UG453: RS9116W EVK User's Guide

Version 1.7

10/21/2020

Table of Contents

About this Document

This document covers the RS9116 Module's Evaluation Board (EVB) and its usage for evaluating Silicon Labs' RS9116 based ultra-low-power, single spatial stream, dual-band 802.11n + BT 5.0 Convergence modules in WiSeConnect® mode.

1 Overview

The RS9116 Module Evaluation Kit (EVK) is a platform for evaluating the RS9116 modules with multiple Host Processors/MCUs over interfaces like SPI, USB-CDC, UART . The EVK includes sample driver, supplicant, applications to test the following:

- Wireless Functionality for Wi-Fi, BT/BLE
- Security modes
- Throughputs
- Power Consumption
- Firmware Upgrade

The RS9116 WiSeConnect® module family is based on Silabs RS9116 ultra-low-power, single spatial stream, dual-band 802.11n + BT 5/BLE Convergence SoC. The RS9116 module integrates a multi-threaded MAC processor with integrated analog peripherals and support for digital peripherals, baseband digital signal processor, analog front-end, crystal oscillator, calibration OTP memory, dual-band RF transceiver, dual-band high-power amplifiers, baluns, diplexers, diversity switch and Quad-SPI Flash thus providing a fully-integrated solution for embedded wireless applications.

Note:

All the latest user-level Documents, Firmware Release packages, certifications of the module and other material related to the RS9116 based Modules are available.

For SDIO and USB Interface contact Silicon Labs for availability. https://www.silabs.com/about-us/contact-sales

1.1 The RS9116 WiSeConnect®

The WiSeConnect® module offers WLAN and Bluetooth protocols along with WPA/WPA2-PSK, WPA/WPA2-Enterprise (EAP-TLS, EAP-TTLS, PEAP-MS-CHAP-V2) and a feature-rich networking stack embedded in the device, thus providing a fully-integrated solution for embedded wireless applications. These modules can be interfaced to 8/16/32-bit host processors through SPI, UART, and USB-CDC interfaces.

2 Evaluation Kit Details

2.1 Evaluation Kit Part Numbers

2.1.1 Ordering Information for Evaluation Kits

Single Band - RS9116W-SB-EVK1
Dual-Band - RS9116W-DB-EVK1

2.1.2 Related Links

- https://www.silabs.com/wireless/wi-fi - Check for RS9116 Wi-Fi NCP Modules

2.2 Evaluation Kit Contents

The RS9116 Module Evaluation Kit comes with the following components:

1. RS9116 Module Evaluation Board
2. Micro A/B-type USB cable
3. SDIO Adaptor Cable
4. SPI Adaptor Cable

It is highly recommended to use the Micro A/B type USB cable that comes with the kit. If a longer cable is needed ensure that you use a USB-IF certified cable which can supply peak current of at least 500mA.

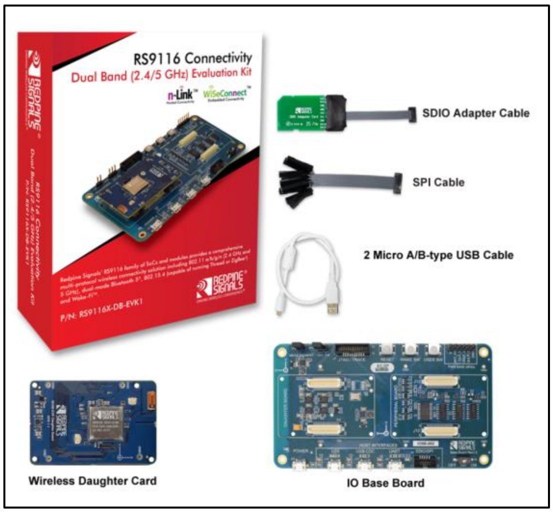


Figure 1: Evaluation Kit Contents

Latest EVK user guide, firmware and reference projects can be downloaded from our portal (www.silabs.com/development-tools/wireless/wi-fi/rs9116x-db-evk-development-kit). Please use the link (https://www.silabs.com/about-us/contact-sales) to contact our Sales Team.

3 Hardware Details

This section describes RS9116 EVB's various components and headers.
The OneBox-Embedded software for the WiSeConnect® modules supports UART, SPI, USB-CDC and USB interfaces to connect to the Host MCU.
As shown in the image below, the RS9116 EVB has four USB connectors for the Power, USB, USB-CDC and UART connections. The UART signals of the module are converted to USB using on-board circuit. The board also has an SDIO/SPI header.

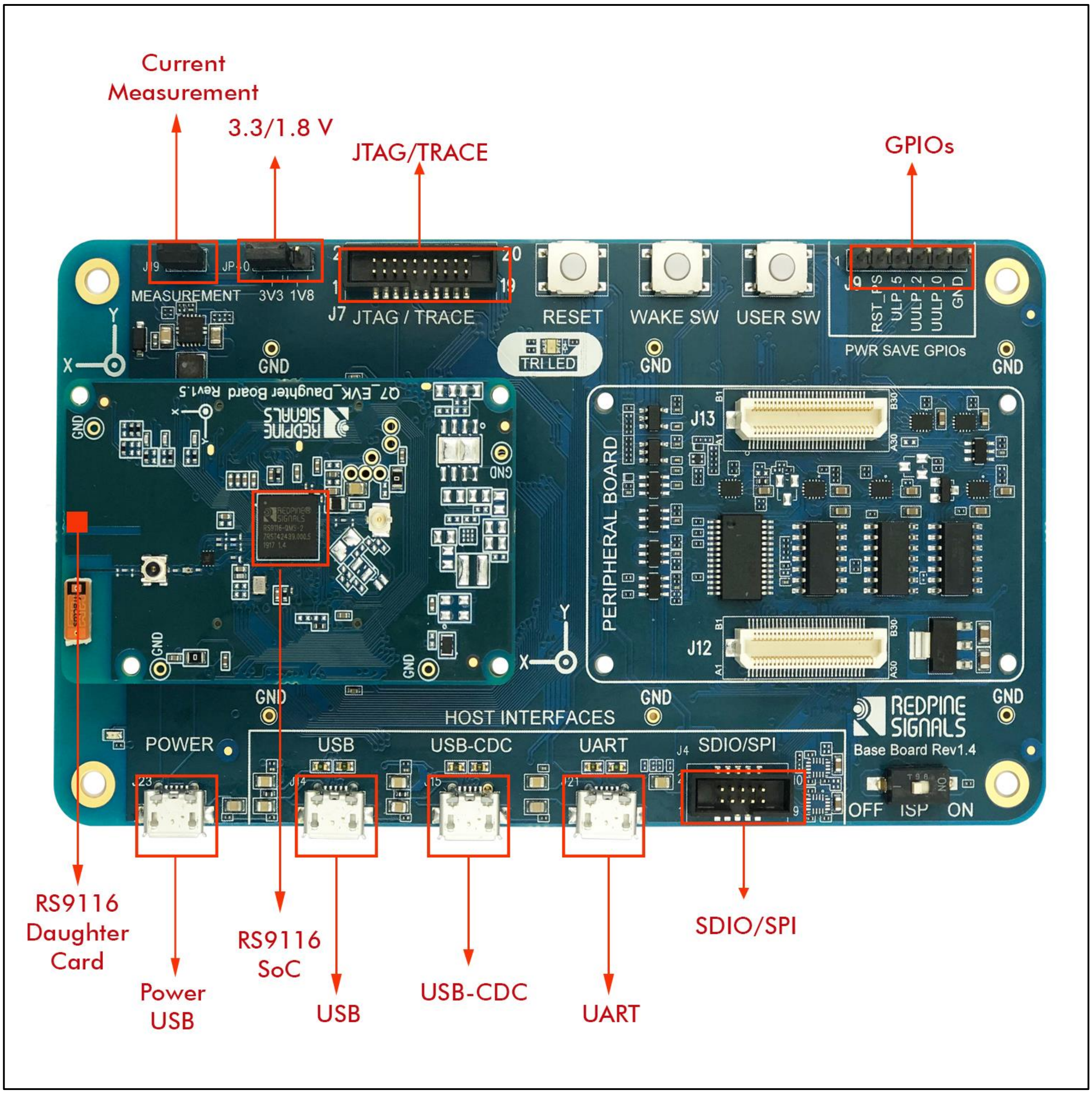


Figure 2: RS9116 EVB

The board is designed to configure the module to use the interface on which power supply is detected. The SDIO and SPI interfaces require the power supply to be provided over the POWER port using a USB cable. Hence, for these interfaces, it is required that the USB Power connection be provided first followed by the SDIO or SPI connection. Follow the steps below to use the EVB with different interfaces:

1. USB, UART, USB-CDC Modes
   a. Connect the Micro A/B-type USB cable between a USB port of a PC/Laptop and the micro-USB port labeled USB, UART or USB-CDC on the EVB.The USB, USB-CDC and UART connections also provide power, so only one USB cable needs to be connected.
2. SPI Mode

a. Connect the Micro A/B-type USB cable between a USB port of a PC/Laptop and the micro-USB port labeled POWER on the EVB.

b. Connect the 10-pin header of the SPI Adaptor Cable to the EVB. Connect the other wires of this connector to the SPI signals of a Host MCU platform. The details of the Header are given in Appendix A.

3. SDIO Mode

a. Connect the Micro A/B-type USB cable between a USB port of a PC/Laptop and the micro-USB port labeled POWER on the EVB.

b. Connect the 10-pin header of the SDIO Adaptor Cable to the EVB. Connect the other wires of this connector to the SDIO signals of a Host MCU platform. The details of the Header are given in Appendix A.

There is a 2-pin inline jumper available for measuring the current being sourced by the module during different stages of operation. This is labeled as "MEASUREMENT" on the baseboard. The user may connect a power meter or an ammeter to this jumper to measure the current.

Note: Assembly drawings of this EVB (Base Board and Daughter Board(CC1 and QMS)) are in Appendix E. Some of the critical parts' Reference Designators of this EVB are shown below.

- J19 - Power Measurement
- JP40 - Select between 3.3V or 1.8V supply voltage
- J7 - JTAG/TRACE header
- J9 - Power Save GPIOs
- J23 - Power to the EVK
- J14 - USB connection/Power
- J15 - USB-CDC connection/Power
- J21 - UART connection/Power
- J4 - SDIO/SPI header

Make sure the ISP switch is in the OFF state. If it is ON state you will not get the boot loader messages.

Important Note:
If the baseboard Rev is 1.1 or below then follow the below procedure:

1. For SDIO/SPI, insert the USB into the Power port first before the SDIO/SPI connector is connected to the Host platform
2. For USB and USB-CDC, please connect the USB port to the Host platform first before connecting the USB for the Power port.

4 Evaluation of WiSeConnect®

4.1 Introduction

The following table describes the available test methods for all supported interfaces on the RS9116 Evaluation board. It also explains the available software mechanisms to evaluate these.

INTERFACE	UART	SPI	SDIO	USB	USB-CDC
Accepted Commands	• AT Commands • Binary Commands (SAPI)	• Binary Commands (SAPI)	• Binary Commands (SAPI)	• Binary Commands (SAPI)	• AT Commands • Binary Commands (SAPI)
Evaluation Options	1. Using Terminal Applications on Windows/Linux using AT commands or Binary commands. 2. Using ready to run Reference projects on Linux. (Available as part of the release package) 3. Performing ABRD in host interaction mode is must for UART mode.	1. Using ready to run Reference projects on the STM Cortex M4 platform. (Available as part of the release package)	1. Ready to run Reference projects on Linux. (Available as part of the release package) 2. Using ready to run Reference projects on the Silabs RS12100 Cortex M4 platform. (Available as part of the release package)	1. Ready to run Reference projects on Linux. (Available as part of the release package)	1. Using Terminal Application on Windows/Linux using AT commands or Binary Commands. 2. Using ready to run Reference projects on Linux. (Available as part of the release package) 3. Performing ABRD in host interaction mode is must for USB-CDC mode.
NOTE: For a complete list of examples available as part of the package, refer to Appendix B.					

4.2 Required Setup

The required setup is illustrated in figures in the sub-sections below for evaluation in the following modes:

1. Wi-Fi Client in PersonalWi-Fi Client in Personal Security ModeSecurity Mode
2. Wi-Fi Client in Enterprise Security Mode
3. Wi-Fi Access Point Mode
4. BLE Evaluation using AT Commands
5. BT Evaluation in UART Mode
6. Wi-Fi + BLE Evaluation in UART Mode

Note:
This section describes the evaluation process of the RS9116 modules using the UART interface. To learn about the SAPI's for SPI, SDIO, USB, and USB-CDC, please view the reference projects and associated readmes included in the release package.

4.2.1 Third-Party Tools

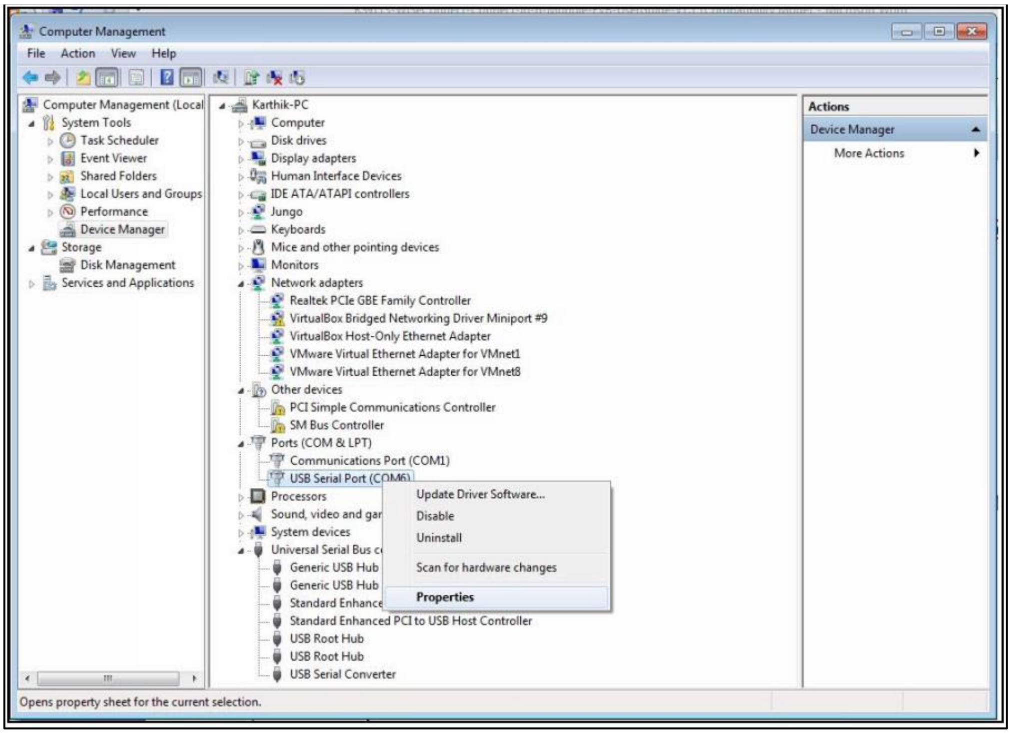
The following third-party tools maybe are required during your evaluation.

1. Docklight
2. Bluetooth SPP Manager (Android)
3. LightBlue Mobile Application (iOS)
4. SENA BTerm Mobile Application (Android)
5. nRF Connect Mobile Application (Android)

4.3 Getting Started

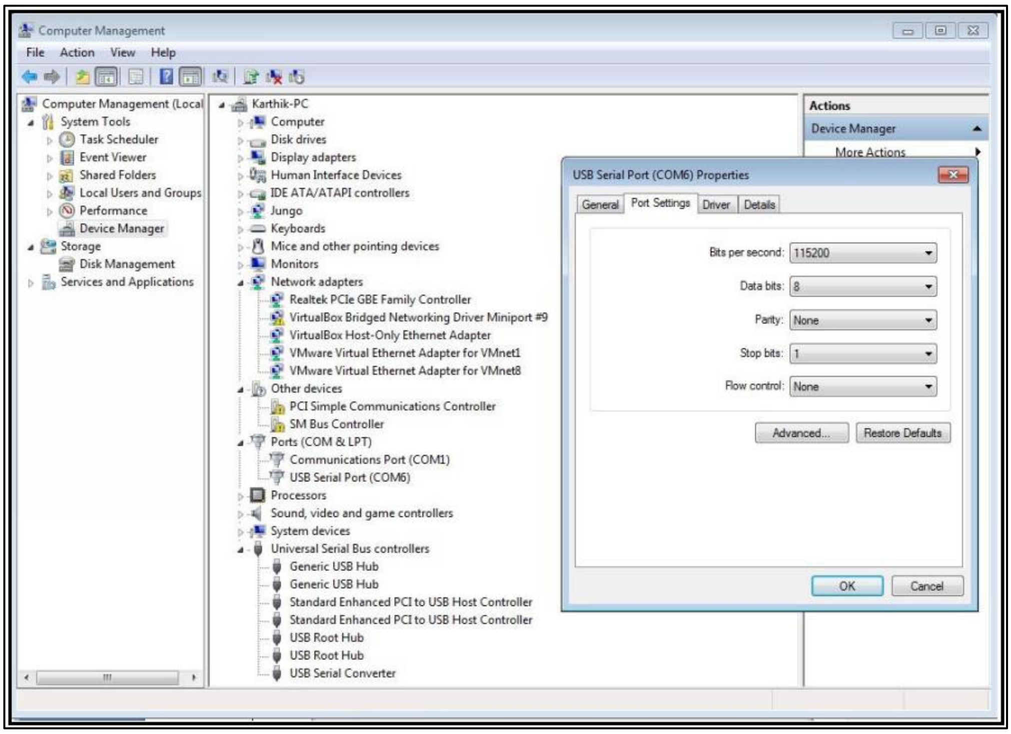
4.3.1 Installing Virtual COM Port Drivers

For UART communication, an FT232R USB-UART bridge is used on the EVB. This will enable a PC host to interface with the device using a USB cable.
Before working with the board, install virtual COM port drivers on the PC host. Detailed installation instructions are available for download from FTDI. The following link directs to the installation guides specific to PC operating systems. http://www.ftdichip.com/Support/Documents/InstallGuides.htm After the driver installation is done as per the guide, ensure the FT232R chip is configured to match with the default baud settings of the EVB. Baud rate setting and serial port settings can be configured from the device manager as shown in the following screen-shots. Navigate to the Device manager-> USB Serial Port(COMx) -> right-click and select "Properties".



Opens property sheet for the current selection.

After a click on the "Properties", one pop-up "USB Serial Port (COMx)" window is open, select the "Port Settings" tab as shown in the screenshot below.


Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Karthik-PC
Computer
Disk drives
Display adapters
Human Interface Devices
IDE ATA/ATAPI controllers
Jungo
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Realtek PCIe GBE Family Controller
VirtualBox Bridged Networking Driver Miniport #9
VirtualBox Host-Only Ethernet Adapter
VMware Virtual Ethernet Adapter for VMnet1
VMware Virtual Ethernet Adapter for VMnet8
Other devices
PCI Simple Communications Controller
SM Bus Controller
Ports (COM & LPT)
Communications Port (COM1)
USB Serial Port (COM6)
Processors
Sound, video and game controllers
System devices
Universal Serial Bus controllers
Generic USB Hub
Generic USB Hub
Standard Enhanced PCI to USB Host Controller
Standard Enhanced PCI to USB Host Controller
USB Root Hub
USB Root Hub
USB Serial Converter
Actions
Device Manager
More Actions
USB Serial Port (COM6) Properties
General
Port Settings
Driver
Details
Advanced...
Restore Defaults
OK
Cancel

Bits per second: 115200
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

Configure the "Port Settings" as mentioned below.
Baud rate: 115200
Data bits: 8
Parity: None
Stop bits: 1
Flow Control: None

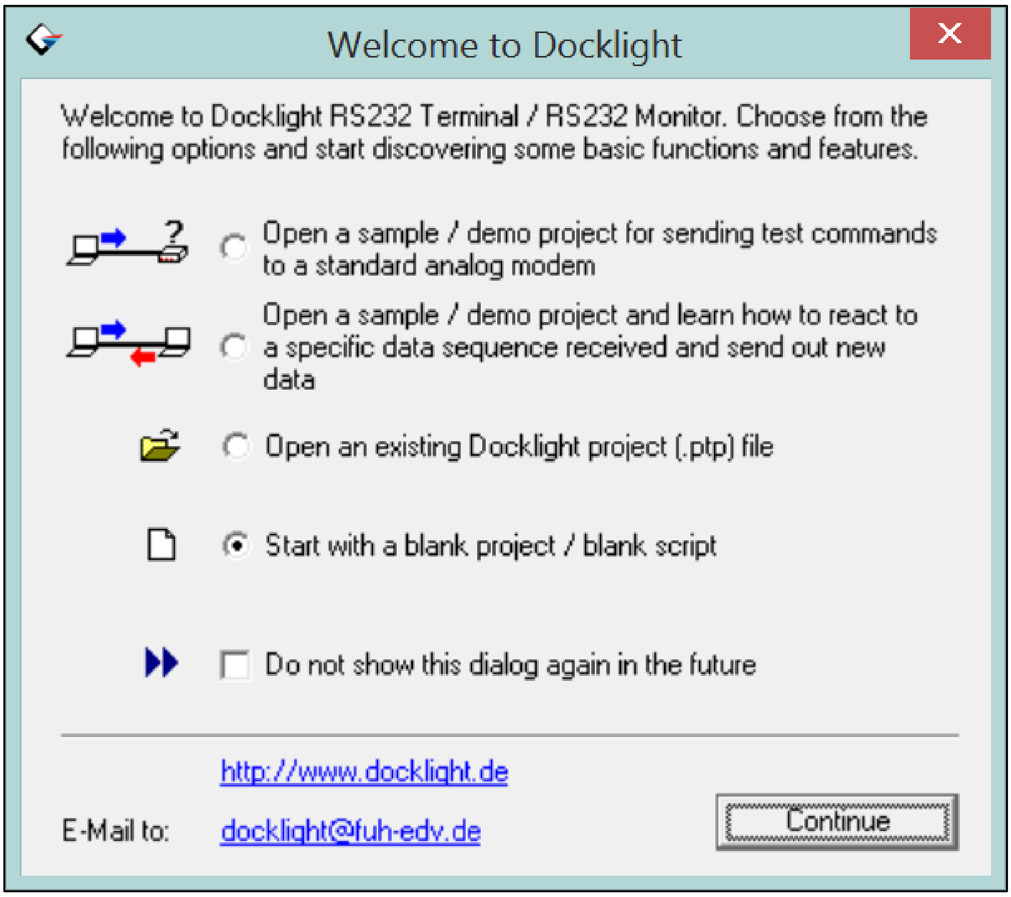
4.3.2 Installing Tools to evaluate over the UART interface

AT Mode over UART interface: Installing and Using Docklight on Windows

4.3.2.1 Installing and Using Docklight on Windows

Please follow the steps below to get started with the evaluation process. This process is explained for evaluation on a Windows PC.

1. Download and install a Serial Emulation program like Docklight, Teraterm, etc. This document uses Docklight for explaining the process. This software is relatively easy to use and allows the user to monitor the serial port data while also enabling sending and receiving data. However, since it does not support the sending of files using Kermit, it cannot be used to upgrade the firmware of the module. For firmware up-gradation, we suggest Teraterm. The process for firmware upgradation is explained in Appendix C. Docklight can be downloaded from http://www.docklight.de/download_en.htm
2. Open Docklight and click OK when asked for Registration, to use it in Evaluation mode.
3. In the dialog box that opens, select "Start with a blank project / blank script" and click Continue.



Welcome to Docklight

Welcome to Docklight RS232 Terminal / RS232 Monitor. Choose from the following options and start discovering some basic functions and features.

○ Open a sample / demo project for sending test commands to a standard analog modem

○ Open a sample / demo project and learn how to react to a specific data sequence received and send out new data

○ Open an existing Docklight project (.ptp) file

● Start with a blank project / blank script

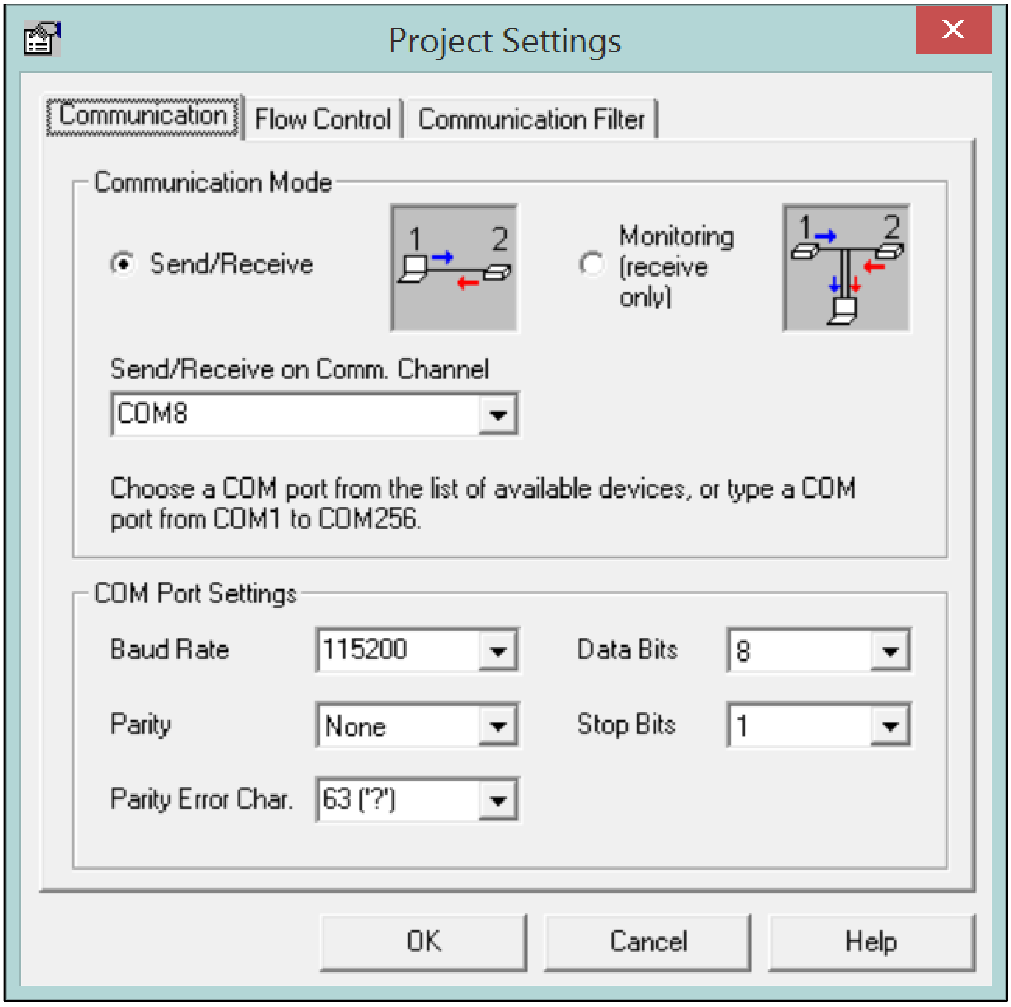
□ Do not show this dialog again in the future

http://www.docklight.de

E-Mail to: docklight@fuh-edv.de

Figure 3: Docklight Startup Dialog Box

4. Next, connect the EVB to the PC using the Micro A/B-type USB cable. Plugin the cable into the micro-USB port labeled "UART" on the EVB.
5. Wait for the drivers to be installed the first time. Disconnect the EVB and connect it again.
   In Docklight, click on Tools -> Project Settings to open the dialog box shown below.



Communication Mode

● Send/Receive ○ Monitoring (receive only)

Send/Receive on Comm. Channel: COM8

Choose a COM port from the list of available devices, or type a COM port from COM1 to COM256.

COM Port Settings

Baud Rate	115200	Data Bits	8
Parity	None	Stop Bits	1
Parity Error Char.	63 ('?')		

Figure 4: Docklight Project Settings Dialog Box

1. Select the following options for the Serial port settings:
   a. Select the COM port in the drop-down menu under "Send/Receive on Comm. Channel". In the above figure, it is COM8.
   b. Select the Baud Rate as 115200.
   c. Click OK.

Note

- *For a complete list of examples available as part of the package, refer to Appendix B.*
- *An Independent user guide for each example is available in the project directory itself.*

4.3.3 Check the Firmware version running on your Evaluation Board

Once you have the drivers installed and are ready to use the Evaluation board, we recommend you to check the firmware version running on the board. Ensure to verify that this is the latest and the greatest firmware released by Silicon labs. Click this link to check the latest software in "Tools & Software" www.silabs.com/development-tools/wireless/wi-fi/rs9116x-db-evk-development-kit

Please use the link (https://www.silabs.com/about-us/contact-sales) to contact our sales.

AT Command: at+rsi_fwversion?/r/n
Binary API: rsi_wlan_get(RSI_FW_VERSION,*response, sizeof(response));

4.3.4 Introduction to Command Types

4.3.4.1 AT+ Commands

The Wi-Fi AT command set represents the frames that are sent from the Host to operate the RS9116-WiSeConnect Module. The command set resembles the standard AT command interface used for modems.
All AT commands start with "at" and are terminated with a carriage return('\r') and a new line('\n') character.
The AT command set for the RS9116-WiSeConnect Module starts with "at+rsi_" followed by the name of the command and any relevant parameters.
In some commands, a '?' character is used after the command to query data from the module.

4.3.4.2 Binary Commands (SAPI)

The Wi-Fi configuration and operation commands are sent to the module and the responses are read from the module using frame write/frame read (as mentioned in the preceding sections) so these configuration and operation commands are called command frames. The command frame is categorized as management or data frames. The management frames are used to configure the Wi-Fi module to access Wi-Fi connectivity, TCP/IP stack, and operate the module. Data frames are used to send the data. Management and data frames are exchanged between the host and the module. The management frame is sent from the Host to the module to configure the module, and also is sent from the module to the host to send responses to these commands.

4.4 Wi-Fi Evaluation in UART Mode

The following sub-sections describe configuring and using the module in different security and operational modes of Wi-Fi.

4.4.1 Wi-Fi Evaluation using AT Commands

4.4.1.1 Wi-Fi Client in Personal Security Mode

The figure below shows the setup required for this process.

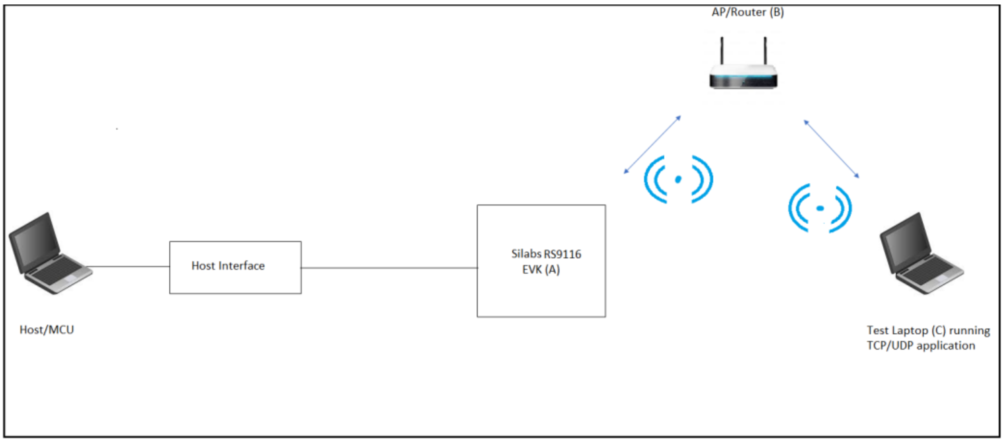
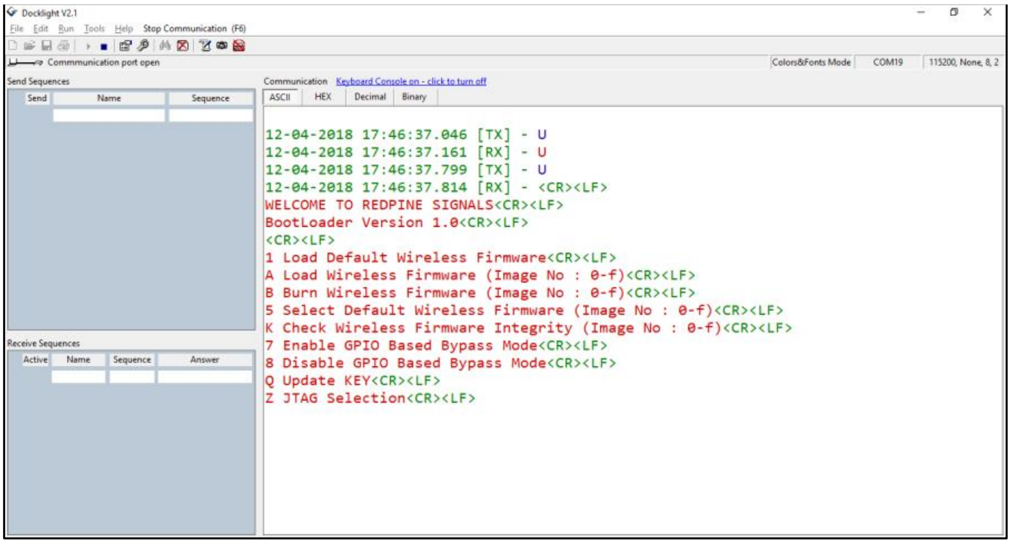


Figure 5: Setup for Wi-Fi Client in Personal Security Mode

In the setup shown in the figure, the RS9116 WiSeConnect EVB is a Wi-Fi client. It connects to an Access Point configured in WPA2-PSK security mode. The Access Point is configured with SSID as "Test_AP" and IP address set as 192.168.50.1. The SSID and IP address are for illustration only. The user is required to configure the AP based on the network domain in which wireless devices operate.

4.4.1.1.1 Wi-Fi Client Configuration

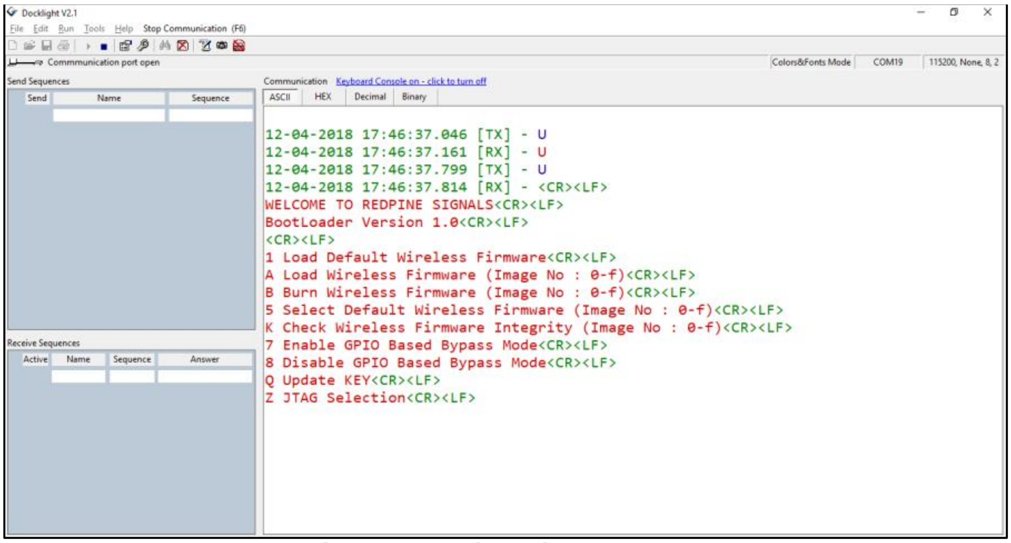
1. Open Docklight.
2. Connect the Micro A/B-type USB cable between the USB port of the PC and the micro-USB port of the EVB labeled "UART".
3. Hit the "F5" key when in the Docklight window to start communicating with EVB.
4. At power-up, the module tries to estimate the baud rate of the Host by exchanging data with it. Please refer to the Software PRM document to understand the Automatic Baud Rate Detection Process for faster bootup. (Shift+ |) then (Shift + U) will do the ABRD process and you will see the boot up message. Please see the figure below.



```
12-04-2018 17:46:37.046 [TX] - U
12-04-2018 17:46:37.161 [RX] - U
12-04-2018 17:46:37.799 [TX] - U
12-04-2018 17:46:37.814 [RX] - <CR><LF>
WELCOME TO REDPINE SIGNALS<CR><LF>
BootLoader Version 1.0<CR><LF>
<CR><LF>
1 Load Default Wireless Firmware<CR><LF>
A Load Wireless Firmware (Image No : 0-f)<CR><LF>
B Burn Wireless Firmware (Image No : 0-f)<CR><LF>
5 Select Default Wireless Firmware (Image No : 0-f)<CR><LF>
K Check Wireless Firmware Integrity (Image No : 0-f)<CR><LF>
7 Enable GPIO Based Bypass Mode<CR><LF>
8 Disable GPIO Based Bypass Mode<CR><LF>
Q Update KEY<CR><LF>
Z JTAG Selection<CR><LF>
```

Figure 6: Module Startup Messages

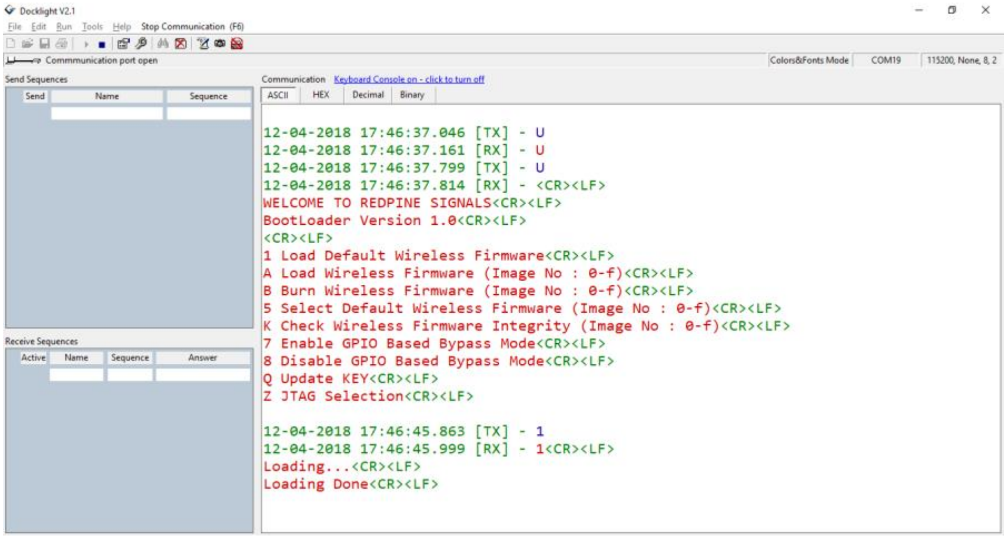
5. Make sure to click on the "Keyboard Console On/Off" button as shown in the figure below to enable keyboard inputs to Docklight.



```
12-04-2018 17:46:37.046 [TX] - U
12-04-2018 17:46:37.161 [RX] - U
12-04-2018 17:46:37.799 [TX] - U
12-04-2018 17:46:37.814 [RX] - <CR><LF>
WELCOME TO REDPINE SIGNALS<CR><LF>
BootLoader Version 1.0<CR><LF>
<CR><LF>
1 Load Default Wireless Firmware<CR><LF>
A Load Wireless Firmware (Image No : 0-f)<CR><LF>
B Burn Wireless Firmware (Image No : 0-f)<CR><LF>
5 Select Default Wireless Firmware (Image No : 0-f)<CR><LF>
K Check Wireless Firmware Integrity (Image No : 0-f)<CR><LF>
7 Enable GPIO Based Bypass Mode<CR><LF>
8 Disable GPIO Based Bypass Mode<CR><LF>
Q Update KEY<CR><LF>
Z JTAG Selection<CR><LF>
```

Figure 7: Keyboard Console On

6. Hit '1' and press Enter. You will see a message that says, "Loading…" followed by "Loading Done".



```
12-04-2018 17:46:37.046 [TX] - U
12-04-2018 17:46:37.161 [RX] - U
12-04-2018 17:46:37.799 [TX] - U
12-04-2018 17:46:37.814 [RX] - <CR><LF>
WELCOME TO REDPINE SIGNALS<CR><LF>
BootLoader Version 1.0<CR><LF>
<CR><LF>
1 Load Default Wireless Firmware<CR><LF>
A Load Wireless Firmware (Image No : 0-f)<CR><LF>
B Burn Wireless Firmware (Image No : 0-f)<CR><LF>
5 Select Default Wireless Firmware (Image No : 0-f)<CR><LF>
K Check Wireless Firmware Integrity (Image No : 0-f)<CR><LF>
7 Enable GPIO Based Bypass Mode<CR><LF>
8 Disable GPIO Based Bypass Mode<CR><LF>
Q Update KEY<CR><LF>
Z JTAG Selection<CR><LF>

12-04-2018 17:46:45.863 [TX] - 1
12-04-2018 17:46:45.999 [RX] - 1<CR><LF>
Loading...<CR><LF>
Loading Done<CR><LF>
```

Figure 8: Firmware Loading Messages

7. The following commands can now be issued to the module. Please refer to the Software PRM document for a detailed description of each command and the expected responses. A command should not be sent until the response for the previous command is received.

NOTE: Each AT command should have a suffix of Carriage Return <CR> (Keyboard keys are Ctrl+Enter) and Line Feed <LF> (Keyboard keys are Ctrl+Shift+Enter). This is enabled by default in Docklight.

- at+rsi_opermode=0,1,4,0

This command configures the module as a Wi-Fi client. The module responds with "OK"

- at+rsi_band=0

This command configures the operating band of the Wi-Fi client to 2.4GHz. The module responds with "OK"

- at+rsi_init

This command initializes the Wi-Fi module in the EVB. The module responds with OK<MAC_Address>.

- at+rsi_fwversion?

This command displays the current firmware version in use.

- at+rsi_scan=0

This command scans for available Access Points operating in the 2.4 GHz band. The module responds with information of the Access Points scanned. The data received might have some unreadable characters because of ASCII conversion. You can use the HEX tab of Docklight to see the bytes sent by the module.

- at+rsi_psk=1,12345678

This command configures the PSK of the Wi-Fi client with the key entered by the user. The User can enter any other key as PSK.

- at+rsi_join=Test_AP,0,2,2

This command connects the Wi-Fi client to the Access Point with SSID "Test_AP". On successful association, the module responds with OK.

- at+rsi_ipconf=0,192.168.50.10,255.255.255.0,192.168.50.1

at+rsi_ipconf=1,0,0,0
This command configures the IP address of the module. The IP address configured in the above command is for illustration only. The user has to configure the IP address as per the Access Point's settings using either Manual (first command above) or DHCP mode (second command above).
For the Manual mode, ensure that the desired IP is in the same subnet as the Access Point's subnet. The module responds to this command by sending the configured IP address to the Host. In the terminal, this response might appear as unreadable characters because of ASCII conversion. You can use the HEX tab of Docklight to see the bytes sent by the module.

4.4.1.1.2 Test Procedure

The IP addresses configured in this process are meant for illustration only. It is assumed that the Wi-Fi client of the EVB is assigned an IP address of 192.168.50.10 and Laptop C, connected to the Access Point is assigned an IP address of 192.168.50.20.
The applications provided in the USB drive (as part of the release package) send and receive TCP and UDP packets. TCP and UDP applications are provided along with a release package for execution on the Laptop. These applications are located in the path RS9116.NBZ.WC.GEN.OSI.x.x.x\utils\peer_applications\Windows where RS9116.NBZ.WC.GEN.OSI.x.x.x is a software package directory.

1. Open a TCP Server socket on the Wi-Fi Client (EVB) side using the following AT command:

   at+rsi_ltcp=5001,1,0

   The module's response will look as follows:

   OK<ip_version><socket_type><socket_handle><Lport><module_ipaddr>\r\n
   The socket_handle in the response above is used for subsequent commands.

2. Open a TCP client socket on Laptop C by running the TCP.exe application as follows in the Windows Command Prompt:

   AT+RSI_LTCP_CONNECT=<ip_version><socket_descriptor><dest_port_no><dest_ipaddr><mss><window_size><src_port_no>\r\n

   a. For testing the Receive mode of the Wi-Fi Client (EVB), follow the steps below:

b. Type 1 in the TCP.exe window on Laptop C.

c. On being prompted to enter a data string to be transmitted, type any string and hit Enter to transmit the typed data.

d. When the data is received on the Wi-Fi Client (EVB) side, you will see a response (asynchronous) from the module as follows:

AT+RSI_READ<ip_version><socket_handle><payload_len><source_ip_addr><source_port><payload>

a. For testing the Transmit mode of the Wi-Fi Client (EVB), follow the steps below:

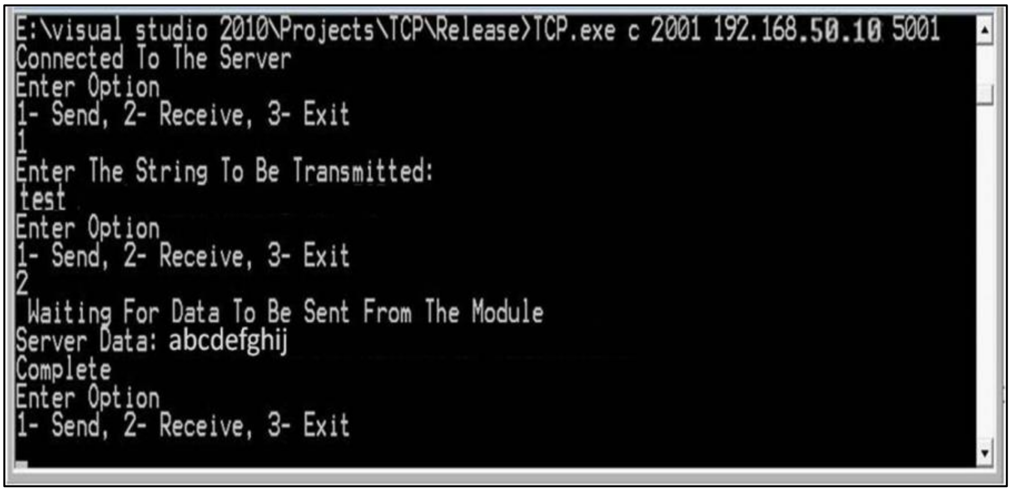
b. Type 2 in the TCP.exe window on Laptop C.

c. On the Wi-Fi Client (EVB) side, send the command below to transmit data to the Laptop C.

at+rsi_snd=<socket_handle>,<payload_len>,<dest_ipaddr>,<dest_port>,<payload >

a. The transmitted data is displayed on the TCP.exe window of Laptop C.

b. The figure below is a snapshot of the TCP.exe application window



```
E:\visual studio 2010\Projects\TCP\Release>TCP.exe c 2001 192.168.50.10 5001
Connected To The Server
Enter Option
1- Send, 2- Receive, 3- Exit
1
Enter The String To Be Transmitted:
test
Enter Option
1- Send, 2- Receive, 3- Exit
2
 Waiting For Data To Be Sent From The Module
Server Data: abcdefghij
Complete
Enter Option
1- Send, 2- Receive, 3- Exit
```

Figure 9: TCP Application Window

4.4.1.2 Wi-Fi Client in Enterprise Security Mode

The figure below shows the setup required for this process.

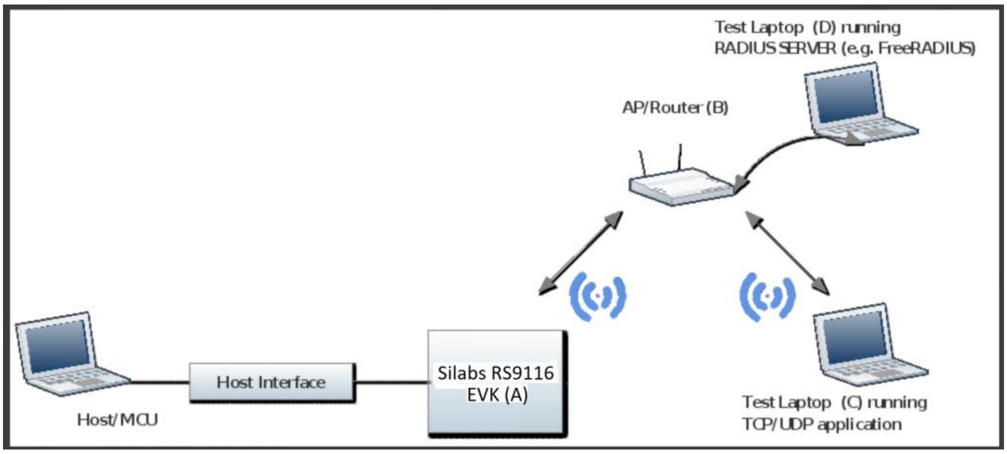


Figure 10: Setup for Wi-Fi Client in Enterprise Security Mode

In the setup shown in the above figure, the WiSeConnect® module on the RS9116 EVB acts as a Wi-Fi client. It connects to an Enterprise Security enabled Access Point. The WiSeConnect® module supports four Enterprise Security modes:

1. EAP-TLS
2. EAP-TTLS

3. EAP-PEAP

4.4.1.2.1 Radius Server Configuration

Follow the steps below to set up a Radius Server on Laptop D as per the setup shown in Figure 10(see above). The process explained here is for a Windows Laptop. A similar process may be followed for other OS.

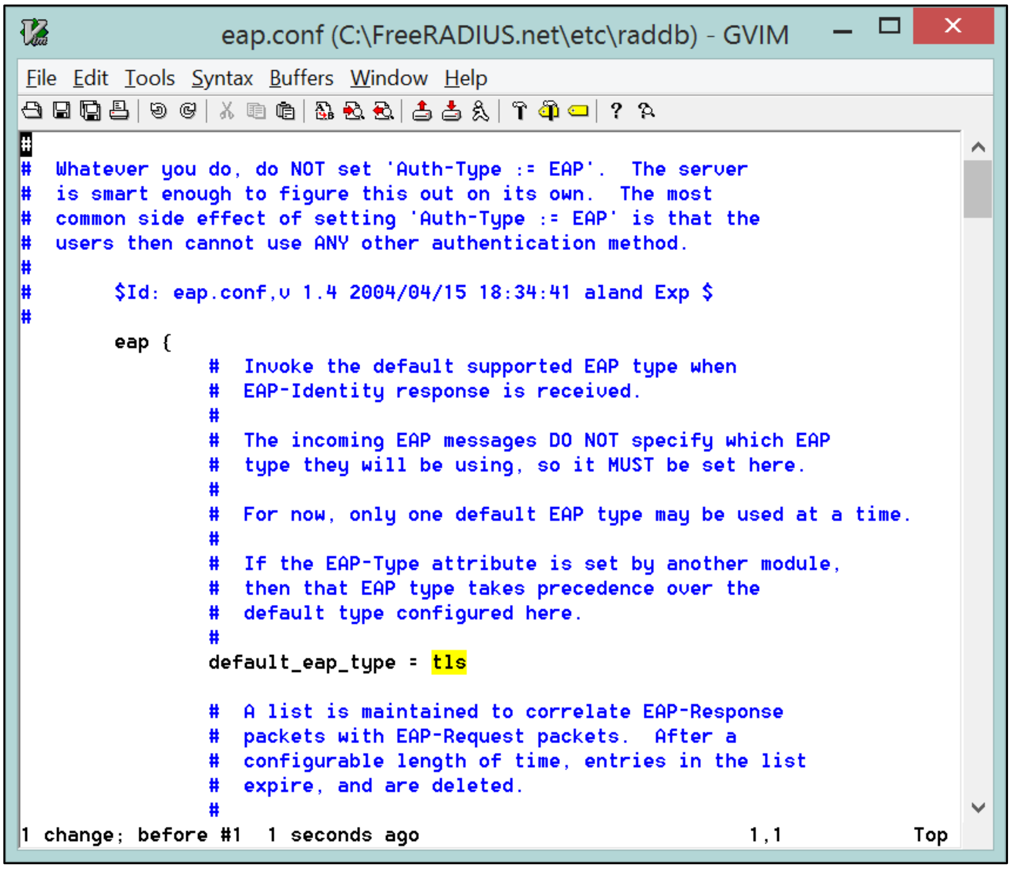
Download and install the FreeRADIUS server version 2.2.3 or above. The FreeRADIUS server software is available at http://freeradius.org/older_releases/ (for Windows installation file please contact our support and we can share through FTP).

1. Once installed, go to the C:\FreeRADIUS\etc\raddb folder and make the following modifications.
2. Open the clients.conf file and add the following lines at the end of the file.

```
client 192.168.50.1/24 {
secret=12345678
shortname=private-network-1
}
```

The IP address in the above lines (192.168.50.1) is the IP address of the Access Point in this example setup. The "12345678" input is the key to be entered in the Access Point's configuration to authenticate it with the Radius Server.

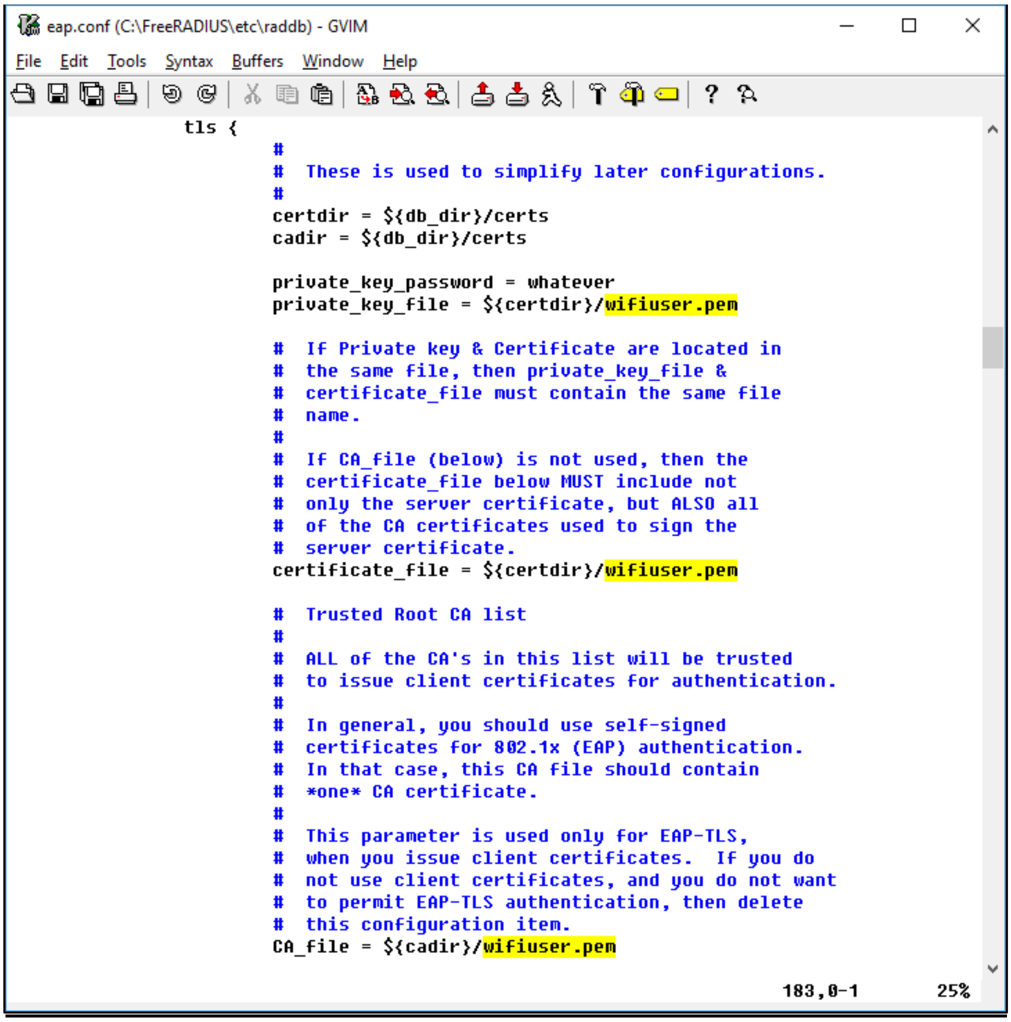
1. Open the eap.conf file and make the following changes:
   a. Change the input for the "default_eap_type" field under the "eap" section to "tls", as shown in the figure below.


eap.conf (C:\FreeRADIUS.net\etc\raddb) - GVIM
File Edit Tools Syntax Buffers Window Help

```
#
#  Whatever you do, do NOT set 'Auth-Type := EAP'.  The server
#  is smart enough to figure this out on its own.  The most
#  common side effect of setting 'Auth-Type := EAP' is that the
#  users then cannot use ANY other authentication method.
#
#       $Id: eap.conf,v 1.4 2004/04/15 18:34:41 aland Exp $
#
        eap {
                #  Invoke the default supported EAP type when
                #  EAP-Identity response is received.
                #
                #  The incoming EAP messages DO NOT specify which EAP
                #  type they will be using, so it MUST be set here.
                #
                #  For now, only one default EAP type may be used at a time.
                #
                #  If the EAP-Type attribute is set by another module,
                #  then that EAP type takes precedence over the
                #  default type configured here.
                #
                default_eap_type = tls

                #  A list is maintained to correlate EAP-Response
                #  packets with EAP-Request packets.  After a
                #  configurable length of time, entries in the list
                #  expire, and are deleted.
                #
1 change; before #1  1 seconds ago                        1,1          Top
```

Figure 11: Default EAP Type

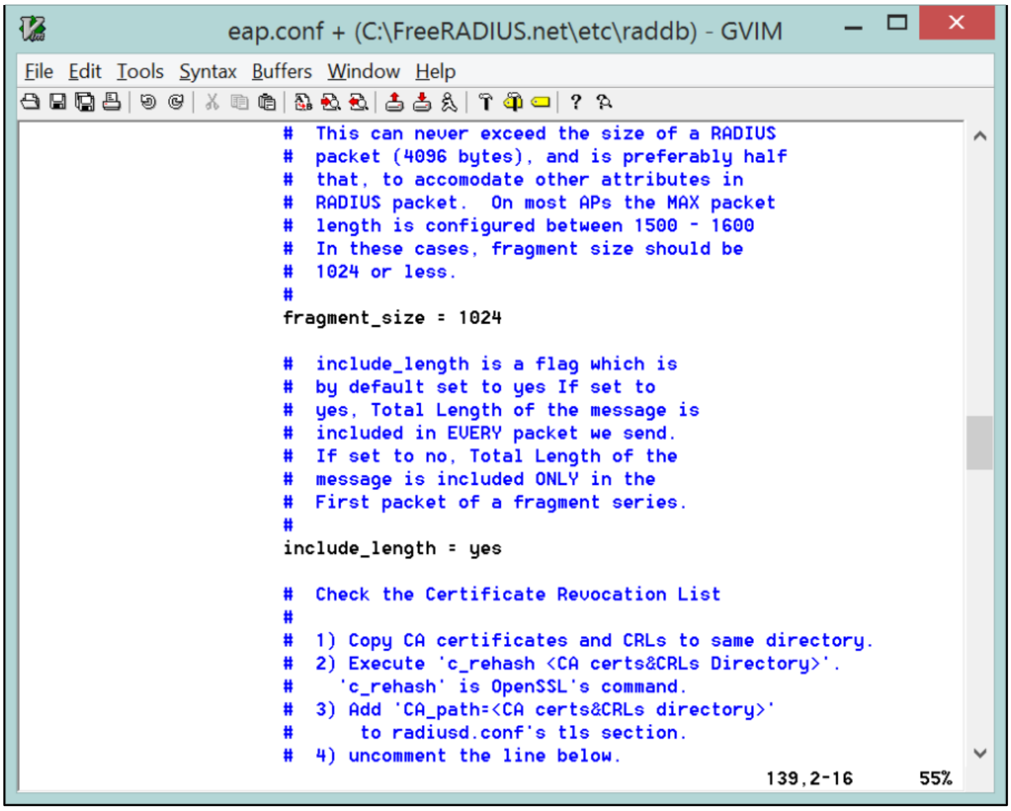
2. Change the inputs for "private_key_file", "certificate_file" and "CA_file" fields under the "tls" section to "${certdir}/wifiuser.pem", as show in the figure below.


eap.conf (C:\FreeRADIUS\etc\raddb) - GVIM
File Edit Tools Syntax Buffers Window Help
183,0-1 25%

```
                tls {
                        #
                        #  These is used to simplify later configurations.
                        #
                        certdir = ${db_dir}/certs
                        cadir = ${db_dir}/certs

                        private_key_password = whatever
                        private_key_file = ${certdir}/wifiuser.pem

                        #  If Private key & Certificate are located in
                        #  the same file, then private_key_file &
                        #  certificate_file must contain the same file
                        #  name.
                        #
                        #  If CA_file (below) is not used, then the
                        #  certificate_file below MUST include not
                        #  only the server certificate, but ALSO all
                        #  of the CA certificates used to sign the
                        #  server certificate.
                        certificate_file = ${certdir}/wifiuser.pem

                        #  Trusted Root CA list
                        #
                        #  ALL of the CA's in this list will be trusted
                        #  to issue client certificates for authentication.
                        #
                        #  In general, you should use self-signed
                        #  certificates for 802.1x (EAP) authentication.
                        #  In that case, this CA file should contain
                        #  *one* CA certificate.
                        #
                        #  This parameter is used only for EAP-TLS,
                        #  when you issue client certificates.  If you do
                        #  not use client certificates, and you do not want
                        #  to permit EAP-TLS authentication, then delete
                        #  this configuration item.
                        CA_file = ${cadir}/wifiuser.pem
```

Figure 12: TLS Section - I

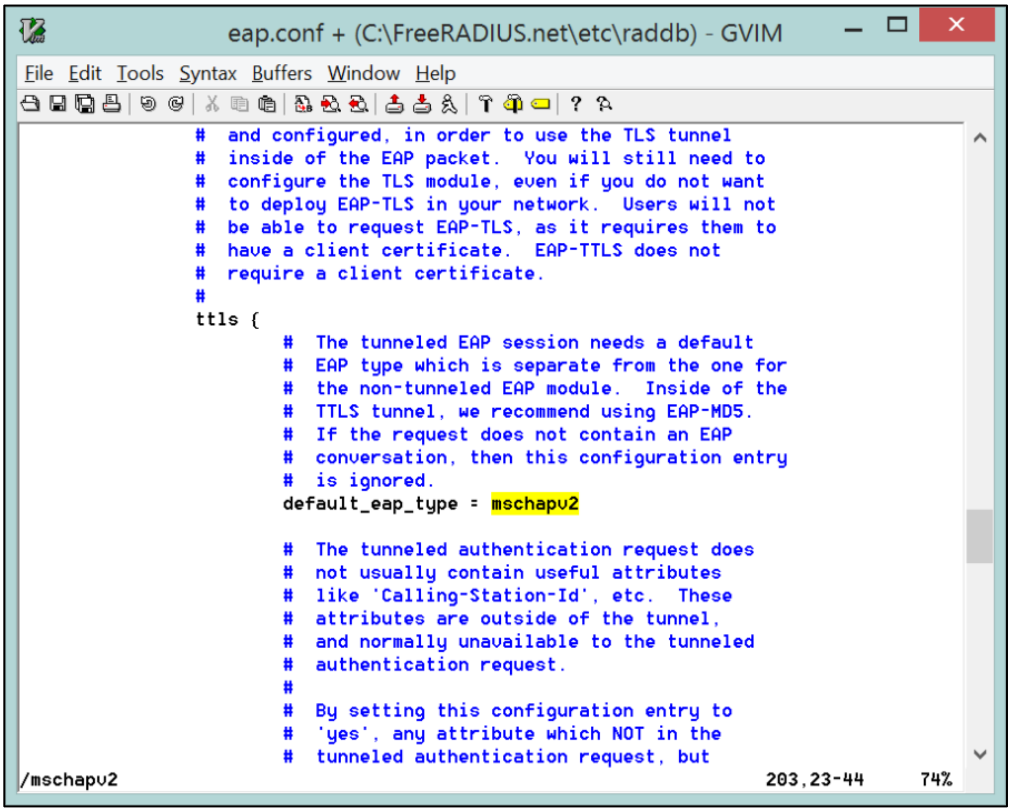
3. Uncomment the "fragment_size" and "include_length" lines under the "tls" section, as shown in the figure below.


eap.conf + (C:\FreeRADIUS.net\etc\raddb) - GVIM
File Edit Tools Syntax Buffers Window Help
139,2-16 55%

```
                        #  This can never exceed the size of a RADIUS
                        #  packet (4096 bytes), and is preferably half
                        #  that, to accomodate other attributes in
                        #  RADIUS packet.  On most APs the MAX packet
                        #  length is configured between 1500 - 1600
                        #  In these cases, fragment size should be
                        #  1024 or less.
                        #
                        fragment_size = 1024

                        #  include_length is a flag which is
                        #  by default set to yes If set to
                        #  yes, Total Length of the message is
                        #  included in EVERY packet we send.
                        #  If set to no, Total Length of the
                        #  message is included ONLY in the
                        #  First packet of a fragment series.
                        #
                        include_length = yes

                        #  Check the Certificate Revocation List
                        #
                        #  1) Copy CA certificates and CRLs to same directory.
                        #  2) Execute 'c_rehash <CA certs&CRLs Directory>'.
                        #    'c_rehash' is OpenSSL's command.
                        #  3) Add 'CA_path=<CA certs&CRLs directory>'
                        #      to radiusd.conf's tls section.
                        #  4) uncomment the line below.
```

Figure 13: TLS Section – II

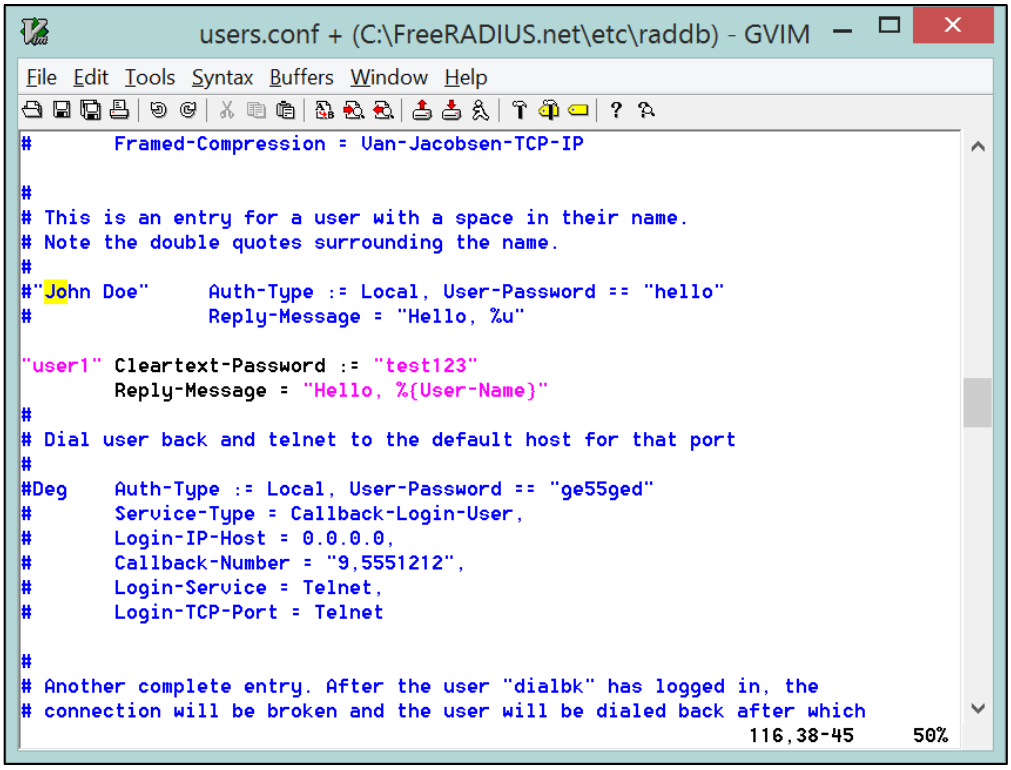
4. Change the input for the "default_eap_type" field under the "ttls" section to "mschapv2", as shown in the figure below.


eap.conf + (C:\FreeRADIUS.net\etc\raddb) - GVIM
File Edit Tools Syntax Buffers Window Help

```
                #  and configured, in order to use the TLS tunnel
                #  inside of the EAP packet.  You will still need to
                #  configure the TLS module, even if you do not want
                #  to deploy EAP-TLS in your network.  Users will not
                #  be able to request EAP-TLS, as it requires them to
                #  have a client certificate.  EAP-TTLS does not
                #  require a client certificate.
                #
                ttls {
                        #  The tunneled EAP session needs a default
                        #  EAP type which is separate from the one for
                        #  the non-tunneled EAP module.  Inside of the
                        #  TTLS tunnel, we recommend using EAP-MD5.
                        #  If the request does not contain an EAP
                        #  conversation, then this configuration entry
                        #  is ignored.
                        default_eap_type = mschapv2

                        #  The tunneled authentication request does
                        #  not usually contain useful attributes
                        #  like 'Calling-Station-Id', etc.  These
                        #  attributes are outside of the tunnel,
                        #  and normally unavailable to the tunneled
                        #  authentication request.
                        #
                        #  By setting this configuration entry to
                        #  'yes', any attribute which NOT in the
                        #  tunneled authentication request, but
/mschapv2                                                     203,23-44     74%
```

Figure 14: TTLS Section

5. Open the users.conf file and add the lines shown in the figure below starting with "user1". This adds a user with username "user1" and password "test123".


users.conf + (C:\FreeRADIUS.net\etc\raddb) - GVIM
File Edit Tools Syntax Buffers Window Help

```
#       Framed-Compression = Van-Jacobsen-TCP-IP

#
# This is an entry for a user with a space in their name.
# Note the double quotes surrounding the name.
#
#"John Doe"      Auth-Type := Local, User-Password == "hello"
#                Reply-Message = "Hello, %u"

"user1" Cleartext-Password := "test123"
        Reply-Message = "Hello, %{User-Name}"
#
# Dial user back and telnet to the default host for that port
#
#Deg    Auth-Type := Local, User-Password == "ge55ged"
#       Service-Type = Callback-Login-User,
#       Login-IP-Host = 0.0.0.0,
#       Callback-Number = "9,5551212",
#       Login-Service = Telnet,
#       Login-TCP-Port = Telnet

#
# Another complete entry. After the user "dialbk" has logged in, the
# connection will be broken and the user will be dialed back after which
                                                       116,38-45     50%
```

Figure 15: User Addition

6. Copy the wifiuser.pem file from RS9116.NBZ.WC.GEN.OSI.x.x.x\utils\Radius_Server\raddb\certs folder to C:\FreeRADIUS\etc\raddb\certs folder.

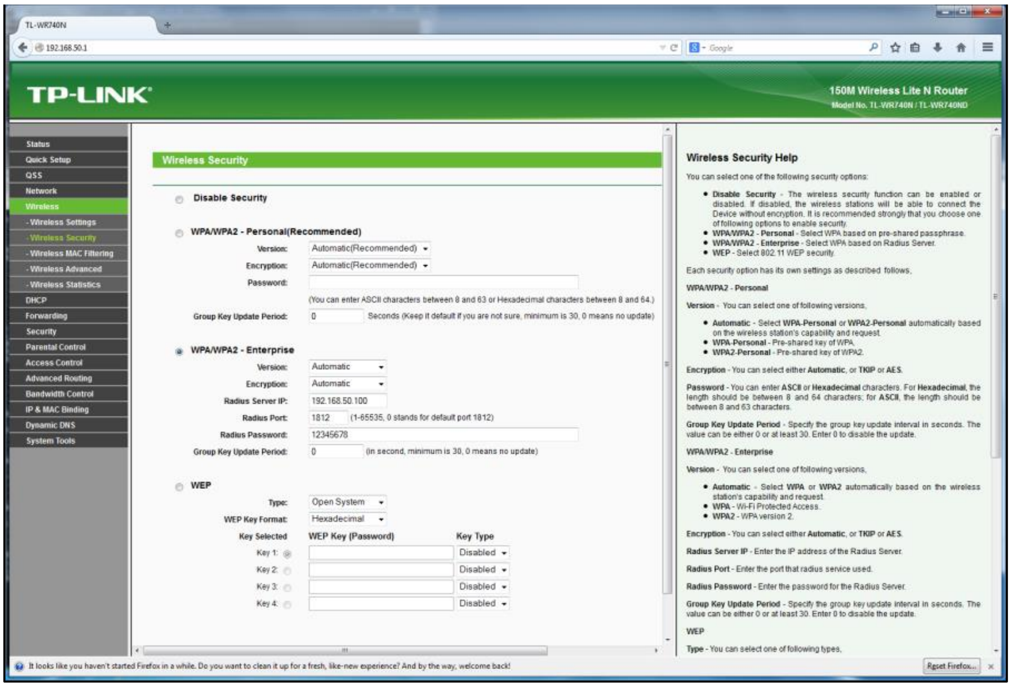
7. Ensure that the FreeRADIUS server is not running. Open the Windows Command Prompt with Administrator privileges and navigate to the C:\FreeRADIUS\sbin folder.

8. Run the "StartServer.cmd" file. You will see a series of prints on the screen. Monitor the prints to ensure that all changes are done correctly. The Radius server has started successfully if you see a print at the end which says, "Ready to process requests.

4.4.1.2.2 Access Point Configuration

Follow the steps below to configure the Access Point in the setup shown in Figure 10 to work with the Radius server started on Laptop D.

1. Connect the Access Point to Laptop D over Ethernet and open the Access Point pages in a browser by typing the IP address of the Access Point.
2. Navigate to the Wireless Security section and enable the "WPA/WPA2 – Enterprise" option, as shown in the figure below. The page below is for a TP-Link Access Point.



Wireless Security

○ Disable Security

○ WPA/WPA2 - Personal(Recommended)

Version: Automatic(Recommended)
Encryption: Automatic(Recommended)
Password:
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)
Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

● WPA/WPA2 - Enterprise

Version: Automatic
Encryption: Automatic
Radius Server IP: 192.168.50.100
Radius Port: 1812 (1-65535, 0 stands for default port 1812)
Radius Password: 12345678
Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

○ WEP

Type: Open System
WEP Key Format: Hexadecimal

Key Selected	WEP Key (Password)	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

Wireless Security Help

You can select one of the following security options:

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Device without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WPA/WPA2 - Personal** - Select WPA based on pre-shared passphrase.
- **WPA/WPA2 - Enterprise** - Select WPA based on Radius Server.
- **WEP** - Select 802.11 WEP security.

Each security option has its own settings as described follows,

WPA/WPA2 - Personal

Version - You can select one of following versions,

- **Automatic** - Select **WPA-Personal** or **WPA2-Personal** automatically based on the wireless station's capability and request.
- **WPA-Personal** - Pre-shared key of WPA.
- **WPA2-Personal** - Pre-shared key of WPA2.

Encryption - You can select either **Automatic**, or **TKIP** or **AES**.

Password - You can enter **ASCII** or **Hexadecimal** characters. For **Hexadecimal**, the length should be between 8 and 64 characters; for **ASCII**, the length should be between 8 and 63 characters.

Group Key Update Period - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

WPA/WPA2 - Enterprise

Version - You can select one of following versions,

- **Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.
- **WPA** - Wi-Fi Protected Access.
- **WPA2** - WPA version 2.

Encryption - You can select either **Automatic**, or **TKIP** or **AES**.

Radius Server IP - Enter the IP address of the Radius Server.

Radius Port - Enter the port that radius service used.

Radius Password - Enter the password for the Radius Server.

Group Key Update Period - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

WEP

Type - You can select one of following types,

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

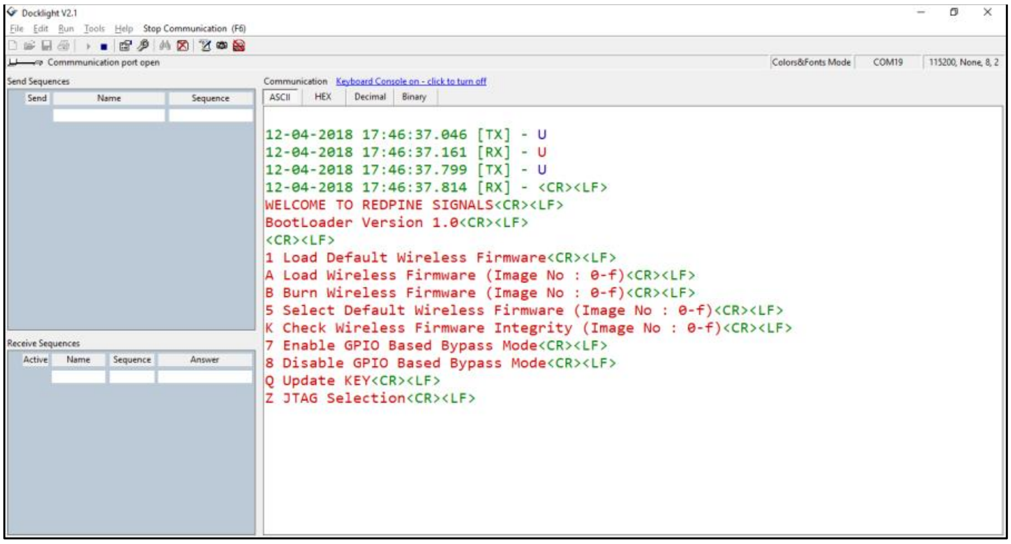
Figure 16: Wireless Security Configuration of Access Point

3. Enter the IP address of the Radius Server in the field labeled, "Radius Server IP". In the above figure, it is 192.168.50.100.

4. Enter the Radius Password as "12345678". This is the same as that entered in the clients.conf file of the Radius Server.

4.4.1.2.3 Wi-Fi Enterprise Client Configuration

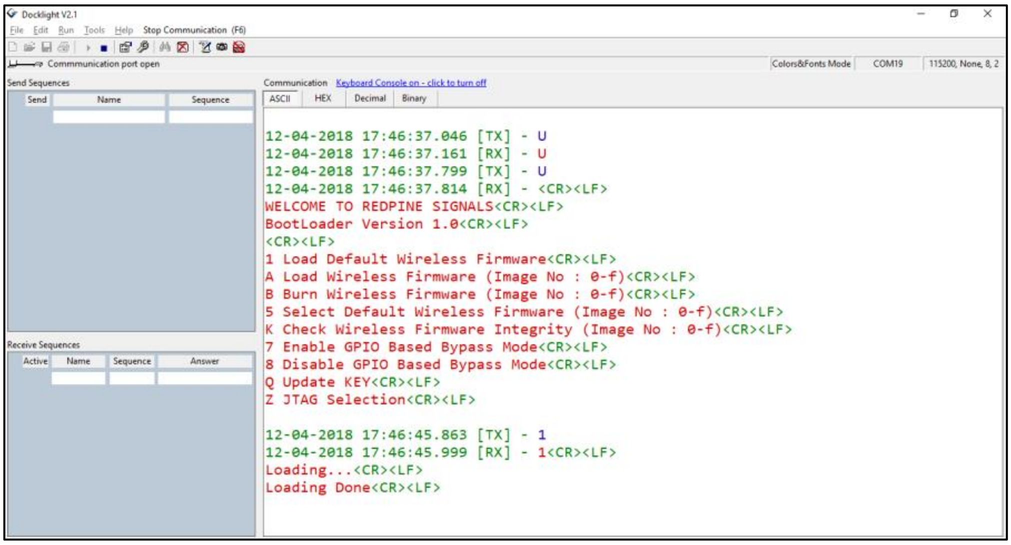
1. Open Docklight.
2. Connect the Micro A/B-type USB cable between the USB port of the PC and the micro-USB port of the EVB labeled "UART".
3. Hit the "F5" key when in the Docklight window to start communicating with EVB over the serial COM port.
4. At power up, the module tries to estimate the baud rate of the Host by exchanging data with it. Please refer to the Software PRM document to understand the Automatic Baud Rate Detection Process for faster bootup. (Shift + |) then (Shift + U) will do the ABRD process and you will see the boot up message. Please see the figure below.



```
12-04-2018 17:46:37.046 [TX] - U
12-04-2018 17:46:37.161 [RX] - U
12-04-2018 17:46:37.799 [TX] - U
12-04-2018 17:46:37.814 [RX] - <CR><LF>
WELCOME TO REDPINE SIGNALS<CR><LF>
BootLoader Version 1.0<CR><LF>
<CR><LF>
1 Load Default Wireless Firmware<CR><LF>
A Load Wireless Firmware (Image No : 0-f)<CR><LF>
B Burn Wireless Firmware (Image No : 0-f)<CR><LF>
5 Select Default Wireless Firmware (Image No : 0-f)<CR><LF>
K Check Wireless Firmware Integrity (Image No : 0-f)<CR><LF>
7 Enable GPIO Based Bypass Mode<CR><LF>
8 Disable GPIO Based Bypass Mode<CR><LF>
Q Update KEY<CR><LF>
Z JTAG Selection<CR><LF>
```

Figure 17: Module Startup Messages

5. Hit '1' and present Enter. You will see a message that says, "Loading…" followed by "Loading Done".



```
12-04-2018 17:46:37.046 [TX] - U
12-04-2018 17:46:37.161 [RX] - U
12-04-2018 17:46:37.799 [TX] - U
12-04-2018 17:46:37.814 [RX] - <CR><LF>
WELCOME TO REDPINE SIGNALS<CR><LF>
BootLoader Version 1.0<CR><LF>
<CR><LF>
1 Load Default Wireless Firmware<CR><LF>
A Load Wireless Firmware (Image No : 0-f)<CR><LF>
B Burn Wireless Firmware (Image No : 0-f)<CR><LF>
5 Select Default Wireless Firmware (Image No : 0-f)<CR><LF>
K Check Wireless Firmware Integrity (Image No : 0-f)<CR><LF>
7 Enable GPIO Based Bypass Mode<CR><LF>
8 Disable GPIO Based Bypass Mode<CR><LF>
Q Update KEY<CR><LF>
Z JTAG Selection<CR><LF>

12-04-2018 17:46:45.863 [TX] - 1
12-04-2018 17:46:45.999 [RX] - 1<CR><LF>
Loading...<CR><LF>
Loading Done<CR><LF>
```

Figure 18: Firmware Loading Messages

6. The following commands can now be issued to the module. Please refer to the Software PRM document for a detailed description of each command and the expected responses. A command should not be sent until the response for the previous command is received.

NOTE: Each AT command should have a suffix of Carriage Return <CR> and Line Feed <LF>. This is enabled by default in Docklight.

- at+rsi_opermode=2,0,4,0

  This command configures the module as a Wi-Fi client. The module responds with "OK"

- at+rsi_band=0

  This command configures the operating band of the Wi-Fi client to 2.4GHz. The module responds with "OK"

- at+rsi_init

  This command initializes the Wi-Fi module in the EVB. The module responds with OK<MAC_Address>.

Note: You may need to switch to HEX mode to see the MAC address in HEX.

- at+rsi_eap=TLS,MSCHAPV2,user1,test123,0
  (If the EAP method is TLS)

These commands set the EAP mode for the module and set the authentication credentials (username and password). Issue one of them based on which mode needs to be evaluated.

1. To verify the EAP-TLS mode, a security certificate file should be loaded into the module. A Python-based script is provided to do the same since the loading of certificate files cannot be done through Docklight. Please download and install Python for Windows from https://www.python.org/downloads/release/python-279/. In addition, please download and install the Pyserial program for accessing the Serial COM port from Python. This is available at https://pypi.python.org/pypi/pyserial.

NOTE: Please download the 32-bit version of Python for Windows from the above link even if your PC is 64-bit since the 64-bit version does not update the registry correctly, which causes a problem during the installation of the Pyserial application.

2. Open the load_certificate.py file and change the serial port name to "COM8" as shown in the line below. This is the Serial COM port that was detected in Docklight earlier.

```
sp=serial.Serial(port="COM8",baudrate=115200,timeout=0.01)
```

3. Disable Docklight's serial port connection to the EVB by hitting 'F6' when the Docklight window is open.

4. Open the Windows Command Prompt and navigate to the RS9116.NBZ.WC.GEN.OSI.x.x.x\utils\Python folder and give the following command:

```
C:\Python27\python.exe load_certificate.py 1 ..\Radius_Server\raddb\certs\wifiuser.pem
```

This command loads the TLS Certificate into the module.

5. Go back to the Docklight window and hit "F5" to enable the serial port connection between Docklight and the EVB and continue giving the commands below.

6. For non-TLS modes, issue the command below to clear any certificates that might have been loaded previously.

```
at+rsi_cert=1,0,0,0
```

This command should NOT be given for TLS mode after the at+rsi_eap command.

- at+rsi_scan=0

This command scans for available Access Points operating in the 2.4 GHz band. The module responds with information of the Access Points scanned. The data received might have some unreadable characters because of ASCII conversion. You can use the HEX tab of Docklight to see the bytes sent by the module.

- at+rsi_join=Test_AP,0,2,6

This command connects the Wi-Fi client to the Access Point with SSID "Test_AP". On successful association, the module responds with OK.

- at+rsi_ipconf=0,192.168.50.10,255.255.255.0,192.168.50.1

at+rsi_ipconf=1,0,0,0
This command configures the IP address of the module. The IP address configured in the above command is for illustration only. The user has to configure the IP address as per the Access Point's settings using either Manual (first command above) or DHCP mode (second command above).
For the Manual mode, ensure that the desired IP is in the same subnet as the Access Point's subnet. The module responds to this command by sending the configured IP address to the Host. In the terminal, this response might appear as unreadable characters because of ASCII conversion. You can use the HEX tab of Docklight to see the bytes sent by the module.

- at+rsi_ltcp=5001,1,0

This command opens a Listen TCP socket with port number 5001.

4.4.1.2.4 Test Procedure

1. Connect Laptop C to the Access Point. It should have proper security credentials to connect to the AP.
2. A "ping The module responds to a ping request sent from a remote terminal. There is no command to send a ping request from the module. This is true in all the modes- Client, AP and Wi-Fi Direct." can be issued from Laptop C to the Wi-Fi module to verify connectivity through the AP.
3. TCP and UDP applications are provided along with the release package for execution on the Laptop C. These applications are located in the path RS9116.NBZ.WC.GEN.OSI.x.x.x\utils\peer_applications\Windows where RS9116.NBZ.WC.GEN.OSI.x.x.x is a software package directory. Open a client TCP socket on the Laptop C using the following command in a Windows Command Prompt.

```
TCP.exe c 2001 <EVB IP address> 5001
```

4. The above command opens a new window with the following options:

1. Send
2. Receive
3. Exit

5. Observe that the terminal on the Wi-Fi Client-side (EVB) prints the following message, once the TCP connection is set up with Laptop C.

AT+RSI_LTCP_CONNECT=<ip_version><socket_descriptor><dest_port_no><dest_ipaddr><mss><window_size><src_port_no>\r\n

1. For testing the Receive mode of the Wi-Fi Client (EVB), follow the steps below:
2. Type 1 in the TCP.exe window on Laptop C.
3. On being prompted to enter a data string to be transmitted, type any string and hit Enter to transmit the typed data.
4. When the data is received on the Wi-Fi Client (EVB) side, you will see a response (asynchronous) from the module as follows:

AT+RSI_READ<ip_version><socket_handle><payload_len><source_ip_addr><source_port><payload>

1. For testing the Transmit mode of the Wi-Fi Client (EVB), follow the steps below:
2. Type 2 in the TCP.exe window on Laptop C.
3. On the Wi-Fi Client (EVB) side, send the command below to transmit data to the Laptop C.

at+rsi_snd=<socket_handle>,<payload_len>,<dest_ipaddr>,<dest_port>,<payload >

1. The transmitted data is displayed on the TCP.exe window of Laptop C.

NOTE: To switch between Enterprise Security and any other security modes (WPA2-PSK, WPA, WEP) Operation mode has to be changed. Enterprise security works in Operation mode 2 and for other security modes, the Operation mode is 0. The Change in the Operation mode command can happen just after the Reset (soft reset or hard reset) so Reset is required to toggle between Enterprise Security and other security modes.

4.4.1.3 Wi-Fi Access Point Mode

The figure below shows the setup required for this process.

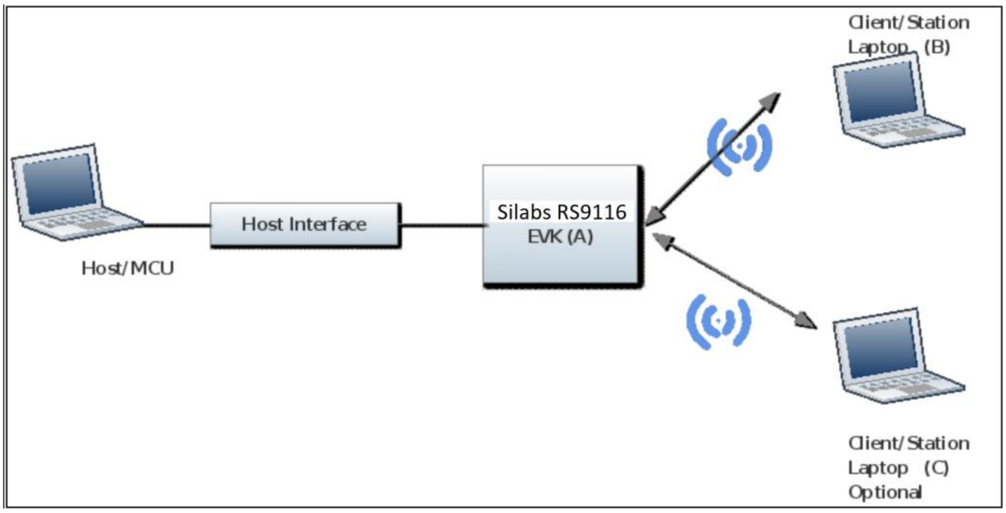


Figure 19: Setup for Access Point Mode

Access Point Configuration Through AT Commands

1. Follow steps in section "Start-Up Messages on Power-Up" from RS9116W_Wi-Fi_AT_Command_Programming_Reference_Manual(PRM) from https://docs.silabs.com/rs9116 to power up the EVB and load the firmware.
2. Enter the following commands. A command should be entered only after getting the response of the previous command

   ○ at+rsi_opermode=6,1,18,0
   This configures the EVB to function in AP mode. The module responds with "OK".

- at+rsi_band=0
  This configures the operating band of the EVB. The module responds with "OK".

- at+rsi_init
  This initializes the WiFi module in the EVB. The module responds with OK<mac_address>
- at+rsi_fwversion?
  This is an optional command to report the firmware version in use.
- at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168.0.30
  This command configures the IP (192.168.0.30 in this example) of the AP. If this command is not issued, a default IP of 192.168.100.76 will be used.
- at+rsi_apconf=6,SILABS_AP,0,0,0,100,2,3
  The SSID is configured as "SILABS_AP", to operate on channel 6. Please refer to the Software PRM for more details on the other parameters of this command.
- at+rsi_join=SILABS_AP,0,2,0
  This starts the Access Point functionality in the module.

The module is now configured as an Access Point. Its IP address is 192.168.0.30. A Laptop can now scan for networks and the SSID of the module, "SILABS_AP" will be displayed in the Laptop's list of Scanned APs. After the client Laptop (C) connects to the AP, it acquires an IP address over DHCP. The IP address assigned to the laptop can be known by opening the Windows Command Prompt and issuing the command "ipconfig". It is assumed for illustrative purposes that the IP of the Laptop is 192.168.0.32.

4.4.1.3.1 Test Procedure

The applications provided in the USB drive (as part of the release package) send and receive TCP and UDP packets. TCP and UDP applications are provided along with a release package for execution on the Laptop. These applications are located in the path RS9116.NB0.WC.GENR.OSI.x.x.x\utils\peer_applications\Windows where RS9116.NB0.WC.GENR.OSI.x.x.x is a software package directory.

1. Open a TCP Server socket on the Wi-Fi Client (EVB) side using the following AT command:

   Open a TCP client socket on Laptop C by running the TCP.exe application as follows in the Windows Command Prompt:

TCP.exe c 2001 192.168.0.30 5001
Ensure that you run the Windows Command Prompt program as an Administrator and any firewalls which block the creation of sockets are disabled before running the application.

1. The above command opens a new window with the following options:
   a. Send
   b. Receive
   c. Exit
2. Observe that the Docklight on the Wi-Fi AP side (EVB) prints the following message, once the TCP connection is set up with Laptop C.

AT+RSI_LTCP_CONNECT=<ip_version><socket_descriptor><dest_port_no><dest_ipaddr><mss><window_size><src_port_no>\r\n

1. For testing the Receive mode of the Wi-Fi AP (EVB), follow the steps below:
2. Type 1 in the TCP.exe window on Laptop C.
3. On being prompted to enter a data string to be transmitted, type any string and hit Enter to transmit the typed data.
4. When the data is received on the Wi-Fi AP (EVB) side, you will see a response (asynchronous) from the module as follows:

AT+RSI_READ<ip_version><socket_handle><payload_len><source_ip_addr><source_port><payload>

1. For testing the Transmit mode of the Wi-Fi AP (EVB), follow the steps below:
2. Type 2 in the TCP.exe window on Laptop C.
3. On the Wi-Fi AP (EVB) side, send the command below to transmit data to the Laptop C.

at+rsi_snd=<socket_handle>,<payload_len>,<dest_ipaddr>,<dest_port>,<payload >

1. The transmitted data is displayed on the TCP.exe window of Laptop C.

4.5 BLE Evaluation in UART Mode

The following sub-sections describe configuring and using the module in different security and operational modes of BLE in UART mode.

4.5.1 BLE Evaluation using AT Commands

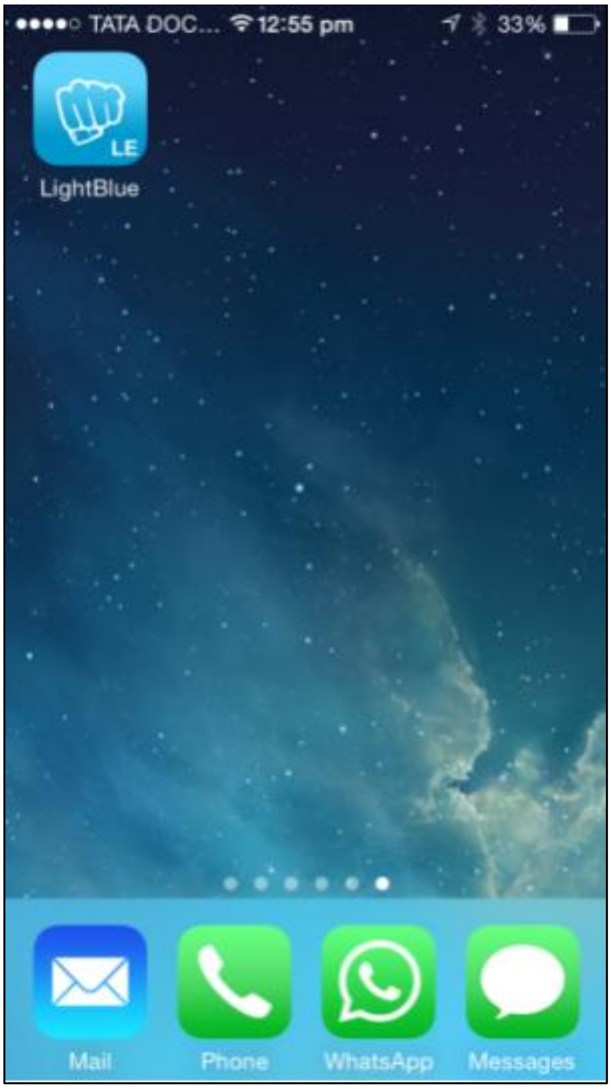
4.5.1.1 BLE in Peripheral (Slave) Mode

4.5.1.1.1 BLE Peripheral Mode Configuration through AT commands

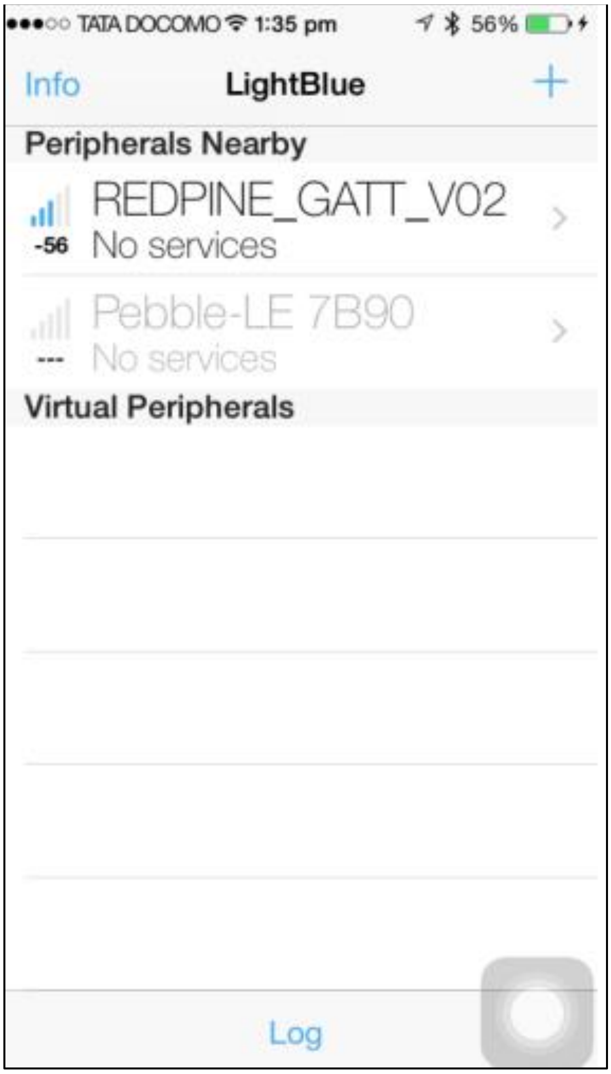
```
[TX] - at+rsi_opermode=851968,0,1,2147483648,2149580800,3221225472,0,1966080<CR><LF>
[RX] - OK<CR><LF>
bt_loaded<CR><LF>
This opermode enables Wi-Fi+BLE mode of operation. The message bt_loaded indicates successful operation of
the command.
[TX] - at+rsibt_setlocalname=11,RS9116W_BLE<CR><LF>
[RX] - OK <CR><LF>
Used to set name to the local device
[TX] - at+rsibt_getlocalbdaddr?<CR><LF>
[RX] - OK 00-23-A7-4C-24-95<CR><LF>
Used to query the BD address of the local device
[TX] - at+rsibt_addservice=2,180A,3,30<CR><LF>
[RX] - OK 1558C,A<CR><LF>
used to add the new service Record in BLE GATT record list. The module responds with a service record handle if
the service is created successfully. In this example, the service record handle is 1558C. This is used to add
attribute records to the service.
[TX] - at+rsibt_addattribute=1558C,B,2,2803,2,6,8,0,0C,00,A1,1A<CR><LF>
[RX] - OK <CR><LF>
This is used to add a characteristic attribute record to the above created service using the service record handle
1558C and UUID 2803.
[TX] - at+rsibt_addattribute=1558C,C,2,1AA1,8,a,1,2,3,4,5,6,7,8,9,0<CR><LF>
[RX] - OK <CR><LF>
This is used to add a characteristic attribute record to the above created service using the service record handle
1558C and UUID 1AA1.
[TX] - at+rsibt_addattribute=1558C,D,2,2803,2,6,1A,0,0E,00,B1,1B<CR><LF>
[RX] - OK <CR><LF>
This is used to add a characteristic attribute record to the above created service using the service record handle
1558C and UUID 2803
[TX] - at+rsibt_addattribute=1558C,E,2,1BB1,1A,10,52,65,64,70,69,6E,65,5F,73,69,67,6E,61,6C,73,30<CR><LF>
[RX] - OK <CR><LF>
This is used to add a characteristic attribute record to the above created service using the service record handle
1558C and UUID 1BB1.
[TX] - at+rsibt_addattribute=1558C,F,2,2902,A,2,0,0<CR><LF>
[RX] - OK <CR><LF>
This is used to add the notify property to the above created characteristic attribute record (1BB1) using the service
record handle 1558C and UUID 2902.
[TX] - at+rsibt_setadvertisedata=8,2,1,6,4,9,72,72,72<CR><LF>
[RX] - OK <CR><LF>
This command is used to set the advertise data to expose remote devices.
[TX] - at+rsibt_advertise=1,128,0,0,0,32,32,0,7<CR><LF>
[RX] - OK <CR><LF>
This is used to expose or advertise about local device to the remote BT devices.
```

4.5.1.1.2 Test procedure

- Go to "LightBlue" iPhone app



- Once you open the APP you can see "REDPINE_GATT_V02"



Peripherals Nearby

REDPINE_GATT_V02
-56 No services

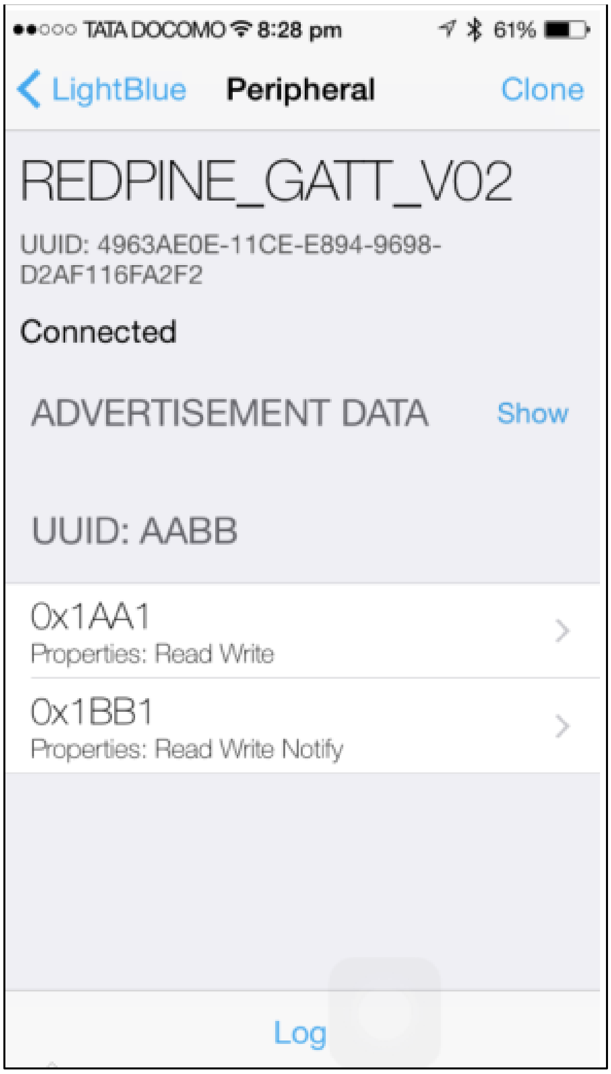
Pebble-LE 7B90
--- No services

Virtual Peripherals

- Now connect to "REDPINE_GATT_V02". You will see a BT CONN event on the module side.
- You will see an asynchronous message to indicate that a BLE device has connected.

```
AT+RSIBT_LE_DEVICE_CONNECTED=1,44-0F-69-AE-48-0D,0<CR><LF>
AT+RSIBT_LE_REMOTE_MTU_SIZE 44-0F-69-AE-48-0D,64<CR><LF>
```

- Once connected you will see as below:



●●○○○ TATA DOCOMO 8:28 pm 61%

LightBlue Peripheral Clone

REDPINE_GATT_V02

UUID: 4963AE0E-11CE-E894-9698-D2AF116FA2F2

Connected

ADVERTISEMENT DATA Show

UUID: AABB

0x1AA1
Properties: Read Write

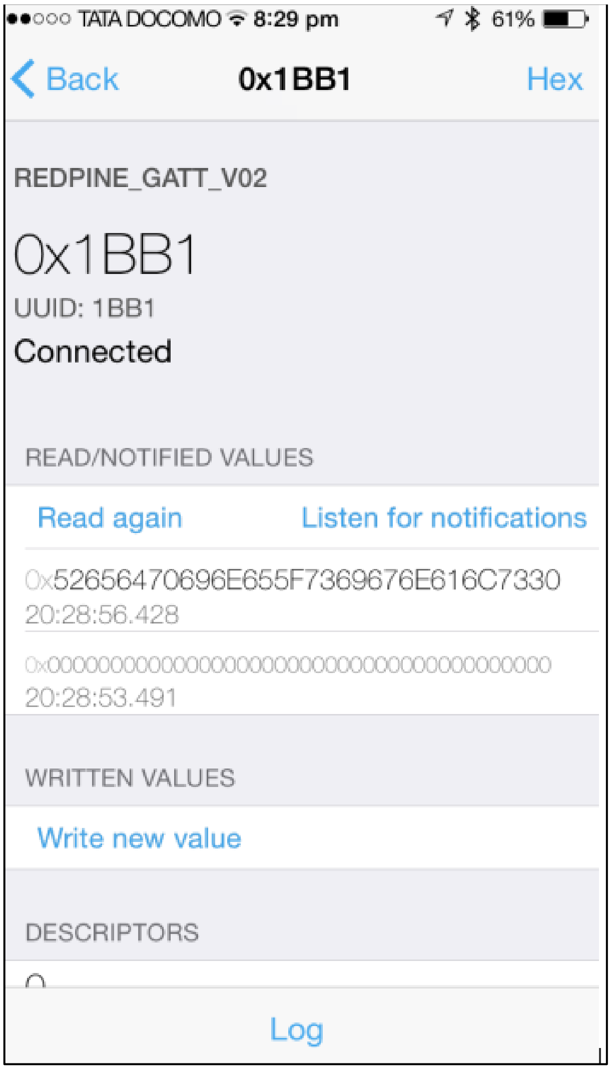
0x1BB1
Properties: Read Write Notify

Log

- Now you need to select 1BB1, which is a Read Write Notify service.
- Enable the "Listen for notification". This will show the hex stream e.g. 0x52656470696E655F7369676E616C7330
- In ASCII Redpine_signals0
- You will see the asynchronous message at the module side like below after enabling the notification.

AT+RSIBT_WRITE,5E-BB-8F-07-6B-D8,F,2,1,0<CR><LF>

- You can see here data every time when we send something to the module by writing in the 1BB1 service.



4.5.1.2 BLE in Central (Master) Mode

4.5.1.2.1 BLE Central Mode Configuration through AT commands

1. Follow steps in section "Start-Up Messages on Power-Up" from RS9116W_Wi-Fi_AT_Command_Programming_Reference_Manual(PRM) from https://docs.silabs.com/rs9116 to power up the EVB and load the firmware.
2. Enter the following commands. A command should be entered only after getting the response of the previous command

[TX] - at+rsi_opermode=851968,0,1,2147483648,2149580800,3221225472,0,1966080<CR><LF>
[RX] - OK <CR><LF>
bt_loaded<CR><LF>
This opermode enables Wi-Fi+BLE mode of operation. The message bt_loaded indicates successful operation of the command.
[TX] - at+rsibt_getlocalname?<CR><LF>
[RX] - OK <CR><LF>
Used to query the name of the local device
[TX] - at+rsibt_getlocalbdaddr?<CR><LF>
[RX] - OK <CR><LF>
Used to query the BD address of the local device
[TX] - at+rsibt_addservice=2,180A,3,30<CR><LF>
[RX] - OK 1558C,A<CR><LF>
used to add the new service Record in BLE GATT record list. The module responds with a service record handle if the service is created successfully. In this example, the service record handle is 1558C. This is used to add attribute records to the service.
[TX] - at+rsibt_addattribute=1558C,B,2,2803,2,6,8,0,0C,00,00,2A<CR><LF>

```
[RX] - OK <CR><LF>
```

This is used to add a characteristic attribute record to the above created service using the service record handle 1558C and UUID 2803.

```
[TX] -at+rsibt_addattribute=1558C,C,2,2A00,8,a,1,2,3,4,5,6,7,8,9,0<CR><LF>
[RX] - OK <CR><LF>
```

This is used to add a characteristic attribute record to the above created service using the service record handle 1558C and UUID 2A00.

```
[TX] - at+rsibt_scan=1,0,0<CR><LF>
[RX] - OK <CR><LF>
```

Used to scan for remote LE advertise devices

```
[TX] - at+rsibt_connect=0,<BD Address of the peripheral device><CR><LF>
[RX] - OK <CR><LF>
```

Used to create connection with remote LE device

```
[TX] - at+rsibt_getallprofiles=<BD Address of the peripheral device>,1,10<CR><LF>
[RX] - OK 3<LF>
1,5,2,1800<LF>
6,9,2,1801<LF>
A,C,2,180A<LF><CR><LF>
```

Used to query the entire supported profiles list from the connected remote device.

```
[TX] - at+rsibt_getcharservices=<BD Address of the peripheral device>,1,10<CR><LF>
[RX] - OK 4, 2,2,3,2,2A00<LF>
4,2,5,2,2A01<LF>
7,10,8,2,2A05<LF>
B,8,C,2,2A00<LF><CR><LF>
```

Used to query characteristic services, with in the particular range, from the connected remote device

```
[TX] - at+rsibt_writevalue=<BD Address of the peripheral device>,C,a,1,e,d,e,b,c,e,f,a,1<CR><LF>
[RX] - OK <CR><LF>
```

Used to Set attribute value of the connected remote device.

4.5.1.3 Test Procedure

Choose a BLE peripheral device, not its BD address and configure it to advertise. Run the commands explained above on an RS9116 EVB to configure it in the BLE central mode, scan for nearby peripherals and connect to the desired peripheral device. Ensure to replace the <BD Address of the peripheral device> with the BD address of the desired peripheral device.

4.6 BT Evaluation in UART Mode

The following sub-sections describe configuring and using the module in different security and operational modes of BT.

4.6.1 BT Evaluation using AT Commands

4.6.1.1 BT in Master Mode

4.6.1.1.1 BT Master Mode Configuration through AT commands

Configure the module to UART mode using the steps given in the EVB user guide.
For the demo, we have used the "SENA BTerm" application on Android.

Note 1: Bluetooth spp manager application also supports BT in Master mode.

1. Power up the module and the module sends the following messages at the boot-up.

```
WELCOME TO REDPINE SIGNALS<CR><LF>
BootLoader Version 1.0<CR><LF>
<CR><LF>
1 Load Default Wireless Firmware<CR><LF>
A Load Wireless Firmware (Image No : 0-f)<CR><LF>
B Burn Wireless Firmware (Image No : 0-f)<CR><LF>
5 Select Default Wireless Firmware (Image No : 0-f)<CR><LF>
K Check Wireless Firmware Integrity (Image No : 0-f)<CR><LF>
7 Enable GPIO Based Bypass Mode<CR><LF>
8 Disable GPIO Based Bypass Mode<CR><LF>
Q Update KEY<CR><LF>
Z JTAG Selection<CR><LF>
```

- Select the appropriate option. As shown above, to load firmware option 1(**Load Default Wireless Firmware**) is selected.
  [TX] - 1
  [RX] - 1<CR><LF>

- Once the module loads firmware it will indicate with the message "Loading…" and "Loading Done" as shown below:

  Loading...<CR><LF>
  Loading Done<CR><LF>

- First, select the BT profile using the *at+rsi_opermode* command. For the BT profile give the first parameter as 327680.

  [TX] - at+rsi_opermode=327680,0,1,2147483648,2150629376,1073741824<CR><LF>

  [RX] - OK<CR><LF>

  bt_loaded<CR><LF>

- Now set the BT profile using the *at+rsibt_setprofilemode* command. For the SPP profile select the parameter as 1.
  [TX] - at+rsibt_setprofilemode=1<CR><LF>
  [RX] - OK<CR><LF>

- Set the module name using *at+rsibt_setlocalname* command e.g. "BT_MASTER"

  [TX] - at+rsibt_setlocalname=9,BT_MASTER<CR><LF>

  [RX] - OK<CR><LF>

- Set the discovery mode by using *at+rsibt_setdiscvmode* command. Give value 1 to set the mode.

  [TX] - at+rsibt_setdiscvmode=1<CR><LF>

  [RX] - OK <CR><LF>

- Set the connection mode by using the *at+rsibt_setconnmode* command. Give value 1 to set the mode.

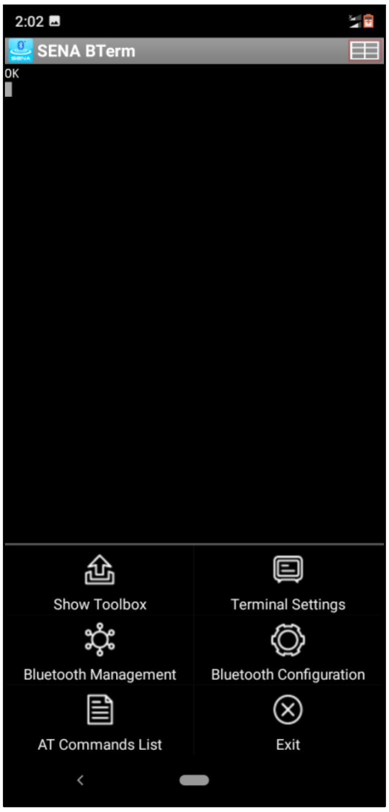
  [TX] - at+rsibt_setconnmode=1<CR><LF>

  [RX] - OK <CR><LF>

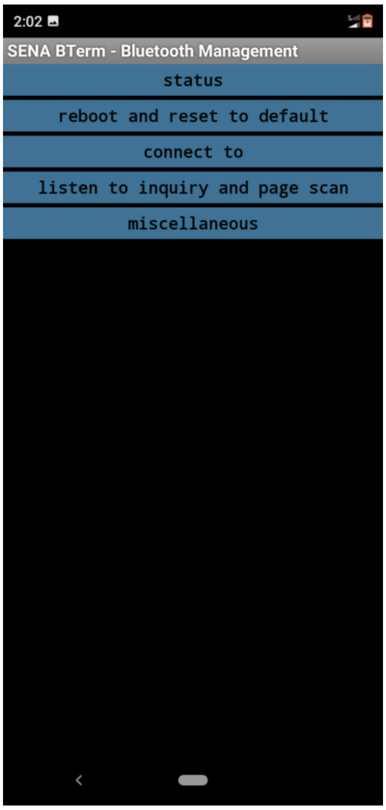
4.6.1.1.2 Test Procedure

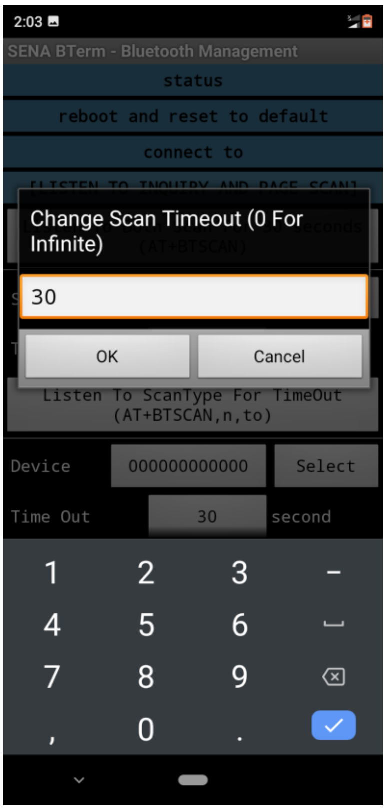
- Now open the SENA BTerm app in your android phone and turn on Bluetooth.

- Click on the table symbol which is on the right side and then select the "Bluetooth Management" to configure the application in listen mode.



- Now click on the "listen to inquiry and page scan" and then change scan timeout as 0 for infinite timeout.


2:02
SENA BTerm - Bluetooth Management
status
reboot and reset to default
connect to
listen to inquiry and page scan
miscellaneous

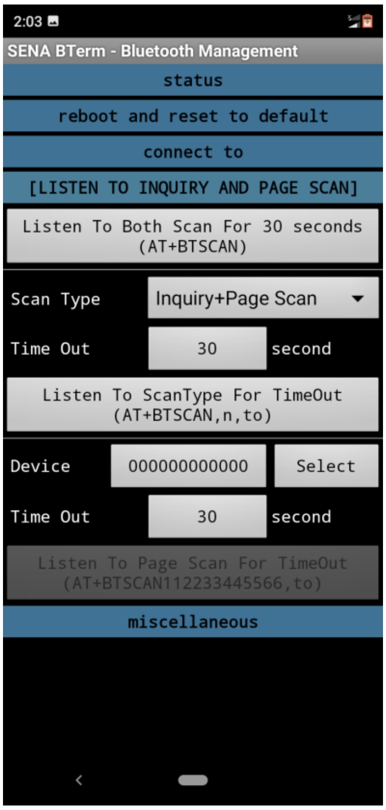


Change Scan Timeout (0 For Infinite)

30

2:03
SENA BTerm - Bluetooth Management
status
reboot and reset to default
connect to
[LISTEN TO INQUIRY AND PAGE SCAN]
OK
Cancel
Listen To ScanType For TimeOut (AT+BTSCAN,n,to)
Device
000000000000
Select
Time Out
30
second
1
2
3
-
4
5
6
7
8
9
,
0
.

- Now put the application in discoverable mode by clicking "Listen to ScanType for TimeOut".



Scan Type: Inquiry+Page Scan

Time Out: 30 second

Device: 000000000000

Time Out: 30 second

2:03
SENA BTerm - Bluetooth Management
status
reboot and reset to default
connect to
[LISTEN TO INQUIRY AND PAGE SCAN]
Listen To Both Scan For 30 seconds (AT+BTSCAN)
Listen To ScanType For TimeOut (AT+BTSCAN,n,to)
Select
Listen To Page Scan For TimeOut (AT+BTSCAN112233445566,to)
miscellaneous

- Now give an inquiry command to scan the Bluetooth devices which are available around the module by giving *at+rsibt_inquiry.*

  [TX]at+rsibt_inquiry=1,10000,10<CR><LF>

  [RX] - OK <CR><LF>

- It will give the names of the devices which are available by giving the asynchronous messages given below:

  [RX] - AT+RSIBT_INQRESP 1,50-8F-4C-A1-05-D2,5,redmi,-71,5A020C<CR><LF>

  AT+RSIBT_INQRESP 1,4C-BB-58-E4-41-8D,0,,-100,2010C<CR><LF>

AT+RSIBT_INQRESP 1,BC-85-56-68-AE-FA,0,,-96,2010C<CR><LF>

AT+RSIBT_INQRESP 1,98-54-1B-C9-B4-8F,0,,-96,2010C<CR><LF>

AT+RSIBT_INQRESP 1,88-DA-1A-16-E5-85,0,,-82,240428<CR><LF>

AT+RSIBT_INQRESP 1,C4-0B-CB-DA-82-16,0,,-84,5A020C<CR><LF>

AT+RSIBT_INQRESP 1,64-5A-04-9A-4A-89,0,,-94,2010C<CR><LF>

AT+RSIBT_INQCOMPLETE<CR><LF>

- Now connect to the device you want to connect by giving the *at+rsi_bond* command. In that give the MAC address of the device which is also shown with its name in the **AT+RSIBT_INQRESP** message.
  [TX] - at+rsibt_bond=50-8F-4C-A1-05-D2<CR><LF>
  [RX] - OK <CR><LF>
- It will send an asynchronous response to the module as shown below:

  [RX] - AT+RSIBT_BONDRESP 50-8F-4C-A1-05-D2,0<CR><LF>

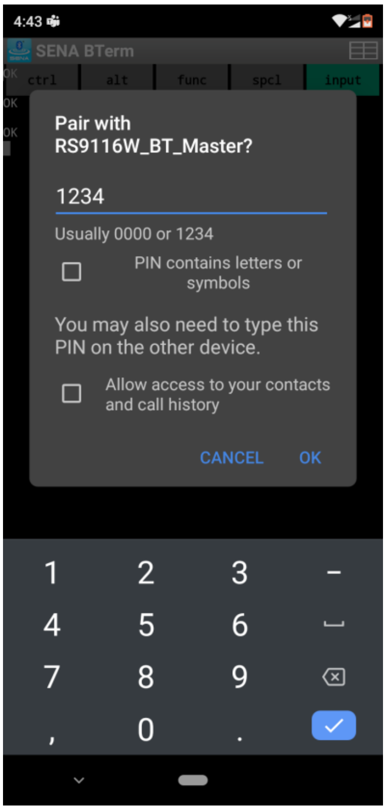
  [RX] - AT+RSIBT_USRLINKKEYREQ 50-8F-4C-A1-05-D2<CR><LF>
- We need to send the link key command *at+rsibt_usrlinkkey.*

  [TX] - at+rsibt_usrlinkkey=50-8F-4C-A1-05-D2,0,1234<CR><LF>

  [RX] - OK<CR><LF>
- Then it will send an asynchronous response to the module as shown below:
  AT+RSIBT_USRPINCODEREQ 50-8F-4C-A1-05-D2<CR><LF>
- The module needs to send an authentication code (Enter the same PIN as entered last time) e.g. 1234 here using *at+rsibt_usrpincode* command.

  [TX] - at+rsibt_usrpincode=50-8F-4C-A1-05-D2,1,1234<CR><LF>

  [RX] - OK<CR><LF>
- It will give Popup on the application to enter the PIN for the pairing process.



Pair with
RS9116W_BT_Master?

1234

Usually 0000 or 1234

□ PIN contains letters or symbols

You may also need to type this PIN on the other device.

□ Allow access to your contacts and call history

- As soon as you enter the pin and click "OK" on this window, it will send an asynchronous response to the module as shown below.

  [RX] - AT+RSIBT_USRLINKKEYSAVE 50-8F-4C-A1-05-D2,D9,96,25,99,88,38,BD,BC,78,72,55,51,4,F2,7D,99<CR><LF>

[RX] - AT+RSIBT_AUTHENTICATION_STATUS 50-8F-4C-A1-05-D2,1<CR><LF>

[RX] - AT+RSIBT_CLASSIC_DISCONNECTED 50-8F-4C-A1-05-D2,4E13<CR><LF>

- Now again give bond command

  [TX] - at+rsibt_bond=50-8F-4C-A1-05-D2<CR><LF>

  [RX] - OK <CR><LF>

- It will send an asynchronous response to the module as shown below:

  AT+RSIBT_BONDRESP 50-8F-4C-A1-05-D2,0<CR><LF>

  AT+RSIBT_USRLINKKEYREQ 50-8F-4C-A1-05-D2<CR><LF>

- We need to send the link key command *at+rsibt_usrlinkkey with the key which we got on LINKKEYSAVE and with a positive reply.*

  [TX] - at+rsibt_usrlinkkey=50-8F-4C-A1-05-D2,1,D9,96,25,99,88,38,BD,BC,78,72,55,51,4,F2,7D,99<CR><LF>

  [RX] - OK<CR><LF>

- Then it will send an asynchronous response to the module as shown below.

  [RX] - AT+RSIBT_AUTHENTICATION_STATUS 50-8F-4C-A1-05-D2,1<CR><LF>

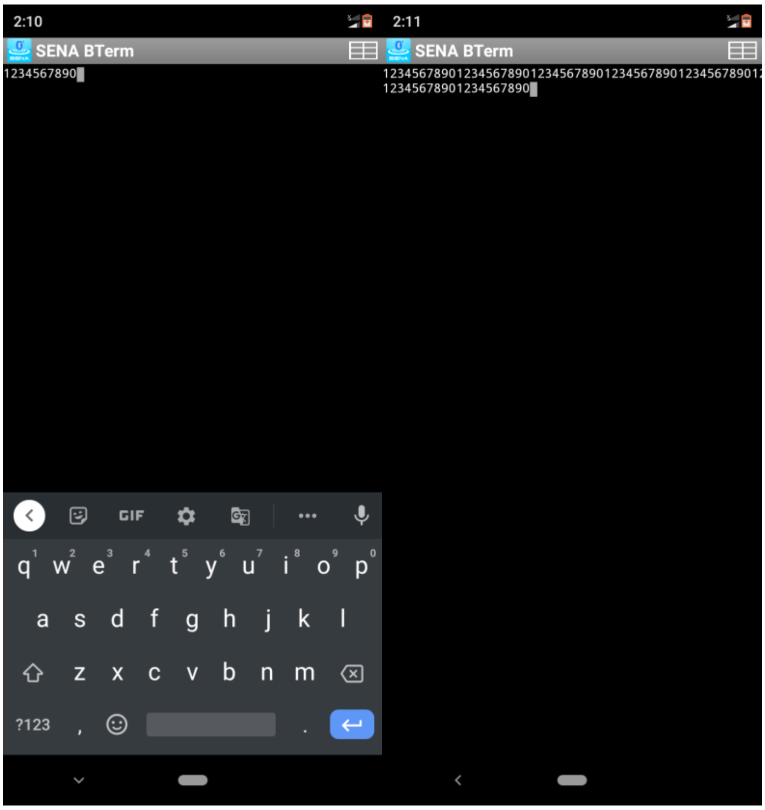
- Now give SPP connect command from the module by giving the command.

  [TX] - at+rsibt_sppconn=50-8F-4C-A1-05-D2<CR><LF>

- After a successful connection, an asynchronous message from the module given below will come on the terminal.

  [RX] - AT+RSIBT_SPPCONNECTED 50-8F-4C-A1-05-D2<CR><LF>

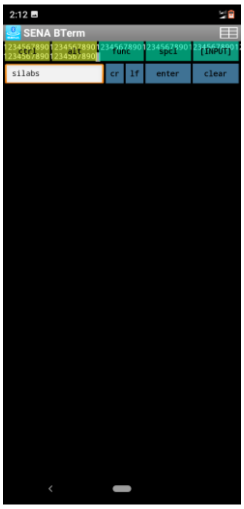
- Now start communicating with the other Bluetooth device through these terminals by sending the SPP TRANSFER command.
  [TX] - at+rsibt_spptx=10,1234567890<CR><LF>
  [RX] - OK<CR><LF>
  This string will be received on the application side.



```
1234567890
```

```
1234567890123456789012345678901234567890123456789012
12345678901234567890
```

- In the same way, we can send any random data from the application to the Module. Click on the "Show Toolbox" from the table symbol and then select the "[INPUT]" to enter the data to the Module.



- It will send an asynchronous response to the module as shown below.

  [RX] - AT+RSIBT_SPPRX 6,silabs<CR><LF>

  [RX] - AT+RSIBT_SPPRX 6,silabs<CR><LF>

  [RX] - AT+RSIBT_SPPRX 6,silabs<CR><LF>

  [RX] - AT+RSIBT_SPPRX 6,silabs<CR><LF>
- **BT in Slave Mode**
-
- **BT Slave Mode Configuration through AT commands**
-

  Configure the module to UART mode using the steps given in the EVB user guide and an Android phone with an application for the BT SPP profile support.

  For the demo, we have used the "Bluetooth spp pro" application.

  Note: This application works with Android v4.0+.
- Power up the module and the module sends the following messages at the boot-up.

  WELCOME TO REDPINE SIGNALS<CR><LF>

  BootLoader Version 1.0<CR><LF><CR><LF>

  1 Load Default Wireless Firmware<CR><LF>

  A Load Wireless Firmware (Image No : 0-f)<CR><LF>

  B Burn Wireless Firmware (Image No : 0-f)<CR><LF>

  5 Select Default Wireless Firmware (Image No : 0-f)<CR><LF>

  K Check Wireless Firmware Integrity (Image No : 0-f)<CR><LF>

  7 Enable GPIO Based Bypass Mode<CR><LF>

  8 Disable GPIO Based Bypass Mode<CR><LF>

  Q Update KEY<CR><LF>

  Z JTAG Selection<CR><LF>
- Select the appropriate option. As shown above, to load firmware option 1(**Load Default Wireless Firmware**) is selected.

  [TX] - 1
  [RX] - 1<CR><LF>

- Once the module loads firmware it will indicate with the message "Loading…" and "Loading Done" as shown below:

  Loading...<CR><LF>

  Loading Done<CR><LF>

- First, select the BT profile using the *at+rsi_opermode* command. For the BT profile give the first parameter as 327680.

  ```
  [TX] - at+rsi_opermode=327680,0,1,2147483648,2150629376,1073741824<CR><LF>
  [RX] - OK<CR><LF>
  bt_loaded<CR><LF>
  ```

- Now set the BT profile using the *at+rsibt_setprofilemode* command. For the SPP profile select the parameter as 1.

  ```
  [TX] - at+rsibt_setprofilemode=1<CR><LF>
  [RX] - OK<CR><LF>
  ```

- Set the module name using *at+rsibt_setlocalname* command e.g. "BT_Slave"

  ```
  [TX] - at+rsibt_setlocalname=16,RS9116W_BT_Slave<CR><LF>
  [RX] - OK<CR><LF>
  ```

- Set the discovery mode by using *at+rsibt_setdiscvmode* command. Give value 1 to set the mode.

  ```
  [TX] - at+rsibt_setdiscvmode=1<CR><LF>
  [RX] - OK <CR><LF>
  ```

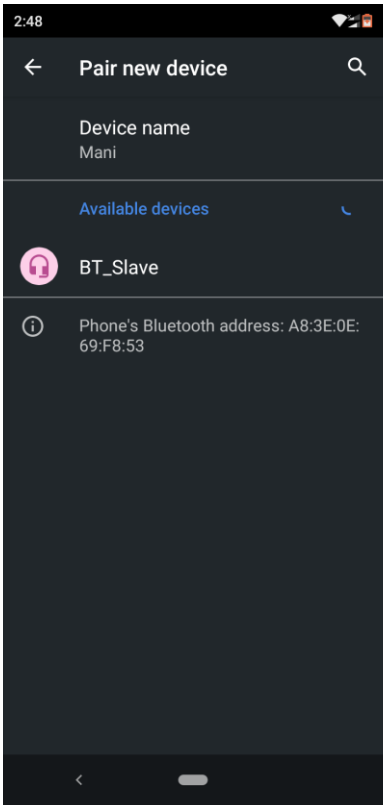
- Set the connection mode by using the *at+rsibt_setconnmode* command. Give value 1 to set the mode.

  ```
  [TX] - at+rsibt_setconnmode=1<CR><LF>
  [RX] - OK <CR><LF>
  ```

Note*:Once the pysical level connection happends then only the "Bluetooth spp Manager" will detect the device. So, please flow the below procedure for the pysical level connection followed by "Bluetooth spp Manager" functioning*.

4.6.1.1.3 Test Procedure

- In the Android phone go to ***Settings-> Wireless and network-> Bluetooth Settings***. Turn on the Bluetooth set device and make it visible. Click on the "pair a new device" option.



2:48

Pair new device

Device name
Mani

Available devices

BT_Slave

Phone's Bluetooth address: A8:3E:0E:69:F8:53

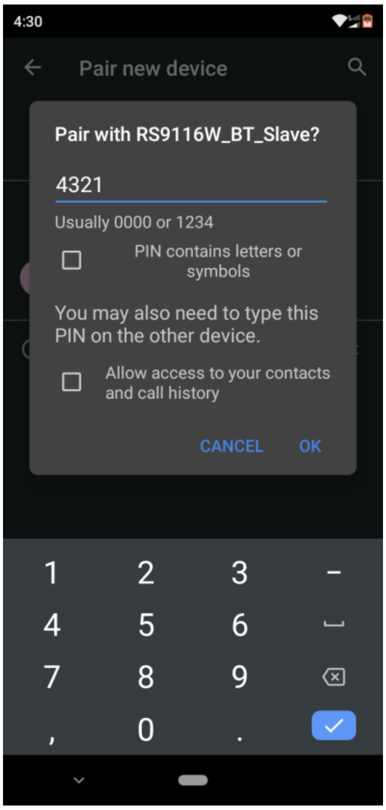
- Click on the "RS9116W_BT_Slave". You will get the below request.

  [RX] - AT+RSIBT_USRPINCODEREQ A8-3E-0E-69-F8-53<CR><LF>

  [TX] - at+rsibt_usrpincode=A8-3E-0E-69-F8-53,1,4321<CR><LF>

  [RX] - OK <CR><LF>

- Need to enter the "4321" pin code in the pair dialogue box. as shown in below



4:30

Pair new device

Pair with RS9116W_BT_Slave?

4321

Usually 0000 or 1234

□ PIN contains letters or symbols

You may also need to type this PIN on the other device.

□ Allow access to your contacts and call history

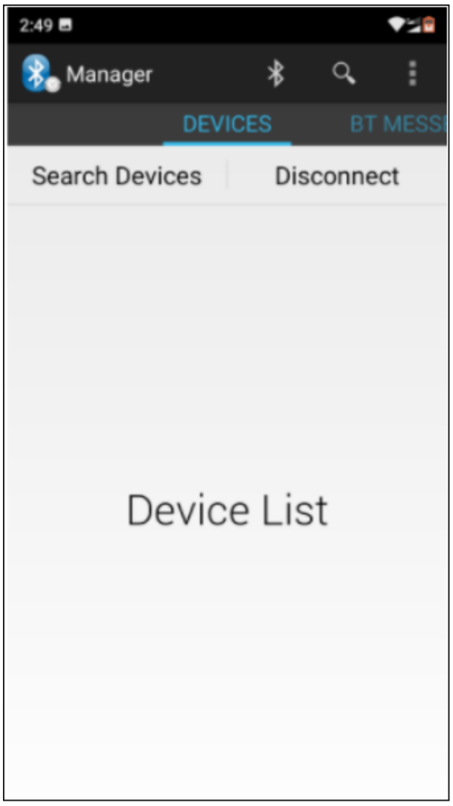
- For the first time, the disconnection is happens. you will see the linkeysave in the serial termianla as below.

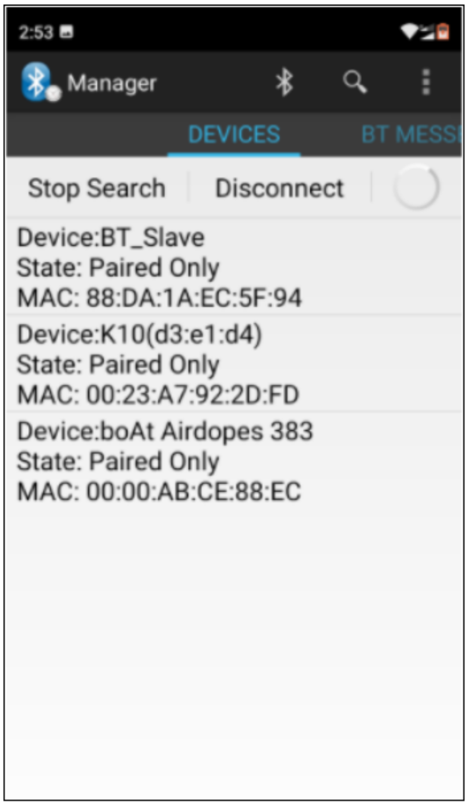
  [RX] - AT+RSIBT_USRLINKKEYSAVE A8-3E-0E-69-F8-53,8B,11,16,7C,37,8,2C,FB,43,BA,FB,98,8E,5B,7E,1F<CR><LF>

  [RX] - AT+RSIBT_BONDRESP A8-3E-0E-69-F8-53,0<CR><LF>

  [RX] - AT+RSIBT_CLASSIC_DISCONNECTED A8-3E-0E-69-F8-53,4E13<CR><LF>

- Open the "Bluetooth spp Manager" application. And clieck on the "search devices" option for scanning other bluetooth devices.





Device:BT_Slave
State: Paired Only
MAC: 88:DA:1A:EC:5F:94

Device:K10(d3:e1:d4)
State: Paired Only
MAC: 00:23:A7:92:2D:FD

Device:boAt Airdopes 383
State: Paired Only
MAC: 00:00:AB:CE:88:EC

- Click on the "BT_Slave". You will get the dialogue box as below.

  [RX] - AT+RSIBT_BONDRESP A8-3E-0E-69-F8-53,0<CR><LF>

  [RX] - AT+RSIBT_USRLINKKEYREQ A8-3E-0E-69-F8-53<CR><LF>

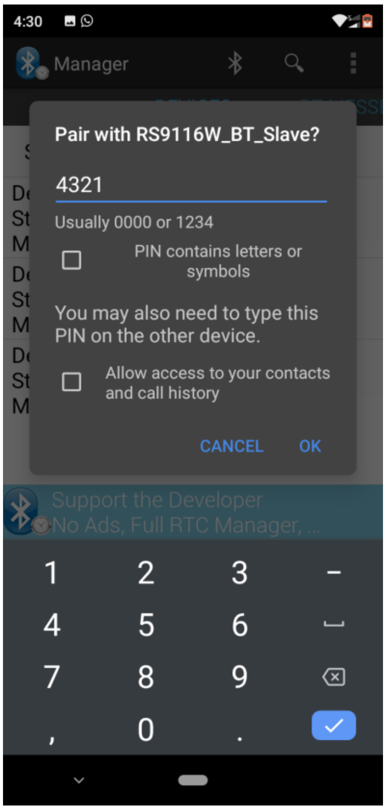
  [TX] - at+rsibt_usrlinkkey=A8-3E-0E-69-F8-53,0,4321<CR><LF>

  [RX] - OK <CR><LF>

  AT+RSIBT_USRPINCODEREQ A8-3E-0E-69-F8-53<CR><LF>

  [TX] - at+rsibt_usrpincode=A8-3E-0E-69-F8-53,1,4321<CR><LF>

  [RX] - OK <CR><LF>



Pair with RS9116W_BT_Slave?

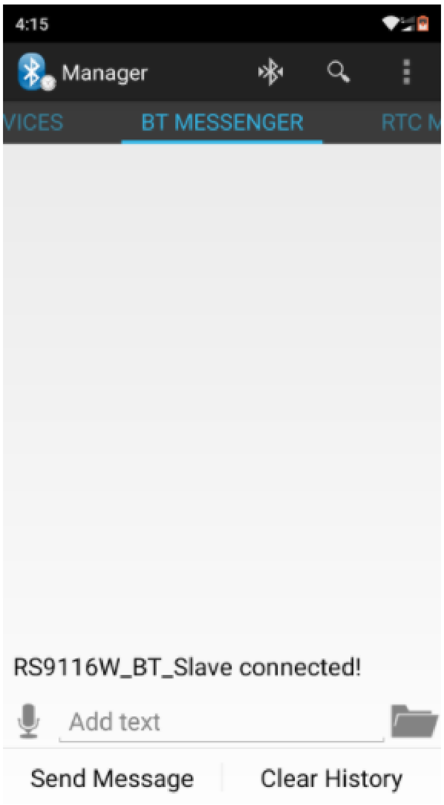
4321

Usually 0000 or 1234

☐ PIN contains letters or symbols

You may also need to type this PIN on the other device.

☐ Allow access to your contacts and call history

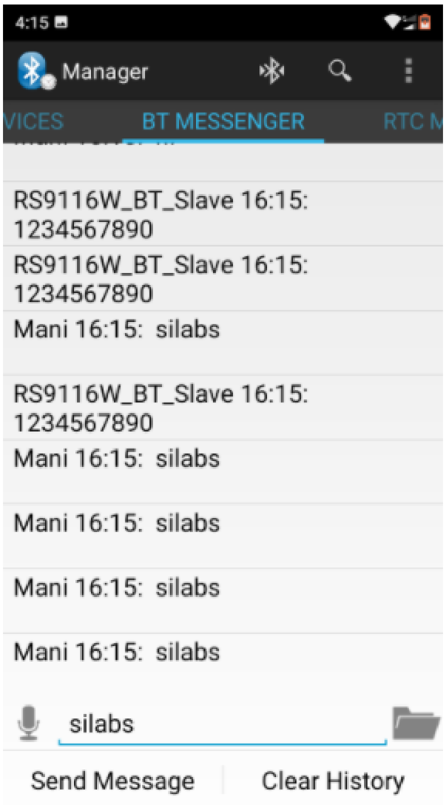


RS9116W_BT_Slave connected!

- Once the connection is happen then you will get the below userlinkysave in the serial terminal.

```
[RX] - AT+RSIBT_USRLINKKEYSAVE A8-3E-0E-69-F8-
53,A7,BA,4B,14,CA,C,49,80,C5,AC,8A,58,72,41,E5,7<CR><LF>
[RX] - AT+RSIBT_AUTHENTICATION_STATUS A8-3E-0E-69-F8-53,1<CR><LF>
[RX] - AT+RSIBT_SPPCONNECTED A8-3E-0E-69-F8-53<CR><LF>
[TX] - at+rsibt_spptx=10,1234567890<CR><LF>
[RX] - OK <CR><LF>
[TX] - at+rsibt_spptx=10,1234567890<CR><LF>
```

```
[RX] - OK <CR><LF>
[TX] - at+rsibt_spptx=10,1234567890<CR><LF>
[RX] - OK <CR><LF>
[RX] - AT+RSIBT_SPPRX 7,silabs<LF><CR>
<LF>
[RX] - AT+RSIBT_SPPRX 7,silabs<LF><CR>
<LF>
[RX] - AT+RSIBT_SPPRX 7,silabs<LF><CR>
<LF>
[RX] - AT+RSIBT_MODECHANGED A8-3E-0E-69-F8-53,2,792<CR><LF>
```



RS9116W_BT_Slave 16:15: 1234567890

RS9116W_BT_Slave 16:15: 1234567890

Mani 16:15: silabs

RS9116W_BT_Slave 16:15: 1234567890

Mani 16:15: silabs

Mani 16:15: silabs

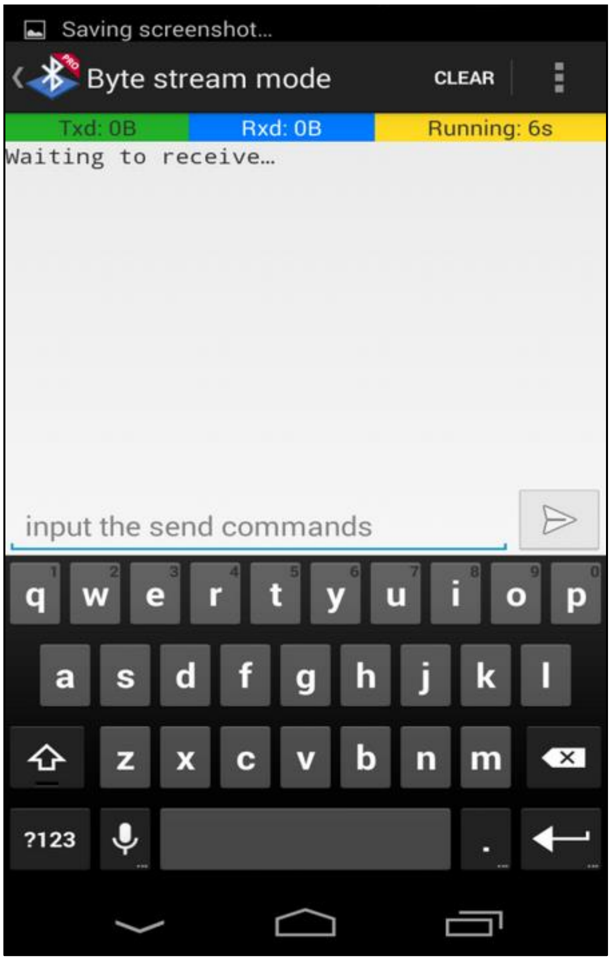
Mani 16:15: silabs

Mani 16:15: silabs

silabs

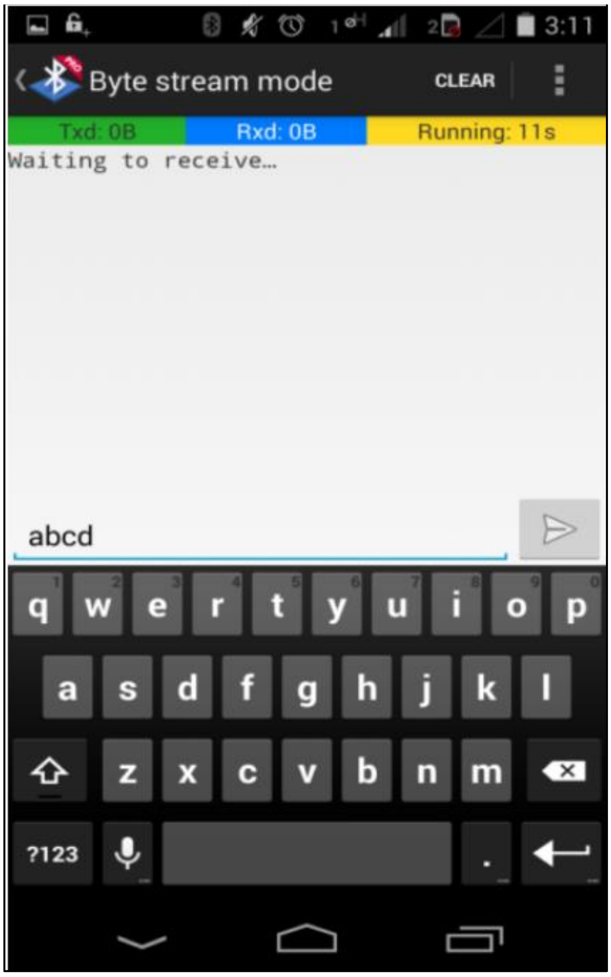
Select "Byte Stream mode" on that screen.

- Selection of Byte Stream mode will open a communication window as shown below:



Waiting to receive…

- Now send some bytes (e.g. string "abcd" here) from Phone to module, by typing abcd and pressing the arrow to send:



Byte stream mode

CLEAR

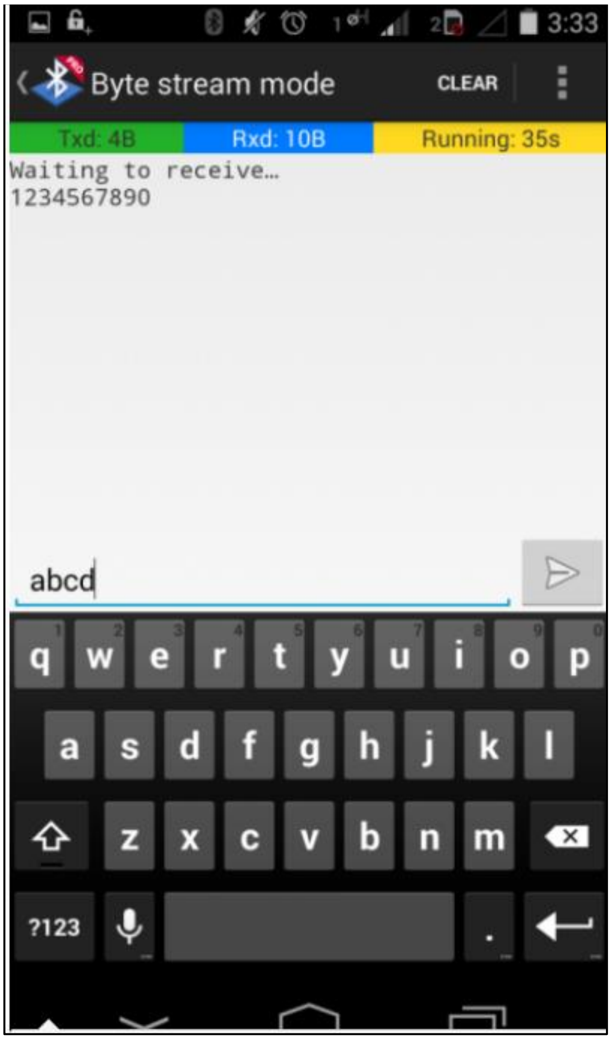
Txd: 0B | Rxd: 0B | Running: 11s

Waiting to receive…

abcd

This string will be received on the module as *SPPRX* as shown below:
AT+RSIBT_SPPRX 4,abcd<CR><LF>

- Similarly, the module can also send some bytes to the phone by giving *SPPTX* command. Give the data you want to send in the 2nd argument of this command. for ex., let the data is 1234567890.
  [TX] - at+rsibt_spptx=10,1234567890<CR><LF>
  [RX] - OK<CR><LF>
  This string will be received on the Phone as shown below:



Waiting to receive…
1234567890

abcd

4.7 Wi-Fi + BLE Evaluation in UART Mode

The following sub-sections describe configuring and using the module in different operational modes of Wi-Fi + BLE.

4.7.1 Wi-Fi + BLE Evaluation using AT Commands

4.7.1.1 Wi-Fi Client + BLE Peripheral Mode

4.7.1.1.1 Wi-Fi Client + BLE Peripheral Mode Configuration

In order to run the Wi-Fi client and BT-LE coexistence mode, issue the operating mode as the first command with the relevant coexistence parameters. After the operating mode command, the module will operate in both WiFi and BT LE mode and will respond to WiFi commands as well as BT LE commands in parallel.

Common Command: Set the operating mode command with below parameters to run in Wi-Fi + BT-LE Coex Mode.
Oper_mode = ((wifi_oper_mode) | (coex_mode << 16))
Wifi_oper_mode = 0 (to operate wifi in STA mode)
Coex_mode=13(to operate in WiFi+BT LE coex mode)
Feature_bit_map = 0
Tcp_ip_feature_bit_map =4 (DHCPv4 client)
Custom_feature_bit_map=0
ext_custom_feature_bit_map=As required
bt_custom_feature_bit_map=As required
ext_tcp_ip_feature_bit_map=0
ble_custom_feature_bit_map=As required
at+rsi_opermode=851968,0,4,2147483648,2149580800,3221225472,0,1966080
Wi-Fi Command Sequence to Associate with Access Point:

- **Band :** This command sets the operating mode of the module

- **Init :**This command initializes the module
- **Scan:** This command scans for Access points in the vicinity and reports them.
- **Join:** This command associates the module to the AP

Refer to Sections Wi-Fi Client in Personal Security Mode for the full list of commands and corresponding descriptions.
BLE Command Sequence:

- **Advertise:** This command advertises the local name of the module in peripheral roles.
  Refer to Sections BLE in Peripheral (Slave) Mode for the full list of commands and corresponding descriptions.

4.7.1.1.2 Test Procedure Refer to Sections Wi-Fi Client in Personal Security Mode and BLE in Peripheral (Slave) Mode for the respective test procedures.

4.7.1.2 Wi-Fi Client + BLE Central Mode

Wi-Fi Client + BLE Central Mode Configuration

In order to run the Wi-Fi client and BT-LE coexistence mode, issue the operating mode as the first command with the relevant coexistence parameters. After the operating mode command, the module will operate in both WiFi and BT LE mode and will respond to WiFi commands as well as BT LE commands in parallel.
Common Command: Set the operating mode command with below parameters to run in Wi-Fi + BT-LE Coex Mode.
Oper_mode = ((wifi_oper_mode) | (coex_mode << 16))
Wifi_oper_mode = 0 (to operate wifi in STA mode)
Coex_mode=13(to operate in WiFi+BT LE coex mode)
Feature_bit_map = 0
Tcp_ip_feature_bit_map =4 (DHCPv4 client)
Custom_feature_bit_map=0
ext_custom_feature_bit_map=As required
bt_custom_feature_bit_map=As required
ext_tcp_ip_feature_bit_map=0
ble_custom_feature_bit_map=As required
at+rsi_opermode=851968,0,4,2147483648,2149580800,3221225472,0,1966080

Wi-Fi Command Sequence to Associate with Access Point:

- **Band:** This command sets the operating mode of the module
- **Init:** This command initializes the module
- **Scan:** This command scans for Access points in the vicinity and reports them.
- **Join:** This command associates the module to the AP

Refer to Sections Wi-Fi Client in Personal Security Mode for the full list of commands and corresponding descriptions.
BLE Command Sequence:

- **Scan:** This command scans for BT LE devices and reports the devices found
- **Connect:** This command initializes a connection to a remote peripheral device.
  Refer to Sections BLE Evaluation using AT Commands for the full list of commands and corresponding descriptions.

4.7.1.2.1 Test Procedure

Refer to Sections Wi-Fi Client in Personal Security Mode and BLE Evaluation using AT Commands for the respective test procedures.

4.7.1.3 Wi-Fi AP + BLE Peripheral Mode

Wi-Fi AP + BLE Peripheral Mode Configuration
In order to run the Wi-Fi AP and BT-LE coexistence mode, issue the operating mode as the first command with the relevant coexistence parameters. After the operating mode command, the module will operate in both WiFi and BT LE mode and will respond to WiFi commands as well as BT LE commands in parallel.
Common Command: Set the operating mode command with below parameters to run in Wi-Fi + BT-LE Coex Mode.
Oper_mode = ((wifi_oper_mode) | (coex_mode << 16))
Wifi_oper_mode = 6 (to operate wifi in STA mode)
Coex_mode=13(to operate in WiFi+BT LE coex mode)
Feature_bit_map = 0
Tcp_ip_feature_bit_map = 18 (HTTP server + DHCPv4 server)
Custom_feature_bit_map=0
ext_custom_feature_bit_map=As required

bt_custom_feature_bit_map=As required
ext_tcp_ip_feature_bit_map=0
ble_custom_feature_bit_map=As required
at+rsi_opermode=851974,0,18,2147483648,2149580800,3221225472,0,1966080

Wi-Fi Command Sequence to Associate with Access Point:

- **Band:** This command sets the operating mode of the module.
- **Init:** This command initializes the module.
- **IPConfig:** This command configures the DHCP server on the module.
- **APConfig:** This command configures the AP related parameters on the module.

Refer to Sections Wi-Fi Access Point Mode for the full list of commands and corresponding descriptions.
BLE Command Sequence:

- **Advertise:** This command advertises the local name of the module in a peripheral roles.
  Refer to Sections BLE Evaluation using AT Commands for the full list of commands and corresponding descriptions.

4.7.1.3.1 Test Procedure

Refer to Sections Wi-Fi Access Point Mode for and BLE Evaluation using AT Commands for the respective test procedures.

4.7.1.4 Wi-Fi AP + BLE Central Mode

Wi-Fi AP + BLE Peripheral Mode Configuration
In order to run the Wi-Fi AP and BT-LE coexistence mode, issue the operating mode as the first command with the relevant coexistence parameters. After the operating mode command, the module will operate in both WiFi and BT LE mode and will respond to WiFi commands as well as BT LE commands in parallel.
Common Command: Set the operating mode command with below parameters to run in Wi-Fi + BT-LE Coex Mode.
Oper_mode = ((wifi_oper_mode) | (coex_mode << 16))
Wifi_oper_mode = 6 (to operate wifi in STA mode)
Coex_mode=13(to operate in WiFi+BT LE coex mode)
Feature_bit_map = 0
Tcp_ip_feature_bit_map = 18 (HTTP server + DHCPv4 server)
Custom_feature_bit_map=0
ext_custom_feature_bit_map=As required
bt_custom_feature_bit_map=As required
ext_tcp_ip_feature_bit_map=0
ble_custom_feature_bit_map=As required
at+rsi_opermode=851974,0,18,2147483648,2149580800,3221225472,0,1966080

Wi-Fi Command Sequence to Associate with Access Point:

- **Band:** This command sets the operating mode of the module
- **Init:** This command initializes the module
- **IPConfig:** This command configures the DHCP server on the module.
- **APConfig:** This command configures the AP related parameters on the module.

Refer to Sections Wi-Fi Access Point Mode for the full list of commands and corresponding descriptions.
BLE Command Sequence:

- **Scan:** This command scans for BT LE devices and reports the devices found
- **Connect:** This command initializes a connection to a remote peripheral device.

Refer to Sections BLE Evaluation using AT Commands for the full list of commands and corresponding descriptions.

4.7.1.4.1 Test Procedure

Refer to Sections Wi-Fi Access Point Mode for and BLE Evaluation using AT Commands or the respective test procedures.

5 Configuration over Wi-Fi

The module can be configured wirelessly to join a specific AP (referred to as "auto-connect") or create an Access Point (referred to as "auto-create").

5.1 Configuration to connect to an Access Point

Flow 1: In this flow, an AP is first created in the module, to which a remote device connects and configures the module.

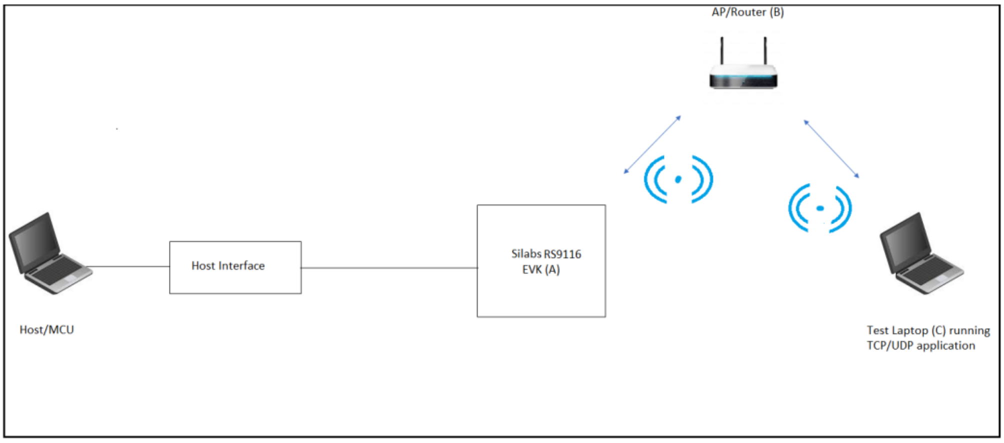


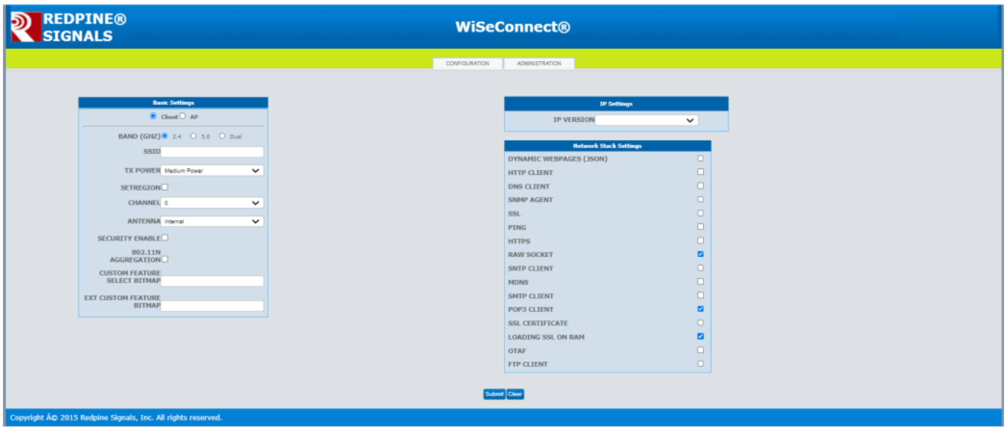
Figure 20: Module Configured as Access Point

1. Connect a PC or Host to the module through the USB and power up the module.
2. Configure the module to become an AP and DHCP Server by issuing commands from PC (P) as in section Evaluation of Access Point Mode. The sequence of commands is given below.

- at+rsi_opermode=6,1,18,0
- at+rsi_band=0
- at+rsi_init
- at+rsi_fwversion?
- at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168.0.30
- at+rsi_apconf=6,SILABS_AP,0,0,0,100,3,4
- at+rsi_join=SILABS_AP,0,2,0

The module is now configured as an Access Point. Its IP address is **192.168.0.30.**

1. Connect a Laptop (B) to the created AP. Open the URL **http://<Module's IP address>**in the Laptop. In this case, the URL is http://192.168.0.30. Make sure the browser in the laptop does not have any proxies enabled.
2. The module's web page opens as shown in the figure below.



Basic Settings

● Client ○ AP

BAND (GHZ) ● 2.4 ○ 5.0 ○ Dual
SSID
TX POWER Medium Power
SETREGION □
CHANNEL 0
ANTENNA Internal
SECURITY ENABLE □
802.11N AGGREGATION □
CUSTOM FEATURE SELECT BITMAP
EXT CUSTOM FEATURE BITMAP

IP Settings

IP VERSION

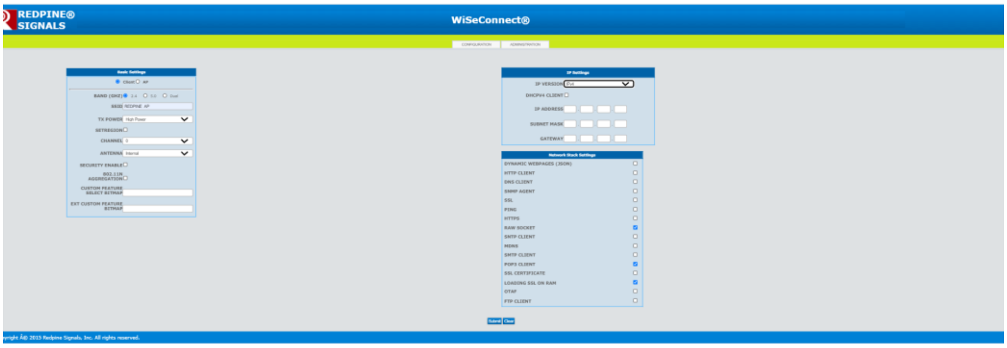
Network Stack Settings

DYNAMIC WEBPAGES (JSON) □
HTTP CLIENT □
DNS CLIENT □
SNMP AGENT □
SSL □
PING □
HTTPS □
RAW SOCKET ☑
SNTP CLIENT □
MDNS □
SMTP CLIENT □
POP3 CLIENT ☑
SSL CERTIFICATE □
LOADING SSL ON RAM ☑
OTAF □
FTP CLIENT □

Copyright Â© 2015 Redpine Signals, Inc. All rights reserved.

Figure 21: Module Webpage

1. On the page, select "Client" under Basic Settings. The page changes to show the settings required to be configured for the module in Client mode, as shown in the figure below.



● Client ○ AP

BAND (GHZ) ● 2.4 ○ 5.0 ○ Dual

SSID REDPINE AP

TX POWER High Power

SETREGION □

CHANNEL 0

ANTENNA Internal

SECURITY ENABLE □

802.11N AGGREGATION □

CUSTOM FEATURE SELECT BITMAP

EXT CUSTOM FEATURE BITMAP

IP VERSION IPv4

DHCPV4 CLIENT □

IP ADDRESS

SUBNET MASK

GATEWAY

DYNAMIC WEBPAGES (JSON) □

HTTP CLIENT □

DNS CLIENT □

SNMP AGENT □

SSL □

PING □

HTTPS □

RAW SOCKET ☑

SNTP CLIENT □

MDNS □

SMTP CLIENT □

POP3 CLIENT ☑

SSL CERTIFICATE □

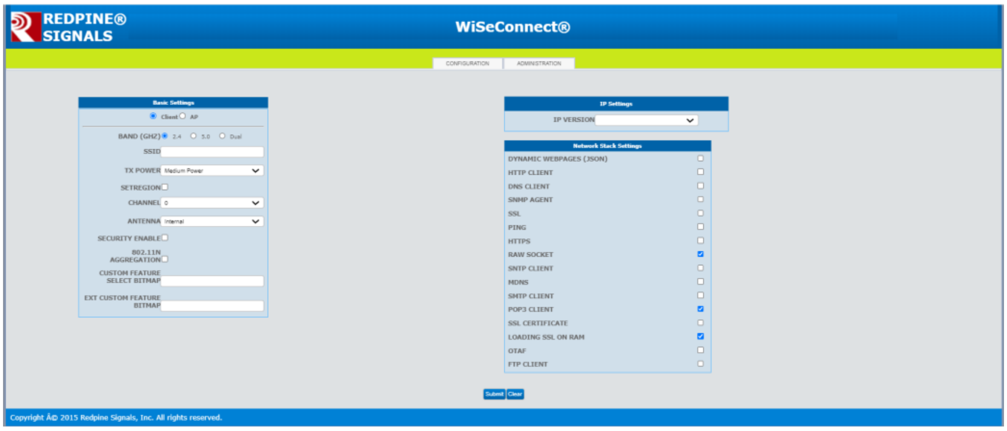
LOADING SSL ON RAM ☑

OTAF □

FTP CLIENT □

Figure 22: Client Mode Webpage

1. Select the Band and enter SSID of the Access Point to which the module needs to be connected to.
2. Set the "TX POWER" to "High Power".
3. Select "0" in the drop-down menu for Channel – this ensures that the module will scan in all the channels for the Access Point.
4. If the Access Point is in Secure mode, click the radio button next to "SECURITY ENABLE" and then input the security parameters as per the Access Point's settings. In this example, the Access Point is in Open (non-Secure) mode.
5. Click the radio button next to "802.11N AGGREGATION" to enable A-MPDU aggregation.
6. For details on the "CUSTOM FEATURE BITMAP", refer to the Software PRM.
7. Under IP Settings, select between IPv4, IPv6 and Both and enter the IP Settings (DHCP Enable/Disable) as per the settings in the Access Point. In this example, we have selected IPv4 and enabled DHCP, as shown in the figure below.



● Client ○ AP

BAND (GHZ) ● 2.4 ○ 5.0 ○ Dual

SSID

TX POWER Medium Power

SETREGION □

CHANNEL 0

ANTENNA Internal

SECURITY ENABLE □

802.11N AGGREGATION □

CUSTOM FEATURE SELECT BITMAP

EXT CUSTOM FEATURE BITMAP

IP VERSION

DYNAMIC WEBPAGES (JSON) □

HTTP CLIENT □

DNS CLIENT □

SNMP AGENT □

SSL □

PING □

HTTPS □

RAW SOCKET ☑

SNTP CLIENT □

MDNS □

SMTP CLIENT □

POP3 CLIENT ☑

SSL CERTIFICATE □

LOADING SSL ON RAM ☑

OTAF □

FTP CLIENT □

Figure 23: Example Client Mode Configuration

1. Click on the "Submit" button. The information is sent to the module and stored in its internal flash.
2. The module should now be power cycled or hard reset. It boots up and then automatically scans channels for the target AP and connects to it and gets an IP address. The module will send out two responses to the Host (PC), the first corresponds to the internally given "Join" command and the second to the "Set IP Parameters" command. Note that once the module is restarted, no commands need to be given. The module automatically scans and joins the target AP, after which the stored configuration parameters can be retrieved using the command "at+rsi_cfgget". If the auto-connect feature needs to be disabled, issue the command "at+rsi_cfgenable=0". Refer to the PRM for more details on these commands.

Flow 2: In this flow, the module is connected to an AP. A remote device connects to the same AP and configures the module.

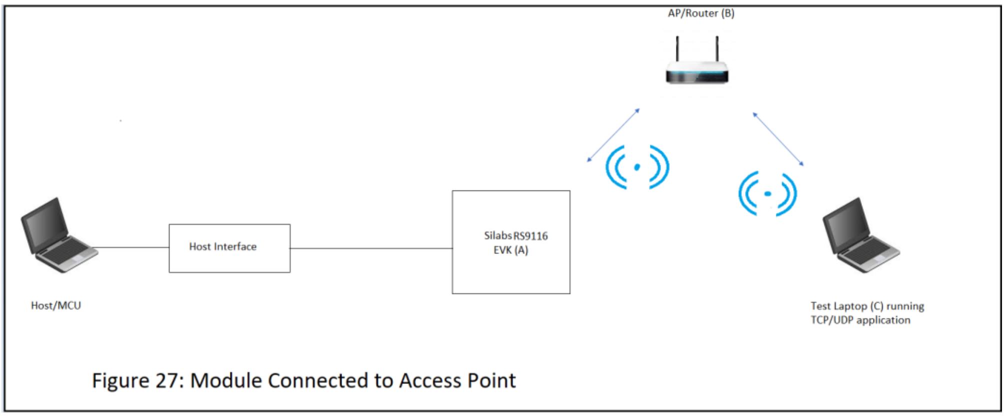


Figure 24: Module Connected to Access Point

1. Connect a PC or Host to the module through the USB and power up the module.
2. Configure the module to become a client and connect to an AP as described in section Wi-Fi Client in Personal Security Mode.
3. Connect a Laptop (C) to the same AP. Open the URL http://<Module's IP address>in the Laptop. For example, if the module was configured to have an IP of 192.168.100.20, then the URL is http://192.168.100.20. Make sure the browser in the laptop does not have any proxies enabled.
4. Follow the instructions in Flow 1 from step 4 to reconfigure the module to connect to a different Access Point.

5.1.1 Configuration to Create an Access Point

Flow 1: In this flow, an AP is first created in the module, to which a remote device connects and configures the module.

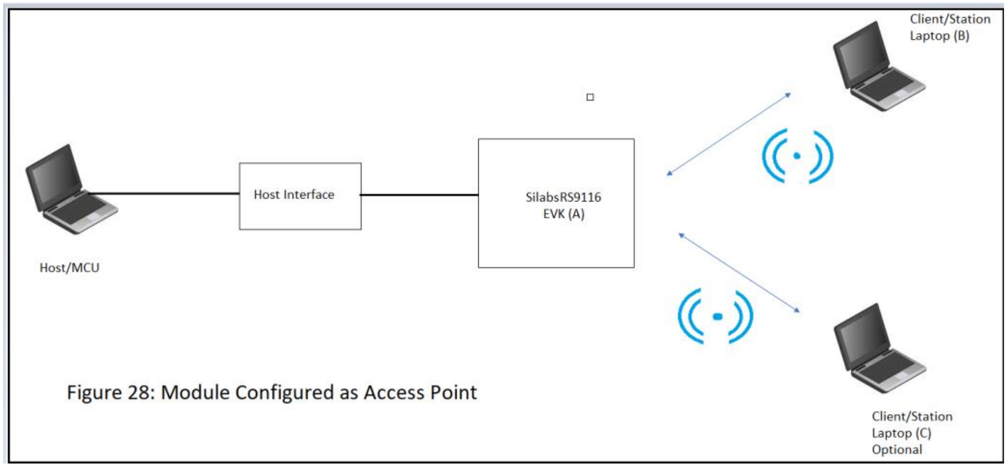


Figure 25: Module Configured as Access Point

For Creating an Access Point, follow the above steps in **Flow 1** that is given under **"Configuration to connect to an Access Point".**

Flow 2: In this flow, the module is connected to an AP. A remote device connects to the same AP and configures the module.

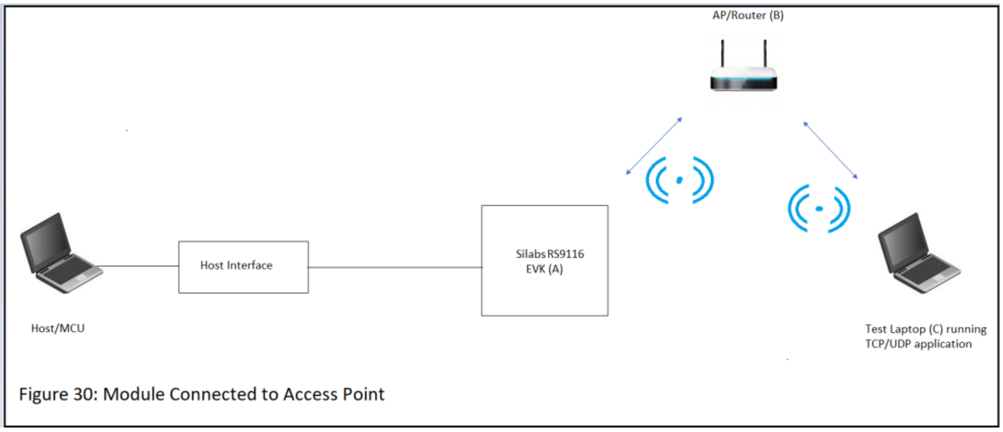


Figure 26: Module Connected to Access Point

1. Connect a PC or Host to the module through the USB and power up the module.
2. Configure the module to become a client and connected to an AP by issuing commands through PC (P).
3. Connect a Laptop (c) to the created AP. Open the URL **http://<Module's IP address>**in the Laptop. For example, if the module was configured to have an IP of 192.168.100.1, then the URL is http://192.168.100.1. Make sure the browser in the laptop does not have any proxies enabled.
4. Follow the instructions in **Flow 1** from step 4 to reconfigure the module as an Access Point.

6 Appendix A_ Headers on the EVB

6.1 Headers' Pin Orientations

The figure below shows the pin orientations for the SDIO/SPI header.

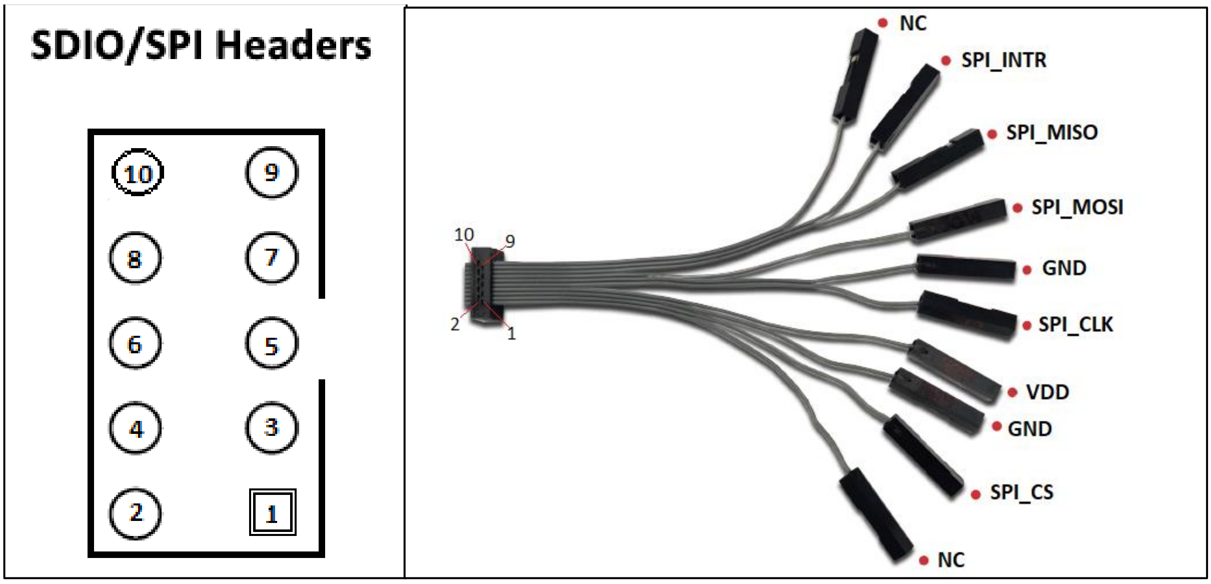


Figure 27: Headers' Pin Orientations

6.2 SPI Header Pin Description

The following table describes the pins of the SPI header.

Table 1: SPI Header Pins

Pin Number	Pin Name	Direction	Description
1	NC	-	This pin must be left open.
2	SPI_CS	Input	SPI slave select from the host(active low)
3	GND	-	Ground
4	VDD	-	Supply voltage.
5	SPI_CLK	Input	Serial clock in from the host. The clock can be up to80 MHz
6	GND	-	Ground
7	SPI_MOSI	Input	SPI data input
8	SPI_MISO	Output	SPI data output
9	SPI_INTR	Output	Active high, level triggered interrupt, used in SPI mode. The interrupt is raised by the EVB to indicate there is data to be read by the Host.
10	NC	-	No Connect

6.3 SDIO Header Pin Description

The following table describes the pins of the SDIO header.

Table 2: SDIO Header Pins

Pin Number	Pin Name	Direction	Description
1	SDIO_DATA3	Input/Output	Data3 of the SDIO interface.
2	SDIO_CMD	Input/Output	SDIO Mode: SDIO interface command signal.
3	GND	-	Ground
4	VDD	-	Supply voltage.
5	SDIO_CLK	Input	This signal is the SDIO clock.
6	GND	-	Ground
7	SDIO_DATA0	Input/Output	Data0 of the SDIO interface.
8	SDIO_DATA1	Input/Output	Data1 of the SDIO interface.
9	SDIO_DATA2	Input/Output	Data2 of the SDIO interface.
10	NC	-	No Connect

Reset - When the EVB is powered through the USB on "Power" port or through the power on any interface (UART, USB, USB-CDC, SDIO/SPI) then it gets the Power-on Reset.

To control the reset there are two methods:

1. Reset Button on the baseboard.
2. The host can control the Reset by controlling the pin #2 (RST_PS) on header J9 via GPIO.

Note:
Signal Integrity Guidelines for SPI/SDIO interface: Glitches in the SPI/SDIO clock can potentially take the SPI/SDIO interface out of synchronization. The quality and integrity of the clock line need to be maintained. In case a cable is used for the board to board connection, the following steps are recommended (please note that this is not an exhaustive list of guidelines and depending on individual cases additional steps may be needed):

1. Minimize the length of the SPI/SDIO bus cable to as small as possible, preferably to within an inch or two.
2. Increase the number of ground connections between the EVB and the Host processor PCB.

7 Example Applications

Example	Description	Application path
WLAN station and TCP client	This example demonstrates how to configure the module in station mode and send data to the remote side using TCP client socket	sapis\examples\wlan\tcp_client
Access point creation and TCP server	This example demonstrates how to Configure the module in access point mode and receive the data from the remote side using the TCP server socket.	sapis\examples\wlan\access_point
BT SPP slave	This application demonstrates how to configure the device in Slave mode and establish an SPP profile connection with the remote Master device and data exchange between two devices using the SPP profile.	sapis\examples\bt\spp_slave
Simple chat using BLE and WLAN station coex	This example demonstrates the data exchanges between BLE and WLAN applications.	sapis\examples\wlan_ble\wlan_station_ble_dual_role_bridge
Simple chat using BT and WLAN station coex	This example demonstrates the data exchanges between BT and WLAN applications	sapis\examples\wlan_bt\wlan_bt_bridge

Note: There are many other examples for WLAN, BT Classic and BLE protocols and co-existence applications, please refer to sapis\examples\ folder in the release package.

Refer AN1282: RS9116W_Guide_for_SAPI_Application_Examples doc from https://docs.silabs.com/rs9116

8 Appendix C_Running Tera Term Scripts

To download and set up TeraTerm, follow these steps:

1. Navigate to the Source-Forge (TeraTerm) website: http://en.sourceforge.jp/projects/ttssh2/releases/

2. Download the emulator.

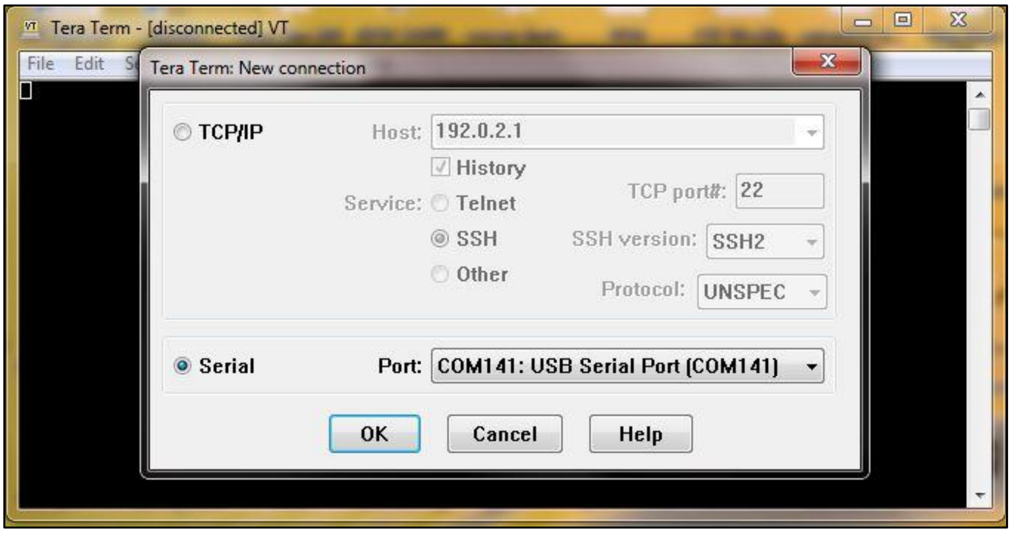
3. Run the downloaded file and navigate through the installer. Select the standard default settings when prompted.

4. Connect Micro A/B-type USB cable between the USB port of the PC and the micro-USB port of the EVB labeled “UART”.

5. Open TeraTerm. Upon opening, TeraTerm prompts for connection information. We are using a serial connection (not the default TCP/IP).

6. Select Serial (**Note:** To be able to select "Serial" port initially RS9116 has to be connected to PC using UART interface)

7. From the Port drop-down menu, choose the COM port which has detected as connected EVB to PC(Check step4 if COM port not detected and restart TeraTerm).



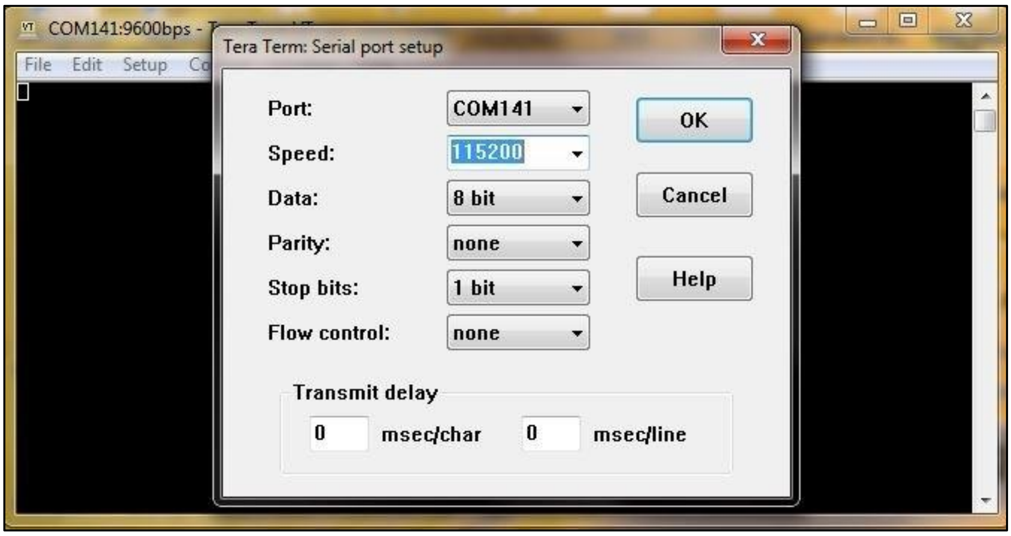
Tera Term: New connection

○ TCP/IP Host: 192.0.2.1
☑ History
Service: ○ Telnet TCP port#: 22
● SSH SSH version: SSH2
○ Other Protocol: UNSPEC

● Serial Port: COM141: USB Serial Port (COM141)

8. Set the serial port’s settings to match the RS9116's communications protocol. To adjust settings, navigate to Setup > Serial port.

9. Adjust the settings (as needed) according to the following:



Tera Term: Serial port setup

Port: COM141
Speed: 115200
Data: 8 bit
Parity: none
Stop bits: 1 bit
Flow control: none

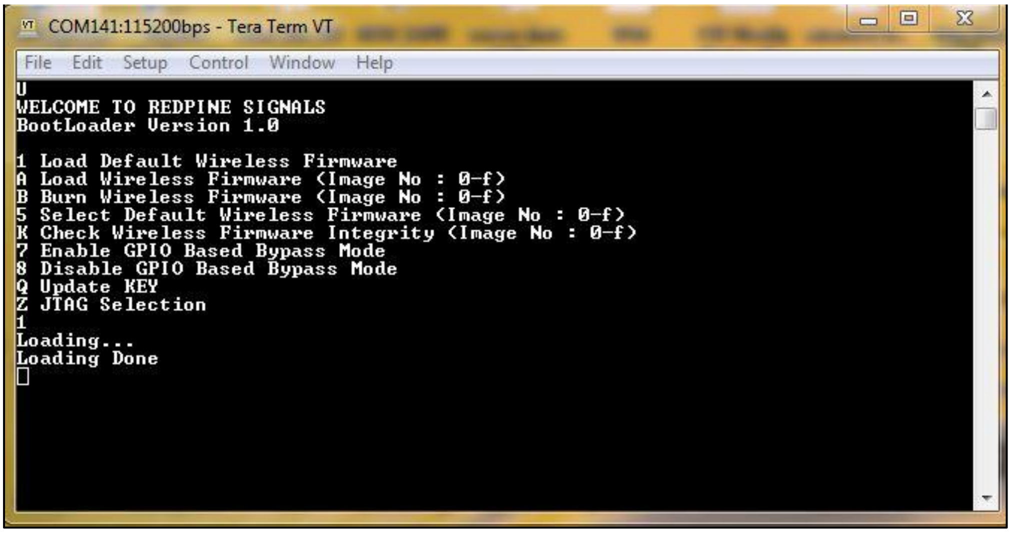
Transmit delay
0 msec/char 0 msec/line

10. Press OK to save the settings and to return to the terminal.

11. Now do the ABRD process by giving "Shift +| and Shift +u" then you will see the below prints.

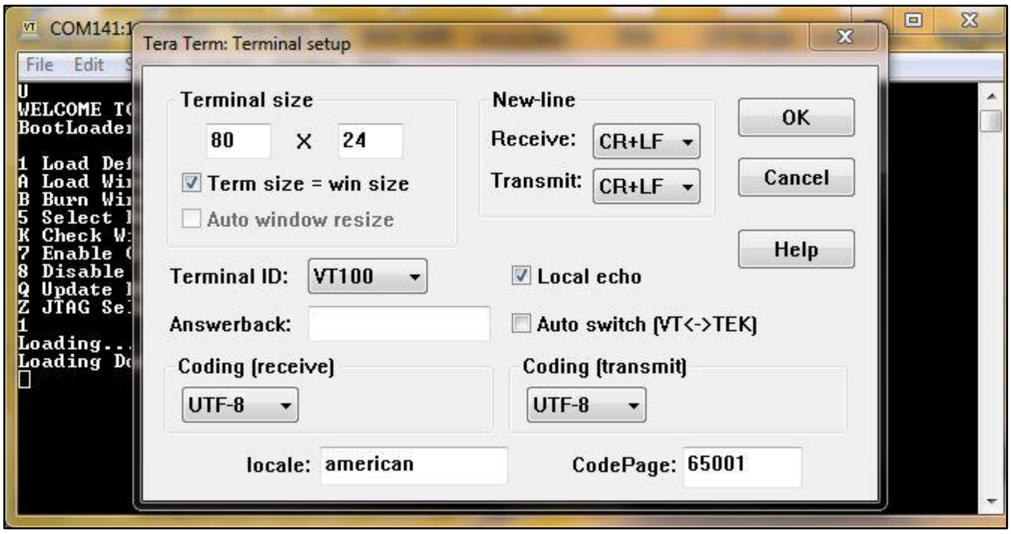
12. Hit ‘1’ and then you will see a message that says, “Loading…” followed by “Loading Done”.

13. If "Loading Done" doesn't appear check if the Module is in Binary mode. If yes, refer to "**Note 2**" (see below) and execute all these steps once again from the beginning.


COM141:115200bps - Tera Term VT
File Edit Setup Control Window Help

```
U
WELCOME TO REDPINE SIGNALS
BootLoader Version 1.0

1 Load Default Wireless Firmware
A Load Wireless Firmware (Image No : 0-f)
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
1
Loading...
Loading Done
```

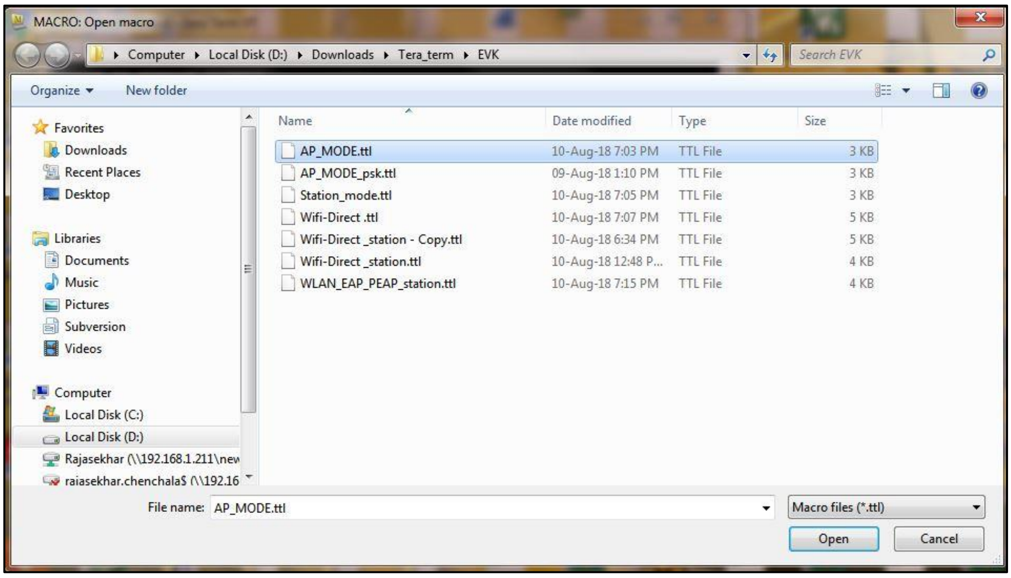
14. Set the Terminal settings by navigating to Setup > Terminal.



Terminal size: 80 X 24
☑ Term size = win size
☐ Auto window resize
New-line
Receive: CR+LF
Transmit: CR+LF
Terminal ID: VT100
☑ Local echo
Answerback:
☐ Auto switch (VT<->TEK)
Coding (receive): UTF-8
Coding (transmit): UTF-8
locale: american
CodePage: 65001

15. Finally, Choose the TTL script to run the example project by navigating to Control > Macro.

TeraTerm scripts are available in the release package at the following path: ***RS9116.NB0.WC.GENR.OSI.x.x.x\utils\scripts\TeraTerm_TTL_Scripts***

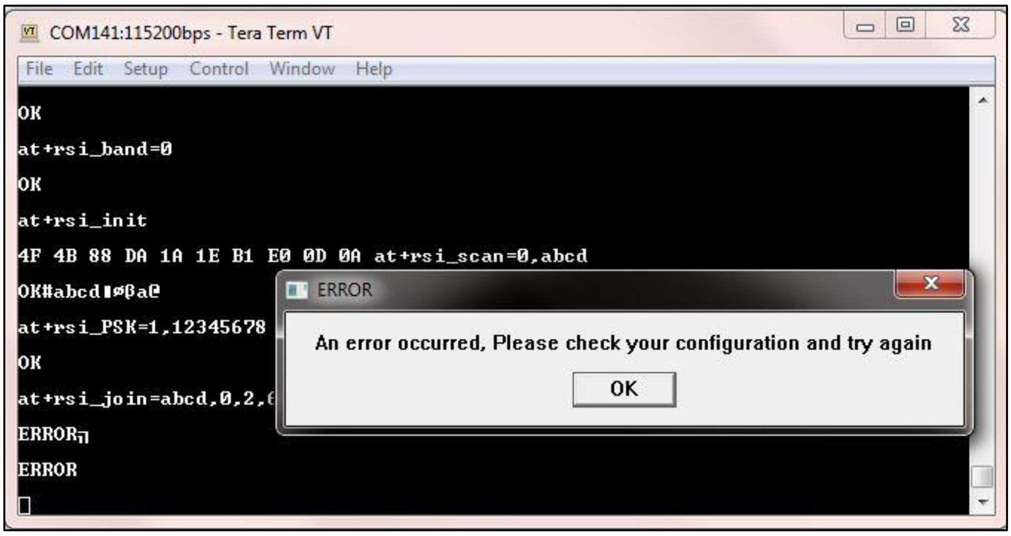


Name	Date modified	Type	Size
AP_MODE.ttl	10-Aug-18 7:03 PM	TTL File	3 KB
AP_MODE_psk.ttl	09-Aug-18 1:10 PM	TTL File	3 KB
Station_mode.ttl	10-Aug-18 7:05 PM	TTL File	3 KB
Wifi-Direct .ttl	10-Aug-18 7:07 PM	TTL File	5 KB
Wifi-Direct _station - Copy.ttl	10-Aug-18 6:34 PM	TTL File	5 KB
Wifi-Direct _station.ttl	10-Aug-18 12:48 P...	TTL File	4 KB
WLAN_EAP_PEAP_station.ttl	10-Aug-18 7:15 PM	TTL File	4 KB

File name: AP_MODE.ttl
Macro files (*.ttl)

16. If any error occurs pop up window will display "An error occurred, please check your configuration and try again",

Hit 'OK' and power recycle the module and then starts from the beginning.


COM141:115200bps - Tera Term VT
File Edit Setup Control Window Help

```
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 1E B1 E0 0D 0A at+rsi_scan=0,abcd
OK#abcd▮øßa@
at+rsi_PSK=1,12345678
OK
at+rsi_join=abcd,0,2,6
ERROR╖
ERROR
```

ERROR

An error occurred, Please check your configuration and try again

Note 1: If the Module is in binary to change from binary mode to AT mode, the user must give 'U' in the bootloader options.

Note 2 : For Low Power StandBy_Associated WiFi Station.ttl script present in folder "utils\scripts\TeraTerm_TTL_Scripts" there is no step by step execution procedure below, you can refer AN1280: RS9116W Power Save Application Notes from https://docs.silabs.com/rs9116

Note 3 : Before running “FW_upgrade_over_wifi.ttl” script, you need to clear the webpages which were loaded in the Module flash using following command’s.

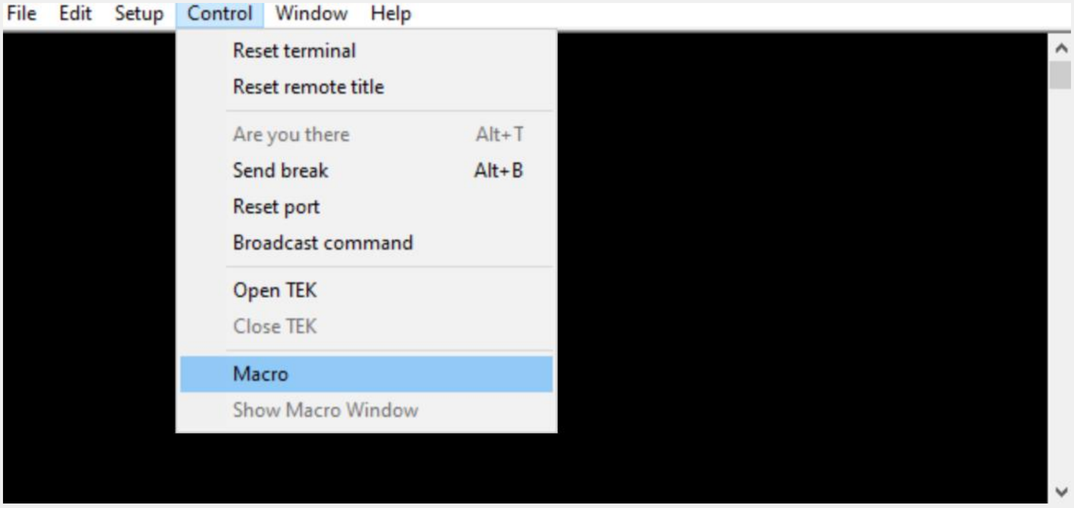
a)If you remember the webpage file name loaded in flash use the following command to erase the file : “at+rsi_erasefile=<filename>\r\n”

b)If you did not remember the webpage file name loaded in flash use the following command : “at+rsi_clearfiles=1\r\n”

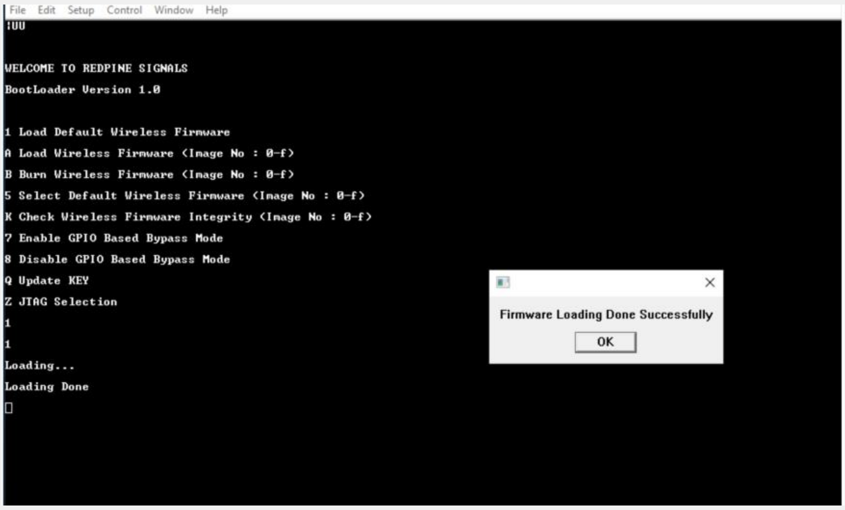
For detailed description, user can refer to the "RS9116W Wi-Fi AT Command Programming Reference Manual" from https://docs.silabs.com/rs9116

Note 4 : For all the Wi-Fi client related scripts(Station_mode, Low Power StandBy_Associated WiFi Station and BLE Advertising, Low Power StandBy_Associated WiFi Station.ttl) are in “WPA2_PSK” security mode. User need to configure the third party AP's in “WPA/WAP2_PSK” mode.

Note 5: All the ttl scripts are provided with default ABRD, user need to select the macro as is to run the ttl scripts. Ensure that the Teraterm settings which are mentioned in Step #7 to #10 are done before selecting the macro. Below image describes selecting the TTL scripts



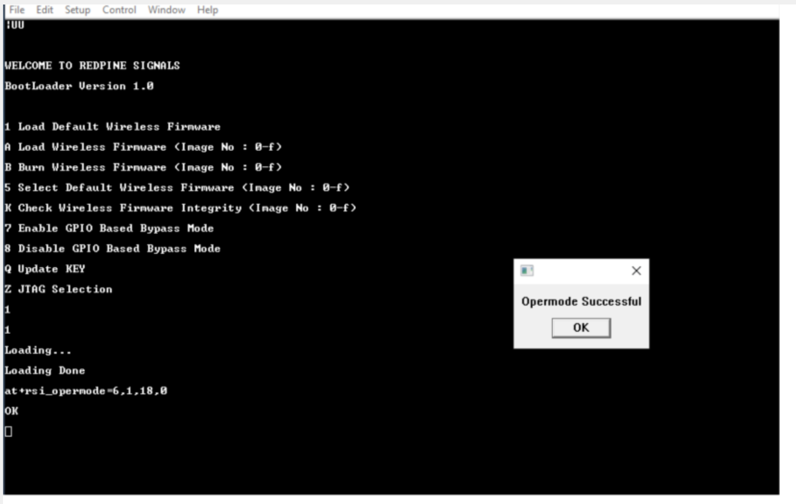
1. On the window that will pop-up, select the respective script from WiSeConnect release package in the following path "RS9116.NB0.WC.GENR.OSI.x.x.xx\utils\scripts\TeraTerm_TTL_Scripts",
2. The following pop will be displayed, PRESS OK on the popup



```
!UU

WELCOME TO REDPINE SIGNALS
BootLoader Version 1.0

1 Load Default Wireless Firmware
A Load Wireless Firmware (Image No : 0-f)
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
1
1
Loading...
Loading Done
```

Firmware Loading Done Successfully

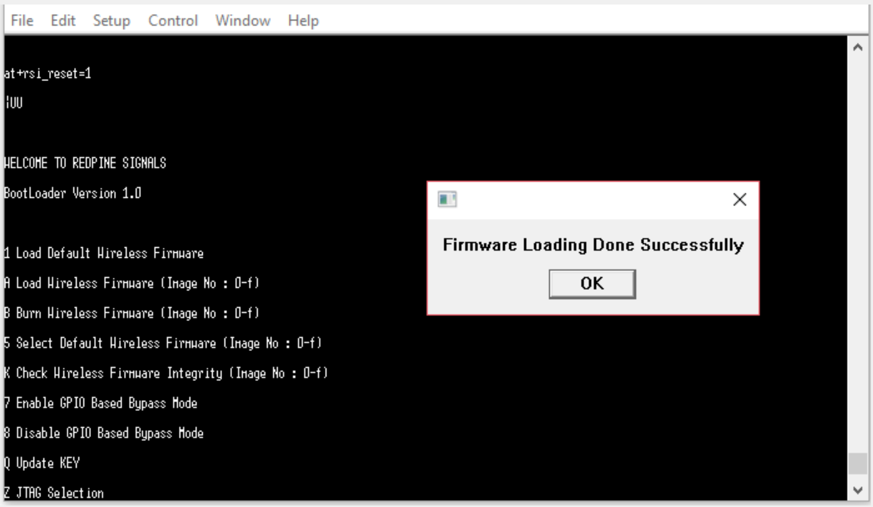
3. Then the actual scripts starts from the OPERMODE, the below image is for reference.



```
!UU

WELCOME TO REDPINE SIGNALS
BootLoader Version 1.0

1 Load Default Wireless Firmware
A Load Wireless Firmware (Image No : 0-f)
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
1
1
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
```

Opermode Successful

Note 6: If the user want to perform the ABRD manually as mentioned in step #11 and #12, after the successful ABRD user has to give RESET command as "at+rsi_reset=1", so that user should be able to select the required TTL Script from the path "RS9116.NB0.WC.GENR.OSI.x.x.xx\utils\scripts\TeraTerm_TTL_Scripts".

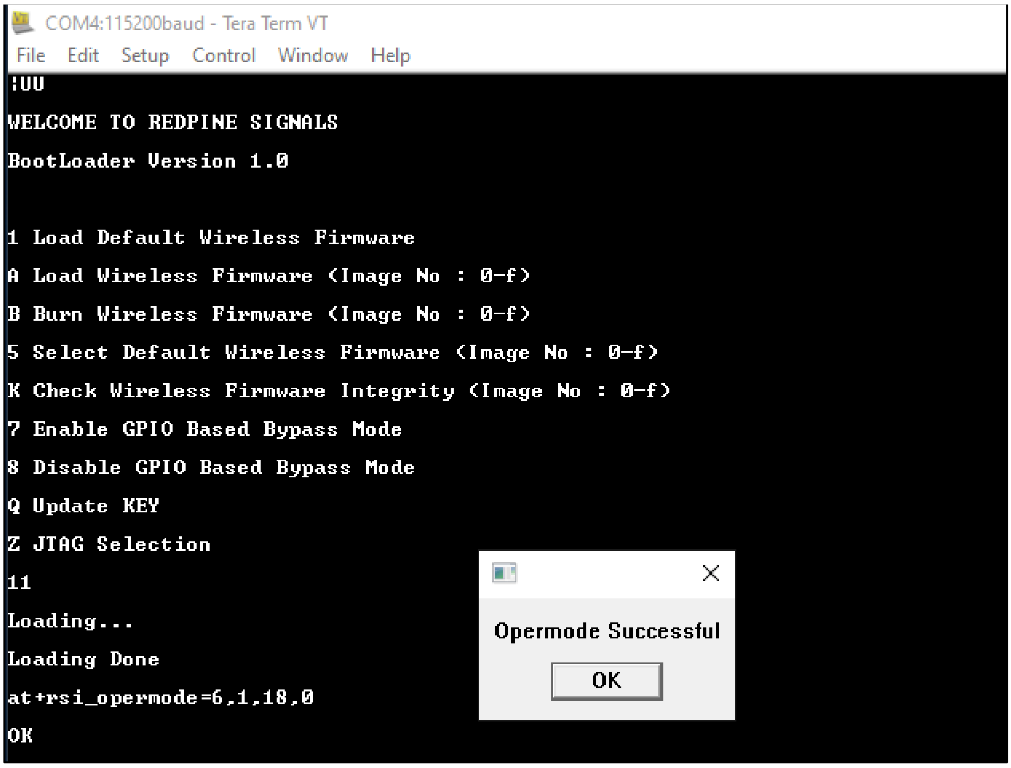


```
at+rsi_reset=1
!UU

WELCOME TO REDPINE SIGNALS
BootLoader Version 1.0

1 Load Default Wireless Firmware
A Load Wireless Firmware (Image No : 0-f)
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
```

Firmware Loading Done Successfully

8.1 Access Point Mode

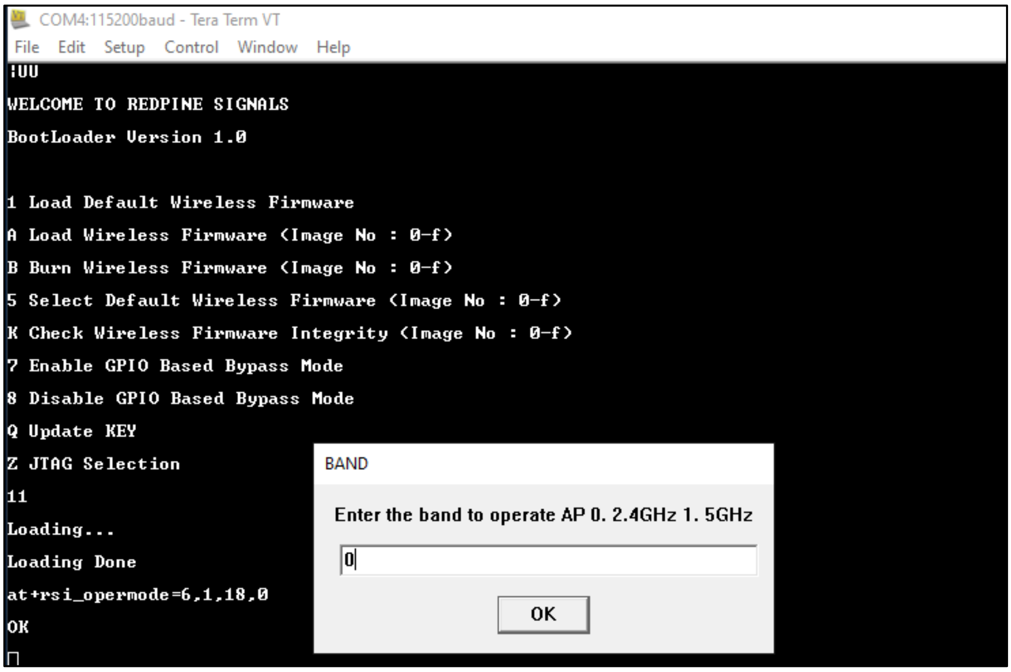
1. For running this script users need to use AP_MODE.ttl from the list.
2. The Opermode command "at+rsi_opermode=6,1,18,0" , This configures the EVB to function in AP mode. The module responds with “OK”.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
¦UU
WELCOME TO REDPINE SIGNALS
BootLoader Version 1.0

1 Load Default Wireless Firmware
A Load Wireless Firmware (Image No : 0-f)
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
```

Opermode Successful

3. Tera term will pop up for input (Band - 2.4 GHz or 5 GHz) from the user, user needs to enter the band value (0) and hit 'OK', (at+rsi_band=0) This configures the operating band 2.4 GHz of the EVB. The module responds with “OK”.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

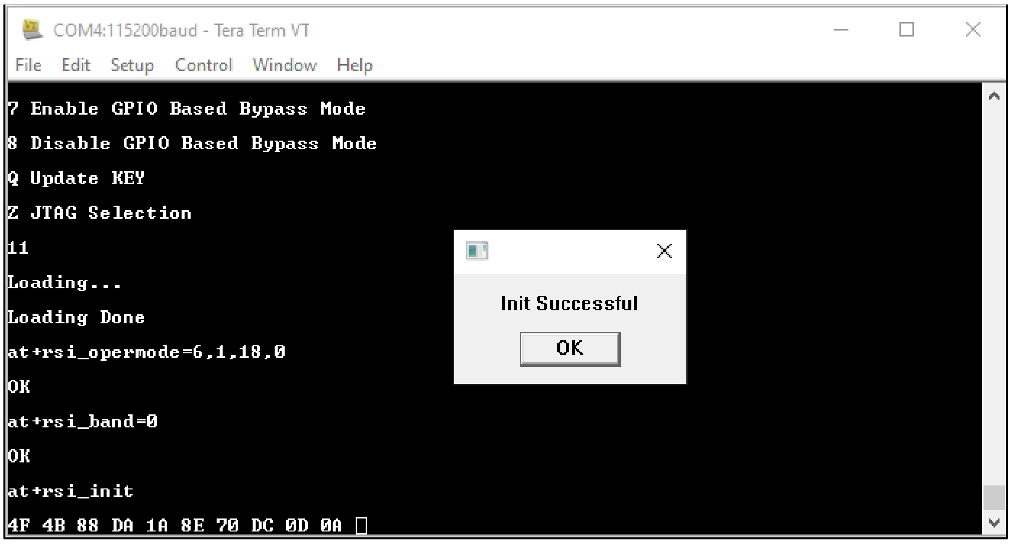
```
¦UU
WELCOME TO REDPINE SIGNALS
BootLoader Version 1.0

1 Load Default Wireless Firmware
A Load Wireless Firmware (Image No : 0-f)
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
```

BAND

Enter the band to operate AP 0. 2.4GHz 1. 5GHz

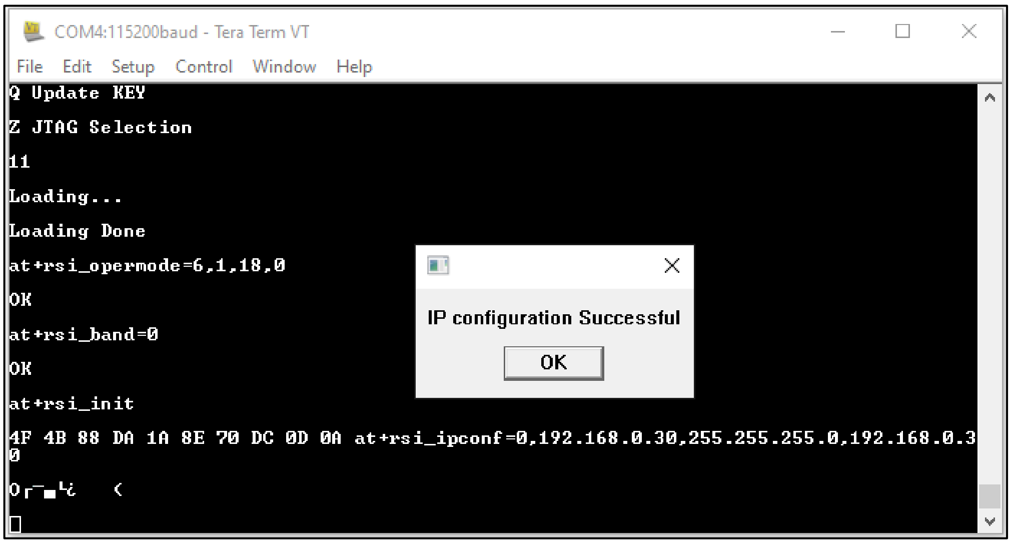
0

4. "at+rsi_init" command initializes the RF of the module. The module responds with OK<MAC_Address>.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
Init Successful
OK

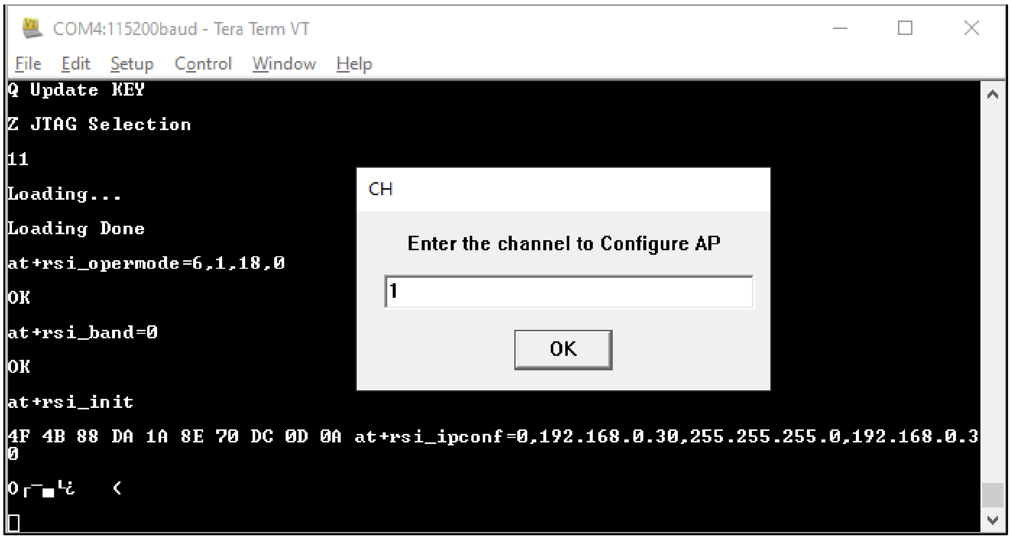
```
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A
```

5. If a user wants to configure a different subnet and gateway than ipconfig command has to be issued at this stage else AP will be configured to default subnet and gateway. e.g. "at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168.0.30", This command configures the IP (192.168.0.30 in this example) of the AP.The module responds with “OK”.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
IP configuration Successful
OK

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168.0.3
0
O┌‾▄Ł¿   ‹
```

6. Tera term will pop up for input (operating channel) from the user, user can enter any value between 1 to 11 e.g. enter the channel(1) and hit 'OK' as shown:

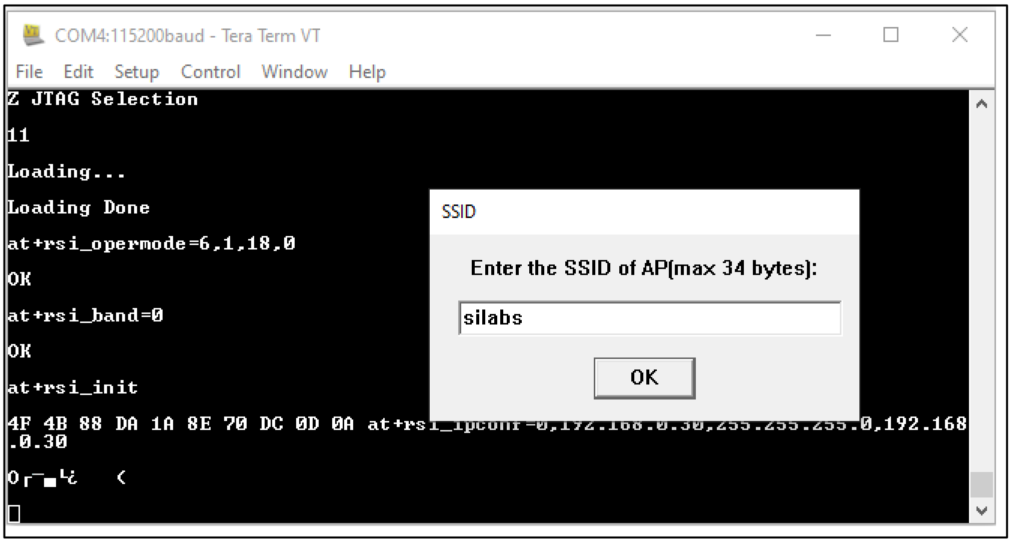

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
CH
OK

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168.0.3
0
0┌▄└¿   <
```

Enter the channel to Configure AP

1

7. Tera term will now pop up for input (SSID of the AP) from the user, user needs to enter the SSID (e.g. Silabs) and hit 'OK':

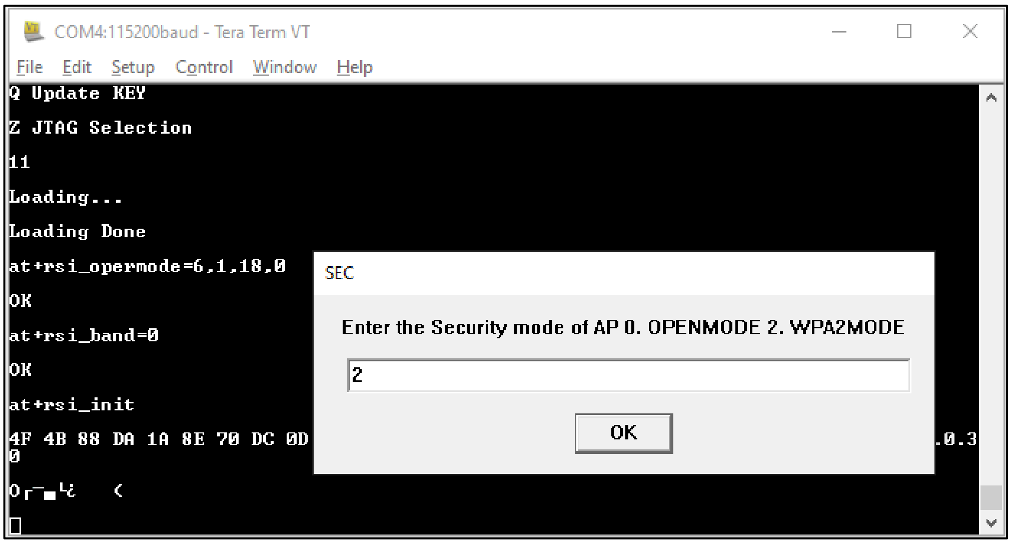

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
SSID
OK

```
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168
.0.30
0┌▄└¿   <
```

Enter the SSID of AP(max 34 bytes):

silabs

8. The next pop up is for input (security mode) from the user, user needs to enter the security mode(2) and hit 'OK',
0 - Open Security
2 - WPA2 PSK Security

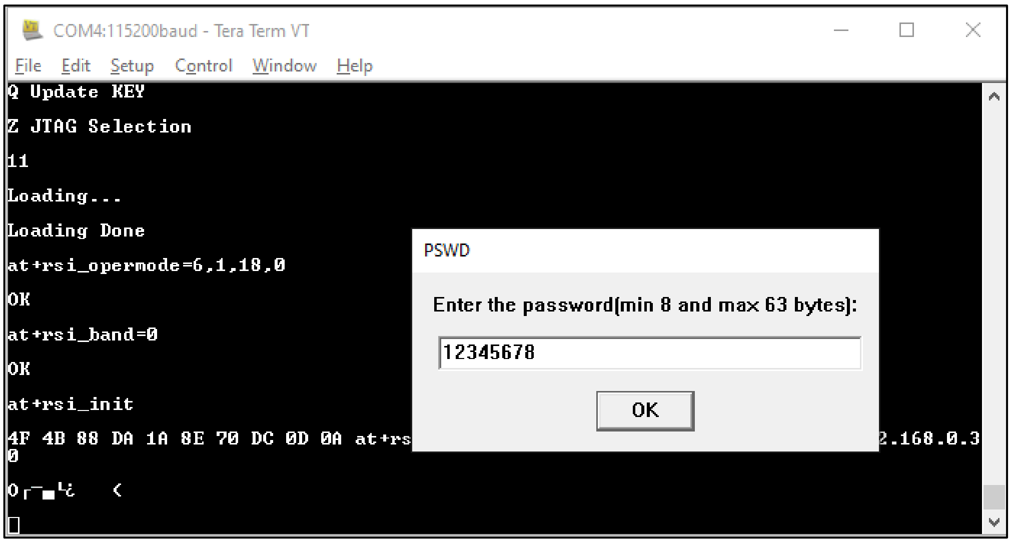

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
SEC
OK

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D                                        .0.3
0
0┌▄└¿   <
```

Enter the Security mode of AP 0. OPENMODE 2. WPA2MODE

2

9. Tera term will pop up for input (PSK of the AP) from the user, the user needs to enter the PSK (12345678) and hit 'OK'.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rs                                  2.168.0.3
0
```

PSWD

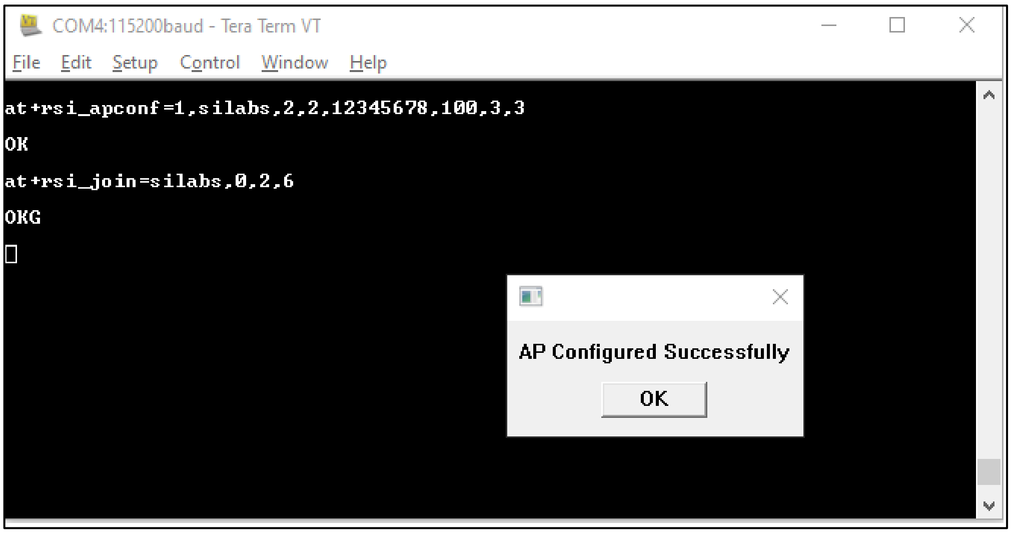
Enter the password(min 8 and max 63 bytes):

12345678

10. The command will go as "at+rsi_apconf=1,silabs,2,2,12345678,100,3,3"
The SSID is configured as “silabs” operate in channel 1 and the WPA2 PSK set is "12345678"

11. The next command will go as at+rsi_join=silabs,0,2,6, This starts the Access Point functionality in the module. The module is now configured as an Access Point. Its IP address is 192.168.0.30.

A remote peer can now scan for networks and the SSID of the module, “silabs” will be displayed in the remote peer’s list of Scanned APs. After the remote peer connects to the AP, it acquires an IP address over DHCP.

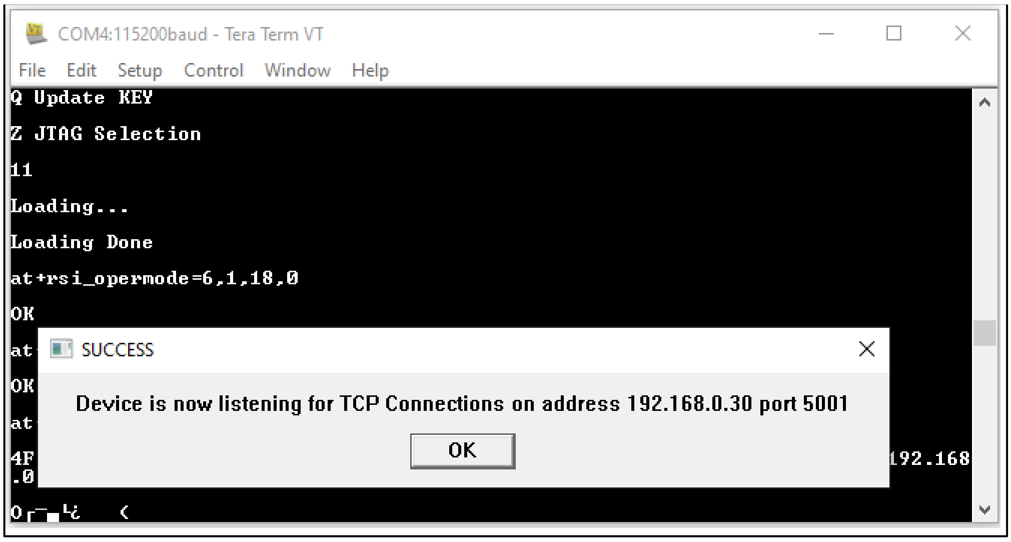

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
at+rsi_apconf=1,silabs,2,2,12345678,100,3,3
OK
at+rsi_join=silabs,0,2,6
OKG
```

AP Configured Successfully

12. It will open a TCP Server socket on the Wi-Fi Client (EVB) side using the following AT command 'at+rsi_ltcp=5001', The module’s response will look as follows:

OK<ip_version><socket_type><socket_handle><Lport><module_ipaddr>\r\n, pop up window will display "Device is now listening for TCP connections on address 192.168.0.30 and port 5001".



COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at
OK
at
4F                                                                    192.168
.0
0┌─▄└¿   <
```

SUCCESS

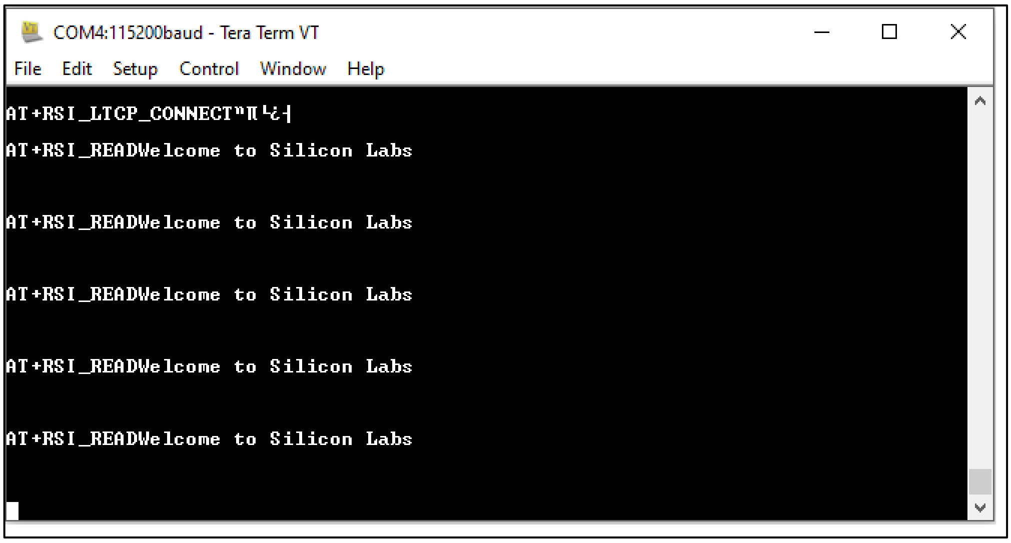
Device is now listening for TCP Connections on address 192.168.0.30 port 5001

13. Open a TCP client socket on the remote peer (e.g. mobile or PC running iPerf or any third-party application) and connect to Server socket by giving server IP and port number.'

14. Observe that the Teraterm on the Wi-Fi Client-side (EVB) prints the following message, once the TCP connection is set up with the remote peer.

    AT+RSI_LTCP_CONNECT=<ip_version><socket_descriptor><dest_port_no><dest_ipaddr><mss><window_size ><src_port_no>\r\n The data received might have some unreadable characters because of ASCII conversion

15. When the data is received on the Wi-Fi Client (EVB) side, you will see a response (asynchronous) from the module as follows:



COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
AT+RSI_LTCP_CONNECT"π└¿┤
AT+RSI_READWelcome to Silicon Labs


AT+RSI_READWelcome to Silicon Labs


AT+RSI_READWelcome to Silicon Labs


AT+RSI_READWelcome to Silicon Labs


AT+RSI_READWelcome to Silicon Labs
```

8.2 BLE Central (Master) Mode

- For running this script user need to use ble_central.ttl from the list.

This example demonstrates How to connect with remote BLE devices in BLE central mode.

→ To run this example script user required to enter the **Address type**(0- for Public and 1- for random) of the remote device and **remote device BD address**(XX-XX-XX-XX-XX-XX) in the mentioned format.

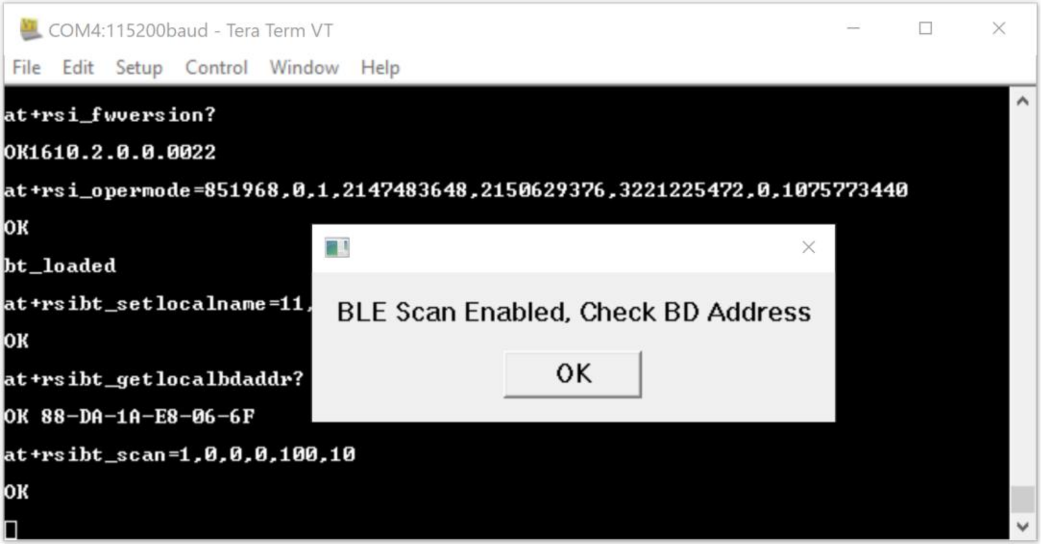
→ Command sequence in this scripts are:

1. Opermode

2. Setlocalname

3.Get local address

→ After this commands "Scan" start and advertise reports will come .

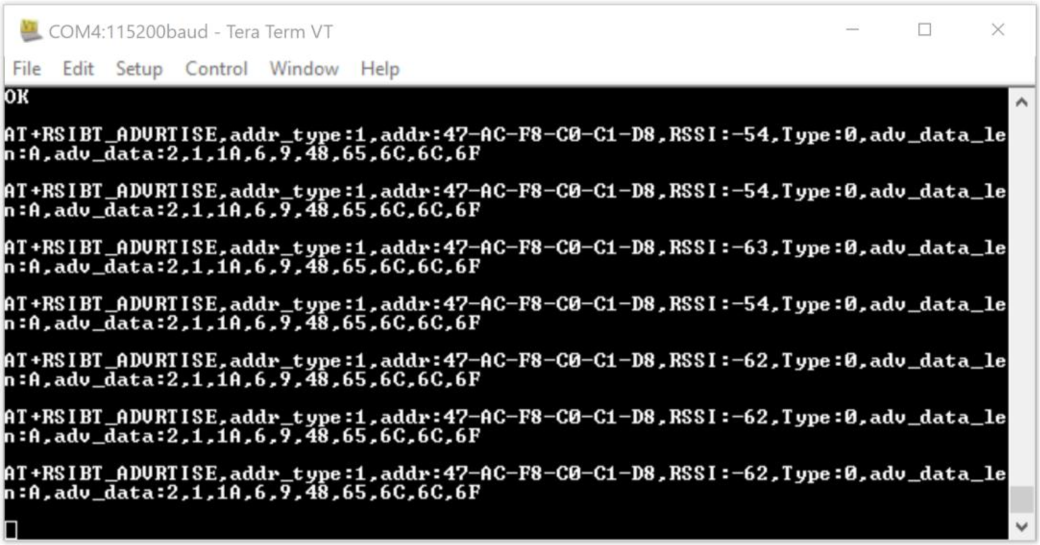

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
at+rsi_fwversion?
OK1610.2.0.0.0022
at+rsi_opermode=851968,0,1,2147483648,2150629376,3221225472,0,1075773440
OK
bt_loaded
at+rsibt_setlocalname=11,
OK
at+rsibt_getlocalbdaddr?
OK 88-DA-1A-E8-06-6F
at+rsibt_scan=1,0,0,0,100,10
OK
```

BLE Scan Enabled, Check BD Address

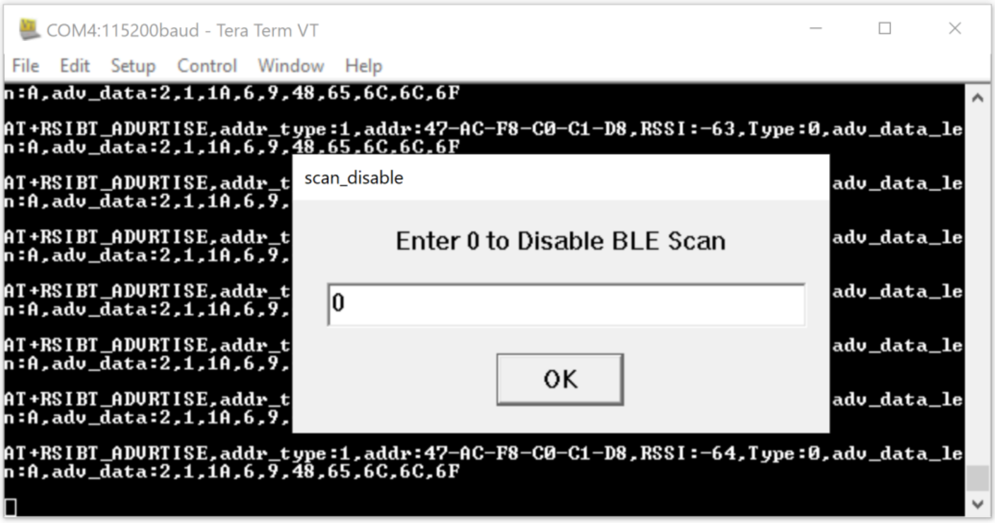
OK

→ Advertise reports come up with "Address" "RSSI" , "Adv data length" & "Adv data" .


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
OK
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-54,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-54,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-63,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-54,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-62,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-62,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-62,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
```

→ After Advertise reports pop-up will ask for disabling the "scan".


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-63,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
AT+RSIBT_ADVRTISE,addr_t                                        adv_data_le
n:A,adv_data:2,1,1A,6,9,
AT+RSIBT_ADVRTISE,addr_t                                        adv_data_le
n:A,adv_data:2,1,1A,6,9,
AT+RSIBT_ADVRTISE,addr_t                                        adv_data_le
n:A,adv_data:2,1,1A,6,9,
AT+RSIBT_ADVRTISE,addr_t                                        adv_data_le
n:A,adv_data:2,1,1A,6,9,
AT+RSIBT_ADVRTISE,addr_t                                        adv_data_le
n:A,adv_data:2,1,1A,6,9,
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-64,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
```

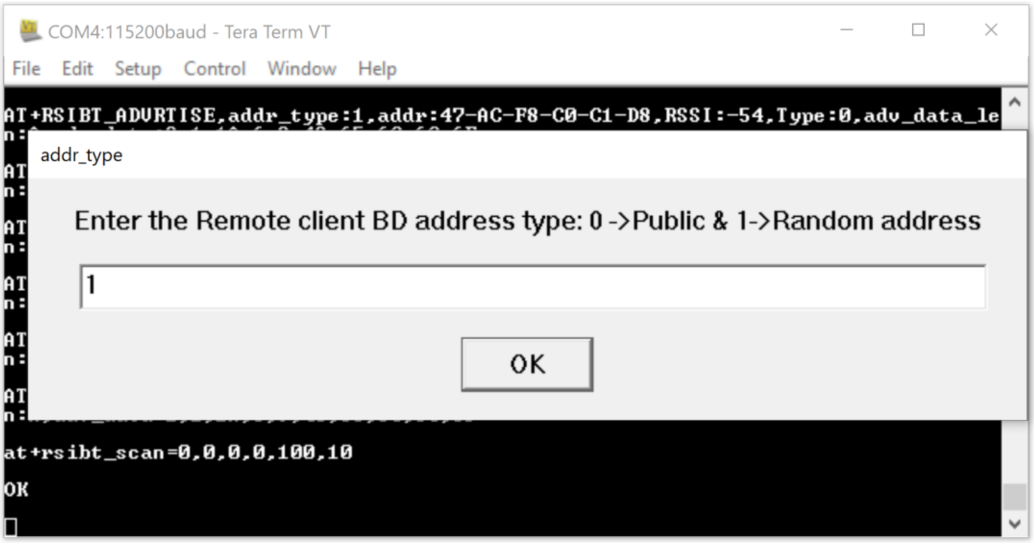
scan_disable

Enter 0 to Disable BLE Scan

0

OK

→ Enter the address type user needs to enter the Address type(i.e. 0 - Public address and 1 - Random address) as given below , we share here "**Random Address**".


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
addr_type
OK

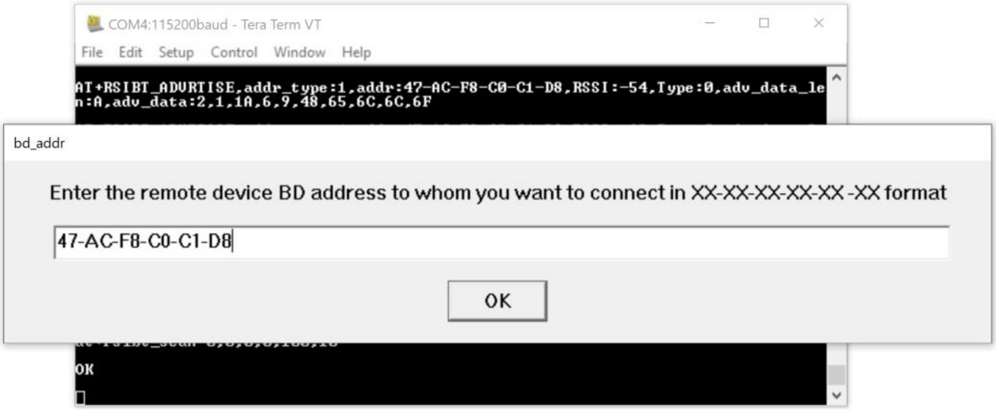
```
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-54,Type:0,adv_data_le
```

Enter the Remote client BD address type: 0 ->Public & 1->Random address

1

```
at+rsibt_scan=0,0,0,0,100,10
OK
```

→ After address selection user need to enter the Address to connect to the Silabs BLE Central.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
bd_addr
OK

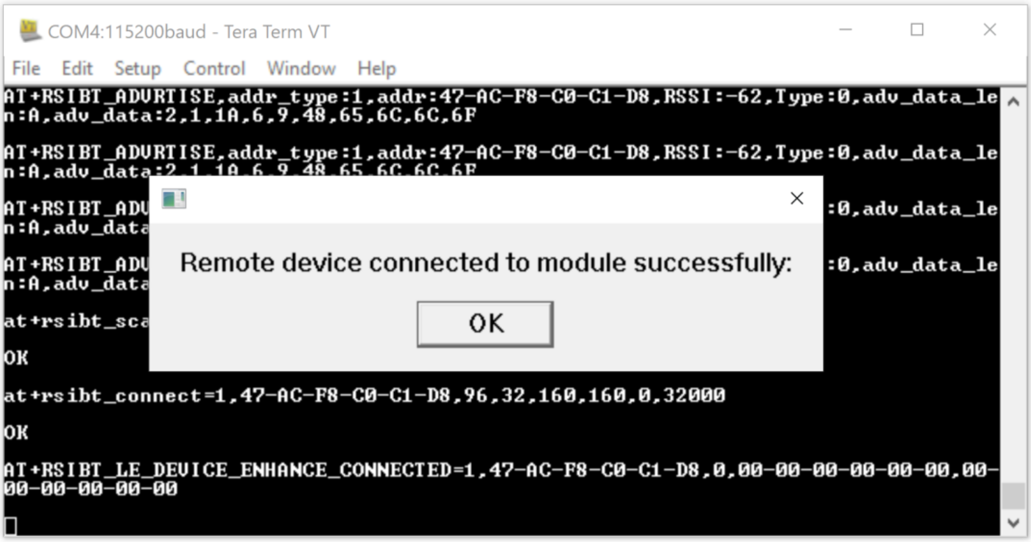
```
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-54,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F
```

Enter the remote device BD address to whom you want to connect in XX-XX-XX-XX-XX -XX format

47-AC-F8-C0-C1-D8

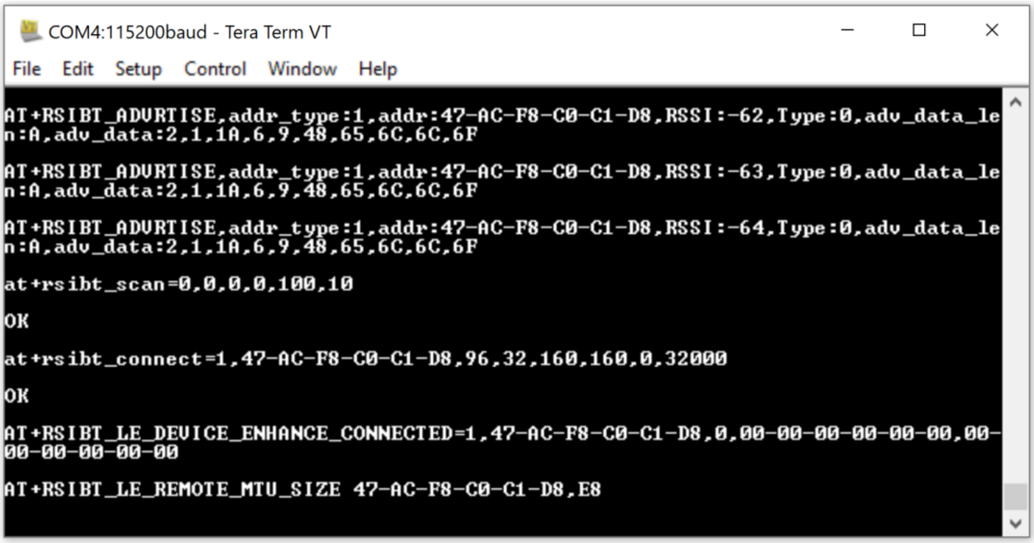
```
OK
```

→ After entering the Remote BLE Device Address Silabs BLE Central device will initiate connection with the Remote BLE Device .


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-62,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F

AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-62,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F

AT+RSIBT_ADV                                                      :0,adv_data_le
n:A,adv_data

AT+RSIBT_ADV                                                      :0,adv_data_le
n:A,adv_data

at+rsibt_sca

OK

at+rsibt_connect=1,47-AC-F8-C0-C1-D8,96,32,160,160,0,32000

OK

AT+RSIBT_LE_DEVICE_ENHANCE_CONNECTED=1,47-AC-F8-C0-C1-D8,0,00-00-00-00-00-00,00-
00-00-00-00-00
```

Remote device connected to module successfully:


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-62,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F

AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-63,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F

AT+RSIBT_ADVRTISE,addr_type:1,addr:47-AC-F8-C0-C1-D8,RSSI:-64,Type:0,adv_data_le
n:A,adv_data:2,1,1A,6,9,48,65,6C,6C,6F

at+rsibt_scan=0,0,0,0,100,10

OK

at+rsibt_connect=1,47-AC-F8-C0-C1-D8,96,32,160,160,0,32000

OK

AT+RSIBT_LE_DEVICE_ENHANCE_CONNECTED=1,47-AC-F8-C0-C1-D8,0,00-00-00-00-00-00,00-
00-00-00-00-00

AT+RSIBT_LE_REMOTE_MTU_SIZE 47-AC-F8-C0-C1-D8,E8
```

→ This is the demo for Simple BLE central.

TIP :- In case too many devices in scan user can also open "BLE scanner/ nrf connect " app in another mobile and scan to check advertiser address with name.

8.3 BLE Peripheral (Slave) Mode

For running this script user need to use ble_peripheral.ttl from the list.

1. This example demonstrates how to configure the Silabs device in Simple peripheral mode and how to connect from remote Central devices like (Mobile phones/BT dongles etc).

   → To run this example user required **nRF connect** application in Android phone and **LightBLue** application in iOS.

   → Command sequence in this scripts are:

   1. Opermode

   2. Set localname

   3. Query local BD address

   4. Set advertisementdata

   5. Addservice

   6. Add attribute

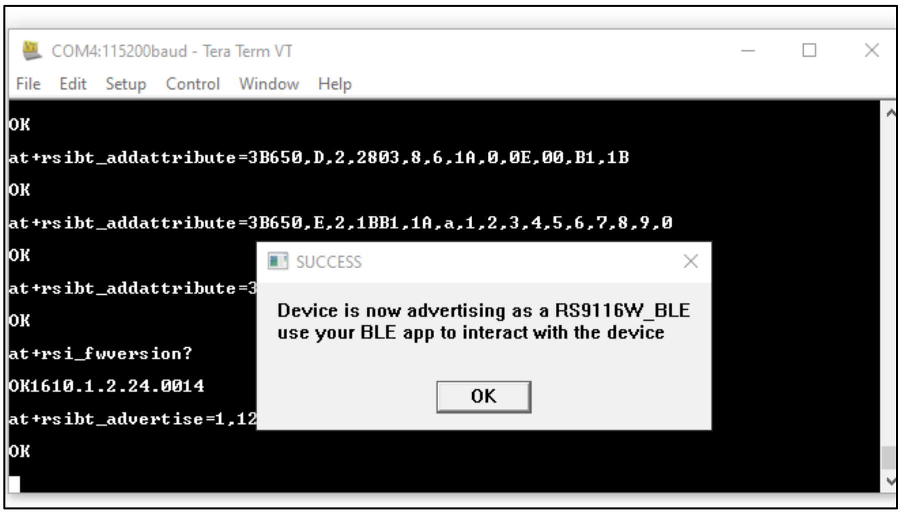
   7. Add attribute

   8. Add attribute

   9. Query Firmware version

   9. Advertise

   → After this commands user will see the Silabs device with the name "RS9116W_BLE" in Central device.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
SUCCESS
OK

```
OK
at+rsibt_addattribute=3B650,D,2,2803,8,6,1A,0,0E,00,B1,1B
OK
at+rsibt_addattribute=3B650,E,2,1BB1,1A,a,1,2,3,4,5,6,7,8,9,0
OK
at+rsibt_addattribute=3
OK
at+rsi_fwversion?
OK1610.1.2.24.0014
at+rsibt_advertise=1,12
OK
```

Device is now advertising as a RS9116W_BLE
use your BLE app to interact with the device

→ When the Central device give the connect command,Module will receive Enhanced connection update event like below.

AT+RSIBT_LE_DEVICE_ENHANCE_CONNECTED=1,6B-63-FE-FE-3D-FD,0,88-DA-1A-9E-81-55,00-00-00-00-00-00

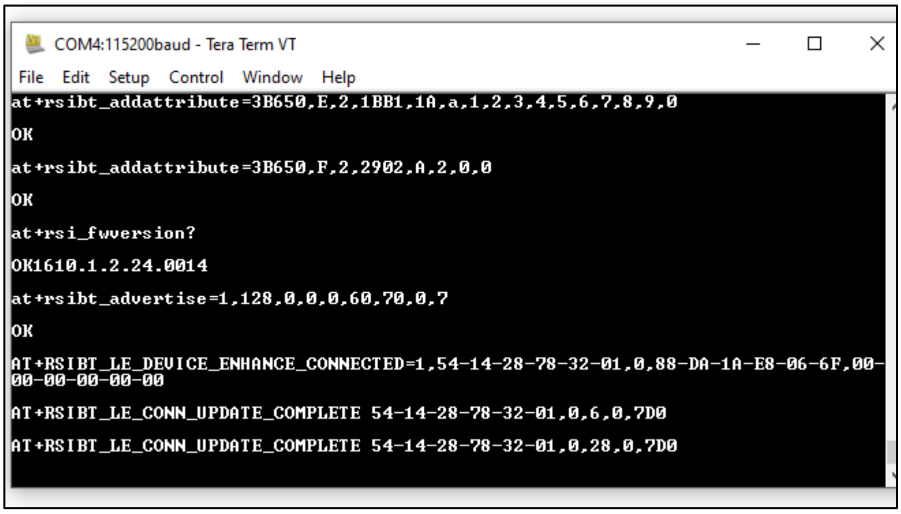
→ Also, some phones will give the data length update event like below.

AT+RSIBT_LE_DATA_LENGTH_UPDATE 6B-63-FE-FE-3D-FD,7B,448,7B,448

→ After this connection update events will come to the host.

AT+RSIBT_LE_CONN_UPDATE_COMPLETE 6B-63-FE-FE-3D-FD,0,6,0,1F4

AT+RSIBT_LE_CONN_UPDATE_COMPLETE 6B-63-FE-FE-3D-FD,0,24,0,1F4


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
at+rsibt_addattribute=3B650,E,2,1BB1,1A,a,1,2,3,4,5,6,7,8,9,0
OK
at+rsibt_addattribute=3B650,F,2,2902,A,2,0,0
OK
at+rsi_fwversion?
OK1610.1.2.24.0014
at+rsibt_advertise=1,128,0,0,0,60,70,0,7
OK
AT+RSIBT_LE_DEVICE_ENHANCE_CONNECTED=1,54-14-28-78-32-01,0,88-DA-1A-E8-06-6F,00-
00-00-00-00-00
AT+RSIBT_LE_CONN_UPDATE_COMPLETE 54-14-28-78-32-01,0,6,0,7D0
AT+RSIBT_LE_CONN_UPDATE_COMPLETE 54-14-28-78-32-01,0,28,0,7D0
```

1. Once these events come it means Silabs module got connected to the Central device.

→ Central can send the data to the Silabs module. And a host will get the event like below.

AT+RSIBT_WRITE,6B-63-FE-FE-3D-FD,E,6,31,32,33,34,35,36

Note:- Here in this example we have added Service as a Device Information(0x180A) and attribute as a custom characteristic attribute 0x1AA1. Users can change the service as well as attributes as per their requirements.

How to change the values are present in PRM. please follow PRM.

8.4 BT SPP Master

For running this script user need to use spp_master.ttl from the list.

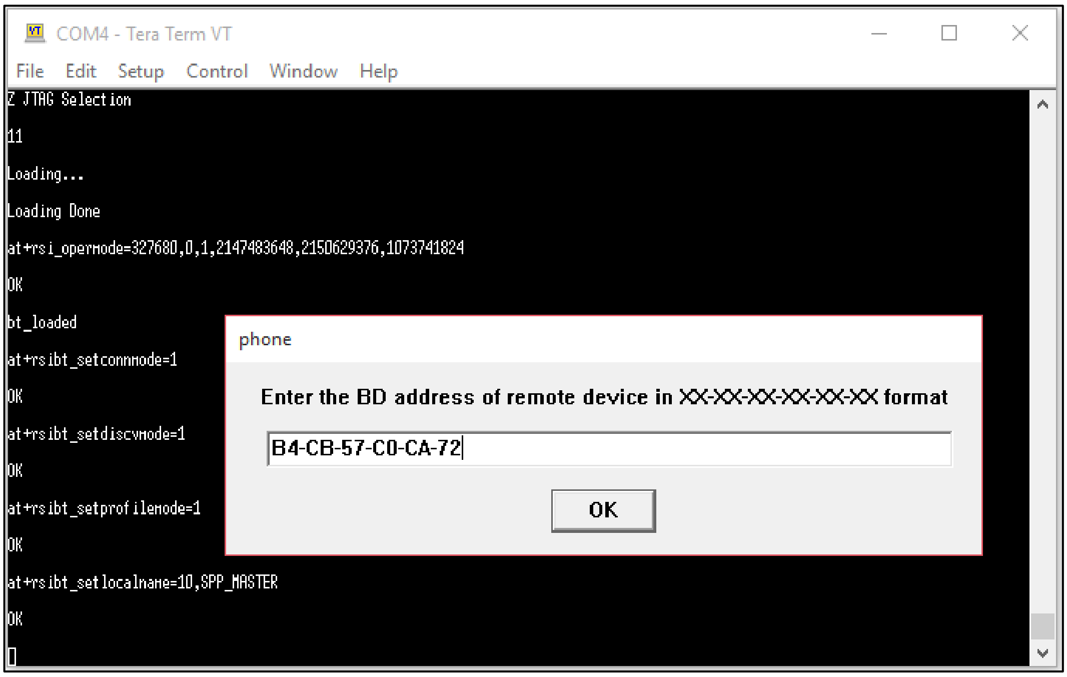
Note: To run this script user required "Bluetooth SPP Manager" or "Sena Bterm" application in Android phone for data transfer.

This example demonstrates how to configure the Silabs device in Master mode and establish an SPP profile connection with a remote slave device and data exchange between two devices.

→ Command sequence in this scripts are:

1. Opermode
2. Set connectable mode
3. Set discoverable mode
4. Set profile mode
5. Set local name

→ After these commands, the remote slave devices needs to be in connectable mode. And once it will be in connectable mode, the user needs to give bond command. For this BD address of the remote device needs to be entered here.

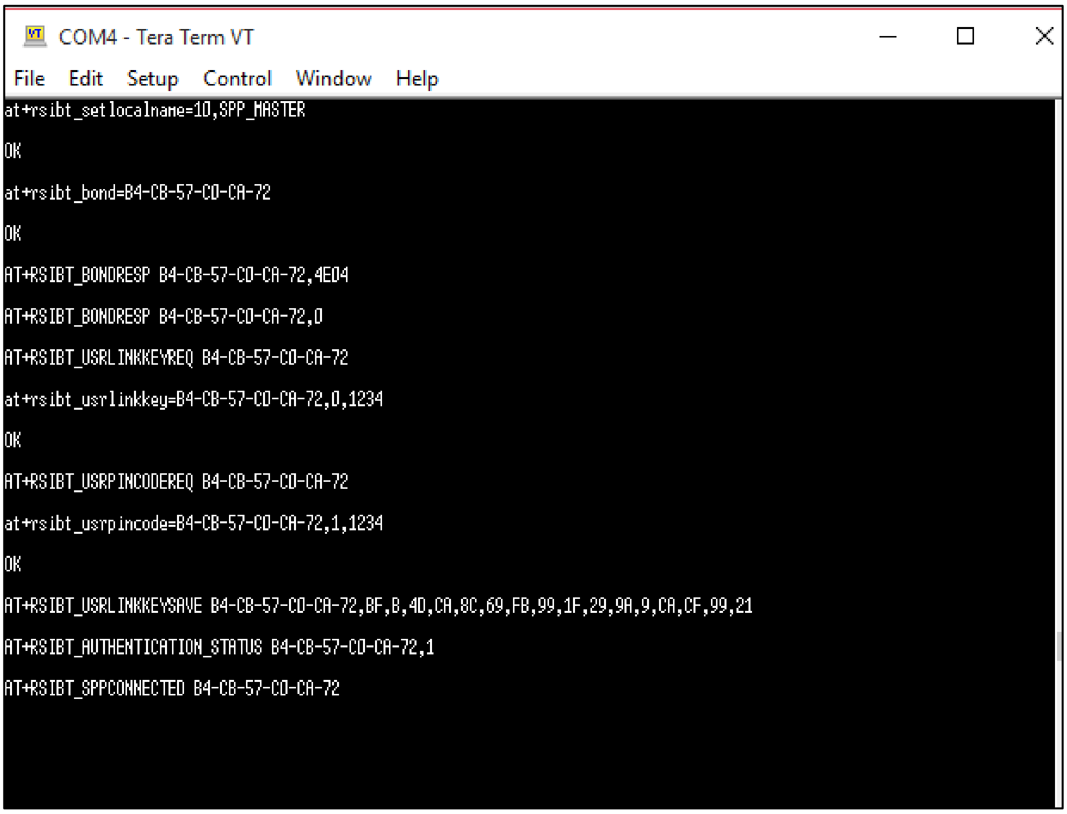


```
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=327680,0,1,2147483648,2150629376,1073741824
OK
bt_loaded
at+rsibt_setconnmode=1
OK
at+rsibt_setdiscvmode=1
OK
at+rsibt_setprofilemode=1
OK
at+rsibt_setlocalname=10,SPP_MASTER
OK
```

Enter the BD address of remote device in XX-XX-XX-XX-XX-XX format

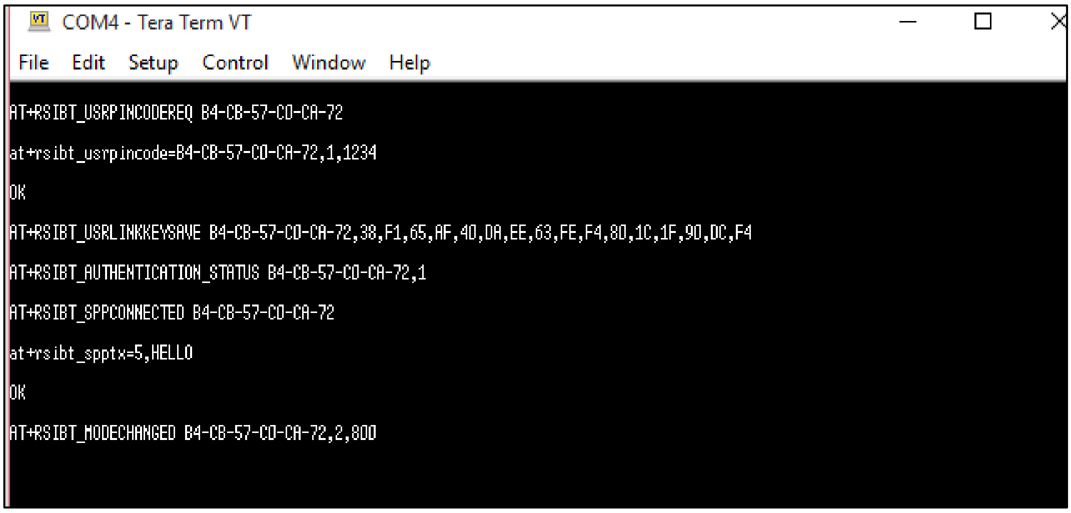
B4-CB-57-C0-CA-72

→ After this host will get a bond response as well as the "link key" req event in the terminal screen. And as per request user needs to give a response to the module(i.e. if on terminal bond response and after that "user pincode" request event come user need to click send "user pincode" response and for the "userlinkkey" request userlinkkey response need to give). After this event remote slave device is paired. Again give the "spp connect" command and the host will get the AT+RSIBT_SPPCONNECTED event.



```
at+rsibt_setlocalname=10,SPP_MASTER

OK

at+rsibt_bond=B4-CB-57-C0-CA-72

OK

AT+RSIBT_BONDRESP B4-CB-57-C0-CA-72,4E04

AT+RSIBT_BONDRESP B4-CB-57-C0-CA-72,0

AT+RSIBT_USRLINKKEYREQ B4-CB-57-C0-CA-72

at+rsibt_usrlinkkey=B4-CB-57-C0-CA-72,0,1234

OK

AT+RSIBT_USRPINCODEREQ B4-CB-57-C0-CA-72

at+rsibt_usrpincode=B4-CB-57-C0-CA-72,1,1234

OK

AT+RSIBT_USRLINKKEYSAVE B4-CB-57-C0-CA-72,BF,B,4D,CA,8C,69,FB,99,1F,29,9A,9,CA,CF,99,21

AT+RSIBT_AUTHENTICATION_STATUS B4-CB-57-C0-CA-72,1

AT+RSIBT_SPPCONNECTED B4-CB-57-C0-CA-72
```

→ AT+RSIBT_SPPCONNECTED event come means SPP level connection done. Now both devices can communicate. using selecting option 3.



```
AT+RSIBT_USRPINCODEREQ B4-CB-57-C0-CA-72

at+rsibt_usrpincode=B4-CB-57-C0-CA-72,1,1234

OK

AT+RSIBT_USRLINKKEYSAVE B4-CB-57-C0-CA-72,38,F1,65,AF,40,DA,EE,63,FE,F4,80,1C,1F,90,DC,F4

AT+RSIBT_AUTHENTICATION_STATUS B4-CB-57-C0-CA-72,1

AT+RSIBT_SPPCONNECTED B4-CB-57-C0-CA-72

at+rsibt_spptx=5,HELLO

OK

AT+RSIBT_MODECHANGED B4-CB-57-C0-CA-72,2,800
```

Note:- Command sequence for the SPP profile connection is like below.

TX EVENT

← AT+RSIBT_USRLINKKEYREQ C0-EE-FB-DA-49-7C

at+rsibt_usrlinkkey=C0-EE-FB-DA-49-7C,0,1234 →

← AT+RSIBT_USRPINCODEREQ C0-EE-FB-DA-49-7C

at+rsibt_usrpincode=C0-EE-FB-DA-49-7C,1,1234 →

← AT+RSIBT_USRLINKKEYSAVE C0-EE-FB-DA-49-7C,B2,6C,91,49,D7,27,60,82,68,2,78,2,60,78,F8,AE

← AT+RSIBT_AUTHENTICATION_STATUS C0-EE-FB-DA-49-7C,1

at+rsibt_sppconn=C0-EE-FB-DA-49-7C →

← AT+RSIBT_SPPCONNECTED C0-EE-FB-DA-49-7C

at+rsibt_spptx=5,HELLO →

← AT+RSIBT_SPPRX 1,1

So like above mentioned, commands you need to give module when different events come.

8.5 BT SPP Slave

For running this script user need to use spp_slave.ttl from the list.

1. This example demonstrates how to configure the Silabs device in Slave mode and establish an SPP profile connection with remote Master device and data exchange between two devices.

Note: To run this example, the user needs to mention the BD address of Master in below MACRO before running the application.

phone= 'BD address of mobile'

--> To run this script user required "**Bluetooth SPP Manager"** application in Android phone.

--> Command sequence in this scripts are:

1. Opermode

2. Set connectable mode

3. Set discoverable mode

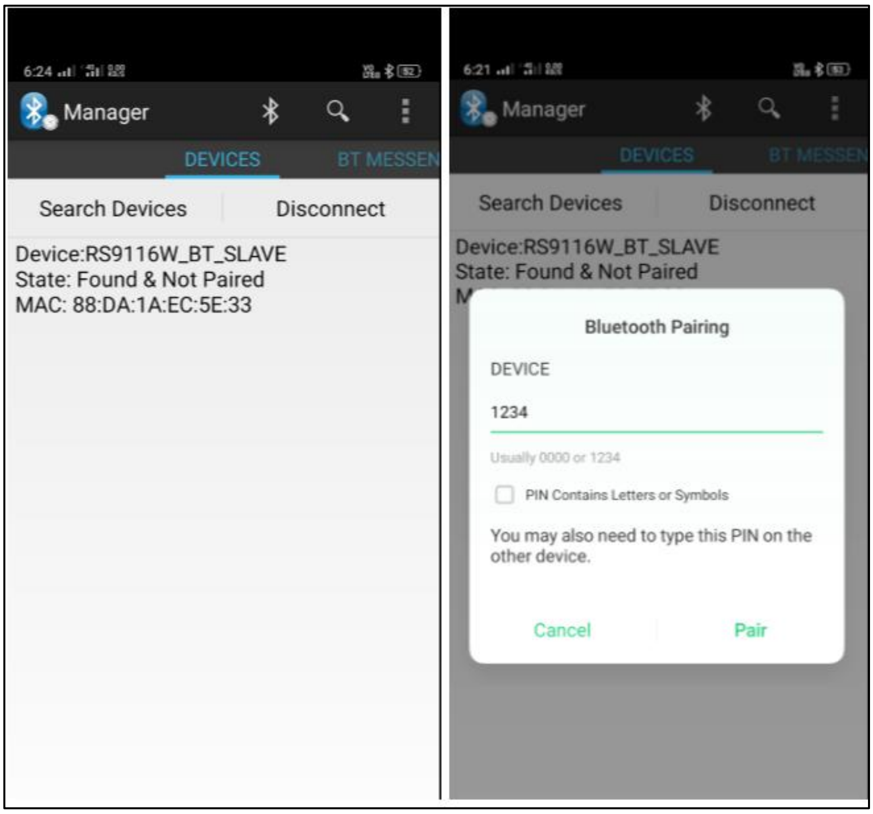
4. Set profile mode

5. Set local name

--> After these commands user can open the application and scan the devices around the vicinity. Select the device name "RS9116W_BT_SLAVE" and click "pair" button.

--> After this host will get a bond response as well as linkkey req event in the terminal screen. And as per request user needs to give a response to the module (i.e. if on terminal bond response and after that userpincode request event come user need to click send userpincode response and for the userlinkkey request userlinkkey response needs to give).

After this event on mobile phone you will see the device is paired. Again scan the device and click the "connect" button. And give commands as per events.



Device:RS9116W_BT_SLAVE
State: Found & Not Paired
MAC: 88:DA:1A:EC:5E:33

Device:RS9116W_BT_SLAVE
State: Found & Not Paired

Bluetooth Pairing

DEVICE

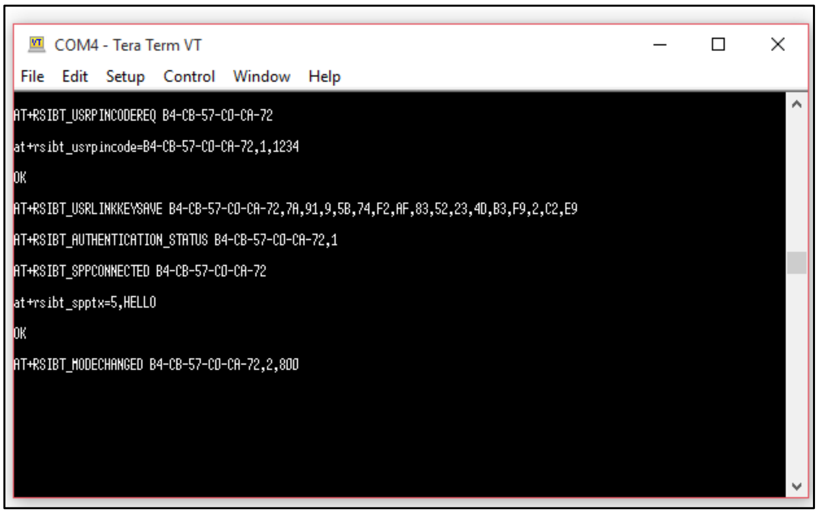
1234

Usually 0000 or 1234

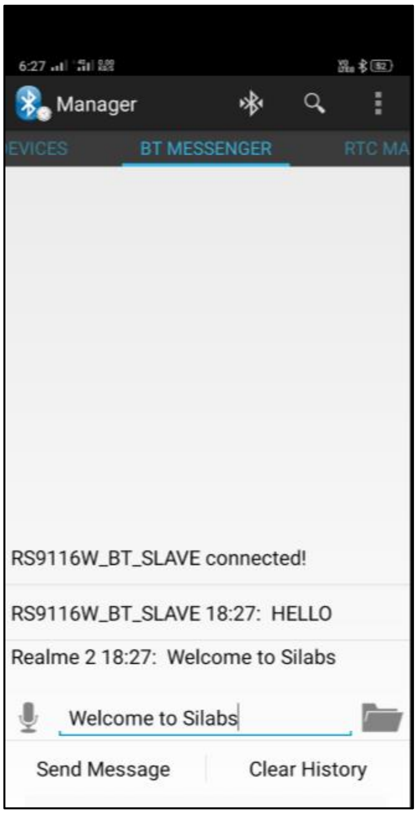
□ PIN Contains Letters or Symbols

You may also need to type this PIN on the other device.

--> Once the SPP level connection completed, the Host will get AT+RSI_SPPCONNECTED event. After this host can send the data and receive data from mobile.



```
AT+RSIBT_USRPINCODEREQ B4-CB-57-C0-CA-72
at+rsibt_usrpincode=B4-CB-57-C0-CA-72,1,1234
OK
AT+RSIBT_USRLINKKEYSAVE B4-CB-57-C0-CA-72,7A,91,9,5B,74,F2,AF,83,52,23,4D,B3,F9,2,C2,E9
AT+RSIBT_AUTHENTICATION_STATUS B4-CB-57-C0-CA-72,1
AT+RSIBT_SPPCONNECTED B4-CB-57-C0-CA-72
at+rsibt_spptx=5,HELLO
OK
AT+RSIBT_MODECHANGED B4-CB-57-C0-CA-72,2,800
```

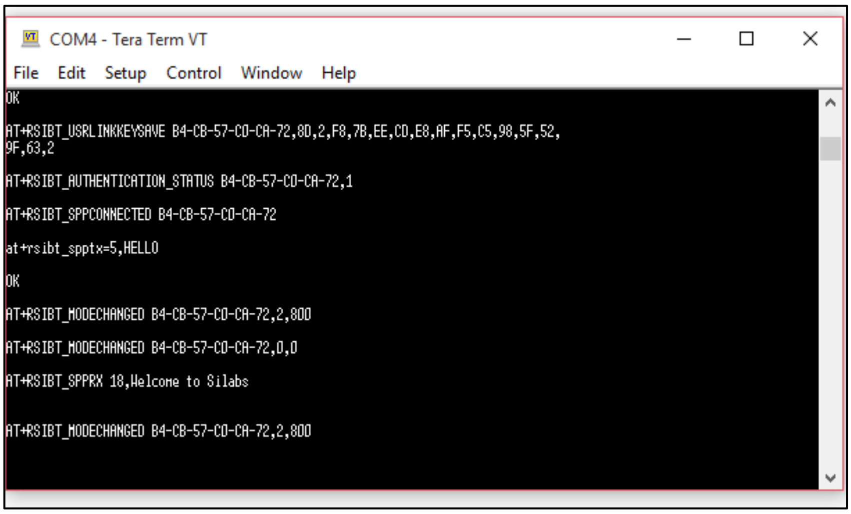


RS9116W_BT_SLAVE connected!

RS9116W_BT_SLAVE 18:27: HELLO

Realme 2 18:27: Welcome to Silabs

Welcome to Silabs

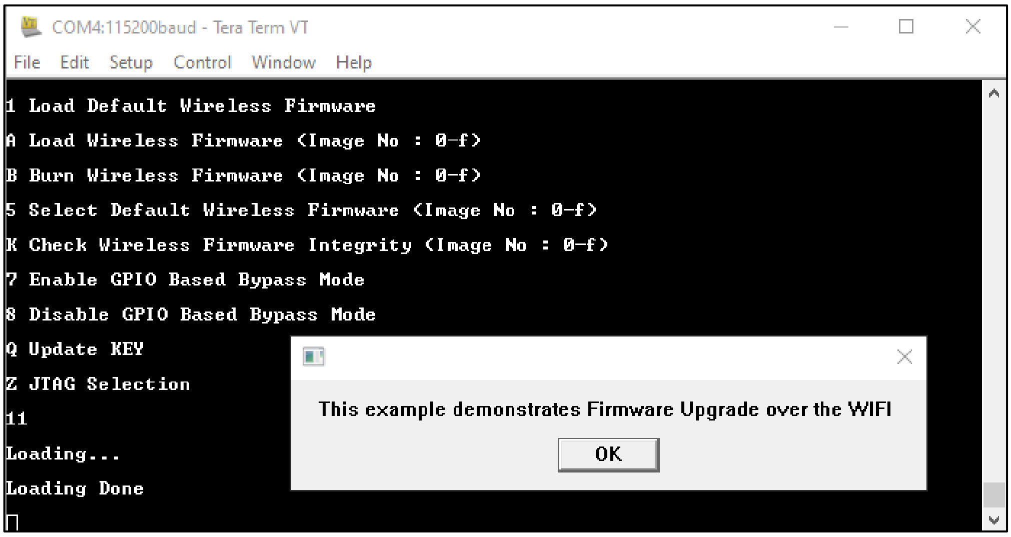


```
OK

AT+RSIBT_USRLINKKEYSAVE B4-CB-57-C0-CA-72,8D,2,F8,7B,EE,CD,E8,AF,F5,C5,98,5F,52,
9F,63,2

AT+RSIBT_AUTHENTICATION_STATUS B4-CB-57-C0-CA-72,1

AT+RSIBT_SPPCONNECTED B4-CB-57-C0-CA-72

at+rsibt_spptx=5,HELLO

OK

AT+RSIBT_MODECHANGED B4-CB-57-C0-CA-72,2,800

AT+RSIBT_MODECHANGED B4-CB-57-C0-CA-72,0,0

AT+RSIBT_SPPRX 18,Welcome to Silabs


AT+RSIBT_MODECHANGED B4-CB-57-C0-CA-72,2,800
```

→ Demo application as mentioned, the user needs to provide responses for the request.

8.6 FW_Upgrade_Over_WiFi

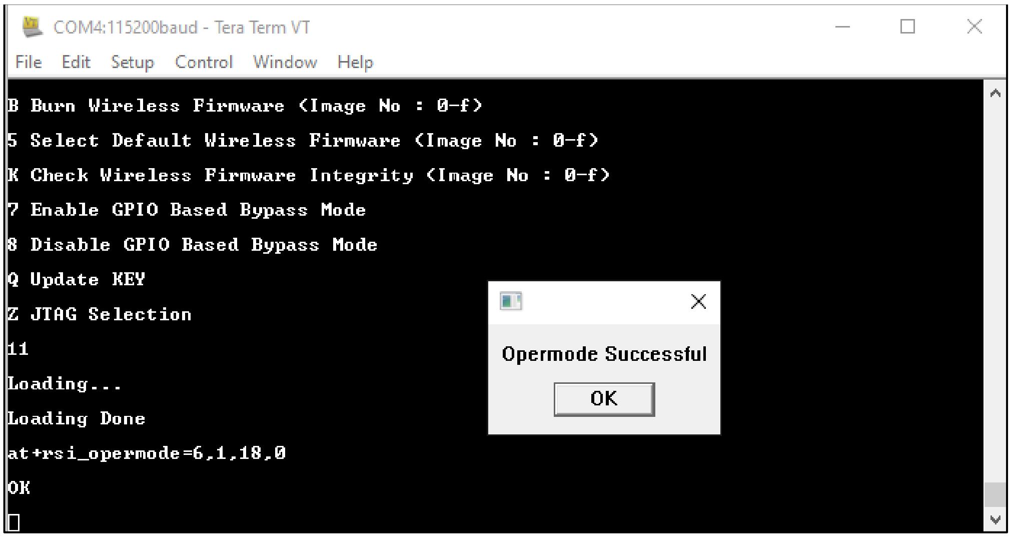
1. After running FW_Upgrade_over_wifi.ttl script, it will pop up as shown.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
1 Load Default Wireless Firmware
A Load Wireless Firmware (Image No : 0-f)
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
```

This example demonstrates Firmware Upgrade over the WIFI

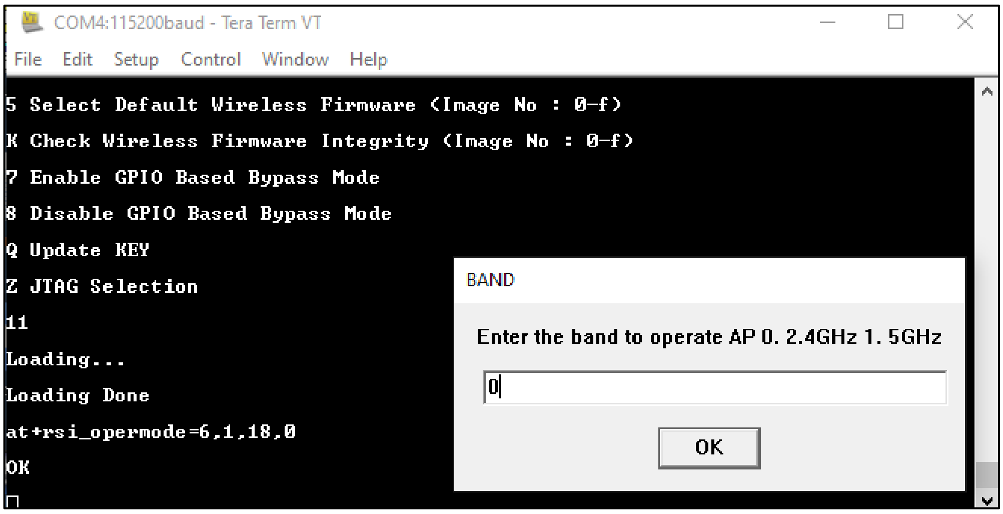
2. Next command is opermode command "at+rsi_opermode=6,1,18,0" , This configures the EVK to function in AP mode. The module responds with “OK”.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
```

Opermode Successful

3. Tera term will pop up for input (Band - 2.4 GHz or 5 GHz) from the user, user needs to enter the band value (0) and hit 'OK', (at+rsi_band=0) This configures the operating band 2.4 GHz of the EVK. The module responds with “OK”.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

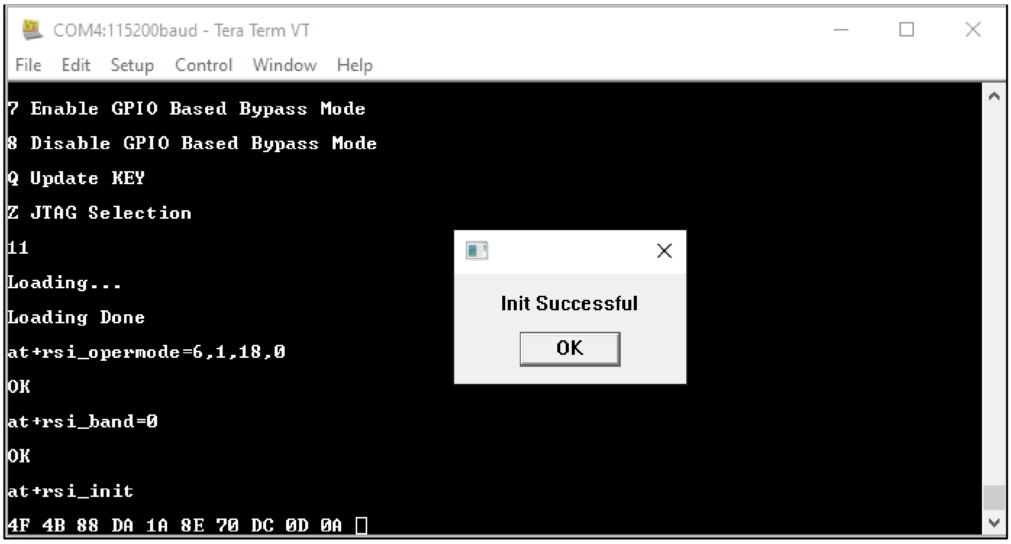
```
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
```

BAND

Enter the band to operate AP 0. 2.4GHz 1. 5GHz

0

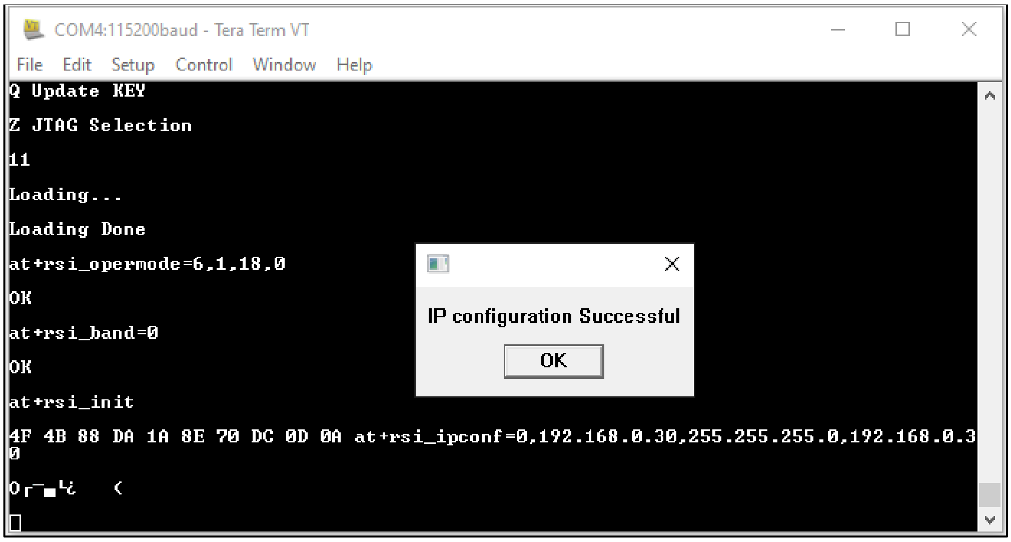
4. "at+rsi_init" command initializes the RF of the module. The module responds with OK<MAC_Address>.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A
```

Init Successful

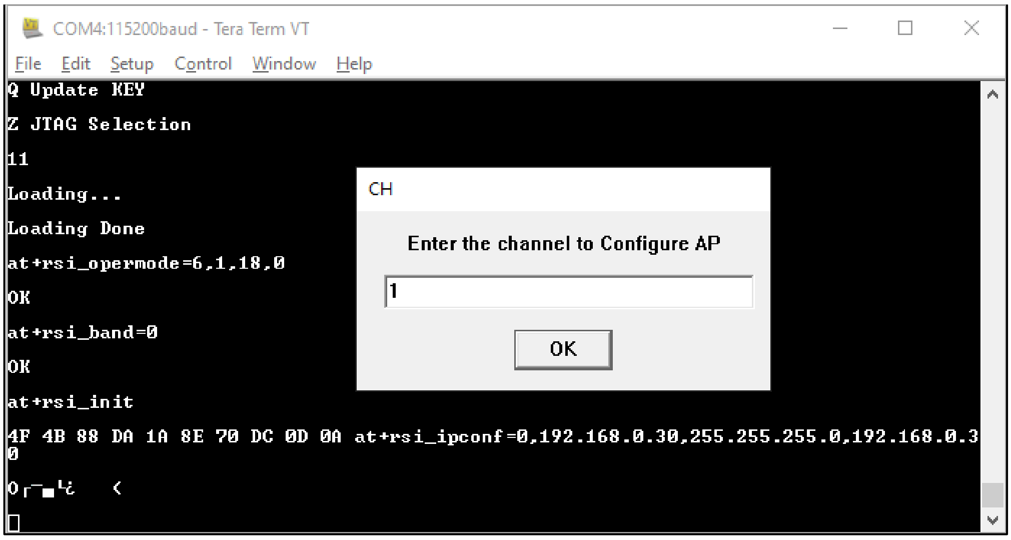
5. If a user wants to configure a different subnet and gateway than ipconf command has to be issued at this stage else AP will be configured to default subnet and gateway. e.g."at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168.0.30", This command configures the IP (192.168.0.30 in this example) of the AP. The module responds with “OK”.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168.0.3
0
Or┌¯▄└¿   (
```

IP configuration Successful

6. Tera term will pop up for input (operating channel) from the user, user can enter any value between 1 to 11 e.g. enter the channel(1) and hit 'OK' as shown:

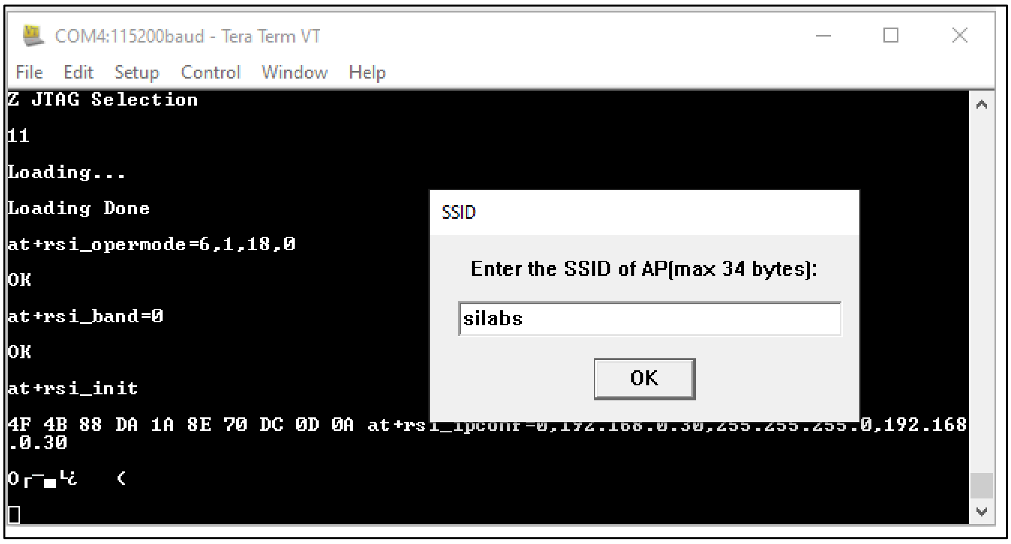

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
CH
OK

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168.0.3
0
O┌¯▄└¿   <
```

Enter the channel to Configure AP

1

7. Tera term will now pop up for input (SSID of the AP) from the user, user needs to enter the SSID (e.g. Silabs) and hit 'OK',


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
SSID
OK

```
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_ipconf=0,192.168.0.30,255.255.255.0,192.168
.0.30
O┌¯▄└¿   <
```

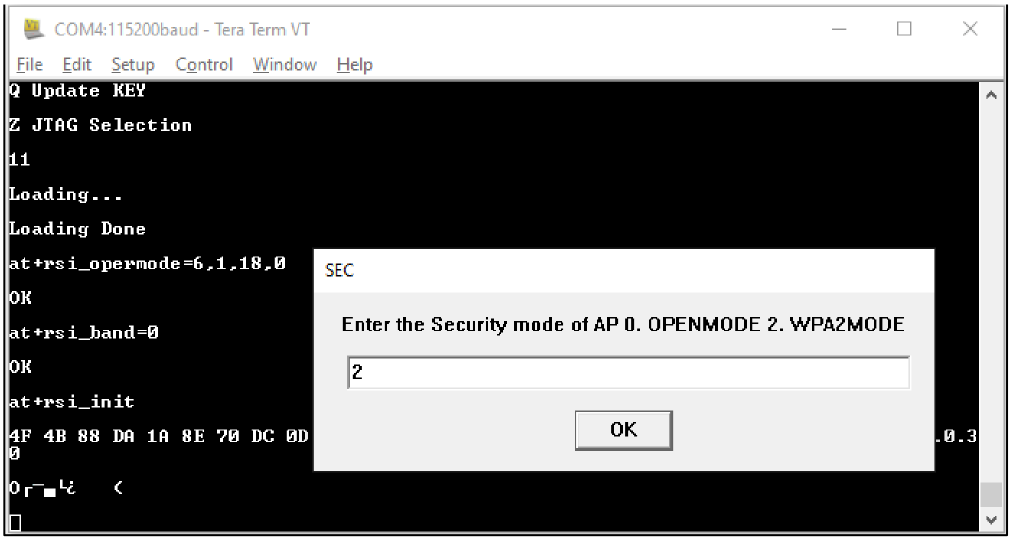
Enter the SSID of AP(max 34 bytes):

silabs

8. The next pop up is for input (security mode) from the user, user needs to enter the security mode(2) and hit 'OK',

0 - Open Security

2 - WPA2 PSK Security

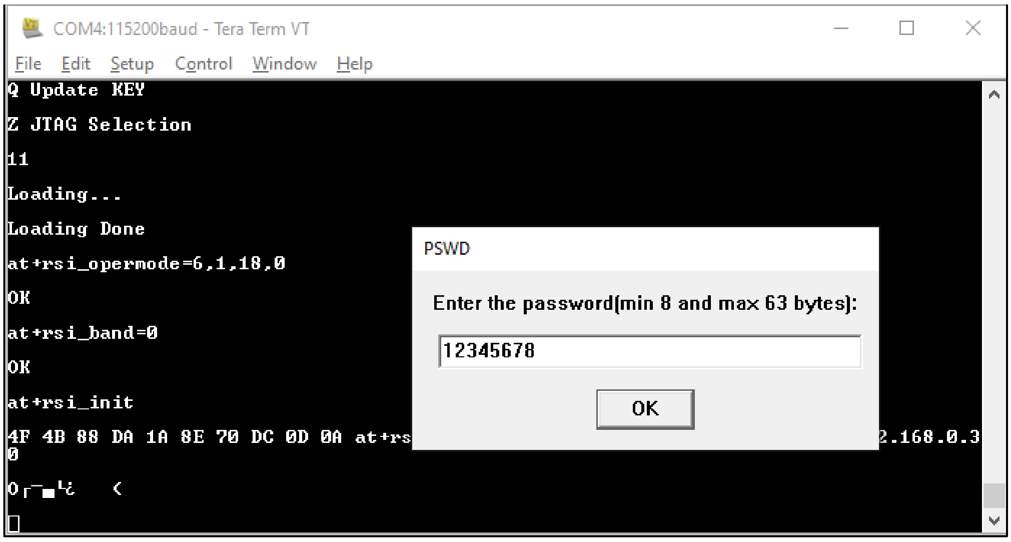

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
SEC
OK

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D                                          .0.3
0
O┌¯▄└¿   <
```

Enter the Security mode of AP 0. OPENMODE 2. WPA2MODE

2

9. Tera term will pop up for input (PSK of the AP) from the user, the user needs to enter the PSK (12345678) and hit 'OK'.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rs                    2.168.0.3
0
O┌‾▄└¿   <
```

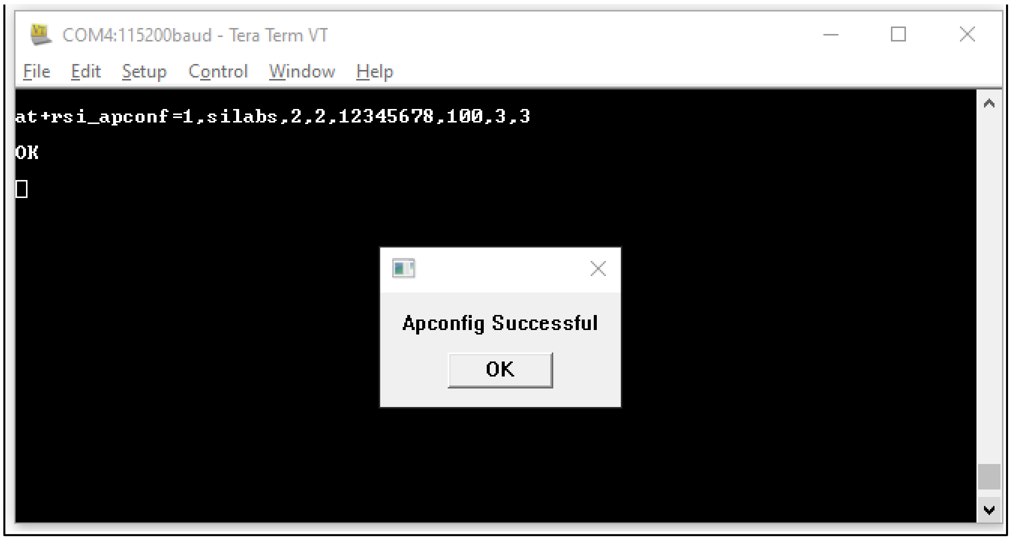
PSWD

Enter the password(min 8 and max 63 bytes):

12345678

10. The command will go as "at+rsi_apconf=1,silabs,2,2,12345678,100,3,3"

The SSID is configured as “silabs” operate in channel 1 and the WPA2 PSK set is "12345678"

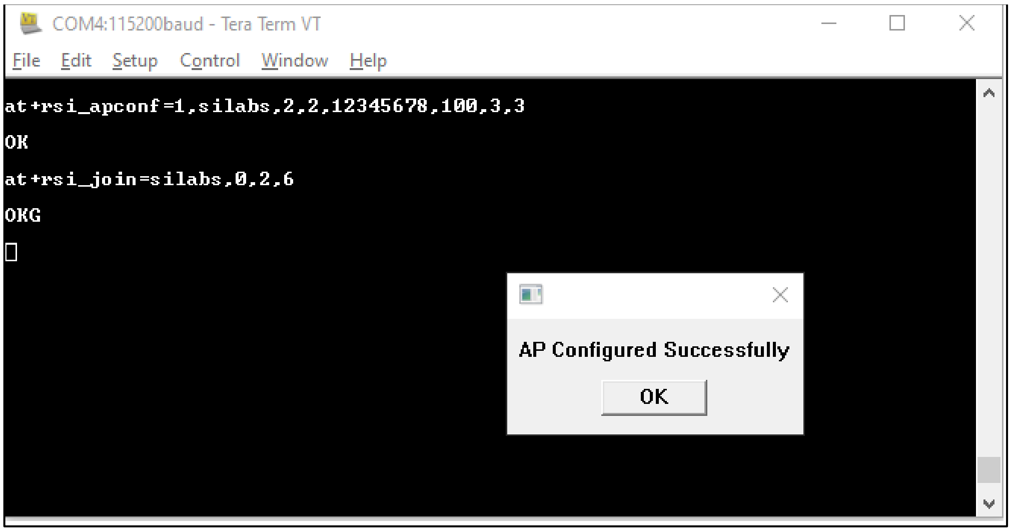

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
at+rsi_apconf=1,silabs,2,2,12345678,100,3,3
OK
```

Apconfig Successful

11. The next command will go as at+rsi_join=silabs,0,2,6, This starts the Access Point functionality in the module. The module is now configured as an Access Point. Its IP address is 192.168.0.30.

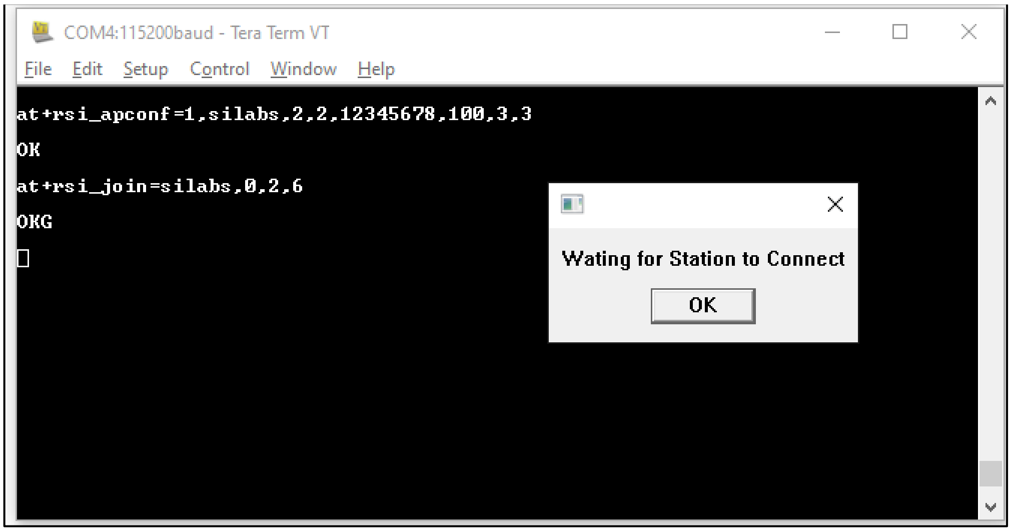
A remote peer can now scan for networks and the SSID of the module, “silabs” will be displayed in the remote peer’s list of Scanned APs. After the remote peer connects to the AP, it acquires an IP address over DHCP.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
at+rsi_apconf=1,silabs,2,2,12345678,100,3,3
OK
at+rsi_join=silabs,0,2,6
OKG
```

AP Configured Successfully

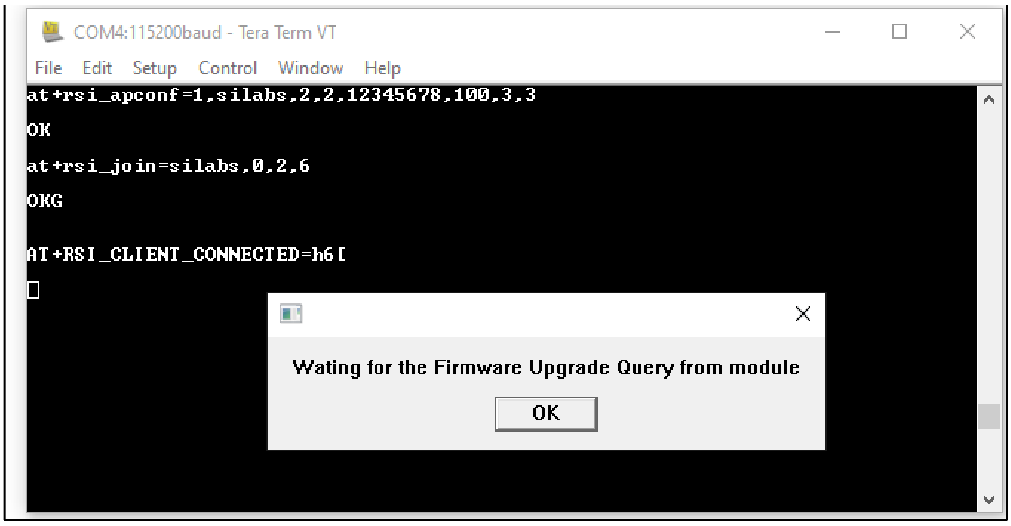
12. After It will popup as shown then Module configured as an Access Point: Connect a Laptop which has the new firmware file (.rps extension) to the module.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
at+rsi_apconf=1,silabs,2,2,12345678,100,3,3
OK
at+rsi_join=silabs,0,2,6
OKG
```

Wating for Station to Connect

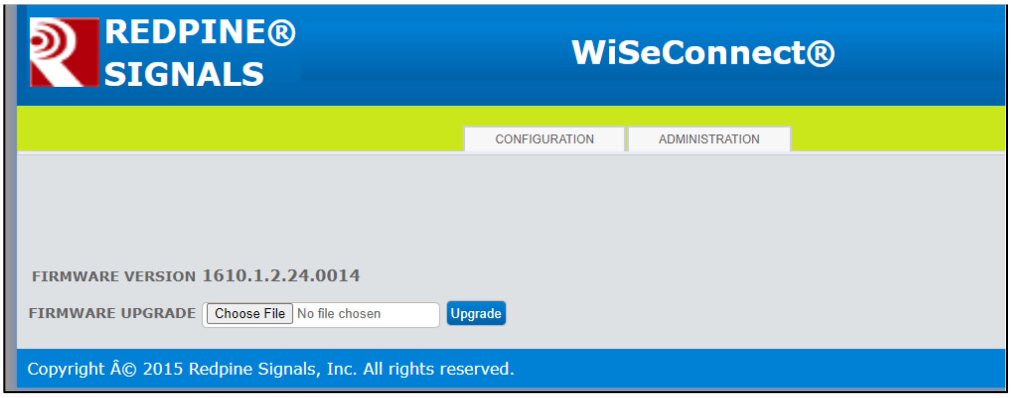
13. Connect a Laptop that has the new firmware file (.rps extension) to the Access Point. After The module respond with “Waiting for the Firmware Upgrade Query from the module”


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
at+rsi_apconf=1,silabs,2,2,12345678,100,3,3
OK
at+rsi_join=silabs,0,2,6
OKG

AT+RSI_CLIENT_CONNECTED=h6[
```

Wating for the Firmware Upgrade Query from module

14. Open the URL **http://<Module's IP address>**in the Laptop. For example, if the module was configured to have an IP of 192.168.0.30, then the URL is http://192.168.0.30. Make sure the browser in the laptop does not have any proxies enabled. On the webpage that opens, click on the "ADMINISTRATION" tab.



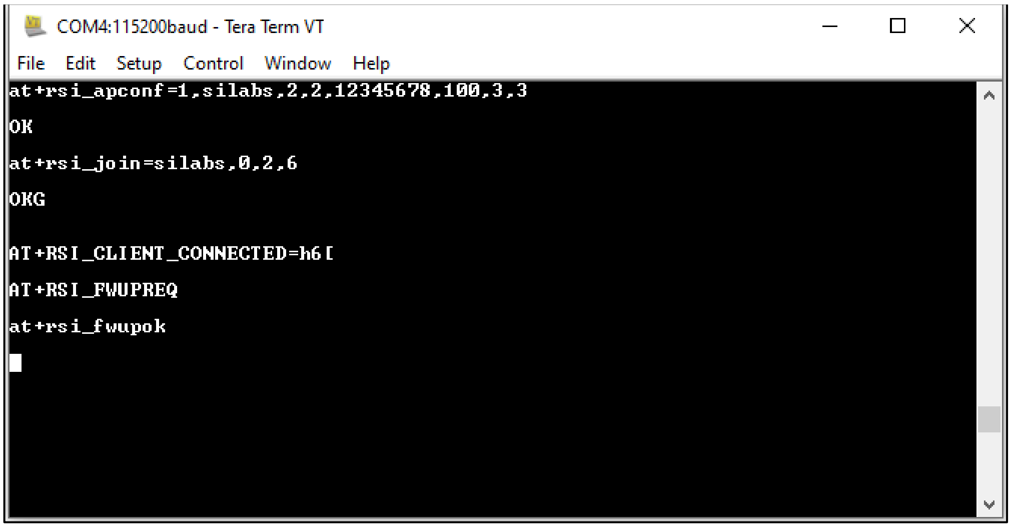
FIRMWARE VERSION 1610.1.2.24.0014

FIRMWARE UPGRADE No file chosen

Copyright Â© 2015 Redpine Signals, Inc. All rights reserved.

15. Click on "Browse" to navigate to the location of the firmware file (.rps extension), select the file and click "Open". Next, click on "Upgrade".

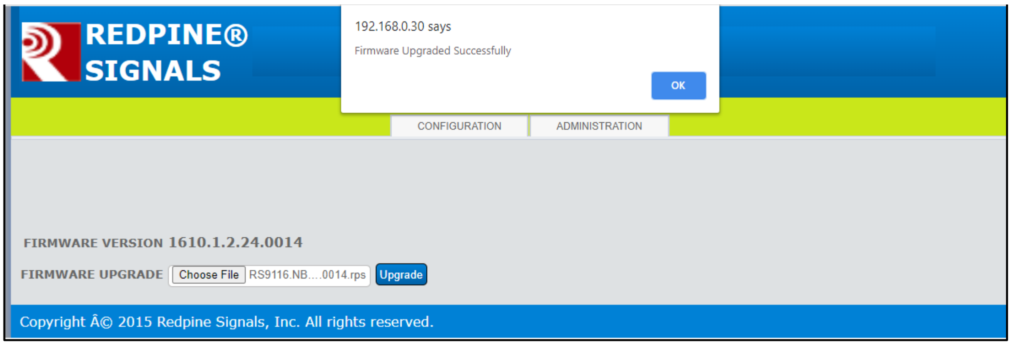
16. The module sends a response (AT+RSI_FWUPREQ) to the Host PC to confirm the Firmware Upgrade, as shown in the figure below. The Host has to send the confirmation command (AT+RSI_FWUPOK) to start upgrading the firmware.



COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
at+rsi_apconf=1,silabs,2,2,12345678,100,3,3
OK
at+rsi_join=silabs,0,2,6
OKG

AT+RSI_CLIENT_CONNECTED=h6[
AT+RSI_FWUPREQ
at+rsi_fwupok
```

17. Once the up-gradation is done, a "Firmware Upgraded Successfully" message is displayed, as shown in the figure below.



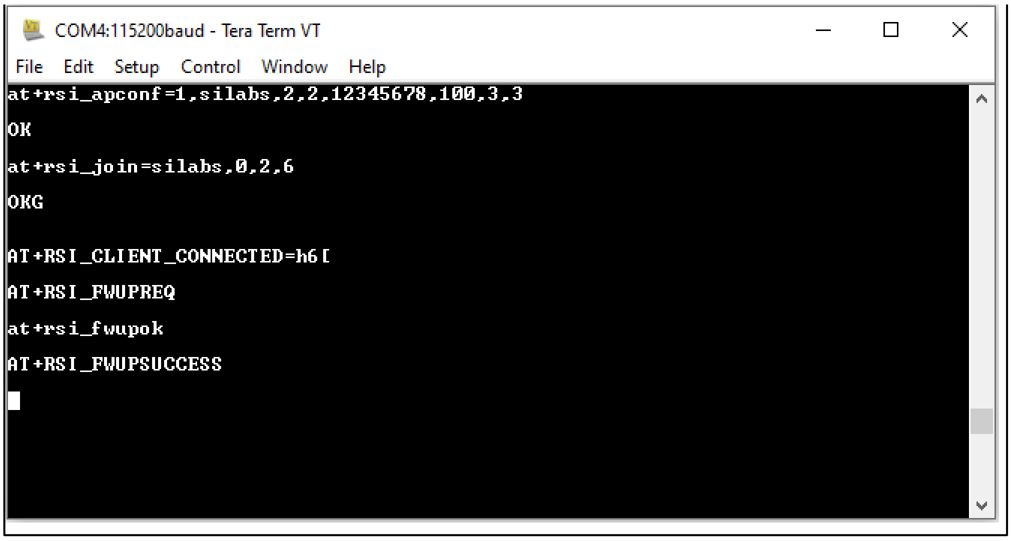
192.168.0.30 says

Firmware Upgraded Successfully

FIRMWARE VERSION 1610.1.2.24.0014

FIRMWARE UPGRADE RS9116.NB.....0014.rps

Copyright Â© 2015 Redpine Signals, Inc. All rights reserved.

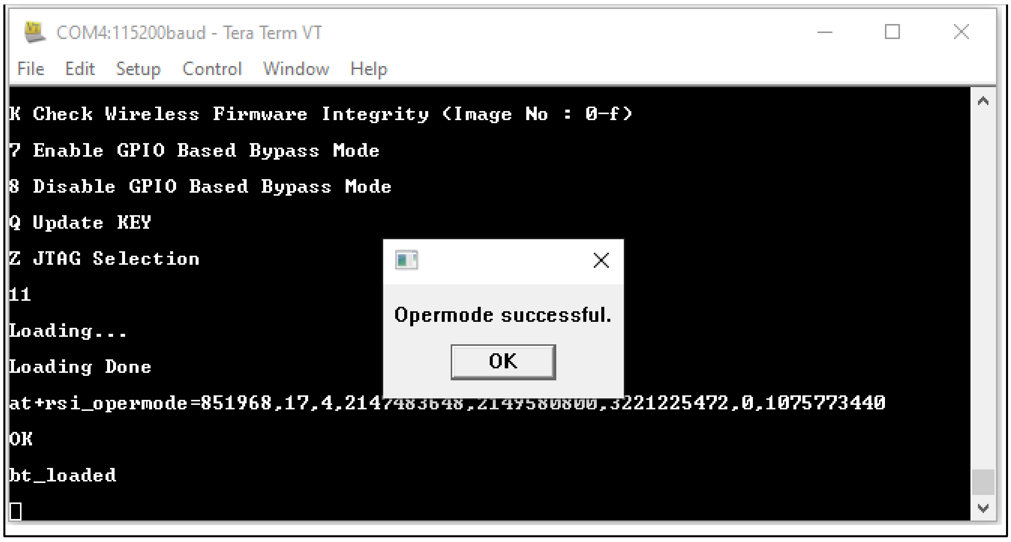


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
at+rsi_apconf=1,silabs,2,2,12345678,100,3,3
OK
at+rsi_join=silabs,0,2,6
OKG

AT+RSI_CLIENT_CONNECTED=h6[
AT+RSI_FWUPREQ
at+rsi_fwupok
AT+RSI_FWUPSUCCESS
```

8.7 Low Power Standby_Associated WiFi Station and BLE Advertising

1. For running this script user need to use “Low Power Standby_Associated WiFi Station and BLE Advertising.ttl” from the list.
2. After that Opermode command 'at+rsi_opermode=851968,17,4,2147483648,2149580800,3221225472,0,1075773440’ configures the module as Wi-Fi client and Ble advertising. The module responds with “OK” & “bt_loaded”.

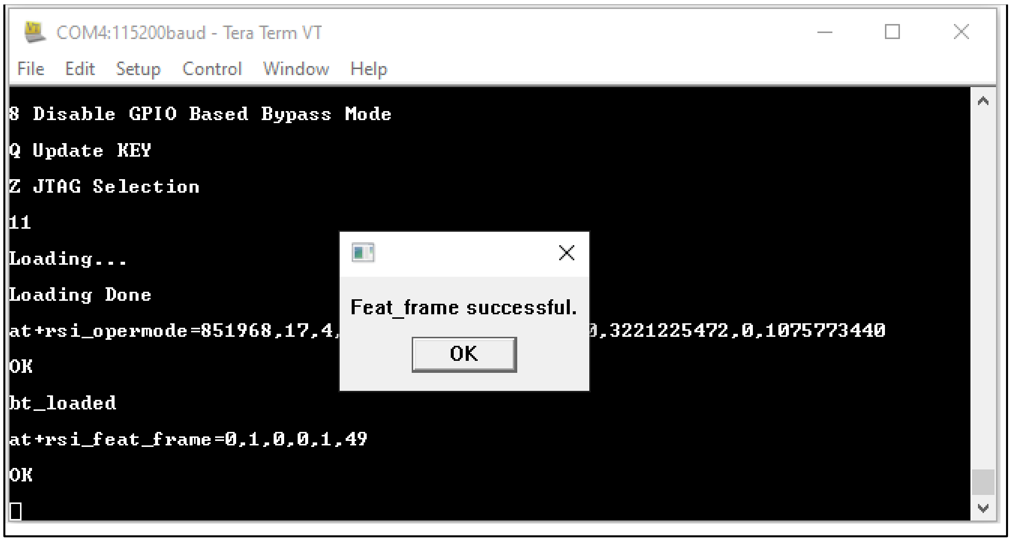

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=851968,17,4,2147483648,2149580800,3221225472,0,1075773440
OK
bt_loaded
```

Opermode successful.

3. Next following commands run one by one and finally one pop will come. “Device is now advertising as a RS9116W_BLE use your BLE app to check for the device”.

> Feat_frame after this frame Success pop will come to go with “ok”


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=851968,17,4,                    0,3221225472,0,1075773440
OK
bt_loaded
at+rsi_feat_frame=0,1,0,0,1,49
OK
```

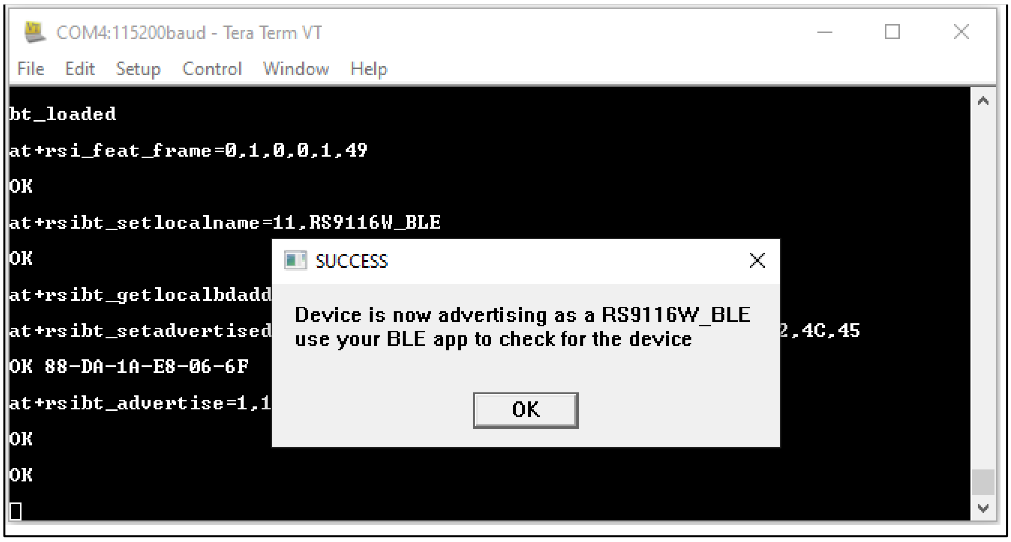
Feat_frame successful.

>Set Local Name

>Get a local BD address.

>Set Advertise Data

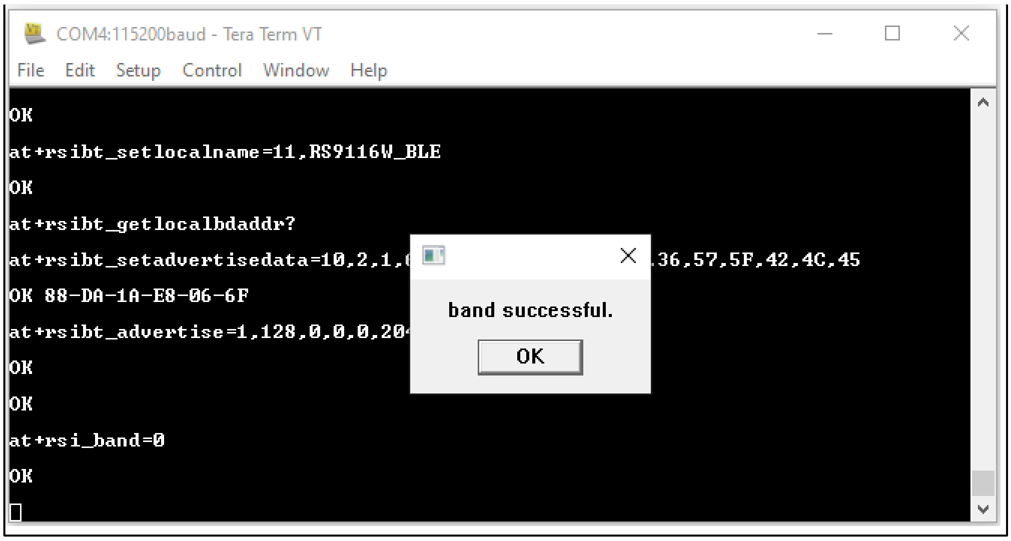
>Advertise command.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
SUCCESS
OK

```
bt_loaded
at+rsi_feat_frame=0,1,0,0,1,49
OK
at+rsibt_setlocalname=11,RS9116W_BLE
OK
at+rsibt_getlocalbdadd
at+rsibt_setadvertised                                  2,4C,45
OK 88-DA-1A-E8-06-6F
at+rsibt_advertise=1,1
OK
OK
```

Device is now advertising as a RS9116W_BLE use your BLE app to check for the device

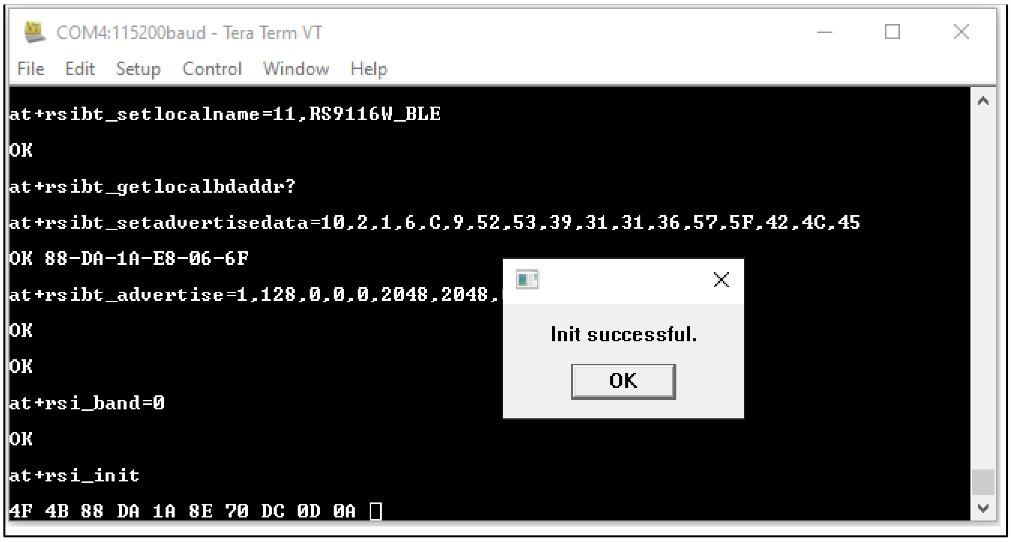
4. The band configured is 2.4Ghz in the Scripts. Once the band is configured , The module responds with “OK”.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
OK
at+rsibt_setlocalname=11,RS9116W_BLE
OK
at+rsibt_getlocalbdaddr?
at+rsibt_setadvertisedata=10,2,1,(                     .36,57,5F,42,4C,45
OK 88-DA-1A-E8-06-6F
at+rsibt_advertise=1,128,0,0,0,204
OK
OK
at+rsi_band=0
OK
```

band successful.

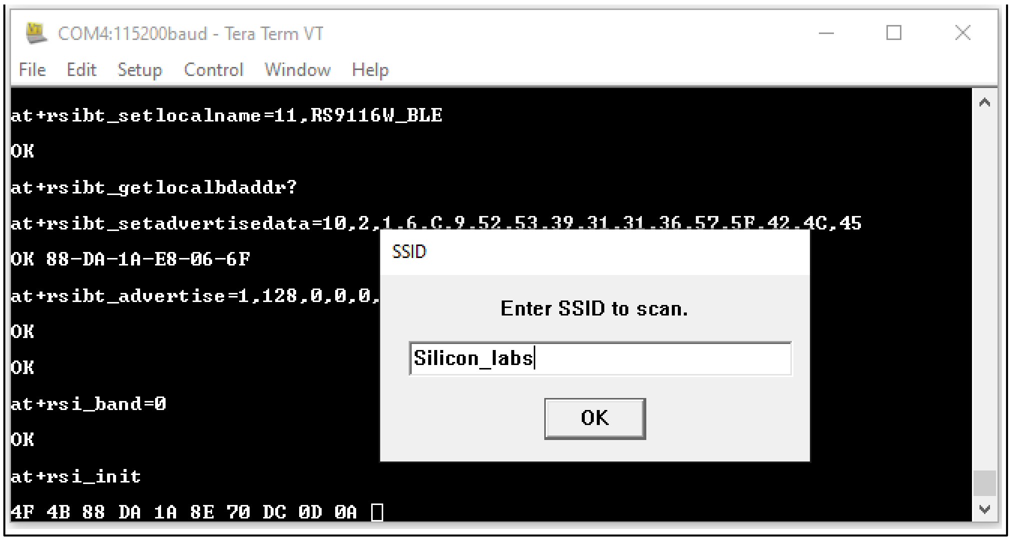
5. "at+rsi_init" command initializes the RF of the module. The module responds with OK<MAC_Address>.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
at+rsibt_setlocalname=11,RS9116W_BLE
OK
at+rsibt_getlocalbdaddr?
at+rsibt_setadvertisedata=10,2,1,6,C,9,52,53,39,31,31,36,57,5F,42,4C,45
OK 88-DA-1A-E8-06-6F
at+rsibt_advertise=1,128,0,0,0,2048,2048,
OK
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A
```

Init successful.

6. Tera term will pop up for scan SSID input from the user, user needs to enter the SSID to scan and hit 'OK', (at+rsi_scan=0, Silicon_labs)This command scans for particular Access Point operating in the 2.4 GHz band.
The module responds with information of the Access Points scanned. The data received might have some unreadable characters because of ASCII conversion.

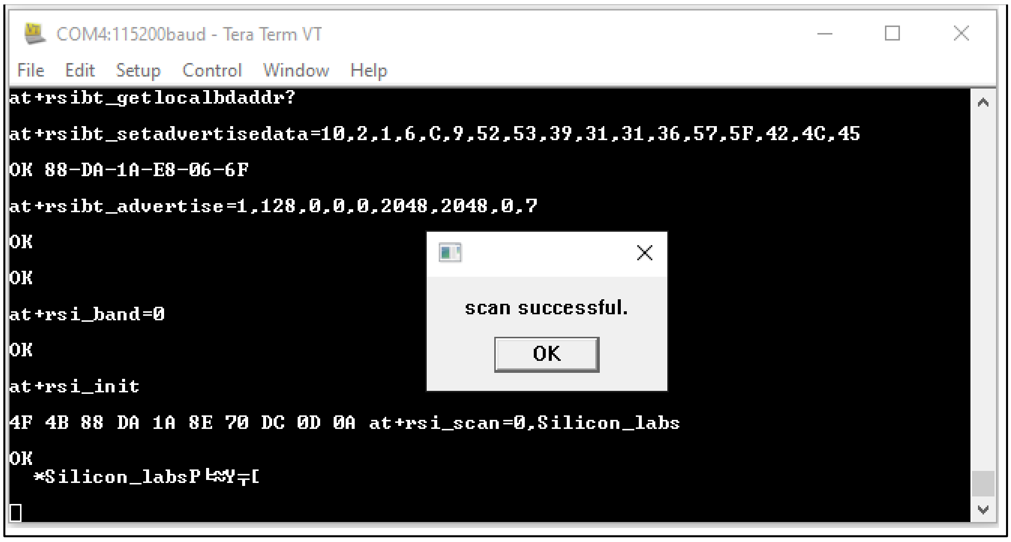

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
SSID
OK

```
at+rsibt_setlocalname=11,RS9116W_BLE
OK
at+rsibt_getlocalbdaddr?
at+rsibt_setadvertisedata=10,2,1,6,C,9,52,53,39,31,31,36,57,5F,42,4C,45
OK 88-DA-1A-E8-06-6F
at+rsibt_advertise=1,128,0,0,0,
OK
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A
```

Enter SSID to scan.

Silicon_labs

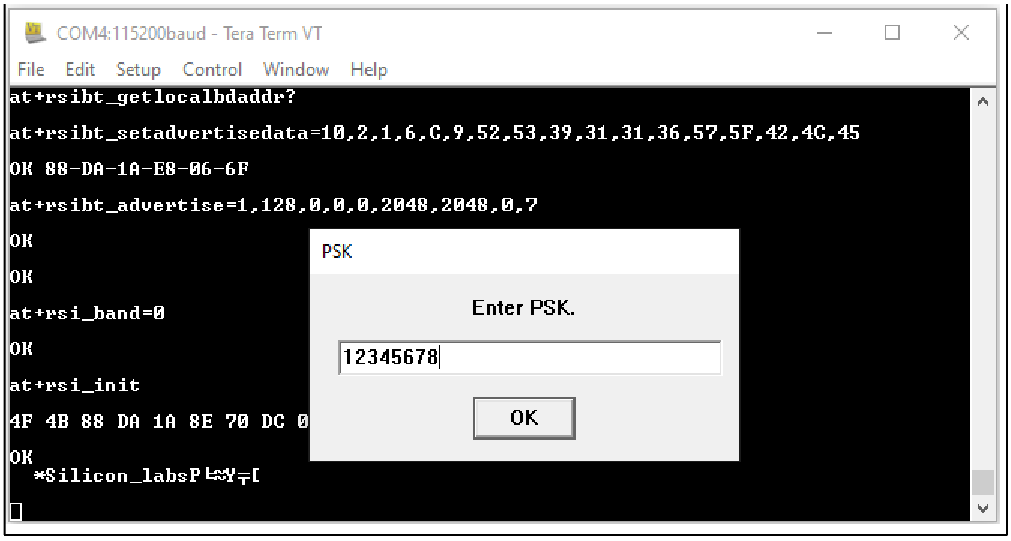
7. After Scan response, one pop with “scan successful” come, go with the “OK” button.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
at+rsibt_getlocalbdaddr?
at+rsibt_setadvertisedata=10,2,1,6,C,9,52,53,39,31,31,36,57,5F,42,4C,45
OK 88-DA-1A-E8-06-6F
at+rsibt_advertise=1,128,0,0,0,2048,2048,0,7
OK
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_scan=0,Silicon_labs
OK
 *Silicon_labsP╘≈Y╤[
```

scan successful.

8. Tera term will pop up for psk input from the user, the user needs to enter the psk and hit 'OK', This command configures the PSK of the Wi-Fi client with the key entered by the user.

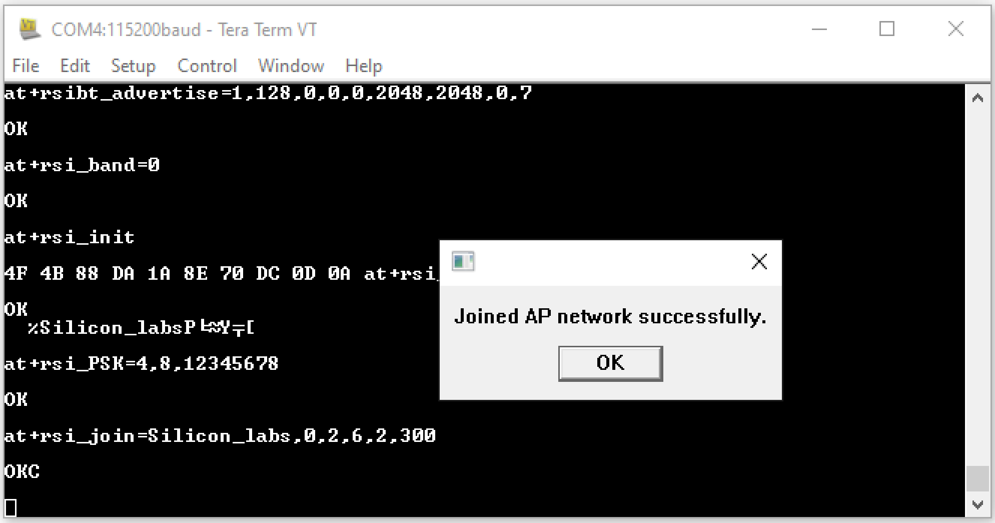

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
PSK
OK

```
at+rsibt_getlocalbdaddr?
at+rsibt_setadvertisedata=10,2,1,6,C,9,52,53,39,31,31,36,57,5F,42,4C,45
OK 88-DA-1A-E8-06-6F
at+rsibt_advertise=1,128,0,0,0,2048,2048,0,7
OK
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0
OK
 *Silicon_labsP╘≈Y╤[
```

Enter PSK.

12345678

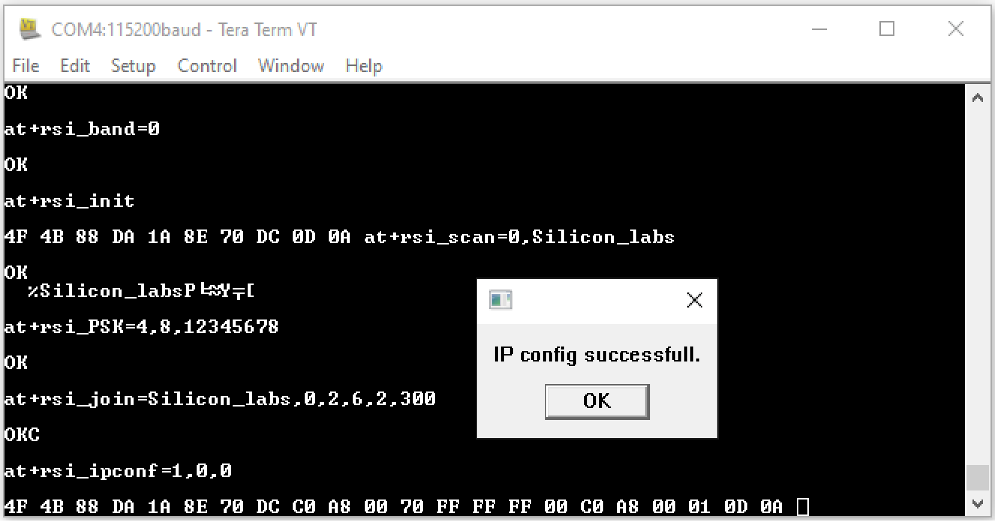
9. The next command will go as 'at+rsi_join=Silicon_labs,0,2,6' This command connects the Wi-Fi client to the Access Point with SSID "Silicon_labs”. On successful association, the module responds with OK.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
at+rsibt_advertise=1,128,0,0,0,2048,2048,0,7
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_
OK
 %Silicon_labsP╘≈Y╤[
at+rsi_PSK=4,8,12345678
OK
at+rsi_join=Silicon_labs,0,2,6,2,300
OKC
```

Joined AP network successfully.

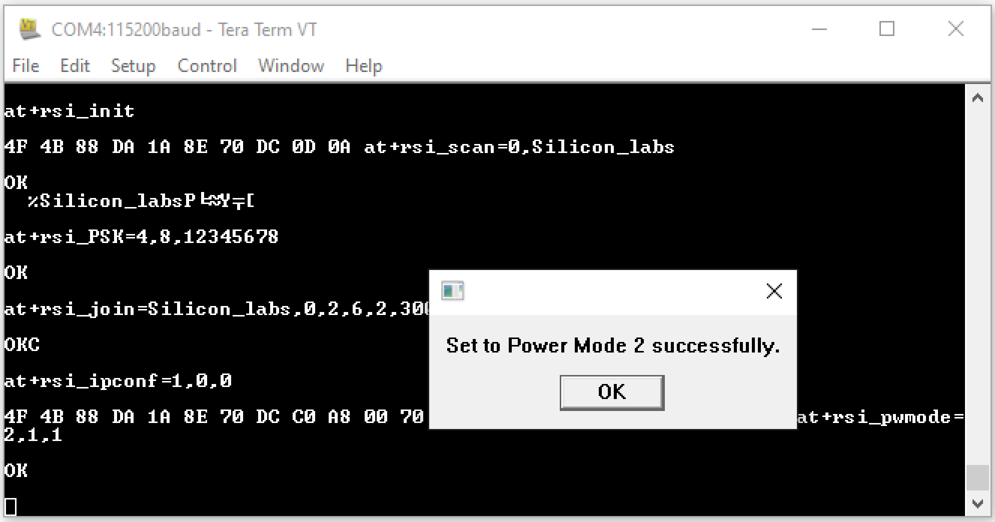
10. After join successful next command will go as 'at+rsi_ipconf=1', This command configures the IP address of the module.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_scan=0,Silicon_labs
OK
  %Silicon_labsP╘≈Y╤[
at+rsi_PSK=4,8,12345678
OK
at+rsi_join=Silicon_labs,0,2,6,2,300
OKC
at+rsi_ipconf=1,0,0
4F 4B 88 DA 1A 8E 70 DC C0 A8 00 70 FF FF FF 00 C0 A8 00 01 0D 0A
```

IP config successfull.

11. After successful ipconfig Power save success pop up will come. Go with "ok" response.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

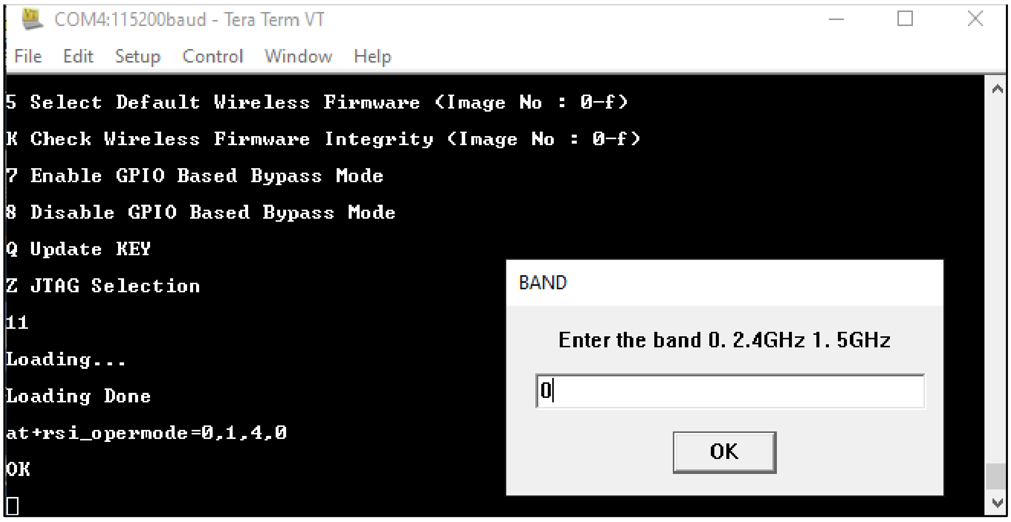
```
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_scan=0,Silicon_labs
OK
  %Silicon_labsP╘≈Y╤[
at+rsi_PSK=4,8,12345678
OK
at+rsi_join=Silicon_labs,0,2,6,2,300
OKC
at+rsi_ipconf=1,0,0
4F 4B 88 DA 1A 8E 70 DC C0 A8 00 70                              at+rsi_pwmode=
2,1,1
OK
```

Set to Power Mode 2 successfully.

8.8 Station Mode

1. For running this script user need to use Station_mode.ttl from the list.
2. The Opermode command 'at+rsi_opermode=0,1,4,0' configures the module as Wi-Fi client. The module responds with "OK"

3. Tera term will pop up for input (band) from the user, user needs to enter the band and hit 'OK', (at+rsi_band=0)This command configures the operating band of Wi-Fi client to 2.4GHz. The module responds with "OK".

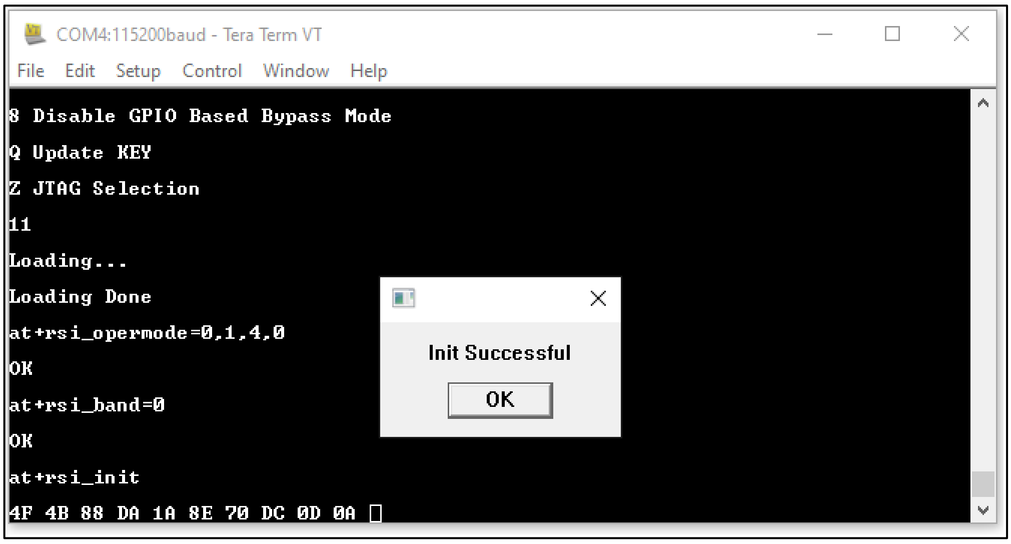

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
BAND
OK

```
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=0,1,4,0
OK
```

Enter the band 0. 2.4GHz 1. 5GHz

0

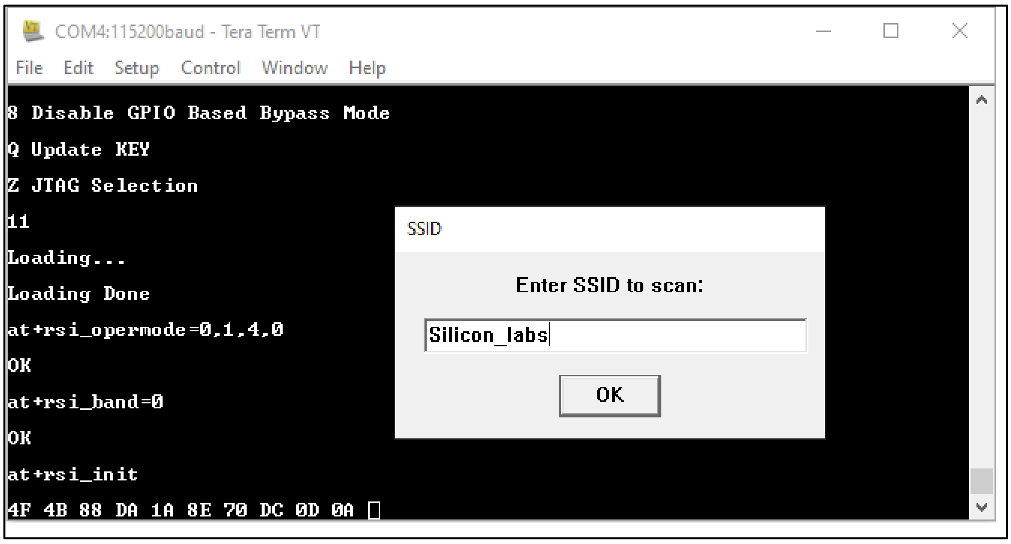
4. The next command will go as 'at+rsi_init', This command initializes the Wi-Fi module in the EVB. The module responds with OK<MAC_Address>.
Here 4F 4B is for OK and the remaining data is for MAC Address.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=0,1,4,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A
```

Init Successful

5. Tera term will pop up for scan SSID input from the user, user needs to enter the SSID to scan and hit 'OK', (at+rsi_scan=0, Silicon_labs)This command scans for particular Access Point operating in the 2.4 GHz band. The module responds with information of the Access Points scanned. The data received might have some unreadable characters because of ASCII conversion.

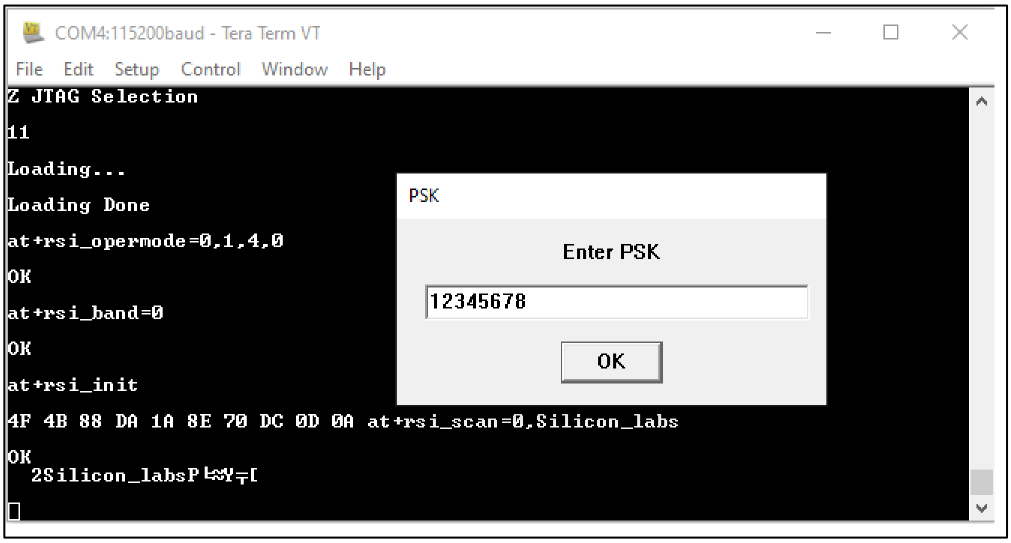

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
SSID
OK

```
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=0,1,4,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A
```

Enter SSID to scan:

Silicon_labs

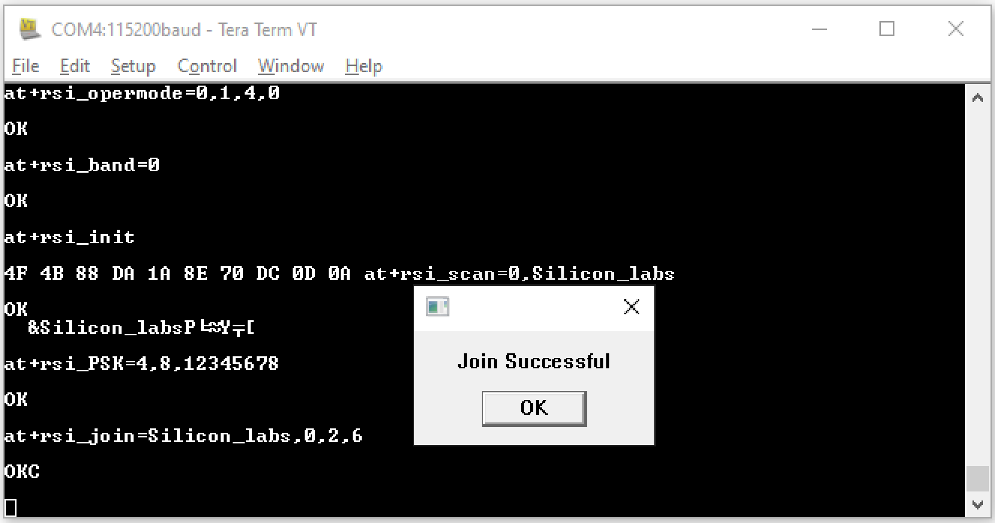
6. Tera term will pop up for psk input from the user, user needs to enter the psk and hit 'OK', This command configures the PSK of the Wi-Fi client with the key entered by the user


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
PSK
Enter PSK
OK

```
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=0,1,4,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_scan=0,Silicon_labs
OK
  2Silicon_labsP└≈Y╤[
```

12345678

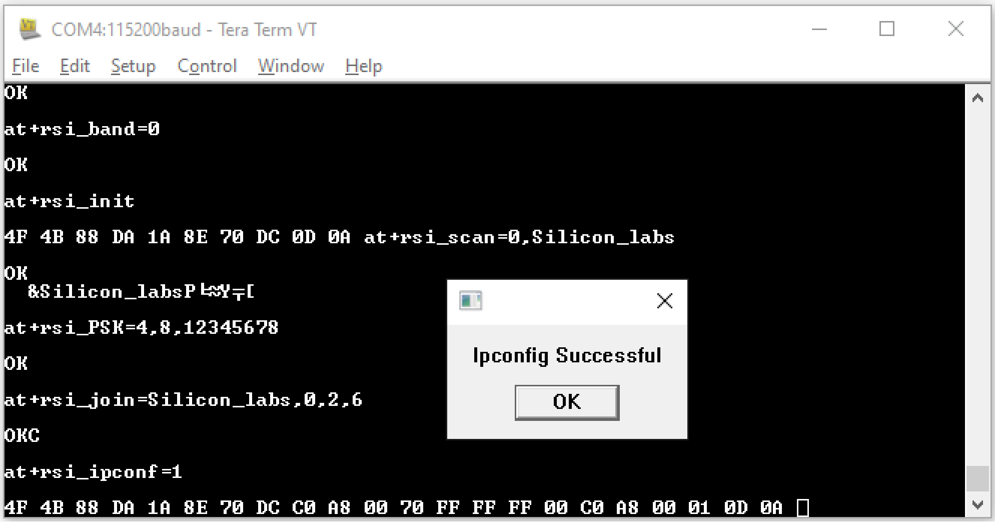
7. The next command will go as 'at+rsi_join=Silicon_labs,0,2,6' This command connects the Wi-Fi client to the Access Point with SSID "Silicon_labs”. On successful association, the module responds with OK.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
at+rsi_opermode=0,1,4,0
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_scan=0,Silicon_labs
OK
  &Silicon_labsP└≈Y╤[
at+rsi_PSK=4,8,12345678
OK
at+rsi_join=Silicon_labs,0,2,6
OKC
```

Join Successful

8. After join successful next command will go as 'at+rsi_ipconf=1', This command configures the IP address of the module

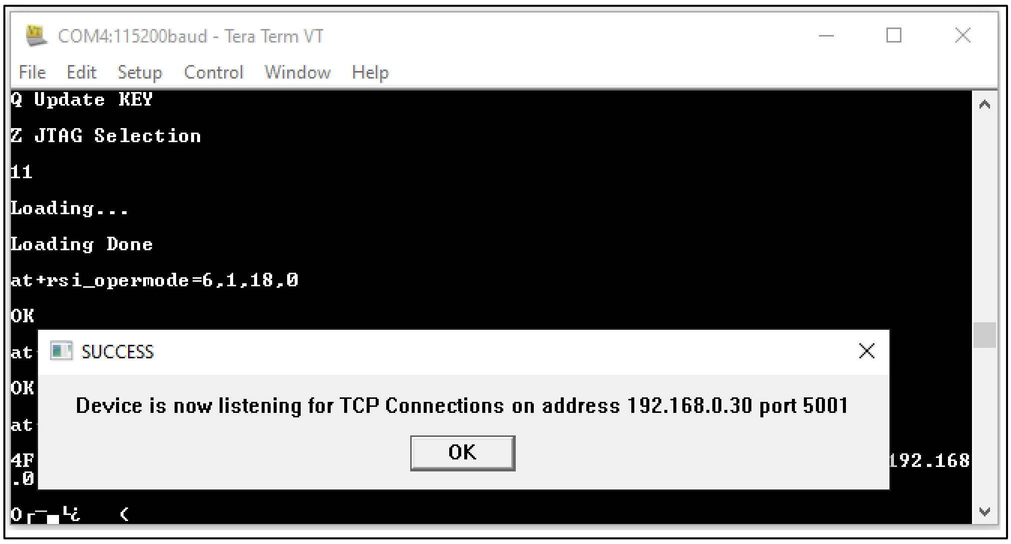

COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
OK
at+rsi_band=0
OK
at+rsi_init
4F 4B 88 DA 1A 8E 70 DC 0D 0A at+rsi_scan=0,Silicon_labs
OK
  &Silicon_labsP└≈Y╤[
at+rsi_PSK=4,8,12345678
OK
at+rsi_join=Silicon_labs,0,2,6
OKC
at+rsi_ipconf=1
4F 4B 88 DA 1A 8E 70 DC C0 A8 00 70 FF FF FF 00 C0 A8 00 01 0D 0A
```

Ipconfig Successful

9. It will open a TCP Server socket on the Wi-Fi Client (EVB) side using the following AT command 'at+rsi_ltcp=5001', The module's response will look as follows:

OK<ip_version><socket_type><socket_handle><Lport><module_ipaddr>\r\n, pop up window will display "Device is now listening for TCP connections on address x.x.x.x and port y" here x.x.x.x Ip address of the Module and 'y' is the port number of the Module Socket.


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help
SUCCESS
OK

```
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=6,1,18,0
OK
at
OK
at
4F                                                        192.168
.0
0┌─▄└¿   ‹
```

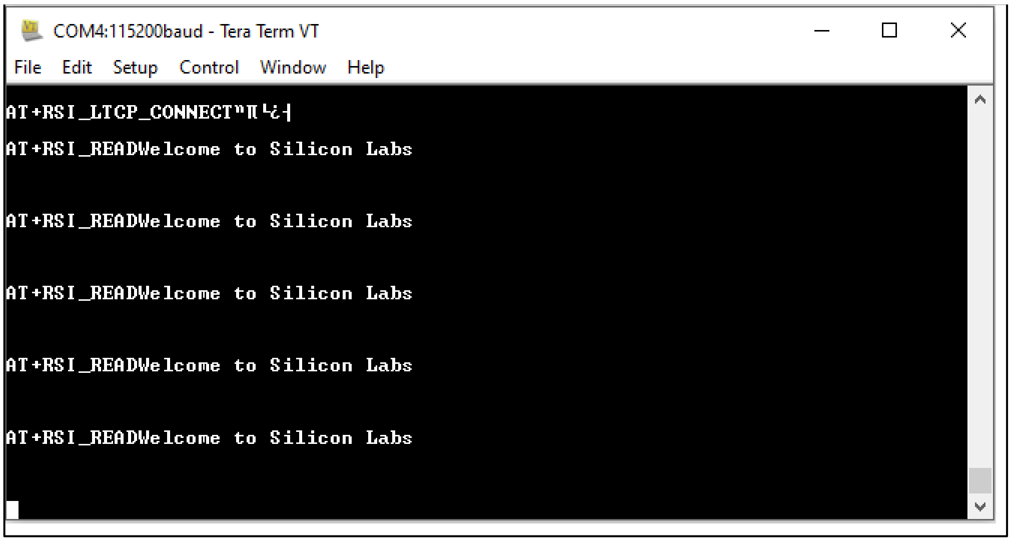
Device is now listening for TCP Connections on address 192.168.0.30 port 5001

10. Open a TCP client socket on a remote peer and connect to the Server socket by giving the server IP and port number.

11. Observe that the Teraterm on the Wi-Fi Client-side (EVB) prints the following message, once the TCP connection is set up with the remote peer.

    AT+RSI_LTCP_CONNECT=<ip_version><socket_descriptor><dest_port_no><dest_ipaddr><mss><window_size><src_port_no>\r\n The data received might have some unreadable characters because of ASCII conversion

12. When the data is received on the Wi-Fi Client (EVB) side, you will see a response (asynchronous) from the module as follows:



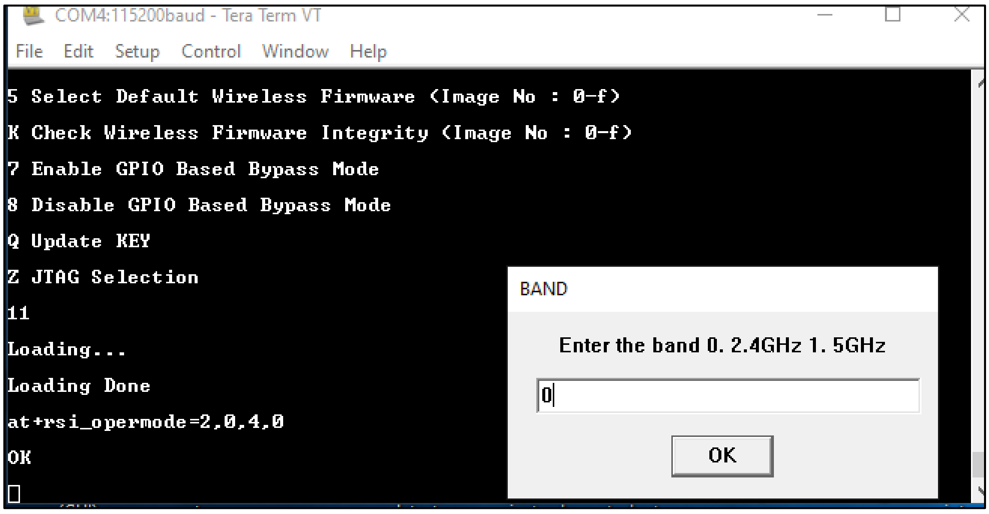
COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
AT+RSI_LTCP_CONNECT"╥╘¿┤
AT+RSI_READWelcome to Silicon Labs

AT+RSI_READWelcome to Silicon Labs

AT+RSI_READWelcome to Silicon Labs

AT+RSI_READWelcome to Silicon Labs

AT+RSI_READWelcome to Silicon Labs
```

Note : In order to measure **low power** in STA or Client mode, use "Low Power StandBy_Associated WiFi Station" script present in folder Release packageRS9116.NB0.WC.GENR.OSI.x.x.xx\utils\scripts\TeraTerm_TTL_Scripts. For executing this ttl script please refer to document AN1280: RS9116W Power Save Application Notes from https://docs.silabs.com/rs9116

8.9 Wi-Fi Client in Enterprise Security Mode

1. For running this script user need to use WLAN_EAP_PEAP_station.ttl from the list.
2. The first command it will go as "at+rsi_opermode=2,0,4,0" after running the TTL script, This command configures the module as a Wi-Fi client. The module responds with “OK”
3. Tera term will pop up for input (band) from the user, the user needs to enter the band and hit 'OK', (at+rsi_band=0)This command configures the operating band of the Wi-Fi client to 2.4GHz. The module responds with “OK”



COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
11
Loading...
Loading Done
at+rsi_opermode=2,0,4,0
OK
```

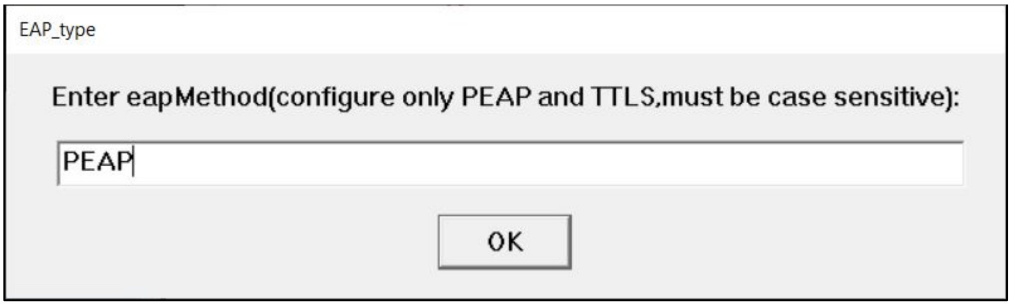
BAND

Enter the band 0. 2.4GHz 1. 5GHz

0

OK

4. The next command will go as 'at+rsi_init', This command initializes the Wi-Fi module in the EVB. The module responds with OK<MAC_Address>.
5. Tera term will pop up for input (eap method) from the user, the user needs to enter the EAP method and hit 'OK'.

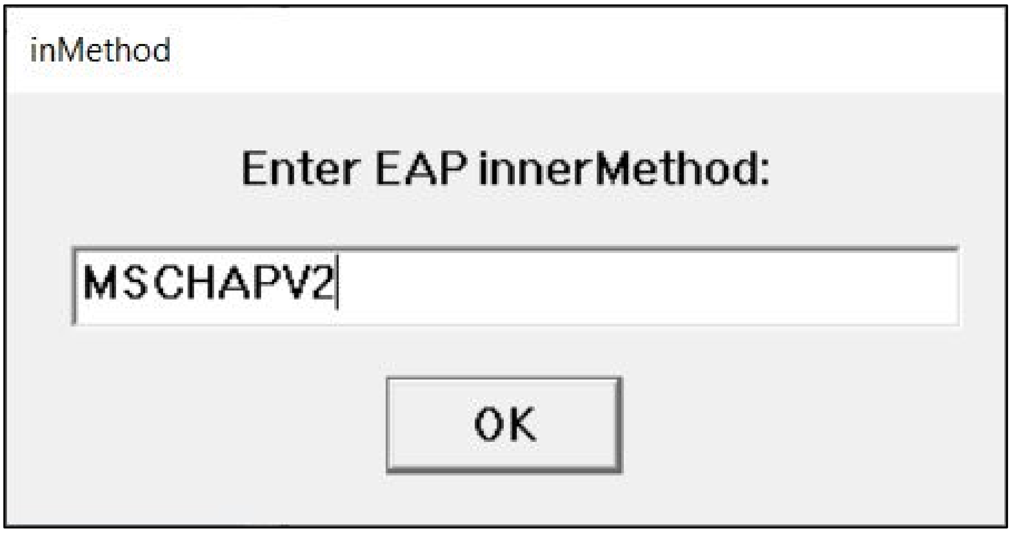


EAP_type

Enter eapMethod(configure only PEAP and TTLS,must be case sensitive):

PEAP

6. Tera term will pop up for input (EAP inner method) from the user, the user needs to enter the eap inner method and hit 'OK'.

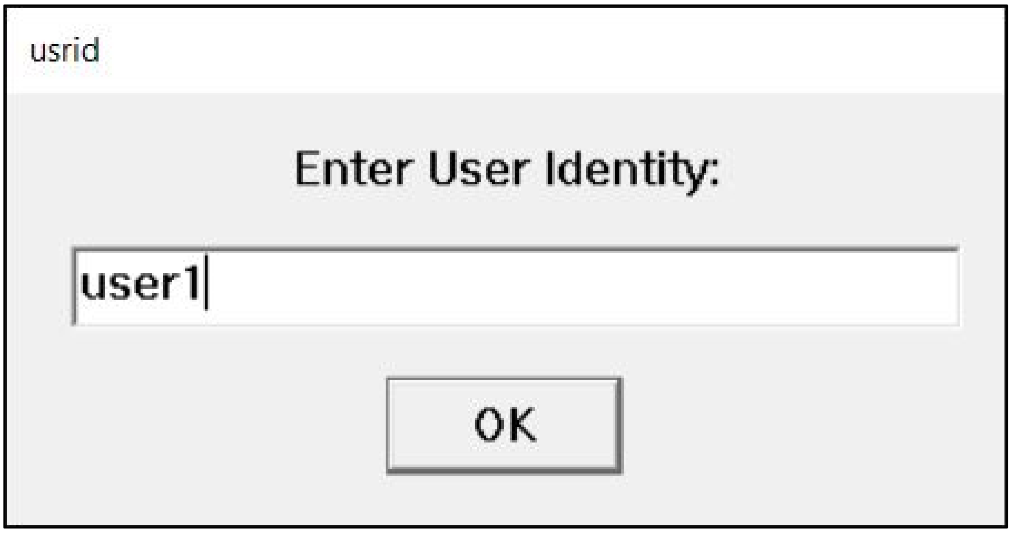


inMethod

Enter EAP innerMethod:

MSCHAPV2

7. Tera term will pop up for input (User identity) from the user, the user needs to enter the User identity and hit 'OK'.

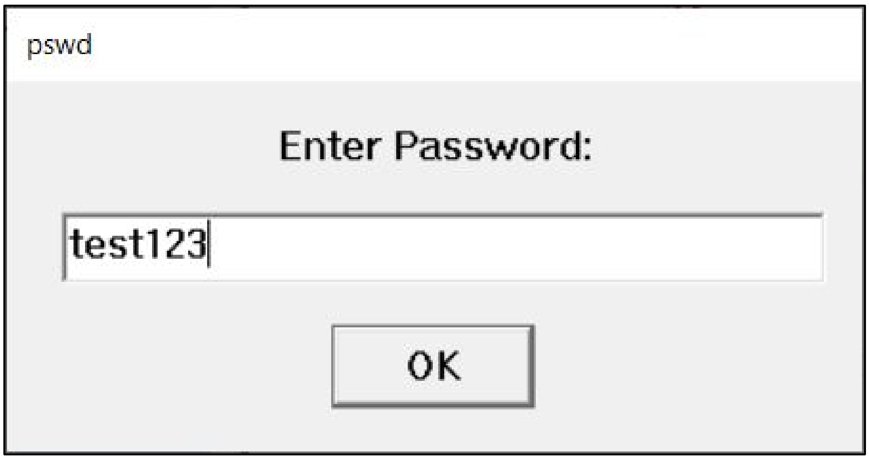


usrid

Enter User Identity:

user1

8. Tera term will pop up for input (password) from the user, the user needs to enter the password and hit 'OK'.



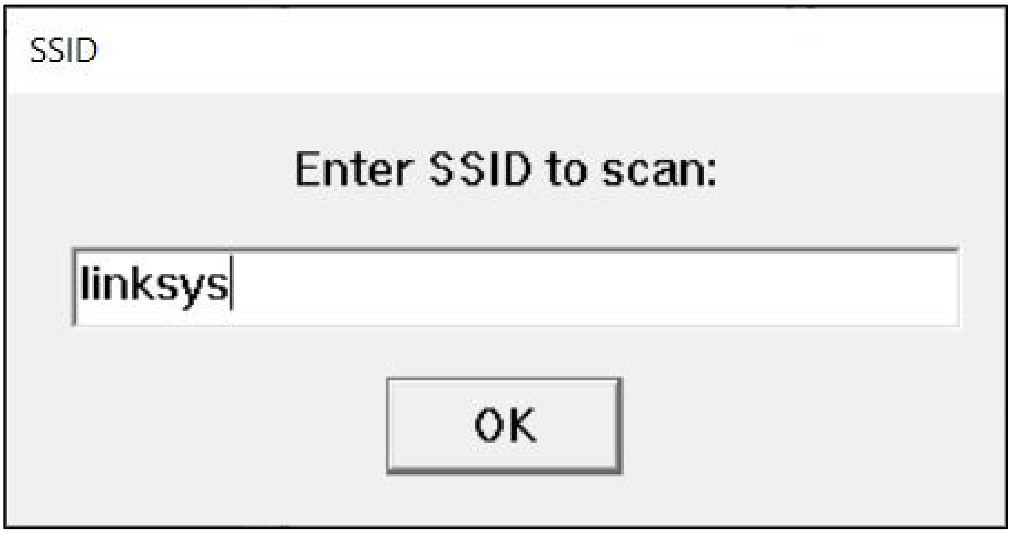
pswd

Enter Password:

test123

9. The command will go as "at+rsi_eap=PEAP,MSCHAPV2,user1,test123", This command set the EAP mode for the module and set the authentication credentials (username and password).
10. Tera term will pop up for scan SSID input from the user, the user needs to enter the SSID to scan and hit 'OK', (at+rsi_scan=0,linksys) This command scans for particular Access Point operating in the 2.4 GHz band.

    The module responds with information of the Access Points scanned. The data received might have some unreadable characters because of ASCII conversion.

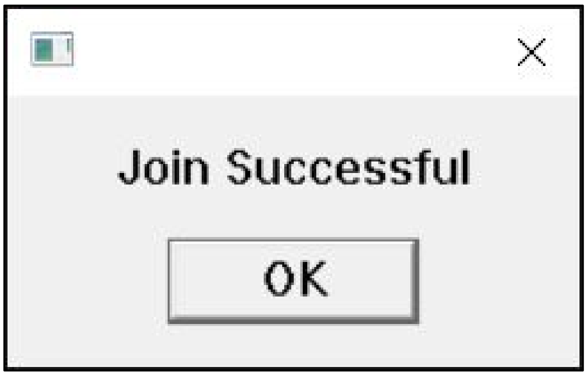


SSID

Enter SSID to scan:

linksys

11. The next command will go as 'at+rsi_join=linksys,0,2,6' This command connects the Wi-Fi client to the Access Point with SSID "linksys”. On successful association, the module responds with OK.

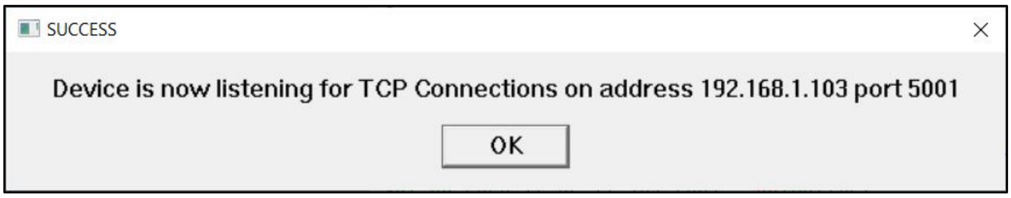


Join Successful

12. After join successful next command will go as 'at+rsi_ipconf=1', This command configures the IP address of the module

13. It will open a TCP Server socket on the Wi-Fi Client (EVB) side using the following AT command 'at+rsi_ltcp=5001', The module’s response will look as follows:

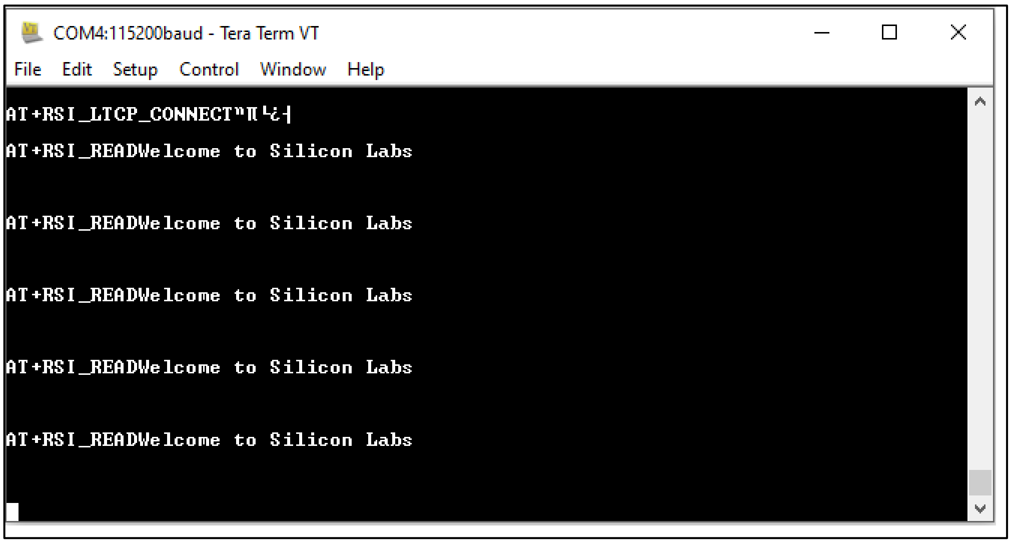
    OK<ip_version><socket_type><socket_handle><Lport><module_ipaddr>\r\n, pop up window will display "Device is now listening for TCP connections on address x.x.x.x and port y" here x.x.x.x Ip address of the Module and 'y' is the port number of the Module Socket.



Device is now listening for TCP Connections on address 192.168.1.103 port 5001

14. Open a TCP client socket on a remote peer and connect to the Server socket by giving the server IP and port number.
15. Observe that the Teraterm on the Wi-Fi Client-side (EVB) prints the following message, once the TCP connection is set up with the remote peer.

    AT+RSI_LTCP_CONNECT=<ip_version><socket_descriptor><dest_port_no><dest_ipaddr><mss><window_size><src_port_no>\r\n The data received might have some unreadable characters because of ASCII conversion
16. When the data is received on the Wi-Fi Client (EVB) side, you will see a response (asynchronous) from the module as follows:


COM4:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
AT+RSI_LTCP_CONNECT"π└¿┤
AT+RSI_READWelcome to Silicon Labs


AT+RSI_READWelcome to Silicon Labs


AT+RSI_READWelcome to Silicon Labs


AT+RSI_READWelcome to Silicon Labs


AT+RSI_READWelcome to Silicon Labs
```

9 Appendix D_ WiSeConnect® Firmware Upgrade

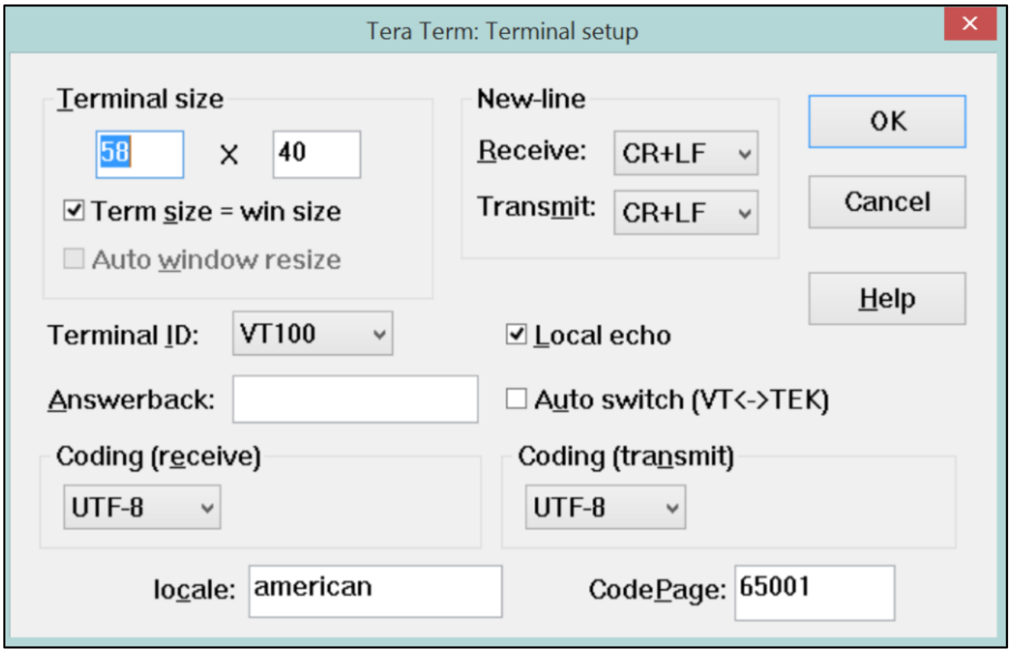
The WiSeConnect® firmware of the module can be upgraded either from the Host or over the Wi-Fi connection. This section describes both these options, with UART being the Host interface. For details on upgrading over other interfaces (SPI, USB and USB-CDC), refer to the Software PRM.

NOTE:

1. The EVK is shipped with the WiSeConnect® firmware pre-loaded. So, a firmware upgrade is not necessary unless there is a newer version available or the EVB has been used in n-Link® mode and the user wants to evaluate the EVB in WiSeConnect® mode after that.
2. The process explained below is for upgrading the WiSeConnect® firmware over UART from a Windows PC using Teraterm. The Software PRM gives details related to the process and commands to be used to upgrade over other interfaces and MCU platforms.

9.1 Firmware Upgrade over UART

1. Download and install Teraterm from http://en.sourceforge.jp/projects/ttssh2/releases/
2. Open Teraterm. You will be asked to set up a "New connection". Click Cancel.
3. In the Teraterm window, click on Setup -> Terminal…In the dialog box that opens, change the following settings:
   a. Under "New-line", select "CR+LF" for Receive and Transmit
   b. Enable "Local echo".
   c. Click OK



Tera Term: Terminal setup

Terminal size: 58 x 40

☑ Term size = win size

☐ Auto window resize

New-line

Receive: CR+LF

Transmit: CR+LF

Terminal ID: VT100

☑ Local echo

Answerback:

☐ Auto switch (VT<->TEK)

Coding (receive): UTF-8

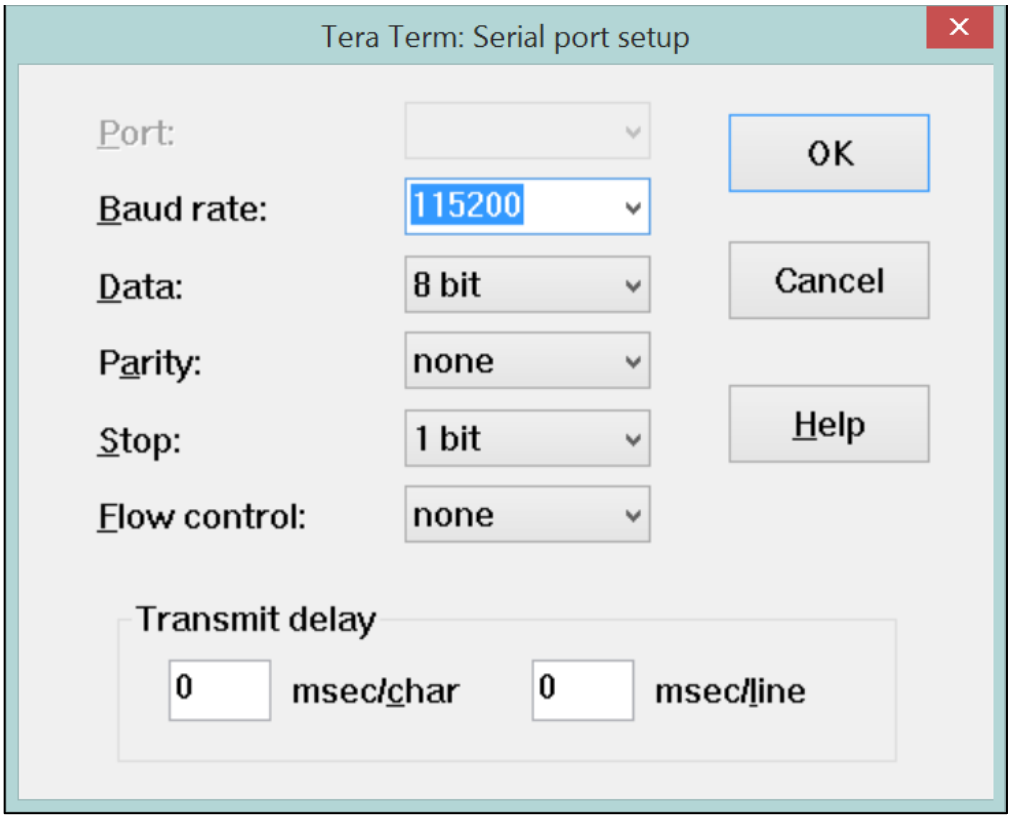
Coding (transmit): UTF-8

locale: american

CodePage: 65001

Figure 28: Terminal Settings for Teraterm

4. Next, click on Setup -> Serial port… In the dialog box that opens, select the Baud Rate as 115200 and Click OK.



Tera Term: Serial port setup

Port:

Baud rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow control: none

Transmit delay

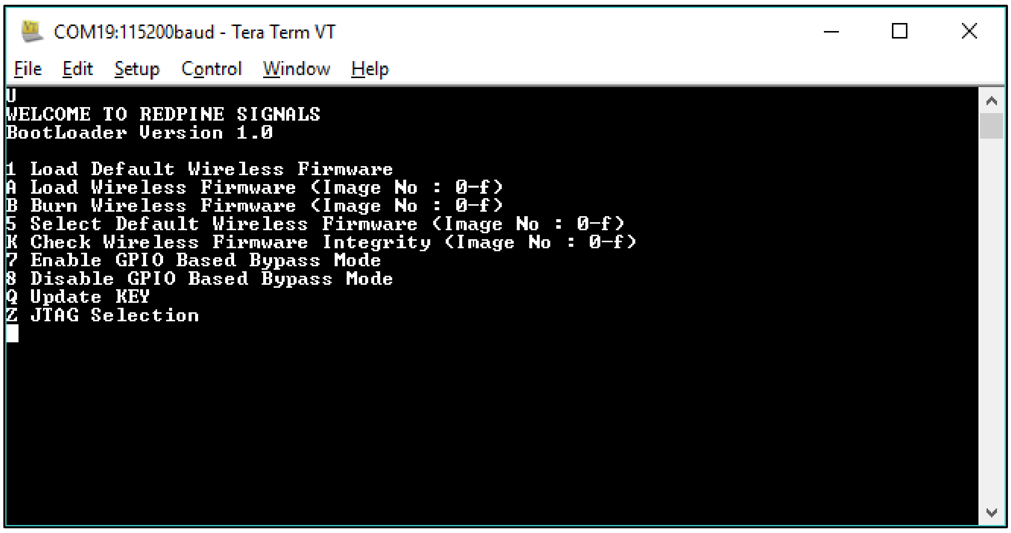
0 msec/char 0 msec/line

Figure 29: Serial Port Settings for Teraterm

5. Connect the EVB to the PC using the Micro A/B-type USB cable. Plugin the cable into the micro-USB port labeled "UART" on the EVB.

6. Click on File -> New connection… In the dialog box that opens, select the Serial option and select the COM Port from the drop-down menu. It is COM8 in the figure below. Click OK.

7. After the Automatic Baud Rate Detection timeout, you will see the Welcome message and available options on the Teraterm screen.

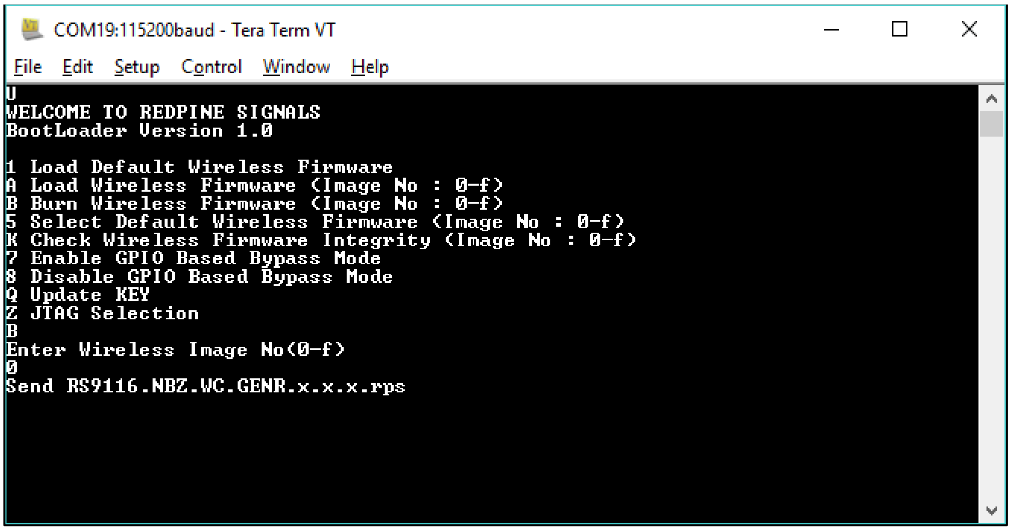


COM19:115200baud - Tera Term VT

```
U
WELCOME TO REDPINE SIGNALS
BootLoader Version 1.0

1 Load Default Wireless Firmware
A Load Wireless Firmware (Image No : 0-f)
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
```

Figure 30: Module Startup Messages

8. Hit 'B' to select Firmware Upgradation mode. You will be requested to send the Firmware file. For the EVK, the firmware file in the RS9116.NB0.WC.GENR.OSI.x.x.x\Firmware folder. Here, x.x.x is the release version.


COM19:115200baud - Tera Term VT
File Edit Setup Control Window Help

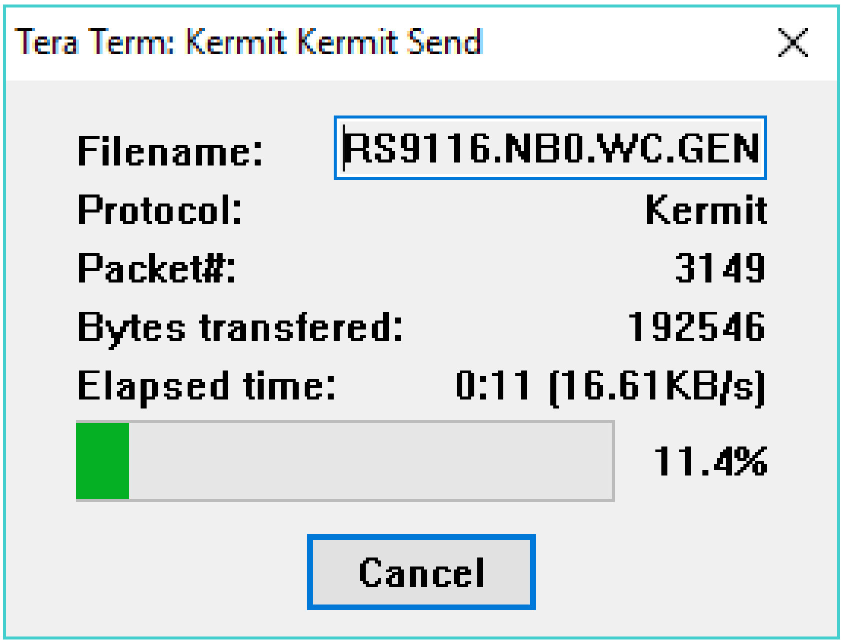
```
U
WELCOME TO REDPINE SIGNALS
BootLoader Version 1.0

1 Load Default Wireless Firmware
A Load Wireless Firmware (Image No : 0-f)
B Burn Wireless Firmware (Image No : 0-f)
5 Select Default Wireless Firmware (Image No : 0-f)
K Check Wireless Firmware Integrity (Image No : 0-f)
7 Enable GPIO Based Bypass Mode
8 Disable GPIO Based Bypass Mode
Q Update KEY
Z JTAG Selection
B
Enter Wireless Image No(0-f)
0
Send RS9116.NBZ.WC.GENR.x.x.x.rps
```

Figure 31: Request for Firmware File

9. Click on File -> Transfer -> Kermit -> Send…

10. In the dialog box that opens, navigate to the RS9116.NBZ.WC.GEN.OSI.x.x.x\Firmware folder and select the RS9116.NBZ.WC.GEN.OSI.x.x.x.rps file.

11. A dialog box will open, showing the transfer of the firmware file.



Filename: RS9116.NB0.WC.GEN
Protocol: Kermit
Packet#: 3149
Bytes transfered: 192546
Elapsed time: 0:11 (16.61KB/s)
11.4%

Figure 32: Firmware Transfer Progress

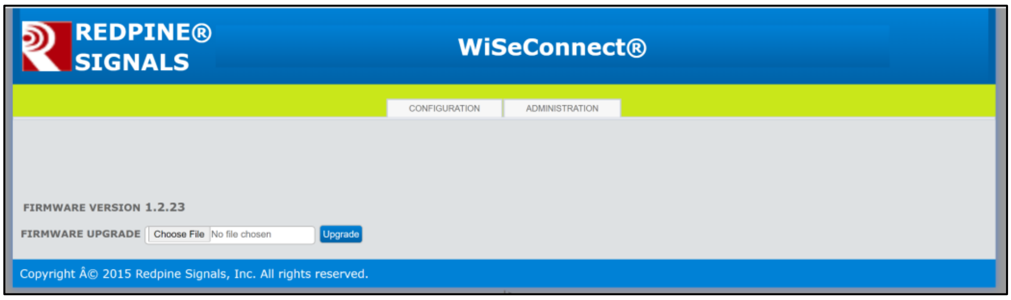
12. Once the firmware is transmitted to the module successfully, the module boots up with the updated firmware and requests the user to select the option.

13. You may continue to use the EVB without disconnecting it. If you wish to switch to Docklight from Teraterm, you can click on File -> Disconnect in Teraterm, open Docklight and hit 'F5' to start the communication from Docklight.

9.2 Firmware Upgrade over Wi-Fi

1. Module configured as an Access Point: Connect a Laptop that has the new firmware file (.rps extension) to the module.
2. Module configured as a Client and connected to an Access Point: Connect a Laptop which has the new firmware file (.rps extension) to the Access Point.
3. Ensure that the Laptop has an IP assigned.

4. Open the URL **http://<Module's IP address>**in the Laptop. For example, if the module was configured to have an IP of 192.168.0.30, then the URL is http://192.168.0.30. Make sure the browser in the laptop does not have any proxies enabled.
5. On the webpage that opens, click on the "ADMINISTRATION" tab.



FIRMWARE VERSION 1.2.23

FIRMWARE UPGRADE No file chosen

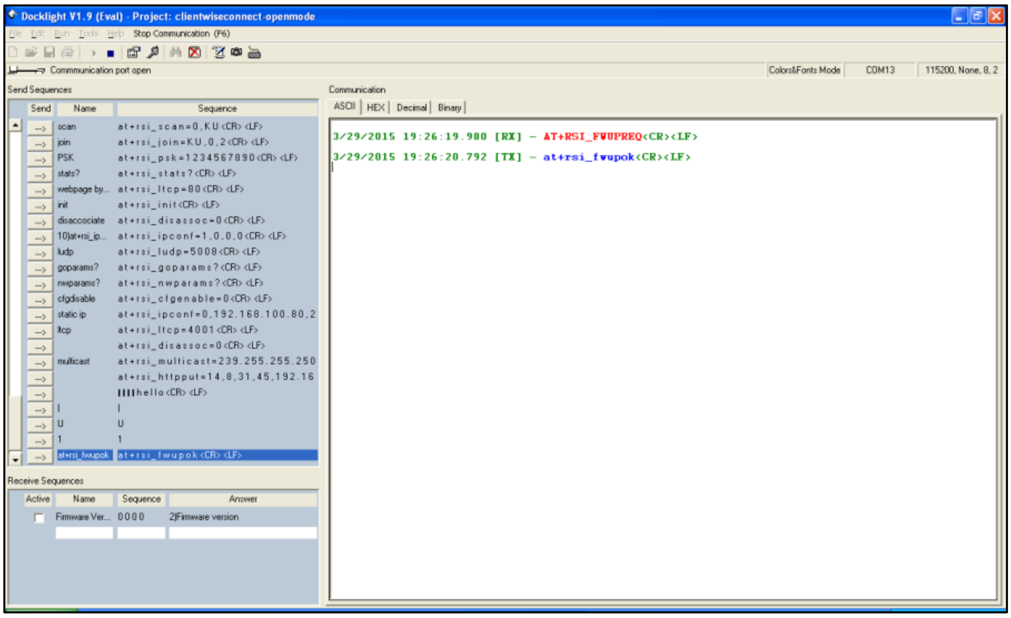
Copyright Â© 2015 Redpine Signals, Inc. All rights reserved.

Figure 33: ADMINISTRATION Tab

6. Click on "Browse" to navigate to the location of the firmware file (.rps extension), select the file and click "Open".

7. Next, click on "Upgrade".

8. The module sends a response (AT+RSI_FWUPREQ) to the Host PC to confirm the Firmware Upgrade, as shown in the figure below. The Host has to send the confirmation command (AT+RSI_FWUPOK) to start upgrading the firmware.


Docklight V1.9 (Eval) - Project: clientwiseconnect-openmode
File Edit Run Tools Help Stop Communication (F6)
Send Sequences
Receive Sequences
Communication
ASCII
HEX
Decimal
Binary

Commmunication port open

Colors&Fonts Mode | COM13 | 115200, None, 8, 2

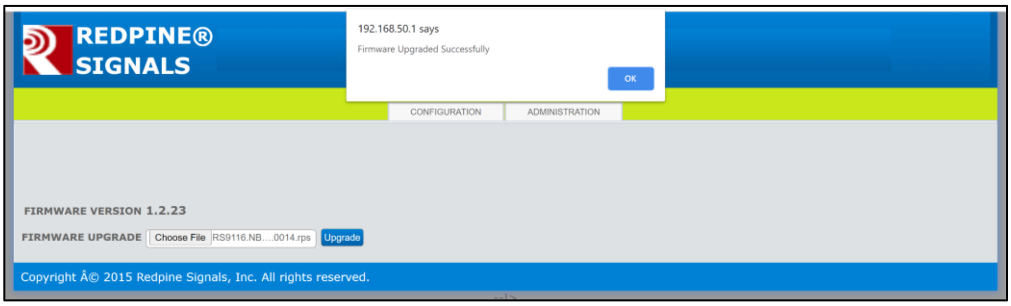
Send	Name	Sequence
--->	scan	at+rsi_scan=0,KU<CR><LF>
--->	join	at+rsi_join=KU,0,2<CR><LF>
--->	PSK	at+rsi_psk=1234567890<CR><LF>
--->	stats?	at+rsi_stats?<CR><LF>
--->	webpage by...	at+rsi_ltcp=80<CR><LF>
--->	init	at+rsi_init<CR><LF>
--->	disaccociate	at+rsi_disassoc=0<CR><LF>
--->	10)at+rsi_ip...	at+rsi_ipconf=1,0,0,0<CR><LF>
--->	ludp	at+rsi_ludp=5008<CR><LF>
--->	goparams?	at+rsi_goparams?<CR><LF>
--->	nwparams?	at+rsi_nwparams?<CR><LF>
--->	cfgdisable	at+rsi_cfgenable=0<CR><LF>
--->	static ip	at+rsi_ipconf=0,192.168.100.80,2
--->	ltcp	at+rsi_ltcp=4001<CR><LF>
--->		at+rsi_disassoc=0<CR><LF>
--->	multicast	at+rsi_multicast=239.255.255.250
--->		at+rsi_httpput=14,8,31,45,192.16
--->		IIIIhello<CR><LF>
--->	I	I
--->	U	U
--->	1	1
--->	at+rsi_fwupok	at+rsi_fwupok<CR><LF>

Active	Name	Sequence	Answer
□	Firmware Ver...	0000	2)Firmware version

```
3/29/2015 19:26:19.980 [RX] - AT+RSI_FWUPREQ<CR><LF>
3/29/2015 19:26:20.792 [TX] - at+rsi_fwupok<CR><LF>
```

Figure 34: Firmware Upgrade Confirmation

9. Once the up-gradation is done, a "Firmware Upgraded Successfully" message is displayed, as shown in the figure below.



192.168.50.1 says

Firmware Upgraded Successfully

FIRMWARE VERSION 1.2.23

FIRMWARE UPGRADE RS9116.NB....0014.rps

Copyright Â© 2015 Redpine Signals, Inc. All rights reserved.

Figure 35: Firmware Upgraded Successfully

9.3 Firmware Upgrade using OTAF(Over the AIR Firmware) Feature

Another method is to upgrade using the OTAF feature. In this method, users need to run a TCP server.

Details are provided in the "AN1282: RS9116W_Guide_for_SAPI_Application_Examples_vx.x.pdf "
from https://docs.silabs.com/rs9116

Please refer to the section "Over The Air Firmware Upgradation From Server example". Reference TCP server application for Linux is also provided in the example folder (Path: RS9116.NB0.WC.GENR.OSI.x.x.x\host\sapis\examples\wlan\otaf).

10 Appendix E_EVB Assembly Drawings

10.1 Base Board Assembly Drawings:

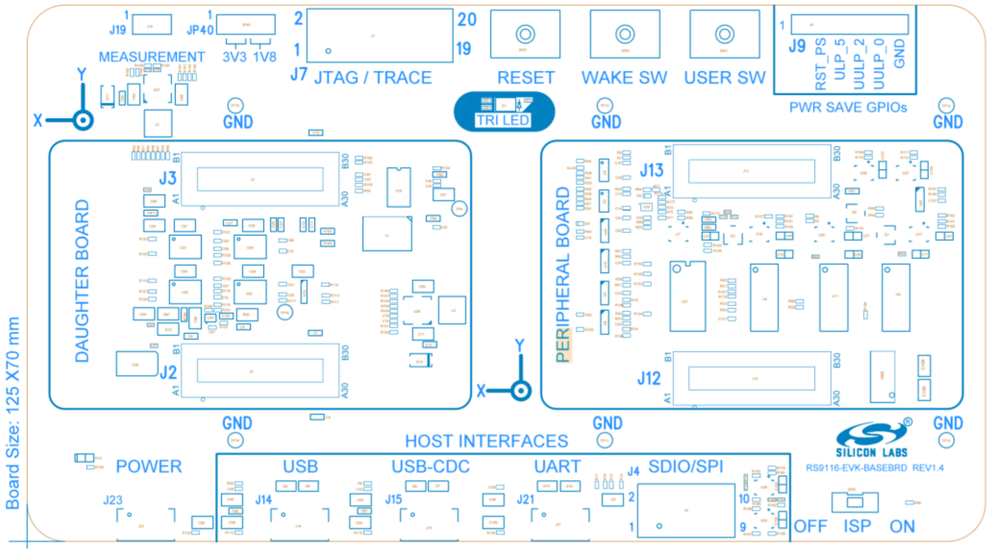


Figure 36: Base Board Assembly Drawings

10.2 QMS Daughter Board Assembly Drawings:

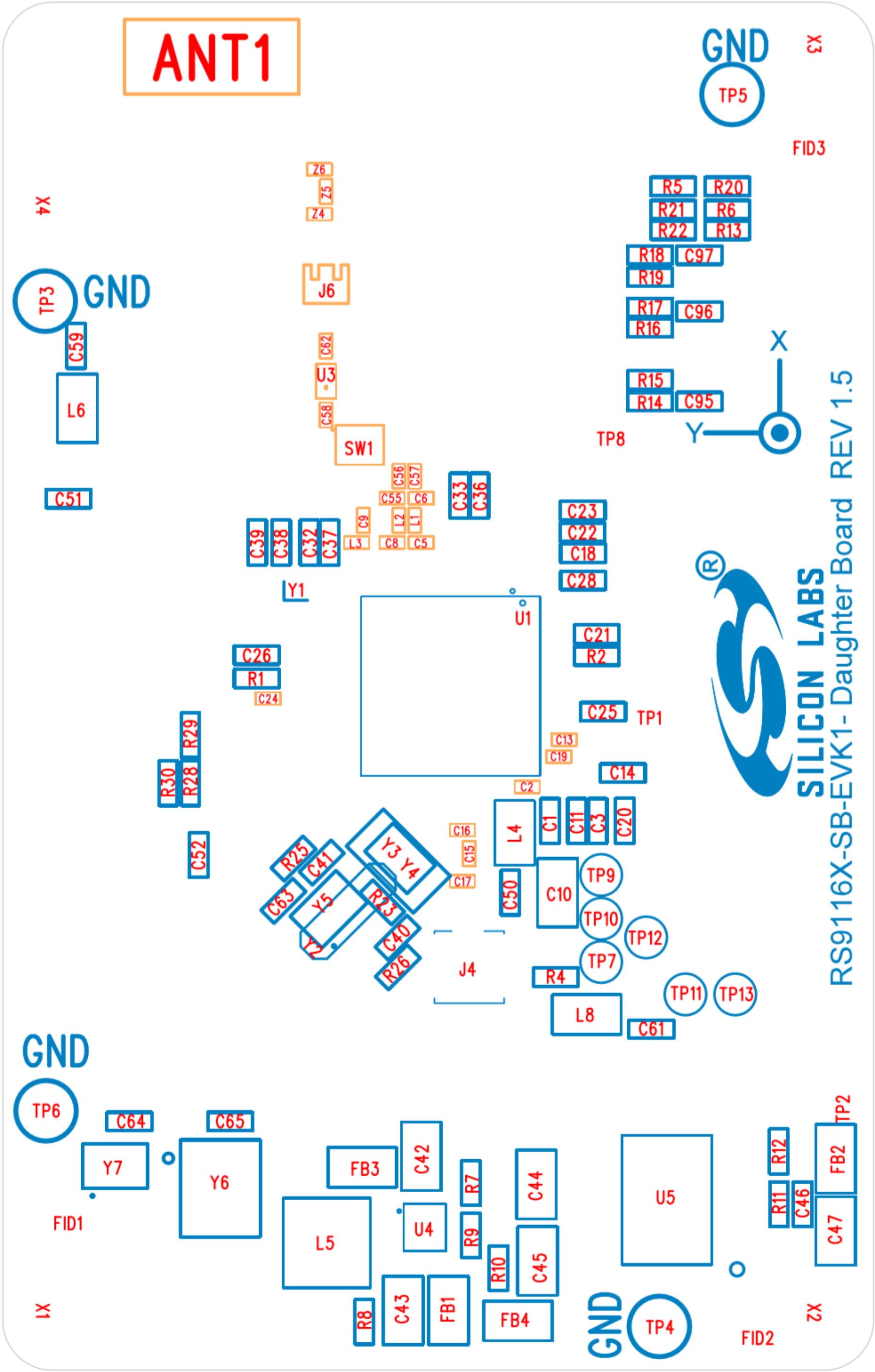


Figure 37: Daughter Board Assembly Drawing

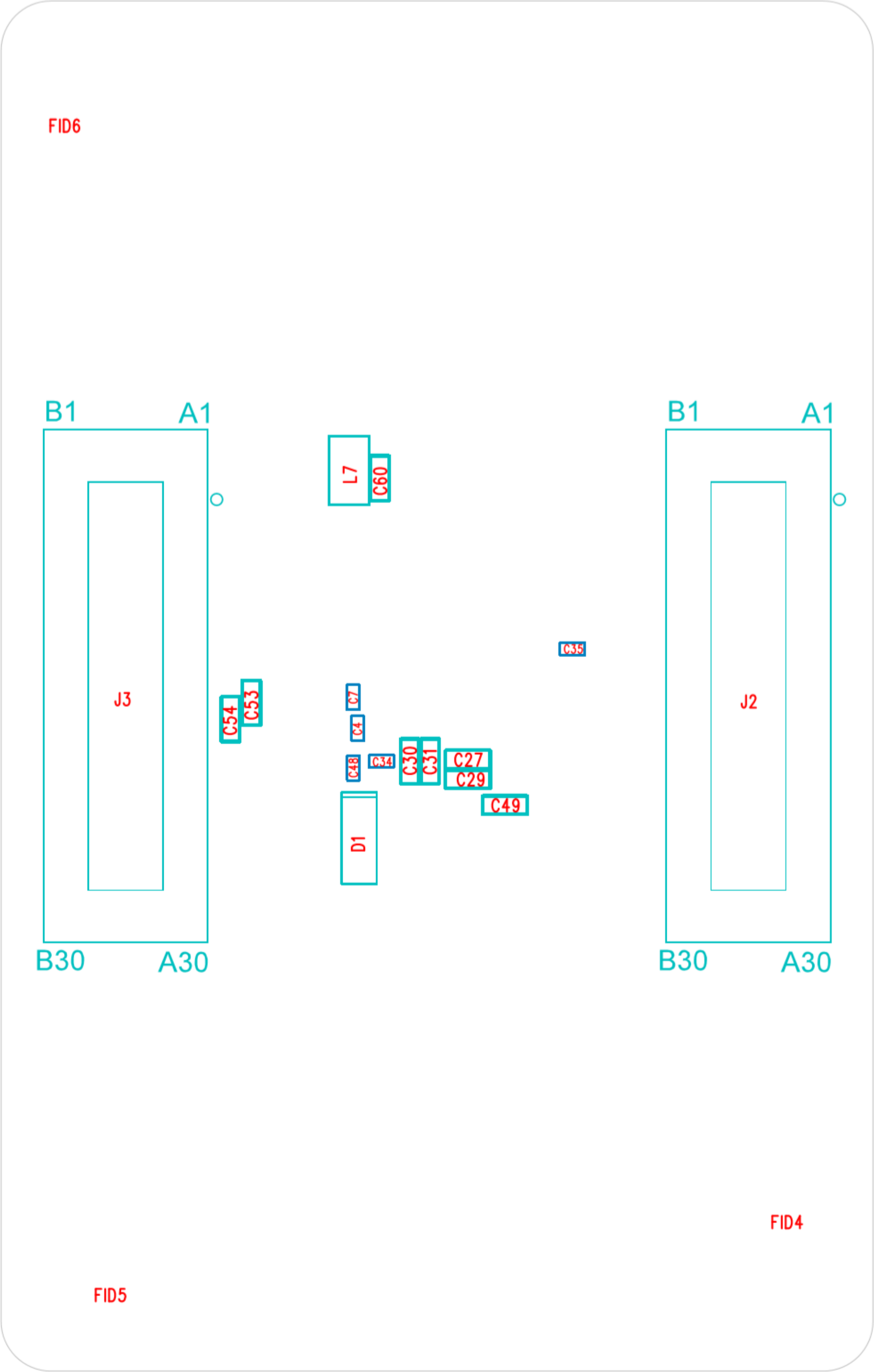


Figure 38: Daughter Board Assembly Drawing

10.3 CC1 Daughter Board Assembly Drawings:

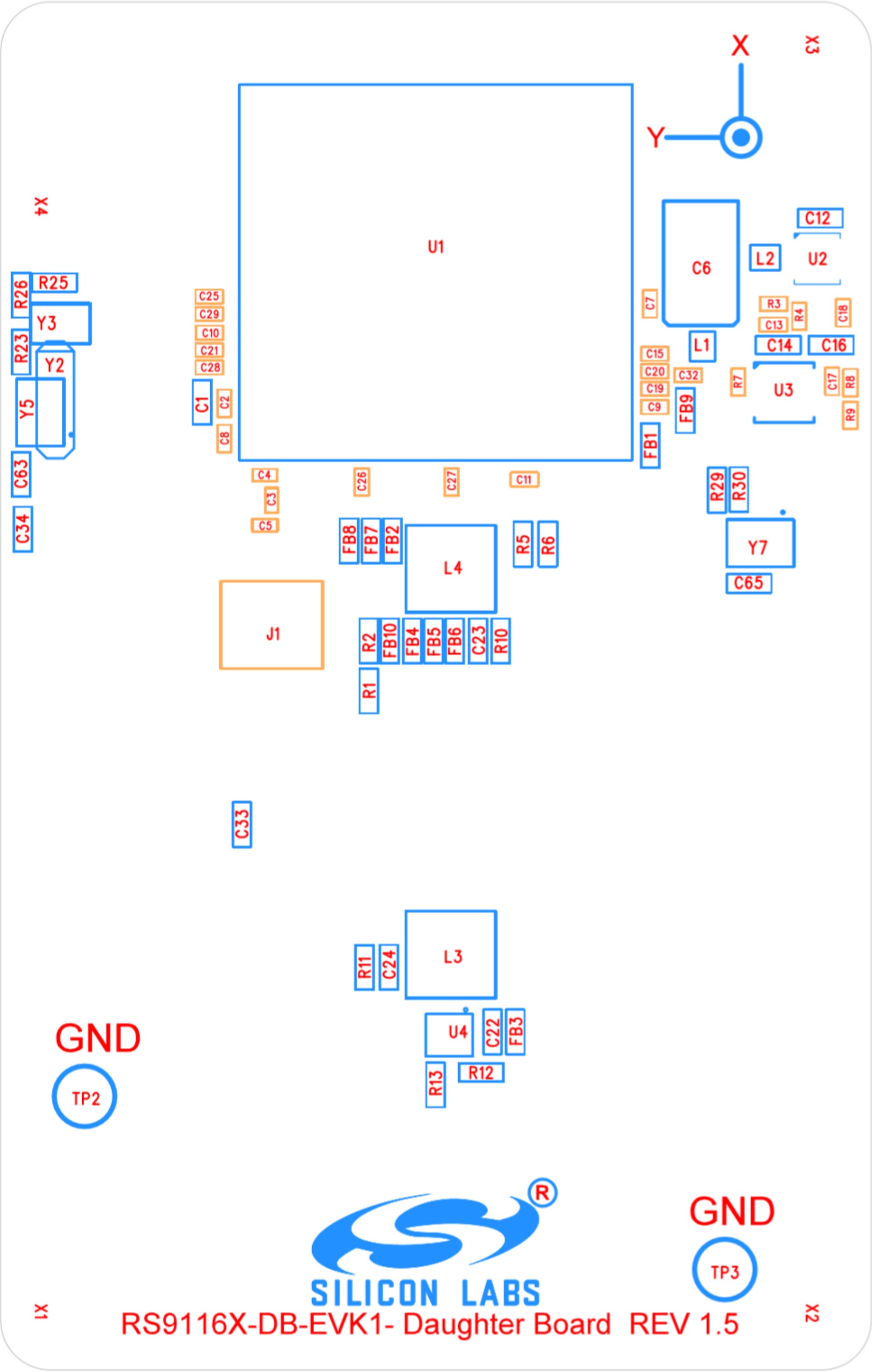


Figure 39: Daughter Board Assembly Drawing

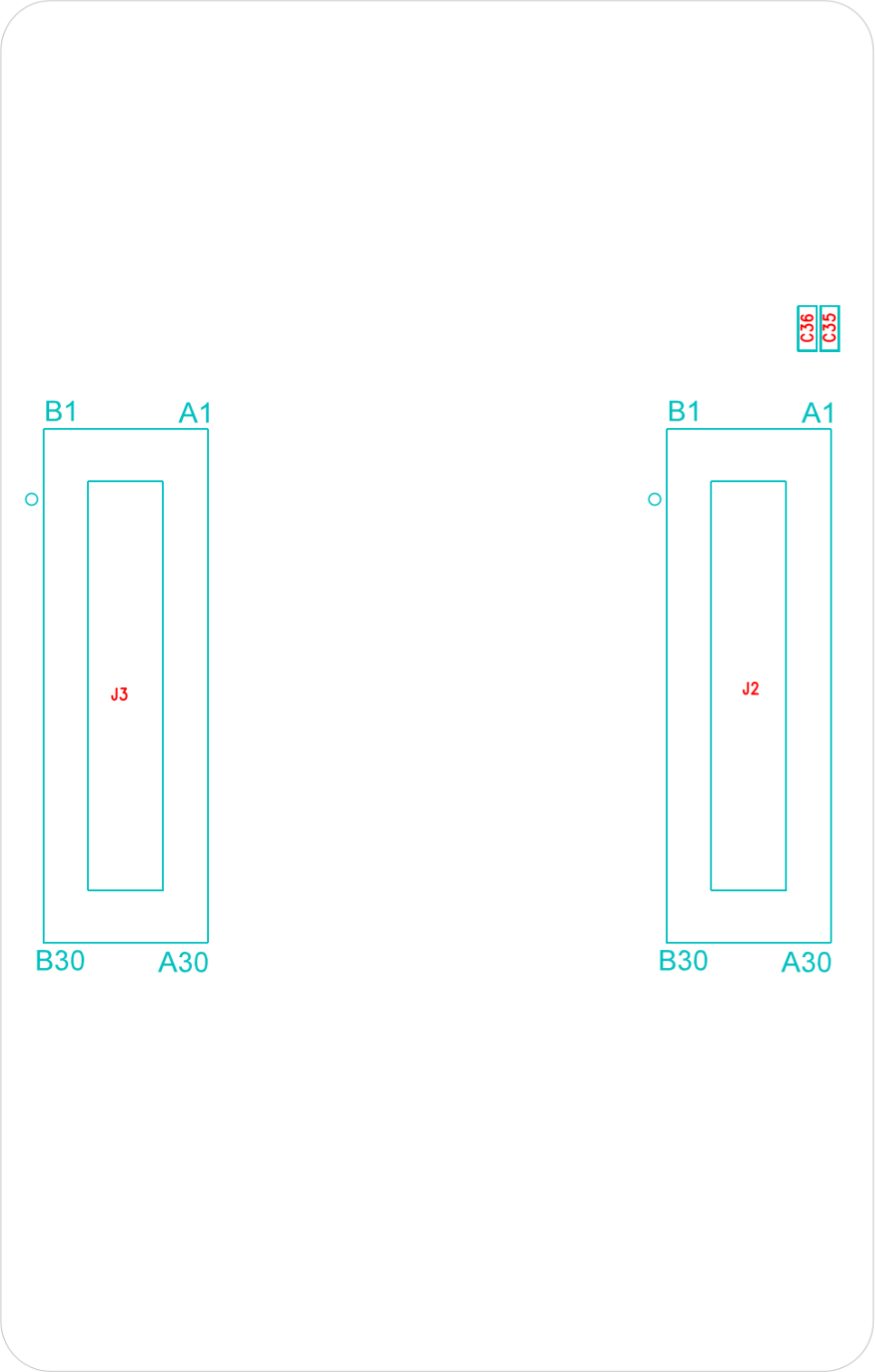


Figure 40: Daughter Board Assembly Drawing

10.4 B00 Daughter Board Assembly Drawings:

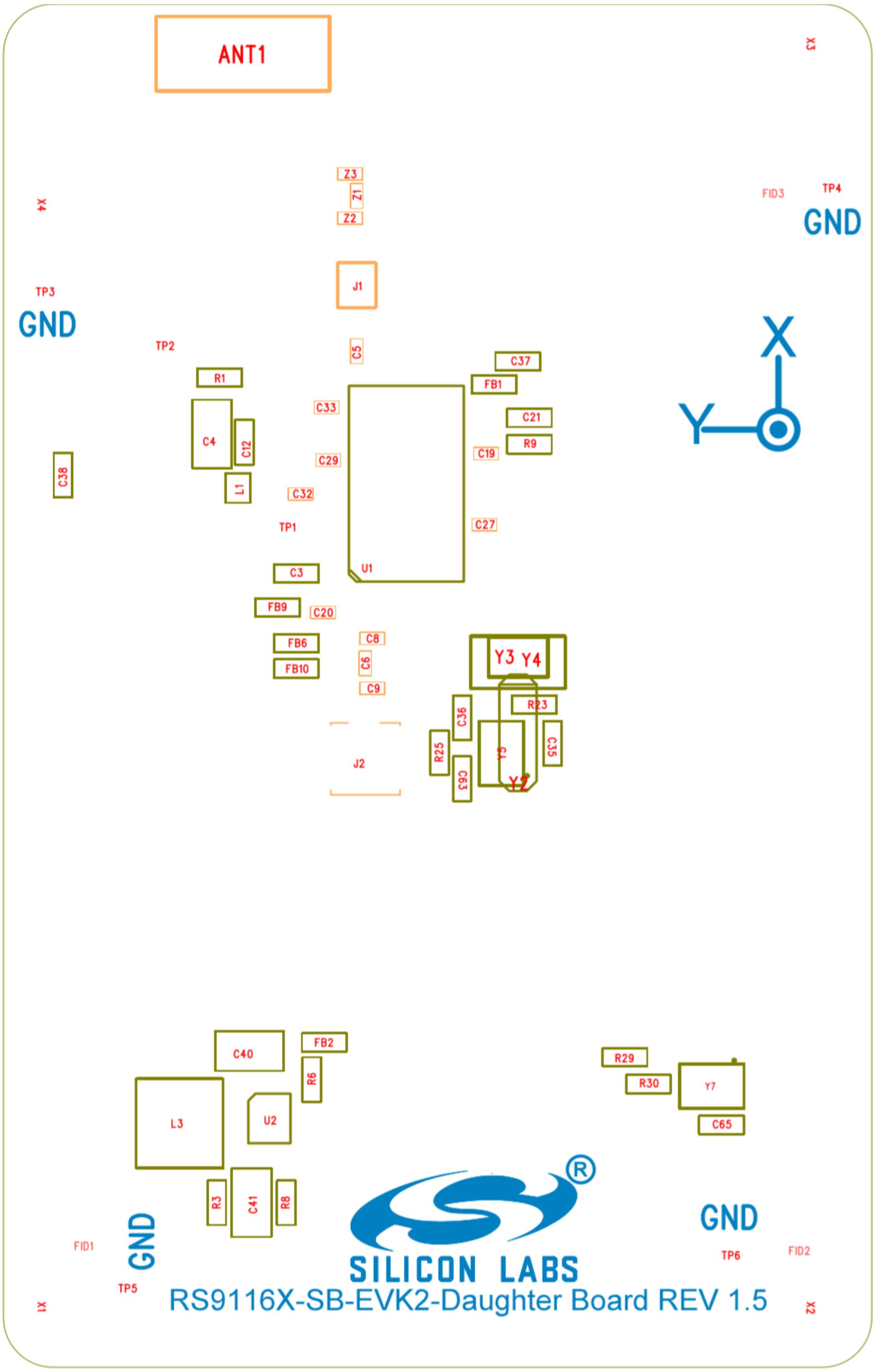


Figure 41: Daughter Board Assembly Drawing

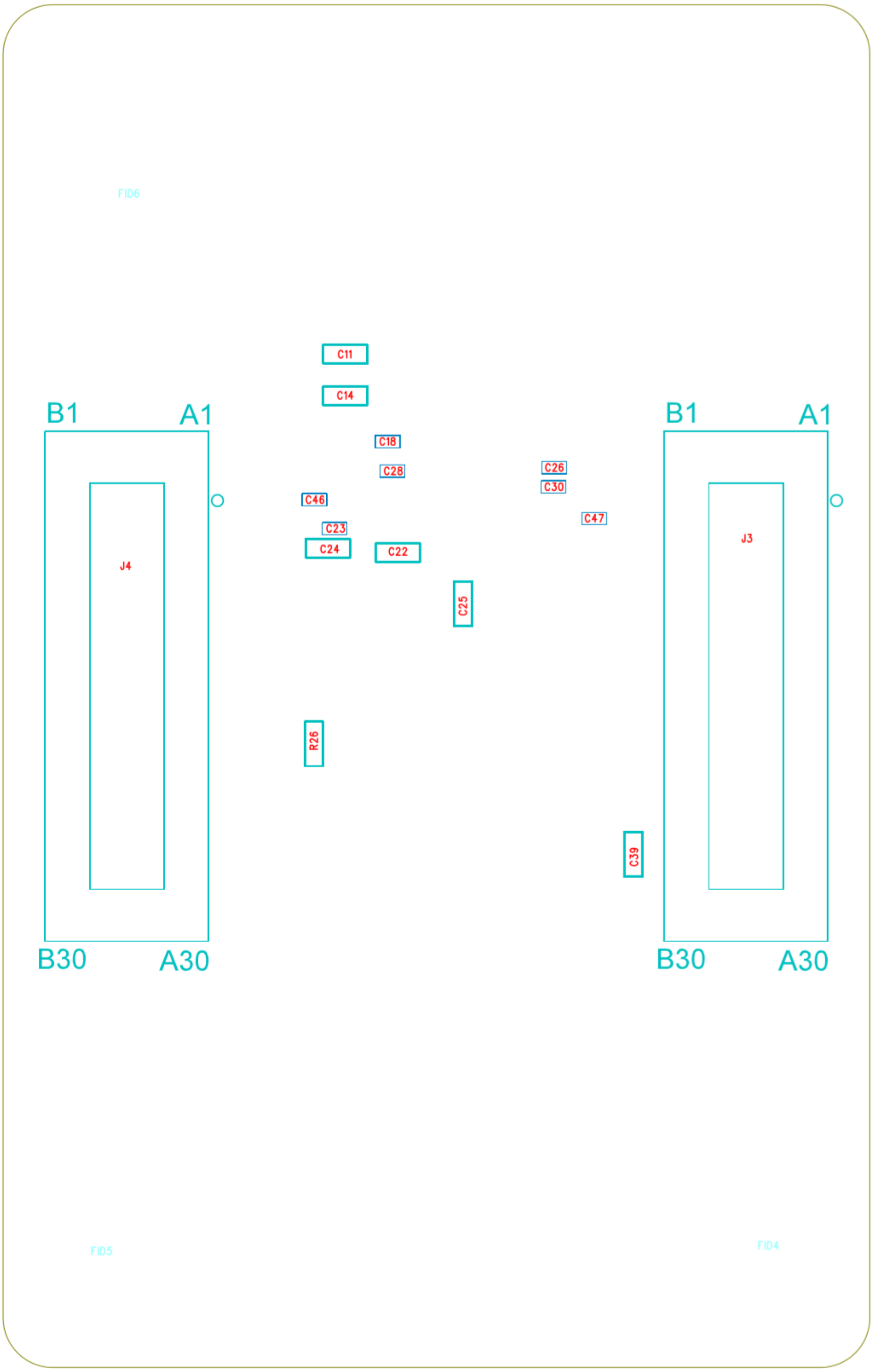
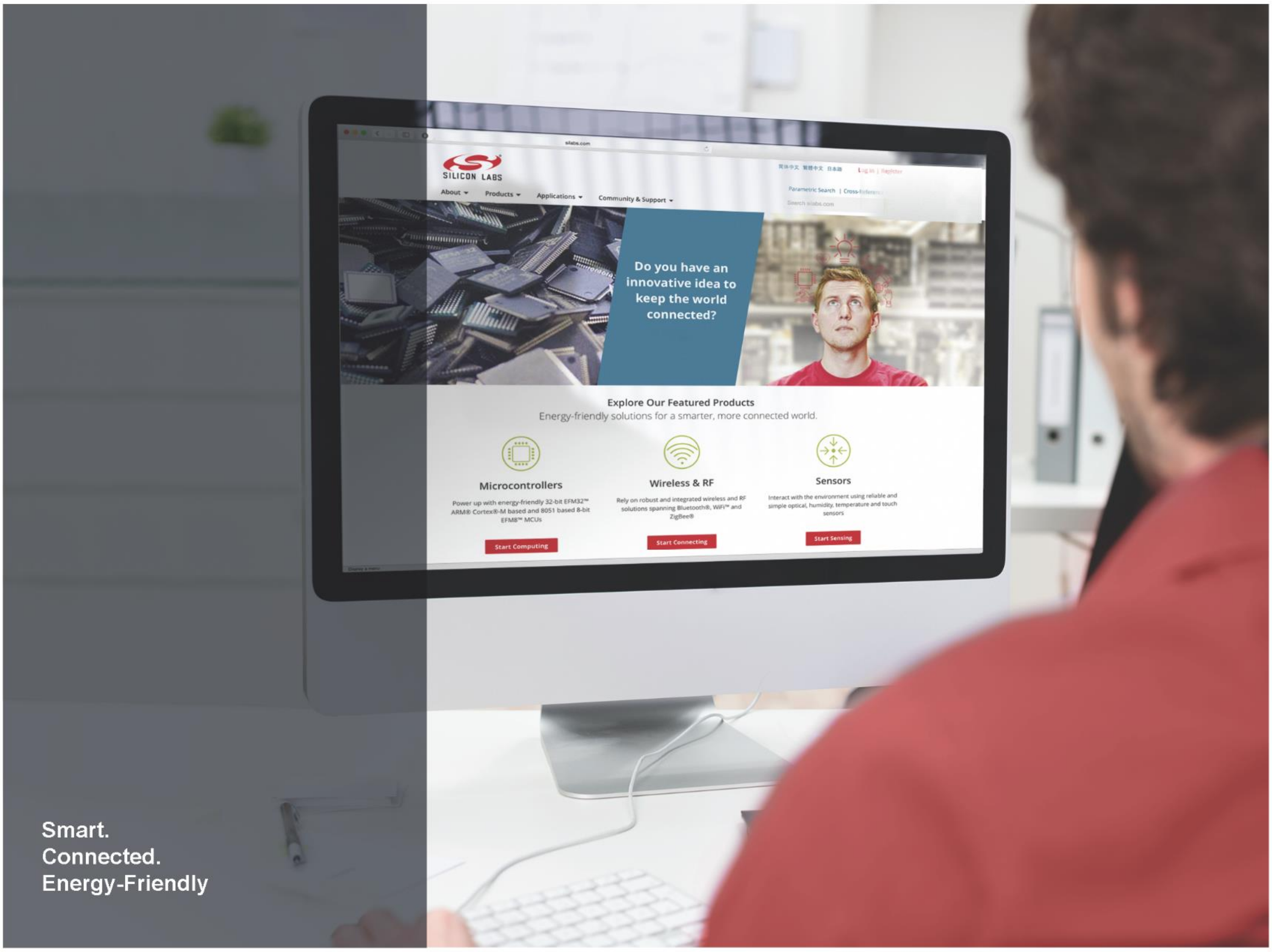


Figure 42: Daughter Board Assembly Drawing

11 Revision Report

Revision No.	Version No.	Date	Changes
1	1.0	May 2018	Include changes
2	1.1	June 2018	Include changes
3	1.2	Oct 2018	1. Corrected OpenKM path 2. Corrected Radius server path 3. DevCPP example update 4. Added details to run UART examples with TeraTerm Script
4	1.3	Jan 2019	1. Corrected figure 21. 2. Added the ABRD requirement for UART.
5	1.4	March 2019	1. Deleted the Zigbee section 2. SDIO related updates.
6	1.5	June 2019	Corrected wifiuser.pem path
7	1.6	May 2020	1. Folder paths updated as per new release package 2.Updated spell mistakes
8	1.7	Oct 2020	1.Added Note in the Hardware details section for Assembly drawings info for EVB 2. Added Appendix E_EVB Assembly Drawings page for the same. 3. Corrected some block diagrams. 4. Dev C++ related information removed. 5. Added FW TTL Scripts steps for execution. 6. Default ABRD is provided in the ttl scripts as default. 7.Updated the Website URL's with latest .


Do you have an innovative idea to keep the world connected?
Explore Our Featured Products
Energy-friendly solutions for a smarter, more connected world.
Microcontrollers
Wireless & RF
Sensors
Start Computing
Start Connecting
Start Sensing
Smart.
Connected.
Energy-Friendly

Products
www.silabs.com/products

Quality
www.silabs.com/quality

Support and Community
community.silabs.com

Disclaimer
Silicon Laboratories intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Laboratories products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Laboratories reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Laboratories shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products must not be used within any Life Support System without the specific written consent of Silicon Laboratories. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Laboratories products are generally not intended for military applications. Silicon Laboratories products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

Trademark Information
Silicon Laboratories Inc., Silicon Laboratories, Silicon Labs, SiLabs and the Silicon Labs logo, CMEMS®, EFM, EFM32, EFR, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZMac®, EZRadio®, EZRadioPRO®, DSPLL®, ISOmodem ®, Precision32®, ProSLIC®, SiPHY®, USBXpress® and others are trademarks or registered trademarks of Silicon Laboratories Inc. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. All other products or brand names mentioned herein are trademarks of their respective holders.

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701

http://www.silabs.com