

Description: Ack policy supports normal Ack or no Ack (AC_BK, AC_BE, AC_VI, AC_VO)
Value:

AckPolicy=0;0;0;0

0: No ack
1: normal Ack

Note: All WMM parameters do not support iwpriv command but 'WmmCapable'', please store all parameter to RT2800AP.dat, and restart driver.

2.1.41 NoForwarding

Description: enable or disable No forwarding STA packet within the same BSSID
Value:

NoForwarding=0

0: disable
1: enable

2.1.42 NoForwardingBTNBSSID

Description: enable or disable No Forwarding between each BSSID interface.
Value:

NoForwardingBTNBSSID=0

0: disable
1: enable

2.1.43 NoForwardingMBCast

Description: enable or disable No Forwarding multicast/broadcast packets between each BSSID interface.
Value:

NoForwardingMBCast=0

0: disable
1: enable

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxian@cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.44 HideSSID

Description: enable or disable Hidden SSID support
Value:

HideSSID=0

0: disable
1: enable

2.1.45 StationKeepAlive

Description: enable or disable Auto-detect the alive status of the station periodically
Value:

StationKeepAlive=0

0: disable
1~65535 seconds

2.1.46 ShortSlot

Description: enable or disable short slot time
Value:

ShortSlot=1

0: disable
1: enable

2.1.47 AutoChannelSelect

Description: enable or disable Auto Channel Select support
Value:

AutoChannelSelect=0

0: disable
1: Old Channel Selection Algorithm
2: New Channel Selection Algorithm

2.1.48 IEEE8021X

Description: enable or disable 8021X-WEP mode on, this field is enabled only when Radius-WEP or Radius-NONE mode on, otherwise must disable.
Value:

IEEE8021X=0

MEDIATEK CONFIDENTIAL FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

0: disable
1: enable

2.1.49 IEEE80211H

Description: enable or disable IEEE 802.11H support (DFS)
Value:

IEEE80211H=0

0: disable
1: enable

2.1.50 CSPeriod

Description: Set how many beacons with Channel Switch Announcement Element will be sent before changing a new channel.
Value:

CSPeriod=10

0 ~ 255. The default is 10.

Note: Channel switch period (Beacon count), unit is based on Beacon interval.

2.1.51 WirelessEvent

Description: enable or disable sending wireless event to the system log (Linux only)
Value:

WirelessEvent=0

0: disable
1: enable

2.1.52 IdsEnable

Description: enable or disable intrusion detection system
Value:

IdsEnable=0

0: disable
1: enable

2.1.53 AuthFloodThreshold

Description: enable or disable Authentication frame flood threshold
Value:

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

AuthFloodThreshold=32

0: disable
1~65535. (default=32)

2.1.54 ReassocReqFloodThreshold

Description: enable or disable Reassocation request frame flood threshold
Value:

ReassocReqFloodThreshold=32

0: disable
1~65535. (default=32)

2.1.55 ProbeReqFloodThreshold=32

Description: enable or disable Probe request frame flood threshold
Value:

ProbeReqFloodThreshold=32

0: disable
1~65535. (default=32)

2.1.56 DisassocFloodThreshold

Description: enable or disable disassocation frame flood threshold
Value:

DisassocFloodThreshold=32

0: disable
1~65535. (default=32)

2.1.57 DeauthFloodThreshold

Description: enable or disable deauthentication frame flood threshold
Value:

DeauthFloodThreshold=32

0: disable
1~65535. (default=32)

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.58 EapReqFooldThreshold

Description: enable or disable EAP request frame flood threshold
Value:

EapReqFooldThreshold=32

0: disable
1~65535. (default=32)

2.1.59 PreAuth

Description: enable or disable WPA2 pre-authentication mode
Value:

PreAuth=0

0: disable
1: enable

2.1.60 AuthMode

Description: WLAN security Authentication mode
Value:

AuthMode=OPEN

OPEN	For open system
SHARED	For shared key system
WEPAUTO	Auto switch between OPEN and SHARED
WPAPSK	For WPA pre-shared key (Infra)
WPA2PSK	For WPA2 pre-shared key (Infra)
WPANONE	For WPA pre-shared key (Adhoc)
WPA	For enterprise mode (Need wpa_supplicant)
WPA2	For enterprise mode (Need wpa_supplicant)

2.1.61 EncrypType

Description: WLAN security Encryption type
Value:

EncrypType=NONE

NONE	For AuthMode=OPEN
WEP	For AuthMode=OPEN or AuthMode=SHARED
TKIP	For AuthMode=WPAPSK or WPA2PSK
AES	For AuthMode=WPAPSK or WPA2PSK

FOR wangxiang@vnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.62 RekeyInterval

Description: Set group rekey interval. 0 to disable rekey. Unit:1seconds/1000packets dependent on Rekeytype.
Value:

RekeyInterval=0

0~0x3FFFFFFF

2.1.63 RekeyMethod

Description: Set group rekey interval-unit's type for WPA2.
Value:

RekeyMethod=DISABLE

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

2.1.64 PMKCachePeriod

Description: Set the alive time of PMKID in PMK-Cache table for WPA2.
Value:

PMKCachePeriod=10

0~65535 (unit minutes)

2.1.65 WPAPSK

Description: WLAN Security string for (TKIP/AES)
Value:

WPAPSK=

8~63 ASCII
Or
64 HEX characters

2.1.66 DefaultKeyID

Description: Default key ID
Value:

DefaultKeyID=1

1~4

FOR wangxian@ cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.67 Key1Type

Description: Key 1 type
Value:

Key1Type=0

0: Hexadecimal type
1: ASCII type

2.1.68 Key1Str

Description: Key 1 string
Value:

Key1Str=
10 or 26 characters (key type=0)
5 or 13 characters (key type=1)

2.1.69 Key2Type

Description: Key 2 type
Value:

Key2Type=0

0: Hexadecimal type
1: ASCII type

2.1.70 Key2Str

Description: Key 2 string
Value:

Key2Str=
10 or 26 characters (key type=0)
5 or 13 characters (key type=1)

2.1.71 Key3Type

Description: Key 3 type
Value:

Key3Type=0

0: Hexadecimal type
1: ASCII type

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.72 Key3Str

Description: Key 3 string
Value:

Key3Str=
10 or 26 characters (key type=0)
5 or 13 characters (key type=1)

2.1.73 Key4Type

Description: Key 4 type
Value:

Key4Type=0

0: Hexadecimal type
1: ASCII type

2.1.74 Key4Str

Description: Key 4 string
Value:

Key4Str=
10 or 26 characters (key type=0)
5 or 13 characters (key type=1)

2.1.75 AccessPolicy0

Description: Set the access policy of ACL table 0.
Value:

AccessPolicy0=0

0: Disable this function
1: Allow all entries of ACL table to associate AP
2: Reject all entries of ACL table to associate AP

2.1.76 AccessControlList0

Description: Set the entry's MAC address into ACL table 0.
Value:

AccessControlList0=

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

Example:

MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

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

Note: ACL for Bssid0, max=64

2.1.77 AccessPolicy1

Description: Set the access policy of ACL table 1.
Value:

AccessPolicy1=0

0: Disable this function
1: Allow all entries of ACL table to associate AP
2: Reject all entries of ACL table to associate AP

2.1.78 AccessControlList1

Description: Set the entry's MAC address into ACL table 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: ACL for Bssid0, max=64

2.1.79 AccessPolicy2

Description: Set the access policy of ACL table 2.
Value:

AccessPolicy2=0

0: Disable this function
1: Allow all entries of ACL table to associate AP
2: Reject all entries of ACL table to associate AP

2.1.80 AccessControlList2

Description: Set the entry's MAC address into ACL table2.
Value:

AccessControlList2=

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

Example:

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangjian@cvnchina.com USE ONLY

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

Note: ACL for Bssid0, max=64

2.1.81 AccessPolicy3

Description: Set the access policy of ACL table 3.
Value:

AccessPolicy3=0

0: Disable this function
1: Allow all entries of ACL table to associate AP
2: Reject all entries of ACL table to associate AP

2.1.82 AccessControlList3

Description: Set the entry's MAC address into ACL table 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: ACL for Bssid0, max=64

2.1.83 WdsEnable

Description: config WDS mode
Value:

WdsEnable=0

0: Disable - Disable all WDS function.
1: Restrict mode - Same as Repeater mode.
2: Bridge mode - Turn on WDS function, the peer WDS APs are according to the mac address listed in "WdsList" field below. In this mode, AP will not send beacon out and will not deal with probe request packets, therefore STA will not possible to connect with it.
3: Repeater mode - Turn on WDS function, the peer WDS APs are according to the mac address listed in "WdsList" field below.
4: Lazy mode - Turn on WDS function, and auto learning from WDS packet which with addr4 field.

2.1.84 WdsEncrypType

Description:

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangjian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Value:

WdsEncrypType=NONE

NONE
WEP
TKIP
AES

For example:

WdsEncrypType=OPEN;TKIP;WEP;AES
The encrptytion of wds0 is OPEN
The encrptytion of wds1 is TKIP
The encrptytion of wds2 is WEP
The encrptytion of wds3 is AES

2.1.85 WdsList

Description: WDS list
Value:

WdsList=

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

Note: maximum WDS-link is 4.

2.1.86 WdsKey

Description: The key for WDS link
Value:

WdsKey=

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

2.1.87 RADIUS_Server

Description: Configure radius server IP address
Value:

RADIUS_Server=

IP address.
Example: RADIUS_Server=192.168.2.3

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.88 RADIUS_Port

Description: Configure radius server port number
Value:

    RADIUS_Port=1812
    Deafult: 1812

2.1.89 RADIUS_Key

Description: Configure radius key string
Value:

    RADIUS_Key=

    Example:
        RADIUS_Key=ralink

2.1.90 own_ip_addr

Descripion: Configure SoftAP itself IP Address
Value:

    own_ip_addr=

    Example:
        own_ip_addr=192.168.1.1

2.1.91 EAPifname

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

    EAPifname=

    Example:
        EAPifname=br0

2.1.92 PreAuthifname

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

    PreAuthifname=

    Example:

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

PreAuthifname=br0

2.1.93 HT_HTC

Description: enable or disable Support the HT control field
Value:

HT_HTC=0

0: disable
1: enable

Note: HTC Control field(4-octet) is following QOS field. An MPDU that contains the HT control field is referred to as a +HTC frame.

2.1.94 HT_RDG

Description: Enable or disable HT Reverse Direction Grant
Value:

HT_RDG=1

0: disable
1: enable

2.1.95 HT_EXTCHA

Description: To locate the 40MHz channel in combination with the control
Value:

HT_EXTCHA=0

0: Below
1: Above

2.1.96 HT_LinkAdapt

Decription: enable ir disable HT Link Adaptation Control
Value:

HT_LinkAdapt=0

0: disable
1: enable

2.1.97 HT_OpMode

Description: HT operation mode

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Value:

HT_OpMode=0

0: HT mixed mode
1: HT Greenfield mode

2.1.98 HT_MpduDensity

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

HT_MpduDensity=4

0~7
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

2.1.99 HT_BW

Description: HT channel Bandwidth
Value:

HT_BW=1

0: 20 MHz
1: 40 MHz

2.1.100 VHT_BW

Description: Enable/disable 11AC 80MHz Bandwidth Support
Value:

VHT_BW=1

0: disable
1: enable

Note: 11AC chipset only.

2.1.101 VHT_DisallowNonVHT

Description: Enable/disable to reject non-VHT STA to connect
Value:

VHT_DisallowNonVHT=1

MEDIATEK CONFIDENTIAL FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

0: disable
1: enable to reject non-VHT STA

Note: 11AC chipset only.

2.1.102 HT_BADecline

Description: Enable or disable decline Block Ack to peer
Value:

HT_BADecline=0

0: disable
1: enable

2.1.103 HT_AutoBA

Description: Enable or disable auto build Block Ack section with peer
Value:

HT_AutoBA=1

0: disable
1: enable

2.1.104 HT_AMSDU

Description: Enable or disable AMSDU section
Value:

HT_AMSDU=0

0: disable
1: enable

2.1.105 HT_BAWinSize

Description: Block Ack window size
Value:

HT_BAWinSize=64

1~64

2.1.106 HT_GI

Description: HT Guard interval support
Value:

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

HT_GI=1

0: Long guard interval
1: short guard interval

2.1.107 HT_MCS

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

HT_MCS=33

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

2.1.108 HT_MIMOPSMode

Description: 802.11n SM power save mode
Value:

HT_MIMOPSMode=3

0: Static SM Power Save Mode
2: Reserved
1: Dynamic SM Power Save Mode
3: SM enabled
(not fully support yet)

2.1.109 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

2.1.110 HT_STBC

Description: Enable or disable HT STBC support
Value:

HT_STBC=0

0: disable
1: enable

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.111 WscManufacturer

Description: WPS manufacturer string
Value:

WscManufacturer=

Less than 64 characters

2.1.112 WscModelName

Description: WPS Mode name string
Value:

WscModelName=

Less than 32 characters

2.1.113 WscDeviceName

Description: WPS Device name string
Value:

WscDeviceName=

Less than 32 characters

2.1.114 WscModelNumber

Description: WPS Device model number string
Value:

WscModelNumber=

Less than 32 characters

2.1.115 WscSerialNumber

Description: WPS serial number string
Value:

WscSerialNumber=

Less than 32 characters

2.1.116 Wsc4digitPinCode

Description: WPS 4 digit pin code string

MEDIATEK CONFIDENTIAL FOR wangjian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Value:

    Wsc4digitPinCode=0

    4 digit

2.1.117 MACRepeaterEn

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

    MACRepeaterEn=0

    0: Disable
    1: Enable

2.1.118 PMFMFPC

Description: Disable or enable Protection Management Frame Capable
Value:

    PMFMFPC=0

    0: Disable
    1: Enable

2.1.119 PMFMFPR

Description: Disable or enable Protection Management Frame Required
Value:

    PMFMFPR=0

    0: Disable
    1: Enable

2.1.120 PMFSHA256

Description: Disable or enable use SHA256 for Encryption
Value:

    PMFSHA256=0

    0: Disable
    1: Enable

2.1.121 VLANID

Description: set VLAN ID
Value:

    VLANID=0

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

0: Disable

2.1.122 VLANPriority

Description: set VLAN Priority
Value:

VLANPriority=0

0: Disable

2.1.123 Ext_LNA

Description: support External or internal LNA
Value:

Ext_LNA

0: Internal LNA
1: External LNA

Note: MT7620 iNIC driver only profile

2.1.124 Ext_PA

Description: support External or internal PA
Value:

Ext_PA

0: Internal PA
1: External PA

Note: MT7620 iNIC driver only profile

2.1.125 ExtEEPROM

Description: Support driver to read EEPROM from an external file
Value:

ExtEEPROM=1

0: read EERPM data from EEPROM chip
1: read EEPROM data from an external file

Note: The external EEPROM file must be exactly the same format as EEPROM format.
iNIC driver only profile.

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

2.1.126 Mem

Description: Support WLAN profile can configure iNIC system address value
Value:

    Mem=addr1,value1;addr2,value2;

Example:

    Mem=b0110014,ff7f5555;b011008c,2404040;
    iNIC firmware will Set
    1. memory address (0xb0110014) value (0xff7f5555);
    2. memory address (0xb011008c) value (0x2404040);

Note: This parameter is only for iNIC driver.

2.1.127 IgmpAdd1

Description: Add wihte list to passthrough IGMPsnooping
Value:

    IgmpAdd1=MAC address-MAC address-MAC address

Example:

    IgmpAdd1=01:00:5e:7f:ff:fa-01:00:5e:00:00:fb

Note: update to 32 set of MAC address.

2.1.128 E2pAccessMode

Description: Select the EEPROM access mode from interface start-up
Value:

    E2pAccessMode=2

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

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3 Wi-Fi SoftAP driver iwpriv command

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

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

3.1.1 Debug

Description: config WLAN driver Debug level.
Value:

```
iwpriv ra0 set Debug=3
```

0~5
0: Debug Off
1: Debug Error
2: Debug Warning
3: Debug Trace
4: Debug Info
5: Debug Loud

3.1.2 DriverVersion

Description: Check driver version by iwpriv command. (Need to enable debug mode)
Value:

```
iwpriv ra0 set DriverVersion=0
```

Any value

3.1.3 CountryRegion

Description: Set Country Region
Value:

```
iwpriv ra0 set CountryRegion=1
```

Region	Channels
0	1-11
1	1-13
2	10-11
3	10-13
4	14
5	1-14

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

6	3-9
7	5-13
31	1-14
32	1-11 active scan, 12 and 13 passive scan
33	1-14 all active scan, 14 b mode only

3.1.4 CountryRegionABand

Description: Set Country Region for 5G Hz WLAN regulation
Value:

```
iwpriv ra0 set CountryRegionABand=7
```

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

3.1.5 CountryCode

Description: configure country code
Value:

```
iwpriv ra0 set CountryCode=TW
```

2 characters, like TW for Taiwan.

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

3.1.6 AccessPolicy

Description: Configure access policy of ACL table
Value:

```
iwpriv ra0 set AccessPolicy=0
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

0: Disable this function
1: Allow all entries of ACL table to associate AP
2: Reject all entries of ACL table to associate AP

3.1.7 ResetCounter

Description:Reset all statistic counter
Value:

```
iwpriv ra0 set ResetCounter=1
```

3.1.8 RadioOn

Description: enable or disable RF
Value:

```
iwpriv ra0 set RadioOn=1
```

0: off
1: on

3.1.9 SiteSurvey

Description: In SoftAP mode to issue a site survey to the driver.
Value:

```
iwpriv ra0 set SiteSurvey=1
```

1

3.1.10 CountryString

Description: configure country string
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

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

	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

FOR wangtian@xiaomi.com USE ONLY MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

	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

3.1.11 SSID

Description: Set AP SSID

Value:

```
iwpriv ra0 set SSID=11n-AP
```

0~z, 1~32 ASCII characters

3.1.12 WirelessMode

Description: Set WLAN mode

Value:

```
iwpriv ra0 set WirelessMode=5
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

FOR wangxian@cymmetrik.com USE ONLY
MEDIATEK CONFIDENTIAL

0: legacy 11b/g mixed
1: legacy 11B only
2: legacy 11A only
3: legacy 11a/b/g mixed
4: legacy 11G only
5: 11ABGN mixed
6: 11N only
7: 11GN mixed
8: 11AN mixed
9: 11BGN mixed
10: 11AGN mixed
11: 11N only in 5G band only
14: 11A/AN/AC mixed 5G band only (Only 11AC chipset support)

3.1.13 FixedTxMode

Description: Fix Tx mode to CCK or OFDM for MCS rate selection
Value:

```
iwpriv ra0 set FixedTxMode=CCK
```

CCK
OFDM

3.1.14 OFDMBasicRate

Description: configure OFDM basic rate
Value:

```
iwpriv ra0 set OFDMBasicRate=
```

0~4095

Basic Rate Bit Map (max. 12-bit, represent max. 12 basic rates)												
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											

Note: Be careful to set this value, if you don't know what this is, please don't set this field.

3.1.15 Channel

Description: Configure Wi-Fi Channel
Value:

```
iwpriv ra0 set Channel=6
```

MEDIATEK CONFIDENTIAL FOR wangxm@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

802.11b/g:	1 ~ 14 (it must agree with the CountryRegion setting)
802.11a:	36~165 (it must agree with the CountryRegionABand setting)

3.1.16 BeaconPeriod

Description: configure Beacon period
Value:

```
iwpriv ra0 set BeaconPeriod=100
```

20 ~ 1024 (unit is in milli-seconds)

3.1.17 DtimPeriod

Description: Configure DTIM period
Value:

```
iwpriv ra0 set DtimPeriod=1
```

1~5

3.1.18 TxPower

Description: Set Transmit Power by percentage
Value:

```
iwpriv ra0 set TxPower=100
```

0~100

Note:

91 ~ 100% & AUTO, 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
0 ~ 9 %, treat as MIN(~3%) in terms of mW	-12dBm

3.1.19 BGProtection

Description: Enable or disable 11B, 11G protection
Value:

```
iwpriv ra0 set BGProtection=0
```

0: disable
1: Always on
2:Always off

MEDIATEK CONFIDENTIAL FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.20 DisableOLBC

Description: enable or disable OLBC
Value:

```
iwpriv ra0 set DisableOLBC=0

0: disable
1: enable
```

3.1.21 TxPreamble

Description: enable or disable Tx preamble
Value:

```
iwpriv ra0 set TxPreamble=1

0: disable
1: enable
```

3.1.22 RTSThreshold

Description: Set RTS Threshold
Value:

```
iwpriv ra0 set RTSThreshold=2347

1~2347
```

3.1.23 FragThreshold

Description: Set Fragment threshold
Value:

```
iwpriv ra0 set FragThreshold=2346

256~2346
```

3.1.24 TxBurst

Description: enable or disable Tx burst mode
Value:

```
iwpriv ra0 set TxBurst=0

0: disable
1: enable
```

FOR MEDIATEK CONFIDENTIAL USE ONLY wangxian@cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.25 PktAggregate

Description: enable or disable packet aggregation (Ralink to Ralink only)
Value:

```
iwpriv ra0 set PktAggregate=1

0: disable
1: enable
```

3.1.26 NoForwarding

Description: enable or disable no forwarding packet between STAs in the same BSSID
Value:

```
iwpriv ra0 set NoForwarding=0

0: disable
1: enable
```

3.1.27 NoForwardingBTNBSSID

Description: enable or disable No Forwarding between each BSSID interface.
Value:

```
iwpriv ra0 set NoForwardingBTNBSSID=1

0: disable
1: enable
```

3.1.28 NoForwardingMBCast

Description: enable or disable No Forwarding multicast/broadcast packets between each BSSID interface.
Value:

```
iwpriv ra0 set NoForwardingMBCast=1

0: disable
1: enable
```

3.1.29 HideSSID

Description: enable or disable hidden SSID
Value:

```
iwpriv ra0 set HideSSID=1

0: disable
1: enable
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

3.1.30 ShortSlot

Description: enable or disabllle short slot time
Value:

```
iwpriv ra0 set ShortSlot=0
```

0: disable
1: enable

3.1.31 DisConnectSta

Description: Disconnect one specific STA which connected with this SoftAP manually
Value:

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

[MAC address]

3.1.32 DisConnectAllSta

Description: Disconnect all STAs which connected with this SoftAP manually.
Value:

```
iwpriv ra0 set DisconnectAllSta=1
```

1

3.1.33 McastPhyMode

Description: Configure multicast physical mode
Value:

```
iwpriv ra0 set McastPhyMode=0
```

0:	Disable
1:	CCK
2:	OFDM
3	HTMIX

3.1.34 McastMcs

Description: Specify the MCS of multicast packets.
Value:

```
iwpriv ra0 set McastMcs=0
```

0~15

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.35 WscVendorPinCode

Description: Set vendor pin code as pin code of WPS AP's enrollee
Value:

```
iwpriv ra0 WscVendorPinCode=xxxxxxx

xxxxxxxx //Valid PIN code
```

3.1.36 ACLAddEntry

Description: To insert one or several MAC addresses into Access control MAC table list, up to 64 MAC address at one time.
Value:

```
iwpriv ra0 set ACLAddEntry="xx:xx:xx:xx:xx:xx"

[MAC address];[MAC address];...;[MAC address]"
Example:
iwpriv ra0 set
ACLAddEntry="00:0c:43:28:aa:12;00:0c:43:28:aa:11;00:0c:43:28:aa:10"
```

3.1.37 ACLClearAll

Description: To clear all the MAC address entries in an Access control MAC table list.
Value:

```
iwpriv ra0 set ACLClearAll=1

1: indicate to clear the table
Other value is invalid.
```

3.1.38 FixedTxMode

Description: To limit the transmission mode only for CCK and OFDM
Value:

```
iwpriv ra0 set FixedTxMode=CCK

CCK
OFDM
```

3.1.39 WpaMixPairCipher

Description: It provides a more flexible cipher combination.
Value:

```
iwpriv ra0 set WpaMixPairCipher=WPA_AES_WPA2_TKIPAES
```

FOR MEDIATEK CONFIDENTIAL wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

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

3.1.40 MaxStaNum

Description: To limit the maximum number of associated clients per BSS.
Value:

```
iwpriv ra0 set MaxStaNum=0
```

0: disable this function
1~32 (default:32)

3.1.41 AutoFallBack

Description: enable or disable auto fall back rate control function
Value:

```
iwpriv ra0 set AutoFallBack=1
```

0: disable
1: enable

3.1.42 ApCliTxMode

Description: Configure APclient Tx traffic mode
Value:

```
iwpriv apcli0 set ApCliTxMode=HT
```

CCK
OFDM
HT

3.1.43 ApCliTxMcs

Description: Set transmission MCS for AP-Client traffic.
Value:

```
iwpriv apcli0 set ApCliTxMcs=33
```

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

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.44 GreenAP

Description: enable or disable Green AP fucntion
Value:

```
iwpriv ra0 set GreenAP=0
```

0: disable
1: enable

3.1.45 AutoChannelSel

Description: auto channel select when driver is loaded
Value:

```
iwpriv ra0 set AutoChannelSel=2
```

0:	Disable
1:	Old Channel Selection Algorithm
2:	New Channel Selection Algorithm

3.1.46 MBSSWirelessMode

Description: Set MBSS Wireless phy Mode. Only support in v2.5.0.0 and after version.
Value:

0:	802.11 B/G mixed
1:	802.11 B only
2:	802.11 A only
4:	802.11 G only
6:	802.11 N only
7:	802.11 G/N mixed
8:	802.11 A/N mixed
9:	802.11 B/G/N mixed
10:	802.11 A/G/N mixed
11:	802.11 N in 5G band only

Example:
ra0: B/G/N fixed
ra1: B only
ra2: B/G mixed
ra3: G only
Must set main BSS (ra0) first then set other MBSS WirelessMode. Can’t have A & B mode fixed in MBSS.

```
iwpriv ra0 set WirelessMode=9
iwpriv ra1 set MBSSWirelessMode=1
iwpriv ra2 set MBSSWirelessMode=0
iwpriv ra3 set MBSSWirelessMode=4
```

MEDIATEK CONFIDENTIAL
FOR wangxiang@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.47 HwAntDiv

Description: enable or disable Hardware antenna diversity
Value:

```
iwpriv ra0 set HwAntDiv=0
```

0: disable
1: enable
Note: Only support in RT5350.

3.1.48 HtBw

Description: Set HT WLAN Bandwidth
Value:

```
iwpriv ra0 set HtBw=1
```

0: 20 MHz
1: 40MHz

3.1.49 VhtBw

Description: Enable or disable 11AC 80MHz Bandwidth support
Value:

```
iwpriv ra0 set VhtBw=1
```

0: disable
1: enable

3.1.50 HtMcs

Description: Set WLAN Modulation and Coding Scheme (MCS)
Value:

```
iwpriv ra0 set  HtMcs=33
```

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

HT Mixed Mode, Refer to IEEE P802.11n Figure n67 HT Greenfield, Refer to IEEE P802.11n Figure n68	
MCS = 0 (1S)	(BW=0, SGI=0) 6.5Mbps
MCS = 1	(BW=0, SGI=0) 13Mbps
MCS = 2	(BW=0, SGI=0) 19.5Mbps
MCS = 3	(BW=0, SGI=0) 26Mbps
MCS = 4	(BW=0, SGI=0) 39Mbps
MCS = 5	(BW=0, SGI=0) 52Mbps

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

MCS = 6	(BW=0, SGI=0) 58.5Mbps
MCS = 7	(BW=0, SGI=0) 65Mbps
MCS = 8 (2S)	(BW=0, SGI=0) 13Mbps
MCS = 9	(BW=0, SGI=0) 26Mbps
MCS = 10	(BW=0, SGI=0) 39Mbps
MCS = 11	(BW=0, SGI=0) 52Mbps
MCS = 12	(BW=0, SGI=0) 78Mbps
MCS = 13	(BW=0, SGI=0) 104Mbps
MCS = 14	(BW=0, SGI=0) 117Mbps
MCS = 15	(BW=0, SGI=0) 130Mbps
MCS = 32	(BW=1, SGI=0) HT duplicate 6Mbps
Notes: When BW=1, PHY_RATE = PHY_RATE * 2 When SGI=1, PHY_RATE = PHY_RATE * 10/9 The effects of BW and SGI are accumulative. When MCS=0~7(1S, One Tx Stream), SGI option is supported. BW option is supported. When MCS=8~15(2S, Two Tx Stream), SGI option is supported. BW option is supported. When MCS=32, only SGI option is supported. BW option is not supported. (BW =1) Other MCS code in HT mode are reserved.	

3.1.51 HtGi

Description: Set WLAN Guard interval support
Value:

```
iwpriv ra0 set HtGi=1
```

0: long guard interval
1: short guard interval

3.1.52 HtOpMode

Description: HT operation Mode
Value:

```
iwpriv ra0 set HtOpMode=0
```

0: HT mixed mode
1: HT Greenfield mode

3.1.53 HtStbc

Description: Enable or disable HT STBC
Value:

```
iwpriv ra0 set HtStbc=1
```

0: disable

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

1: enable

3.1.54 HtExtcha

Description: To locate the 40MHz channel in combination with the control
Value:

```
iwpriv ra0 set HtExtcha=0
```

0: below
1: Above

3.1.55 HtMpduDensity

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

```
iwpriv ra0 set HtMpduDensity=4
```

0~7
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

3.1.56 HtBaWinSize

Description: Block Ack window size
Value:

```
iwpriv ra0 set HtBaWinSize=64
```

1~64

3.1.57 HtRdg

Description: Enable or disable HT Reverse Direction Grant
Value:

```
iwpriv ra0 set HtRdg=1
```

0: disable
1: enable

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.58 HtAmsdu

Description: Enable or disable AMSDU section
Value:

```
Iwpriv ra0 set HtAmsdu=0

0: disable
1: enable
```

3.1.59 HtAutoBa

Description: Enable or disable auto build Block Ack section with peer
Value:

```
iwpriv ra0 set HtAutoBa=1

0: disable
1: enable
```

3.1.60 HtBaDecline

Description: Enable or disable decline Block Ack to peer
Value:

```
iwpriv ra0 set HtBaDecline=0

0: disable
1: enable
```

3.1.61 HtProtect

Description: Enable or disable HT protect
Value:

```
iwpriv ra0 set HtProtect=0

0: disable
1: enable
```

3.1.62 HtMimoPs

Description: Enable or disable HT MIMO Power saving mode
Value:

```
iwpriv ra0 set HtMimoPs=0

0: disable
1: enable
```

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.63 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
```

3.1.64 AP2040Rescan

Description: Trigger HT20/40 coexistence to rescan
Value:

```
iwpriv ra0 set AP2040Rescan=1

1: trigger to rescan
```

3.1.65 HtBssCoex

Description: Enable or disable HT BSS coexistence
Value:

```
iwpriv ra0 set HtBssCoex=0

0: disable
1: enable
```

3.1.66 PktAggregate

Description: Enable or disable 11B/G packet aggregation
Value:

```
iwpriv ra0 set PktAggregate=1

0: disable
1: enable
```

3.1.67 WmmCapable

Description: Enable or disable WMM support
Value:

```
iwpriv ra0 set WmmCapable=1

0: disable
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

1: enable

3.1.68 IEEE80211H

Description: Enable or disable IEEE 802.11h function. Spectrum management.
This field can only be enabled in A band.
Value:

```
iwpriv ra0 set IEEE80211H=0
```

0: disable
1: enable

3.1.69 AuthMode

Description: WLAN security Authentication mode
Value:

```
iwpriv ra0 set AuthMode=OPEN
```

OPEN	For open system
SHARED	For shared key system
WEPAUTO	Auto switch between OPEN and SHARED
WPAPSK	For WPA pre-shared key (Infra)
WPA2PSK	For WPA2 pre-shared key (Infra)
WPANONE	For WPA pre-shared key (Adhoc)
WPA	For enterprise mode (Need wpa_supplicant)
WPA2	For enterprise mode (Need wpa_supplicant)

3.1.70 EncrypType

Description: WLAN security Encryption type
Value:

```
iwpriv ra0 set EncrypType=NONE
```

NONE	For AuthMode=OPEN
WEP	For AuthMode=OPEN or AuthMode=SHARED
TKIP	For AuthMode=WPAPSK or WPA2PSK
AES	For AuthMode=WPAPSK or WPA2PSK

3.1.71 DefaultKeyID

Description: Default key ID
Value:

```
iwpriv ra0 set DefaultKeyID=1
```

1~4

FOR wangxian@ cvt-china.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.72 Key1

Description: Key 1 string
Value:

iwpriv ra0 set Key1=aaaaa

10 or 26 characters
5 or 13 characters

3.1.73 Key2

Description: Key 2 string
Value:

iwpriv ra0 set Key2=aaaaa

10 or 26 characters
5 or 13 characters

3.1.74 Key3

Description: Key 3 string
Value:

iwpriv ra0 set Key3=aaaaa

10 or 26 characters
5 or 13 characters

3.1.75 Key4

Description: Key 4 string
Value:

iwpriv ra0 set Key4=aaaaa

10 or 26 characters
5 or 13 characters

3.1.76 WPAPSK

Description: WLAN Security string for (TKIP/AES)
Value:

iwpriv ra0 set WPAPSK=12345678

8~63 ASCII
Or
64 HEX characters

MEDIATEK CONFIDENTIAL FOR wangjian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.77 ResetCounter

Description: reset WLAN statistic counter
Value:

```
iwpriv ra0 set ResetCounter=1
```

1

3.1.78 MACRepeaterEn

Description: Enable or disable MAC Repeater function
Value:

```
iwpriv ra0 set MACRepeaterEn=1
```

0: disable
1: enable

3.1.79 PMFMFPC

Description: Enable or disable Protection Management Frame Capable
Value:

```
iwpriv ra0 set PMFMFPC=1
```

0: disable
1: enable

3.1.80 PMFMFPR

Description: Enable or disable Protection Management Frame Required
Value:

```
iwpriv ra0 set PMFMFPR=1
```

0: disable
1: enable

3.1.81 SHA256

Description: Enable or disable use SHA256 for Encryption
Value:

```
iwpriv ra0 set SHA256=1
```

0: disable
1: enable

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

3.1.82 WDSVLANID

Description: set WDS VLAN ID
Value:

```
iwpriv ra0 set WDSVLANID=1

1~16
```

Note: iNIC driver only

3.1.83 WDSVLANPriority

Description: set WDS VLAN priority
Value:

```
iwpriv ra0 set WDSVLANPriority=1

1~16
```

Note: iNIC driver only

3.1.84 ApCliVLANID

Description: set APclient VLAN ID
Value:

```
iwpriv ra0 set ApCliVLANID=1

1~16
```

Note: iNIC driver only

3.1.85 ApCliVLANPriority

Description: set APclient VLAN priority
Value:

```
iwpriv ra0 set ApCliVLANPriority=1

1~16
```

Note: iNIC driver only

3.1.86 QAEnable

Description: enable or disable QA test tool function.

```
iwpriv ra0 set QAEnable=1

0: disable
1: enable
```

MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Note: iNIC driver only.

3.1.87 Console

Description: redirect console information to host.

```
iwpriv ra0 set Console=1

0: disable
1: enable
```

Note: iNIC driver only.

3.1.88 EfuseUploadToHost

Description: This command is specific to iNIC solution.
The content of efuse will be uploaded to the iNIC host in iNIC_e2p.bin or iNIC_e2p1.bin .

```
iwpriv ra0 set EfuseUploadToHost=1

0: disable
1: enable
```

Note: iNIC driver only

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

4 iwpriv ra0 usage

This section describes parameters set using iwpriv. Please refer to the Readme section for more general data.
A detailed explanation of each parameter for iwpriv is shown subsequently. Refer to the Readme before using this section.

iwpriv ra0 [parameters]

4.1 get_site_survey

Description: Show site survey result
Value:

```
iwpriv ra0 get_site_survey
```

Note: Works only after iwpriv ra0 set SiteSurvey=1

4.2 get_mac_table

Description: Show STA's MAC address which associated with AP
Value:

```
iwpriv ra0 get_mac_table
```

4.3 get_wsc_profile

Description: Display WPS profile information in detailed
Value:

```
iwpriv ra0 get_wsc_profile
```

4.4 get_ba_table

Description: Show Block ACK Table raw data information
Value:

```
iwpriv ra0 get_ba_table
```

4.5 stat

Description: Display WLAN static counter
Value:

```
iwpriv ra0 stat
```

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxian@ cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

4.6 bbp (Debug only)

Description: Display/Write bbp content
Value:

```
//Display
iwpriv ra0 bbp offset

//Write bbp
iwpriv ra0 bbp offset=value

offset = hex address
value= hex value
```

4.7 mac (Debug only)

Description: Display/Write mac content
Value:

```
//Display
iwpriv ra0 mac offset

//Write mac
iwpriv ra0 mac offset=value

offset = hex address
value= hex value
```

4.8 rf (Debug only)

Description: Display/Write rf content
Value:

```
//Display
iwpriv ra0 rf offset

//Write
iwpriv ra0 rf offset=value

offset = hex address
value= hex value
```

4.9 e2p (Debug only)

Description: Read/Write EEPROM content
Value:

```
//Read
iwpriv ra0 e2p offset
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangxian@ cvnchina.com USE ONLY

```
//Write EEPROM
iwpriv ra0 e2p offset=value

offset = hex address
value= hex value
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

5 iwpriv ra0 show command

This section describes parameters set using iwpriv. Please refer to the Readme section for more general data.

Display parameter which has been currently configured in the WLAN driver.

iwpriv ra0 show [parameters]

[Parameters list]

1. stainfo - Show associated STA's MAC address
2. descinfo - Show Descriptor information.
3. driverinfo - Show driver version.
4. wdsinfo - Show WDS list information.
5. bainfo - Show Block ACK Table. (String message)
6. stat - Show statistics counter.
7. stat_reset - Show, then reset statistics counter.
8. igmpinfo - Show all entrys in IGMP table.
9. mcastrate - Show multicast phy mode and MCS rate.
10. stacountinfo – show associated STA’s Tx, Rx byte counts.
11. stasecinfo – show associated STA’s BSS and security information.
12. mbss – show MBSS phy mode information.

Example: show stainfo

```
iwpriv ra0 show stainfo
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

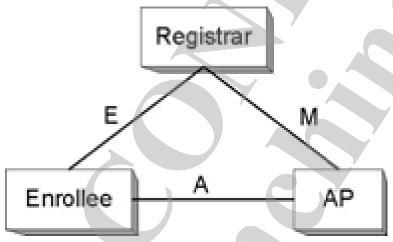
6 WPS Wi-Fi PROTECTED SETUP

Simple Config Architectural Overview
This section presents a high-level description of the Simple Config architecture. Much of the material is taken directly from the Simple Config specification.
Figure 1 depicts the major components and their interfaces as defined by Wi-Fi Simple Config Spec. There are three logical components involved: the Registrar, the access point (AP), and the Enrollee.

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

A **Registrar** is an entity with the authority to issue and revoke domain credentials. A registrar can be integrated into an AP.

The **AP** can be either a WLAN AP or a wireless router.



Registration initiation is ordinarily accomplished by a user action such as powering up the Enrollee and, optionally, running a setup wizard on the Registrar (PC).

Note: The WLAN driver needs to set HAS_WSC=y in order to enable WPS functions.

6.1 WPS Profile settings

Configure WPS setting in RT2860AP.dat or RT2860AP.dat.

Syntax:
[Parameter]=[Value]

6.1.1 WscConfMode

Description: Set WPS function, bitwise.
Value:

WscConfMode=0x2

0x0: Disable
0x1: Enrollee
0x2: Proxy
0x4: Registrar

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

6.1.2 WscConfStatus

Description: Set WPS AP SC (Simple Config) State
Value:

WscConfStatus=1

1: AP is un-configured
2: AP is configured

6.1.3 WscConfMethods

Description: The Config Methods Data component lists the configuration methods the Enrollee or Registrar supports. The list is a bitwise OR of values from the table below. If you don't know what this is, please don't set this field.

Value:

WscConfMethods=16

1	- USBA (Flash Drive)
2	- Ethernet
4	- Label
8	- Display
16	- External NFC Token
32	- Integrated NFC Token
64	- NFC Interface
128	- PushButton
256	- Keypad

6.1.4 WscKeyASCII

Description: Define WPS WPAPSK format and key length for un-configured internal WPS Registrar AP.
Value:

WscKeyASCII=0

0: Hex (64-bytes). Default is 0.
1: ASCII(random length)
8 ~ 63: ASCII length

6.1.5 WscSecurityMode

Description: Define WPS regitrar's unconfiguraed -> configuraed security mode.
Value:

WscSecurityMode=0

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

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

6.1.6 WscDefaultSSID0

Description: Default WPS SSID for AP. After WPS process completes with Enrollee when AP acts as un-configured Registrar, AP will use this SSID as new SSID.

Value:

WscDefaultSSID0=SSID

1~32 characters

6.1.7 WscV2Support

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

WscV2Support=1

0: disable
1: enable

6.2 WPS iwpriv command

This section describes parameters set using iwpriv. Please refer to the Readme section for more general data.

iwpriv ra0 set [parameter]=[Value]

Note: Wireless extension private handlers.

6.2.1 WscConfMode

Description: set WPS conf mode
Value:

iwpriv ra0 set WscConfMode=1

0x0: Disable
0x1: Enrollee
0x2: Proxy
0x4: Registrar

6.2.2 WscConfStatus

Description: Set WPS SC (simple config) state
Value:

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

iwpriv ra0 set WscConfStatus=1

1: AP is un-configured
2: AP is configured

6.2.3 WscMode

Description: WPS mode, PBC or PIN
Value:

iwpriv ra0 set WscMode=1

1: PIN (Personal Identification Number) Mode
2: PBC (Push Button Communication) Mode

6.2.4 WscStatus

Description: Get WPS Configured Methods.
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:	Receive EAP-Rsp(ID)
7:	Receive EAP-Req with wrong WSC SMI Vendor Id
8:	Receive EAPReq with wrong WSC Vendor Type
9:	Sending EAP-Req(WSC_START)
10:	Send M1
11:	Received M1
12:	Send M2
13:	Received M2
14:	Received M2D
15:	Send M3
16:	Received M3
17:	Send M4
18:	Received M4
19:	Send M5
20:	Received M5
21:	Send M6
22:	Received M6
23:	Send M7
24:	Received M7

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

25: Send 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: Configured

6.2.5 WscPinCode

Description: Input Enrollee's Pin Code to AP-Registrar.
Value:

```
iwpriv ra0 WscPinCode xxxxxxxx

xxxxxxx = {00000000 ~ 99999999}
```

6.2.6 WscOOB

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

```
iwpriv ra0 set WscOOB=1

0: disable
1:  enable
```

6.2.7 WscGetConf

Description: Trigger WPS AP to do simple config with WPS Client.
Value:

```
iwpriv ra0 set WscGetConf=1

0: disable
1: enable
```

6.2.8 WscGenPinCode

Description: Randomly generate enrollee PIN code
Value:

```
iwpriv ra0 set WscGenPinCode=1

1
```

FOR wangxian@cvnchina.com USE ONLY MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

6.2.9 WscVendorPinCode

Description: Input vendor's Pin Code to AP-Registrar.
Value:

```
iwpriv ra0 set WscVendorPinCode=xxxxxxxx

xxxxxxxx: 8 digit pin code
```

6.2.10 WscSecurityMode

Description: Set WPS regitrar's unconfiguraed -> configuraed security mode.
Value:

```
iwpriv ra0 set WscSecurityMode=0

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

6.2.11 WscMultiByteCheck

Description: Set multi byte check is enabled or disabled.
Value:

```
iwpriv ra0 set WscMultiByteCheck=1

0: disable
1: enable
```

6.2.12 WscVersion

Description: Set WPS support version
Value:

```
iwpriv ra0 set WscVersion=10

xx: Hex value
```

6.2.13 WscVersion2

Description: Set WPS version of V2 support
Value:

```
iwpriv ra0 set WscVersion2=10

xx: Hex Value
```

MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

6.2.14 WscV2Support

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

```
iwpriv ra0 WscV2Support=1
```

0: disable
1: enable

6.2.15 WscFragment

Description: enable or disable WPS fragment
Value:

```
iwpriv ra0 WscFragment=0
```

0: disable
1: enable

6.2.16 WscFragmentSize

Description: Set the size of WPS fragmentation.
Value:

```
iwpriv ra0 set WscFragmentSize=128
```

128~300

6.2.17 WscSetupLock

Description: enable or disable WPS setup lock
Value:

```
iwpriv ra0 set WscSetupLock=1
```

0: disable
1: enable

6.2.18 WscSetupLockTime

Description: Configure WPS setup lock time
Value:

```
iwpriv ra0 set WscSetupLockTime=0
```

0: lock forever
Unit: minute

MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

6.2.19 WscMaxPinAttack

Description: Configure WPS pin attack Max time.
Value:

```
iwpirv ra0 set WscMaxPinAttack

0:Disable
1-10
```

6.2.20 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
```

6.2.21 WscExtraTlvType

Description: Define data format of extra TLV value
Value:

```
iwpriv ra0 set WscExtraTlvType=1

0: ASCII string
1: Hex string
```

6.2.22 WscExtraTlvData

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

```
iwpriv ra0 set WscExtraTlvData=

ASCII string or Hex string
```

6.2.23 WPS iwpriv command example

6.2.23.1 Disable WPS support

```
iwpriv ra0 set WscConfMode=0
```

6.2.23.2 Enable WPS Function

```
iwpriv ra0 set WscConfMode =7 (Binary: 111)
(AP could be Registrar(0x4), Proxy(0x2) or Enrollee(0x1))
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wangxian@ cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

6.2.23.3 WPS AP SC (Simple Config) State

iwpriv ra0 set WscConfStatus=1 (AP is un-configured)
iwpriv ra0 set WscConfStatus=2 (AP is configured)

6.2.23.4 WPS Configured Methods

iwpriv ra0 set WscMode =1 (use PIN code)
iwpriv ra0 set WscMode =2 (use PBC)

6.2.23.5 Input Enrollee's Pin Code to AP-Registrar

iwpriv ra0 set WscPinCode=xxxxxxxx

6.2.23.6 Reset WPS AP to the OOB configuration

iwpriv ra0 set WscOOB=1
(Security: WPAPSK/TKIP, psk: "RalinkInitialAPxx1234" ; SC state: 0x1)
(SSID: RalinkInitialAPxxxxxx, last three characters of AP MAC address)

6.2.23.7 Trigger WPS AP to do simple config with WPS Client

iwpriv ra0 set WscGetConf=1

6.2.23.8 AP services as Enrollee by using PIN code

iwpriv ra0 set WscMode=1
iwpriv ra0 set WscGetConf=1

6.2.23.9 AP services as Enrollee by using PBC

iwpriv ra0 set WscMode=2
iwpriv ra0 set WscGetConf=1

6.2.23.10 AP services as Internal Registrar using PIN code

iwpriv ra0 set WscMode=1
iwpriv ra0 set WscPinCode=xxxxxxxx (PIN code from Enrollee, len=8)
iwpriv ra0 set WscGetConf=1

6.2.23.11 AP services as Internal Registrar using PBC

iwpriv ra0 set WscMode=2
iwpriv ra0 set WscGetConf=1

6.2.23.12 Get WPS Profile from external registrar

iwpriv ra0 get_wsc_profile

6.3 WPS AP Setup Procedure

To run the Access Point (as Enrollee or with Registrar capabilities).
The following scenarios are currently supported:

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

1. Initial Access Point (AP) setup, with the Registrar configuring the Access Point
   1.1. One WiFi-enabled laptop is setup as the AP acting as an Enrollee
   1.2. Another WiFi-enabled laptop is setup as a station acting as the Registrar
   1.3. Two sub cases are 1a) using EAP transport and 1b) using UPnP transport

2. Configuration of a WiFi client, using an AP with a built-in registrar
   2.1. One WiFi-enabled laptop is setup as the AP with registrar functionality Another WiFi-enabled laptop is setup as a station acting as an Enrollee

3. Configuration of a WiFi client using an external registrar. AP acts as a proxy and communicates with the client over EAP and with the Registrar over UPnP.
   3.1. One WiFi-enabled laptop is setup as a station acting as an Enrollee
   3.2. Second WiFi-enabled laptop is setup as the AP with proxy functionality
   3.3. Third laptop is setup as the registrar. The registrar and the AP are connected over Ethernet.

6.3.1 Running the WPS command-line application

Run the protocol from the console.
First, run UPNP deamon like below:

```
wscd -w /etc/xml -m 1 -d 3 & (if your xml file in /etc/xml)
```

use iwpriv command trigger wps, like below:

```
iwpriv ra0 set WscConfMode=7
iwpriv ra0 set WscConfStatus=1
iwpriv ra0 set WscMode=1
iwpriv ra0 set WscPinCode=31668576
iwpriv ra0 set WscGetConf=1
iwpriv ra0 set WscStatus=0
```

1. AP services as Enrollee:
   1.1. If AP-Enrollee SC state is 0x1, AP will restart with new configurations.
   1.2. If AP-Enrollee SC state is 0x2, AP sends own configurations to external-registrar and ignores configurations from external-registrar.

2. AP services as Registrar:
   2.1. If AP-Registrar SC state is 0x1, the security mode will be WPAPSK/TKIP and generate random 64bytes psk; after process, AP will restart with new security.

3. WPS AP only services one WPS client at a time.
   3.1. WPS AP only can work in ra0.
   3.2. After WPS configuration finishes, Ralink AP driver writes new configuration to Cfg structure and DAT file.

4. Write items to MBSSID Cfg structure are as below:
   4.1. Ssid
   4.2. AuthMode
   4.3. WepStatus
   4.4. PMK
   4.5. DefaultKeyId.

FOR wangxian@cvnchina.com USE ONLY MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

5. Write items to SharedKey table are as below:
   5.1. Key
   5.2. CipherAlg

6. Write items to DAT file are as belw:
   6.1. SSID
   6.2. AuthMode
   6.3. EncrypType
   6.4. WPAPSK
   6.5. WscConfStatus
   6.6. DefaultKeyID

Note: wscd daemon must be ported to the target platform first.

6.3.2 Initial AP setup with Registrar Configuring AP (EAP/UPnP)

To run command-line console in this mode do:

[Unconfigured AP] ← EAP/UPnP → [Registrar]

Note:

Please make sure upnp deamon is running. After the success of WPS registration, Configured AP will act as a proxy forward EAP and Upnp.)

1. **PIN**
   (1) on AP side
   - iwpriv ra0 set WscConfMode=7
   - iwpriv ra0 set WscConfStatus=1
   - iwpriv ra0 set WscMode=1
   - iwpriv ra0 set WscGetConf=1

   (2) on Registrar side
   - When prompted for the enrollee's PIN, Enter the AP's PIN. Enter the new SSID and new Security for the AP when prompted.
   - The registration process will start, and the application will display the result of the process on completion.

2. **PBC**
   (1) on AP side
   - iwpriv ra0 set WscConfMode=7
   - iwpriv ra0 set WscConfStatus=1
   - iwpriv ra0 set WscMode=2
   - iwpriv ra0 set WscGetConf=1

   (2) on Registrar side
   - Select push-button".
   - The registration process will start, and the application will display the result of the process on completion.

The security config will be written out to the AP and registrar config files.

6.3.3 Adding an Enrollee to AP+Registrar (EAP)

To run command-line console in this mode do:

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL FOR wangxiang@cwchina.com USE ONLY

[AP+Registrar] 🡐 EAP 🡒 [Client]

Note:

Please make sure WPS AP configure status is configured, if AP is un-configure, when WPS AP configure client, it will change configure status to configured and auth mode are WPA-PSK)

1. **PIN**
   (1) **on AP side**
   - iwpriv ra0 set WscConfMode=7
   - iwpriv ra0 set PinCode=31668576 (enter the enrollee's PIN, the PIN from WPS client)
   - iwpriv ra0 set WscMode=1
   - iwpriv ra0 set WscGetConf=1.
   - The registration process will begin, and the console will display the result of the process on completion.

   (2) **on Client (Enrollee) side**
   - Select PIN process.
   - The process will start, and the application will display the result of the process on completion
2. **PBC**
   (1) **on AP side**
   - iwpriv ra0 set WscConfMode=7
   - iwpriv ra0 set WscMode=2
   - iwpriv ra0 set WscGetConf=1.
   - The registration process will start, and the application will display the result of the process on completion.

   (2) **on Client (Enrollee) side**
   - Select PBC process.
   - The process will start, and the application will display the result of the process on completion

If the registration is successful, on the client will be re-configured with the new parameters, and will connect to the AP with these new parameters.

6.3.4 Adding an Enrollee with Eternal Registrar (UPnP/EAP)

To run command-line console in this mode do:

[Registrar] 🡐 PnP 🡒 [AP] 🡐 EAP 🡒 [Client]

1. **PIN**
   (1) **on Registrar side**
   - When prompted for the enrollee's PIN, Enter the enrollee's PIN.
   - AP Nothing to be selected..
   - The registration process will begin, and the application will display the result of the process on completion.

   (2) **on Client (Enrollee) side**
   - Select PIN process
   - The process will start, and the application will display the result of the process on completion
2. **PBC**
   (1) **on Registrar side**
   - Select "push-button".
   - AP Nothing to be selected.
   - The registration process will begin, and the application will display the result of the process on completion.

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL FOR wangyian@cvte.com USE ONLY

(2) on Client (Enrollee) side

- Select PBC process
- The registration process will start, and the application will display the result of the process on completion.

6.3.5 WPS Config status

6.3.5.1 Over View

The 'Simple Config State' of WPS attribute in WPS IEs contained in beacon and probe response indicates if a device is configured.If an AP is shipped from the factory in the Not-Configured state (Simple Config State set to 0x01), then the AP must transition to the Configured state (Simple Config State set to 0x02) if any of the following occur:

1. Configuration by an external registrar.

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

2. Automatic configuration by internal registrar.

The AP receives the WSC_Done response in the Enrollee Registration Process from the first Enrollee.
Note:
The internal registrar waits until successful completion of the protocol before applying the automatically generated credentials to avoid an accidental transition from unconfigured to configured 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 user.

A user manually configures the AP using whatever interface(s) it provides to modify any one of the following:

- the SSID
- the encryption algorithm
- the authentication algorithm
- any key or pass phrase

If the AP is shipped from the factory in the Not Configured state (Simple Config State set to 0x01), then a factory reset must revert the Simple Config State to Not Configured.
If the AP is shipped from the factory pre-configured with WPA2-Personal mixed mode and a randomly generated key, the Simple Config State may be set to 'Configured' (0x2) to prevent an external registrar from overwriting the factory settings. A factory reset must restore the unit to the same configuration as when it was shipped.

6.4 Basic operation of Ralink WPS AP

6.4.1 Configure APUT using PIN method through a WLAN external Registrar

1. [Ralink AP] - Turn on the Ralink AP
2. [Ralink AP] - To change AP ability “iwpriv ra0 set WscConfMode=7”

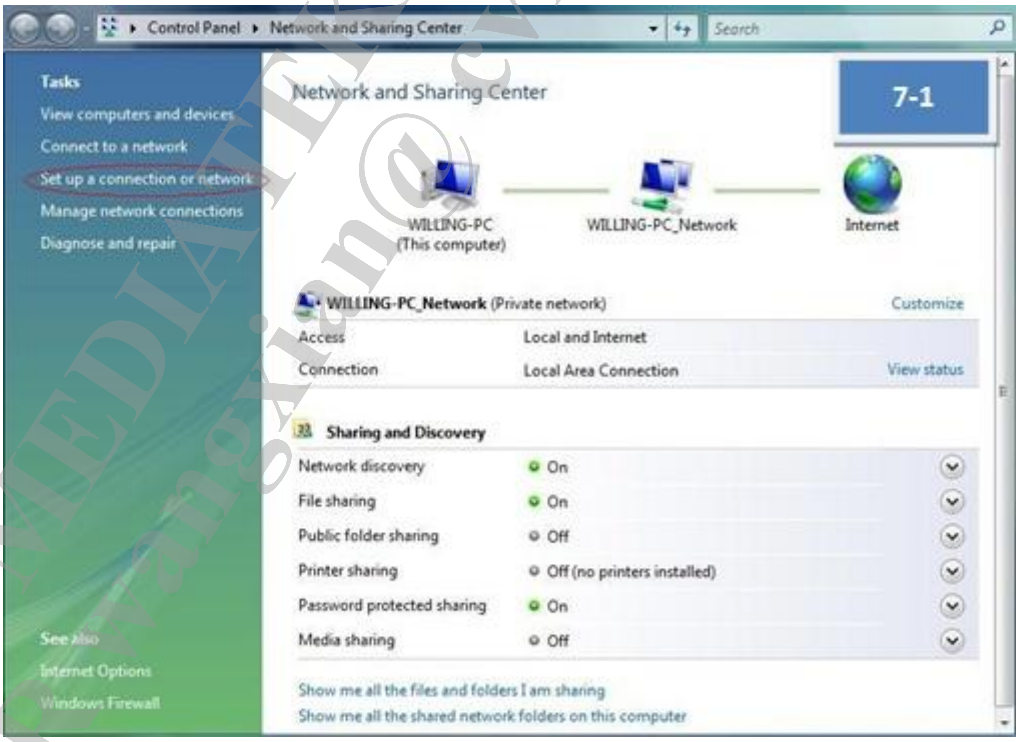
This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wangjian@cvtechina.com USE ONLY
MEDIATEK CONFIDENTIAL

3. [Ralink AP] - To change from configured to un-configured state: “iwpriv ra0 set WscConfStatus=1 “
4. [Ralink AP] - To change config method to PIN “iwpriv ra0 set WscMode=1”
5. [Ralink AP] - Trigger Ralink AP start process WPS protocol “iwpriv ra0 set WscGetConf=1”
6. [Intel WPS STA] - The Registrar on Intel STA will be configured with the new parameters (SSID = “scaptest4.1.2ssid” and WPA(2)-PSK=”scaptest4.1.2psk”) which should be entered when prompted
7. [Intel WPS STA] - Read AP's PIN from console and enter the PIN at Intel STA.
8. [Intel WPS STA] - Verify that Intel STA successes to ping to Ralink AP
9. [Ralink STA] - Manually configure Ralink STA with the new parameters (SSID = “scaptest4.1.2ssid” and WPA (2)-PSK = “scaptest4.1.2psk”).
10. [Intel WPS STA] - Verify that Intel STA successes to ping to Ralink STA

6.4.2 Configure APUT using PIN method through a wired external registrar

1. [Ralink AP] - Turn on the Ralink AP
2. [Ralink AP] - Connect the Ethernet cable between AP and extern registrar(Windows Vista) and make sure you can pin our device from extern registrar first!
3. [Ralink AP] - To change AP ability “iwpriv ra0 set WscConfMode=7”
4. [Ralink AP] - To change from configured to un-configured state: “iwpriv ra0 set WscConfStatus=1 “
5. [Ralink AP] - To change config method to PIN “iwpriv ra0 set WscMode=1”
6. [Ralink AP] - Trigger Ralink AP start process WPS protocol “iwpriv ra0 set WscGetConf=1”
7. [Microsoft STA] - The Registrar on Microsoft STA will be configured with the new wireless configuration settings (SSID = “scaptest4.1.3ssid” and WPA (2)-PSK=”scaptest4.1.3psk”), which should be entered when prompted.

Please refer to below figures [7-1] to [7-6].



WILLING-PC_Network (Private network)

Access	Local and Internet
Connection	Local Area Connection

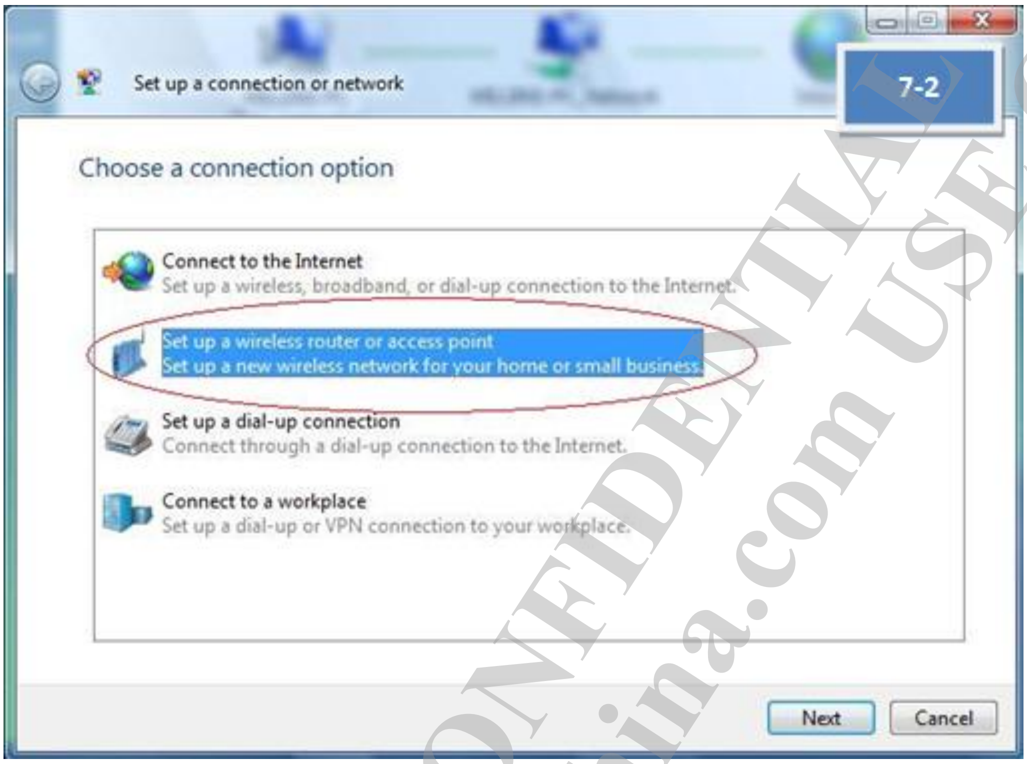
Sharing and Discovery

Network discovery	On
File sharing	On
Public folder sharing	Off
Printer sharing	Off (no printers installed)
Password protected sharing	On
Media sharing	Off

Show me all the files and folders I am sharing
Show me all the shared network folders on this computer

FOR MEDIATEK CONFIDENTIAL USE ONLY
vangxian@cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.



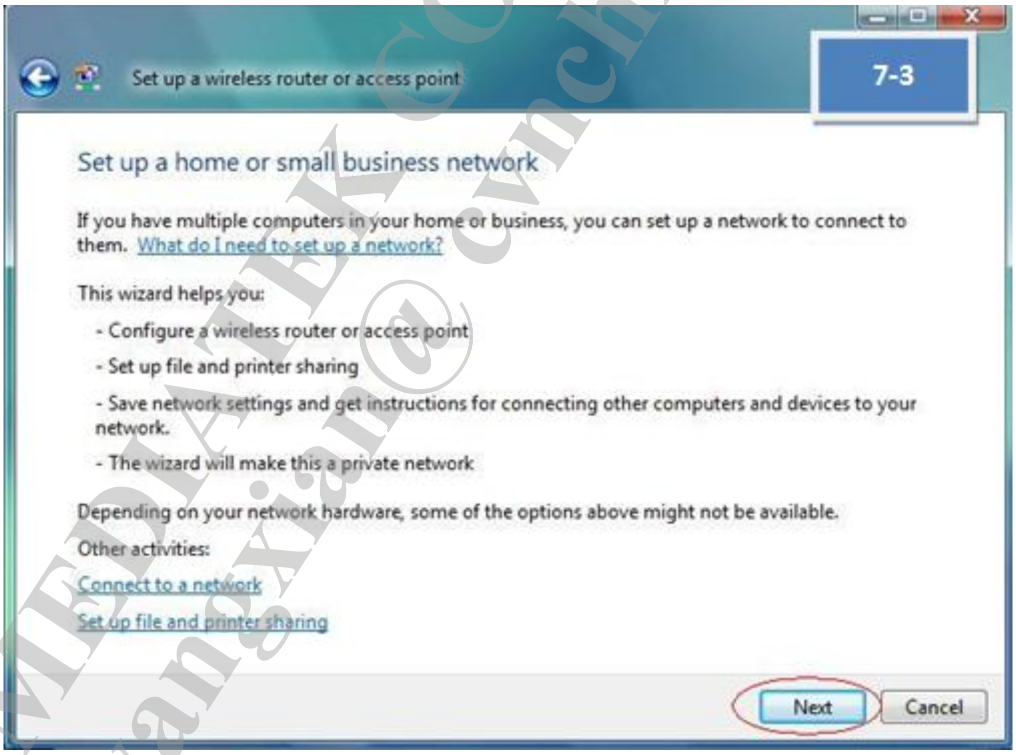
Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a wireless router or access point
Set up a new wireless network for your home or small business.

Set up a dial-up connection
Connect through a dial-up connection to the Internet.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.



Set up a home or small business network

If you have multiple computers in your home or business, you can set up a network to connect to them. What do I need to set up a network?

This wizard helps you:

- Configure a wireless router or access point
- Set up file and printer sharing
- Save network settings and get instructions for connecting other computers and devices to your network.
- The wizard will make this a private network

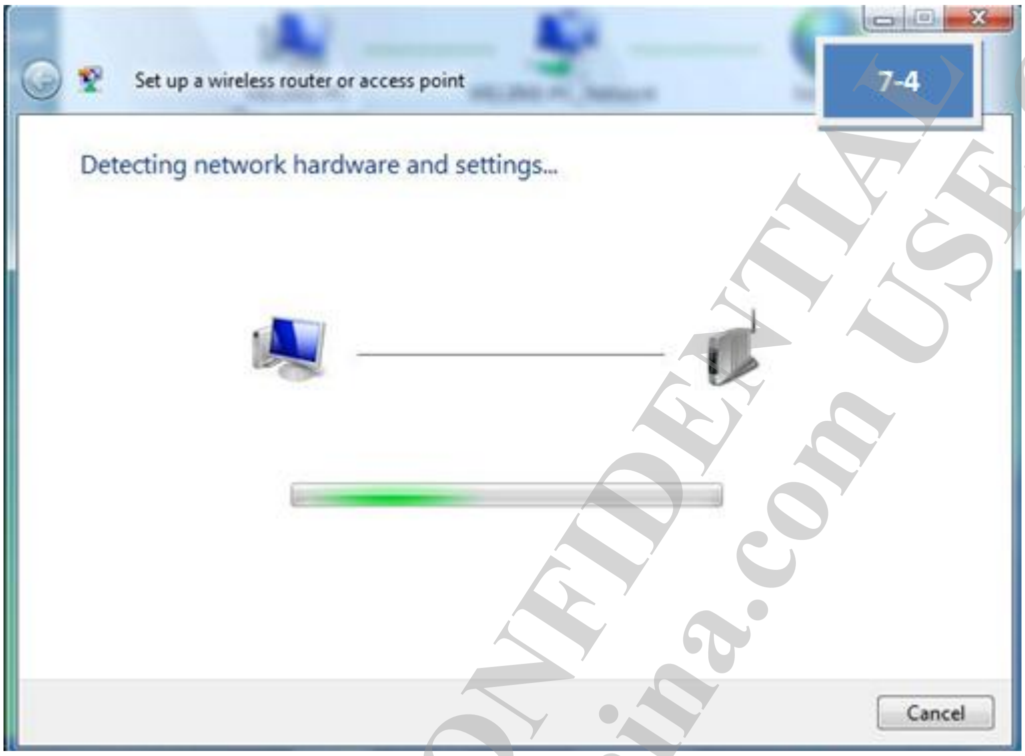
Depending on your network hardware, some of the options above might not be available.

Other activities:

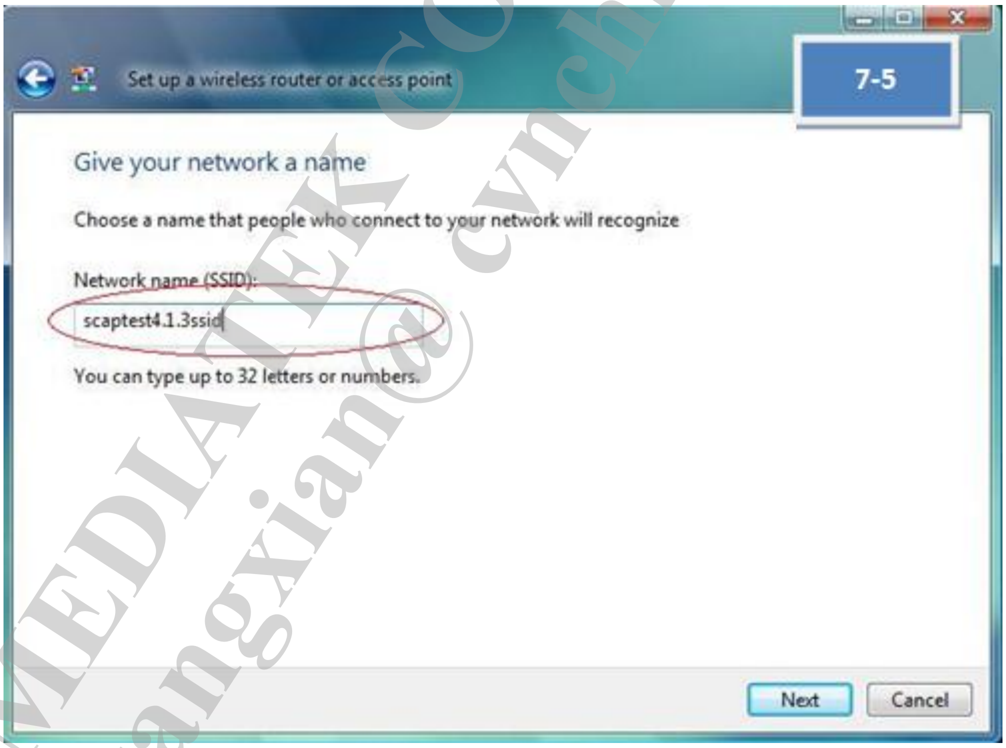
Connect to a network
Set up file and printer sharing

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.



Detecting network hardware and settings...



Give your network a name

Choose a name that people who connect to your network will recognize

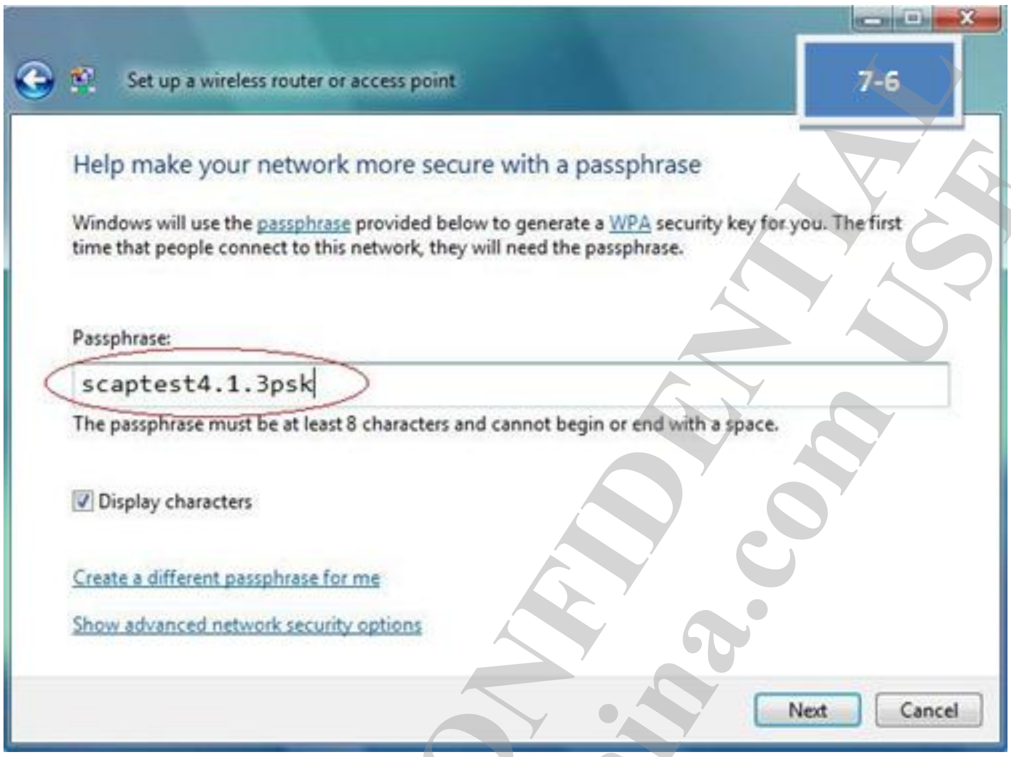
Network name (SSID):

scaptest4.1.3ssid

You can type up to 32 letters or numbers.

FOR wangxian@ cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.



Help make your network more secure with a passphrase

Windows will use the passphrase provided below to generate a WPA security key for you. The first time that people connect to this network, they will need the passphrase.

Passphrase:

scaptest4.1.3psk

The passphrase must be at least 8 characters and cannot begin or end with a space.

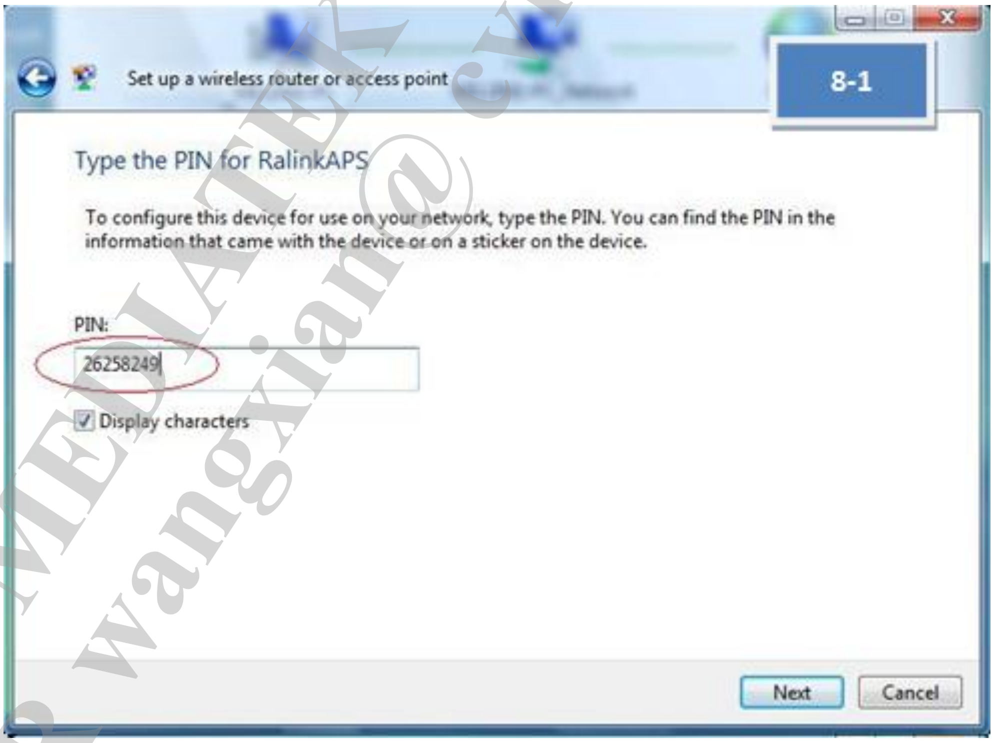
☑ Display characters

Create a different passphrase for me

Show advanced network security options

1. [Microsoft STA] - Read AP's PIN from console and enter the PIN at Microsoft STA.

Please refer to below figures [8-1] to [8-2].



Type the PIN for RalinkAPS

To configure this device for use on your network, type the PIN. You can find the PIN in the information that came with the device or on a sticker on the device.

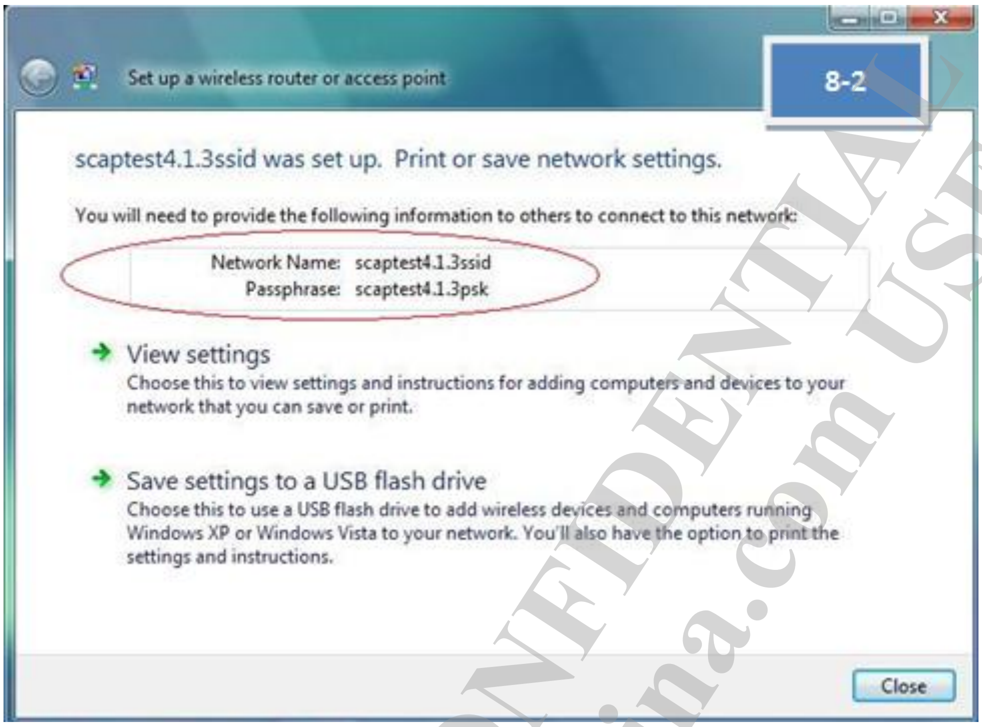
PIN:

26258249

☑ Display characters

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.


Set up a wireless router or access point

scaptest4.1.3ssid was set up. Print or save network settings.

You will need to provide the following information to others to connect to this network:

Network Name: scaptest4.1.3ssid
Passphrase: scaptest4.1.3psk

View settings
Choose this to view settings and instructions for adding computers and devices to your network that you can save or print.

Save settings to a USB flash drive
Choose this to use a USB flash drive to add wireless devices and computers running Windows XP or Windows Vista to your network. You'll also have the option to print the settings and instructions.

1. [Ralink STA] - Manually configure Ralink STA with the new parameters (SSID = “scaptest4.1.3ssid” and WPA (2)-PSK passphrase= “scaptest4.1.3psk”).
2. [Ralink STA] - Verify that Ralink STA successes to ping to Microsoft STA.

6.4.3 Add devices using external Registrars

1. [Ralink AP] - Turn on the APUT.
2. [Ralink STA] - Turn on the Ralink STA.
3. [Ralink STA] - Push PIN button.
4. [Microsoft STA] - Search will be configure enrollee (you can in control->network and internet->network and sharing center->add a device to the network). Enter the enrollee’s PIN(Ralink STA) at Microsoft STA when prompted.
5. [Ralink AP] - Do not thing.
6. [Ralink STA] - Verify that Ralink STA successes to ping Ralink A.

6.4.4 How to know WPS AP services as Internal Registrar, Enrollee or Proxy

It depends on the content of EAP-Response/Identity from WPS Client.

⇨ When identity is “WFA-SimpleConfig-Registrar-1-0”:
WPS AP would service as Enrollee. (After set trigger command)

⇨ When identity is “WFA-SimpleConfig-Enrollee-1-0”:
WPS AP would service as Internal Registrar and Proxy.
Without trigger command, WPS AP services as proxy only.

MEDIATEK CONFIDENTIAL
FOR wangxiang@evinchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

6.4.5 How to know WPS AP PinCode

Use ioctl query **RT_OID_WSC_PIN_CODE** OID to get AP PinCode.

6.4.6 Notes for WPS

1. AP services as Enrollee:
   1.1. If AP-Enrollee SC state is 0x1, AP's configuration is changeable and will restart with new configurations.
   1.2. If AP-Enrollee SC state is 0x2, AP's configuration is un-changeable. AP sends own configurations to external-registrar and ignores configurations from external-registrar.
2. AP services as Registrar:
   2.1. If AP-Registrar SC state is 0x1, the security mode will be WPAPSK/TKIP and generate random 64bytes psk; after process, AP will restart with new security.
3. AP services as Proxy:
   3.1. The value of SC state has no effect in proxy mode.
   3.2. WPS AP only services one WPS client at a time.
   3.3. WPS AP only can work in ra0.

6.4.7 Compile flag for WPS AP

```
WFLAGS += -DWSC_SUPPORT
```

6.4.8 WPS related Document

1. Wi-Fi Protected Setup Specification v1.0 (member only)
2. Wi-Fi Protected Setup White Paper
3. Introducing Wi-Fi Protected Setup
4. WSC Linux* Reference Implementation
5. How to Use Windows Connect Now Configuration to Enable Simple Setup for Consumer Wi-Fi Networks [WinHEC 2006; 5.83 MB]
6. Network Infrastructure Device Implementer's Guide

6.5 UPNP Daemon HOWTO

6.5.1 Build WPS UPnP Daemon

Requirements:

1. Linux platform
2. Ralink wireless driver version which support WPS
3. Libupnp
   ⇨ You can download the libupnp source code from the following URL: http://upnp.sourceforge.net/
   ⇨ libupnp-1.3.1 is preferred version. For other versions, you may need to patch our modification to the library yourself.
4. POSIX thread library
   ⇨ Both libupnp and our WPS UPnP daemon need the POSIX thread library, following are recommended pthread library version.
      ■ For uCLibc, need the version >= 0.9.27

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

- For GLIBC, need the version >= 2.3.2

⇨ If your pthread library is older than upper list, you may need to upgrade it.

Build and Run:

1. Modify the “$(work_directory)/wsc_upnp/Makefile” and change the compile flags depends on your target platform.
   ⇨ Ex. For arm-Linux target platform, you may need to set the following fags:
   - CROSS_COMPILE = arm-Linux-
   - TARGET_HOST = arm-Linux
   - **WIRELESS_H_INCLUDE_PATH = /usr/src/kernels/2.6.11-1.1369_FC4-smp-i686/include/**
2. Modify the “$(work_directory)/wsc_upnp/libupnp-1.3.1/Makefile.src” and change the configure parameters.
   ⇨ Ex. For big-endian system, you may need to add CFAGS as following:
   - ./configure --host=$(TARGET_HOST) CFLAGS="-mbig-endian"
3. Compile it
   ⇨ Run “make” in “$(work_directory)/wsc_upnp”, after successful compilation, you will get an execution file named “wscd”.
4. Install
   ⇨ Create a sub-directory named “xml” in the “/etc” of your target platform
   ⇨ Copy all files inside in “$(work_directory)/wsc_upnp/xml” to “/etc/xml”
   - Copy the “wscd” to the target platform.
5. Run it
   ⇨ Before run it, be sure the target platform already **has set the default route or has a route entry for subnet 239.0.0.0 (For UuPnP Multicast)**. Or the WPS daemon will failed when do initialization.
   ⇨ Now you can run it by following command:
   - /bin/wscd –m 1 –d 3

Related Document:

1. WPS Specification (Simple_Config_v1.0g.pdf)
2. UPnP Device Architecture 1.0
3. Windows Connect Now-NET Version 1.0
4. WFAWLANConfig:1 Service Template Version 1.01
5. WFA Device:1 Device Template Version 1.01

6.6 WPS Command & OID Example

6.6.1 Iwpriv command without argument

iwpriv command:

```
iwpriv ra0 wsc_start
iwpriv ra0 wsc_stop
iwpriv ra0 wsc_gen_pincode
```

OID:

Example:
memset(&lwreq, 0, sizeof(lwreq));

FOR wangxian@cvhina.com USE ONLY MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
sprintf(lwreq.ifr_name, "ra0", 3);
iwreq.u.mode = WSC_STOP;
/* Perform the private ioctl */
if(ioctl(skfd, RTPRIV_IOCTL_SET_WSC_PROFILE_U32_ITEM, &lwreq) < 0)
{
fprintf(stderr, "Interface doesn't accept private ioctl...\n");
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

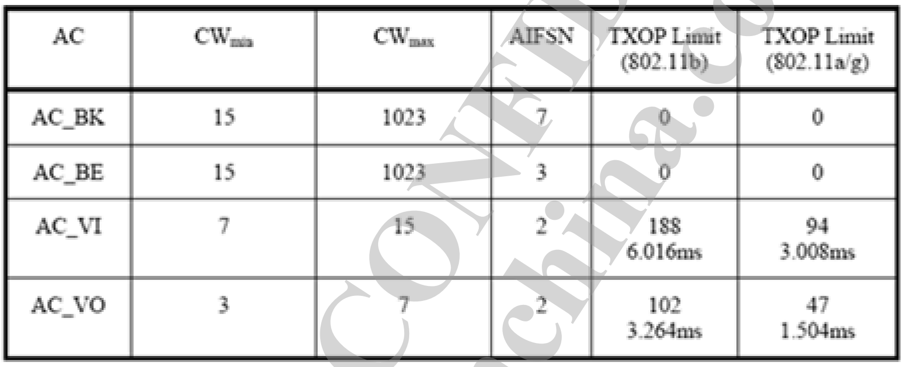
This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

7 WMM PARAMETERS

7.1 Setting Parameters

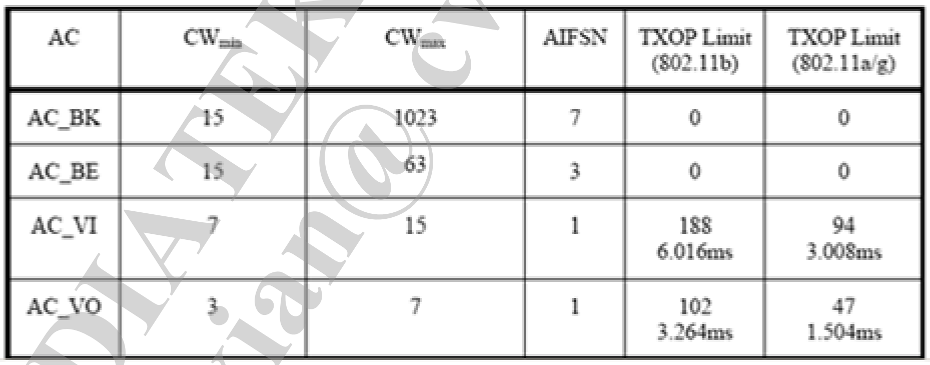
1. Set ‘WmmCapable’ as 1 to turn on WMM QoS support
2. Parameters of ‘APAifsn’, ‘APCwmin’, ‘APCwmax’, ‘APTxop’, ‘APACM’ are WMM parameter for AP
3. Parameters of ‘BSSAifsn’, ‘BSSCwmin’, ‘BSSCwmax’, ‘BSSTxop’, ‘BSSACM’ are WMM parameter for station
4. Parameter of AckPolicy is for Ack policy which support normal Ack or no Ack
5. Default WMM parameters for STA and AP

Table 4 Default WMM Parameters for the STA



AC	CW_{min}	CW_{max}	AIFSN	TXOP Limit (802.11b)	TXOP Limit (802.11a/g)
AC_BK	15	1023	7	0	0
AC_BE	15	1023	3	0	0
AC_VI	7	15	2	188 6.016ms	94 3.008ms
AC_VO	3	7	2	102 3.264ms	47 1.504ms

Table 5 Default WMM Parameters for the AP



AC	CW_{min}	CW_{max}	AIFSN	TXOP Limit (802.11b)	TXOP Limit (802.11a/g)
AC_BK	15	1023	7	0	0
AC_BE	15	63	3	0	0
AC_VI	7	15	1	188 6.016ms	94 3.008ms
AC_VO	3	7	1	102 3.264ms	47 1.504ms

1. All WMM parameters do not support iwpriv command but ‘WmmCapable’’, please store all parameter to RT2800AP.dat, and restart driver.
2. The format for WMM parameter is as followed,
   APAifsn=3;7;1;1 //AC_BE, AC_BK, AC_VI, AC_VO

7.2 How to Run WMM test

1. **WmmCapable=1**
   For each BSSID:
      0: Disable WMM,
      1: Enable WMM

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

(If the parameter sets to 1, the relative BSSID will turn on WMM)

2. **TxBurst=0**
3. **Parameters for AP (for each AC (access category))**

```
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
```

4. **Parameters for all STAs (for each AC (access category))**

```
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
```

5. **Ack policy**

```
AckPolicy=0;0;0;0                  // AC_BE;AC_BK;AC_VI;AC_VO;
                                   // 0: Normal ACK, 1: No ACK
```

All default values comply with Wi-Fi spec.

7.3 WMM "The Ack"

1. **Current driver of RT2800AP only support NORMAL_ACK and NO_ACK.**
   Section 11.1, item 4
   Parameter of AckPolicy is for an Ack policy which supports **normal Ack or no Ack**.
   The other two ack types have to be supported by the hardware.
2. **The difference of ACKs**
   - **a.** NORMAL_ACK is used to ACK data packet.
   - **b.** NO_ACK is used never ACK any data packet.
   - **c.** NO_EXPLICIT_ACK have two ways to implement,
     - ●By received packet count threshold to ACK.
     - ●By timeing period threshold to ACK.
   - **d.** BLOCK_ACK is used to ACK data packet per ACK request packet received.
     - ●If peer didn't request to ACK then never ACK.
     - ●This type of ACK is depends on what AIR quality is.
       - **1.)** AIR quality is bad, then the ACK should be mostly required.
       - **2.)** AIR quality is good, then the ACK period maybe longer or even needn't ACK.
3. **Reference:**
   Below table is pasted from IEEE802.11e-D13.0 for your reference.(Page 27 and 28)

Table 3.2—Ack policy field in QoS control field of QoS data frames

Bits in QoS Control field		Meaning
Bit 5	Bit 6	
0	0	Normal acknowledgement. The addressed recipient returns an ACK or

FOR wangxin@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

		QoS +CF-Ack frame after a SIFS period, according to the procedures defined in 9.2.8, 9.3.3 and 9.9.2.3. The Ack Policy field is set to this value in all directed frames in which the sender requires acknowledgement. For QoS Null (no data) frames, this is the only permissi-ble value for the Ack Policy field.
1	0	No Acknowledgement. The addressed recipient takes no action upon receipt of the frame. More details are provided in 9.11. The Ack Policy is set to this value in all directed frames in which the sender does not require acknowledgement. This combination is also used for broadcast and multicast frames that use the QoS frame format.
0	1	No Explicit Acknowledgement. There may be a response frame to the frame that is received, but it is neither the ACK nor any Data frame of subtype +CF-Ack. For Data frames of subtype QoS CF-Poll and subtype QoS CF-Ack+CF-Poll, this is the only permissible value for the Ack Policy field.
1	1	Block Acknowledgement. The addressed recipient takes no action upon the receipt of the frame except for recording the state. The recipient can expect a BlockAckReq frame in the future to which it responds using the procedure described in 9.10.

7.4 Access Precedence and Outgoing Frame Classification

1. 802.1e-D13

1.1. Section 7.3.2.16 Traffic Classification (TCLAS) Element

Table 20.7—Frame classifier type

Classifier Type	Classifier Parameters
0	Ethernet parameters
1	TCP/UDP IP parameters
2	IEEE 802.1D/Q Parameters
3-255	Reserved

1.2. Section 9.1.3.1 HCF contention-based channel access (EDCA)

Table 20.23—User priority to Access Category mappings

Priority	User priority (UP - Same as 802.1D User Priority)	802.1D Designation	Access Category (AC)	Designation (Informative)
lowest	1	BK	AC_BK	Background
	2	-	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
highest	7	NC	AC_VO	Voice

2. 802.1Q-2003

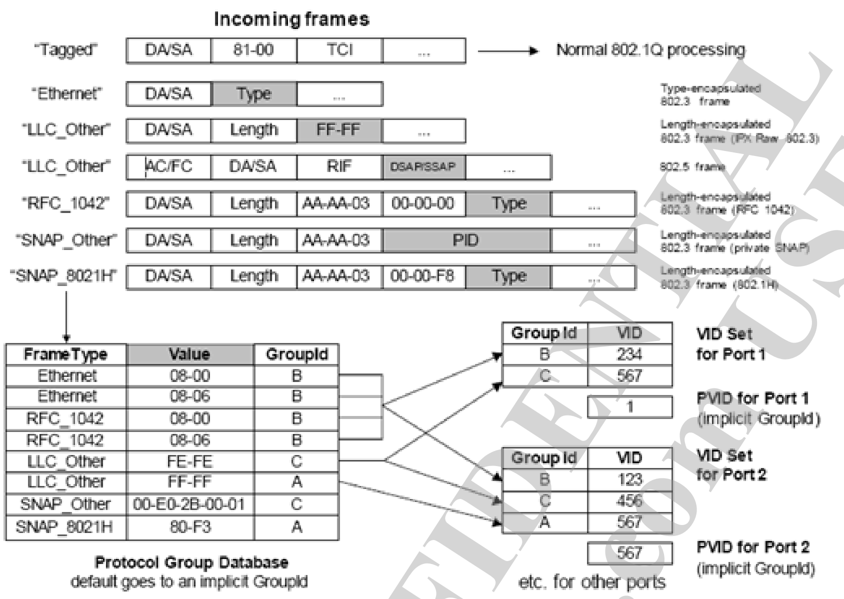
2.1. Section 8.9 VLAN classification

3. 802.1q-rev-d4.0-2005-05-19

3.1. Section 6.8 Protocol VLAN classification

FOR wangxiao@cmchina.com USE ONLY MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.


Incoming frames
"Tagged" DA/SA 81-00 TCI ... → Normal 802.1Q processing
"Ethernet" DA/SA Type ... Type-encapsulated 802.3 frame
"LLC_Other" DA/SA Length FF-FF ... Length-encapsulated 802.3 frame (IPX Raw 802.3)
"LLC_Other" AC/FC DA/SA RIF DSAP/SSAP ... 802.5 frame
"RFC_1042" DA/SA Length AA-AA-03 00-00-00 Type ... Length-encapsulated 802.3 frame (RFC 1042)
"SNAP_Other" DA/SA Length AA-AA-03 PID ... Length-encapsulated 802.3 frame (private SNAP)
"SNAP_8021H" DA/SA Length AA-AA-03 00-00-F8 Type ... Length-encapsulated 802.3 frame (802.1H)
VID Set for Port 1
PVID for Port 1 (implicit GroupId)
VID Set for Port 2
PVID for Port 2 (implicit GroupId)
etc. for other ports
Protocol Group Database
default goes to an implicit GroupId

FrameType	Value	GroupId
Ethernet	08-00	B
Ethernet	08-06	B
RFC_1042	08-00	B
RFC_1042	08-06	B
LLC_Other	FE-FE	C
LLC_Other	FF-FF	A
SNAP_Other	00-E0-2B-00-01	C
SNAP_8021H	80-F3	A

Group Id	VID
B	234
C	567
	1

Group Id	VID
B	123
C	456
A	567
	567

NOTE—The PID shown in this figure is a Protocol Identifier, as defined in 5.3 of IEEE Std 802. It is a 5-octet value consisting of a 3-octet OUI value followed by a 2-octet locally administered identifier.

Figure 6-2—Example of operation of port-and-protocol based classification

3.2. Section 9. Tagged frame format

Table 9-1—802.1Q Ethernet Type allocations		
Tag Type	Name	Value
VLAN TAG	802.1Q Tag Protocol Type (802.1QTagType)	81-00

4. RFC 2474

Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (802.11e - Differentiated Services Code Point (DSCP))

5. RFC 791

Internet Protocol

6. RFC 795

6.1. Service mappings – TOS of IP Header

The IP Type of Service has the following fields:

Bit 0-2	Precedence.
Bit 3	0 = Normal Delay, 1 = Low Delay.
Bit 4	0 = Normal Throughput, 1 = High Throughput.
Bit 5	0 = Normal Relibility, 1 = High Relibility.
Bit 6-7	Reserved for Future Use.

0	1	2	3	4	5	6	7
PRECEDENCE			D	T	R	00	
111 - Network Control 110 - Internetwork Control 101 - CRITIC/ECP 100 - Flash Override 011 - Flash 010 - Immediate 001 – Priority 000 - Routine							

MEDIATEK CONFIDENTIAL
FOR wangxiaole@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

8 IEEE802.11h+d

DFS - Dynamic Frequency Selection

8.1 IEEE802.11d

Regulatory Domains

1. To turn on IEEE802.11d, just fill up the parameter of ‘CountryCode’, according to ISO3166 code list. This parameter can work in A/B/G band.
2. The parameter of “CountryCode’ needs to match with ‘CountryRegion’ or ‘CountryRegionABand’ depends on A or B/G band
3. Wi-Fi test requirement for IEEE802.11d
   - Country code IE(0x07) includes in beacon frame and probe response
   - Power constraint IE(32) includes in beacon frame and probe response

8.2 IEEE802.11h

Spectrum and Transmit Power Management

1. To turn on IEEE802.11h, just fill up the parameters of ‘IEEE80211H’, ‘AutoChannelSelect’ as 1, WirelessMode set as 3 to support A band. This parameter can work in only A band.
2. Use ‘CSPeriod’ to determine how many beacons before channel switch
3. Driver will turn off BBP tuning temporarily in radar detection mode
4. If turn on IEEE802.11h, AP will have 60sec to do channel available check, and will not send beacon and can not be connect.
5. Wi-Fi test requirement for IEEE802.11h
   - Force AP switch channel, AP will stop beacon transmit between 15 sec
   - At least five beacon includes channel switch announcement IE (37)in beacon frame
6. ETSI test requirement, please refer to ETSI EN 301 893 for V1.2.3 detail

MEDIATEK CONFIDENTIAL FOR wangxian@cvchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Table D.1: DFS requirement values

Parameter	Value
Channel Availability Check Time	60 s
Channel Move Time	10 s
Channel Closing Transmission Time	260 ms

Table D.2: Interference Threshold values, Master

Maximum Transmit Power	Value (see note)
≥ 200 mW	-64 dBm
< 200 mW	-62 dBm
NOTE: This is the level at the input of the receiver assuming a 0 dBi receive antenna.	

Table D.3: Interference Threshold values, Slave

Maximum Transmit Power	Value (see note)
≥ 200 mW	-64 dBm
< 200 mW	N/A
NOTE: This is the level at the input of the receiver assuming a 0 dBi receive antenna.	

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

9 SECURITY POLICY

9.1 All possible combinations of security policy

Type I. No Radius

(Must set parameter of IEEE8021X as 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)

(Must set parameter of IEEE8021X as TRUE)

	OPEN
NONE	V
WEP	V
802.1x daemon	On

Type III. With WPA

(Must set parameter of IEEE8021X as FALSE)

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

The "off" of 802.1x daemon means may be off, it also can be "on"

However "on" of 802.1x daemon means must be "on"

There are no relationship between the parameter of IEEE8021X and 802.1x daemon (RT2860apd).

9.2 WP2 Setting

All settings are same as WPA, but modify attributes --- AuthMode, EncrypType, PreAuth, PMKCachePeriod.

9.3 Examples

9.3.1 OPEN/NONE

On Step-by-Step setting of how to set SoftAP using OPEN security mechanism.

FOR MEDIATEK CONFIDENTIAL USE ONLY wangxian@cvtchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

1. load WLAN SoftAP driver
2. iwpriv ra0 set AuthMode=OPEN
3. iwpriv ra0 set EncrypType=NONE
4. iwpriv ra0 set IEEE8021X=0
5. iwpriv ra0 set SSID=myownssid

9.3.2 SHARED/WEP

On Step-by-Step setting of how to set SoftAP using WEP security mechanism. Assume RT2800 SoftAP uses user-defined key.

1. load WLAN SoftAP driver
2. iwpriv ra0 set AuthMode=SHARED
3. iwpriv ra0 set EncrypType=WEP
4. iwpriv ra0 set IEEE8021X=0
5. iwpriv ra0 set Key1=0123456789
6. iwpriv ra0 set DefaultKeyID=1
7. iwpriv ra0 set SSID=myownssid

9.3.3 WPAPSK/TKIP

On Step-by-Step setting of how to set SoftAP using WPAPSK security mechanism with encryption method TKIP. Assume RT2800 SoftAP set PreShared Key as "myownpresharedkey". Please ensure to set SSID, before/after set WPAPSK.

1. load WLAN SoftAP driver
2. iwpriv ra0 set AuthMode=WPAPSK
3. iwpriv ra0 set EncrypType=TKIP
4. iwpriv ra0 set IEEE8021X=0
5. iwpriv ra0 set SSID=myownssid
6. iwpriv ra0 set WPAPSK=myownpresharedkey
7. iwpriv ra0 set DefaultKeyID=2
8. iwpriv ra0 set SSID=myownssid

9.3.4 WPAPSK/AES

Change setting to WPAPSK with AES.
1. iwpriv ra0 set AuthMode=WPAPSK
2. iwpriv ra0 set EncrypType=AES
3. iwpriv ra0 set IEEE8021X=0
4. iwpriv ra0 set SSID=MySsid
5. iwpriv ra0 set WPAPSK=MyPassword
6. iwpriv ra0 set DefaultKeyID=2
7. iwpriv ra0 set SSID=MySsid

Note:
Step 3 is a must for calculating WPAPSK Key, which requires both SSID and WPAPSK.
Step 5 will make driver to reload all settings. step5 must be the same with step3.

MEDIATEK CONFIDENTIAL
FOR wangyan@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

10 Authenticator

rt2860apd - user space IEEE 802.1X Authenticator

rt2860apd is an optional user space component for RT2800 SoftAP driver.
It adds 802.1x Authenticator feature using external RADIUS Authentication Server (AS).

10.1 I EEE 802.1X features in rt2860apd

IEEE Std 802.1X-2001 is a standard for port-based network access control. It introduces a extensible mechanism for authenticating and authorizing users.
rt2860apd implements partial IEEE 802.1x features that helps AS authorizing Supplicant and in the mean time proves itself a valid Authenticator for AS.
Noticed that Key management state machine is not included in rt2860apd. And those keys management is included in RT2800 SoftAP driver.
rt2860apd relays the frames between the Supplicant and the AS. Not until either one timeout or Success or Fail frame indicated does rt2860apd finish the authentication process.
The port control entity is implemented in SoftAP driver for RT2800.

10.2 How to start rt2860apd

Manually start rt2860apd, type “$rt2860apd”.

10.3 rt2860apd configuration for IEEE 802.1X

When rt2860apd starts, it reads the configuraion file to derive parameters. For any changes to make, one need to first edit the configuration file, then restart rt2860apd.
Please add 4 required parameters in the configuration file for WLAN SoftAP driver (RT2860AP.dat/RT2870AP.dat).

```
RADIUS_Server='192.168.2.3'
RADIUS_Port='1812'
RADIUS_Key='password'
own_ip_addr='your_ip_addr'
```

The word in ' ' must be replaced with your own correct setting. Please make sure 'your_ip_addr' and RADIUS_Server is connected and RADIUS_Server's IAS (or related) services are started.

The optional variables as below,

- session_timeout_interval is for 802.1x reauthentication setting.
  - set to zero to disable 802.1x reauthentication service for each session.
  - session_timeout_interval unit is second and must be larger than 60.

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangxian@ cvnchina.com USE ONLY

- For example,
  - session_timeout_interval = 120
    reauthenticate each session every 2 minutes.

  - session_timeout_interval = 0
    disable reauthenticate service.

- EAPifname is assigned as the binding interface for EAP negotiation.
  - Its default value is "br0". But if the wireless interface doesn't attach to bridge interface or the bridge interface name isn't "br0", please modify it.
  - For example,
    - EAPifname=br0
- PreAuthifname is assigned as the binding interface for WPA2 Pre-authentication.
  - Its default value is "br0". But if the ethernet interface doesn't attach to bridge interface or the bridge interface name isn't "br0", please modify it.
  - For example,
    - PreAuthifname=br0

10.4 Support Multiple RADIUS Servers

We use complier option to turn on/off the multiple RADIUS servers for 802.1x.
If you want to enable the feature, make sure that "MULTIPLE_RADIUS" is defined in Makefile. Default is disabled. Besides, you must modify the file "RT2860AP.dat" to co-operate with 802.1x. We extend some variables to support individual RADIUS server IP address, port and secret key for MBSS.
E.g.
```
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
```
Or
```
RADIUS_Key1=ralink_1
RADIUS_Key2=ralink_2
RADIUS_Key3=ralink_3
RADIUS_Key4=ralink_4
```
For backward compatibility, the driver parses "RADIUS_Key" or RADIUS_KeyX"(X=1~4) for radius key usage. But the paramter "RADIUS_Key" has the first priority.
This implies,
The RADIUS server IP of ra0 is 192.168.2.1, its port is 1811 and its secret key is ralink_1.
The RADIUS server IP of ra1 is 192.168.2.2, its port is 1812 and its secret key is ralink_2.
The RADIUS server IP of ra2 is 192.168.2.3, its port is 1813 and its secret key is ralink_3.
The RADIUS server IP of ra3 is 192.168.2.4, its port is 1814 and its secret key is ralink_4.
If your wireless interface prefix is not "ra", please modify these variables.

10.5 Enhance dynamic wep keying

In OPEN-WEP with 802.1x mode, the authentication process generates broadcast and unicast key. The unicast key is unique for every individual client so it is always generated

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

randomly by 802.1x daemon. But the broadcast key is shared for all associated clients; it can be pre-set manually by users or generated randomly by 802.1x daemon.
Through the parameter "DefaultKeyID" and its corresponding parameter "KeyXStr"(i.e. X = the value of DefaultKeyID) in RT2860Ap.dat, the 802.1x daemon would use it as the broadcast key material. But if the corresponding parameter "KeyXStr" is empty or unsuitable, the broadcast key would be generated randomly by the 802.1x daemon.
The 802.1x daemon need to read RT2860AP.dat to decide whether the broadcast key is generated randomly or not, so please update the RT2860AP.dat and restart rt2860apd if those correlative parameters are changed.

10.6 Examples for Radius server configuration

10.6.1 Example I

This is a step-by-step guide to set SoftAP using WPA security mechanism. Assume RT2800 SoftAP has ip address 192.168.1.138, AS (Authentication Server) has IP address 192.168.1.1, Radius Secret is myownkey.

1. load WLAN SoftAP driver
   - $insmod rt2860ap.o
2. First edit configuration file with correct value, esp. the following parameters that relate to the authentication features of RT2800AP.dat
   ```
   RADIUS_Server=192.168.1.1
   RADIUS_Port=1812
   RADIUS_Key=myownkey
   own_ip_addr=192.168.1.138
   ```
3. start RT2800apd daemon by typing.
   - $rt2860apd
4. iwpriv ra0 set AuthMode=WPA
5. iwpriv ra0 set EncrypType=TKIP
6. iwpriv ra0 set DefaultKeyID=2
7. iwpriv ra0 set IEEE8021X=0
8. iwpriv ra0 set SSID=myownssid

10.6.2 Example II

Change 802.1x settings to WPA with TKIP, using 802.1x authentication.

1. Modify 4 parameters
   ```
   RADIUS_Server=192.168.2.3
   RADIUS_Port=1812
   RADIUS_Key=password
   own_ip_addr=192.168.1.123
   ```
   in the RT2860AP.dat and save.
2. iwpriv ra0 set AuthMode=WPA
3. iwpriv ra0 set EncrypType=TKIP

MEDIATEK CONFIDENTIAL FOR wangxiang@cmetina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

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

Note:

Step 4 restarts the rt2860apd, and is essential.

10.6.3 Example III

Change setting to OPEN/WEP with 802.1x.

1. iwpriv ra0 set AuthMode= OPEN
2. iwpriv ra0 set EncrypType= WEP
3. iwpriv ra0 set IEEE8021X=1

Note:

"IEEE8021X=1" only when Radius-WEP or Radius-NONE mode on, otherwise must "IEEE8021X=0".

10.6.4 Example V

Change setting to OPEN/NONE with 802.1x.

1. iwpriv ra0 set AuthMode= OPEN
2. iwpriv ra0 set EncrypType= NONE
3. iwpriv ra0 set IEEE8021X=1

Note:

"IEEE8021X=1" only when Radius-WEP or Radius-NONE mode on , otherwise must "IEEE8021X=0".

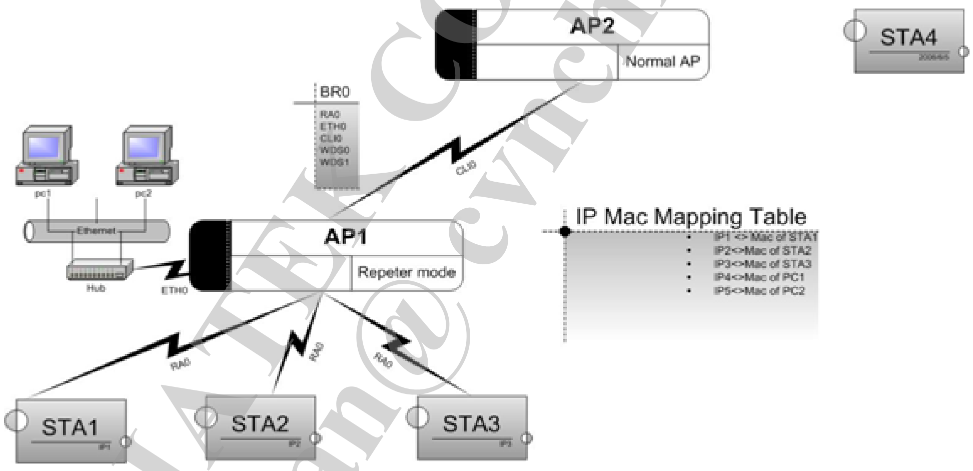
MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

11 AP CLIENT

The AP-Client function provides a 1-to-N MAC address mapping mechanism such that multiple stations behind the AP can transparently connect to the other AP even they didn't support WDS. When enable the AP-Client function, RT2800 driver will create two interfaces, one is the AP interface which provide the features of Access Point, the other is the station interface used to connect to the remote AP. Besides, the software bridge function is used to forward packets between these two interfaces.

The figure 1 shows the network topology and operation module of our AP-client function. The AP1 is an AP-Client feature enabled Access Point and have two wireless interfaces, ra0 and cli0, which provide the AP and station functions, respectively. The AP2 is a legacy Access Point that supports normal AP functions. STA1 associated to AP1 and the STA4 associated to AP2. In general, if the STA1 want to communicate with STA4, the AP2 and AP1 must support WDS or a physical network connection between AP1 and AP2. Now, with the support the AP-Client function, the AP1 can use build-in station interface cli0 connect to AP2, and then STA1 can communicate with STA4 transparently and didn't do any modifications. Also, the stations connect to the AP1 through the Ethernet line also can communicate with STA4 or access the Internet through AP2 transparently.



Before enable the AP-Client feature, there are some restrictions need to remind

(1). Due to the limitation of 1-to-N MAC address mapping, AP-Client function currently only support following protocols:
   (a). All IP-based network applications
   (b). ARP
   (c). DHCP
   (d). PPPoE

(2). The last 2 hexadecimal number of the Mac address of our device must be the multiple of 4.

(3). The OS must provide a software bridge function can bridge multiple network interfaces.

It's simple to enable the feature of AP-Client; you just need to set the flag "HAS_APCLIENT" as "y" in the driver Makefile and got it.

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxian@cvnchina.com

11.1 Setup AP Client

1. Edit file in /etc/Wireless/RT2800AP/RT2800AP.dat to add
    a) ApCliEnable=1
    b) ApCliSsid=AP2
    c) ApCliBssid=00:10:20:30:40:50 (optional)
    d) ApCliAuthMode=WPAPSK
    e) ApCliEncrypType=TKIP
    f) ApCliWPAPSK=12345678
2. Like the procedure of bringing up main BSSID (ra0), it also must to add "/sbin/ifconfig apcli0 up" and "/usr/sbin/brctl addif br0 apcli0".
3. The AP-client's security policy only supports NONE, WEP (OPEN, SHARED), WPAPSK and WPA2PSK (TKIP, AES).
4. Set the "HAS_APCLI" flag as "y" in config.mk to enable or disable this function.
5. If enable AP client function, the maximum multiple BSSID number would be 7 and the field 'BssidNum' shall larger than 1 and less than 7.
6. Users can also configure AP Client by iwpriv command.

11.2 Support Parameters in RT2860AP.dat

11.2.1 ApCliEnable

Description: enable or disable AP client function
Value:

```
ApCliEnable=1

0: disable
1: enable
```

11.2.2 ApCliSsid

Description: The target SSID which AP client is going to connect with it.
Value:

```
ApCliSsid=target_ssid

1~32 characters
```

11.2.3 ApCliBssid

Description: Set the BSSID which the AP Client wants to join
Value:

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

[MAC address]
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Note: It is an optional command. Users can indicate the desired BSSID by this command.Otherwise, AP Client can also get appropriate BSSID according to SSID automatically.

11.2.4 ApCliWPAPSK

Description: Set the WPA pre-shared key of AP client.
Value:

```
ApCliWPAPSK=12345678

8 ~ 63 ASCII characters or
64 hexadecimal characters
```

11.2.5 ApCliAuthMode

Description: Set the AP Client authentication mode
Value:

```
ApCliAuthMode=OPEN

OPEN
SHARED
WPAPSK
WPA2PSK
```

11.2.6 ApCliEncrypType

Description: Set the AP client encryption type.
Value:

```
ApCliEncrypType=NONE

NONE:   ApCliAuthMode =OPEN
WEP:    ApCliAuthMode =OPEN or SHARED
TKIP:   ApCliAuthMode =WPAPSK or WPA2PSK
AES:    ApCliAuthMode =WPAPSK or WPA2PSK
```

11.2.7 ApCliDefaultKeyID

Description: Set the default key index of AP client
Value:

```
ApCliDefaultKeyID=1

1~4
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

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 eg: 012345678
5 or 13 ASCII characters eg: passd

11.2.10 ApCliKey1Type

Descripion: Set the WEP key type of AP client for key index 1.
Value:

ApCliKey1Type=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 eg: 012345678
5 or 13 ASCII characters eg: passd

11.2.12 ApCliKey2Type

Descripion: Set the WEP key type of AP client for key index 2.
Value:

ApCliKey2Type=0

0: Hexadecimal
1: ASCII

MEDIATEK CONFIDENTIAL
FOR wangxiang@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

11.2.13 ApCliKey3Str

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

ApcliKey3Str=012345678

10 or 26 hexadecimal characters eg: 012345678
5 or 13 ASCII characters eg: passd

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 eg: 012345678
5 or 13 ASCII characters eg: passd

11.2.16 ApCliTxMode

Description: Set transmission mode for AP-Client traffic
Value:

ApCliTxMode=HT

cck|CCK,
ofdm|OFDM,
ht|HT

11.2.17 ApCliTxMcs

Description: Set TX MCS for AP client
Value:

ApCliTxMcs=33

0~15, or 33 (Auto)

FOR wangxian@ cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

11.2.18 ApCliWscSsid

Description: Set the SSID which the AP-Client wants to negotiate WPS
Value:

    ApCliWscSsid=target_ssid

    1~32 characters

11.3 AP Client iwpriv command

Syntax:

iwpriv apcli0 set [Paramster]=[Value]

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: Set the target SSID which AP Client wants to connect with
Value:

    iwpriv apcli0 set ApCliSsid=target_ssid

    1~32 characters

11.3.3 ApCliBssid

Description: Set BSSID which AP Client wants to join
Value:

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

    [MAC address]

Note: It is an optional command. Users can indicate the desired BSSID by this command. Otherwise, AP Client can also get appropriate BSSID according to SSID automatically.

11.3.4 ApCliWPAPSK

Description: AP Client WPA Pre-Shared Key

MEDIATEK CONFIDENTIAL FOR wangran@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Value:

iwpriv apcli0 set ApCliWPAPSK=12345678

8~63 ASCII
64 HEX characters

11.3.5 ApCliAuthMode

Description: Set AP Client Authentication mode
Value:

iwpriv apcli0 set ApCliAuthMode=OPEN

OPEN
SHARED
WPAPSK
WPA2PSK

11.3.6 ApCliEncrypType

Description: Set AP Client Encryption Type
Value:

iwpriv apcli0 set ApCliEncrypType=NONE

NONE
WEP
TKIP
AES

11.3.7 ApCliWscSsid

Description: Set the SSID which the AP-Client wants to negotiate WPS
Value:

iwpriv apcli0 set ApCliWscSsid=target_ssid

1~32 characters

11.3.8 ApCliDefaultKeyID

Description: Set the default key index of AP client
Value:

iwpriv apcli0 set ApCliDefaultKeyID=1

1~4

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxian@ cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

11.3.9 ApCliKey1Type

Descripion: Set the WEP key type of AP client for key index 1.
Value:

```
iwpriv apcli0 set ApCliKey1Type=0
```

0: Hexadecimal
1: ASCII

11.3.10 ApCliKey1Str

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

```
iwpriv apcli0 set  ApcliKey1Str=012345678
```

10 or 26 hexadecimal characters eg: 012345678
5 or 13 ASCII characters eg: passd

11.3.11 ApCliKey1Type

Descripion: Set the WEP key type of AP client for key index 1.
Value:

```
iwpriv apcli0 set ApCliKey1Type=0
```

0: Hexadecimal
1: ASCII

11.3.12 ApCliKey2Str

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

```
iwpriv apcli0 set ApcliKey2Str=012345678
```

10 or 26 hexadecimal characters eg: 012345678
5 or 13 ASCII characters eg: passd

11.3.13 ApCliKey2Type

Descripion: Set the WEP key type of AP client for key index 2.
Value:

```
iwpriv apcli0 set ApCliKey2Type=0
```

0: Hexadecimal
1: ASCII

MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

11.3.14 ApCliKey3Str

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

```
iwpriv apcli0 set ApcliKey3Str=012345678

10 or 26 hexadecimal characters eg: 012345678
5 or 13 ASCII characters eg: passd
```

11.3.15 ApCliKey4Type

Descripion: Set the WEP key type of AP client for key index 4.
Value:

```
iwpriv apcli0 set ApCliKey4Type=0

0: Hexadecimal
1: ASCII
```

11.3.16 ApCliKey4Str

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

```
iwpriv apcli0 set ApcliKey4Str=012345678

10 or 26 hexadecimal characters eg: 012345678
5 or 13 ASCII characters eg: passd
```

11.4 AP Client Examples

11.4.1 Enable AP Client with OPEN/NONE data security

```
iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliAuthMode=OPEN
iwpriv apcli0 set ApCliEncrypType=NONE
iwpriv apcli0 set ApCliSsid=AP2
iwpriv apcli0 set ApCliEnable=1
```

11.4.2 Enable AP Client with OPEN/WEP security

```
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=AP2
iwpriv apcli0 set ApCliEnable=1
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wanggai@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

11.4.3 Enable AP Client with SHARED/WEP security

```
iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliAuthMode=SHARED
iwpriv apcli0 set ApCliEncrypType=WEP
iwpriv apcli0 set ApCliDefaultKeyID=2
iwpriv apcli0 set ApCliKey2=2345678901
iwpriv apcli0 set ApCliSsid=AP2
iwpriv apcli0 set ApCliEnable=1
```

11.4.4 Enable AP Client with WPAPSK/TKIP security

```
iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliAuthMode=WPAPSK
iwpriv apcli0 set ApCliEncrypType=TKIP
iwpriv apcli0 set ApCliSsid=AP2
iwpriv apcli0 set ApCliWPAPSK=12345678
iwpriv apcli0 set ApCliEnable=1
```

11.4.5 Enable AP Client with WPAPSK/AES security

```
iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliAuthMode=WPA2PSK
iwpriv apcli0 set ApCliEncrypType=AES
iwpriv apcli0 set ApCliSsid=AP2
iwpriv apcli0 set ApCliWPAPSK=12345678
iwpriv apcli0 set ApCliEnable=1
```

11.4.6 AP Client WPS sample command

PIN mode:

```
iwpriv apcli0 set WscConfMode=1
iwpriv apcli0 set WscConfStatus=1
iwpriv apcli0 set WscMode=1
iwpriv apcli0 set WscGetConf=1
```

PBC Mode:

```
iwpriv apcli0 set WscConfMode=1
iwpriv apcli0 set WscConfStatus=1
iwpriv apcli0 set WscMode=2
iwpriv apcli0 set WscGetConf=1
```

FOR wangjian@cychina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

12 WDS

Wireless Distribution System.

Each WDS APs need seting as **same channel**, **encryption type**. (not support mixed mode, like WPAPSKWPA2PSK).

WDS Security support up to pre-shared key, this is inter AP's security and **no 802.1x support**.

In case want have auto-learning WDS peers, Lazy mode is the one. But have to note that can't set each AP to Lazy mode, otherwise no addr4 will be carried by each AP. This means that there at least has one AP have to fill WDS list.

12.1 HOW to Steup WDS

1. edit file in /etc/Wireless/RT2860AP/RT2860AP.dat to add
   (a). WdsEnable=1
   (b). WdsList=00:10:20:30:40:50; ;Another AP's MAC address
   (c). WdsEncrypType=NONE ;the encryption type in WDS interface
2. edit script file bridge_setup according to **the number of WDS-AP**
   add "/usr/sbin/brctl addif br0 wds0" and "/sbin/ifconfig wds0 0.0.0.0" to relative place.
3. re-load WLAN driver(rt2860ap.o)
4. run bridge_setup

12.2 WDS Individual Encryption

If the WDS mode is enabled and set as LAZY mode, the all WDS-link shall share the same encryption type and key material (based on wds0 setting). Otherwise, each WDS-link has own individual security setting. No matter what WDS mode is set; it has no any relation to the encryption of BSSIDs.
Although the new WDS implementation has been provided, it alos supports previous WDS configuration.

A: WdsKey:
WdsKey is used for all WDS interface and support AES or TKIP encryption only. WEP key will follow main-AP's setting. Wds0Key/Wds1Key/Wds2Key/Wds3Key is used to support all of the encryption per WDS interface, WEP, TKIP, and AES.

B: AuthMode:
Follows the main-AP's setting.

Case 1: main AP choose open mode, and WDS choose WEP or AES

AuthMode: OPEN, take from main-AP
EncrypType: WDS = WEP or AES
⇨ WEP key will follow main-AP's setting,
Or, take from Wds0Key… depend on which WDs interface.

FOR MEDIATEK CONFIDENTIAL USE ONLY
yangxian@cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

⇨ AES key will take from WdsKey or Wds0Key, depend on which WDs interface.
Please use PING to check the data whether encrypted or not.

Case 2: main AP is wep mode, and WDS is AES mode

AuthMode: WEP

12.3 Supported Paramters in RT2860AP.dat

12.3.1 WdsEnable

Description: Enable or disable WDS function
Value:

WdsEnable=0

0: Disable - Disable all WDS function.
1: Restrict mode - Same as Repeater mode.
2: Bridge mode - Turn on WDS function, the peer WDS APs are according to the mac address listed in "WdsList" field below. In this mode, AP will not send beacon out and will not deal with probe request packets, therefore STA will not possible to connect with it.
3: Repeater mode - Turn on WDS function, the peer WDS APs are according to the mac address listed in "WdsList" field below.
4: Lazy mode - Turn on WDS function, and auto learning from WDS packet which with addr4 field.

12.3.2 WdsList

Description: WDS list for making the connection
Value:

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

Maximun up to 4 lists

12.3.3 WdsEncrypType

Description: WDS encryption type
Value:

WdsEncrypType=NONE

NONE
WEP
TKIP
AES

Example:
WdsEncrypType= OPEN;TKIP;WEP;AES

The encrptytion of wds0 is OPEN
The encrptytion of wds1 is TKIP

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

The encrptytion of wds2 is WEP
The encrptytion of wds3 is AES

12.3.4 WdsKey

Description: The Key of WDS Link
Value:

WdsKey=12345678

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

Note: Combinationsof WDS security mode

Main BSSID's EncrypType	WDS's WdsEncrypType	Peer AP WDS's WdsEncrypType	Remark
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 Link0
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 for TKIP or AES
64 hexadecimal characters for TKIP or AES

12.3.6 Wds1Key

Description: WDS key for Link1
Value:

Wds1Key=12345678

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

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

12.3.7 Wds2Key

Description: WDS key for Link2
Value:

```
Wds2Key=12345678
```

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

12.3.8 Wds3Key

Description: WDS key for Link3
Value:

```
Wds3Key=12345678
```

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

12.3.9 WdsDefaultKeyID

Description: The default key index setting
Value:

```
WdsDefaultKeyID=1
```

1~4
Example:

```
WdsDefaultKeyID=1;2;3;4
```

The key index of wds0 is 1
The key index of wds1 is 2
The key index of wds2 is 3
The key index of wds3 is 4

12.3.10 WdsPhyMode

Description: configure WDS Link physical mode
Value:

```
WdsPhyMode=HTMIX
```

CCK
OFDM
HTMIX

FOR wangran@ cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

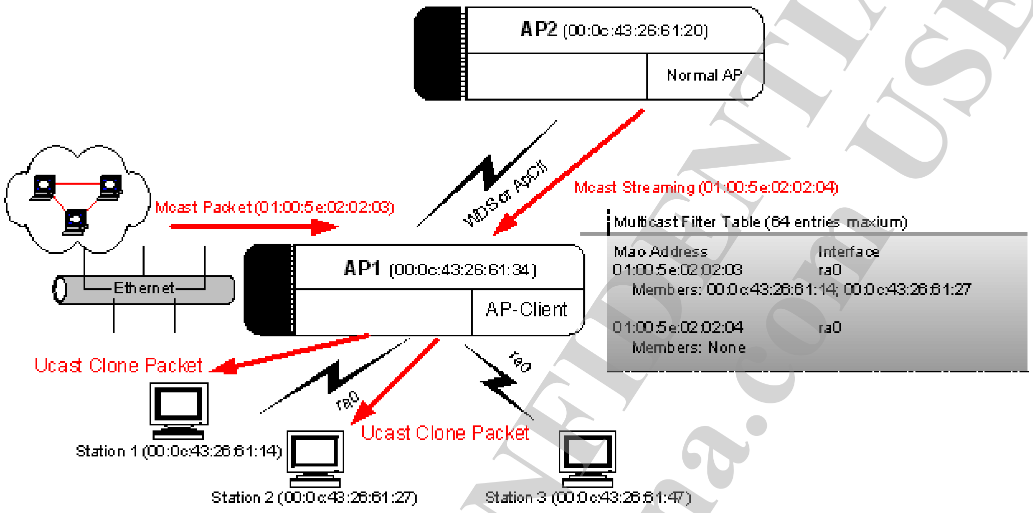
This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

GREENFIELD

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

13 IGMP SNOOPING


AP2 (00:0c:43:26:61:20)
Normal AP
WDS or ApCli
Mcast Streaming (01:00:5e:02:02:04)
Mcast Packet (01:00:5e:02:02:03)
Ethernet
AP1 (00:0c:43:26:61:34)
AP-Client
Multicast Filter Table (64 entries maxium)
Mac Address
Interface
01:00:5e:02:02:03
ra0
Members: 00:0c:43:26:61:14; 00:0c:43:26:61:27
01:00:5e:02:02:04
ra0
Members: None
Ucast Clone Packet
ra0
Ucast Clone Packet
ra0
Station 1 (00:0c:43:26:61:14)
Station 2 (00:0c:43:26:61:27)
Station 3 (00:0c:43:26:61:47)

13.1 IMGP Table Learning

An IGMP table entry consists of Group-Id (Multicast MAC Address), Net-Interface and Member-List. For example, in the picture above we see the “Multicast Filter Table” of AP1 have two IGMP entries. One is “01:00:5e:02:02:03” with two members and another is “01:00:5e:02:02:04 with empty member list”. AP will automatically insert or remove the entry from table by snooping the IGMP-Membership report packet from Station behind AP. And it also could be manual add and del by iwpriv command.

13.2 Multicast Packet Process

Once a multicast packet whether it comes from portal, WDS or AP-Client. AP will go through the Multicast-filter table to find a match rule for the incoming packet. If have no any match rule in the table then AP will simply drops it. If it does then there are two cases how AP handles a multicast packet. The first cast is the match entry has no member then AP just forwards it to all stations behind the net-interface. If the match entry has members then AP will do unicast clone for all members.

For example, AP1 receive a multicast packet with group-Id, “01:00:5e:02:02:03”, comes from Ethernet then AP1 check the multicast table using group-Id and fount it match the entry with 2 members. So AP1 clone the multicast packet and sent them to Station 1 and Station 2. Another case a multicast packet with group-id (01:00:5e:02:02:04) be sent to AP1 then AP1 just forward it to all Stations behind interface, ra0 since the match entry have no member.

FOR wangxian@cwnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

13.3 IGMP SNOOPING in RT2860.dat support

13.3.1 IgmpSnEnable

Description: enable or disable IGMP snooping function
Value:

```
IgmpSnEnable=1

0: disable
1: enable
```

13.4 Iwpriv command for IGMP SNOOPING

Syntax:

```
iwpriv ra0 set [Parameter]=[Value]
```

13.4.1 IgmpSnEnable

Description: enable or disable IGMP SNOOPING
Value:

```
iwpriv ra0 set IgmpSnEnable=1

0: disable
1: enable
```

Note: If the command returns failed, please make sure IGMPSNOOP_SUPPORT is selected or not in driver config.mk

13.4.2 IgmpAdd

Description: It also provide a command let user add an entry by iwpriv command "set IgmpAdd=<Group-ID>", Group-ID could be a MAC address or a IP address.
Also can add members into a Group by command "set IgmpAdd=<Group-ID-[Member]-… >", Group-ID could be a MAC address or an IP address.

Value:

```
//Add Group-ID
iwpriv ra0 set IgmpAdd=226.2.2.3
or
iwpriv ra0 set IgmpAdd=01:00:5e:02:02:03

//Add Group-ID-member
iwpriv ra0 set IgmpAdd=226.2.2.3-00:0c:43:26:61:27-00:0c:43:26:61:28
or
iwpriv ra0 set IgmpAdd=01:00:5e:02:02:03-00:0c:43:26:61:27-00:0c:43:26:61:28
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangjian@cvnchina.com USE ONLY

13.4.3 IgmpDel

Description: the entry can be deleted by command “set IgmpDelEntry=<Group-ID>”.
Also can delete a member from a Group by command “set IgmpDel=<Group-ID-[Member]-... >”, Group-ID could be a MAC address or an IP address.

Value:

```
//Delete by Group-ID
iwpriv ra0 set IgmpDel=226.2.2.3
iwpriv ra0 set IgmpDel=01:00:5e:02:02:03

//Delete by Group-ID-Member
iwpriv ra0 set IgmpDel=226.2.2.3-00:0c:43:26:61:27-00:0c:43:26:61:28
iwpriv ra0 set IgmpDel=01:00:5e:02:02:03-00:0c:43:26:61:27-00:0c:43:26:61:28
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

14 MAC Repeater

The MAC repeater acts as a Wi-Fi proxy for its clients. For each device connected to the repeater, the extender must create a connection to the root AP separately. The MAC repeater will make connections according to its own wireless capability and security mode. When the device is disconnected from the repeater, the repeater must disconnect the connection between root AP and the repeater for this device. The repeater makes the root AP unaware of what are behind the repeater. From the Root AP side, it just sees all the repeater clients in the same BSS.

All communications between the repeater clients and Root AP are utilizing one “AP client” interface on the repeater.

Bridge: Ethernet / Wireless (AP / AP client)

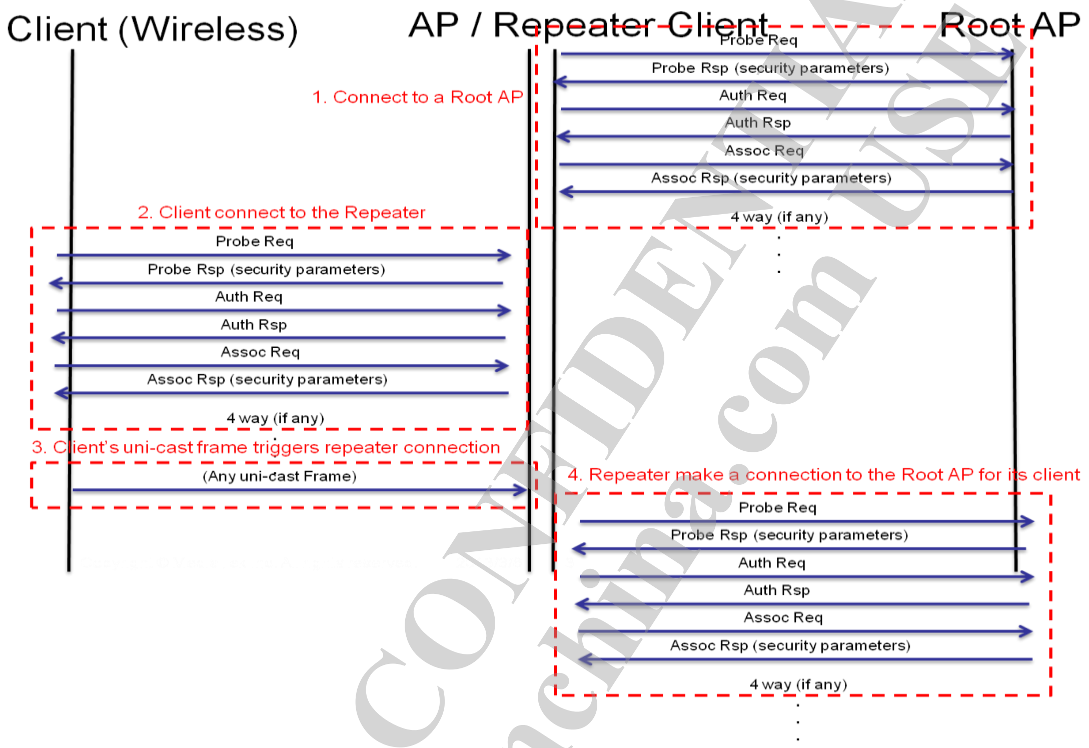
The implement must enable apcli function and bridge all network interfaces.

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

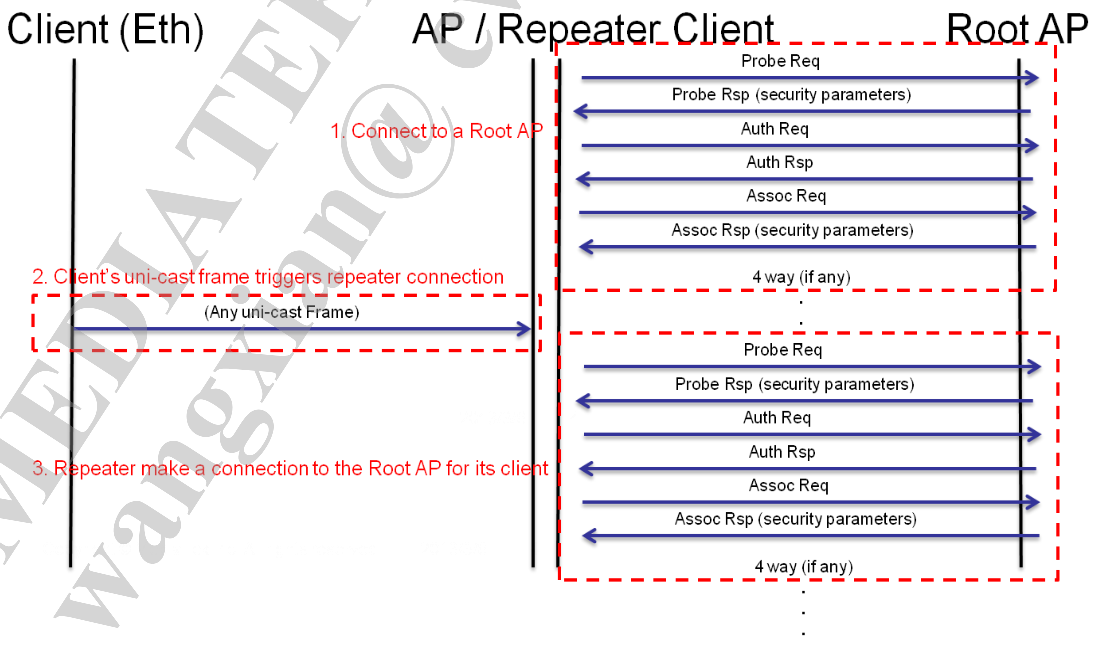
This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

14.1 MAC Repeater Management Flow

Management Flow Chart (Wireless):


Client (Wireless)
AP / Repeater Client
Root AP
1. Connect to a Root AP
Probe Req
Probe Rsp (security parameters)
Auth Req
Auth Rsp
Assoc Req
Assoc Rsp (security parameters)
4 way (if any)
2. Client connect to the Repeater
Probe Req
Probe Rsp (security parameters)
Auth Req
Auth Rsp
Assoc Req
Assoc Rsp (security parameters)
4 way (if any)
3. Client's uni-cast frame triggers repeater connection
(Any uni-cast Frame)
4. Repeater make a connection to the Root AP for its client
Probe Req
Probe Rsp (security parameters)
Auth Req
Auth Rsp
Assoc Req
Assoc Rsp (security parameters)
4 way (if any)

Management Flow Chart (Ethernet):

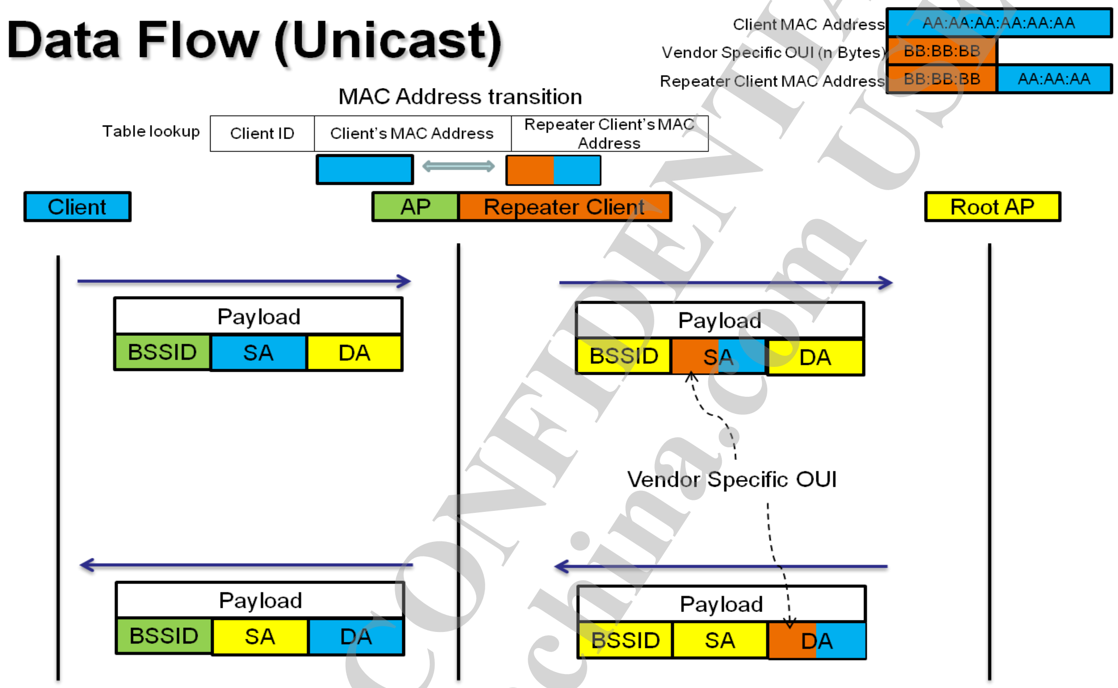

Client (Eth)
AP / Repeater Client
Root AP
1. Connect to a Root AP
Probe Req
Probe Rsp (security parameters)
Auth Req
Auth Rsp
Assoc Req
Assoc Rsp (security parameters)
4 way (if any)
2. Client's uni-cast frame triggers repeater connection
(Any uni-cast Frame)
3. Repeater make a connection to the Root AP for its client
Probe Req
Probe Rsp (security parameters)
Auth Req
Auth Rsp
Assoc Req
Assoc Rsp (security parameters)
4 way (if any)

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

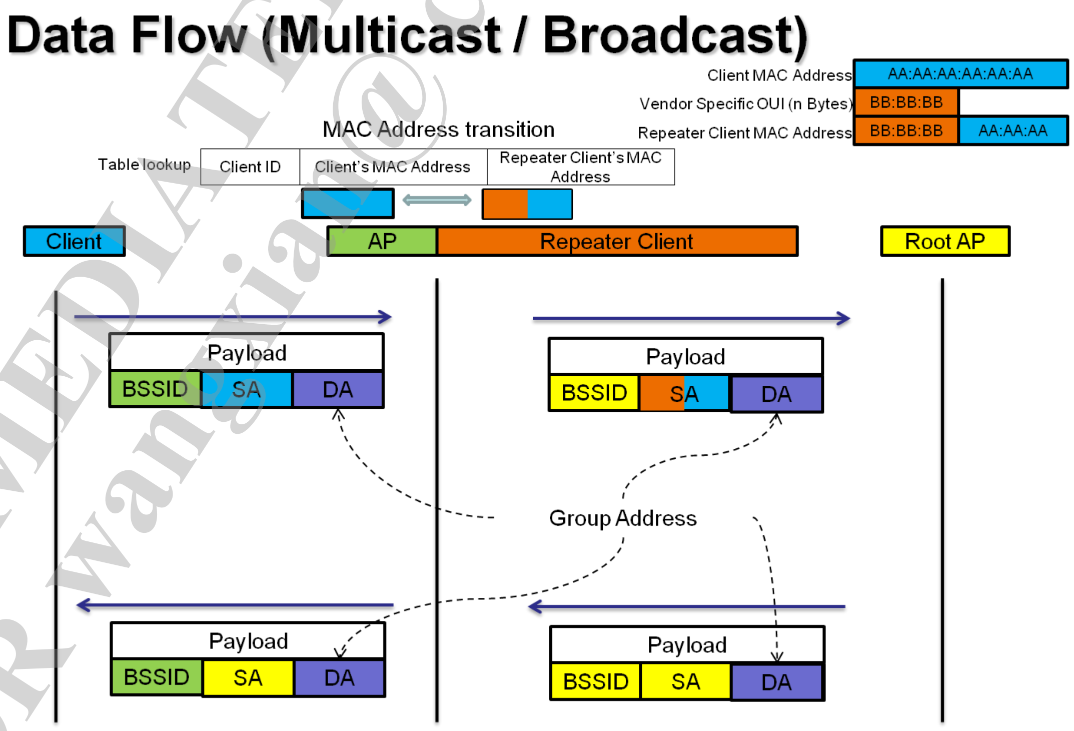
This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

14.2 MAC Repeater Data Flow

14.2.1 Unicast Data Flow



14.2.2 Multicast / Broadcast Data Flow



MEDIATEK CONFIDENTIAL
FOR wangxiao@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

14.3 MAC Repeater Limitation

- Roaming of STAs between different BSSs is not supported.
- WPA2-Enterprise Security is not supported.
- Supported protocols: IPv4 / ARP / DHCP
- The repeater does not response for an end-to-end reliability and security.
- Support max 16 repeater clients; the others are treated as AP clients.
- Impact CPU utilization due to parse all received packets from the STA and all multicast and broadcast packets.

14.4 MAC Repeater Example command

14.4.1 MAC Repeater by Wi-Fi Profile:

To enable MAC Repeater:

Add MACRepeaterEn = 1 into the WLAN profile “RT2860AP.dat”.

To disable MAC Repeater:

Add MACRepeaterEn = 0 into the WLAN profile.

14.4.2 MAC Repeater by Wi-Fi command:

```
iwpriv ra0 set MACRepeaterEn=1
ifconfig apcli0 up
iwpriv apcli0 set ApCliEnable=0
iwpriv apcli0 set ApCliSsid=MT7610_RootAP
iwpriv apcli0 set ApCliAuthMode=OPEN
iwpriv apcli0 set ApCliEncrypType=NONE
iwpriv apcli0 set ApCliEnable=1
brctl addif br0 apcli0
```

MEDIATEK CONFIDENTIAL
FOR wangjian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

15 Multiple BSSID Setup

1. Before turn on multiple BSSID, make sure the byte5 of MAC address in EEPROM is a multiple of 1/2/4/8 and reserve multiple MAC address when manufacturing. example, 00:0A:0B:0C:0D:04; 00:0A:0B:0C:0D:88.
2. When enable multiple BSSID function, the field 'BssidNum' shall larger than 1 and less than 8.
3. BssidNum can only be modified with editing configure file.
   When change the ' BssidNum ' field, the driver must restart, and modify bridge_setup file to group virtual interface.
   Others parameters can pass through iwpriv according to their interface.
4. The parameter that support **multiple BSSID** is listed as followed,

SSID
AuthMode
EncrypType
WPAPSK
DefaultKeyID
Key1Type
Key1Str
Key2Type
Key2Str
Key3Type
Key3Str
Key4Type
Key4Str
AccessPolicy
AccessContro
lList
NoForwarding
IEEE8021X
HideSSID
PreAuth
WmmCapable

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

5. Example of notation to represent multiple ssid's parameter:
    1.) BssidNum=4
    2.) SSID=SSID-A;SSID-B;SSID-C;SSID-D
    3.) AuthMode=OPEN;SHARED;WPAPSK;WPA
    4.) EncrypType=NONE;WEP;TKIP;AES
6. The WDS's security policy must be the same as main BSSID and only support NONE, WEP, TKIP, and AES.
7. MBSSID and WDS.
   There 64 security key table in MAC(RT2800).

Entry 0:	For reserved.
Entry 1 - 59:	For Associated STA and WDS link.

   Current driver defined WDS number to 4.

MEDIATEK CONFIDENTIAL
FOR wangxian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

16 Concurrent A+G Settings

Below table is brief example for two interfaces.
For example, Linux HotPlug system found new device would create one driver instance (create new space for driver image) for new device to hold private information (memory consumed).

RT2800 Interface Bring Up Sequence						
NIC#	Sequence	Normal	WDS(Virtual)			
			1	2	3	4
Two	ifconfig ra0 up	ra0	wds0	wds1	wds2	wds3
	ifconfig ra1 up	ra1	wds4	wds5	wds6	wds7

NIC#	Sequence	Normal	MBSSID (Physical)			WDS(Virtual)			
						1	2	3	4
Two	ifconfig ra0 up	ra0	ra2	ra3	ra4	wds0	wds1	wds2	wds3
	ifconfig ra1 up	ra1	ra5	ra6	ra7	wds4	wds5	wds6	wds7

WDS IS A VIRTUAL INTERFACE WITHOUT IOCTL FUNCTIONALITY.

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

17 SNMP MIBs Support List

17.1 RT2860AP Supported v.s. IEEE802dot11-MIB

IEEE802dot11-MIB	Access	Support	OID	RT2860AP.dat
ieee802dot11				
dot11smt		-		
dot11StationConfigTable	not-accessible	-		
dot11StationConfigEntry	not-accessible	-		
dot11StationID	read-write	Y	OID_802_3_CURRENT_ADDRESS	N
dot11MediumOccupancyLimit	read-write	N		N
dot11CFPollable	read-only	N		N
dot11CFPPeriod	read-write	N		N
dot11CFPMaxDuration	read-write	N		N
dot11AuthenticationResponseTimeOut	read-write	N		N
dot11PrivacyOptionImplemented	read-only	Y	RT_OID_802_11_PRIVACYOPTIONIMPLEMENTED	N
dot11PowerManagementMode	read-write	Y	RT_OID_802_11_POWERMANAGEMENTMODE	N
dot11DesiredSSID	read-write	N		N
dot11DesiredBSSType	read-write	N		N
dot11OperationalRateSet	read-write	N		N
dot11BeaconPeriod	read-write	N		N
dot11DTIMPeriod	read-write	N		N
dot11AssociationResponseTimeOut	read-write	N		N
dot11DisassociateReason	read-only	N		N
dot11DisassociateStation	read-only	N		N
dot11DeauthenticateReason	read-only	N		N
dot11DeauthenticateStation	read-only	N		N
dot11AuthenticateFailStatus	read-only	N		N
dot11AuthenticateFailStation	read-only	N		N
dot11AuthenticationAlgorithmsTable	not-accessible	-		-
dot11AuthenticationAlgorithmsEntry	not-	-		-

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxiao@cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

	access ible			
dot11AuthenticationAlgorithmsIndex	not-access ible	Y		N
dot11AuthenticationAlgorithm	read-only	Y		N
dot11AuthenticationAlgorithmsEnabl e	read-write	Y		N
dot11WEPDefaultKeysTable	not-access ible	-		-
dot11WEPDefaultKeysEntry	not-access ible	-		-
dot11WEPDefaultKeyIndex	not-access ible	Y		N
dot11WEPDefaultKeyValue	read-write	Y	OID_802_11_WEPDEFAULTKEYVALUE	Y
dot11WEPKeyMappingsTable	not-access ible	-		-
dot11WEPKeyMappingsEntry	not-access ible	-		-
dot11WEPKeyMappingIndex	not-access ible	N		N
dot11WEPKeyMappingAddress	read-create	N		N
dot11WEPKeyMappingWEPOn	read-create	N		N
dot11WEPKeyMappingValue	read-create	N		N
dot11WEPKeyMappingStatus	read-create	N		N
dot11PrivacyTable	not-access ible	-		
dot11PrivacyEntry	not-access ible	-		
dot11PrivacyInvoked	read-write	Y		N
dot11WEPDefaultKeyID	read-write	Y	OID_802_11_WEPDEFAULTKEYID	Y
dot11WEPKeyMappingLength	read-write	Y	RT_OID_802_11_WEPKEYMAPPINGLENGT H	N
dot11ExcludeUnencrypted	read-write	N		N
dot11WEPICVErrorCount	read-only	N		N
dot11WEPExcludedCount	read-only	N		N
dot11SMTnotification	-	-		
dot11Disassociate	-	N		N
dot11Deauthenticate	-	N		N
dot11AuthenticateFail	-	N		N
dot11mac				
dot11OperationTable	not-access	-		

FOR MEDIATEK CONFIDENTIAL wangxiang@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

	ible			
dot11OperationEntry	not-access ible	-		
dot11MACAddress	read-only	Y	RT_OID_802_11_MAC_ADDRESS	N
dot11RTSThreshold	read-write	Y	OID_802_11_RTS_THRESHOLD	Y
dot11ShortRetryLimit	read-write	Y	OID_802_11_SHORTRETRYLIMIT	N
dot11LongRetryLimit	read-write	Y	OID_802_11_LONGRETRYLIMIT	N
dot11FragmentationThreshold	read-write	Y	OID_802_11_FRAGMENTATION_THRESHOL D	Y
dot11MaxTransmitMSDULifetime	read-write	N		N
dot11MaxReceiveLifetime	read-write	N		N
dot11ManufacturerID	read-only	Y	RT_OID_802_11_MANUFACTUREID	N
dot11ProductID	read-only	Y	RT_OID_802_11_PRODUCTID	N
dot11CountersTable	not-access ible	-		
dot11CountersEntry	not-access ible	-		
dot11TransmittedFragmentCount	read-only	Y	OID_802_11_STATISTICS	N
dot11MulticastTransmittedFrameCo unt	read-only	Y	OID_802_11_STATISTICS	N
dot11FailedCount	read-only	Y	OID_802_11_STATISTICS	N
dot11RetryCount	read-only	Y	OID_802_11_STATISTICS	N
dot11MultipleRetryCount	read-only	Y	OID_802_11_STATISTICS	N
dot11FrameDuplicateCount	read-only	Y	OID_802_11_STATISTICS	N
dot11RTSSuccessCount	read-only	Y	OID_802_11_STATISTICS	N
dot11RTSFailureCount	read-only	Y	OID_802_11_STATISTICS	N
dot11ACKFailureCount	read-only	Y	OID_802_11_STATISTICS	N
dot11ReceivedFragmentCount	read-only	Y	OID_802_11_STATISTICS	N
dot11MulticastReceivedFrameCount	read-only	Y	OID_802_11_STATISTICS	N
dot11FCSErrorCount	read-only	Y	OID_802_11_STATISTICS	N
dot11TransmittedFrameCount	read-only	N		N
dot11WEPUndecryptableCount	read-only	N		N
dot11GroupAddressesTable	not-access ible	-		-
dot11GroupAddressesEntry	not-access ible	-		-

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL FOR wangxiang@cvnchina.com USE ONLY

dot11GroupAddressesIndex	not-accessible	N		N
dot11Address	read-create	N		N
dot11GroupAddressesStatus	read-create	N		N
dot11res				
dot11resAttribute				
dot11ResourceTypeIDName	read-only	-		
dot11ResourceInfoTable	not-accessible	-		
dot11ResourceInfoEntry	not-accessible	-		
dot11manufacturerOUI	read-only	Y	RT_OID_802_11_MANUFACTUREROUI	N
dot11manufacturerName	read-only	Y	RT_OID_802_11_MANUFACTURERNAME	N
dot11manufacturerProductName	read-only	Y	RT_OID_DEVICE_NAME	N
dot11manufacturerProductVersion	read-only	Y	RT_OID_VERSION_INFO	N
dot11phy				
dot11PhyOperationTable	not-accessible	-		
dot11PhyOperationEntry	not-accessible	-		
dot11PHYType	read-only	Y	RT_OID_802_11_PHY_MODE	N
dot11CurrentRegDomain	read-write	Y		Y
dot11TempType	read-only	N		N
dot11PhyAntennaTable	not-accessible	-		
dot11PhyAntennaEntry	not-accessible	-		
dot11CurrentTxAntenna	read-write	Y	OID_802_11_TX_ANTENNA_SELECTED	N
dot11DiversitySupport	read-only	Y	OID_802_11_RX_ANTENNA_SELECTED	N
dot11CurrentRxAntenna	read-write	Y	OID_802_11_RX_ANTENNA_SELECTED	N
dot11PhyTxPowerTable	not-accessible	-		
dot11PhyTxPowerEntry	not-accessible	-		
dot11NumberSupportedPowerLevels	read-only	N		N
dot11TxPowerLevel1	read-only	N		N
dot11TxPowerLevel2	read-only	N		N

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

dot11TxPowerLevel3	read-only	N		N
dot11TxPowerLevel4	read-only	N		N
dot11TxPowerLevel5	read-only	N		N
dot11TxPowerLevel6	read-only	N		N
dot11TxPowerLevel7	read-only	N		N
dot11TxPowerLevel8	read-only	N		N
dot11CurrentTxPowerLevel	read-write	N		N
dot11PhyFHSSTable	not-accessible	-		
dot11PhyFHSSEntry	not-accessible	-		
dot11HopTime	read-only	N		N
dot11CurrentChannelNumber	read-write	N		N
dot11MaxDwellTime	read-only	N		N
dot11CurrentDwellTime	read-write	N		N
dot11CurrentSet	read-write	N		N
dot11CurrentPattern	read-write	N		N
dot11CurrentIndex	read-write	N		N
dot11PhyDSSSTable	not-accessible	-		
dot11PhyDSSSEntry	not-accessible	-		
dot11CurrentChannel	read-write	Y	OID_802_11_CURRENTCHANNEL	Y
dot11CCAModeSupported	read-only	N		N
dot11CurrentCCAMode	read-write	N		N
dot11EDThreshold	read-write	N		N
dot11PhyIRTable	not-accessible	-		
dot11PhyIREntry	not-accessible	-		
dot11CCAWatchdogTimerMax	read-write	N		N
dot11CCAWatchdogCountMax	read-write	N		N
dot11CCAWatchdogTimerMin	read-write	N		N
dot11CCAWatchdogCountMin	read-write	N		N

FOR wangxiang@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

dot11RegDomainsSupportedTable	not-accessible	-		
dot11RegDomainsSupportEntry	not-accessible	-		
dot11RegDomainsSupportIndex	not-accessible	Y		N
dot11RegDomainsSupportValue	read-only	Y		N
dot11AntennasListTable	not-accessible	-		
dot11AntennasListEntry	not-accessible	-		
dot11AntennaListIndex	not-accessible	Y		N
dot11SupportedTxAntenna	read-write	Y	OID_802_11_TX_ANTENNA_SELECTED	N
dot11SupportedRxAntenna	read-write	Y	OID_802_11_RX_ANTENNA_SELECTED	N
dot11DiversitySelectionRx	read-write	Y	OID_802_11_RX_ANTENNA_SELECTED	N
dot11SupportedDataRatesTxTable	not-accessible	-		
dot11SupportedDataRatesTxEntry	not-accessible	-		
dot11SupportedDataRatesTxIndex	not-accessible	Y		N
dot11SupportedDataRatesTxValue	read-only	Y	OID_802_11_DESIRED_RATES	N
dot11SupportedDataRatesRxTable	not-accessible	-		
dot11SupportedDataRatesRxEntry	not-accessible	-		
dot11SupportedDataRatesRxIndex	not-accessible	Y	OID_802_11_DESIRED_RATES	
dot11SupportedDataRatesRxValue	read-only	Y		
dot11PhyOFDMTable	not-accessible	-		
dot11PhyOFDMEntry	not-accessible	-		
dot11CurrentFrequency	read-write	N	OID_802_11_CURRENTCHANNEL	Y
dot11TIThreshold	read-write	N		N
dot11FrequencyBandsSupported	read-only	N		N

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

17.2 RALINK OID for SNMP MIB

RALINK OID for SNMP		
Value	Name	Structure
0x010B	OID_802_11_NUMBER_OF_ANTENNAS	USHORT numant;
0x010C	OID_802_11_RX_ANTENNA_SELECTED	USHORT whichant;
0x010D	OID_802_11_TX_ANTENNA_SELECTED	USHORT whichant;
0x050C	RT_OID_802_11_PHY_MODE	ULONG linfo;
0x050E	OID_802_11_DESIRED_RATES	typedef UCHAR NDIS_802_11_RATES[NDIS_802_11_LENGTH_RATES]; #define NDIS_802_11_LENGTH_RATES 8
0x0514	OID_802_11_RTS_THRESHOLD	ULONGlinfo;
0x0515	OID_802_11_FRAGMENTATION_THRESHOLD	ULONGlinfo;
0x0607	RT_OID_DEVICE_NAME	char name[128];

0x0608	RT_OID_VERSION_INFO	typedef struct PACKED _RT_VERSION_INFO{
		UCHAR DriverVersionW;
		UCHAR DriverVersionX;
		UCHAR DriverVersionY;
		UCHAR DriverVersionZ;
		UINT DriverBuildYear;
		UINT DriverBuildMonth;
		UINT DriverBuildDay;
		} RT_VERSION_INFO, *PRT_VERSION_INFO;

0x060A	OID_802_3_CURRENT_ADDRESS	char addr[128];

0x060E	OID_802_11_STATISTICS	typedef struct _NDIS_802_11_STATISTICS
		{
		ULONG Length; // Length of structure
		ULONG TransmittedFragmentCount;
		ULONG MulticastTransmittedFrameCount;
		ULONG FailedCount;
		ULONG RetryCount;
		ULONG MultipleRetryCount;
		ULONG RTSSuccessCount;
		ULONG RTSFailureCount;
		ULONG ACKFailureCount;
		ULONG FrameDuplicateCount;
		ULONG ReceivedFragmentCount;

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR wangxiang@cvnchina.com USE ONLY

		ULONG MulticastReceivedFrameCount;
		ULONG FCSErrorCount;
		} NDIS_802_11_STATISTICS, PNDIS_802_11_STATISTICS;

0x0700	RT_OID_802_11_MANUFACTURER OUI	char oui[128];
0x0701	RT_OID_802_11_MANUFACTURER NAME	char name[128];
0x0702	RT_OID_802_11_RESOURCETYPEI DNAME	char name[128];
0x0703	RT_OID_802_11_PRIVACYOPTIONI MPLEMENTED	ULONG linfo;
0x0704	RT_OID_802_11_POWERMANAGE MENTMODE	ULONG linfo;

0x0705	OID_802_11_WEPDEFAULTKEYVAL UE	typedef struct _DefaultKeyIdxValue
		{
		UCHARKeyIdx;
		UCHARValue[16];
		}DefaultKeyIdxValue;

0x0706	OID_802_11_WEPDEFAULTKEYID	UCHARkeyid;
0x0707	RT_OID_802_11_WEPKEYMAPPIN GLENGTH	UCHAR len;
0x0708	OID_802_11_SHORTRETRYLIMIT	ULONGlinfo;
0x0709	OID_802_11_LONGRETRYLIMIT	ULONGlinfo;
0x0710	RT_OID_802_11_PRODUCTID	char id[128];
0x0711	RT_OID_802_11_MANUFACTUREID	char id[128];
0x0712	OID_802_11_CURRENTCHANNEL	UCHAR channel
0x0713	RT_OID_802_11_MAC_ADDRESS	char macaddress[128]

MEDIATEK CONFIDENTIAL
FOR wangxian@wnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

18 IOCTL I/O Control Interface

18.1 Parameters for iwconfig's IOCTL

Access	Description	ID	Parameters
Get	BSSID, MAC Address	SIOCGIFHWADDR	wrq->u.name, (length = 6)
	WLAN Name	SIOCGIWNAME	wrq->u.name = "RT2800 SoftAP", length = strlen(wrq->u.name)

	SSID	SIOCGIWESSID	struct iw_point *erq = &wrq->u.essid;
			erq->flags=1;
			erq->length = pAd->PortCfg.MBSSID[pAd->IoctlIF].SsidLen;
			if(erq->pointer)
			{
			  if(copy_to_user(erq->pointer,
			            pAd->PortCfg.MBSSID[pAd->IoctlIF].Ssid,
			            erq->length))
			  {
			    Status = -EFAULT;
			    break;
			  }
			}

	Channel / Frequency (Hz)	SIOCGIWFREQ	wrq->u.freq.m = pAd->PortCfg.Channel;
			wrq->u.freq.e = 0;
			wrq->u.freq.i = 0;

	Bit Rate (bps)	SIOCGIWRATE	wrq->u.bitrate.value =
			     RateIdTo500Kbps[pAd->PortCfg.MBSSID[pAd->IoctlIF].TxRate] * 500000;
			wrq->u.bitrate.disabled = 0;

	AP's MAC address	SIOCGIWAP	wrq->u.ap_addr.sa_family = ARPHRD_ETHER;
			memcpy(wrq->u.ap_addr.
			        sa_data,
			        &pAd->PortCfg.MBSSID[pAd->IoctlIF].Bssid, ETH_ALEN);

	Operation Mode	SIOCGIWMODE	wrq->u.mode = IW_MODE_INFRA;

	Range of Parameters	SIOCGIWRANGE	range.we_version_compiled = WIRELESS_EXT;
			range.we_version_source = 14;

	Scanning Results	SIOCGIWSCAN	typedef struct _NDIS_802_11_SITE_SURVEY_TABLE
			{
			   LONG Channel;
			   LONG Rssi;
			   UCHAR Ssid[33];
			   UCHAR Bssid[18];
			   UCHAR EncrypT[8];
			} NDIS_802_11_SITE_SURVEY_TABLE, *PNDIS_802_11_SITE_SURVEY_TABLE;
			
			wrq->u.data.length = N* sizeof(NDIS_802_11_SITE_SURVEY_TABLE);
			copy_to_user(wrq->u.data.pointer, site_survey_table, wrq->u.data.length);

	Client	SIOCGIWAPLIST	typedef struct _NDIS_802_11_STATION_TABLE

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

MEDIATEK CONFIDENTIAL
FOR wangxian@cvrchina.com USE ONLY

	Association List		{
			  UCHAR MacAddr[18];
			  ULONG Aid;
			  ULONG PsMode;
			  ULONG LastDataPacketTime;
			  ULONG RxByteCount;
			  ULONG TxByteCount;
			  ULONG CurrTxRate;
			  ULONG LastTxRate;
			} NDIS_802_11_STATION_TABLE, *PNDIS_802_11_STATION_TABLE;
			
			wrq->u.data.length = i * sizeof(NDIS_802_11_STATION_TABLE);
			copy_to_user(wrq->u.data.pointer, sta_list_table, wrq->u.data.length);

Set	Trigger Scanning	SIOCSIWSCAN	ApSiteSurvey(pAd);

18.2 Parameters for iwpriv's IOCTL

Please refer section 4 and 5 to have iwpriv parameters and values.
Parameters:

```
int      socket_id;
char     name[25];                         // interface name
char     data[255];                        // command string
struct   iwreq wrq;
```

Default setting:

```
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;
```

18.2.1 Iwpriv Set DATA

THESE PARAMETERS ARE THE SAME AS IWPRIV

Command and IOCTL Function		
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);

18.2.2 Iwpriv Get DATA

THESE PARAMETERS ARE THE SAME AS IWPRIV

Command and IOCTL Function

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wangxian@cvtchina.com USE ONLY MEDIATEK CONFIDENTIAL

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_GET_MAC_TABLE	Iwpriv ra0 get_mac_table	sprintf(name, "ra0");
		strcpy(data, "get_mac_table”);
		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_GET_MAC_TABLE, &wrq);

RTPRIV_IOCTL_SHOW	Iwpriv ra0 show	sprintf(name, "ra0");
		strcpy(data, "get_mac_table”);
		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);

RTPRIV_IOCTL_WSC_PROFILE	Iwpriv ra0 get_wsc_profile	sprintf(name, "ra0");
		strcpy(data, "get_mac_table”);
		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_WSC_PROFILE, &wrq);

RTPRIV_IOCTL_QUERY_BATABLE	Iwpriv ra0 get_ba_table	sprintf(name, "ra0");
		strcpy(data, "get_mac_table”);
		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_QUERY_BATABLE, &wrq);

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

18.2.3 Iwpriv Set Data: BBP, MAC and EEPROM

Command and IOCTL Function		
Set Data: BBP, MAC and EEPROM, Parameters is Same as iwpriv		
Type	Command	IOCTL

RTPRIV_IOCTL_BBP
(Set BBP Register Value)
	Iwpriv ra0 bbp 17=32	sprintf(name, "ra0");
		strcpy(data, " bbp 17=32");
		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_BBP, &wrq);

RTPRIV_IOCTL_MAC
(Set MAC Register Value)
	Iwpriv ra0 mac 3000=12345678	sprintf(name, "ra0");
		strcpy(data, " mac 3000=12345678");
		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_MAC, &wrq);

RTPRIV_IOCTL_E2P
(Set EEPROM Value)
	Iwpriv ra0 e2p 40=1234	sprintf(name, "ra0");
		strcpy(data, " e2p 40=1234");
		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_E2P, &wrq);

18.2.4 Iwpriv Get Data: BBP, MAC and EEPROM

Command and IOCTL Function		
Get Data: BBP, MAC and EEPROM , Parameters is Same as iwpriv		
Type	Command	IOCTL

RTPRIV_IOCTL_BBP
(Get BBP Register Value)
	Iwpriv ra0 bbp 17	sprintf(name, "ra0");
		strcpy(data, " bbp 17");
		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_BBP, &wrq);

RTPRIV_IOCTL_MAC
(Get MAC Register Value)
	Iwpriv ra0 mac 3000	sprintf(name, "ra0");
		strcpy(data, " mac 3000");
		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_MAC, &wrq);

RTPRIV_IOCTL_E2P	Iwpriv ra0 e2p 40	sprintf(name, "ra0");

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wangxian@cvnchina.com USE ONLY MEDIATEK CONFIDENTIAL

(Get EEPROM Value)		strcpy(data, " e2p 40"); 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_E2P, &wrq);

18.2.5 Iwpriv Set Raw Data

IOCTL Function	
Set Raw Data by I/O Control Interface	
Function Type	IOCTL

RTPRIV_IOCTL_RADIUS_DATA	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0x55, 100);
	wrq.u.data.length = 100;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = 0;
	ioctl(socket_id, RTPRIV_IOCTL_RADIUS_DATA, &wrq);

RTPRIV_IOCTL_ADD_WPA_KEY	NDIS_802_11_KEY *vp;
	
	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, sizeof(NDIS_802_11_KEY));
	vp = (NDIS_802_11_KEY *)&data;
	vp->Length = sizeof(NDIS_802_11_KEY);
	memset(vp->addr, 0x11, 6);
	vp->KeyIndex = 2;
	vp->KeyLength = 32;
	memset(vp->KeyMaterial, 0xAA, 32);
	wrq.u.data.length = sizeof(NDIS_802_11_KEY);
	wrq.u.data.pointer = data;
	wrq.u.data.flags = 0;
	ioctl(socket_id, RTPRIV_IOCTL_ADD_WPA_KEY, &wrq);

RTPRIV_IOCTL_ADD_PMKID_CACHE	NDIS_802_11_KEY *vp;
	
	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, sizeof(NDIS_802_11_KEY));
	vp = (NDIS_802_11_KEY *)&data;
	vp->Length = sizeof(NDIS_802_11_KEY);
	memset(vp->addr, 0x11, 6);
	vp->KeyIndex = 2;
	vp->KeyLength = 32;
	memset(vp->KeyMaterial, 0xBB, 32);
	wrq.u.data.length = sizeof(NDIS_802_11_KEY);
	wrq.u.data.pointer = data;
	wrq.u.data.flags = 0;
	ioctl(socket_id, RTPRIV_IOCTL_ADD_PMKID_CACHE, &wrq);

MEDIATEK CONFIDENTIAL FOR wangxian@cynthina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

18.2.6 Set Raw Data with Flags

IOCTL Function	
Set Raw Data by I/O Control Interface with Flags	
Function Type	IOCTL

RT_SET_APD_PID	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, 4);
	data[0] = 12;
	wrq.u.data.length = 4;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_SET_APD_PID;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_SET_DEL_MAC_ENTRY	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0xdd, 6);
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = 6;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_SET_DEL_MAC_ENTRY;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_OID_WSC_SET_SELECTED_REGISTRAR	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, decodeStr, decodeLen);
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = decodeLen;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_OID_WSC_SET_SELECTED_REGISTRAR;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_OID_WSC_EAPMSG	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, wscU2KMsg, wscU2KMsgLen);
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = wscU2KMsgLen;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_OID_WSC_EAPMSG;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

18.2.7 Get Raw Data with Flags

IOCTL Function	
Get Raw Data by I/O Control Interface with Flags	
Function Type	IOCTL

RT_QUERY_ATE_TXDONE_COUNT	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, sizeof(ULONG));
	wrq.u.data.length = sizeof(ULONG);
	wrq.u.data.pointer = data;

MEDIATEK CONFIDENTIAL FOR wangxian@cvtchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

	wrq.u.data.flags = RT_QUERY_ATE_TXDONE_COUNT;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_QUERY_SIGNAL_CONTEXT	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, sizeof(RT_SIGNAL_STRUC));
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = sizeof(RT_SIGNAL_STRUC);
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_QUERY_SIGNAL_CONTEXT;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_OID_WSC_QUERY_STATUS	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, sizeof(INT));
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = sizeof(INT);
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_OID_WSC_QUERY_STATUS;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_OID_WSC_PIN_CODE	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, sizeof(ULONG));
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = sizeof(ULONG);
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_OID_WSC_PIN_CODE;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_OID_WSC_UUID	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, sizeof(UCHAR));
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = sizeof(UCHAR);
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_OID_WSC_UUID;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_OID_WSC_MAC_ADDRESS	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, MAC_ADDR_LEN);
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = MAC_ADDR_LEN;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_OID_WSC_MAC_ADDRESS;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_OID_GET_PHY_MODE	sprintf(name, "ra0");
	strcpy(wrq.ifr_name, name);
	memset(data, 0, sizeof(ULONG));
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = sizeof(ULONG);
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_OID_GET_PHY_MODE;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

RT_OID_GET_LLTD_ASSO_TANLE	sprintf(name, "ra0");

FOR wangxian@cyinchina.com USE ONLY MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

	strcpy(wrq.ifr_name, name);
	memset(data, 0, sizeof(RT_LLTD_ASSOICATION_TABLE));
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = sizeof(RT_LLTD_ASSOICATION_TABLE);
	wrq.u.data.pointer = data;
	wrq.u.data.flags = RT_OID_GET_LLTD_ASSO_TANLE;
	ioctl(socket_id, RT_PRIV_IOCTL, &wrq);

18.3 Sample user space Applications

```
//==========================================================================
//
// rtuser:
//          1. User space application to demo how to use IOCTL function.
//          2. Most of the IOCTL function is defined as "CHAR" type and return with string message.
//          3. Use sscanf to get the raw data back from string message.
//          4. The command format "parameter=value" is same as iwpriv command format.
//          5. Remember to insert driver module and bring interface up prior execute rtuser.
//                  change folder path to driver "Module"
//                  dos2unix *                  ; in case the files are modified from other OS environment
//                  chmod 644 *
//                  chmod 755 Configure
//                  make config
//                  make
//                  insmod RT2800ap.o
//                  ifconfig ra0 up
//
// Refer Linux/if.h to have
//                  #define ifr_name    ifr_ifrn.ifrn_name              /* interface name    */
//
// 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>                         /* for close */
#include <Linux/wireless.h>

//==================================================================================

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

//
//SET/GET CONVENTION :
// * ------------------
// * Simplistic summary :
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxian@cvnchina.com

```
// *         o even numbered ioctls are SET, restricted to root, and should not
// *     return arguments (get_args = 0).
// *         o odd numbered ioctls are GET, authorised to anybody, and should
// *     not expect any arguments (set_args = 0).
//
#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)


#define OID_GET_SET_TOGGLE                                   0x8000

#define RT_QUERY_ATE_TXDONE_COUNT                            0x0401
#define RT_QUERY_SIGNAL_CONTEXT                              0x0402
#define RT_SET_APD_PID                                       (OID_GET_SET_TOGGLE + 0x0405)
#define RT_SET_DEL_MAC_ENTRY                                 (OID_GET_SET_TOGGLE + 0x0406)

//---------------------------------------------------------

#ifndef    TRUE
#define    TRUE                1
#endif

#ifndef    FALSE
#define    FALSE    0
#endif

#define MAC_ADDR_LEN                                         6
#define ETH_LENGTH_OF_ADDRESS                                6
#define MAX_LEN_OF_MAC_TABLE                                 64

//---------------------------------------------------------

typedef struct _COUNTERS
{
        unsigned long       TxSuccessTotal;;
        unsigned long       TxSuccessWithRetry;
        unsigned long       TxFailWithRetry;
        unsigned long       RtsSuccess;
        unsigned long       RtsFail;
        unsigned long       RxSuccess;
        unsigned long       RxWithCRC;
        unsigned long       RxDropNoBuffer;
        unsigned long       RxDuplicateFrame;
        unsigned long       FalseCCA;
        unsigned long       RssiA;
        unsigned long       RssiB;
}       COUNTERS;
```

PS. User can check with "iwpriv ra0 stat" to make sure the TXRX status is correct when porting the ATE related test program.

```
//---------------------------------------------------------
```

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangjian@ cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

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

//---------------------------------------------------------

typedef union  _MACHTTRANSMIT_SETTING {
           struct      {
           unsigned short             MCS:7;            // MCS
           unsigned short             BW:1;                         //channel bandwidth 20MHz or 40 MHz
           unsigned short             ShortGI:1;
           unsigned short             STBC:2;           //SPACE
           unsigned short             rsv:3;
           unsigned short             MODE:2;           // Use definition MODE_xxx.
           }           field;
           unsigned short             word;
 } MACHTTRANSMIT_SETTING, *PMACHTTRANSMIT_SETTING;

typedef struct _RT_802_11_MAC_ENTRY {
   unsigned char                      Addr[6];
   unsigned char                      Aid;
   unsigned char                      Psm;                          // 0:PWR_ACTIVE, 1:PWR_SAVE
   unsigned char                      MimoPs;           // 0:MMPS_STATIC, 1:MMPS_DYNAMIC, 3:MMPS_Enabled
   MACHTTRANSMIT_SETTING              TxRate;
} RT_802_11_MAC_ENTRY, *PRT_802_11_MAC_ENTRY;

typedef struct _RT_802_11_MAC_TABLE {
   unsigned long                      Num;
   RT_802_11_MAC_ENTRY Entry[MAX_LEN_OF_MAC_TABLE];
} RT_802_11_MAC_TABLE, *PRT_802_11_MAC_TABLE;

// Key mapping keys require a BSSID
typedef struct _NDIS_802_11_KEY
{
           unsigned long              Length;       // Length of this structure
           unsigned char              addr[6];
           unsigned long              KeyIndex;
           unsigned long              KeyLength;       // length of key in bytes
           unsigned char              KeyMaterial[32];  // variable length depending on above field
} NDIS_802_11_KEY, *PNDIS_802_11_KEY;

typedef struct _RT_SIGNAL_STRUC {
           unsigned short             Sequence;
           unsigned char              MacAddr[MAC_ADDR_LEN];
           unsigned char              CurrAPAddr[MAC_ADDR_LEN];
           unsigned char              Sig;
} RT_SIGNAL_STRUC, *PRT_SIGNAL_STRUC;

//---------------------------------------------------------

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

//=========================================================================
```

MEDIATEK CONFIDENTIAL
FOR wangxiao@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

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

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

        // set interface name as "ra0" -------------------------------------------
        sprintf(name, "ra0");
        memset(data, 0x00, 255);
//
//example of iwconfig ioctl function ==========================================
//
        // get wireless name ----------------------------------------------------
        strcpy(wrq.ifr_name, name);
        wrq.u.data.length = 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.name);
//
//example of iwpriv ioctl function ============================================
//
        //WPAPSK, remove "set" string --------------------------------------------
        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;
        }
        //set e2p, remove "e2p" string -------------------------------------------
        memset(data, 0x00, 255);
        strcpy(data, "80=1234");
        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_E2P, &wrq);
        if(ret != 0)
```

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
{
        printf("\nrtuser::error::set eeprom\n\n");
        goto rtuser_exit;
}

//printf("\n%s\n", wrq.u.data.pointer);
{
        int addr, value, p1;

        // string format: "\n[0x%02X]:0x%04X  " ==> "[0x20]:0x0C02"
        sscanf(wrq.u.data.pointer, "\n[%dx%02X]:%04X  ", &p1, &addr, &value);
        printf("\nSet EEP[0x%02X]:0x%04X\n", addr, value);
}
```

//get e2p, remove "e2p" string --

```
memset(data, 0x00, 255);
strcpy(data, "80");
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_E2P, &wrq);
if(ret != 0)
{
        printf("\nrtuser::error::get eeprom\n\n");
        goto rtuser_exit;
}

//printf("\n%s\n", wrq.u.data.pointer);
{
        int addr, value, p1, p2;

        // string format: "\n[0x%02X]:0x%04X  " ==> "[0x20]:0x0C02"
        sscanf(wrq.u.data.pointer, "\n[%dx%04X]:%dx%X  ", &p1, &addr, &p2, &value);
        printf("\nGet EEP[0x%02X]:0x%04X\n", addr, value);
}
```

//set mac, remove "mac" string --

```
memset(data, 0x00, 255);
strcpy(data, "2b4f=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_MAC, &wrq);
if(ret != 0)
{
        printf("\nrtuser::error::set mac register\n\n");
        goto rtuser_exit;
}

//printf("\n%s\n", wrq.u.data.pointer);
{
        int addr, value, p1;

        // string format: "\n[0x%02X]:0x%04X  " ==> "[0x20]:0x0C02"
        sscanf(wrq.u.data.pointer, "\n[%dx%08X]:%08X  ", &p1, &addr, &value);
        printf("\nSet MAC[0x%08X]:0x%08X\n", addr, value);
}
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvmchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
//get mac, remove "mac" string --------------------------------------------
memset(data, 0x00, 255);
strcpy(data, "2b4f");
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_MAC, &wrq);
if(ret != 0)
{
        printf("\nrtuser::error::get mac register\n\n");
        goto rtuser_exit;
}

//printf("\n%s\n", wrq.u.data.pointer);
{
        int addr, value, p1;

        // string format: "\n[0x%02X]:0x%04X  " ==> "[0x20]:0x0C02"
        sscanf(wrq.u.data.pointer, "\n[%dx%08X]:%08X  ", &p1, &addr, &value);
        printf("\nGet MAC[0x%08X]:0x%08X\n", addr, value);
}

//set bbp, remove "bbp" string --------------------------------------------
memset(data, 0x00, 255);
strcpy(data, "17=32");
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_BBP, &wrq);
if(ret != 0)
{
        printf("\nrtuser::error::set bbp register\n\n");
        goto rtuser_exit;
}

//printf("\n%s\n", wrq.u.data.pointer);
{
        int id, addr, value, p1;

        // string format: "\n[0x%02X]:0x%04X  " ==> "[0x20]:0x0C02"
        sscanf(wrq.u.data.pointer, "\nR%02d[%dx%02X]:%02X\n", &id, &p1, &addr, &value);
        printf("\nSet BBP R%02d[0x%02X]:0x%02X\n", id, addr, value);
}

//get bbp, remove "bbp" string --------------------------------------------
memset(data, 0x00, 255);
strcpy(data, "17");
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_BBP, &wrq);
if(ret != 0)
{
        printf("\nrtuser::error::get bbp register\n\n");
        goto rtuser_exit;
}
```

MEDIATEK CONFIDENTIAL
FOR wangxia@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
	//printf("\n%s\n", wrq.u.data.pointer);
	{
		int id, addr, value, p1;

		// string format: "\n[0x%02X]:0x%04X  " ==> "[0x20]:0x0C02"
		sscanf(wrq.u.data.pointer, "\nR%02d[%dx%02X]:%02X  ", &id, &p1, &addr, &value);
		printf("\nGet BBP R%02d[0x%02X]:0x%02X\n", id, addr, value);
	}
```

//get statistics, remove "stat" string -----------------------------------

```
	memset(data, 0x00, 2048);
	strcpy(data, "");
	strcpy(wrq.ifr_name, name);
	wrq.u.data.length = 0;
	wrq.u.data.pointer = data;
	wrq.u.data.flags = 0;
	ret = ioctl(socket_id, RTPRIV_IOCTL_STATISTICS, &wrq);
	if(ret != 0)
	{
		printf("\nrtuser::error::get statistics\n\n");
		goto rtuser_exit;
	}

	printf("\n========= Get AP Statistics ==========\n");
	{
		int i;
		char *sp = wrq.u.data.pointer;
		unsigned long *cp = (unsigned long *)&counter;

		for (i = 0 ; i < 13 ; i++)
		{
			sp = strstr(sp, "= ");
			sp = sp+2;
			sscanf(sp, "%ul", (unsigned int *)&cp[i]);
		}
	  printf("Tx success					= %u\n", (unsigned int)counter.TxSuccessTotal);
	  printf("Tx success without retry			= %u\n", (unsigned int)

	counter.TxSuccessWithoutRetry);
	  printf("Tx success after retry		= %u\n", (unsigned int)counter.TxSuccessWithRetry);
	  printf("Tx fail to Rcv ACK after retry	= %u\n", (unsigned int)counter.TxFailWithRetry);
	  printf("RTS Success Rcv CTS				= %u\n", (unsigned int)counter.RtsSuccess);
	  printf("RTS Fail Rcv CTS			= %u\n", (unsigned int)counter.RtsFail);
	  printf("Rx success					= %u\n", (unsigned int)counter.RxSuccess);
	  printf("Rx with CRC					= %u\n", (unsigned int)counter.RxWithCRC);
	  printf("Rx drop due to out of resource= %u\n", (unsigned int)counter.RxDropNoBuffer);
	  printf("Rx duplicate frame			= %u\n", (unsigned int)counter.RxDuplicateFrame);
	  printf("False CCA (one second)			= %u\n", (unsigned int)counter.FalseCCA);
	  printf("RSSI-A					= %d\n", (  signed int)counter.RssiA);
	  printf("RSSI-B (if available)		= %d\n", (  signed int)counter.RssiB);
	}

#if 0
	//set AP to do site survey, remove "set" string --------------------------
	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;
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
MEDIATEK CONFIDENTIAL FOR yangjian@ cvnchina.com USE ONLY

```
        ret = ioctl(socket_id, RTPRIV_IOCTL_SET, &wrq);
#endif

        //get AP's site survey, remove "get_site_survey" string -------------------
        memset(data, 0x00, 2048);
        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%s\n", wrq.u.data.pointer);
        printf("\n========== Get Site Survey AP List ==========");
        if(wrq.u.data.length > 0)
        {
                int        i, apCount;
                char *sp, *op;
                int        len = wrq.u.data.length;

                op = sp = wrq.u.data.pointer;
                sp = sp+1+8+8+35+19+8+1;
                i = 0;
                // santy check
                //         1. valid char data
                //         2. rest length is larger than per line length ==> (1+8+8+35+19+8+1)
                while(*sp && ((len - (sp-op)) > (1+8+8+35+19+8)))
                {
                        //if(*sp++ == '\n')
                        //         continue;
                        //printf("\n\nAP Count: %d\n", i);

                        sscanf(sp, "%d", (int *)&SiteSurvey[i].channel);
                        //printf("channel: %d\n", SiteSurvey[i].channel);

                        sp = strstr(sp, "-");
                        sscanf(sp, "-%d", (int *)&SiteSurvey[i].rssi);
                        //printf("rssi: -%d\n", SiteSurvey[i].rssi);

                        sp = sp+8;
                        strncpy((char *)&SiteSurvey[i].ssid, sp, 32);
                        SiteSurvey[i].ssid[32] = '\0';
                        //printf("ssid: %s\n", SiteSurvey[i].ssid);

                        sp = sp+35;
                        sscanf(sp, "%02x:%02x:%02x:%02x:%02x:%02x",
                                        (int *)&SiteSurvey[i].bssid[0], (int *)&SiteSurvey[i].bssid[1],
                                        (int *)&SiteSurvey[i].bssid[2], (int *)&SiteSurvey[i].bssid[3],
                                        (int *)&SiteSurvey[i].bssid[4], (int *)&SiteSurvey[i].bssid[5]);
                        //printf("bssid: %02x:%02x:%02x:%02x:%02x:%02x\n",
                        //              SiteSurvey[i].bssid[0], SiteSurvey[i].bssid[1],
                        //              SiteSurvey[i].bssid[2], SiteSurvey[i].bssid[3],
                        //              SiteSurvey[i].bssid[4], SiteSurvey[i].bssid[5]);

                        sp = sp+19;
```

MEDIATEK CONFIDENTIAL
FOR wangjian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
                strncpy((char *)&SiteSurvey[i].security, sp, 8);
                SiteSurvey[i].security[8] = '\0';
                //printf("security: %s\n", SiteSurvey[i].security);

                sp = sp+8+1;
                i = i+1;
        }

        apCount = i;
        printf("\n%-4s%-8s%-8s%-35s%-20s%-8s\n",
                "AP", "Channel", "RSSI", "SSID", "BSSID", "Security");
        for(i = 0 ; i < apCount ; i++)
        {//4+8+8+35+20+8
                printf("%-4d", i+1);
                printf("%-8d", SiteSurvey[i].channel);
                printf("-%-7d", SiteSurvey[i].rssi);
                printf("%-35s", SiteSurvey[i].ssid);
                printf("%02X:%02X:%02X:%02X:%02X:%02X   ",
                                SiteSurvey[i].bssid[0], SiteSurvey[i].bssid[1],
                                SiteSurvey[i].bssid[2], SiteSurvey[i].bssid[3],
                                SiteSurvey[i].bssid[4], SiteSurvey[i].bssid[5]);
                printf("%-8s\n", SiteSurvey[i].security);
        }
}

//get AP's mac table, remove "get_mac_table" string -----------------------
memset(data, 0x00, 2048);
strcpy(data, "");
strcpy(wrq.ifr_name, name);
wrq.u.data.length = 2048;
wrq.u.data.pointer = data;
wrq.u.data.flags = 0;
ret = ioctl(socket_id, RTPRIV_IOCTL_GET_MAC_TABLE, &wrq);
if(ret != 0)
{
        printf("\nrtuser::error::get mac table\n\n");
        goto rtuser_exit;
}

printf("\n========== Get Associated MAC Table ==========");
{
        RT_802_11_MAC_TABLE             *mp;
        int                     i;

        mp = (RT_802_11_MAC_TABLE *)wrq.u.data.pointer;
        printf("\n%-4s%-20s%-4s%-10s%-10s%-10s\n",
                "AID", "MAC_Address", "PSM", "LastTime", "RxByte", "TxByte");

        for(i = 0 ; i < mp->Num ; i++)
        {
                printf("%-4d", mp->Entry[i].Aid);
                printf("%02X:%02X:%02X:%02X:%02X:%02X   ",
                                mp->Entry[i].Addr[0], mp->Entry[i].Addr[1],
                                mp->Entry[i].Addr[2], mp->Entry[i].Addr[3],
                                mp->Entry[i].Addr[4], mp->Entry[i].Addr[5]);
                printf("%-4d", mp->Entry[i].Psm);
                printf("%-10u", (unsigned int)mp->Entry[i].HSCounter.LastDataPacketTime);
                printf("%-10u", (unsigned int)mp->Entry[i].HSCounter.TotalRxByteCount);
                printf("%-10u", (unsigned int)mp->Entry[i].HSCounter.TotalTxByteCount);
                printf("\n");
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
                }
                printf("\n");
        }

//set: raw data
//      RTPRIV_IOCTL_RADIUS_DATA
//      RTPRIV_IOCTL_ADD_WPA_KEY
//      RTPRIV_IOCTL_ADD_PMKID_CACHE

        //set RADIUS Data --------------------------------------------------------
        printf("\nrtuser::set radius data\n\n");
        memset(data, 0x55, 100);
        strcpy(wrq.ifr_name, name);
        wrq.u.data.length = 100;
        wrq.u.data.pointer = data;
        wrq.u.data.flags = 0;
        ret = ioctl(socket_id, RTPRIV_IOCTL_RADIUS_DATA, &wrq);
        if(ret != 0)
        {
                printf("\nrtuser::error::set radius data\n\n");
                goto rtuser_exit;
        }

        //add WPA Key -------------------------------------------------------------
        printf("\nrtuser::add wpa key\n\n");
        {
                NDIS_802_11_KEY         *vp;

                memset(data, 0, sizeof(NDIS_802_11_KEY));
                vp = (NDIS_802_11_KEY *)&data;

                vp->Length = sizeof(NDIS_802_11_KEY);
                memset(vp->addr, 0x11, 6);
                vp->KeyIndex = 2;
                vp->KeyLength = 32;
                memset(vp->KeyMaterial, 0xAA, 32);

                strcpy(wrq.ifr_name, name);
                wrq.u.data.length = sizeof(NDIS_802_11_KEY);
                wrq.u.data.pointer = data;
                wrq.u.data.flags = 0;
                ret = ioctl(socket_id, RTPRIV_IOCTL_ADD_WPA_KEY, &wrq);
                if(ret != 0)
                {
                        printf("\nrtuser::error::add wpa key\n\n");
                        goto rtuser_exit;
                }
        }

        //add PMKID_CACHE --------------------------------------------------------
        printf("\nrtuser::add PMKID_CACHE\n\n");
        {
                NDIS_802_11_KEY         *vp;

                memset(data, 0, sizeof(NDIS_802_11_KEY));
                vp = (NDIS_802_11_KEY *)&data;

                vp->Length = sizeof(NDIS_802_11_KEY);
                memset(vp->addr, 0x11, 6);
                vp->KeyIndex = 2;
```

MEDIATEK CONFIDENTIAL
FOR wangxran@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
                        vp->KeyLength = 32;
                        memset(vp->KeyMaterial, 0xBB, 32);

                        strcpy(wrq.ifr_name, name);
                        wrq.u.data.length = sizeof(NDIS_802_11_KEY);
                        wrq.u.data.pointer = data;
                        wrq.u.data.flags = 0;
                        ret = ioctl(socket_id, RTPRIV_IOCTL_ADD_PMKID_CACHE, &wrq);
                        if(ret != 0)
                        {
                                printf("\nrtuser::error::add PMKID_CACHE\n\n");
                                goto rtuser_exit;
                        }
                }

        //set: raw data
        //      RT_SET_APD_PID
        //      RT_SET_DEL_MAC_ENTRY

                //set APD_PID -----------------------------------------------------------
                printf("\nrtuser::set APD_PID\n\n");
                memset(data, 0, 4);
                data[0] = 12;
                strcpy(wrq.ifr_name, name);
                wrq.u.data.length = 4;
                wrq.u.data.pointer = data;
                wrq.u.data.flags = RT_SET_APD_PID;
                ret = ioctl(socket_id, RT_PRIV_IOCTL, &wrq);
                if(ret != 0)
                {
                        printf("\nrtuser::error::set APD_PID\n\n");
                        goto rtuser_exit;
                }

                //set DEL_MAC_ENTRY ----------------------------------------------------
                printf("\nrtuser::set DEL_MAC_ENTRY\n\n");
                memset(data, 0xdd, 6);
                strcpy(wrq.ifr_name, name);
                wrq.u.data.length = 6;
                wrq.u.data.pointer = data;
                wrq.u.data.flags = RT_SET_DEL_MAC_ENTRY;
                ret = ioctl(socket_id, RT_PRIV_IOCTL, &wrq);
                if(ret != 0)
                {
                        printf("\nrtuser::error::set DEL_MAC_ENTRY\n\n");
                        goto rtuser_exit;
                }

        //get: raw data
        //      RT_QUERY_ATE_TXDONE_COUNT
        //      RT_QUERY_SIGNAL_CONTEXT

                //get ATE_TXDONE_COUNT ---------------------------------------------------
                printf("\nrtuser::get ATE_TXDONE_COUNT\n\n");
                memset(data, 0, 4);
                strcpy(wrq.ifr_name, name);
                wrq.u.data.length = 4;
                wrq.u.data.pointer = data;
                wrq.u.data.flags = RT_QUERY_ATE_TXDONE_COUNT;
                ret = ioctl(socket_id, RT_PRIV_IOCTL, &wrq);
```

MEDIATEK CONFIDENTIAL
FOR wangxiao@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
        if(ret != 0)
        {
                printf("\nrtuser::error::get ATE_TXDONE_COUNT\n\n");
                goto rtuser_exit;
        }
        printf("\nATE_TXDONE_COUNT:: %08lx\n\n", (unsigned long)*wrq.u.data.pointer);

        //get SIGNAL_CONTEXT -----------------------------------------------------
        printf("\nrtuser::get SIGNAL_CONTEXT\n\n");
        {
                RT_SIGNAL_STRUC                 *sp;

                memset(data, 0, sizeof(RT_SIGNAL_STRUC));
                strcpy(wrq.ifr_name, name);
                wrq.u.data.length = sizeof(RT_SIGNAL_STRUC);
                wrq.u.data.pointer = data;
                wrq.u.data.flags = RT_QUERY_SIGNAL_CONTEXT;
                ret = ioctl(socket_id, RT_PRIV_IOCTL, &wrq);
                if(ret != 0)
                {
                        printf("\nrtuser::error::get SIGNAL_CONTEXT\n\n");
                        goto rtuser_exit;
                }
                sp = (RT_SIGNAL_STRUC *)wrq.u.data.pointer;
                printf("\n===== SIGNAL_CONTEXT =====\n\n");
                printf("Sequence    = 0x%04x\n", sp->Sequence);
                printf("Mac.Addr    = %02x:%02x:%02x:%02x:%02x:%02x\n",
                                        sp->MacAddr[0], sp->MacAddr[1],
                                        sp->MacAddr[2], sp->MacAddr[3],
                                        sp->MacAddr[4], sp->MacAddr[5]);
                printf("CurrAP.Addr = %02x:%02x:%02x:%02x:%02x:%02x\n",
                                        sp->CurrAPAddr[0], sp->CurrAPAddr[1],
                                        sp->CurrAPAddr[2], sp->CurrAPAddr[3],
                                        sp->CurrAPAddr[4], sp->CurrAPAddr[5]);
                printf("Sig         = %d\n\n", sp->Sig);
        }

        //SSID, remove "set" string ----------------------------------------------
        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;
}
```

MEDIATEK CONFIDENTIAL
FOR wangxian@cvte.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

19 SingleSKU Example file (New feature for MT76XX)

19.1 2.4GHz example SingleSKU.dat

```
# Single SKU Max Power Table
# |CCK 1~11 | |   OFDM 6 ~ 54     | |          HT20 MCS 0 ~ 15              | |          HT40 MCS 0 ~ 15              |
ch1 23 23 23 23 21 21 21 21 21 21 20 20 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16
ch2 23 23 23 23 22 22 22 22 22 22 20 20 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch3 23 23 23 23 22 22 22 22 22 22 20 20 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch4 23 23 23 23 22 22 22 22 22 22 20 20 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch5 23 23 23 23 22 22 22 22 22 22 20 20 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch6 23 23 23 23 22 22 22 22 22 22 20 20 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch7 23 23 23 23 22 22 22 22 22 22 20 20 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch8 23 23 23 23 22 22 22 22 22 22 20 20 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch9 23 23 23 23 22 22 22 22 22 22 20 20 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch10 23 23 23 23 22 22 22 22 22 22 20 20 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch11 23 23 23 23 19 19 19 19 19 19 19 19 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch12 23 23 23 23 19 19 19 19 19 19 19 19 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch13 23 23 23 23 19 19 19 19 19 19 19 19 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17 17
ch14 23 23 23 23
```

Note: default SingleSKU profile path in driver is defined “/etc_ro/Wireless/RT2860AP/SingleSKU.dat”

For the detailed usage of SingleSKU in profile support, please refer to the MTK_SingleSKU_InProfile_User_manual.pdf and contact with MTK support windows.

19.2 5GHz example SingleSKU.dat

```
# Single SKU Max Power Table
#   OFDM 6 ~ 54            | |                   HT20 MCS 0 ~ 15                   | |                HT40 MCS 0 ~ 15                   | |             VHT80
MCS 0 ~ 9           |
ch36 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
13 13 13 13 13 13
ch38 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
13 13 13 13 13 13
ch40 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
13 13 13 13 13 13
ch42 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13
13 13 13 13 13 13
ch44 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13
13 13 13 13 13 13
ch46 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13
13 13 13 13 13 13
ch48 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13
13 13 13 13 13 13
ch52 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13
13 13 13 13 13 13
ch54 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13
13 13 13 13 13 13
ch56 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13
13 13 13 13 13 13
ch58 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13
13 13 13 13 13 13
ch60 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
13 13 13 13 13 13
ch62 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
13 13 13 13 13 13
ch64 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
13 13 13 13 13 13
ch100 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
13 13 13 13 13 13
```

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxian@cvnchina.com

```
ch102 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
13 13 13 13 13 13
ch104 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
13 13 13 13 13 13
ch106 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 13 13 13 13
13 13 13 13 13 13
ch108 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 13 13 13 13
13 13 13 13 13 13
ch110 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 13 13 13 13
13 13 13 13 13 13
ch112 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 13 13 13 13
13 13 13 13 13 13
ch116 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch118 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch120 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch122 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch124 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch126 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch128 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch132 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 18 18 18 18
18 18 18 18 18 18
ch134 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 18 18 18 18
18 18 18 18 18 18
ch136 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 18 18 18 18
18 18 18 18 18 18
ch140 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch149 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch151 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch153 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch155 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch157 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch159 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch161 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch165 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch169 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
ch173 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18 18
18 18 18 18 18 18
# End of Single SKU Table
```

Note: default SingleSKU profile path in driver is defined “/etc_ro/Wireless/RT2860AP/SingleSKU.dat”

For the detailed usage of SingleSKU in profile support, please refer to the MTK_SingleSKU_InProfile_User_manual.pdf and contact with MTK support windows.

FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

20 Q&A

20.1 Why WPAPSK can not work?

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

20.2 How to switch driver to operate in A band?

Make sure the IC supports A band.
Check parameter "WirelessMode" is set to support A band.
Channel set to 36, 40…..

20.3 When I set channel as 1, but it will appear in channel 3. Why?

Make sure the channel is match with CountryRegion or CountryRegionABand.

20.4 How can I know the version of the WLAN Driver?

Check the definition of DRIVER_VERSION in rt_config.h.
Use command "iwpriv ra0 set DriverVersion=0", it will export to debug console.

20.5 Can SoftAP support Antenna diversity?

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

20.6 Can you tell me what is 11n Bit Rate Derivation?

The BitRate of 11n need below information on MAC driver and the real rates will be triggered by PHY layer depends on below three factors.

a. MCS
b. BW
c. GI

Bandwidth: Data subcarriers on different bandwidth, 20MHz and 40MHz.

a. N_{SD}: Number of data subcarriers.
N_{SD}[40Mhz] = 108
N_{SD}[20Mhz] = 52
N_{SD}[40Mhz]/N_{SD}[20MHz] = **108/52**
= 2.0769230769230769230769230769231

Example:

MCS=15, GI=800ns, BW=20MHz, DataRate = 130Mbps
MCS=15, GI=800ns, BW=40MHz, DataRate = 130 * [$N_{sd(40Mhz)}$ / $N_{sd(20Mhz)}$]

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.
FOR wangxian@cvnchina.com USE ONLY
MEDIATEK CONFIDENTIAL

= 130 * [108 / 52]
= 270Mbps

b. Please refer to “IEEE P802.11n/D2.04, June 2007” on page 314 for below table.

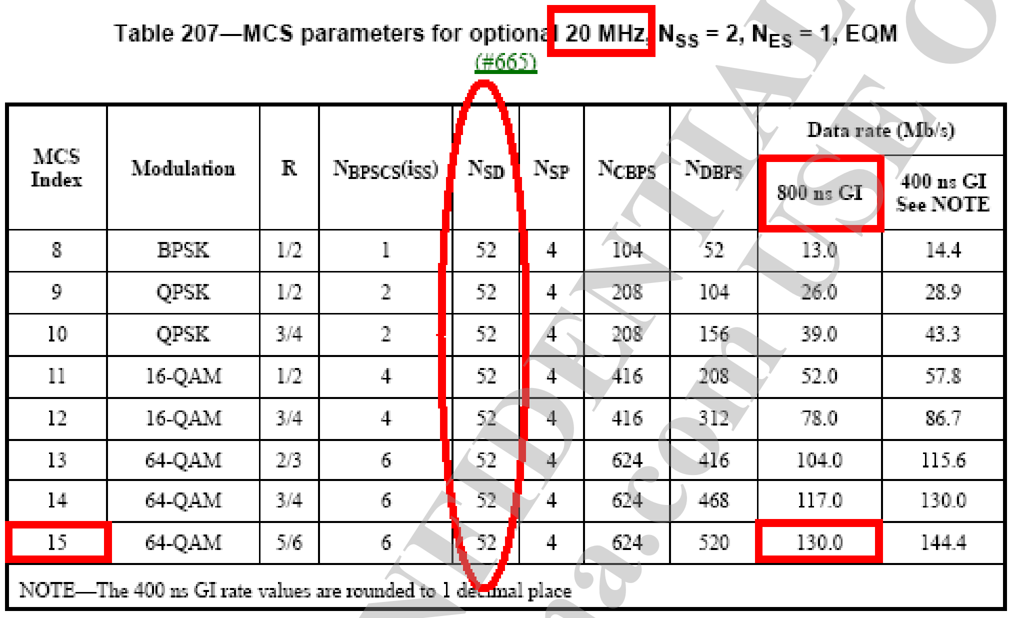


Table 207—MCS parameters for optional 20 MHz, N_{SS} = 2, N_{ES} = 1, EQM (#665)

MCS Index	Modulation	R	$N_{BPSCS}(iss)$	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data rate (Mb/s)	
								800 ns GI	400 ns GI See NOTE
8	BPSK	1/2	1	52	4	104	52	13.0	14.4
9	QPSK	1/2	2	52	4	208	104	26.0	28.9
10	QPSK	3/4	2	52	4	208	156	39.0	43.3
11	16-QAM	1/2	4	52	4	416	208	52.0	57.8
12	16-QAM	3/4	4	52	4	416	312	78.0	86.7
13	64-QAM	2/3	6	52	4	624	416	104.0	115.6
14	64-QAM	3/4	6	52	4	624	468	117.0	130.0
15	64-QAM	5/6	6	52	4	624	520	130.0	144.4

NOTE—The 400 ns GI rate values are rounded to 1 decimal place

1. Guard Interval.

a. Definition:
T_{sym}: 4us , Symbol Interval
T_{syms}: 3.6us , Symbol interval of Short GI.

b. Ratio of symbol interval on GI, refer to below EWC PHY Sepc.
Tsym / Tsyms = 4usec / 3.6usec
= 10/9

Example:
MCS=15, 40MHz Bandwidth, and 400ns Short Guard Interval.
270.0 * (10/9) = 300.0 for Short GI.

c. Reference:
1) IEEE 802.11n draft 2.04, page 316 and

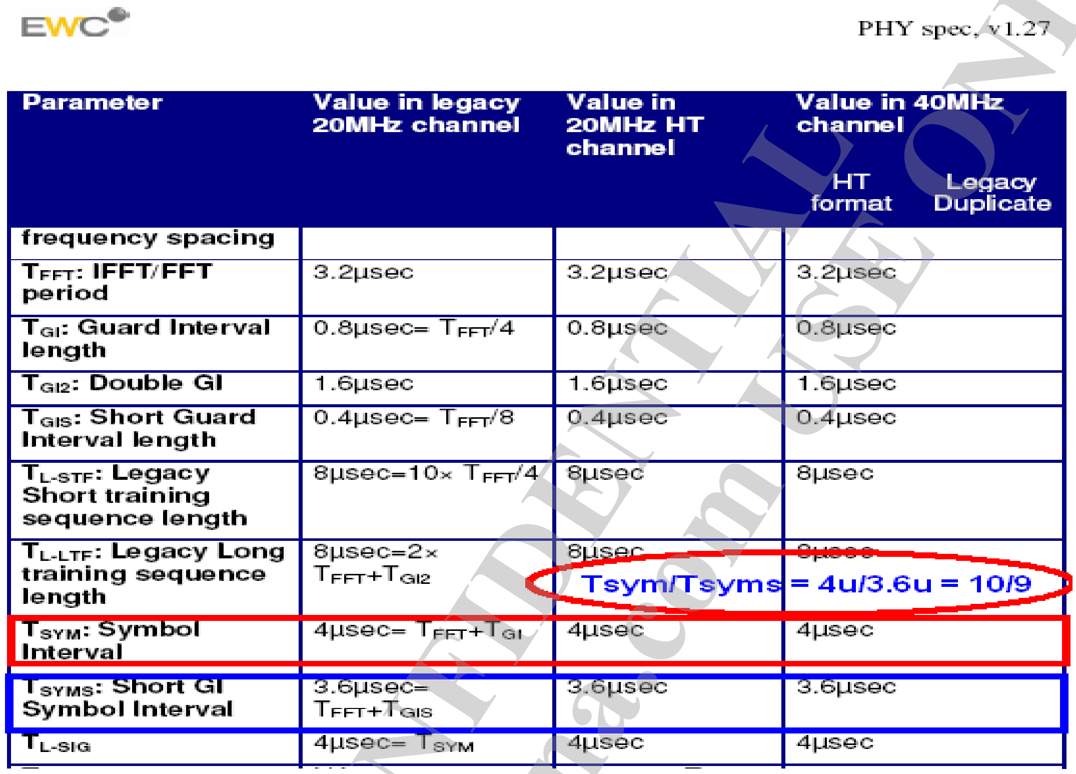
Table 211—MCS parameters for optional 40 MHz, N_{SS} = 2, N_{ES} = 1, EQM (#665)

MCS Index	Modulation	R	$N_{BPSCS}(iss)$	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data rate (Mb/s)	
								800 ns GI	400 ns GI
8	BPSK	1/2	1	108	6	216	108	27.0	30.0
9	QPSK	1/2	2	108	6	432	216	54.0	60.0
10	QPSK	3/4	2	108	6	432	324	81.0	90.0
11	16-QAM	1/2	4	108	6	864	432	108.0	120.0
12	16-QAM	3/4	4	108	6	864	648	162.0	180.0
13	64-QAM	2/3	6	108	6	1296	864	216.0	240.0
14	64-QAM	3/4	6	108	6	1296	972	243.0	270.0
15	64-QAM	5/6	6	108	6	1296	1080	270.0	3

MEDIATEK CONFIDENTIAL FOR wangxiao@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

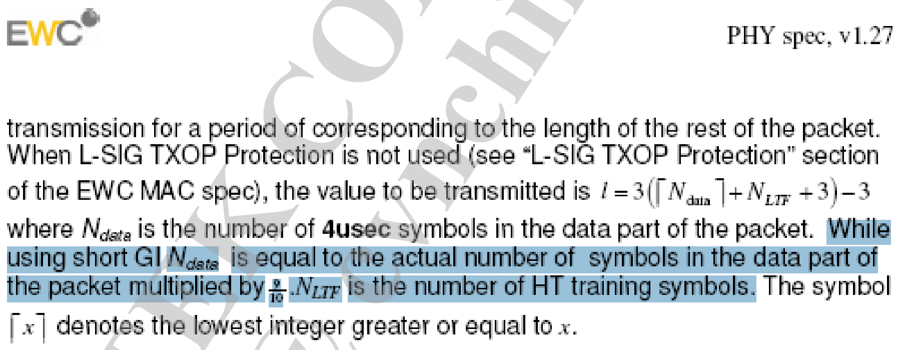
EWC PHY spec. page 13.



PHY spec, v1.27

Parameter	Value in legacy 20MHz channel	Value in 20MHz HT channel	Value in 40MHz channel
			HT format / Legacy Duplicate
frequency spacing			
T_{FFT}: IFFT/FFT period	3.2μsec	3.2μsec	3.2μsec
T_{GI}: Guard Interval length	0.8μsec= $T_{FFT}/4$	0.8μsec	0.8μsec
T_{GI2}: Double GI	1.6μsec	1.6μsec	1.6μsec
T_{GIS}: Short Guard Interval length	0.4μsec= $T_{FFT}/8$	0.4μsec	0.4μsec
T_{L-STF}: Legacy Short training sequence length	8μsec=10× $T_{FFT}/4$	8μsec	8μsec
T_{L-LTF}: Legacy Long training sequence length	8μsec=2× $T_{FFT}+T_{GI2}$	8μsec	8μsec
T_{SYM}: Symbol Interval	4μsec= $T_{FFT}+T_{GI}$	4μsec	4μsec
T_{SYMS}: Short GI Symbol Interval	3.6μsec= $T_{FFT}+T_{GIS}$	3.6μsec	3.6μsec
T_{L-SIG}	4μsec= T_{SYM}	4μsec	4μsec

Tsym/Tsyms = 4u/3.6u = 10/9



PHY spec, v1.27

transmission for a period of corresponding to the length of the rest of the packet. When L-SIG TXOP Protection is not used (see "L-SIG TXOP Protection" section of the EWC MAC spec), the value to be transmitted is $l = 3(\lceil N_{data} \rceil + N_{LTF} + 3) - 3$ where N_{data} is the number of **4usec** symbols in the data part of the packet. While using short GI N_{data} is equal to the actual number of symbols in the data part of the packet multiplied by $\frac{9}{10}$. N_{LTF} is the number of HT training symbols. The symbol $\lceil x \rceil$ denotes the lowest integer greater or equal to x.

20.7 FixTxMode iwpriv command samples

11 B only Mode:

```
iwpriv ra0 set HtOpMode=1
iwpriv ra0 set FixedTxMode=1
iwpriv ra0 set WirelessMode=1
iwpriv ra0 set HtMcs=2
iwpriv ra0 set BasicRate=3
iwpriv ra0 set SSID=RT3052_AP
```

11 G only Mode:

```
iwpriv ra0 set HtOpMode=0
iwpriv ra0 set FixedTxMode=2
iwpriv ra0 set WirelessMode=4
```

FOR MEDIATEK CONFIDENTIAL USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
iwpriv ra0 set HtMcs=5
iwpriv ra0 set BasicRate=351
iwpriv ra0 set SSID=RT3052_AP
```

11 N only Mode:

```
iwpriv ra0 set HtOpMode=1
iwpriv ra0 set FixedTxMode=0
iwpriv ra0 set WirelessMode=6
iwpriv ra0 set HtMcs=13
iwpriv ra0 set BasicRate=15
iwpriv ra0 set SSID=RT3052_AP
```

11 B/G/N mixed Mode:

```
iwpriv ra0 set HtOpMode=0
iwpriv ra0 set FixedTxMode=0
iwpriv ra0 set WirelessMode=9
iwpriv ra0 set HtMcs=5
iwpriv ra0 set BasicRate=15
iwpriv ra0 set SSID=RT3052_AP
```

20.8 DFS Test example

Case 1: Band 2 & 3 select one channel for test
Test Condition:
Run 30% throughput between STA and AP.

DFS Debug command:
```
iwpriv ra0 set RadarDebug=0x10
```

DFS CE certification setting in the profile:
```
IEEE80211H=1
DfsOutdoor=0
RDRegion=CE
CountryCode=GB
```

Result:
All major test items are all passed.

Case 2: Band 2 & 3 select one channel for test.
Test condition:
Run video stream throughput between STA and AP. (Set AP Fix Tx Rate to MCS0)
Bandwidth setting 20MHz and 20/40MHz Auto.

DFS Debug command:

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

```
iwpriv ra0 set RadarDebug=0x10
```

DFS FCC certification setting in the profile:

```
IEEE80211H=1
DfsOutdoor=0
RDRegion=FCC
CountryCode=US
```

Result:
When Radar signal run in 5498~5502MHz, Radar type 3 & 4 fail in BW 40MHz test.
Radar type 1 fail in BW 20MHz test, Recommend to make the Radar signal run in 5495~5525MHz with BW 40MHz test. In 5494~5506MHz in BW 20MHz test. All major test items are all passed.

Case 3: Detect DFS signal without move channel. (For Lab testing)
Command Example:

```
iwpriv ra0 set Debug=3
iwpriv ra0 set Channel=100
iwpriv ra0 set RadarDebug=0x10
iwpriv ra0 set ChMovTime=2
iwpriv ra0 set DfsSwDisable=0
```

Result:
When Radar signals run in channl 100, the AP will display DFS detected information on the console.

DFS deteched consloe log may look like below:

```
DFS HW check channel = 0x4
T= XXXXX W= XXX detected by ch 2
```

20.9 New BSSID Mode MAC Address Limitation (for RT55XX/RT53XX series)

When the NEW_MBSS_MODE is enabled, HW uses the byte0 of MAC address to distinguish different BSSID.

1. The Bit0 of MAC address Byte0 is broadcast/multicast bit.
2. The Bit1 of MAC address Byte0 is local administration bit and should be set to 1 in extended multiple BSSIDs'.
3. The Bit5:Bit2 of MAC address Byte0 is extended multiple BSSID index if the 16 MBSS mode is set.

Please follow the bit-reserved rule as below,
The **bit5 ~ bit2** of **Byte0** need to be reserved as 0 in **16 MBSS** mode.
The **bit4 ~ bit2** of **Byte0** need to be reserved as 0 in **8 MBSS** mode.
The **bit3 ~ bit2** of **Byte0** need to be reserved as 0 in **4 MBSS** mode.
The **bit2** of **Byte0** need to be reserved as 0 in **2 MBSS** mode.

FOR MEDIATEK CONFIDENTIAL USE ONLY
wangxiang@cvnchina.com

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

20.10 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
```

MEDIATEK CONFIDENTIAL FOR wangxian@cvnchina.com USE ONLY

This document contains information that is proprietary to MediaTek Inc.
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.