RA4W1 Group

Bluetooth Mesh Startup Guide

Introduction

This document describes how to get started Bluetooth Mesh with Bluetooth Mesh Stack.

Bluetooth Mesh Stack is the software library to build a mesh network that is compliant with Bluetooth Mesh Networking Specification and to perform many-to-many wireless communication.

Target Device

RA4W1 Group

Related Documents

The following documents are published on Renesas website.

Document Title	Document No.
RA4W1 Group User's Manual: Hardware	R01UH0883
RA Flexible Software Package Documentation	–
RA4W1 Group Bluetooth Mesh Startup Guide	R01AN5847 This document
RA4W1 Group Bluetooth Mesh sample application Application Note	R01AN5848
RA4W1 Group Bluetooth Mesh Development Guide	R01AN5849
RA4W1 Group EK-RA4W1 Quick Start Guide	R20QS0015
RA4W1 Group EK-RA4W1 User's Manual	R20UT4683

Contents

1. Features

This chapter introduces the features of Bluetooth Mesh Network implemented by the Bluetooth Mesh Stack software.

1.1 Communication Topology

Communication topologies provided by Bluetooth Low Energy technology are Point-to-Point and Broadcast. Bluetooth Mesh Stack software uses the Bluetooth Low Energy technology and build a Mesh network. Figure 1-1 shows the communication topologies.

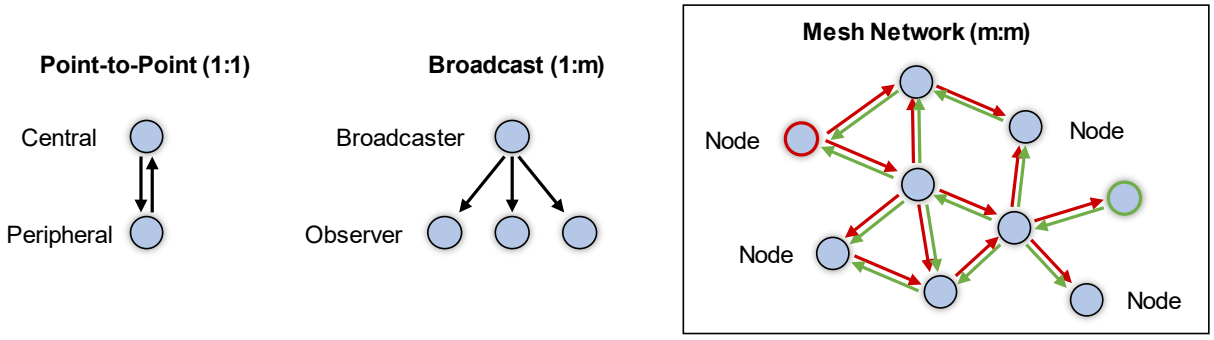

Figure 1-1 Communication Topologies

- **Point-to-Point**

  In a Point-to-Point topology, Central communicates with Peripheral bidirectionally. For example, central device is a smartphone and peripheral device is a fitness tracker respectively. Smartphone informs the tracker that a user starts exercise and then the tracker sends measurement data such as user's exercise intensity.

- **Broadcast**

  In a Broadcast topology, Broadcaster broadcasts data to unspecified Observers, while each Observer decides whether to use received data. For example, Broadcaster device is a beacon for shopping coupon and Observer device is a smartphone respectively. Beacon sends a coupon ID and then the smartphone gets a coupon corresponding the coupon ID via internet.

- **Mesh Network**

  In a Mesh Network topology, many Nodes communicate with each other bidirectionally. Each node can send messages in any timing. Moreover, a node can communicate with the nodes in a place where the message originator node cannot communicate directly, because neighbor nodes relay the message. An example of use-case is a building automation system composed of lightings, air-conditioners, control panel, and smartphones. Building administrator controls whole lightings and air-conditioners of a floor, and building users adjust operations of the lightings and air-conditioner in a room.

1.2 Mesh Network Operation

Operation of Bluetooth Mesh Network is shown below. Also, a network implementing this mesh operation is defined as a **Managed-Flood-based Mesh Network**.

Figure 1-2 shows the operation of nodes making a mesh network. One node (SRC in the figure) sends a message, and neighbor nodes relay the message one after another. The message spreads in whole network and finally arrives at destination node (DST in the figure).

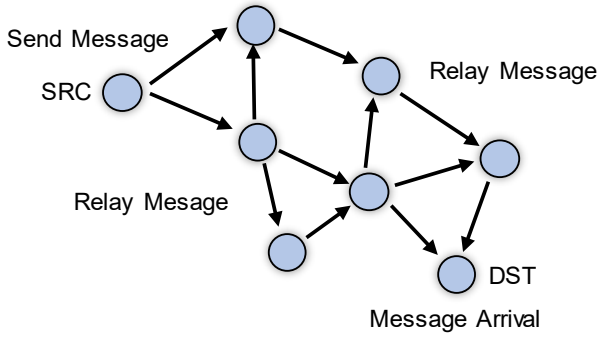

Figure 1-2 Mesh Network Operation

Moreover, nodes use the two method not to relay each message unlimitedly.

- **Message Cache method**

  When receiving a message, each node relays it and caches it in own list. After that, when receiving the same message again, the node does not relay it.

- **Time to Live method**

  Before sending a message, each node sets limitation of the number of relaying times to TTL (Time to Live) value in the message. Maximum number that can be set is 127. Other nodes decrement the TTL value by 1 and relays the message. Message which TTL value is 0 is not relayed.

1.3 Lifecycle of a Mesh Device

Figure 1-3 shows typical lifecycle of a device supporting Bluetooth Mesh.

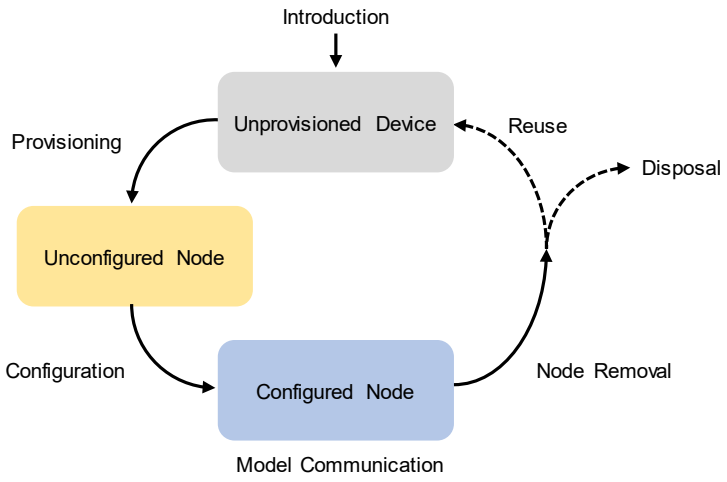

Figure 1-3 Mesh Network Operation

A device supporting Bluetooth Mesh is authenticated and receives Provisioning Data such as a Network Key and Unicast Addresses of each element by Provisioning process.

After Provisioning, device referred to as a node receives configuration required for model operations such as Application Keys, Publish Address, and Subscription Addresses by Configuration process.

After Configuration, the node can communicate with other nodes with models. Also, configuration of the node may be changed by performing Configuration process again.

When there can be a security risk related to Network Keys or/and Application Keys, Configuration Client refreshes these encryption keys. Moreover, unnecessary nodes have risks such as leakage of currently used encryption keys, so the Configuration adds unnecessary nodes into blacklist. Blacklisted nodes cannot receive new encryption keys.

Configuration Client can remove unnecessary node to from a network by Node Removal Procedure. Device removed from a network may be reused or discarded.

2. Overview

2.1 Bluetooth Mesh Demonstration

The sample program included in "Bluetooth Mesh sample application Application Note" (R01AN5848) performs the following four demonstration phases.

- Demo Phase1: Provisioning
- Demo Phase2: Configuration
- Demo Phase3: Model Communication
- Demo Phase4: Node Removal

To perform the demonstration, Mesh Mobile Application (hereinafter referred to as "Mesh Mobile") which works on a smart phone is included in this document. The Mesh Mobile will perform as Provisioner and Configuration Client.

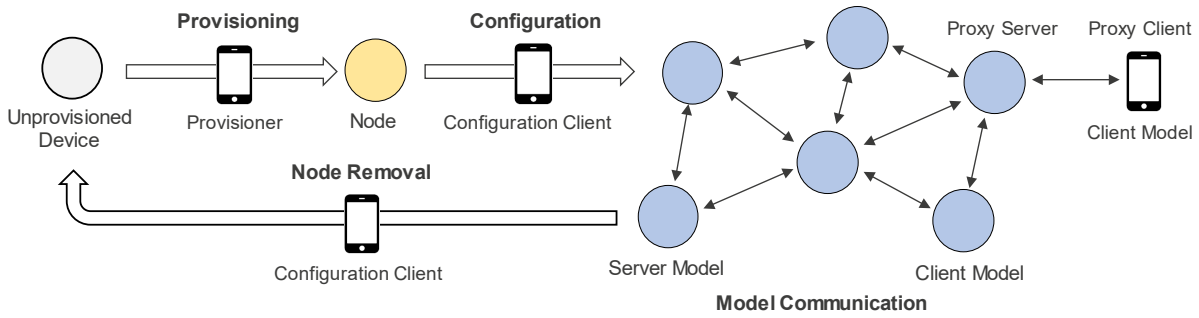

Figure 2-1 Overview of Mesh Demonstration

2.1.1 Demo-Phase1: Provisioning

Each Unprovisioned Device needs to be provisioned by a Provisioner. Provisioning is the process of authenticating and providing basic information such as Unicast Addresses and a Network Key to transmit or receive messages in a mesh network as a node. Also, Provisioner is typically mobile computing device such as smart phone.

The sample program works as a Unprovisioned Device (Provisioning Server). After power on, the sample program starts transmitting Unprovisioned Device beacon and connectable advertising alternately to be discovered by a Provisioner.

On the other hand, Mesh Mobile Application works as a Provisioner (Provisioning Client) and performs provisioning by receiving a connectable advertising.

2.1.2 Phase2: Configuration

After provisioned, provisioned device is called a Node. Configuration Client distributes configuration for mesh model communication such as Application Keys, Publish Address and Subscription List to each Node which works as Configuration Server. Also, Configuration Client is typically a smart phone or other mobile computing device.

The sample program works as a Configuration Server. After Provisioning, the sample program transmits Connectable Advertising to connect to Configuration Client.

On the other hand, Mesh Mobile Application works as a Configuration Client and performs configuration by receiving a connectable advertising.

2.1.3 Phase3: Model Communication

After Configuration, each node encrypts messages with the Application Key and sends them to the Publish Address. Also, it receives the message sent to the address in the Subscription List and decrypts it with the Application Key.

Original Vendor Server and Vendor Client as well as Generic OnOff Server and Generic OnOff Client are implemented in the sample program.

When a switch (SW1) on EK-RA4W1 is pushed, Generic OnOff Client sends Generic OnOff Set Unacknowledged message that includes value representing either On or Off. When receiving the message, Generic OnOff Server controls a LED on EK-RA4W1 in accordance with the value included in the message.

When character string is input to console on PC connected to EK-RA4W1, Vendor Client sends Vendor Set Unacknowledged message that includes the character string. When receiving the message, Vendor Server Vendor Client outputs the character string included in the message to console on PC.

Mesh Mobile Application can work as Generic OnOff Client and Vendor Client and send messages. It connects to a Proxy node to transmit and receive messages. Proxy node forwards massages to neighbor nodes, and each node relays messages, then messages spread in the mesh network.

2.1.4 Phase4: Node Removal

Configuration Clien can remove a node from a mesh network by sending Config Node Reset message.

When receiving a Config Node Reset message, the sample program reset its configuration information and perform Provisioning again.

3. Hardware Requirement

"Bluetooth Mesh sample application Application Note" (R01AN5848) includes the sample program that works on the following EK-RA4W1. It is recommended to use two or more boards for developing applications.

3.1 EK-RA4W1

EK-RA4W1 can be used for developing applications using Bluetooth Mesh Stack. It has on-board debugger (J-Link OB), so you can develop software without external emulator.

For more information regarding EK-RA4W1, refer to "RA4W1 Group EK-RA4W1 Quick Start Guide" (R20QS0015) and "RA4W1 Group EK-RA4W1 User's Manual" (R20UT4683).

3.2 Smart Phone or Mobile Computing Device

An Android or iOS smartphone capable of Bluetooth Low Energy Communication is required to run the Mesh Mobile Application included in this document. Typically, Mobile Computing Device such as Smart Phone is used as a Provisioner and Configuration Client.

The following versions of devices have been confirmed to work.

- Android: 12
- iOS: 14.7.1

4. Software Requirement

4.1 Bluetooth Mesh Stack

Bluetooth Mesh Stack (hereinafter referred to as "Mesh Stack") provides applications with the Bluetooth Mesh Networking features for many-to-many wireless communication in a mesh network.

Mesh Stack is provided as a FSP. And, Sample programs are included in "Bluetooth Mesh sample application Application Note" (R01AN5848).

4.2 Bluetooth Low Energy Protocol Stack

Mesh Stack requires the Bluetooth Low Energy Protocol Stack to use Bluetooth Low Energy technology.

Bluetooth Low Energy Protocol Stack is provided as a FSP.

4.3 Mesh Mobile Application

Bluetooth Mesh Mobile Application (hereinafter referred to as "Mesh Mobile") is a sample application for demonstration and works on Android and iOS. You can get Mesh Mobile application from following link. Install the application to your device.

For Android: https://play.google.com/store/apps/details?id=com.renesas.meshmobile

For iOS: https://apps.apple.com/app/renesas-meshmobile/id1641877699

This document includes Mesh Mobile application package (*.apk), too. Install the application package according to following procedures.

NOTE: Application for Android only is included in this document. If you will use iOS device, build and install the application in accordance with "\mesh_mobile\mesh_mobile_guide.pdf" included this document.

NOTE: Mesh Mobile for Android requires some permissions; Location, Nearby devices, and Storage.

1. Copy the following package file from PC to Android via USB.

   `\mesh_mobile\app-debug.apk`

2. Execute the package file using any file manager application on Android.

About Mesh Mobile application for iOS, refer to section 4.5.2

4.4 Tool required for writing sample program

Table 4-1 shows a tool required for writing the sample program included in "Bluetooth Mesh sample application Application Note" (R01AN5848) to EK-RA4W1.

Table 4-1 Tool

Software	Version	Description
SEGGER J-Flash Lite	V6.86 or later	SEGGER J-Flash Lite (hereinafter referred to as "J-Flash Lite") is a tool for writing firmware to the on-chip flash memory of RA4W1. The EK-RA4W1 has an on-board debugger (J-Link OB), therefore it is not necessary to prepare an emulator.

4.5 Third-party Software

4.5.1 Serial Terminal Emulator

The sample program sends log messages over UART. Serial terminal emulator that supports CSI (Control Sequence Indicator) of ANSI escape sequence can be used for checking log message.

Tera Term

Serial port configurations to get log messages from the sample program are following.

Table 4-2 Serial Port Setting

Item	Setting
Baud rate	115200 bps
Data	8 bits
Parity	none
Stop	1 bit
Flow Control	none

Refer to section 6.1 about example of log massages.

4.5.2 Development Tools required for building Mesh Mobile

The following development tools are required for building Mesh Mobile. You can get them from the internet. Regarding how to build and install Mesh Mobile, refer to "\mesh_mobile\mesh_mobile_guide.pdf" included this document.

npm (Node Package Manager) included in Node.js

Python

Capacitor and Ionic framework

Android Studio, for building the Mesh Mobile for Android

Xcode, for building the Mesh Mobile for iOS

NOTE: Xcode works on Mac PC only. To download this, Apple ID is required. Moreover, to develop the iOS App products, paid license is required.

Apple Developer Program, for distributing Apps via App Store
Apple Developer Enterprise Program, for In-house Apps

5. Demonstration

This chapter describes how to operate the sample program and Mesh Mobile for mesh demonstration. It is recommended to use at least two EK-RA4W1 for this demonstration; one works as a Client and the other works as a Server.

Write firmware to EK-RA4W1 by using the J-Flash Lite. As for how to write, refer to "RA4W1 Group EK-RA4W1 Quick Start Guide" (R20QS0015). Firmware for demonstration is included in "Bluetooth Mesh sample application Application Note" (R01AN5848). Binary files for Server and Client are the followings.

```
ekra4w1_mesh_client_baremetal.srec
ekra4w1_mesh_server_baremetal.srec
```

5.1 Phase1: Provisioning

To start demonstration, power on all EK-RA4W1 and launch the Mesh Mobile.

NOTE: Mesh Mobile for Android requires some permissions; Location, Nearby devices, and Storage.

NOTE: If SCAN operation fails on Mesh Mobile for Android, remove the permissions above once and then set the permissions again.

Repeat the following steps to provision all EK-RA4W1.

1. To start searching Unprovisioned Devices, move to PROVISION tab and tap SCAN button.
2. Select any device in result of searching to provision it.
3. Establishing a connection and provisioning are performed.
4. When the device supports OOB Public Key and/or any of the Authentication method, the Mesh Mobile shows a screen to select whether to use OOB Public Key and select any of Authentication method. For simplicity of procedure in this demo, check "No OOB Public Key is used" and "No OOB Authentication is used", and tap PROVISIONING START button.

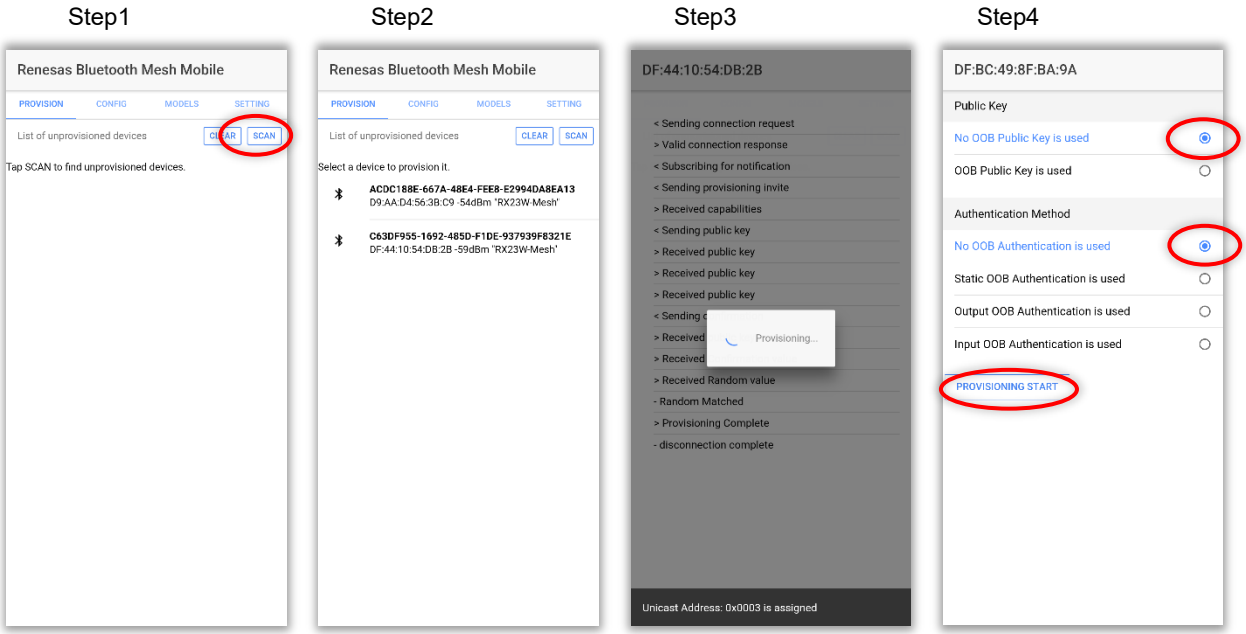

Figure 5-1 Provisioning

5.2 Phase2: Configuration

After all EK-RA4W1 are provisioned, repeat the following steps to configure all EK-RA4W1.

5.2.1 When selecting Demo group

1. To start searching nodes, move to CONFIG tab and tap SCAN button.
2. Connectable nodes are displayed in green. To connect and perform Configuration, select any node displayed in green.

   NOTE: Node suspends Connectable Advertising transmission after 60seconds. If device to be configured is not displayed in green, long-press the SW1 of EK-RA4W1 longer than 2seconds to resume Connectable Advertising transmission.
3. After Composition Data is displayed, move to CONFIGURATION tab.

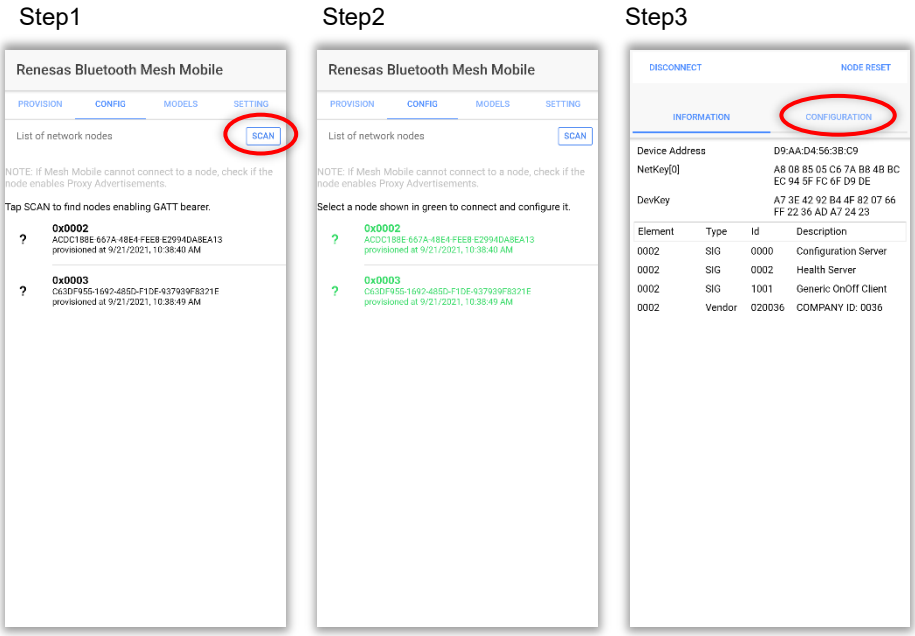

Figure 5-2 Configuration (1/2)

4. In the CONFIGURATION tab, configure to enable Relay, Proxy, and Friend and register "Demo" Group.
5. Tap APPLY button.
6. After Configured, tap DISCONNECT button.

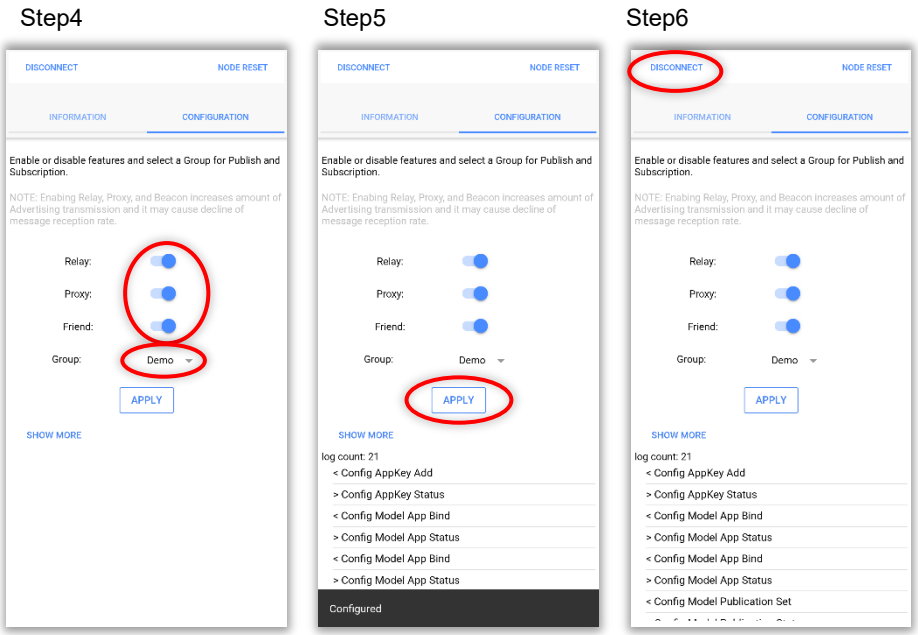

Figure 5-3 Configuration (2/2)

5.2.2 When adding any group

Group selected by Configuration is used when the application makes a group to operate multiple nodes. Any group can be added by the following steps.

1. Move to MODELS tab and tap ADDGROUP button.
2. In the Add Group dialog, enter any group name like a "Kitchen".
3. Check the group is added.

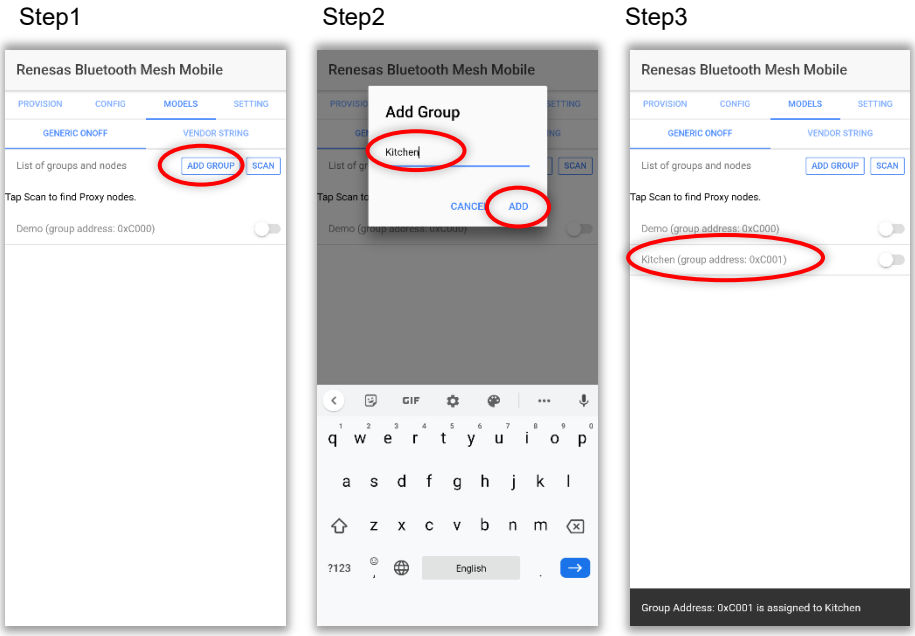

Figure 5-4 Add Group

5.3 Phase3: Model Communication

After EK-RA4W1 are configured, Mesh Mobile and EK-RA4W1 can send model messages. First, follow the steps below to establish a Proxy connection between Mesh Mobile and one of EK-RA4W1. Mesh Mobile sends messages to any nodes over the connected Proxy node.

1. To start searching Proxy Nodes, move to MODELS tab and tap SCAN button.
2. To connect a Proxy node, select any node displayed in green. After a connection is established, node is displayed in blue.
3. Tapping the node displayed in blue can disconnect a connection.

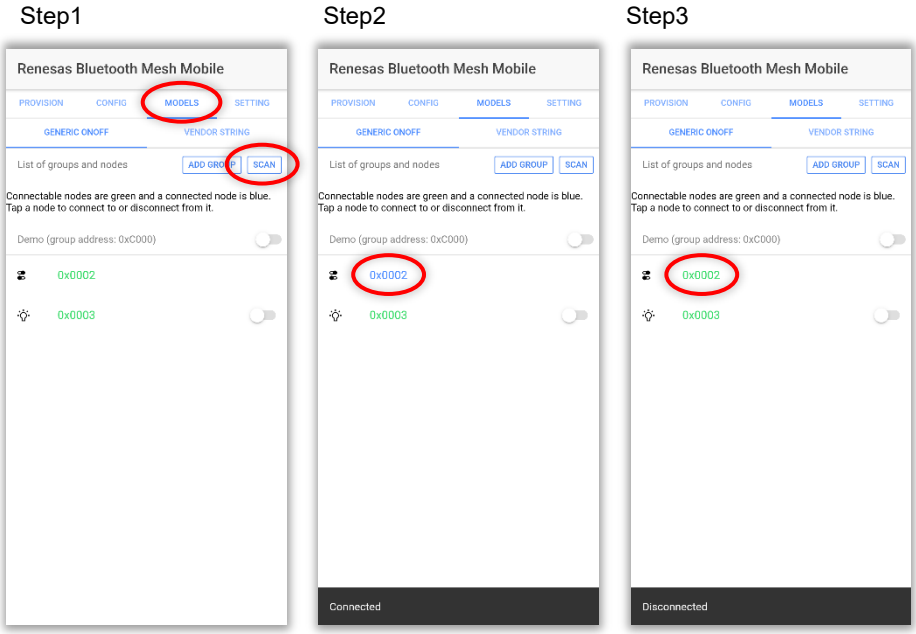

Figure 5-5 Proxy Connection

5.3.1 Generic OnOff State Control by Mesh Mobile

1. In the GENERIC ONOFF of the MODELS tab, switch a toggle button of the group repeatedly.
   You can see that LEDs of all EK-RA4W1 working as Generic OnOff Server follow the Generic OnOff SET messages received.

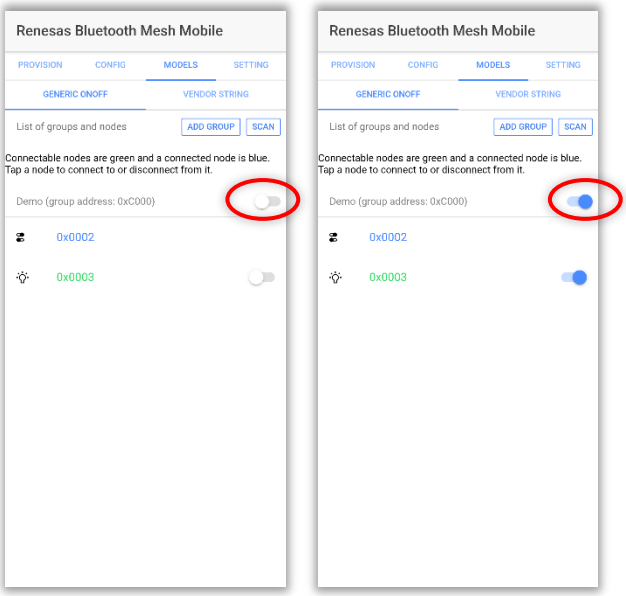

Figure 5-6 Publication of Generic OnOff SET Messages to Unicast Address

2. In the GENERIC ONOFF tab of the MODELS tab, switch a toggle button of any EK-RA4W1 repeatedly.
   You can see that a LED of the EK-RA4W1 working as Generic OnOff Server follows the Generic OnOff SET messages received.

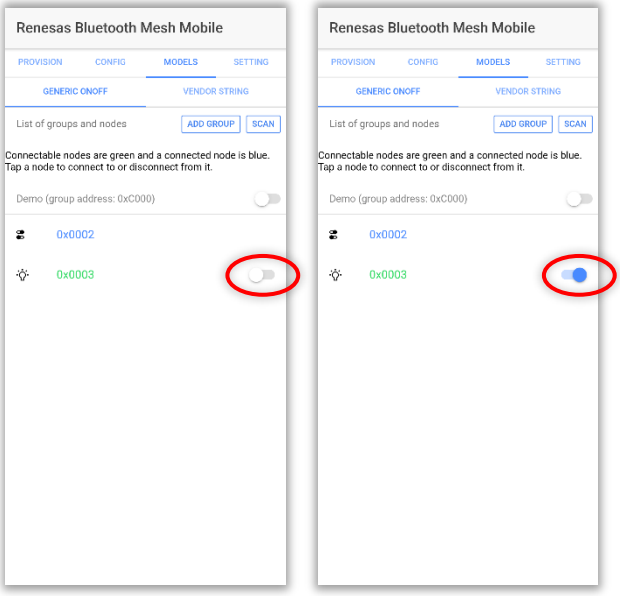

Figure 5-7 Publication of Generic OnOff SET Messages to Group Address

5.3.2 Generic OnOff State Control by EK-RA4W1

1. Push the SW1 on each EK-RA4W1 working as Generic OnOff Client repeatedly.

   You can see that LEDs of all EK-RA4W1 working as Generic OnOff Server follow the Generic OnOff SET messages received.

5.3.3 Vendor State Control by Mesh Mobile

1. In the VENDOR STRING of the MODELS tab, tap the STRING button of the group. Next, enter any character string and tap SEND button in the dialog.

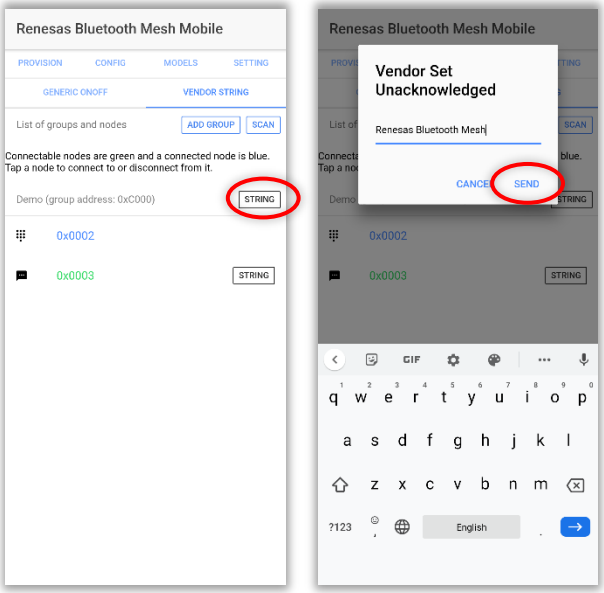

Figure 5-8 Publication of Vendor SET Messages to Group Address

You can see that all EK-RA4W1 working as Vendor Server output the character string included in the Vendor SET messages received to console.

```
Vendor Set src: 0x7F00 dst: 0xC000 len = 23 value: "Renesas Bluetooth Mesh"
```

Figure 5-9 Console Log of Vendor Server Nodes

2. In the VENDOR STRING of the MODELS tab, tap the STRING button of any node. Next, enter any character string and tap SEND button in the dialog.

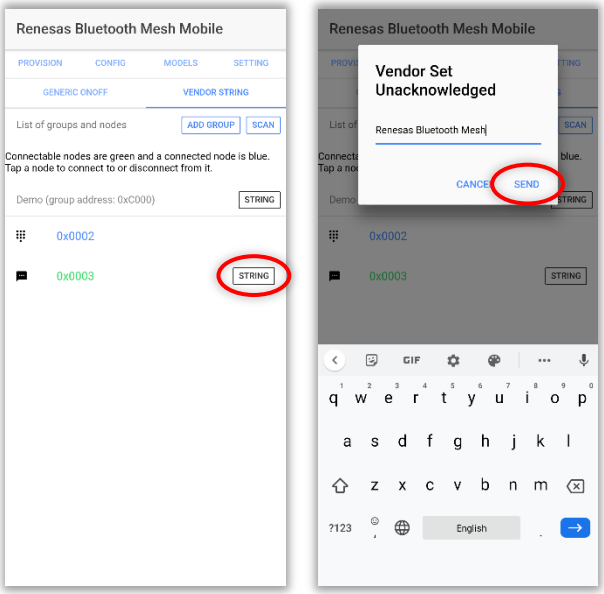

Figure 5-10 Publication of Vendor SET Messages to Unicast Address

You can see that the EK-RA4W1 working as Vendor Server outputs the character string included in the Vendor SET messages received to console.

```
Vendor Set src: 0x7F00 dst: 0x0003 len = 23 value: "Renesas Bluetooth Mesh"
```

Figure 5-11 Console Log of a Vendor Server Node

5.3.4 Vendor State Control by EK-RA4W1

1. Enter any character string and press enter key in the console connected to the EK-RA4W1 which works as Vendor Client.

```
Renesas Bluetooth Mesh
MS_vendor_set_unack() status:0x0000
```

Figure 5-12 Entering Character String in Console of a Vendor Client Node

You can see that the EK-RA4W1 working as Vendor Server outputs the character string included in the Vendor SET messages received to console.

```
Vendor Set src: 0x0002 dst: 0xC000 len = 23 value: "Renesas Bluetooth Mesh"
```

Figure 5-13 Console Log of a Vendor Server Node

5.3.5 Node Reset by Mesh Mobile

1. Connect a node in the CONFIG tab and tap the RESET button. Next, tap the SEND button in the dialog.

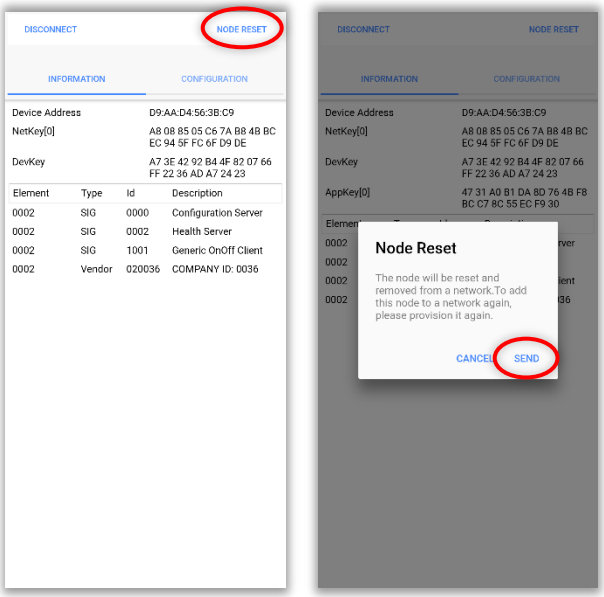

Figure 5-14 Publication of Config Node Reset Message to a Node

You can see that the EK-RA4W1 connecting to Mesh Mobile performs Provisioning again by receiving the Config Node Reset message.

```
MS_ACCESS_CONFIG_NODE_RESET_OPCODE
Reboot platform

Bearer Initialization Completed
         Device Address: D1:7A:AE:3E:B5:CF rnd
Start Observing...
RM_BLE_MESH_ACCESS_Open() status:0x0000
RM_MESH_CONFIG_SRV_Open() status:0x0000
RM_MESH_HEALTH_SERVER_Open() status:0x0000
RM_MESH_GENERIC_ON_OFF_CLT_Open() status:0x0000
MS_vendor_client_init() status:0x0000
RM_BLE_MESH_PROVISION_Open() status:0x0000
RM_BLE_MESH_PROVISION_Setup() status:0x0000
         Role  : UNPROVISIONED DEVICE
         Bearer: BOTH
RM_BLE_MESH_PROVISION_Bind() status:0x0000
         Device UUID: 9DFE158E-4EBF-4074-BC05-69347BCD3673
```

Figure 5-15 Console Log of the Node that received Config Node Reset message

6. Appendix

6.1 Log Message

An example of log message sent from the sample program is shown below. Regarding the serial port setting for terminal tool, refer to Table 4-2 in Chapter 5.

```
Bearer Initialization Completed
         Device Address: DF:BC:49:8F:BA:9A rnd
RM_BLE_MESH_ACCESS_Open() status:0x0000
RM_MESH_CONFIG_SRV_Open() status:0x0000
RM_MESH_HEALTH_SERVER_Open() status:0x0000
RM_MESH_GENERIC_ON_OFF_SRV_Open() status:0x0000
MS_vendor_server_init() status:0x0000
RM_BLE_MESH_PROVISION_Open() status:0x0000
RM_BLE_MESH_PROVISION_Setup() status:0x0000
         Role  : UNPROVISIONED DEVICE
         Bearer: BOTH
RM_BLE_MESH_PROVISION_Bind() status:0x0000
         Device UUID: C8010B0A-429B-4899-F853-7F72EDA2BBAA
BLEBRR_GATT_IFACE_UP
         Device Address: 52:04:EE:2F:0E:91 rnd
BLEBRR_GATT_IFACE_ENABLE
         Device Address: 52:04:EE:2F:0E:91 rnd
RM_BLE_MESH_PROVISION_Bind() status:0x0000
BLE_MESH_PROVISION_EVENT_TYPE_PROVISIONING_SETUP status:0x0000          Start of Provisioning
BLE_MESH_PROVISION_EVENT_TYPE_PROVDATA_INFO status:0x0000
         Unicast Address: 0x0235
         IV Index: 0x00000006
         Flags: 0x00
RM_BLE_MESH_ACCESS_SetProvisioningData() status:0x0000
BLE_MESH_PROVISION_EVENT_TYPE_PROVISIONING_COMPLETE status:0x0000       End of Provisioning
RM_BLE_MESH_ACCESS_GetNetKey() status:0x0000
         NetKey: F9 8B 2D 37 B3 1D 45 51 01 D8 0E B5 5D 41 A9 4E
RM_BLE_MESH_ACCESS_GetDeviceKey()
         DevKey: FA CE 0A 41 07 ED D8 15 5B 37 C0 3D D8 D6 AF A1
BLEBRR_GATT_IFACE_DOWN
         Device Address: 52:04:EE:2F:0E:91 rnd

RM_BLE_MESH_NETWORK_Open() status:0x0000
RM_BLE_MESH_NETWORK_StartProxyServerAdv() status:0x0000
         Identification Type: Node Identity
BLEBRR_GATT_IFACE_UP
         Device Address: F4:03:2A:25:12:60 rnd
MS_PROXY_UP_EVENT                                                       Establishment of Proxy Connection
RM_BLE_MESH_NETWORK_BroadcastSecureBeacon() status:0x0000
BLEBRR_GATT_IFACE_ENABLE
         Device Address: F4:03:2A:25:12:60 rnd

MS_ACCESS_CONFIG_APPKEY_GET_OPCODE                                      Start of Configuration
MS_ACCESS_CONFIG_RELAY_GET_OPCODE
MS_ACCESS_CONFIG_FRIEND_GET_OPCODE
MS_ACCESS_CONFIG_GATT_PROXY_GET_OPCODE
MS_ACCESS_CONFIG_APPKEY_ADD_OPCODE
MS_ACCESS_CONFIG_MODEL_APP_BIND_OPCODE
MS_ACCESS_CONFIG_MODEL_APP_BIND_OPCODE
MS_ACCESS_CONFIG_MODEL_PUBLICATION_SET_OPCODE
MS_ACCESS_CONFIG_MODEL_PUBLICATION_SET_OPCODE
MS_ACCESS_CONFIG_MODEL_SUBSCRIPTION_ADD_OPCODE
MS_ACCESS_CONFIG_MODEL_SUBSCRIPTION_ADD_OPCODE
MS_ACCESS_CONFIG_RELAY_SET_OPCODE
MS_ACCESS_CONFIG_FRIEND_SET_OPCODE
MS_ACCESS_CONFIG_GATT_PROXY_SET_OPCODE                                  End of Configuration
```

```
Generic OnOff Set src: 0x7F00 dst: 0xC001 tid: 0x00 state: ON
Generic OnOff Set src: 0x7F00 dst: 0xC001 tid: 0x01 state: OFF
```

Generic OnOff Server Model

```
Vendor Set src: 0x7F00 dst: 0xC001 len = 36 value: "Renesas Bluetooth Mesh vendor model"
```

Vendor Server Model

6.2 Trouble Shooting

This section describes troubleshooting in the process of running the demo in Chapter 5.

6.2.1 Cannot find device which broadcast Un-provisioned Device beacons

Cause

The device that you are trying to provision may already be provisioned.

Recovery procedure for EK-RA4W1

The Bluetooth Mesh stack stores information such as the network key exchanged with the provisioner during provisioning process in the data flash. At storing the information in the data flash, the Bluetooth Mesh stack writes a magic number on the top of the data flash that indicates this device is already provisioned. The sample program included in the "*Bluetooth Mesh Sample Application*" (R01AN5848) resumes sending un-provisioned device beacons by erasing this magic number as described below.

1. Press SW1 and RESET button on EK-RA4W1.
2. Release only RESET button and keep more than 2 seconds.
3. Release SW1.

In addition, you can also resume un-provisioned beacons by re-programming the sample program with the following procedures.

1. Launch J-Flash Lite and select RA4W1 as device.
2. Erase data flash by pushing *Erase Chip* button.

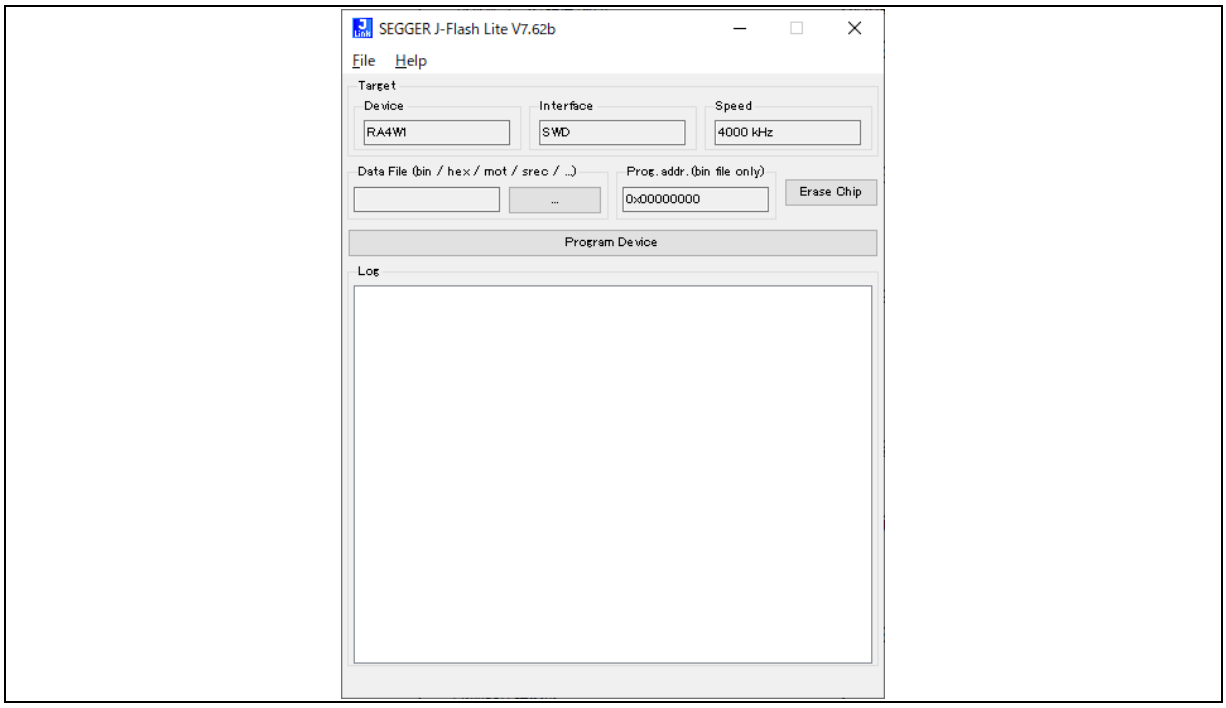

Figure 6-1 Erase Data flash

3. Re-programming the sample program.

Recovery procedure for Mesh mobile application

The Mesh mobile application stores information such as network keys exchanged during provisioning. The Mesh mobile application detect un-provisioned beacons again by deleting the information applying the following procedures.

1. Move to SETTING tab.

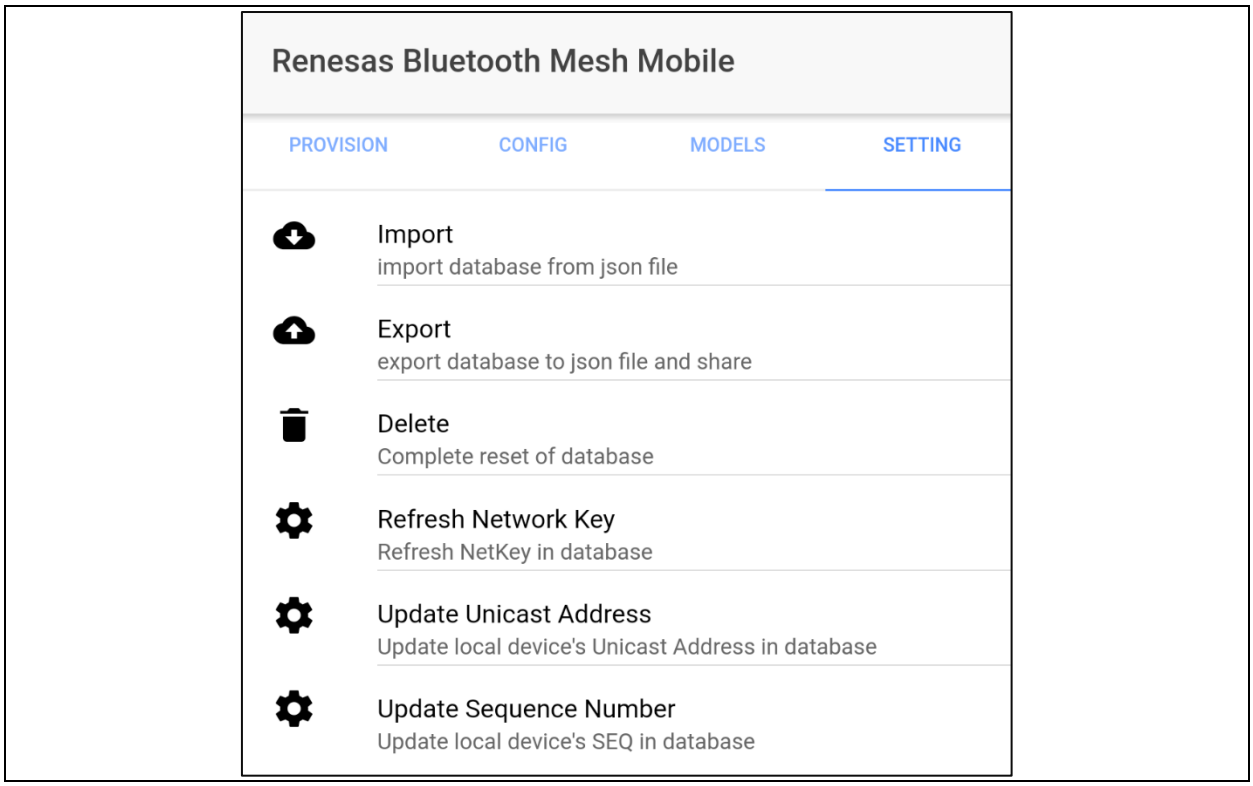

Figure 6-2 SETTING tab

2. Tap Delete and choose OK in following confirmation window.

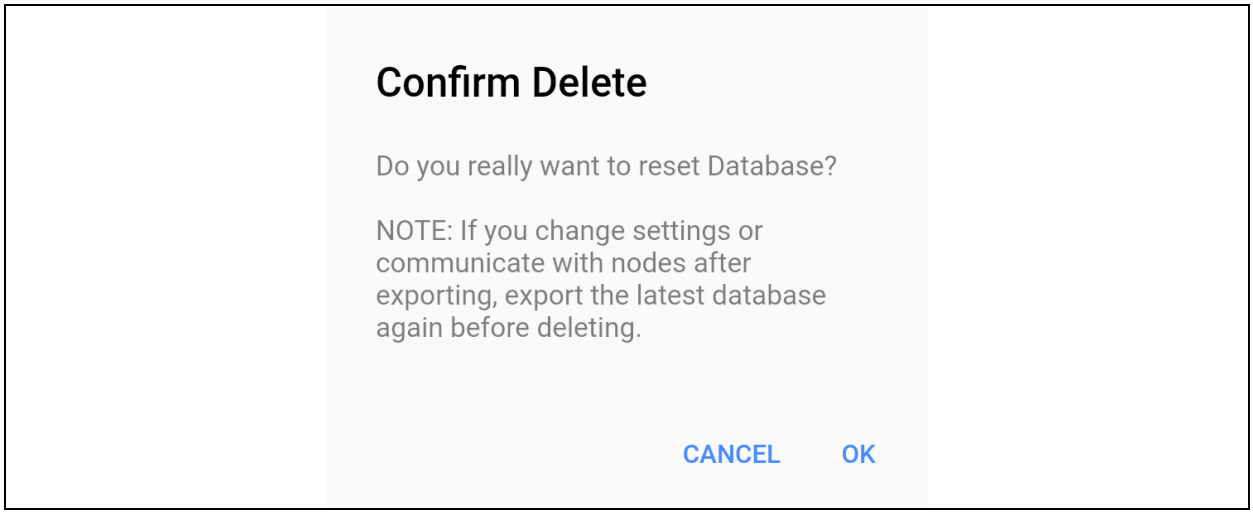

Figure 6-3 Confirmation dialog

3. Back to PROVISION tab and press SCAN button.

6.2.2 Cannot find node which can accept connection

Cause

The node that you are trying to provision may not broadcast connectable advertising PDUs.

Recovery procedure for EK-RA4W1

The sample program included in the "*Bluetooth Mesh Sample Application*" (R01AN5848) continues connectable advertising for 60 seconds to accept the configuration after provisioning is complete. And when you enabled proxy feature, connectable advertising is always performed for message exchange via GATT bearer. Therefore, if 60 seconds or more have passed from provisioning to the start of configuration, or if the proxy function is not enabled, connectable advertising will not be executed, and it will not be detected as a connectable node in the CONFIGURATION or MODEL tab. In such cases, the node resumes connectable advertising for 60 seconds by performing the following steps:

1. Press SW1 on EK-RA4W1 more than 2 seconds.
2. Release SW1.

Trademark and Copyright

The *Bluetooth*® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Renesas Electronics Corporation is under license. Other trademarks and registered trademarks are the property of their respective owners.

RA4W1 Group Bluetooth Mesh Stack uses the following open source software.

- crackle; AES-CCM, AES-128bit functionality
  BSD 2-Clause License

  Copyright (c) 2013-2018, Mike Ryan
  All rights reserved.

  Redistribution and use in source and binary forms, with or without
  modification, are permitted provided that the following conditions are met:

  * Redistributions of source code must retain the above copyright notice, this
    list of conditions and the following disclaimer.

  * Redistributions in binary form must reproduce the above copyright notice,
    this list of conditions and the following disclaimer in the documentation
    and/or other materials provided with the distribution.

  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
  AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
  IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
  DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE
  FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
  DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
  SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
  CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
  OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
  OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Revision History

Rev.	Date	Description	
1.00	Feb. 25, 2022	-	First edition
1.01	Apr.27.2022	P.24 -	Add section 6.2. Updated attached Mesh Mobile.
1.02	Jun.30.2022	P.9	Add the download link mesh mobile application for Android.
1.03	Aug.29.2022	P.8, P.9, P.11, P.13	Updated Mesh Mobile Application.
1.05	Dec.16.2022	P.9 P.13 -	Add the download link mesh mobile application for iOS. Add the note about provisioning. Updated attached Mesh Mobile.

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on

   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. Handling of unused pins

   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.
5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.
6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.
   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.

(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/.