SCM1612
Wi-Fi 6 and BLE 5 Low-Power SoC

Single Board Smoke Test Guide

Version 1.1
Date 2023-08-15

Contact Information
Senscomm Semiconductor (www.senscomm.com)
Room 303, International Building, West 2 Suzhou Avenue,
SIP, Suzhou, China
For sales or technical support, please send email to
info@senscomm.com

Disclaimer and Notice

This document is provided on an “as-is” basis only. Senscomm reserves the right to make corrections, improvements and other changes to it or any specification contained herein without further notice.
All liability, including liability for infringement of any proprietary rights, relating to use of information in this document is disclaimed. No licenses express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.
All third party’s information in this document is provided as is with NO warranties to its authenticity and accuracy.
All trade names, trademarks and registered trademarks mentioned in this document are property of their respective owners and are hereby acknowledged.

Version History

Version	Date	Description
1.1	2023-08-15	Format Modification
1.0	2023-08-04	Version 1.0 Release
0.1	2023-07-19	Initial Draft

Table of Contents

1 Introduction

1.1 Smoke Testing

A smoke test is a preliminary test in the software development process, mainly for a quick basic functionality verification of the software version package, rather than in-depth testing. Before detailed testing, a smoke test is first performed to quickly check if there are any defects in the basic functions of the software. The smoke test mainly includes the Ping test and the Iperf test.

1.2 Ping Testing

Ping is a network testing tool mainly used to detect the quality of network connections. It sends ICMP response request messages to a specified network host and waits for its response to judge the stability of the network connection.

1.3 Iperf Testing

iPerf is a network performance testing tool that can measure the maximum bandwidth performance of TCP and UDP. It can test TCP or UDP traffic from one end to the other and provides information about network bandwidth, latency, jitter, and packet loss.

2 Smoke Test Software Compilation

2.1 Software Compilation Process

To perform a single-board smoke test, compile the corresponding software by following these steps:

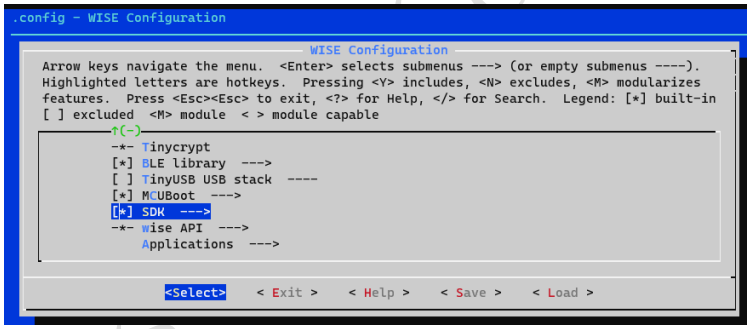
Step 1: Select the corresponding config, scm1612s_defconfig

```
$ cd wise-sdk
$ make distclean
$ make scm1612s_defconfig
```

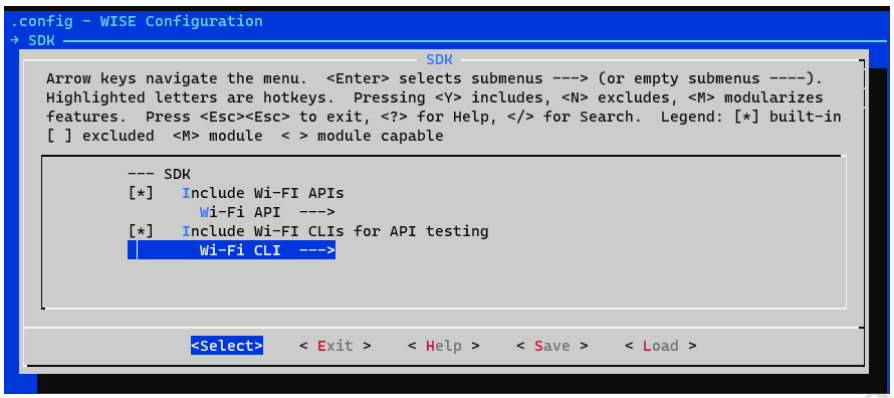
Step 2: Enable test functionalities

```
$ make menuconfig
```

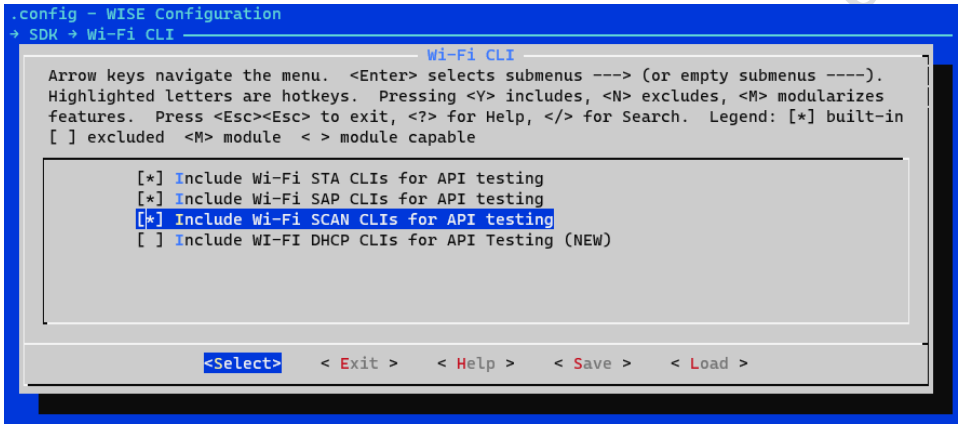
i. Enter SDK



ii. Check "Include Wi-Fi CLIs for API testing," then enter Wi-Fi CLI



iii. Select necessary features: STA, SCAN, SAP



Step 3: Compile

```
$ make
```

Step 4: Confirm that wise.mcuboot.bin is generated in the wise-sdk directory.

3 Wi-Fi STA Single-Board Smoke Test

3.1 Overview

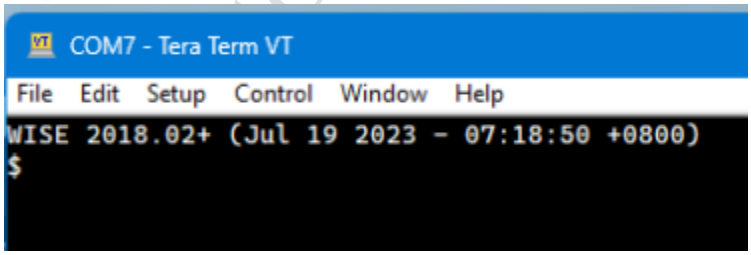
Any device that accesses a wireless AP can be called a station (STA: Station). The smoke test in STA mode mainly implements the connection with the AP device and conducts data communication.

3.2 Test Process

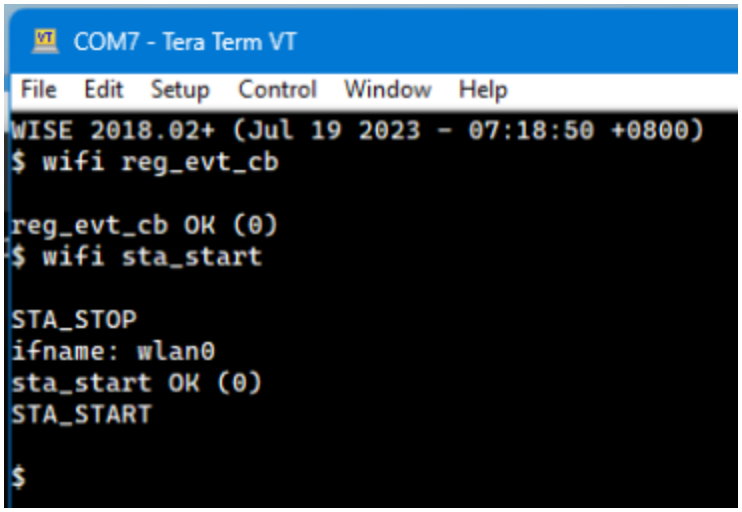
Through the wifi help command, the following command list can be displayed:

```
$ wifi help
wifi sta_cfg <ssid> <auth> <key> <bssid> <pairwise>
  or:  wifi sta_connect
  or:  wifi sta_disconnect
  or:  wifi sta_get_connect
  or:  wifi sta_set_reconnect
  or:  wifi sta_fast_connect <ssid> <auth> <bssid> <pairwise> <psk> <channel>
  or:  wifi sta_start
  or:  wifi sta_get_psk
  or:  wifi sta_scan
  or:  wifi sta_advance_scan <scan_type> <channel>|<ssid>|<bssid>
  or:  wifi sta_scan_results <max_ap_num>
  or:  wifi sap_start
  or:  wifi sap_stop
  or:  wifi sap_cfg <ssid> <key> <ch> <hidden> <auth> <pairwise>
  or:  wifi sap_beacon <interval>
  or:  wifi sap_dtim <period>
  or:  wifi sap_deauth <sta_mac>
  or:  wifi sap_show
  or:  wifi sap_showsta
  or:  wifi ip_set <ifn> <ip> [nm] [gw]
  or:  wifi dhcp_start/dhcp_stop
  or:  wifi dhcps_start/dhcps_stop
  or:  wifi reg_evt_cb
```

Step 1: Reset the single-board.



Step 2: Start STA



Step 3: Scan for networks.

```
$ wifi sta_scan
WiFi: Scan results available
sta_scan OK (0)
```

Step 4: View scan results.

```
$ wifi sta_scan_results 20
SSID: NFC                , CH: 6 , AUTH: wpa_psk
SSID: xiaomi2            , CH: 1 , AUTH: wep
SSID: SC-Ent             , CH: 1 , AUTH: wpa_psk
SSID: SC-Guest           , CH: 1 , AUTH: wpa_psk
SSID: SC-IoT             , CH: 1 , AUTH: wpa_psk
SSID: SC-Ent             , CH: 1 , AUTH: wpa_psk
SSID: xiaohu_test        , CH: 1 , AUTH: open
sta_scan_results OK (0)
```

Step 5: Configure network information for connection.

```
wifi sta_cfg TPTest 0 0 00:00:00:00:00:00 0 0
sta_cfg OK (0)
```

Step 6: Connect to the network.

```
$ wifi sta_connect
sta_connect OK (0)
$
STA_CONNECTED
AP SSID: TPTest
AP BSSID: ec:60:73:08:00:a8
AP CH: 11
AP RSSI: -8
Status: CONNECTED
```

Step 7: Start DHCP Client.

```
$ wifi dhcp_start
dhcp_start OK (0)
$
WIFI GOT IP
```

Step 8: View STA network information.

```
$ wifi sta_get_connect
AP SSID: Test_AP
AP BSSID: 8c:de:f9:b7:70:22
AP CH: 6
AP RSSI: -8
Status: CONNECTED
sta_get_connect OK (0)
$
```

Step 9: Perform ping test.

```
$ ping 192.168.31.1
PING 192.168.31.1 (192.168.31.1) 56(84) bytes of data.
64 bytes from 192.168.31.1 (192.168.31.1): icmp_seq=1 ttl=64 time=117.393 ms
64 bytes from 192.168.31.1 (192.168.31.1): icmp_seq=2 ttl=64 time=115.214 ms
64 bytes from 192.168.31.1 (192.168.31.1): icmp_seq=3 ttl=64 time=108.779 ms
64 bytes from 192.168.31.1 (192.168.31.1): icmp_seq=4 ttl=64 time=128.181 ms
```

Step 10: Perform iperf test.

```
$ iperf3 -c 192.168.31.43 -b 10m -u -t 30 -i 1
Connecting to host 192.168.31.43, port 5201
[ 10] local 0.0.0.0 port 62535 connected to 192.168.31.43 port 5201
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[ 10]   0.00-1.00   sec   687 KBytes  5.62 Mbits/sec  482
[ 10]   1.00-2.00   sec   699 KBytes  5.72 Mbits/sec  490
[ 10]   2.00-3.00   sec   696 KBytes  5.70 Mbits/sec  488
[ 10]   3.00-4.00   sec   689 KBytes  5.64 Mbits/sec  483
```

4 Wi-Fi AP Single-Board Smoke Test

4.1 Overview

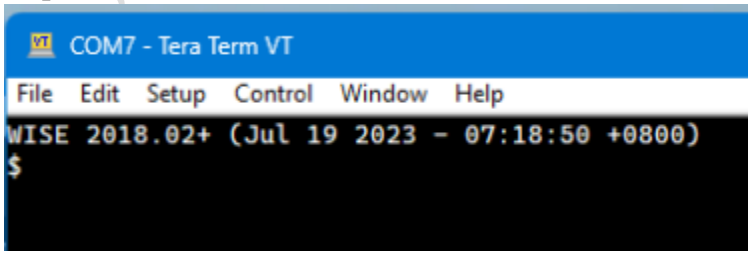
A Wireless Access Point (AP) is a key device in a wireless network. As a network interface, the AP can allow wireless devices to connect. It can also act as a wireless router, wireless gateway, wireless bridge, etc. In this AP mode smoke test, the single board acts as an AP device to communicate with the STA device.

4.2 Test Process

Through the wifi help command, the following command list can be displayed:

```
$ wifi help
wifi sta_cfg <ssid> <auth> <key> <bssid> <pairwise>
  or:  wifi sta_connect
  or:  wifi sta_disconnect
  or:  wifi sta_get_connect
  or:  wifi sta_set_reconnect
  or:  wifi sta_fast_connect <ssid> <auth> <bssid> <pairwise> <psk> <channel>
  or:  wifi sta_start
  or:  wifi sta_get_psk
  or:  wifi sta_scan
  or:  wifi sta_advance_scan <scan_type> <channel>|<ssid>|<bssid>
  or:  wifi sta_scan_results <max_ap_num>
  or:  wifi sap_start
  or:  wifi sap_stop
  or:  wifi sap_cfg <ssid> <key> <ch> <hidden> <auth> <pairwise>
  or:  wifi sap_beacon <interval>
  or:  wifi sap_dtim <period>
  or:  wifi sap_deauth <sta_mac>
  or:  wifi sap_show
  or:  wifi sap_showsta
  or:  wifi ip_set <ifn> <ip> [nm] [gw]
  or:  wifi dhcp_start/dhcp_stop
  or:  wifi dhcps_start/dhcps_stop
  or:  wifi reg_evt_cb
```

Step 1: Reset the single-board.



Step 2: Configure AP settings.

```
$ wifi sap_cfg SAP_test 12345678 6 0 2 1
sap_cfg OK (0)
$
```

Step 3: Start AP.

```
$ wifi sap_start
ifname: wlan1
sap_start OK (0)
$
AP_START
```

Step 4: Set IP address.

```
$ wifi ip_set wlan1 192.168.200.1
ip_set OK (0)
$ ifconfig
lo: flags=11<UP,BROADCAST,LOOPBACK>  mtu 2048  metric 0
        inet 127.0.0.1  netmask 255.0.0.0  broadcast 127.255.255.255
        ether 00:00:00:00:00:00  txqueuelen 0
        RX packets 228 dropped 0
        TX packets 228

wlan0: flags=100355<UP,BROADCAST,MULTICAST>  mtu 1500  metric 0
        inet 192.168.31.228  netmask 255.255.255.0  broadcast 192.168.31.255
        ether 64:f9:47:f0:01:20  txqueuelen 0
        RX packets 229 dropped 0
        TX packets 19718

wlan1: flags=100355<UP,BROADCAST,MULTICAST>  mtu 1500  metric 0
        inet 192.168.200.1  netmask 0.0.0.0  broadcast 255.255.255.255
        ether 66:f9:47:f0:01:20  txqueuelen 0
        RX packets 0 dropped 0
        TX packets 0
```

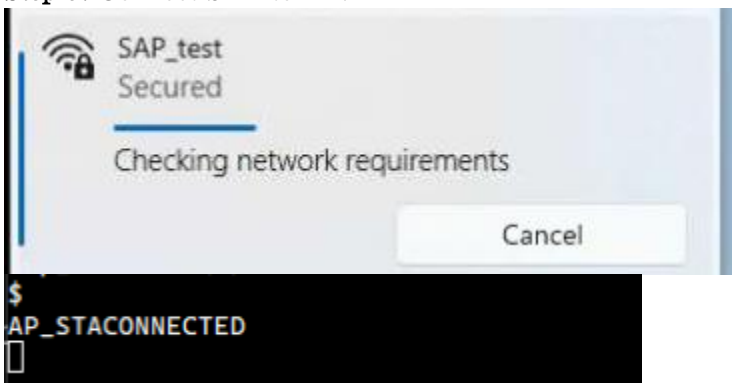
Step 5: Start DHCP server.

```
$ wifi dhcps_start
dhcps_start OK (0)
$
```

Step 6: View AP configuration.

```
$ wifi sap_show
SAP SSID: SAP_test
SAP KEY: 12345678
SAP CH: 6
SAP SSID Hidden: 0
SAP Auth Mode: 2
SAP Pairwise: 1
sap_show OK (0)
$
```

Step 7: Connect STA to AP.



Step 8: View STA information.

```
$ wifi sap_showsta
STA num: 1
STA addr:b0:fc:36:e1:af:c7
STA rssi: -14
STA rate: 0x86
sap_showsta OK (0)
$
```

Step 9: AP ping STA.

```
$ ping 192.168.200.2
PING 192.168.200.2 (192.168.200.2) 56(84) bytes of data.
64 bytes from 192.168.200.2 (192.168.200.2): icmp_seq=1 ttl=128 time=8.816 ms
64 bytes from 192.168.200.2 (192.168.200.2): icmp_seq=2 ttl=128 time=7.580 ms
64 bytes from 192.168.200.2 (192.168.200.2): icmp_seq=3 ttl=128 time=18.023 ms
64 bytes from 192.168.200.2 (192.168.200.2): icmp_seq=4 ttl=128 time=10.367 ms
64 bytes from 192.168.200.2 (192.168.200.2): icmp_seq=5 ttl=128 time=28.039 ms
```

Step 10: Perform Iperf test.

```
$ iperf3 -c 192.168.200.2 -b 10m -u -t 10 -i 1
Connecting to host 192.168.200.2, port 5201
[ 11] local 0.0.0.0 port 62525 connected to 192.168.200.2 port 5201
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[ 11]   0.00-1.00   sec   619 KBytes  5.07 Mbits/sec  434
[ 11]   1.00-2.00   sec   657 KBytes  5.38 Mbits/sec  461
[ 11]   2.00-3.00   sec   615 KBytes  5.04 Mbits/sec  431
[ 11]   3.00-4.00   sec   643 KBytes  5.26 Mbits/sec  451
[ 11]   4.00-5.00   sec   652 KBytes  5.34 Mbits/sec  457
[ 11]   5.00-6.00   sec   699 KBytes  5.72 Mbits/sec  490
```