Contents

1 Executive Summary

Bluetooth positioning technology is a key innovation in TP-Link Omada's business networking solutions, specifically developed for low-cost indoor positioning scenarios. With the explosive growth of Internet of Things (IoT) devices, the high power consumption and high costs of traditional wireless communication technologies (such as Wi-Fi and cellular networks) have become increasingly prominent.

A Bluetooth access point (AP) detects nearby Bluetooth signals and estimates the location of tags based on signal strength. When multiple APs work together, positioning becomes more precise. The collected signals are transmitted to a dedicated positioning server and application server, where tag locations are linked with corresponding functions.

This white paper comprehensively explains the background, principles, configuration, key application scenarios, and deployment examples of Bluetooth positioning technology, helping network administrators and system integrators master this technology and implement their own customized indoor positioning solutions.

2 Introduction

2.1 Industry Challenges and Pain Points

Amid the wave of intelligent interconnections, IoT technology has become a core engine driving industrial upgrades. However, with the exponential growth in the number of devices and the diversification of application scenarios, the industry faces multiple challenges:

- **Device and Protocol Fragmentation:** IoT devices from different manufacturers use heterogeneous protocols such as Wi-Fi, Zigbee, and LoRa, resulting in poor cross-platform compatibility and high system integration costs.

- **Power Consumption and Battery Life Bottlenecks:** The high energy consumption of traditional wireless technologies (such as Wi-Fi) limits the long-term deployment of battery-powered devices (such as sensors and wearables).

- **Insufficient Scalable Networking Capabilities:** In smart homes and industrial monitoring scenarios, traditional star-shaped network architectures struggle to support the high-density

access and dynamic expansion of massive nodes.

- **Security and Privacy Risks:** The use of plaintext transmission and weak authentication mechanisms in inter-device communications make data leakage and cyberattacks a critical threat to the IoT ecosystem.

In the face of these pain points, Bluetooth IoT is emerging as a key short-range solution, offering low power use, broad compatibility, flexible networking, and strong security.

2.2 Purpose

This white paper aims to:

1. Detail the principles and advantages of Bluetooth IoT technology;

2. Provide specific configuration guidelines and application strategies for Bluetooth IoT;

3. Share best practices and performance data based on actual deployments;

4. Demonstrate the role of Bluetooth IoT technology in various application scenarios;

5. Help network administrators and system integrators master Bluetooth IoT technology and implement their own indoor positioning solutions.

2.3 Technology Positioning

Bluetooth IoT technology, with Bluetooth Low Energy (BLE) and Bluetooth Mesh at its core, is designed to build a short-range, lightweight, and highly reliable IoT infrastructure. Its core value lies in:

- **Scenario Adaptability:** Coverage radius ranges from a few meters (indoors) to hundreds of meters (Bluetooth 5.1+ Long-Range Mode), making it suitable for the "last-mile" connectivity in scenarios such as smart homes, Industry 4.0, and smart healthcare.

- **Protocol Compatibility:** Over 5 billion devices worldwide have built-in Bluetooth modules (according to the data from Bluetooth SIG 2023), making it naturally compatible with mobile phones, PCs, and other devices and significantly easier for user access.

- **Energy Efficiency:** BLE’s standby power consumption is at the μA level, enabling the device

to last for years (such as temperature and humidity sensors powered by button cell batteries). This can completely eliminate battery anxiety.

- **Dynamic Self-Organizing Networking:** Bluetooth Mesh supports many-to-many communication, accommodating tens of thousands of nodes in a single network. It achieves decentralized data transmission through “flooding” or “routing” modes.

By upgrading Bluetooth technology from a “device pairing tool” to an “IoT neural network”, Bluetooth IoT is driving short-range communications from “connecting islands” to “global intelligence.”

3 Overview of Bluetooth IoT

3.1 Background and Market Demand

With the explosive growth of IoT devices, the high power consumption and high cost of traditional wireless communication technologies (such as Wi-Fi and cellular networks) have become increasingly prominent. Especially in smart homes, wearables, and industrial sensor scenarios, where devices powered by tiny batteries should last for years, Bluetooth Low Energy (BLE), with its ultra-low energy consumption (1/10th to 1/100th that of Bluetooth Classic), low cost, and lightweight protocol stack, has become a core technology for connecting IoT edge devices.

3.2 Key Advantages

Ultra-Low Power Consumption: BLE utilizes intermittent advertising and a fast connection mechanism, with standby power consumption as low as 0.01-0.5 milliwatts, significantly increasing the number of button cell battery-powered devices.

Lightweight Protocol Stack: The BLE protocol stack is streamlined (requiring only 192 KB of RAM), suitable for resource-constrained microcontrollers (MCUs) and reducing hardware costs.

Wide Compatibility: BLE is natively compatible with smartphones, tablets, and other terminals, enabling direct device connectivity and data transparency without the need for an additional gateway.

Flexible Topology: Star-shaped, broadcast, and mesh networks (Bluetooth Mesh) are supported, covering diverse scenarios from single-point connections to large-scale sensor networks.

4 Principles of Bluetooth IoT

4.1 BLE Protocols

Bluetooth Low Energy (BLE), introduced in the Bluetooth 4.0 specification in 2010, is defined by its low power consumption. Like Bluetooth Classic, it operates in the 2.4–2.4835 GHz band, but with a lower transmission rate, making it unsuitable for large data transfers and better suited for device discovery and simple communications. According to the protocols, both Bluetooth Classic and BLE can cover up to 100 meters. Common BLE protocols include Apple's iBeacon protocol, Google's Eddystone protocol, and other proprietary protocols from manufacturers, such as Minew.

4.1.1 iBeacon Protocol

Based on BLE, iBeacon utilizes the "advertising frame," which is a broadcast frame transmitted periodically and received by BLE-enabled devices. iBeacon embeds Apple's proprietary data format in the payload of the advertising frame.

The iBeacon data consists of four main elements: UUID, Major, Minor, and Measured Power.

UUID (Universally Unique Identifier) is a 128-bit identifier following the ISO/IEC 11578:1996 standard.

Major and Minor are 16-bit identifiers defined by the iBeacon publisher. For example, a retail chain may use Major to represent the region and Minor to specify the store ID. In home appliances, Major can indicate the product model while Minor conveys an error code, allowing external systems to detect malfunctions.

Measured Power is the reference Received Signal Strength Indicator (RSSI) when the iBeacon module and the receiver are 1 meter apart. The receiver can use this reference RSSI and the strength of the received signal to estimate the distance between the transmitting module and the receiver.

The frame payload of Apple’s iBeacon is shown as follows:

- **Apple iBeacon**

Offset	Length	Type	Data	Details
0	1	Data Length	0x02	/
1	1	Flag data type	0x01	/
2	1	Flag data	0x06	/
3	1	Data Length	0x26	/
4	1	Manufacture Data	0xFF	/
5	2	Company ID	0x4C00	(little-endian) 0x004C
7	2	Beacon Type	0x0215	(big-endian) 0x0215
9	16	UUID	0x0112233445566 778899AABBCCDD EEFF0	(big-endian) 0x01122334455 66778899AABB CCDDEEFF0
25	2	Major	0x03E8	(big-endian) 0x03E8
27	2	Minor	0x07D0	(big-endian) 0x07D0
29	1	RSSI at 1m	0xC5	-59dBm

Each iBeacon device has a unique ID (UUID + Major + Minor). When signals are broadcast within a region, the ID information in the signal marks a particular area. UUID is a unique identifier that differentiates your iBeacon device from others. Major is used to group related iBeacon devices together, while Minor identifies a specific individual iBeacon device.

For example, you can deploy iBeacon devices in your chain department stores to provide users with promotional information. As shown below, all your iBeacon transmitters can have the same UUID, but each store will have its own Major value, and each department within the store will have its own Minor value.

Store Location		San Francisco	Paris	London
UUID		D9B9EC1F-3925-43D0-80A9-1E39D4CEA95C		
Major		1	2	3
Minor	Clothing	10	10	10
	Housewares	20	20	20
	Automotive	30	30	30

Additionally, iBeacon has a certain level of proximity awareness. The iBeacon protocol categorizes distance into three ranges: Immediate (very close), Near (1-3 m), and Far (further away). This is achieved through the Measured Power parameter, which lays a foundation for iBeacon's ability to roughly estimate the user's location.

As a location-aware technology, iBeacon mainly has two applications:

1. Detecting whether a user has entered the iBeacon region and pushing relevant messages to them.

2. Performing indoor positioning based on signal strength and information on iBeacon base stations.

4.1.2 Eddystone Protocol

Eddystone is an open-source Bluetooth beacon protocol developed by Google. It is completely open and supports Android, iOS, and even web browsers.

The Eddystone Bluetooth Frame broadcasts the following four parameters:

1. **Eddystone UID:** A unique beacon UID.

2. **Eddystone URL:** Used to broadcast a uniform resource locator (URL).

3. **Eddystone TLM:** Used to broadcast the beacon's own telemetry (i.e., health and status) data.

4. **Eddystone-EID:** A new frame type that defines an encrypted mode to broadcast encrypted information, which can only be decrypted by authorized users.

- **Eddystone TLM**

Offset	Length	Type	Data	Details
0	1	Data Length	0x02	/
1	1	Flag data type	0x01	/
2	1	Flag data	0x06	/
3	1	Data Length	0x03	/
4	1	Complete list of 16-bit Service UUIDs	0x03	/
5	2	UUID data	0xAAFE	(little-endian) 0xFEAE
7	1	Data Length	17	/
8	1	Service data	0x16	/
9	2	UUID data	0xAAFE	(little-endian) 0xFEAE
11	1	Frame Type	0x20	/
12	1	Version	0x00	/
13	2	Battery Voltage	0x0BB8	(big-endian) 3000mV
15	2	Temperature	0x1973	(8.8 fixed-point) 25.44°C
17	4	Adv Count	0x000003E8	(big-endian) 1000 times
21	4	Seconds Count	0x00000258	(big-endian)60 senconds

Eddystone also defines a GATT configuration service to enable interoperability between hardware manufacturers and application developers. This allows beacons to report their capabilities to applications, and enables the reconfiguration of beacon’s broadcast data. It is necessary when

devices need to be securely paired and registered as Eddystone-EID beacons.

Based on the Eddystone beacon, various commercial application scenarios are available as follows:

- **Indoor Navigation:** By installing Eddystone beacons in buildings, people can use their mobile devices to access indoor maps and navigation information.

- **Retail Promotions:** Merchants can place Eddystone beacons near their products to send coupons and promotional information to nearby consumers.

- **Transportation:** Eddystone beacons can be used for vehicle positioning, providing real-time traffic flow information and navigation services.

4.1.3 Proprietary Protocols

In addition to open protocols, many manufacturers have also released some proprietary protocols compatible with their own Bluetooth products. These proprietary protocols often carry a larger amount of information more flexibly. Some widely used proprietary protocols include those from Minew, EnOcean, and MySphera. Here, we will use Minew's protocol as an example.

Minew's protocol is the company's customized Bluetooth iBeacon protocol. Compared to iBeacon and Eddystone, Minew has defined more upload information, such as Local Name, Humidity, Temperature, Battery Level, ACC-axis, Lux Data, Pressure Data, PIR Data, Vibration Data, and AP Data. Minew also sells Bluetooth sensors. With the protocol, its sensors can transmit the data via the BLE iBeacon frame, and the specified receiver can receive and report the data, enabling information collection and updates across the entire area.

- **Minew HT Data**

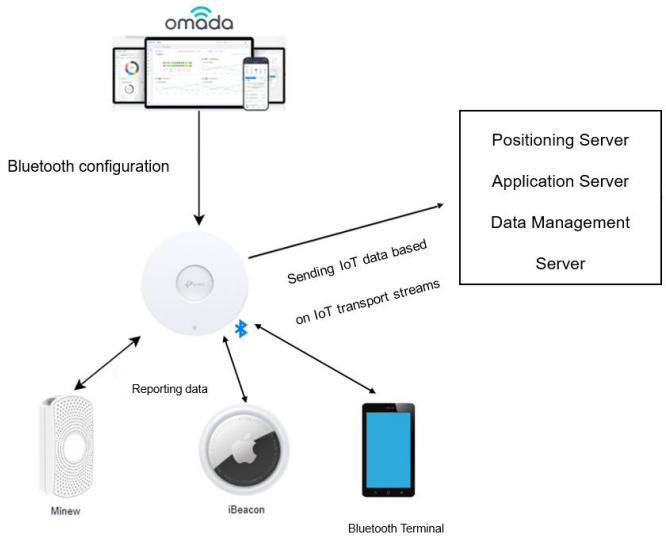
Offset	Length	Type	Data	Details
0	1	Data Length	0x02	/
1	1	Flag data type	0x01	/
2	1	Flag data	0x06	/
3	1	Data Length	0x03	/
4	1	Complete list of 16-bit Service UUIDs	0x03	/
5	2	UUID data	0xE1FF	(little-endian) 0xFFE1
7	1	Data Length	16	/
8	1	Service data	0x16	/
9	2	UUID data	0xE1FF	(little-endian) 0xFFE1
11	1	Frame Type	0xA1	0xA1
12	1	Version Number	0x01	/
13	1	Battery level	0x64	Battery level is 100%
14	2	Temperature	0x1973	(8.8 fixed-point) 25.44°C
16	2	Humidity	0x4864	(8.8 fixed-point) 72.39% (little-endian)
18	6	Mac address	0x009078563412	(little-endian) 12:34:56:78:90:00

4.2 Bluetooth IoT Positioning

4.2.1 Positioning Principle

Bluetooth IoT is a low-cost indoor positioning solution that can achieve Bluetooth terminal positioning, Bluetooth tag positioning, and Bluetooth data reporting. The basic principle is that an EAP has built-in Bluetooth that can detect nearby Bluetooth signals. The EAP can roughly estimate the position of a Bluetooth tag based on the signal strength of the Bluetooth frame, and more EAPs can provide more accurate positioning. Multiple EAPs will send the collected Bluetooth signals to the positioning server and application server dedicated to processing the data in order to coordinate tag positioning with other corresponding functions.

The basic principle diagram is shown as follows:



Bluetooth IoT positioning functionality is mainly divided into three parts:

1. The transmission of Bluetooth signals.

2. The collection and reporting of Bluetooth information.

3. The processing of positioning information and its application.

EAP plays an important role in the transmission, collection, and reporting of Bluetooth signals, while the third part mainly relies on third-party servers, with different processing methods used to realize different functions.

Currently, EAPs can actively transmit iBeacon frames, collect Bluetooth information, and report the data to the specified servers to meet different needs.

4.2.2 Bluetooth Advertising

Bluetooth tags can follow their own protocols to send the Bluetooth broadcast frames with the specified information embedded. The corresponding devices can roughly locate the position of the Bluetooth tags by collecting this information. Currently, EAPs can also actively transmit the corresponding configured iBeacon frames. The UUID + Major + Minor fields in the iBeacon frame can be used to classify the EAPs, and the Measured Power field can be used to locate them. Devices receiving Bluetooth frames can determine their own location from the frame data, enabling specific actions to be triggered at designated positions.

Application example: **Bluetooth Terminal Positioning**

Mobile phones are the most common Bluetooth terminal. After installing a dedicated application, a phone will receive the iBeacon frames sent by the EAP when it enters the EAP coverage area. The application can extract information from the scanned iBeacon frames and report it to the server. The server can analyze the corresponding data to know approximately the current location of the phone, and then push specific promotion messages based on the location information to achieve specific functions.

For example, in such scenarios as shopping malls and parking lots, besides offering Wi-Fi access, an EAP can also provide Bluetooth terminal positioning service through the built-in Bluetooth module. Users can scan the BLE devices with their phones and report the BLE device information to the positioning server to achieve positioning and navigation functions in conjunction with the application. Shops can deploy BLE devices and push shopping guides and promotional information to users via the application when the users scan the broadcast frames sent by these BLE devices.

As shown in the table below, the iBeacon frames transmitted by the EAPs in different areas of the shopping mall are different. The Bluetooth terminal can roughly locate itself according to the fields of the received iBeacon frame, and the server can push different messages based on this location information.

Store Location		Area A	Area B	Area C
UUID		e2c56db5dffb48d2b060d0f5a71096e0		
Major		1	2	3
Minor	Clothing	10	10	10
	Food	20	20	20
	Games	30	30	30

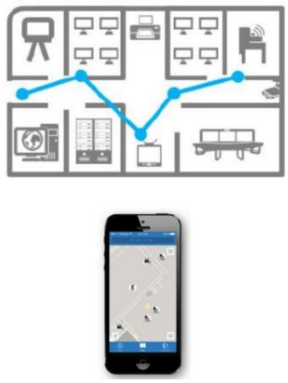
4.2.3 Data Reporting

BLE communication is a one-way communication protocol, with which the Bluetooth tags transmit

the specified data by embedding them in the iBeacon broadcast frames according to different protocols. This data needs to be collected and reported by dedicated devices in order to be processed accordingly to enable the corresponding functions. All data on the IoT server comes from what EAPs report, thus demanding high accuracy and stability for the EAPs to collect and report Bluetooth information. The EAPs have to be able to collect the required Bluetooth information and report it based on our settings.

Application example: **Bluetooth Tag Positioning**

Bluetooth tag sensors will periodically send Bluetooth frames that conform to the iBeacon, Minew, or Eddystone protocols. The iBeacon frame will carry basic information like TxPower and RSSI reference values. Bluetooth frames of other protocols can also carry sensor data and other information. After collection, an EAP will report the information to a third-party positioning server, which will then comprehensively process all the information reported to determine the approximate location of the Bluetooth tags and environmental information. This feature is generally used for location monitoring of important equipment and environmental monitoring of important places to achieve positioning of key asset equipment and key personnel. By fixing the BLE tags on the assets to be tracked and deploying EAPs that can receive iBeacon frames in the office area, the EAPs can report the collected RSSI information to the positioning server, and the asset can be located and tracked through the management platform.



The approximate location obtained based on the processing and reporting of Bluetooth information can also be applied to indoor navigation, personnel management and tracking, and geofencing in such scenarios as shopping malls, scenic spots, and parking lots.

4.2.4 Transmission Protocol

Data exchange between APs and IoT servers relies on transmission protocols, most commonly

HTTP, WebSocket, MQTT, and AMQP. Below is a brief introduction to each:

HTTP

HTTP is the most widely used application layer protocol on the internet, used for communication between clients (such as browsers) and servers based on a request-response model. In IoT scenarios, due to its high message overheads (redundant headers), high TCP connection overheads, and high latency, it is gradually being replaced by other lightweight protocols.

WebSocket

WebSocket is a full-duplex TCP-based communication protocol that enables bidirectional real-time data transmission between clients and servers over a single connection, addressing the unidirectional nature and high latency of the traditional HTTP request-response model. With its bidirectional, real-time communication and low latency, it has become a core protocol for device control and state synchronization in IoT scenarios. It offers significant advantages in areas requiring high-frequency interaction, such as smart homes and industrial monitoring. However, for resource-constrained devices, it requires hybridization with lightweight protocols such as MQTT.

MQTT

Message Queuing Telemetry Transport (MQTT) is a lightweight communication protocol based on the publish-subscribe model. Built on TCP/IP, it was released by IBM in 1999. MQTT's greatest advantage is that it can provide real-time, reliable messaging services for connecting remote devices with minimal code and limited bandwidth. As a low-overhead, low-bandwidth instant messaging protocol, it has a widespread application in the IoT area, small devices, and mobile applications.

AMQP

Advanced Message Queuing Protocol (AMQP) supports multiple messaging models and offers a powerful feature set. Created by JPMorganChase in 2003, it is designed for systems requiring high reliability and complex functionality. AMQP is an application-layer standard for unified messaging services. It is an open standard for application-layer protocols designed for message-oriented middleware. Clients and middleware based on this protocol can exchange messages without being restricted by different client/middleware products or development languages. Compared with MQTT, AMQP is more flexible and supports more message routing methods such as point-to-point, publish-subscribe, and fan-out, while MQTT is lighter and suitable for low-bandwidth, low-power

IoT devices.

5 Configuration Guidelines

5.1 System Requirements and Compatibility

Software Requirements:

Omada Controller v5.15.24 or above.

EAP firmware v1.4.2 or above.

Hardware Compatibility:

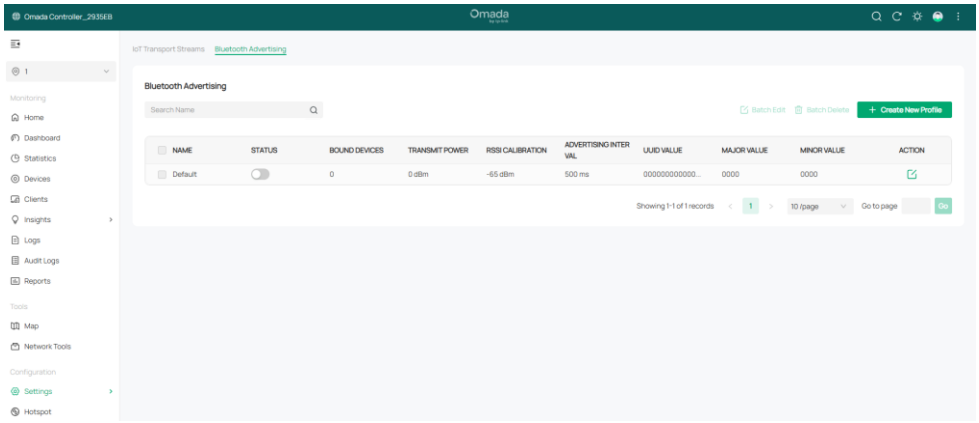
Device Type	Model	Minimum Firmware Version	Features
Access Point	EAP660HD 2.0/ EAP625-OutdoorHD 1.0	v 1.4.2	Fully supported

5.2 Configuration Procedure

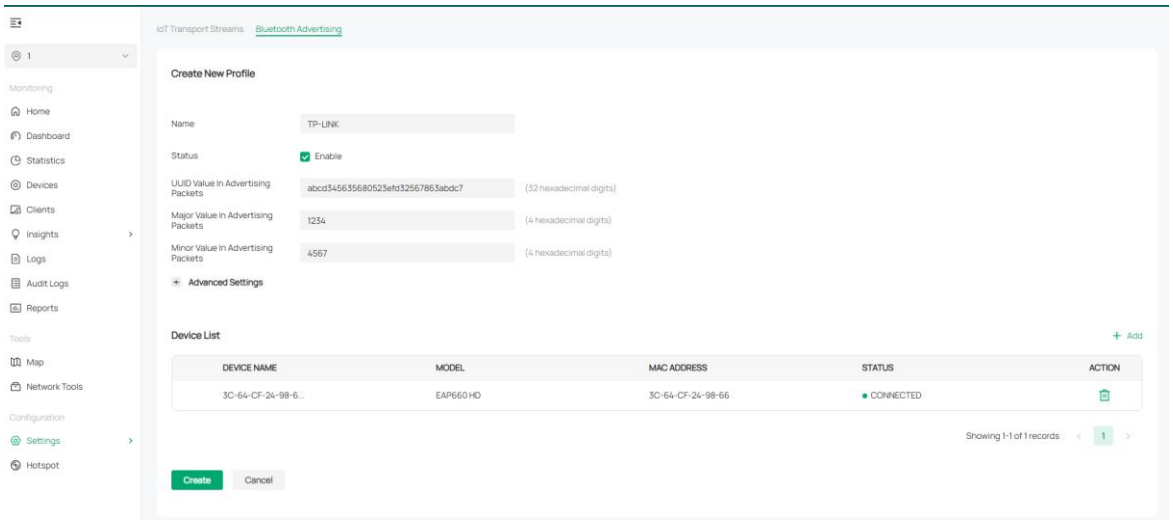
5.2.1 Bluetooth Advertising

After configuring Bluetooth advertising on an EAP, the EAP will send iBeacon advertising frames with a specific configured UUID-Major-Minor-RSSI Calibration Value field, which can help realize Bluetooth terminal positioning in specific application scenarios.

Launch the Omada Controller, go to Settings > Wired & Wireless Networks > Bluetooth to load the following page, and configure the iBeacon frame-related parameters.



Bluetooth-supported EAPs can broadcast iBeacon packets and mobile clients can realize the positioning feature by receiving the iBeacon packets. On the Bluetooth Advertising page, you can configure rules for the EAP to broadcast iBeacon packets. There is a default profile, which cannot be deleted but can be disabled. You can add an Advertising profile and assign it to the specific EAPs.



Explanation:

Item	Configuration
Name	Enter a name to identify the profile.
Status	Enable or disable the profile.
UUID Value In Advertising	The UUID (Universally Unique Identifiers) of the advertising

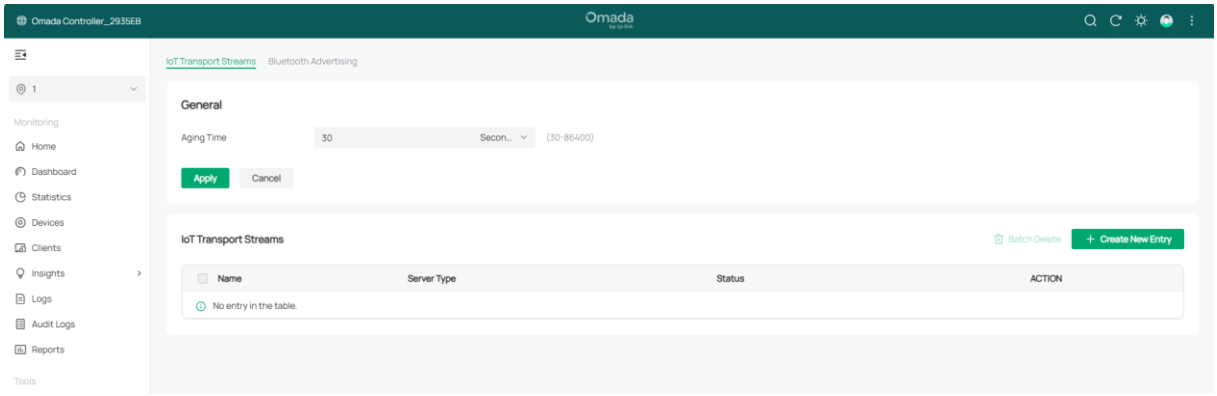
Packets	iBeacon packet. It can help group APs in different locations and help Bluetooth terminals determine their approximate location.
Major Value In Advertising Packets	The Major value of an advertising iBeacon packet, indicating a larger group. It can help group APs in different locations and help Bluetooth terminals determine their approximate location.
Minor Value In Advertising Packets	The Minor value of an adverting iBeacon packet, indicating a smaller group. It can help group APs in different locations and help Bluetooth terminals determine their approximate location.
Transmit Power	Broadcast transmit power (dB). The following values are currently supported: [-20, -18, -15, -12, -10, -9, -6, -5, -3, 0, 1, 2, 3, 4, 5,14, 15, 16, 17, 18, 19, 20] The higher the transmit power, the longer the coverage range. In actual deployment, ensure that the Bluetooth terminal receives the strongest Bluetooth signal from the nearest AP. Adjust this value according to the actual coverage to avoid interfering with the positioning of nearby APs. It is recommended that all APs use the same transmit power.
RSSI Calibration Value	-65dB by default.
Advertising Interval	Specify a value between 100 and 3000 m. The range will be changed to 100-10240.
Device List	The default Site-level entry does not feature this list. Only custom entries support configuration of specific devices. Currently, one Bluetooth Advertising profile can be configured for a single device.

Click **Add** to apply the newly added advertising profile to the specified EAP devices. This way, iBeacon frames sent by EAPs in different areas can be inconsistent to distinguish the locations.

5.2.2 IoT Transport Streams

An AP is used to report IoT data to a specific server. By configuring the IoT transmission streams, the AP can collect the required Bluetooth information and report it to a third-party IoT server.

Go to the **IoT Transport Steams** page.

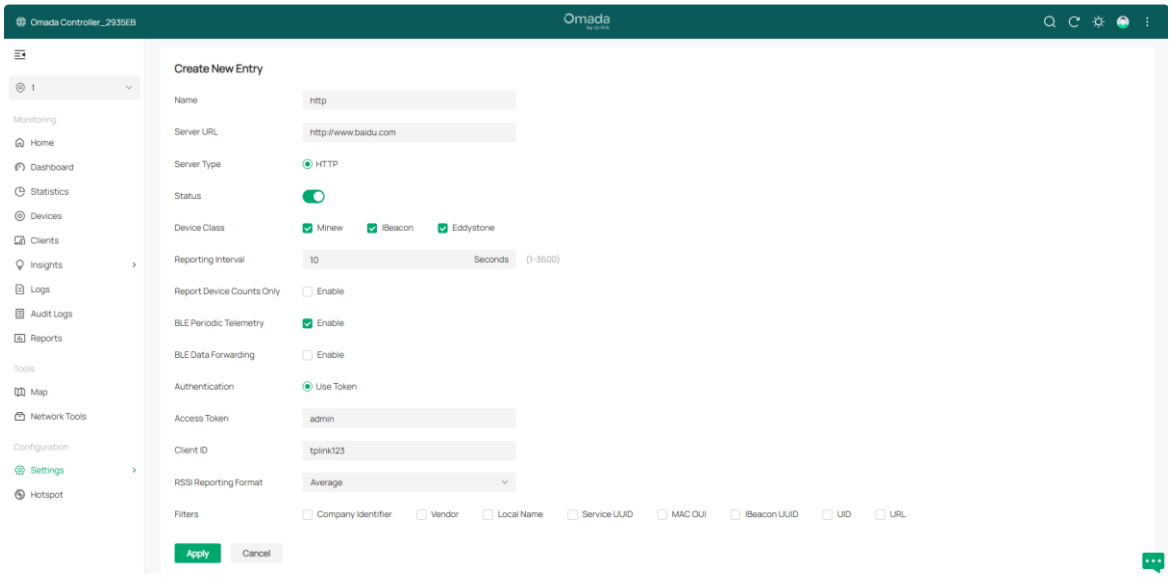


On this page, you can configure rules for the EAP to handle and report IoT data. The configuration is done at the Site level and does not require selecting specific devices. All configuration options will be effective for the wireless devices supported under the current Site, and device-level configuration overrides are not supported.

Parameter Explanation:

Aging Time: In the **General** section, configure the **Aging Time** to control the device aging time. If no data is received from a device within a certain period of time, the entry for that device will be deleted. As a result, the EAP will no longer forward data to the IoT server. If the AP receives data from that device again in the future, the device will be re-added, and its Bluetooth data will continue to be reported. The Aging Time can be configured in seconds, minutes, or hours.

Create New Entry: Click **Create New Entry** to configure the rules for the EAP to forward Bluetooth data. Up to 4 entries are currently supported.



Explanation:

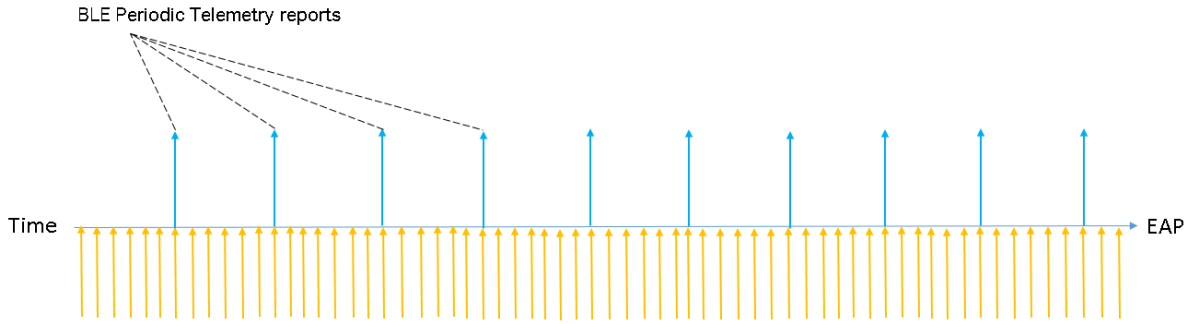
Item	Configuration
Name	Enter a name to identify the entry.
Server URL	Enter the url of the third-party IoT server. URLs with http as the prefix are supported.
Server Type	Only http is supported.
Status	Where to enable or disable the entry.
Device Class	The supported manufacturers and protocols, iBeacon, Eddystone, and Minew. Subsequent newly-supported IoT devices will require EAP firmware upgrades.
Reporting Interval	The reporting interval for the EAP to report IoT information. The shorter the interval, the better the real-time performance.

Report Device Counts Only	When enabled, the EAP will only report the number of Bluetooth devices. Enable this feature if you just need to know the number of Bluetooth devices around an EAP.
BLE Periodic Telemetry	Enabled by default. When disabled, the EAP will not periodically report IoT data.
BLE Data Forwarding	When enabled, APs will report the Bluetooth rawData to the server.
Authentication	Refers to the authentication method of the server. Access Token: Indicates the token used for identity authentication. Client ID: Indicates the ID used for identity authentication. Authentication information is used for server authentication and establishing secure communication with the server. A legal token needs to be generated on the management side of the IoT server. If it is not required by the server, you can leave it blank.
RSSI Reporting Format	Select the RSSI reporting format. There are five options: Average, Max, Last, Smooth, and Bulk. ● Average: Indicates the average RSSI value received during the reporting period. ● Max: Indicates the maximum RSSI value received during the reporting period. ● Last: Indicates the last RSSI value received during the reporting period. ● Smooth: Indicates the smooth value to remove exceptions. ● Bulk: Indicates the last 20 values received during the reporting

	period. If there are less than 20 values, all values will be reported.
Filters	Customize the filters for EAPs to filter IoT devices. ● Company Identifier: Filter devices based on their company identifiers. Only applicable to iBeacon devices. ● Vendor: Filter devices based on their vendors. ● Local Name: Filter devices based on their local names. Only applicable to Minew devices. ● Service UUID: Filter devices based on their Service UUIDs. Only applicable to Minew and Eddystone devices. ● MAC OUI: Filter devices based on their MAC prefixes. ● iBeacon UUID: Filter devices based on their iBeacon UUIDs. Only applicable to iBeacon devices. ● UID: Filter devices based on their UID Namespaces. Only applicable to Eddystone devices. ● URL: Filter devices based on the URL strings of the devices. Only applicable to Eddystone devices.

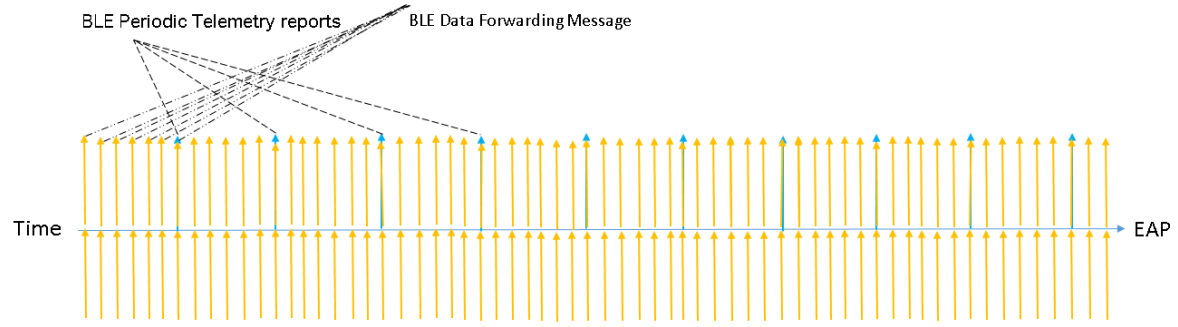
5.2.3 BLE Telemetry

BLE Telemetry is a configuration of periodic reporting. When it is enabled, the AP will periodically report Bluetooth data according to the set interval. The AP will continuously collect Bluetooth information, interpret the data, and then report it in the specified format.



5.2.4 BLE Data Forwarding

When BLE Data Forwarding is enabled, the AP will automatically forward the BLE advertising frames and scan response frames of the specified protocols that it has collected. The raw data received by the AP is forwarded in real time. Therefore, the forwarding frequency can also reflect the advertising interval of other Bluetooth devices. It should be noted that when BLE Data Forwarding is enabled, BLE Telemetry should also be enabled. If BLE Data Forwarding is considered as the primary mode, the reporting interval can be set higher. Furthermore, the Device Class selected in the IoT Transport Streams entry and the filter entry can also affect the data in Data Forwarding. The AP will filter the Bluetooth information based on these two filtering criteria before forwarding the data.



5.3 Parameter Optimization Recommendations

To achieve optimal Bluetooth performance, the following parameter optimization strategies are recommended:

1) EAP Distribution Strategy

Positioning accuracy: To maximize positioning accuracy, mount EAPs below 3 meters high, keep 3–15 meters between each, and ensure at least three EAPs receive each Bluetooth tag message.

Maximum positioning distance: The theoretical range is 100 meters, but the recommended maximum distance between EAPs and clients is no more than 50 meters.

2) Reporting Interval Parameter Configuration

1-10: For scenarios with high traffic volume or high real-time requirements.

10-60: For scenarios with medium traffic volume or moderate real-time requirements.

>60: For scenarios with low traffic volume or low real-time requirements.

5.4 Common Problems and Troubleshooting

Problem	Possible Cause	Troubleshooting
The parsed location information is null.	The Bluetooth client's communication protocol does not currently support parsing the information.	Enable BLE Data Forwarding to check if the transmitted data contains location information.
The positioning is inaccurate.	Severe interference.	Check the EAP location and transmit power configuration.
The location is updated slowly.	Long report interval and high EAP-server latency.	Verify the Report Interval configuration and the connection between the EAP and the server

6 Application Scenarios and Solutions

6.1 Indoor Navigation

When EAPs (BLE or Wi-Fi) are deployed at stores, tourist attractions, or parking lots, and users use a mobile phone with Bluetooth enabled or Wi-Fi connected, the positioning server can collect data from the EAP to calculate the location.

The management platform displays user density, itineraries, and other information. The positioning

server provides the location data to third-party applications, such as maps, through an open API, facilitating user location tracking.

6.2 Asset Location Management

By fixing the BLE tags on the assets to be tracked and deploying EAPs that can receive iBeacon frames in the office area, the EAPs can report the collected RSSI information to the positioning server, and the asset can be located and tracked through the mobile management application.

6.3 Personnel Management and Tracking

When the BLE tags are attached to the wrists of personnel or charges (such as patients) and EAPs that can receive iBeacon frames are deployed in the designated area, the EAPs can upload the collected information such as RSSI to the positioning server, allowing the management platform to monitor the collective location and movement trajectory of the personnel and charges.

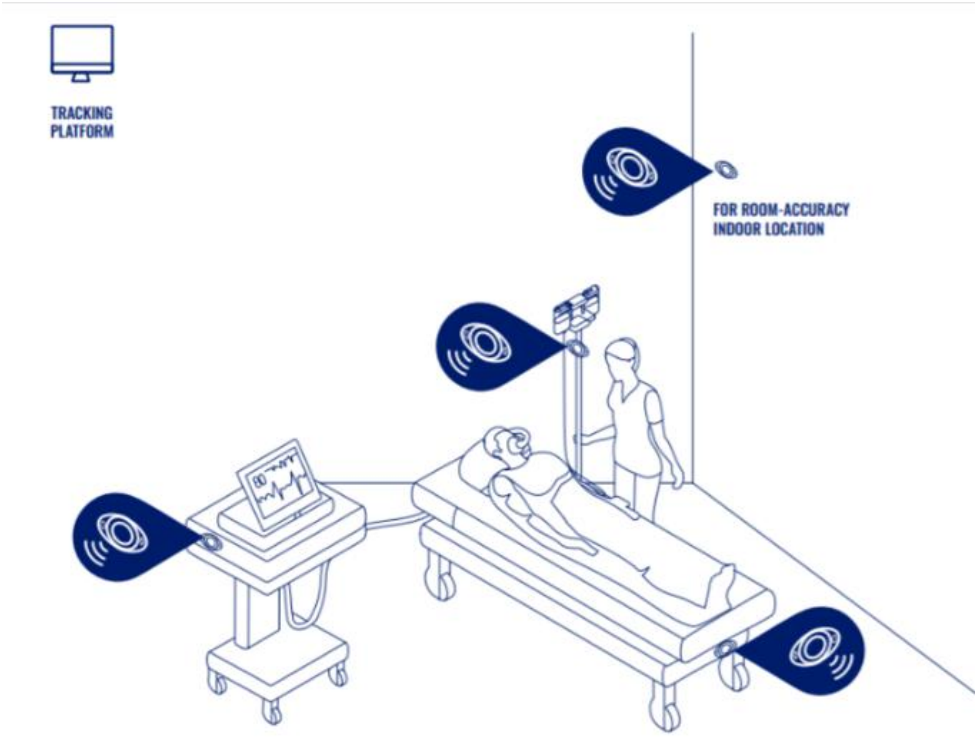
6.4 Geofencing

When employees attach the BLE tags to their wrists or users hold the mobile terminal, and EAPs are deployed in the working area, the positioning server can collect data, such as RSSI, from the EAPs to calculate the user location.

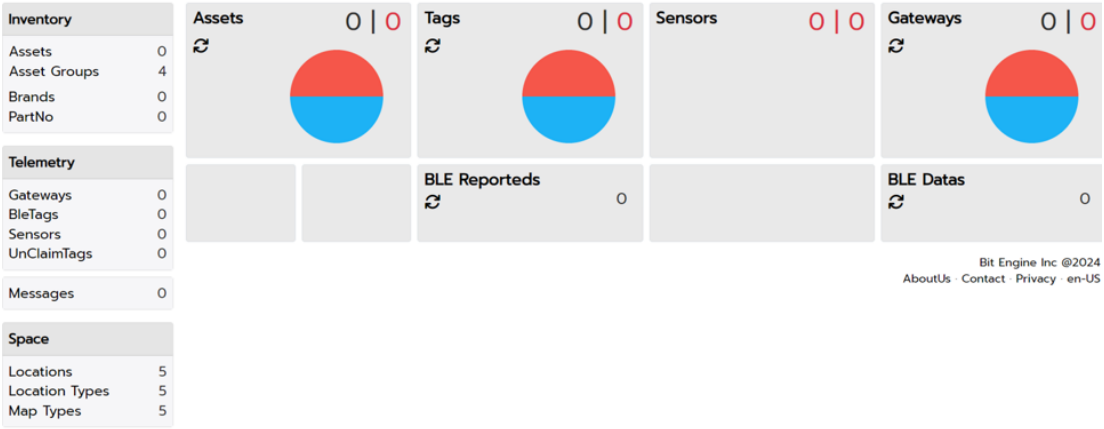
7 Case Studies

7.1 Case 1: Bluetooth IoT Deployment at a Thai Hospital

According to the client’s requirements, Bluetooth tags were deployed to position and manage critical supplies and assets based on the current WLAN deployment.

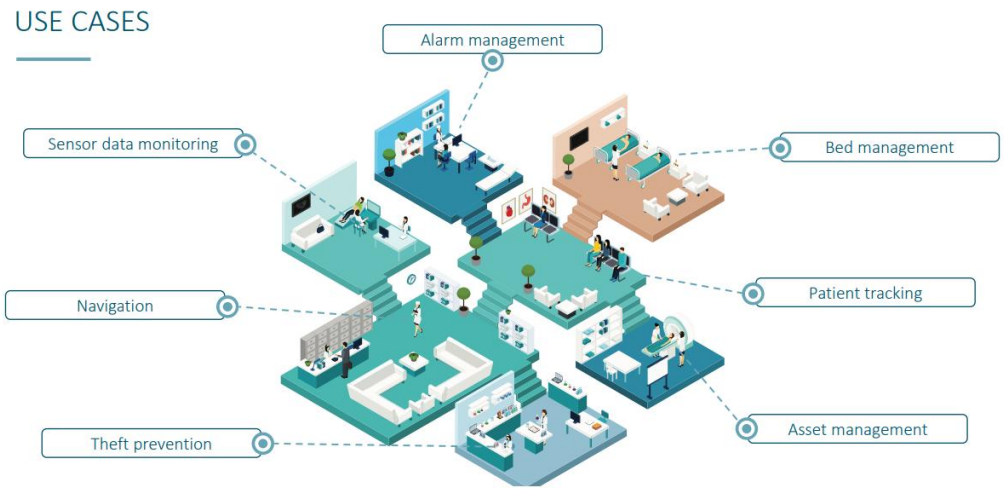


The EAP forwards the scanned BLE messages to the client server, which parses the information and displays it in a clear manner.



7.2 Case 2: Collaboration with a German Security Monitoring Company

The client uses EAPs to collect BLE information for real-time tracking and tracing. Application scenarios include alarm management, sensor data monitoring, navigation, anti-theft, bed management, patient tracking, and asset management.



7.3 Case 3: Collaboration with a Dutch Healthcare Technology Service Provider

The client also implemented a real-time location system (RTLS) via BLE. Application scenarios include healthcare, logistics, industrial, and retail.

8 Future Outlook

With the continuous development of technology and application scenarios, Bluetooth IoT technology is evolving and expected to improve in the following key aspects:

1) Technological Evolution: Pushing the Boundary Between Low Power Consumption and High Accuracy

Improved Positioning Accuracy

Bluetooth 5.4 and above achieve centimeter-level positioning accuracy through the AoA/AoD (Angle of Arrival/Angle of Departure) technology, providing optimized solutions for industrial asset

tracking and indoor navigation scenarios. Combined with firmware upgrades for the smart positioning system, existing devices can seamlessly adapt to high-precision requirements.

Multi-Protocol Integration

The integration of Bluetooth, Wi-Fi 6, UWB, and 5G is becoming a trend. For example, in smart homes, Bluetooth is responsible for connecting low-power sensors, while Wi-Fi handles high-bandwidth data streams, forming a hybrid architecture to meet diverse needs.

Low Power Optimization

Bluetooth 5.4 utilizes efficient energy management technology to further reduce device energy consumption. For instance, industrial sensors can achieve a battery life of more than ten years, driving the widespread use of edge computing devices.

2) Expansion of Application Scenarios: From Consumer to Global IoT

Consumer Electronics and Smart Homes

Shipments of dual-mode Bluetooth devices (Classic + Low Power) continue to grow. LE Audio-enabled TWS earbuds and AR/VR devices are rapidly gaining popularity, enhancing the audio experience. Smart home sensor networks utilize Bluetooth Mesh networking to enable whole-home automation, such as lighting, temperature, and humidity control.

Industry and Smart Cities

Factory equipment monitoring and warehouse logistics using RTLS rely on Bluetooth modules for efficient data exchange, with a compound annual growth rate exceeding 15%. In smart cities, direct Bluetooth and satellite connectivity (e.g., Hubble Network solutions) overcome coverage bottlenecks in remote areas and support global asset tracking.

Healthcare

Remote monitoring devices (e.g., blood glucose meters and ECG patches) utilize Bluetooth 5.3/5.4 for low-power data transmission, extending chronic disease management to home scenarios.

3) Challenges and Future Trends

Interference Prevention and Security Optimization

Congestion in the 2.4 GHz band requires intelligent frequency hopping algorithms (such as Bluetooth 6.0's enhanced CQM) and encrypted broadcast technology. By 2026, packet loss rates in complex environments are expected to drop below 0.1%.

Ubiquitous and Seamless Interactions

Bluetooth modules will become "invisible". By integrating flexible circuits into textiles, building materials, and other carriers, seamless environmental interaction will be possible. By 2030, "Bluetooth + Energy Harvesting" technology may enable over 50% of global consumer electronics to transition away from traditional batteries.

Trend Forecast

Global annual shipments of Bluetooth devices will reach 7.5 billion units in 2028, with a significant increase in the industrial and medical sectors. With the rise of the Ambient Internet of Things (Ambient IoT), Bluetooth modules will be embedded in more passive devices (such as electronic tags), enabling "sensing everywhere."

TP-Link will continue to invest in the research and development to promote innovation in BLE IoT technology and help our clients meet future IoT challenges.

9 Appendix

9.1 Glossary

Term	Explanation
BLE	Bluetooth Low Energy
IoT	Internet of Things
RSSI	Received Signal Strength Indicator, a measurement of wireless signal strength.

HTTP	HyperText Transfer Protocol, the most widely used application-layer protocol.
MQTT	Message Queuing Telemetry Transport, a lightweight, publish–subscribe communication protocol.
AMQP	Advanced Message Queuing Protocol, an application-layer protocol that supports multiple messaging models and offers a powerful feature set.