

Quick Start Guide for starting Soft-AP mode

(A) How to start Soft-AP mode:

- (1) disable network management or other wireless tools, e.g. wpa_supplicant
- (2) uncompress the driver and then compile the driver

```
$ [unpack driver]
$ cd [driver directory]
$ make
```
- (3) insert driver

```
$ insmod 8723as.ko
```
- (4) set IP (using the static ip for testing), suppose interface is “wlan0”, you can use “iwconfig” to check interface name.

```
$ ifconfig wlan0 192.168.0.1
```
- (5) compile HOSTAP, unpack "wpa_supplicant_hostapd-0.8_rtw_XXXXXXX.zip" in the folder (wpa_supplicant_hostapd-0.8/hostapd)

```
$ [unpack wpa_supplicant_hostapd-0.8_rtw_XXXXXXX.zip]
$ cd wpa_supplicant_hostapd-0.8/hostapd/
$ make
```
- (6) start hostapd daemon, and you may need root privileges

```
# ./hostapd rtl_hostapd.conf -B
```

(B) Configure file for Soft-AP mode setting:

- (1) rtl_hostapd.conf is the configure file for functions setting.
- (2) the major variable setting in the rtl_hostapd.conf configure file,

(a) basic configuration

```
interface=wlan0
```

```
ssid=rtwap
```

```
# channel 1-14 is 2.4 GHz ; channel 36, 40, 44, 46, 48, 52, 56, 60,
```

```
# 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149,
```

```
# 153, 157, 161 is 5GHz
```

```
# The channels that are available for use in a particular country differ
```

```
# according to the regulations of that country.
```

```
channel=6
```

```
# Operation mode (a = IEEE 802.11a, b = IEEE 802.11b, g = IEEE
# 802.11g, Default: IEEE 802.11b )
hw_mode=g
```

```
#If the wireless interface is included in a bridge,
#an additional configuration parameter, bridge, is needed
#bridge=br0
```

(b) security mode configuration

```
# This field is a bit field that can be used to enable WPA
# (IEEE 802.11i/D3.0)
# and/or WPA2 (full IEEE 802.11i/RSN):
# bit1 = IEEE 802.11i/RSN (WPA2) (dot11RSNAEnabled)
wpa=2
```

```
# wpa_passphrase=secret passphrase
wpa_passphrase=87654321
```

```
# Set of accepted key management algorithms
# (WPA-PSK, WPA-EAP, or both).
wpa_key_mgmt=WPA-PSK
```

```
# Set of accepted cipher suites (encryption algorithms)
# for pairwise keys
wpa_pairwise=CCMP
```

(c) IEEE 802.11n related configuration

```
# ieee80211n: Whether IEEE 802.11n (HT) is enabled
# 0 = disabled (default)
# 1 = enabled
ieee80211n=1
# ht_capab: HT capabilities (list of flags)
# Supported channel width set: [HT40-] = both 20 MHz and 40 MHz
# with secondary channel below the primary channel;
# [HT40+] = both 20 MHz and 40 MHz with secondary channel upon
# the primary channel
# Note: There are limits on which channels can be used with HT40- and
# HT40+. Following table shows the channels that may be available for
```

```
# HT40- and HT40+ use per IEEE 802.11n Annex J:
# freq          HT40-          HT40+
# 2.4 GHz       5-13           1-7 (1-9 in Europe/Japan)
# 5 GHz         40,48,56,64     36,44,52,60
# Short GI for 20 MHz: [SHORT-GI-20] (disabled if not set)
# Short GI for 40 MHz: [SHORT-GI-40] (disabled if not set)
ht_capab=[SHORT-GI-20][SHORT-GI-40][HT40]
```

(C) check the station connected to softap using hostapd_cli:

```
./hostapd_cli all_sta
```

(D) How to start WPS process as internal registrar?

1. for PIN code = 12345670

```
$>./hostapd_cli wps_pin any 12345670
```

2. for PBC

```
$>./hostapd_cli wps_pbc
```