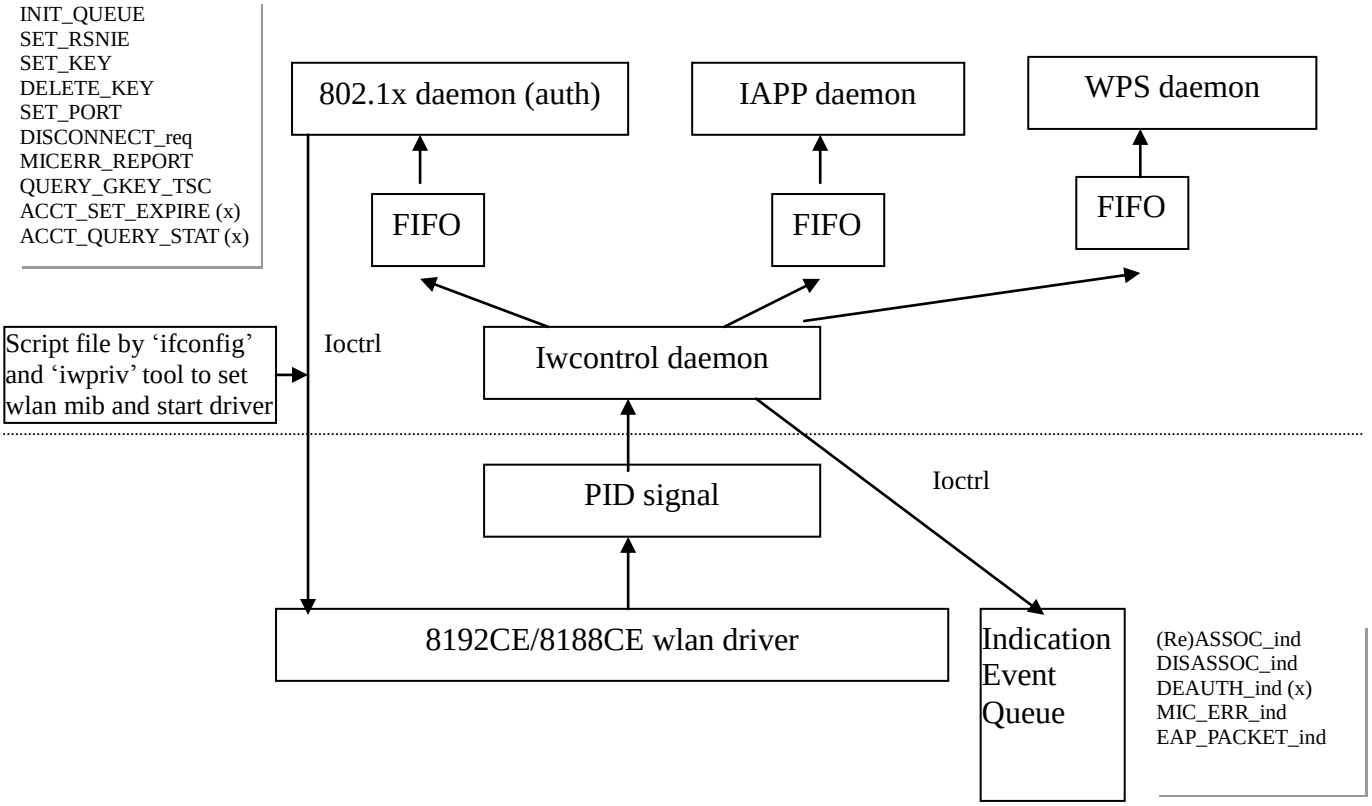
Revision History

Revision	Release date	comment
1.0	2009/11/17	First issue
1.1	2010/1/14	Add comments
1.2	2010/1/29	Add mib of WAPI
1.3	2010/2/24	Add new configuration API support
1.4	2010/4/7	Add mib Add configuration file support
1.5	2010/5/4	Correct explanation of mib
1.6	2010/5/31	Add mib of manual WMM
1.7	2011/3/14	Add dual-band configuration & DFS

Features

- 802.11 b/g/n compatible
- AP mode and client mode support
- Security support 64/128 bits WEP, WPA, and WPA2 (TKIP and AES-CCMP)
- Auto rate adaptive
- Wireless MAC address filter
- Broadcast SSID control
- IAPP (802.11f) support
- Auto channel selection
- Driver based MP functions
- WDS function support
- Universal repeater mode support
- WMM supported for AP mode
- Support for 8192CE and 8188CE ASIC
- WPS function support
- WAPI function support
- Set WMM parameters manually

System Architecture



WLAN Driver Configuration, IOCTL and PROC

Set mac address:
"ifconfig wlan0 hw ether xxxxxxxxxxxx"

Set wlan MIB:
"iwpriv wlan0 set_mib name=value1[,value2,value3…]"
Note 1: value can be a single field or multiple fields separated by ',' without any space between fields. Detail parameter may be referred the following table.
Note 2: if the value is the type of byte array, the format of value will be a string of ASCII of 0~f, which using 2 ASCII standing for one byte. For example, when set Tx power of CCK, it will be
"iwpriv wlan0 set_mib TxPowerCCK=08080909090a0a0a0a0b0b0b0c0c"

Up driver:
"ifconfig wlan0 up"

Close driver:
"ifconfig wlan0 down"

MIB command table:

Name	Meaning	Value	Default	Comment
channel	Operation frequency used	0 for auto channel, 1-14 for 11b/11g, 36-165 for 11a		
ch_low	The lowest channel to scan and use	1-14 for 11b/11g, 36-165 for 11a		
ch_hi	The highest channel to scan and use	1-14 for 11b/11g, 36-165 for 11a		
pwrlevelCCK_A	CCK Tx power level for 14 channels (28 hex digits) for path A	RF module dependent		Type of byte array
pwrlevelCCK_B	CCK Tx power level for 14 channels (28 hex digits) for path B	RF module dependent		Type of byte array
pwrlevelHT40_1S_A	40MHz mode HT OFDM 1 spatial stream Tx power level for 14 channels (28 hex digits) for path A	RF module dependent		Type of byte array
pwrlevelHT40_1S_B	40MHz mode HT OFDM 1 spatial stream Tx power level for 14 channels (28 hex digits) for path B	RF module dependent		Type of byte array
pwrdiffHT40_2S	40MHz mode HT OFDM 2 spatial stream Tx power difference between HT40_1S for 14 channels (28 hex digits). Bit[3:0] for path A. Bit[7:4] for path B.	RF module dependent		Type of byte array
pwrdiffHT20	20MHz mode HT OFDM Tx power difference between HT40_1S for 14 channels (28 hex digits). Bit[3:0] for path A. Bit[7:4] for path B.	RF module dependent		Type of byte array
pwrdiffOFDM	Legacy OFDM Tx power difference between HT40_1S for 14 channels (28 hex digits). Bit[3:0] for path A. Bit[7:4] for path B.	RF module dependent		Type of byte array
preamble	CCK preamble type	0 – long preamble, 1 – short preamble		
trswitch	Enable T/R switch	0 – disable, 1 – enable		
disable_ch14_ofdm	Disable OFDM sending and receiving in channel 14	0 – enable, 1 – disable		
xcap	Crystal Capacitor value	0 – 255		0 stands the value is not calibrated yet.

tssi1	Tx signal strength value of path A	0 – 255		0 stands the value is not calibrated yet.
tssi2	Tx signal strength value of path B	0 – 255		0 stands the value is not calibrated yet.
ther	Thermal value	0 – 255		0 stands the value is not calibrated yet.
MIMO_TR_mode	MIMO mode assignment	1 – 1T2R, 3 – 2T2R, 4 – 1T1R	3	
ssid	SSID	"string_value", SSID with 32 characters in max		
defssid	If don't give SSID in Ad-hoc client mode and no IBSS available, it will start an IBSS with SSID given here.	"string_value", SSID with 32 chars in max	"defaultSSID"	
bssid2join	Besides SSID, designate target BSSID to join	xxxxxxxxxxxx (12 digits mac address)		Type of byte array
bcnint	Beacon interval in ms	20-1024	100	
dtimperiod	DTIM period	1-255	1	Suggest to set 1 because patent issue
swcrypto	S/w encryption enabled/disabled	0 – disable, 1 – enable		
aclmode	Access control mode	0 – disable, 1 – accept, 2 – deny		
aclnum	Set number of ACL	Suggest set '0' whenever driver is re-initialized		
acladdr	Set access control address	xxxxxxxxxxxx (12 digits mac address)		When acl is added, the aclnum will be increased automatically.
oprates	Operational rates	Bit0-bit11 for 1,2,5.5,11,6,9,12,18,24,,36,48,54M	0xfff	
basicrates	Basic rates	Bit0-bit11 for 1,2,5.5,11,6,9,12,18,24,,36,48,54M	0xf	
regdomain	Regulation domain	1-11 (FCC, IC, ETSI, SPAIN, FRANCE, MKK, ISREAL, MKK1, MKK2, MKK3, NCC)	1	
autorate	Auto rate adaptive	0 – disable, 1 – enable	1	
fixrate	Fixed Tx rate	Bit0-bit11 for 1,2,5.5,11,6,9,12,18,24,,36,48,54M Bit12-Bit27 for MCS0,MCS1,…,MCS15		Refer when auto rate is disabled
disable_protection	Forcedly disable protection mode	0 – auto, 1 – disable protection		Normally when 11g is used, driver will auto detect if legacy (11b) device is existed. When 11n is used, driver will auto detect if legacy (11b/g) device is existed. If yes, it will enable protection mode automatically.
disable_olbc	Forcedly OLBC detection	0 – auto, 1 – disable protection		Normally 11g AP should detect OLBC. If disabled, AP will enter protection mode only when legacy device associated.
deny_legacy	Deny the association from legacy STA	0 – disable, 1 – deny		If enabled in B+G mode, AP will deny the association from 11B STA. If enabled in N mode, AP will

<table>
<tr><td></td><td></td><td></td><td></td><td>deny the association from 11B/G STA.</td></tr>
<tr><td>fast_roaming</td><td>Client mode fast roaming</td><td>0 – disable, 1 – enable</td><td></td><td></td></tr>
<tr><td>lowestMlcstRate</td><td>Use lowest basic rate to send multicast and broadcast</td><td>0 – disable
Bit0-bit11 for 1,2,5.5,11,6,9,12,18,24,,36,48,54M
Bit12-Bit27 for MCS0,MCS1,…,MCS15</td><td></td><td></td></tr>
<tr><td>stanum</td><td>Limit max associated sta number</td><td>0-32. 0 – disable (not limit).</td><td></td><td></td></tr>
<tr><td>authtype</td><td>802.11 Authentication type</td><td>0 – open system, 1 – shared key, 2 – auto</td><td>2</td><td></td></tr>
<tr><td>encmode</td><td>Encryption mode</td><td>0 – disabled, 1 – WEP64, 2 – TKIP, 4 – AES(CCMP), 5 – WEP128</td><td></td><td>Set to 2 always under WPA/WPA2 mode</td></tr>
<tr><td>wepdkeyid</td><td>WEP default Tx key</td><td>0-3</td><td></td><td></td></tr>
<tr><td>psk_enable</td><td>PSK mode</td><td>0 – disable, 1 – WPA, 2 – WPA2, 3 – WPA/WPA2 mixed</td><td></td><td></td></tr>
<tr><td>wpa_cipher</td><td>WPA PSK cipher suite</td><td>2 –TKIP, 8 – AES(CCMP), 10 – TKIP/AES mixed</td><td></td><td></td></tr>
<tr><td>wpa2_cipher</td><td>WPA2 PSK cipher suite</td><td>2 –TKIP, 8 – AES(CCMP), 10 – TKIP/AES mixed</td><td></td><td></td></tr>
<tr><td>passphrase</td><td>PSK key</td><td>32 characters or 64 hex digits</td><td></td><td></td></tr>
<tr><td>gk_rekey</td><td>Group key update time</td><td>0 – disable, >1 – enable</td><td></td><td>Time unit is second</td></tr>
<tr><td>802_1x</td><td>Flag of using 802.1x</td><td>0 – disable, 1 – enable</td><td></td><td>When 802.1x is enabled, the Auth daemon must be invoked</td></tr>
<tr><td>default_port</td><td>Default state of 802.1x control port</td><td>0 – data packet is not allowed to pass through until 802.1x authentication is ok
1 – data packet is allowed pass through even 802.1x authentication is not ok</td><td></td><td>Refer when 802_1x is set to 1</td></tr>
<tr><td>wepkey1</td><td>WEP key1</td><td>10 hex digits for WEP64, 26 hex digits for WEP128</td><td></td><td>Type of byte array</td></tr>
<tr><td>wepkey2</td><td>WEP key2</td><td>10 hex digits for WEP64, 26 hex digits for WEP128</td><td></td><td>Type of byte array</td></tr>
<tr><td>wepkey3</td><td>WEP key3</td><td>10 hex digits for WEP64, 26 hex digits for WEP128</td><td></td><td>Type of byte array</td></tr>
<tr><td>wepkey4</td><td>WEP key4</td><td>10 hex digits for WEP64, 26 hex digits for WEP128</td><td></td><td>Type of byte array</td></tr>
<tr><td>opmode</td><td>Operation mode (AP or client)</td><td>16 – AP, 8 – Infrastructure client, 32 – Ad-hoc client</td><td>16</td><td></td></tr>
<tr><td>hiddenAP</td><td>Hidden AP enable/disable</td><td>0 – disabled, 1 – enabled</td><td></td><td></td></tr>
<tr><td>rtsthres</td><td>RTS threshold</td><td>0-2347</td><td>2347</td><td></td></tr>
<tr><td>fragthres</td><td>Fragment threshold</td><td>256-2346</td><td>2346</td><td></td></tr>
<tr><td>shortretry</td><td>Short retry limit</td><td>1-255</td><td>3</td><td></td></tr>
<tr><td>longretry</td><td>Long retry limit</td><td>1-255</td><td>3</td><td></td></tr>
<tr><td>expired_time</td><td>Client inactivity time in 10ms</td><td>>100</td><td>30000</td><td>Time unit is 10 ms.</td></tr>
<tr><td>led_type</td><td>WLAN LED type</td><td><table><tr><th></th><th>LED0</th><th>LED1</th></tr><tr><td>0</td><td>tx</td><td>rx</td></tr><tr><td>1</td><td>enable/tx/rx</td><td>n/a</td></tr><tr><td>2</td><td>link</td><td>tx/rx (d,m)</td></tr><tr><td>3</td><td>link/tx/rx (d,m)</td><td>n/a</td></tr><tr><td>4</td><td>link</td><td>tx/rx (d)</td></tr><tr><td>5</td><td>link/tx/rx (d)</td><td>n/a</td></tr><tr><td>6</td><td>enable</td><td>tx/rx (d)</td></tr><tr><td>7</td><td>enable/tx/rx (d)</td><td>n/a</td></tr><tr><td>8</td><td>11a tx/rx (d)</td><td>11g tx/rx (d)</td></tr></table></td><td></td><td></td></tr>
</table>

<table>
<tr><td></td><td></td><td>0-1 – hw control
2-8 – sw control
d – count data frames
m – count management frames<table><tr><td></td><td>LED2 (GPIO8)</td></tr><tr><td>11</td><td>link/tx/rx (d,m)</td></tr><tr><td>12</td><td>enable/tx/rx (d)</td></tr><tr><td></td><td>LED2 (GPIO10)</td></tr><tr><td>13</td><td>link/tx/rx (d,m)</td></tr><tr><td></td><td>LED1 (GPIO10) (RTL8192D)</td></tr><tr><td>14</td><td>link/tx/rx (d,m)</td></tr><tr><td>50</td><td>enable/tx/rx (d)</td></tr></table>11-14, 50 – sw control
d – count data frames
m – count management frames</td><td></td><td></td></tr>
<tr><td>iapp_enable</td><td>IAPP enable/disable</td><td>0 – disable, 1 - enable</td><td></td><td></td></tr>
<tr><td>block_relay</td><td>Block packet relaying between associated clients</td><td>0 – relay, 1 – block relay and drop, 2 – block relay and indicate to bridge</td><td></td><td></td></tr>
<tr><td>deny_any</td><td>Deny the association SSID of “any” including upper and lower cases</td><td>0 – disable, 1 – enable</td><td></td><td></td></tr>
<tr><td>crc_log</td><td>Calculate CRC error packets</td><td>0 – disable, 1 – enable</td><td></td><td></td></tr>
<tr><td>wifi_specific</td><td>Do WiFi specific check</td><td>0 – disable, 1 – enable</td><td></td><td></td></tr>
<tr><td>disable_txsc</td><td>Tx shortcut enable/disable</td><td>0 – enable, 1 – enable</td><td></td><td></td></tr>
<tr><td>disable_rxsc</td><td>Rx shortcut enable/disable</td><td>0 – enable, 1 – enable</td><td></td><td></td></tr>
<tr><td>disable_brsc</td><td>Bridge shortcut enable/disable</td><td>0 – enable, 1 – enable</td><td></td><td></td></tr>
<tr><td>keep_rsnie</td><td>Don’t clean RSN IE while reinitialize the interface</td><td>0 – erase, 1 – keep</td><td></td><td></td></tr>
<tr><td>band</td><td>Band selection</td><td>1 – 11b, 2 – 11g, 4 – 11a, 8 – 11n</td><td>3</td><td></td></tr>
<tr><td>cts2self</td><td>Use cts2Self for protection mode</td><td>0 – no, 1 – yes</td><td>1</td><td></td></tr>
<tr><td>wds_enable</td><td>WDS enable/disable</td><td>0 – disable, 1 – enable</td><td></td><td></td></tr>
<tr><td>wds_pure</td><td>Flag to enable pure WDS mode that don’t broadcast beacon and don’t accept any station</td><td>0 – disable, 1 – enable</td><td></td><td></td></tr>
<tr><td>wds_priority</td><td>Give WDS packets higher priority</td><td>0 – disable, 1 – enable</td><td></td><td></td></tr>
<tr><td>wds_num</td><td>Set number of WDS</td><td>Suggest set ‘0’ whenever driver is re-initialized</td><td></td><td></td></tr>
<tr><td>wds_add</td><td>Set mac address of peer WDS AP and the rate sent to the peer WDS AP</td><td>xxxxxxxxxxxx (12 digits mac address). The max entry could be added is 8 in default configuration. After mac address, there is a 32-bit variable to give the rate.
Bit0-bit11 for 1,2,5.5,11,6,9,12,18,24,,36,48,54M
Bit12-Bit27 for MCS0,MCS1,…,MCS15</td><td></td><td>When mac address is added, the wds_num will be increased automatically.</td></tr>
<tr><td>wds_encrypt</td><td>WDS encryption mode</td><td>0 – disabled, 1 – WEP64, 2 – TKIP, 4 – AES (CCMP), 5 – WEP128</td><td></td><td></td></tr>
<tr><td>wds_wepkey</td><td>WDS WEP default key</td><td>10 hex digits for WEP64, 26 hex digits for WEP128</td><td></td><td>Type of byte array</td></tr>
<tr><td>wds_passphrase</td><td>WDS PSK key</td><td>32 characters or 64 hex digits</td><td></td><td></td></tr>
<tr><td>nat25_disable</td><td>Disable NAT2.5 transformation in client mode</td><td>0 – enable, 1 – disable</td><td></td><td></td></tr>
<tr><td>macclone_enable</td><td>Enable MAC clone from the first incoming packet</td><td>0 – disable, 1 – enable</td><td></td><td></td></tr>
<tr><td>dhcp_bcst_disable</td><td>Flag of adding broadcast flag into DHCP request</td><td>0 – enable, 1 – disable</td><td></td><td></td></tr>
<tr><td>add_pppoe_tag</td><td>Add extra tag in PPPoE packets by</td><td>0 – disable, 1 – enable</td><td>1</td><td>When set to 0,</td></tr>
</table>

	NAT2.5			NAT2.5 can only support one session buildup at the same time.
clone_mac_addr	Assign the target MAC to clone	xxxxxxxxxxxx (12 digits mac address)		Type of byte array
nat25sc_disable	NAT2.5 shortcut enable/disable	0 – enable, 1 – disable		
show_hidden_bss	Show hidden BSS in site survey	0 – disable, 1 – enable		
ack_timeout	Set ACK timeout value	0-255		0 means using standard value. In unit of us.
private_ie	Send and get private IE	At most 64 hex digits byte array		
groupID	Group ID of virtual AP (multiple SSID)	0-65535		When AP (including root and virtual) set the same group ID, the wlan traffics could be relayed. Root interface: wlan0 Virtual interface: wlan0-va0~wlan0-va3 .
vap_enable	Tell driver if multiple AP function is enabled or disabled	0 – disable, 1 – enable		If multiple AP is enabled, this mib must be set to 1.
func_off	Temporary disable wlan function	0 – normal, 1 – wlan off		
qos_enable	Support WMM and QoS	0 – disable, 1 – enable		
apsd_enable	Support WMM APSD function	0 – disable, 1 – enable		
wsc_enable	Support WiFi Protection Setup	Bit0 for client mode, Bit1 for AP mode		
pin	PIN setting for WPS	“string_value” with 8 characters in max		
supportedmcs	Supported MCS rates	Bit 0-15 for MCS0, …, MCS15	0xffff	
basicmcs	Basic MCS rates	Bit 0-15 for MCS0, …, MCS15		
use40M	Support 40M bandwidth in 11n mode	0 – disable, 1 – enable		
2ndchoffset	Control sideband offset	1 – secondary channel is below the primary channel, 2 – secondary channel is above the primary channel	1	
shortGI20M	Support short GI in 20M bandwidth	0 – disable, 1 – enable		
shortGI40M	Support short GI in 40M bandwidth	0 – disable, 1 – enable		
stbc	Support Space Time Block Coding	0 – disable, 1 – enable		
amsdu	Support packet aggratation	0 – disable, 1 – enable		
lgyEncRstrct	Restrict legacy encryption in N mode	Bit 0: WEP, Bit 1: TKIP		
coexist	Support 20M/40M coexistant mode	0 – disable, 1 – enable		
debug_err	Flag of DEBUG_ERR() macro	Bit value defined in 8185ag_debug.h (in hex)	ffffffff	
debug_info	Flag of DEBUG_INFO() macro	Bit value defined in 8185ag_debug.h (in hex)	0	
debug_warn	Flag of DEBUG_WARN() macro	Bit value defined in 8185ag_debug.h (in hex)	0	
debug_trace	Flag of DEBUG_TRACE() macro	Bit value defined in 8185ag_debug.h (in hex)	0	
ledBlinkingFreq	Multiple of wlan LED blinking frequency.	1~100	1	This value will be referred only when mib value of ‘led_type’ is greater than 1.

wapiType	WAPI mode	0 - Disable 1 - Certificate 2 – PSK	0	
wapiPsk	WAPI PSK	Up to 32 characters		
wapiPsklen	WAPI PSK length	0~32		
wapiUCastKeyType	Unicast key update mode	1 – Disable 2 – Time based 3 – Packet based 4 – Mix mode(Rekey when time or packet number exceeds threshold)		This object selects a mechanism for rekeying the unicast key.
wapiUCastKeyTimeout	Timeout threshold of time-based unicast key update mechanism	Unit: sec.		
wapiUCastKeyPktNum	Packet number threshold of packet based unicast key update mechanism			
wapiMCastKeyType	Multicast key update mode	1 – Disable 2 – Time based 3 – Packet based 4 – Mix mode(Rekey when time or packet number exceeds threshold)		This object selects a mechanism for rekeying the multicast key.
wapiMCastKeyTimeout	Timeout threshold of time-based multicast key update mechanism	Unit: sec.		
wapiMCastKeyPktNum	Packet number threshold of packet based multicast key update mechanism			
manual_edca	Enable / disable EDCA use manual values	0: disable, 1: enable	0	
sta_bkq_acm	Enable / disable AP broadcasting BK queue under ACM	0: disable, 1: enable	0	It is useless in general case
sta_bkq_aifsn	Set AIFS slot number for BK queue broadcasted by AP	1~7	7	Its value in flash is sum of SIFS and total slot time. SIFS is 10 us when 11a/b/g and 16 us when 11n. Slot time is 20 us when 11a/b and 9 us when 11g/n. For example, sta_bkq_aifsn=7 under 11g/n, AIFS is 9*7+16 = 79 us.
sta_bkq_cwmin	Set minimal contention window period for BK queue broadcasted by AP	1~10	4	Slot time will be 2^n-1, 15, by default.
sta_bkq_cwmax	Set maximal contention window period for BK queue broadcasted by AP	1~10	10	Slot time will be 2^n-1, 1023, by default.
sta_bkq_txoplimit	Set TXOP limit for BK queue broadcasted by AP	0~256	0	
sta_beq_acm	Enable / disable AP broadcasting BE queue under ACM	0: disable, 1: enable	0	
sta_beq_aifsn	Set AIFS slot number for BE queue broadcasted by AP	1~7	3	Its value in flash is sum of SIFS and total slot time. SIFS is 10 us when 11a/b/g and 16 us when 11n. Slot time is 20 us when 11a/b and 9 us when 11g/n.

				For example, sta_beq_aifsn=3 under 11g/n, AIFS is 9*3+16 = 43 us.
sta_beq_cwmin	Set minimal contention window period for BE queue broadcasted by AP	1~10	4	Slot time will be 2^n-1, 15, by default.
sta_beq_cwmax	Set maximal contention window period for BE queue broadcasted by AP	1~10	10	Slot time will be 2^n-1, 1023, by default.
sta_beq_txoplimit	Set TXOP limit for BE queue broadcasted by AP	0~256	0	
sta_viq_acm	Enable / disable AP broadcasting VI queue under ACM	0: disable, 1: enable	0	
sta_viq_aifsn	Set AIFS slot number for VI queue broadcasted by AP	1~7	2	Its value in flash is sum of SIFS and total slot time. SIFS is 10 us when 11a/b/g and 16 us when 11n. Slot time is 20 us when 11a/b and 9 us when 11g/n. For example, sta_viq_aifsn=2 under 11g/n, AIFS is 9*2+16 = 34 us.
sta_viq_cwmin	Set minimal contention window period for VI queue broadcasted by AP	1~10	4	Slot time will be 2^n-1, 15, by default.
sta_viq_cwmax	Set maximal contention window period for VI queue broadcasted by AP	1~10	3	Slot time will be 2^n-1, 7, by default.
sta_viq_txoplimit	Set TXOP limit for VI queue broadcasted by AP	0~256	188	Follow SPEC in 11b
sta_voq_acm	Enable / disable AP broadcasting VO queue under ACM	0: disable, 1: enable	0	
sta_voq_aifsn	Set AIFS slot number for VO queue broadcasted by AP	1~7	2	Its value in flash is sum of SIFS and total slot time. SIFS is 10 us when 11a/b/g and 16 us when 11n. Slot time is 20 us when 11a/b and 9 us when 11g/n. For example, sta_voq_aifsn=2 under 11g/n, AIFS is 9*2+16 = 34 us.
sta_voq_cwmin	Set minimal contention window period for VO queue broadcasted by AP	1~10	3	Slot time will be 2^n-1, 7, by default.
sta_voq_cwmax	Set maximal contention window period for VO queue broadcasted by AP	1~10	2	Slot time will be 2^n-1, 3, by default.
sta_voq_txoplimit	Set TXOP limit for VO queue broadcasted by AP	0~256	102	Follow SPEC in 11b
ap_bkq_aifsn	Set AIFS slot number for BK queue used by AP	1~7	7	Its value in flash is sum of SIFS and total slot time. SIFS is 10 us when

				11a/b/g and 16 us when 11n. Slot time is 20 us when 11a/b and 9 us when 11g/n. For example, ap_bkq_aifsn=7 under 11g/n, AIFS is 9*7+16 = 79 us.
ap_bkq_cwmin	Set minimal contention window period for BK queue used by AP	1~10	4	Slot time will be 2^n-1, 15, by default.
ap_bkq_cwmax	Set maximal contention window period for BK queue used by AP	1~10	10	Slot time will be 2^n-1, 1023, by default.
ap_bkq_txoplimit	Set TXOP limit for BK queue used by AP	0~256	0	
ap_beq_aifsn	Set AIFS slot number for BE queue used by AP	1~7	3	Its value in flash is sum of SIFS and total slot time. SIFS is 10 us when 11a/b/g and 16 us when 11n. Slot time is 20 us when 11a/b and 9 us when 11g/n. For example, ap_beq_aifsn=3 under 11g/n, AIFS is 9*3+16 = 43 us.
ap_beq_cwmin	Set minimal contention window period for BE queue used by AP	1~10	4	Slot time will be 2^n-1, 15, by default.
ap_beq_cwmax	Set maximal contention window period for BE queue used by AP	1~10	6	Slot time will be 2^n-1, 63, by default.
ap_beq_txoplimit	Set TXOP limit for BE queue used by AP	0~256	0	
ap_viq_aifsn	Set AIFS slot number for VI queue used by AP	1~7	1	Its value in flash is sum of SIFS and total slot time. SIFS is 10 us when 11a/b/g and 16 us when 11n. Slot time is 20 us when 11a/b and 9 us when 11g/n. For example, ap_viq_aifsn=1 under 11g/n, AIFS is 9*1+16 = 25 us.
ap_viq_cwmin	Set minimal contention window period for VI queue used by AP	1~10	4	Slot time will be 2^n-1, 15, by default.
ap_viq_cwmax	Set maximal contention window period for VI queue used by AP	1~10	3	Slot time will be 2^n-1, 7, by default.
ap_viq_txoplimit	Set TXOP limit for VI queue used by AP	0~256	188	Follow SPEC in 11b
ap_voq_aifsn	Set AIFS slot number for VO queue used by AP	1~7	1	Its value in flash is sum of SIFS and total slot time. SIFS is 10 us when 11a/b/g and 16 us when 11n. Slot time is 20 us when 11a/b and 9 us when 11g/n. For example,

				ap_voq_aifsn=1 under 11g/n, AIFS is 9*1+16 = 25 us.
ap_voq_cwmin	Set minimal contention window period for VO queue used by AP	1~10	3	Slot time will be 2^n-1, 7, by default.
ap_voq_cwmax	Set maximal contention window period for VO queue used by AP	1~10	2	Slot time will be 2^n-1, 3, by default.
ap_voq_txoplimit	Set TXOP limit for VO queue used by AP	0~256	102	Follow SPEC in 11b
phyBandSelect	Set band mode for dual-band	1 – 2G, 2 – 5G	wlan0: 2 wlan1: 1	Please refer to section "Dual-band configuration"
macPhyMode	Set dual or single MAC/PHY mode	0 – Single MAC/PHY, 2 – Dual MAC/PHY	2	Please refer to section "Dual-band configuration"

Note1: The default value of MIB will be '0' if it is not specified.
Note2: The values set to EDCA manually will be applied after driver close and up

Read wlan register command:
"iwpriv wlan0 read_reg type,offset"
- *type* could be b - for byte, w – for word, dw – for double word
- *offset* indicates the register offset in hex

Write wlan register command:
"iwpriv wlan0 write_reg type,offset,value"
- *type* may be b - for byte, w – for word, dw – for double word
- *offset* indicates the register offset in hex
- *value* for write in hex

Read memory command:
"iwpriv wlan0 read_mem type,start,len"
- *type* may be b - for byte, w – for word, dw – for double word
- *start* indicates the memory start address in hex
- *len* is for read length in hex

Write memory command:
"iwpriv wlan0 write_mem type,start,len,value"
- *type* may be b - for byte, w – for word, dw – for double word
- *start* indicates the memory start address in hex
- *len* is for write length in hex
- *value* for write in hex

Note:
The commands above take "wlan0" for example. One can replace "wlan0" with "wlan1" in each command when dual MAC/PHY is enabled.

Driver based MP function:
We supported Driver based MP functions controlled by "iwpriv" utility. Please refer to *"8192C Linux Driver MP.doc"* for detail explanation and usages.

Additional IOCTL commands (for web display):

id	**Meaning**	**Input**	**output**	**comment**
0x8b30	Get station info	None	64 array of sta_info_2_web (note1)	

0x8b31	Get associated station number	None	1 word (2 bytes)	
0x8b32	Get version information	None	2 byte of version infomation	
0x8b33	Issue scan request	None	1 byte of result (-1:fail, 0: success)	
0x8b34	Get scan result and scanned BSS database	1 byte flag (get BSS database or not)	4 bytes of number of entries and array of bss_desc (note4) with flag set to 0	
0x8b35	Issue join request	bss_desc to join	1 byte of result (0: success, 1: scanning, 2: fail)	
0x8b36	Get join result	None	1 byte of result (note5)	
0x8b37	Get BSS info	None	Bss_info_2_web structure (note2)	This is used typically in client mode
0x8b38	Get WDS info	None	8 array of wds_info (note3)	

Note1:

```
typedef struct _sta_info_2_web {
        unsigned short    aid;
        unsigned char     addr[6];
        unsigned long     tx_packets;
        unsigned long     rx_packets;
        unsigned long     expired_time;
        unsigned short    flags; // bit2 indicate whether this entry is valid, bit3 indicates if sta is in sleeping
        unsigned char     TxOperaRate; // current used tx rate in 500 k bps (e.g., 108 for 55M)
        unsigned char     rssi; // received signal strength indication
        unsigned long     link_time; // 1 sec unit
        unsigned long     tx_fail;
        unsigned long     tx_bytes;
        unsigned long     rx_bytes;
        unsigned char     network;
        unsigned char     ht_info;
        unsigned char     resv[6];
} sta_info_2_web;
```

Note2:

```
typedef enum _wlan_mac_state {
      STATE_DISABLED=0, STATE_IDLE, STATE_SCANNING, STATE_STARTED, STATE_CONNECTED,
STATE_WAITFORKEY
} wlan_mac_state;

typedef struct _bss_info_2_web {
      unsigned char state;       // defined in wlan_mac_state
      unsigned char channel;
      unsigned char txRate;
      unsigned char bssid[6];
      unsigned char rssi, sq;
      unsigned char ssid[33];
} bss_info_2_web;
```

Note3:

```
typedef struct _wds_info {
        unsigned char     state;
        unsigned char     addr[6];
        unsigned long     tx_packets;
        unsigned long     rx_packets;
        unsigned long     tx_errors;
        unsigned char     TxOperaRate;
} wds_info;
```

Note4:

```
struct ibss_priv {
        unsigned short  atim_win;    };
struct bss_desc {
        unsigned char   bssid[6];
        unsigned char   ssid[32];
        unsigned char   *ssidptr;
        unsigned short  ssidlen;
        unsigned char   meshid[32];
        unsigned char   *meshidptr;
        unsigned short  meshidlen;
        unsigned int    bsstype;
        unsigned short  beacon_prd;
        unsigned char   dtim_prd;
        unsigned long   t_stamp[2];
        struct ibss_priv ibss_par;
        unsigned short  capability;
        unsigned char   channel;
        unsigned long   basicrate;
        unsigned long   supportrate;
        unsigned char   bdsa[6];
        unsigned char   rssi;
        unsigned char   sq;
        unsigned char   network;
};
```

Note5:
0xff: pending
2-4: success
others: fail

Files under '/proc/wlan0':

- ***cam_info*** – dump h/w encryption cam content
- ***mib_xxx*** – show mib info
- ***sta_info*** – show all associated station info
- ***sta_keyinfo*** – show the encryption keys of all associated station info
- ***txdesc0, …, txdesc5*** – show tx descriptor contents for queue 0 to queue 5
- ***rxdesc*** – show rx descriptor contents
- ***buf_info*** – show the internal buffer pointers and counts
- ***desc_info*** – show tx and rx descriptor pointers, indexes, and register contents
- ***stats*** – show Tx, Rx, and beacon statistics
- ***mib_EDCA*** – show the EDCA parameters will be applied when enabled
- ****.txt*** – MAC and PHY parameter files

Dual-band Configuration

- Dual-band functions are only supported by RTL8192D series.
- Dual MAC/PHY mode is dependent on Linux kernel configuration "RTL8192D dual-MAC-dual-PHY mode"
- For Dual MAC/PHY mode, wlan0 is for 5G only, wlan1 is for 2G only.

Dual-band related mibs:

- *phyBandSelect:* setting the wlan interface as either 5G or 2G
- *macPhyMode:* setting the wlan interface to be started as Dual MAC/PHY (1T1R Concurrent Mode)

or Single MAC/PHY (2T2R Selective Mode)

- *band:* setting the band for wlan interfaces. For example: 5G: 12 (A+N), 2G: 11 (B+G+N)
- *channel:* setting a correct channel according to the band setting.

phyBandSelect	Set band mode for dual-band	1 – 2G, 2 – 5G	wlan0: 2 wlan1: 1	Please refer to section “Dual-band configuration”
macPhyMode	Set dual or single MAC/PHY mode	0 – Single MAC/PHY, 2 – Dual MAC/PHY	2	Please refer to section “Dual-band configuration”
channel	Operation frequency used	0 for auto channel, 1-14 for 11b/11g, 36-165 for 11a		
band	Band selection	1 – 11b, 2 – 11g, 4 – 11a, 8 – 11n	wlan0:12 wlan1:11	
pwrlevel5GHT40_1S_A	40MHz mode HT OFDM 1 spatial stream Tx power level for 196 (channel 1~196) channels (392 hex digits) for path A	RF module dependent		Type of byte array. E.g. Channel 36 should use the 36’th byte.
pwrlevel5GHT40_1S_B	40MHz mode HT OFDM 1 spatial stream Tx power level for 196 (channel 1~196) channels (392 hex digits) for path B	RF module dependent		Type of byte array. E.g. Channel 36 should use the 36’th byte.
pwrdiff5GHT40_2S	40MHz mode HT OFDM 2 spatial stream Tx power difference between HT40_1S for 196 (channel 1~196) channels (392 hex digits). Bit[3:0] for path A. Bit[7:4] for path B.	RF module dependent		Type of byte array. E.g. Channel 36 should use the 36’th byte.
pwrdiff5GHT20	20MHz mode HT OFDM Tx power difference between HT40_1S for 196 (channel 1~196) channels (392 hex digits). Bit[3:0] for path A. Bit[7:4] for path B.	RF module dependent		Type of byte array. E.g. Channel 36 should use the 36’th byte.
pwrdiff5GOFDM	Legacy OFDM Tx power difference between HT40_1S for 196 (channel 1~196) channels (392 hex digits). Bit[3:0] for path A. Bit[7:4] for path B.	RF module dependent		Type of byte array. E.g. Channel 36 should use the 36’th byte.

Note 1: if the value is the type of byte array, the format of value will be a string of ASCII of 0~f, which using 2 ASCII standing for one byte. For example, when set Tx power of pwrlevel5GHT40_1S_A, it will be

“iwpriv wlan0 set_mib
pwrlevel5GHT40_1S_A=00000000000000000000000000000000000000000000000000000000000000000000002828282828282
828282828282828282828282828282828282828282828282800000000000000000000000000000000000000000000000000000
00000000000000000282828282828282828282828282828282828282828282828282828282828282828282828282828282828000
0000000000000028282828282828282828282828282828282828280000000000000000000000000000000000000000000000000000
00000000”

Configuration by “*iwpriv*” Examples:

I. Setting as 5G Single MAC/PHY selective mode

1. disable all wlan interfaces
   > ifconfig wlan0 down
2. setting related mibs
   a. setting single MAC/PHY
   > iwpriv wlan0 set_mib macPhyMode=0

b. setting 5GHz band
> iwpriv wlan0 set_mib phyBandSelect=2
c. setting band as A+N mode
> iwpriv wlan0 set_mib band=12
d. setting channel, e.g channel 44
> iwpriv wlan0 set_mib channel=44
e. setting other mib if necessary, such as 40M bandwidth, encryption, etc.

3. enable wlan interface
> ifconfig wlan0 up

II. Setting as 2G Single MAC/PHY selective mode

1. disable all wlan interfaces
> ifconfig wlan0 down
2. setting related mibs
a. setting single MAC/PHY
> iwpriv wlan0 set_mib macPhyMode=0
b. setting 2.4GHz band
> iwpriv wlan0 set_mib phyBandSelect=1
c. setting band as B+G+N mode
> iwpriv wlan0 set_mib band=11
d. setting channel, e.g channel 6
> iwpriv wlan0 set_mib channel=6
e. setting other mib if necessary, such as 40M bandwidth, encryption, etc.
3. enable wlan interface
> ifconfig wlan0 up

III. Setting as the Dual MAC/PHY concurrent mode

1. disable all wlan interfaces
> ifconfig wlan0 down
> ifconfig wlan1 down
2. setting related mibs
a. setting dual MAC/PHY
> iwpriv wlan0 set_mib macPhyMode=2
> iwpriv wlan1 set_mib macPhyMode=2
b. setting wlan0 as 5GHz band, setting wlan1 as 2.4GHz band
> iwpriv wlan0 set_mib phyBandSelect=2
> iwpriv wlan1 set_mib phyBandSelect=1
c. setting wlan0 band as A+N mode, setting wlan1 band as B+G+N mode
> iwpriv wlan0 set_mib band=12
> iwpriv wlan1 set_mib band=11
d. setting channel, e.g 5G channel 44, 2G channel 6
> iwpriv wlan0 set_mib channel=44
> iwpriv wlan1 set_mib channel=6
e. setting other mib if necessary, such as 40M bandwidth, encryption, etc.

3. enable wlan interface
> ifconfig wlan0 up
>ifconfig wlan1 up

Dynamic Frequency Selection (DFS)

I. DFS is enabled if Linux kernel configuration "DFS support" is enabled.
II. To obey regulation, DFS channels can ONLY be selected by auto-channel selection. The user can see "Auto (DFS)" on the channel column on web UI.
III. If the user want to force the DUT set in a DFS channel for evaluation purpose, one should set console command with "**flash set WLAN0_CHANNEL <*channel #*>**", and then reboot.
Note: Alternatively, the user can use http://192.168.1.254/syscmd.asp to input the command.

5G Channel Plan

regulation domain (mib *regdomain* value)	**supported channels – DFS enabled**	**supported channels – DFS disabled**
FCC (1)	36,40,44,48,52,56,60,64,100,104,108, 112,116, 136,140,149,153,157,161,165	36,40,44,48,149,153,157,161,165
IC (2)	36,40,44,48,52,56,60,64,149,153,157, 161	36,40,44,48,149,153,157,161
ETSI (3)	36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140	36,40,44,48
SPAIN (4)	36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140	36,40,44,48
FRANCE (5)	36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140	36,40,44,48
MKK (6)	36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140	36,40,44,48
ISREAL (7)	36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140	36,40,44,48
MKK1 (8)	34,38,42,46	34,38,42,46
MKK2 (9)	36,40,44,48	36,40,44,48
MKK3 (10)	36,40,44,48,52,56,60,64	36,40,44,48
NCC (11)	56,60,64,100,104,108,112,116,136,140, 149,153,157,161,165	56,60,64,149,153,157,161,165

iwcontrol Daemon Configuration

Need start daemon when:
- 802.1x daemon is used
- IAPP daemon is used
- WPS daemon is used

Note: iwcontrol daemon should be started after 802.1x, IAPP, or WPS daemon is running

Start daemon:
"iwcontrol wlan_interface ...."
➢ *wlan_interface:* wlan interface, e.g., wlan0

Note:
1. *iwcontrol daemon will parse the pid files in "/var/run" and create FIFO files to do IPC with WPS, IAPP, and 1x daemon.*
2. *Multiple wireless interfaces can be supported in iwcontrol parameters.*

802.1x Daemon Configuration

Need start daemon when:
- WPA/WPA2 is used
- WEP + 802.1x (authentication with radius server)
- No encryption + 802.1x (authentication with radius server)

Start 802.1x daemon:
"auth wlan_interface lan_interface auth wpa_conf &"
- *wlan_interface:* wlan interface, e.g., wlan0
- *lan_interfac*e: lan interface, which connects to Radius server, e.g., br0
- *auth*: denote to act as authenticator
- *wpa_conf*: path of wpa config file, e.g., /var/wpa-wlan0.conf

Note:
1. *Multiple 802.1x daemons will be created for different wireless interfaces.*
2. *PID file "/var/run/auth-wlanx.pid" will be created for each 1x daemon*

Parameter format in wpa config file:
"keyword = value"

table of wpa parameters

keyword	**value**	**Comment**
encryption	0 – disable, 1 – WEP, 2 – WPA, 4 – WPA2 only, 6 – WPA2 mixed	
ssid	"string_value", 1-32 char	
enable1x	0/1 – disable/enable 1x Radius authentication	Refer when encryption is set to 0, 1
enableMacAuth	0/1 – disable/enable MAC authentication	
SupportNonWpaClient	0/1 – disable/enable none WPA client support when WPA is set	This feature is not supported now
wepKey	1 – WEP64, 2 – WEP128	Refer when encryption is set 1 (wep)
wepGroupKey	set "" as default	No use
authentication	1 – Radius, 2 – PSK (pre-shared key)	
unicastCipher	1 – TKIP, 2 – AES	
wpa2UnicastCipher	1 – TKIP, 2 – AES	
usePassphrase	0 – use psk value as key in raw data, 1 – use passphrase algorithm to convert psk value	
psk	"string_value", if usePassphrase=0 (raw data), it should be 64 hex digits. If usePassphrase=1, the string length should be >=8 and <=64.	
groupRekeyTime	Group key re-key time	No use
rsPort	UDP Port number of radius server	Normally 1812 is used
rsIP	IP address of radius server (e.g., 192.168.1.1)	
rsPassword	"string_value", password of radius server with 31 char in max	
rs2Port	UDP Port number of radius server set 2	Normally 1812 is used
rs2IP	IP address of radius server (e.g., 192.168.1.1) set 2	
rs2Password	"string_value", password of radius server with 31 char in max set 2	
rsMaxReq	Max retry number of request packet with radius server	Set 3 as default
rsAWhile	Timeout time (in second) of waiting rsp packet of radius server	Set 5 as default
accountRsEnabled	0/1 – disable/enable accounting radius server	
accountRsPort	UDP Port number of accounting radius server	

accountRsIP	IP address of accounting radius server	
accountRsPassword	"string_value", password of accounting radius server with 31 char in max	
accountRsUpdateEnabled	0/1 – disable/enable the feature of statistic update with accounting server	
accountRsUpdateTime	Update time in seconds	
accountMaxReq	Max retry number of request packet with accounting radius server	
accountAWhile	Timeout time (in second)of waiting rsp packet of accounting radius server	

IAPP Configuration

Start IAPP daemon:
"iapp lan_interface wlan_interface …&"

- *lan_interface:* interface name which IAPP daemon use to send IAPP packet (e.g., br0)
- *wlan_interface:* wlan interface, e.g., wlan0

Notes:

1. *IAPP can support multiple wireless interfaces.*
2. *PID file "/var/run/iapp.pid" will be created for iapp deamon.*

WPS Configuration

The driver has already supported WPS function, but it needs to cooperate with WPS daemon in user level. Please refer to *"Realtek_WPS_user_guide.doc"* for detail explanation and usages.

WAPI Configuration

The driver has already supported WAPI function. Please refer to *"WAPI Porting Guide.doc"* for detail explanation and usages.

Configuration File support

The driver can be configured via a ***configuration file*** each time an interface is up.

Kernel configuration:
Select *"Network device support ---> Wireless LAN (non-hamradio) ---> Config File support"*; then rebuild kernel image.

Configuration file:

- *Path*: /etc/Wireless/RTL8192CD.dat
- *Sytax:* 'wlan_interface'_'mib_command' , e.g. wlan0_ssid=xxxx.

Notes:

1. *Add '#' in front of comment lines.*
2. *Space is NOT allowed between 'wlan_interface' and 'mib_command'.*
3. *If the user needs to configure MIB values with special characters, e.g. '#', the value of 'mib_command' MUST be* ***quoted*** *E.g. wlan0_ssid="#XXXXX@##$$%%"*
4. *'wlan_interface': wlan interface, e.g., wlan0, wlan0-va0. However, please* ***DO NOT*** *configure* ***WDS*** *interfaces because WDS is configured in wlan0 interface.*

5. *'mib_command': MIB commands, e.g., ssid=xxxx, please refer to table "MIB command table" and following "Extended MIB command table"*
6. *MIB value should be also configured for each virtual interface separately.*
7. *Each time an interface is up, the configuration file will be loaded.*

Extended MIB command table (available only if Config File support is turned on):

Name	Meaning	Value	Default	Comment
hwaddr	MAC address of WLAN interface	12 hex digits, e.g. 00e04c8192a1	0	
meshSilence	In AP+Mesh mode but not enable mesh function	0 – mesh enabled, 1 – mesh disabled	0	Available if mesh is built with kernel image

iwconfig/iwlist support

The driver has already supported iwconfig and iwlist (Wireless Tools v29) for getting or setting some configurations.

Kernel configuration:
Select *"Network device support ---> Wireless LAN (non-hamradio) ---> Wireless Extensions v18 support"* and *"Network device support ---> Wireless LAN (non-hamradio) ---> Wireless Tools v29 support"*; then rebuild kernel image.

iwconfig – configure a wireless network interface.
Notes: Because *'iwconfig'* cannot fully cover all the configurations of the AP, we suggest the users using *'iwpriv'* to setup the AP.

Synopsis of **iwconfig**:
- iwconfig [*interface*]
- iwconfig *interface* [essid *X*] [mode *M*] [freq *F*] [channel *C*] [ap *A*] [rate *R*] [rts *RT*] [frag *FT*] [enc *E*] [key *K*] [retry *R*]
- iwconfig --help
- iwconfig --version

Parameters of **iwconfig**

Name	Meaning	Value	Access	Comment
essid	ESSID	any string, e.g. iwconfig essid "My SSID"	GET/SET	
mode	operating mode of the device	*Ad-Hoc*, *Managed* (client mode), *Master* (AP mode), *Repeater, Monitor*	GET	
freq	operating frequency	frequency in GHz	GET/SET	
channel	operating channel value	channel value	GET/SET	
ap	MAC address	e.g. *00:e0:4c:01:23:45*	GET	
rate/bit[rate]	maximum available bit rate	bit rate in Mb/s	GET	
rts[_threshold]	RTS threshold	packet size or off	GET/SET	
frag[mentation_threshold]	fragmentation threshold	packet size; off: based on driver setting	GET/SET	
key/enc[ryption]	WEP key settings	mode: open/restricted; keys in 10 or 32 hex-digit	GET	
retry	retry limits	number of retrys	GET	

Notes: for more detailed information, please refer to the manual of iwconfig.

iwlist – Get more detailed wireless information from a wireless interface
Notes: Because *'iwlist'* cannot fully cover all the configurations of the AP, we suggest the users using *'iwpriv'* to access settings of the AP.

Synopsis of **iwlist**:
- iwlist [*interface*] [*keyword*]
- iwlist --help
- iwlist --version

keywords of **iwlist**

Name	**Meaning**	**Value**	**Comment**
scanning	site survey of neighboring WLAN devices	list of Access Points and Ad-Hoc cells in range.	
channel/frequency	supported channel and frequency	frequencies in GHz corresponding to the channels	varied as domain region changed
bitrate/rate	supported rate and extended supported rate announced in beacon	supported bit-rates in Mb/s	HT rates are not listed by iwlist
keys/encryption	WEP encryption information	key sizes, list of available keys and current transmit key	
ap/accsspoints/peers	Associated peer list	list of associated peers	
auth	Authentication capabilities	WPA, WPA2, CIPHER-TKIP, CIPHER-CCMP	

Notes: for more detailed information, please refer to the manual of iwlist.

Limitation

- H/W encryption CAM size is 32
- Multiple BSSID CAM size is 8
- Tx SKB buffer must have 8 bytes space in tail for TKIP MIC
- Support 32 wlan clients in current configuration
- Support 8 WDS number in current configuration