NEW RADIO COMMUNICATION FOR NEW ERA

NRC7394 Evaluation Kit User Guide

(WPS-PBC)

Ultra-low power & Long-range Wi-Fi

Ver 1.0
Apr. 5, 2023

NEWRACOM, Inc.

NRC7394 Evaluation Kit User Guide (WPS-PBC)
Ultra-low power & Long-range Wi-Fi

Office

Newracom, Inc.
505 Technology Drive, Irvine, CA 92618 USA
http://www.newracom.com

Contents

List of Figures

1 WPS (Wi-Fi Protected Setup)

Wi-Fi Protected Setup™ (WPS) is a standard published by the Wi-Fi Alliance with the aim of simplifying the configuration process to establish a secure wireless network. WPS allows devices to be easily added to a network while providing a secure connection. AP and STA that supports WPS use a personal identification number (PIN) and push button connection (PBC) to connect devices. NRC7394 EVK supports WPS-PBC and how to operate will be explained in the next chapter.

2 WPS-PBC operation (Host-mode)

In this chapter, we describe how to build wpa_supplicant and hostapd to support WPS-PBC and how to operate WPS-PBC on both NRC7394 EVK HM(host-mode) STA and AP in detail

2.1 Build Configuration

During WPS operation, WPA Supplicant acts as the Enrollee and therefore it should include WPS config, **CONFIG_WPS=y**, when building SW. Hostapd also should be built with WPS config, **'CONFIG_WPS=y and CONFIG_WPS_UPNP=y (if you want to use external Registrar)'** to support WPS as a role of Registrar

2.2 Command for WPS-PBC

To operate WPS-PBC, both wpa_cli (CLI app. for wpa_supplicant) and hostapd_cli (CLI app. for hostapd) provide 'wpa_pbc' command, which can emulate WPS physical button. Once wpa_pbc is run, AP advertises its WPS information through beacon. The default advertisement time is 2 minutes, so AP stops advertising once a connection is established or there is no connection established within 2 minutes. STA run with WPS-PBC can hear AP's adverting and do the WPS-PBC process to connect to AP. This process will be described in Clause 2.4 in detail

2.3 Configurartion file for wpa_supplicant and hostapd

Figure 1 shows some parameters that should be set in the configuration file on hostapd (AP) to support WPS. (Refer to ap_halow_pbc.conf in /nrc_pkg/script/conf/US/)

Hostapd uses those parameters while operating as a role of WPS Registrar

```
eap_server=1

# WPS configuration (AP configured, do not allow external WPS Registrars)
wps_state=2
ap_setup_locked=1

# If UUID is not configured, it will be generated based on local MAC address.
#uuid=87654321-9abc-def0-1234-56789abc0000
#wps_pin_requests=/var/run/hostapd.pin-req
device_name=NEWRATEK_WPS_PBC
manufacturer=NEWRATEK
model_name= NRCXXXX (Chip name)
model_number=1234
serial_number=4321
device_type=6-0050F204-1
os_version=01020300
config_methods=label display push_button keypad
```

Figure 1. Configuration for WPS-PBC of hostapd on AP

On STA side, there is no need to set parameters because STA earns AP's network configuration automatically during WPS procedures. AP's network information earned during WPS-PBC is stored in the configuration file in wpa_supplicant on STA.

2.4 WPS-PBC Procedure

WPS-PBC can be executed using start.py (in nrc_pkg) on both STA and AP where WPS-PBC is defined as 'security_mode type 4'. (e.g ./start.py 1 **4** US) Figure 2 ~ Figure 6 show the whole process of WPS-PBC.

1. (AP) Start AP and WPS Registrar, and then wait for STA's (Enrollee) connection

```
pi@raspberrypi:~/nrc_pkg/script $ ./start.py 1 4 US
------------------------------
Model            : 7292
STA Type         : AP
Security Mode    : WPA-PBC
Country Selected : US
Download FW      : uni_s1g.bin
TX Power         : 17
cal_use          : 1
------------------------------
NRC AP setting for HaLow...
[*] Set Max CPU Clock on RPi
1400000
1400000
1400000
1400000
Done
[0] Clear
wpa_supplicant: no process found
wireshark-gtk: no process found
[1] Copy
total 640
drwxr-xr-x 2 pi   pi     4096 Sep 15 14:44 .
drwxr-xr-x 4 pi   pi     4096 Sep 15 14:43 ..
-rwxr-xr-x 1 pi   pi      271 Sep 15 14:43 copy
-rwxr-xr-x 1 pi   pi      562 Sep 15 14:43 nrc7292_bd.dat
-rwxr-xr-x 1 pi   pi   316608 Sep 15 14:43 nrc7292_cspi.bin
-rwxr-xr-x 1 root root 316608 Sep 16 13:31 uni_s1g.bin
-rwxr-xr-x 1 root root 316608 Sep 16 13:31 /lib/firmware/uni_s1g.bin
-rw-r--r-- 1 root root 271464 Jan 28  2021 /lib/firmware/uni_s1g_sniffer.bin
====================================
 AP INTERFACE     : wlan0
 AP STATIC IP     : 192.168.200.1
 NET MASK NUM     : 24
====================================
Config for AP is done!
IP and DHCP config done
[2] Loading module
sudo insmod /home/pi/nrc_pkg/sw/driver/nrc.ko hifspeed=20000000 spi_bus_num=0 spi_cs_num=0 spi_gpio_irq=5 spi_g
pio_poll=-1 fw_name=uni_s1g.bin power_save=0 ndp_preq=1 auto_ba=1 disable_cqm=0
[3] Set tx power
Tx power : 17                  Calibration_use : ON
OK
Board Data use                  : off
OK
[4] Set aggregation number
------------------------------ updated aggregation ----------------------------------
AC       : BK           State    : OFF          Value    : 8            Size     : 0
AC       : BE           State    : ON           Value    : 8            Size     : 0
AC       : VI           State    : OFF          Value    : 8            Size     : 0
AC       : VO           State    : OFF          Value    : 8            Size     : 0
-------------------------------------------------------------------------------------
OK
[5] Set guard interval
guard interval : long
OK
[6] Set cal_use
Calibration_use : on                    Country  : ▒▒
OK
[*] Start DHCPCD and DNSMASQ
[6] Start hostapd on wlan0
Configuration file: /home/pi/nrc_pkg/script/conf/US/ap_halow_pbc.conf
wlan0: interface state UNINITIALIZED->COUNTRY_UPDATE
Using interface wlan0 with hwaddr 00:01:02:03:04:05 and ssid "halow_wps_test"
WPS: Converting display to virtual_display for WPS 2.0 compliance
WPS: Converting push_button to virtual_push_button for WPS 2.0 compliance
wlan0: interface state COUNTRY_UPDATE->ENABLED
wlan0: AP-ENABLED
Selected interface 'wlan0'
wlan0: WPS-PBC-ACTIVE
OK
```

Figure 2. Results of WPS-PBC on AP

2. (STA) Start STA and WPS Enrollee, and then try to get AP's configuration during the WPS-PBC process and connect to AP using it.

```
pi@raspberrypi:~/nrc_pkg/script $ ./start.py 0 4 US
------------------------------
Model            : 7292
STA Type         : STA
Security Mode    : WPA-PBC
Country Selected : US
Download FW      : uni_s1g.bin
TX Power         : 17
cal_use          : 1
Power Save Type  : Always On
------------------------------
NRC STA setting for HaLow...
[*] Set Max CPU Clock on RPi
1200000
1200000
1200000
1200000
Done
[0] Clear
hostapd: no process found
wireshark-gtk: no process found
[1] Copy
total 640
drwxrwxrwx 2 pi pi   4096 Sep 15 14:39 .
drwxrwxrwx 4 pi pi   4096 Sep 15 14:39 ..
-rwxrwxrwx 1 pi pi    271 Sep 15 14:39 copy
-rwxrwxrwx 1 pi pi    562 Sep 15 14:39 nrc7292_bd.dat
-rwxrwxrwx 1 pi pi 316608 Sep 15 14:42 nrc7292_cspi.bin
-rwxrwxrwx 1 pi pi 316608 Sep 16 13:34 uni_s1g.bin
-rwxr-xr-x 1 root root 316608 Sep 16 13:34 /lib/firmware/uni_s1g.bin
====================================
 STA INTERFACE    : wlan0
 USE DHCP Client
====================================
Config for STA is done!
IP and DHCP config done
[2] Loading module
sudo insmod /home/pi/nrc_pkg/sw/driver/nrc.ko hifspeed=20000000 spi_bus_num=0 spi_cs_num=0 spi_gpio_irq=5 spi_g
pio_poll=-1 fw_name=uni_s1g.bin power_save=0 ndp_preq=1 disable_cqm=0
[3] Set tx power
Tx power : 17                   Calibration_use : OFF
OK
OK
[4] Set aggregation number
-------------------------------- updated aggregation ----------------------------------
AC       : BK           State    : OFF          Value    : 8            Size     : 0
AC       : BE           State    : ON           Value    : 8            Size     : 0
AC       : VI           State    : OFF          Value    : 8            Size     : 0
AC       : VO           State    : OFF          Value    : 8            Size     : 0
---------------------------------------------------------------------------------------
OK
[5] Set guard interval
guard interval : long
OK
[6] Set cal_use
OK
[*] Start DHCPCD and DNSMASQ
wpa_supplicant: no process found
[6] Start wpa_supplicant on wlan0
Successfully initialized wpa_supplicant
Selected interface 'wlan0'
wlan0: WPS-PBC-ACTIVE
OK
[7] Connect and DHCP
Waiting for IP
wlan0: SME: Trying to authenticate with 00:01:02:03:04:05 (SSID='halow_wps_test' freq=5805 MHz)
wlan0: Trying to associate with 00:01:02:03:04:05 (SSID='halow_wps_test' freq=5805 MHz)
wlan0: Associated with 00:01:02:03:04:05
wlan0: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
wlan0: CTRL-EVENT-EAP-STARTED EAP authentication started
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=14122 method=1
wlan0: CTRL-EVENT-EAP-METHOD EAP vendor 14122 method 1 (WSC) selected
wlan0: WPS-CRED-RECEIVED
wlan0: WPS-SUCCESS
wlan0: CTRL-EVENT-EAP-FAILURE EAP authentication failed
wlan0: CTRL-EVENT-DISCONNECTED bssid=00:01:02:03:04:05 reason=3 locally_generated=1
wlan0: CTRL-EVENT-REGDOM-CHANGE init=CORE type=WORLD
wlan0: CTRL-EVENT-REGDOM-CHANGE init=USER type=COUNTRY alpha2=US
wlan0: SME: Trying to authenticate with 00:01:02:03:04:05 (SSID='halow_wps_test' freq=5805 MHz)
wlan0: Trying to associate with 00:01:02:03:04:05 (SSID='halow_wps_test' freq=5805 MHz)
wlan0: Associated with 00:01:02:03:04:05
wlan0: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
wlan0: WPA: Key negotiation completed with 00:01:02:03:04:05 [PTK=CCMP GTK=CCMP]
wlan0: CTRL-EVENT-CONNECTED - Connection to 00:01:02:03:04:05 completed [id=1 id_str=]
Waiting for IP
        inet 192.168.200.38  netmask 255.255.255.0  broadcast 192.168.200.255
IP assigned. HaLow STA ready
---------------------------------------------------------------------
Done.
```

Figure 3. Results of WPS-PBC on STA

3. (STA) Once STA earns AP's network configuration after WPS-PBC, it is saved in the configuration file of wpa_supplicant. STA can use it whenever (re)connecting to AP. Figure 4 shows network configuration of AP in sta_halow_pbc.conf (in nrc_pkg/script/US/)

```
network={
        ssid="halow_wps_test"
        psk="12345678"
        proto=RSN
        key_mgmt=WPA-PSK
        pairwise=CCMP-256 CCMP
        group=CCMP-256 CCMP TKIP
        auth_alg=OPEN
        pbss=2
}
```

Figure 4. Network Configuration after WPS-PBC on STA

4. (AP) After a connection during WPS-PBC or timeout (2 minutes) of WPS-PBC, AP can restart WPS-PBC again using hostapd_cli like 'sudo hostapd_cli wps_pbc'

```
pi@raspberrypi:~/nrc_pkg/script $ sudo hostapd_cli wps_pbc
Selected interface 'wlan0'
wlan0: WPS-PBC-ACTIVE
OK
```

Figure 5. Restart WPS-PBC by hostapd cli (wps_pbc)

5. (AP) If there is no WPS connection within 2 minutes, AP stop the WPS process

```
pi@raspberrypi:~/nrc_pkg/script $ wlan0: WPS-TIMEOUT
```

Figure 6. Timeout of WPS-PBC on AP

3 WPS-PBC operation (Standalone-mode)

Standalone-mode STA on NRC7394 EVK also supports WPS-PBC via CLI. However, Standalone-mode AP (aka. SoftAP) does NOT support WPS-PBC so you can test WPS-PBC operation with SAM STA and HM AP.

3.1 WPS-PBC Procedure

On Standalone-mode FW, WPS-PBC can be run via target CLI, 'wpa wps_pbc'. Figure 7 shows the whole procedures of WPS-PBC on STA. Please note that it takes more than 10 seconds to complete WPS-PBC because WPS uses the Diffie Helman algorithm to make the public key, plus the target CPU's performance (CM0 or CM3) is much lower than Host-mode CPU on RPi.

```
[4] 8066766 nrc7292_standalone_xip>wpa wps_pbc
WPA: Control interfawpa: ce responseFlush scan
 'OK' (2)
OKscn:
: 0 start0 start

[5] 14817264 nrc7292_standalone_xip>scn: 0 done
Unsupported channel(0). Change it to default (2442)
wim: 0 ch:5805, type:0, width:0
phy: 0 NRF TX GAIN CONTROL DONE(11)...
wim: 0 AID: 2
wim: 0 BSSID: 00:01:02:03:04:05
wim: 0 update short beacon interval in STA: 0
bmt: 0 set to default (100)
bmt: 0 start (bi:100, threshold:1500)
s1g: 0 update beacon interval(1000)
s1g: 0 listen_interval: 100 beacon_interval: 1000
s1g: 0 update short beacon interval(intv: 100)
s1g: 0 listen_interval: 100 short beacon_interval: 100
wpa_ps: 0 set key (mgmt:512, authorized:0)
wim: 0 AID: 2
wim: 0 BSSID: 00:00:00:00:00:00
wim: 0 update short beacon interval in STA: 0
bmt: 0 stop
STA is disconnected! Clear AP-related retent Info
wpa_ps: 0 set key (mgmt:512, authorized:0)
wpa: Flush scan
scn: 0 start
scn: 0 done
wpa: Flush scan
scn: 0 start
scn: 0 done
wpa: Flush scan
scn: 0 start
scn: 0 done
wim: 0 ch:5805, type:0, width:0
phy: 0 NRF TX GAIN CONTROL DONE(11)...
s1g: 0 (STA-assoc) akm type: 2
wim: 0 AID: 2
wim: 0 BSSID: 00:01:02:03:04:05
wim: 0 update short beacon interval in STA: 0
bmt: 0 set to default (100)
bmt: 0 start (bi:100, threshold:1500)
wim: 0 install key [PTK idx:0 aid:2 CCMP 00:01:02:03:04:05]
wim: 0 install key [GTK idx:1 aid:2 CCMP ff:ff:ff:ff:ff:ff]
wpa_ps: 0 set key (mgmt:2, authorized:1)
s1g: 0 update beacon interval(1000)
s1g: 0 listen_interval: 100 beacon_interval: 1000
s1g: 0 update short beacon interval(intv: 100)
s1g: 0 listen_interval: 100 short beacon_interval: 100
```

Figure 7. Results of WPS-PBC on SAM STA

4 Revision history

Revision No	Date	Comments
Ver 1.0	4/5/2023	Initial version