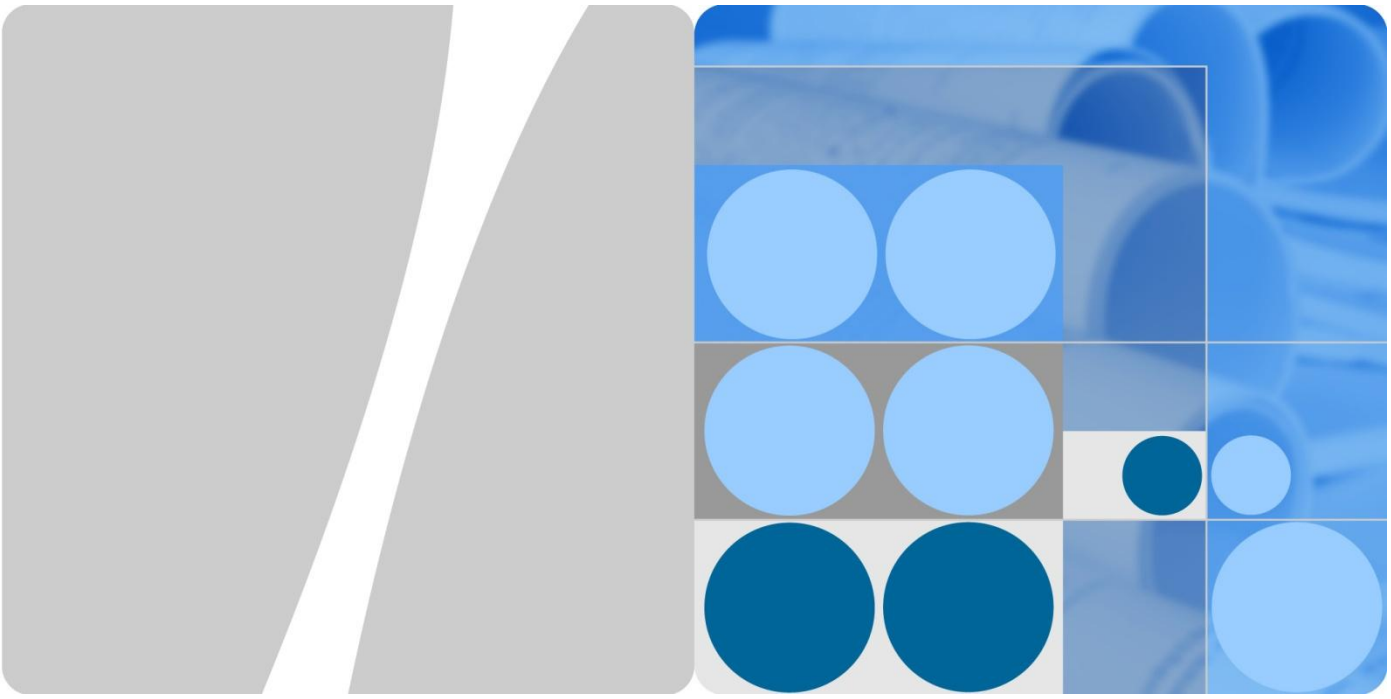


WLAN IoT AP Technology White Paper

Issue 1.0

Date 2016-08-04

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

Email: support@huawei.com

WLAN IoT AP Technology White Paper

Keywords:

IoT, Bluetooth, RFID, ZigBee

Abstract:

Internet of Things (IoT) APs provide Wi-Fi coverage and are equipped with Bluetooth modules. They use Mini PCI-E, USB, or Ethernet ports to establish IoT connections powered by the radio frequency identification (RFID), ZigBee, or other technologies. This document describes the fundamental principles of Huawei IoT APs and typical applications.

Acronyms and Abbreviations

Acronyms and Abbreviations	Full Name
AP	Access Point
AC	Access Control
RFID	Radio Frequency Identification
BLE	Bluetooth Low Energy
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance

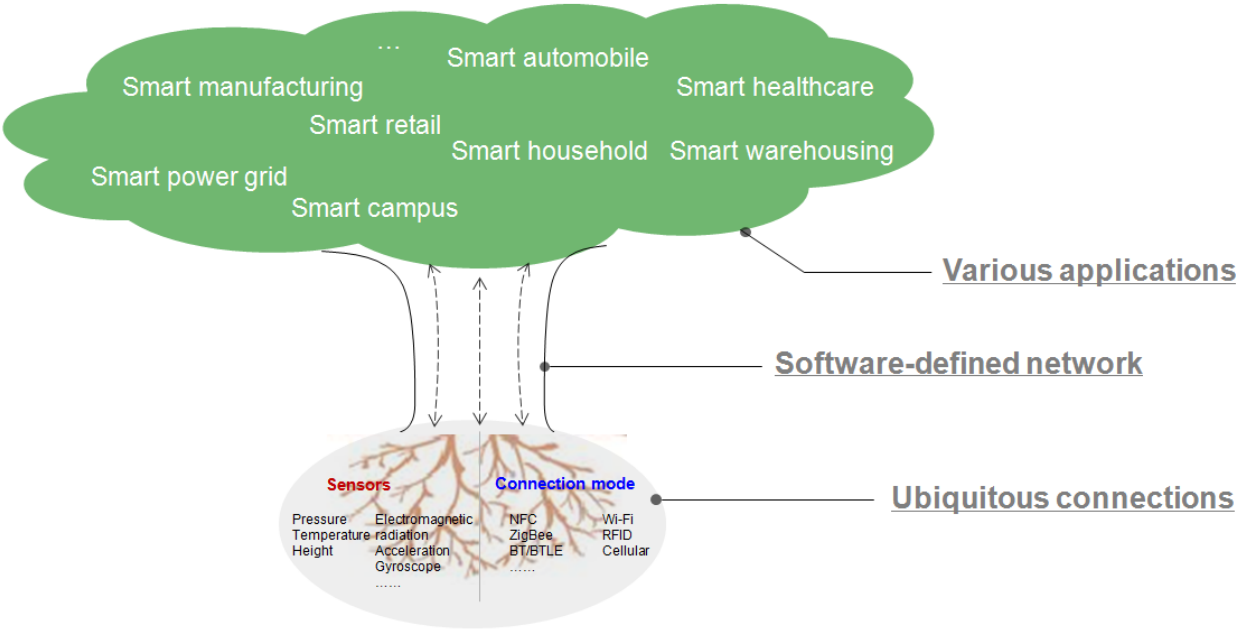
Contents

Figures

1 Background

IoT is known as the third information technology revolution and widely hailed as the Next Big Thing. In addition to automatic teller machines (ATMs), laptops, mobile phones, automobiles, and electricity meters, more and more devices are connected to the Internet through cellular network, Near Field Communication (NFC), RFID, Bluetooth, ZigBee, or Wi-Fi connections. Huawei predicts that there will be over 100 billion connected items by 2025 (excluding individual broadband subscribers). Everything can be connected anytime, anywhere. IoT is transforming how we work and live.

Figure 1-1 Key parts of IoT



In the IoT network, sensors obtain information in the physical world and then transmit the information to various smart applications for information processing and decision making through ubiquitous connections and software-defined networks. This process consists of three parts: information collection, information transmission, and information processing. After processing information, smart applications actuate devices in the physical world based on the processing results so that the controlled devices operate in the expected status. This phase is known as actuation. In the IoT network, connections play an important role. Network edge devices must support various connections, as in the following example.

In the smart education campus field, if wearable devices such as smart wrist watches and smart bands can be used in teaching and learning activities, they will bring a revolutionary change in teaching methodologies. The application of these smart devices and Big Data enables precise location, reverse teaching assessment, and user profile. However, wearable devices are usually connected to and controlled by personal smart phones or tablets through diversified wireless connections such as Bluetooth, ZigBee, and RFID. This necessitates an integrated access node for unified connection and control of these wearable devices. The integrated access node is also a key to the enterprise-level application of smart wrist watches and smart bands.

Huawei introduces IoT APs evolved from widely used mature Wi-Fi products to function as integrated access nodes to offer IoT connections such as Bluetooth, ZigBee, and RFID. A Huawei IoT AP is a shared site for a variety of IoT connections and provides data backhaul services for these IoT connections. It enables unified management of connected devices and features flexible expansion.

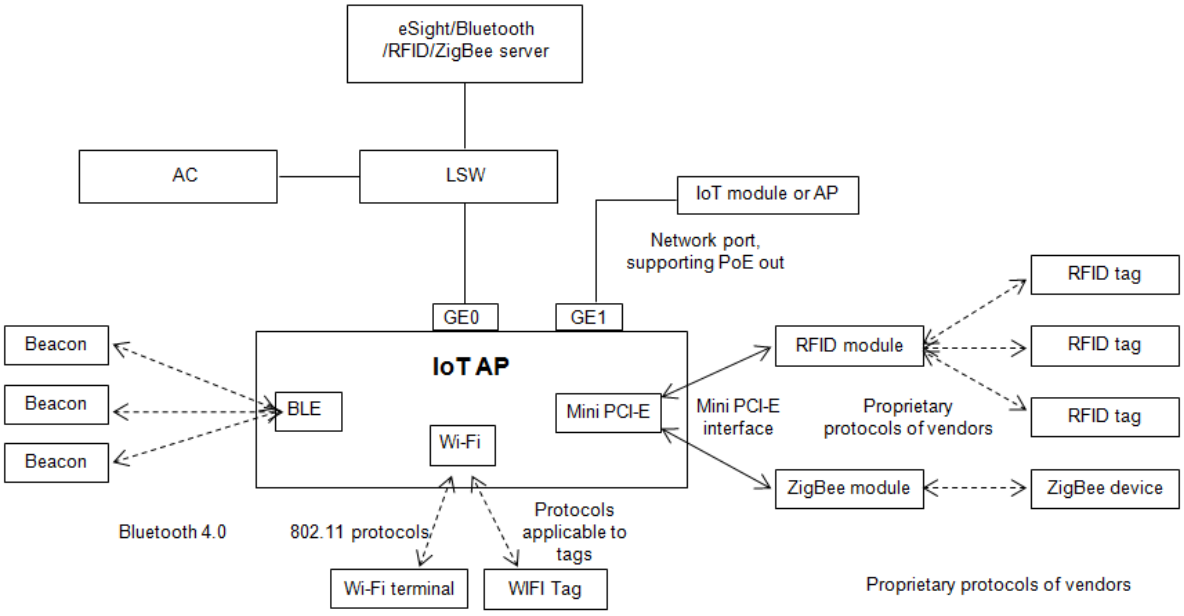
This document describes the fundamental principles of Huawei IoT APs and typical applications.

2 Technical Implementation

2.1 Implementation Architecture

Figure 2-1 shows the technical architecture of an IoT.

Figure 2-1 Technical architecture of an IoT AP



A Huawei IoT AP still has a Wi-Fi module to provide end users with Wi-Fi access services and also offer Wi-Fi tag location services. An IoT AP is also equipped with a Bluetooth 4.0 module to communicate with Beacons to offer location services. Moreover, an IoT AP is equipped with three standard Mini PCI-E slots, which can host IoT modules that comply with the Mini PCI-E interface standard. An IoT AP has two GE ports, one of which supports the PoE out function to supply power (less than 10 W) to 802.3af powered devices (PDs). IoT modules that support access through Ethernet interfaces can access IoT APs through Ethernet interfaces. IoT modules that access IoT APs through Mini PCI-E slots or Ethernet interfaces communicate with IoT terminal devices through proprietary protocols of vendors. IoT APs do

not need to comply with proprietary protocols of vendors. They only need to forward data processed by IoT modules.

Figure 2-2 Physical ports on an IoT AP (1)

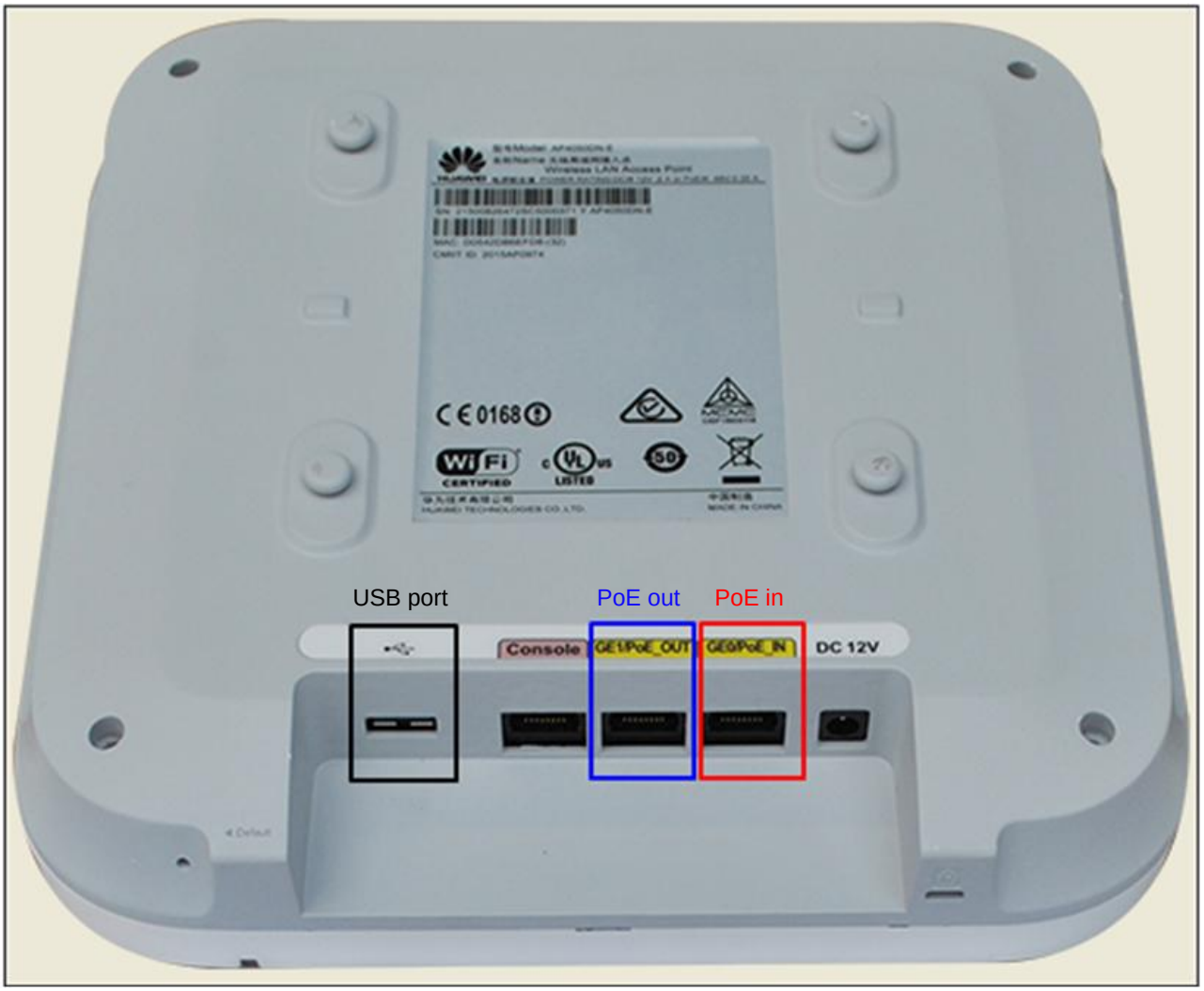
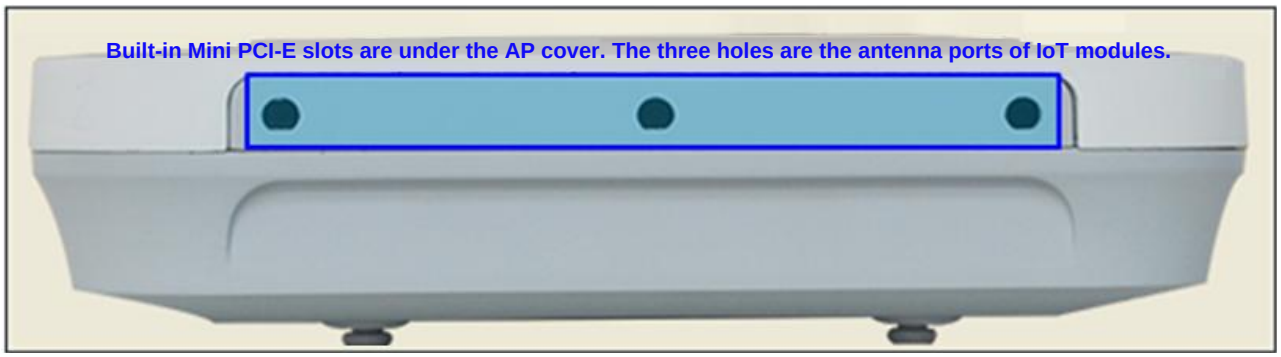


Figure 2-3 Physical ports on an IoT AP (2)



The previous figures show major ports on an IoT AP. The following table lists the purposes of these ports.

No.	Port	Quantity	Purpose
1	GE port	2	1. GE0 receives PoE power. 2. GE1 supplies PoE power (less than 10 W). 3. Both GE0 and GE1 can function as uplink network ports to connect the AP to an access switch and support trunk.
2	Mini PCI-E	3	1. They are standard Mini PCI-E ports, which are used to host IoT modules. 2. They are under the AP cover and can connect to IoT antennas.
3	USB	1	1. It is a standard USB 2.0 port (2.5 W power supply), which can be used to host USB-compatible IoT modules. 2. It can read data from or write data to USB flash drives.

2.2 Wireless Technology

IoT uses a variety of wireless connection technologies such as 2G, 3G, 4G, Wi-Fi, Bluetooth, RFID, ZigBee, and LoRa. These technologies vary with coverage distances, bandwidth, and operating frequencies. The following describes Bluetooth, RFID, and ZigBee technologies used in the IoT field.

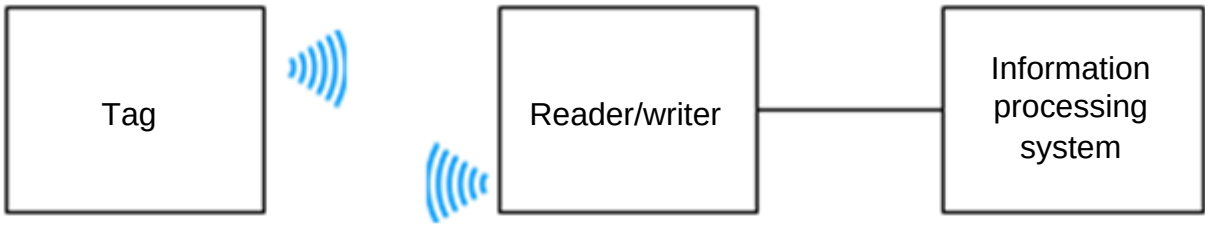
- RFID

  RFID uses radio frequencies to identify objects and can mark, register, store, and manage object information.

  An RFID system has three parts: tag, reader, and antenna.

  - A tag is comprised of an integrated circuit (called an IC or chip) attached to an antenna. It exchanges data with an RFID reader through radio waves.
  - A reader, also known as card reader, reads data from tags. Data can be written to an RFID reader/writer.
  - Antennas include tag antennas and reader antennas. Tag antennas are usually embedded in tags. Reader antennas can be embedded in readers or connected to antenna ports on readers through RF cables.

The following describes the information exchange process between the tag, reader, and information processing system.



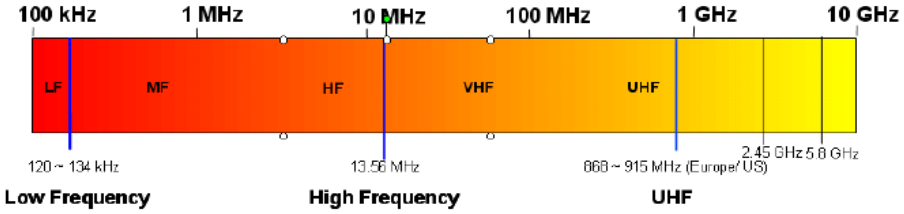
(1) The reader encodes the to-be-transmitted information to high-frequency carrier signals which are sent through antennas.

(2) Tags in the field of the reader receive the signals sent by the reader. Chips in the tags then perform voltage doubling rectification, demodulation, decoding, and decryption. After these actions, the chips check command requests, passwords, and rights.

(3) If the chips receive reading commands, they control logic circuits to read desired information from storage. After encrypting, coding, and modulating the information, chips send the information to the reader through tag antennas. After receiving the information, the reader demodulates, decodes, and decrypts the information and then sends it to the information processing system.

(4) If the tags receive write commands to modify information, the tags control logic circuits to instruct charge pumps in the tags to increase working voltages to erase E2PROMs and write information. If the tags determine that passwords or rights are incorrect, they return error information.

Tags and readers exchange information wirelessly, whereas readers and information processing systems communicate with each other through wired connections. In IoT APs, readers are in the form of built-in cards. They communicate with information processing systems through uplink Ethernet interfaces on IoT APs. Wireless connections between tags and readers usually work on low frequencies, high frequencies, or ultrahigh frequencies (UHFs).



(1) Low frequencies (120 kHz to 134 kHz): The technologies on this band are mature. Most RFID products in the market work on this band. The data size is small and the transmission speed is slow. The read range is less than 10 cm. Low-frequency RFID products are commonly used in access control devices and time and attendance systems.

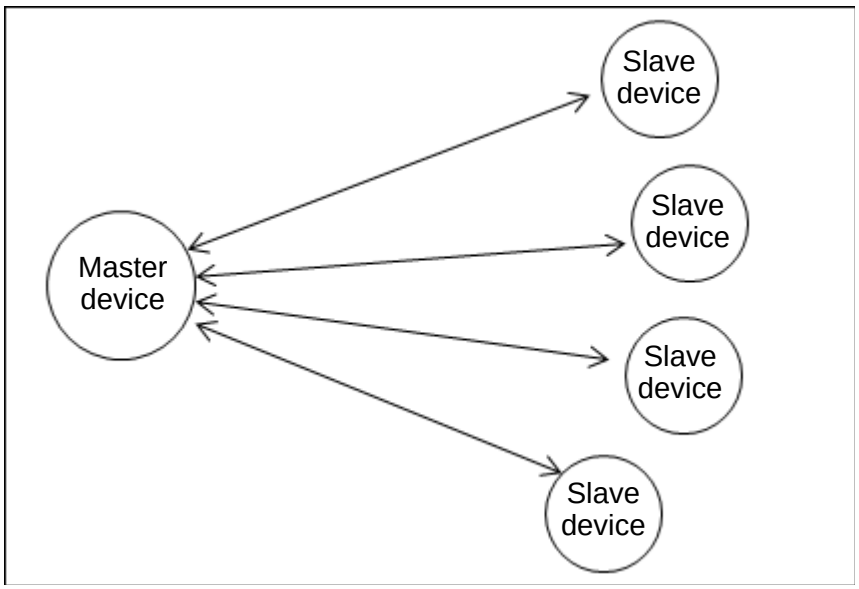
(2) High frequencies (13.56 MHz): The technologies on this band are mature. The market share of high-frequency RFID products is next only to that of low-frequency RFID products. High-frequency RFID products provide a higher transmission speed and longer read range (less than 1 m). They are often used in smart shelves and library management.

(3) UHF (860 MHz-960 MHz, 2.45 GHz, and 5.8 GHz): RFID products on these frequencies see a rapid development. The transmission speed is fast and the read range is long (3 m-50 m). Major application scenarios of RFID products on these frequencies are supply chain management (SCM) and logistics management.

- Bluetooth 4.0

  Bluetooth is one of the most widely used wireless technologies for short-range communications in the world. Bluetooth Special Interest Group (SIG) announced the formal adoption of the Bluetooth 4.0 Specification in July 2010. Bluetooth 4.0 introduces an outstanding technology Bluetooth low energy (BLE) while maintains the compatibility with classic Bluetooth technologies. Bluetooth 4.0 devices come in two flavors: single-mode and dual-mode. Single-mode devices only support BLE while dual-mode devices support BLE and classic Bluetooth technologies. BLE implements a star topology on which the master device manages connections and can connect to multiple slave devices. A slave device can only connect to one master device.

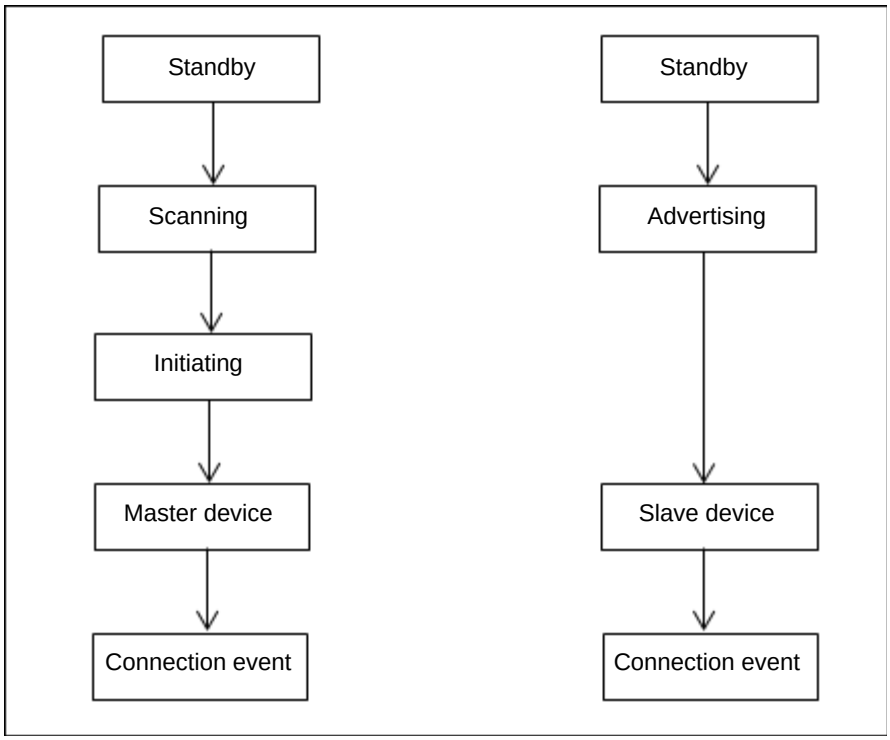
Figure 2-4 BLE star topology



The master and slave devices communicate with each other through wireless connections. In the IoT AP, the master device communicates with the Bluetooth server through the uplink network port on the AP. BLE operates on 40 channels in the 2.4 GHz band, and each channel has 2 MHz bandwidth. Three of these channels are fixed advertising channels, and the other 37 channels are data channels supporting frequency hopping.

Figure 2-5 shows the communication connection establishment between the master and slave devices. The process consists of the following major states.

Figure 2-5 Communication connection establishment between the master and slave devices



(1) Standby state: Devices in the standby state do not transmit or receive any data, and are not connected to other devices.

(2) Advertising state: Devices in the advertising state broadcast messages on the three fixed advertising channels (37, 38, and 39) at a specified interval. Broadcast messages are unidirectional messages. A device in the advertising state is known as an advertiser.

(3) Scanning state: Devices in the scanning state are listening for broadcast messages from the three fixed advertising channels (37, 38, and 39). A device in the scanning state is known as a scanner.

(4) Initiating state: During the initiating process, a scanner and an advertiser establish a connection. The scanner sends a connection request which contains the information about the channel and time. The advertiser accepts the connection request. The two devices enter the connection state. The scanner that initiates the connection is the master device, and the advertiser that accepts the connection request is the slave device.

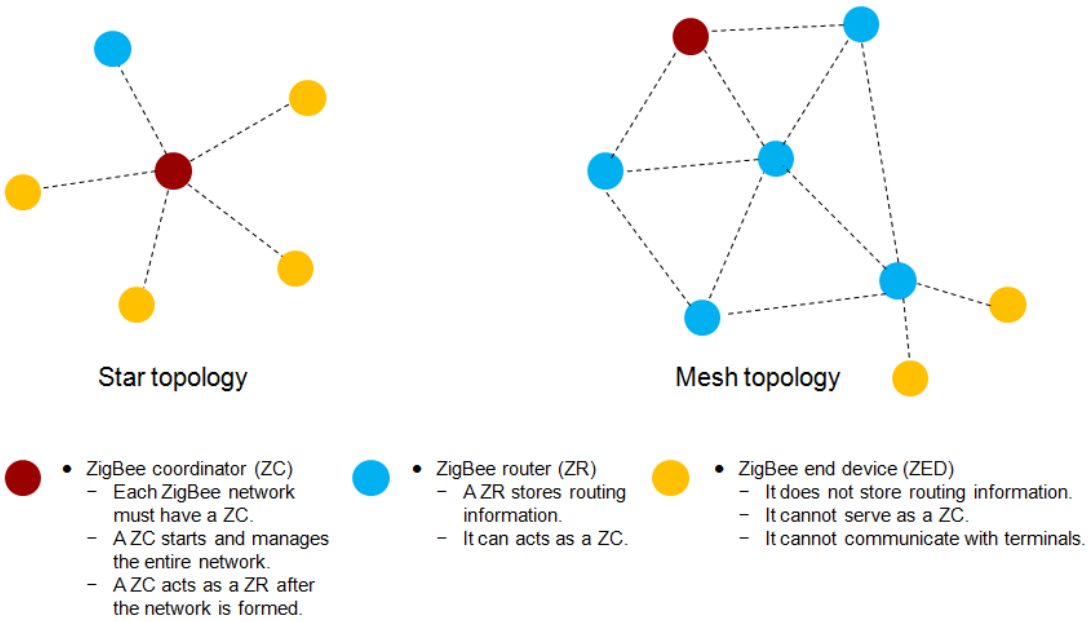
(5) Connection event: After the master and slave devices establish a connection, the communication between them is known as a connection event. The master and slave devices communicate with each other at a specified interval. During the communication, a frequency-hopping scheme is used for changing channels within channels 0 to 36.

The master and slave device can actively disconnect the connection in a connection event. After one end requests the disconnection, the other end must respond the disconnection request before the connection is disconnected.

- ZigBee

  ZigBee is a short-range wireless communication technology featuring low energy consumption, low transmission rate, and self-organizing. The ZigBee standard is released by ZigBee Alliance. ZigBee builds on the physical layer and media access control defined in IEEE standard 802.15.4. ZigBee supports three network topologies: star, mesh, and hybrid (star + mesh).

  Figure 2-6 ZigBee network topologies



  In a ZigBee network, there are three device roles: ZigBee coordinator (ZC), ZigBee router (ZR), and ZigBee end device (ZED). A ZC establishes and manages a network. After a network is established, the ZC also functions as a ZR. A ZR provides route information and controls the joining of other devices to the network. A ZED is not responsible for network maintenance.

  In a ZigBee network, these devices communicate with each other wirelessly. ZigBee devices operate in three bands: 868 MHz (Europe), 915 MHz (USA), and 2.4 GHz (global). These three bands provide 1, 10, and 16 channels respectively with different channel bandwidth, namely, 0.6 MHz, 2 MHz, and 5 MHz. ZigBee provides low transmission rates, that is, 250 kbit/s at 2.4 GHz, 20 kbit/s at 868 MHz, and 40 kbit/s at 915 MHz. Communications between ZigBee devices adopt the random channel access mechanism based on carrier sense multiple access with collision avoidance (CSMA/CA). Although the protocol defines two access mechanisms CSMA/CA and guaranteed time slot (GTS), ZigBee does not support GTS in practice, which is a time division multiplexing technology. ZigBee supports two routing algorithms: tree routing and mesh network routing. There are only two directions a frame can go in tree routing: up the tree or down the tree. No routing table is required, saving storage resources. However, routing is not flexible and routing efficiency is low. The mesh routing is a simplified version of the Ad hoc On-Demand Distance Vector (AODV) routing, which is applicable to ad hoc networks. A routing table must be maintained by a node, occupying storage

resources. It however provides the optimum routing efficiency and allows flexible application.

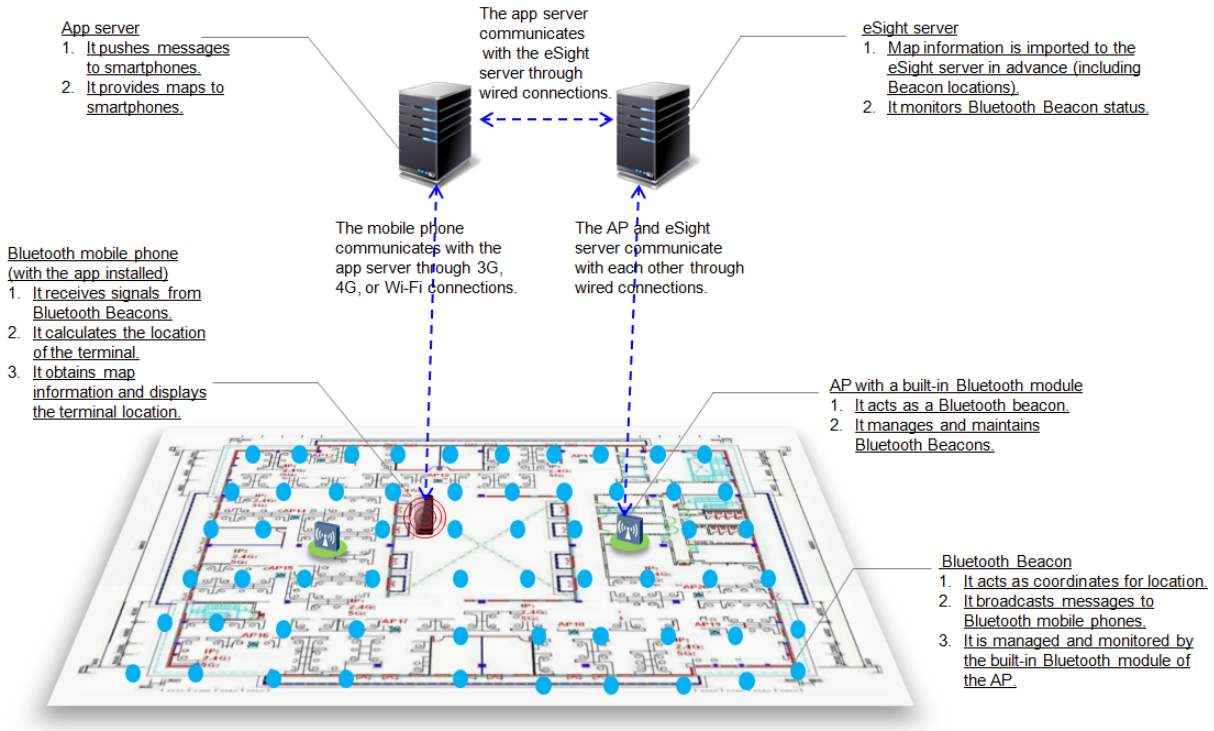
2.3 Bluetooth Location

Today, Bluetooth location is one of the most commonly used solutions in the indoor wireless location field. The benefits of Bluetooth 4.0 such as low energy and fast data transfer promote the wide use of Bluetooth 4.0 in message pushing and location.

Shopkick has deployed Bluetooth 4.0 shopBeacon devices in Macy's shops to provide automatic recommendation and shopping guide services based on customer locations. shopBeacon devices support BLE and can communicate with end devices within their coverage range to wake up business apps on mobile phones. When customers go shopping, they can receive discount information about commodities around them. If location and navigation functions are provided together with message pushing, customers will have a better experience. After customers receive discount information, their apps download the shopping mall map. Customers then can select and locate desired goods. Bluetooth location is the key for providing customers with this experience.

Bluetooth location adopts two location mechanisms: location calculation on a location server or on a terminal. In both of the two mechanisms, a location system usually is comprised of Bluetooth Beacons, APs with built-in Bluetooth modules, Bluetooth mobile phones, app servers, and location servers. The following takes the eSight location solution as an example to introduce the location solution that performs location calculation on terminals.

Figure 2-7 Bluetooth location solution built on eSight



- eSight location solution

  In the eSight location solution, Bluetooth mobile phones receive signals from nearby Bluetooth Beacons and use the three-point positioning and inertial navigation algorithms to calculate phone locations on the mobile phones.

  1. Beacons send signals.

     Bluetooth Beacons broadcast Beacon messages at a specified interval. A Beacon message carries the universally unique identifier (UUID) of a Beacon, major value, minor value, and calibrated RSSI value. The UUID is used to identify a Bluetooth Beacon. The major and minor values can be customized by Beacon owners. For example, a retailer can set the major value to region information and the minor value to the store ID. The calibrated RSSI value is the RSSI at the place 1 m away from the Beacon. It is used to calculate the distance based on the signal strength.

  2. Bluetooth mobile phones listen for signals.

     Bluetooth mobile phones listen for broadcast frames sent by Bluetooth Beacons to obtain Beacon UUIDs and RSSIs. Bluetooth mobile phones then can know the Bluetooth Beacons from which they can receive signals at current locations and the corresponding signal strength.

  3. Bluetooth mobile phones calculate locations.

     Bluetooth mobile phones calculate locations themselves. Before calculating locations, mobile phones must obtain the map information, including the location of each Beacon. The app uses the Beacon signal strength, Beacon locations, and inertial navigation information of the mobile phone sensor to calculate the location of the mobile phone.

     Throughout the process, the mobile phone app and app server communicate with each other through Wi-Fi, 3G, or 4G connections. The interactions between the mobile phone app and app server include message pushing, map information download, and location information upload. The map information is imported to the eSight server in advance, including the map model and Beacon locations. The app server obtains the map information from the eSight server through a wired connection.

- Functions of an IoT AP

  In the Bluetooth location solution, an IoT AP plays the following roles: (1) Its built-in Bluetooth module acts as a Bluetooth Beacon. (2) It manages and maintains Bluetooth Beacons.

  1. An IoT AP acts as a Bluetooth Beacon.

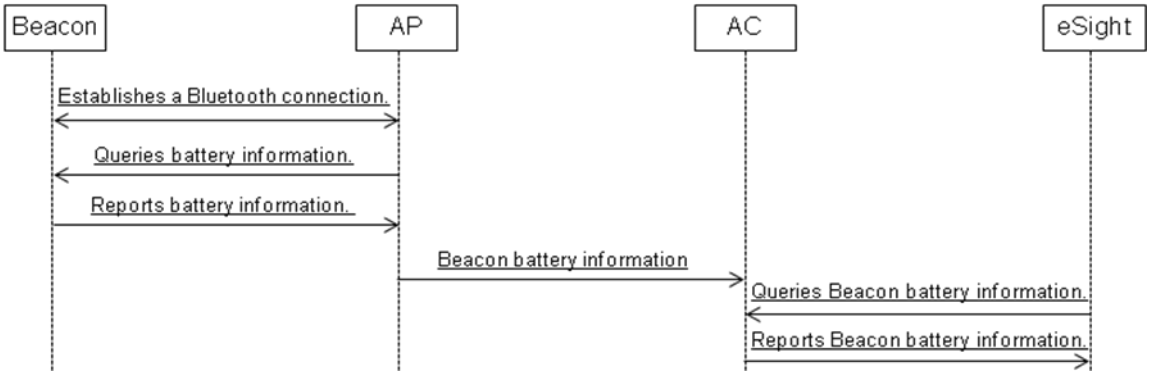
     The built-in Bluetooth module of an IoT AP can work in Bluetooth Beacon (slave device) mode or Bluetooth sniffer (master device) mode or in both modes simultaneously. If the required positioning accuracy is low and no independent Bluetooth Beacons are deployed, the built-in Bluetooth modules of IoT APs can act as Bluetooth Beacons to implement location.

  2. An IoT AP manages and maintains Bluetooth Beacons.

     (1) Obtaining battery information of Bluetooth Beacons

     APs obtain battery information of nearby Bluetooth Beacons in the morning everyday and report the information to the AC. eSight queries battery information of Bluetooth Beacons from the AC. The battery information of the AP's built-in Bluetooth module is always reported as 100%.

Figure 2-8 Obtaining battery information of Bluetooth Beacons

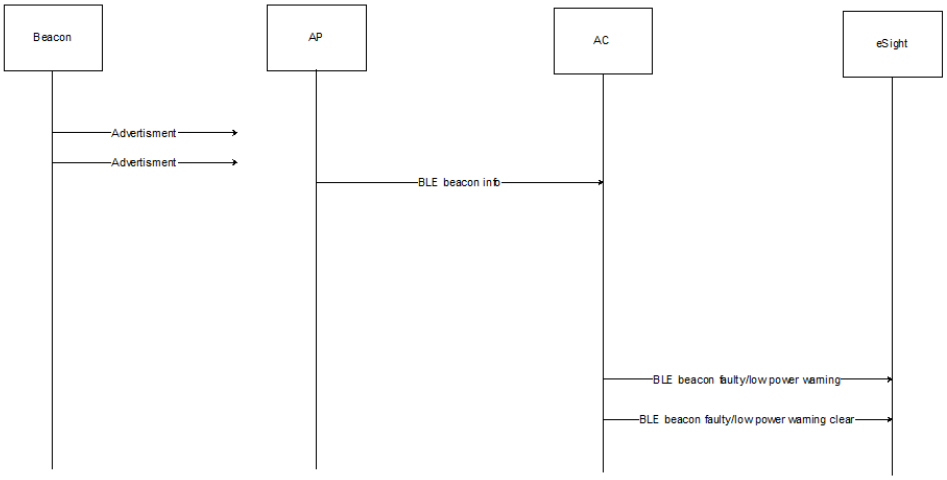


The previous figure shows the process for obtaining battery information of a Bluetooth Beacon. The Bluetooth Beacon must establish a connection event with the built-in Bluetooth module of the AP.

(2) Monitoring operating status of Bluetooth Beacons

The AP uses its built-in Bluetooth module to listen for broadcast packets from nearby Bluetooth Beacons. The AP then reports the information contained in the broadcast packets to the AC. The AC determines whether the Bluetooth Beacons work properly. If a Bluetooth Beacon is disconnected, the AC reports an alarm to eSight. After the Bluetooth Beacon restores, a report is sent to eSight to clear the alarm.

Figure 2-9 Monitoring operating status of Bluetooth Beacons



Criteria for the AC to determine whether a Bluetooth Beacon works properly are as follows: If a Bluetooth Beacon does not report any status update for 30 minutes, a Beacon disconnection alarm is reported. If the Beacon triggering the alarm reports a status update, the reported Beacon disconnection alarm is cleared.

An alarm is reported if the battery power level is low. If battery query results show that the battery power level of a Bluetooth Beacon is low, the AC reports an alarm to eSight.

(3) Delivering Bluetooth Beacon configurations

The WLAN system delivers Beacon device configurations sent by eSight. Configurations on the built-in Bluetooth module of an AP take effect locally. For the configuration of Bluetooth Beacons, users can use terminal apps of Beacon suppliers to configure Beacons during the deployment or they can complete the configuration on eSight and then deliver the configurations through the WLAN. Currently, the later mechanism is not supported.

- Interference between Bluetooth and Wi-Fi

  IoT APs working on the 2.4 GHz band may pose interference on Bluetooth systems that also operate on the 2.4 GHz band. The following measures can be taken to mitigate or avoid such interference.

  - Channels 1, 6, and 11 within the 2.4 GHz band are used for AP deployment if 2.4 GHz Bluetooth systems are in use on the live network. BLE devices perform broadcast services most of the time. The BLE protocol fixes the advertising channels to three 2 MHz wide channels, namely, 2402 MHz, 2426 MHz, and 2048 MHz. Its intention is to avoid overlapping with commonly used channels 1, 6, and 11 in WLAN systems whose center frequencies are 2412 MHz, 2437 MHz, and 2462 MHz.
  - The query for Bluetooth Beacon battery information is scheduled to be performed during off-peak hours. When an AP is to query Bluetooth Beacon battery information, it must establish a Bluetooth connection to the Bluetooth Beacon first. The air interfaces use the frequency-hopping on the 2.4 GHz band, which may cause conflicts with Wi-Fi networks.

    Therefore, the battery information query is scheduled at local 2:00 a.m. to avoid interference with Wi-Fi networks.

If the built-in Bluetooth modules of APs are enabled with Beacon broadcast services, interference between Bluetooth and Wi-Fi signals will occur even if channels are spaced apart because the distance between the Bluetooth antennas in the AP and the IoT AP antennas is short. Wi-Fi networks support clear channel assessment (CCA) to detect free channels, whereas Bluetooth does not support. Therefore, the performance of Wi-Fi air interfaces is impacted obviously. The analysis shows that the peak throughput of Wi-Fi networks deceases by 0.4% approximately.

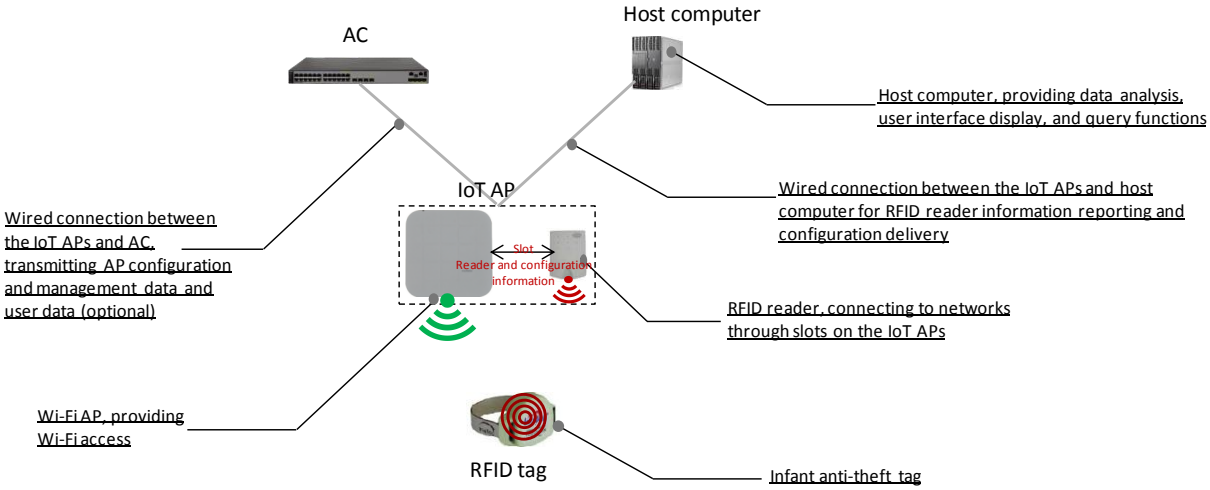
2.4 Infant Safety System Based on RFID

RFID is widely used in ID card and access control, supply chain and inventory tracing, vehicle tolling, anti-theft, production control, and assets management. Based on RFID, Enjoyor Co., Ltd. develops an infant protection system, enabling effective and reliable safety protection for newborns in hospitals. In this system, infants wear RFID tags that are harmless to human bodies, and RFID signal receivers are installed in the area to be controlled. A signal receiver constantly receives RF signals sent by the tags worn by infants and determines the tag status based on the received signals. Therefore, infant locations can be monitored and tracked in real time, and an alarm can be generated immediately if an infant is taken away by strangers. In conjunction with access control, the system is capable of preventing infant theft more efficiently.

Figure 2-10 shows the network architecture of the infant protection system. Information obtained by an RFID reader is reported to the host computer through IoT APs. In most cases, the host computer is a server that provides data analysis, user interface display, and query

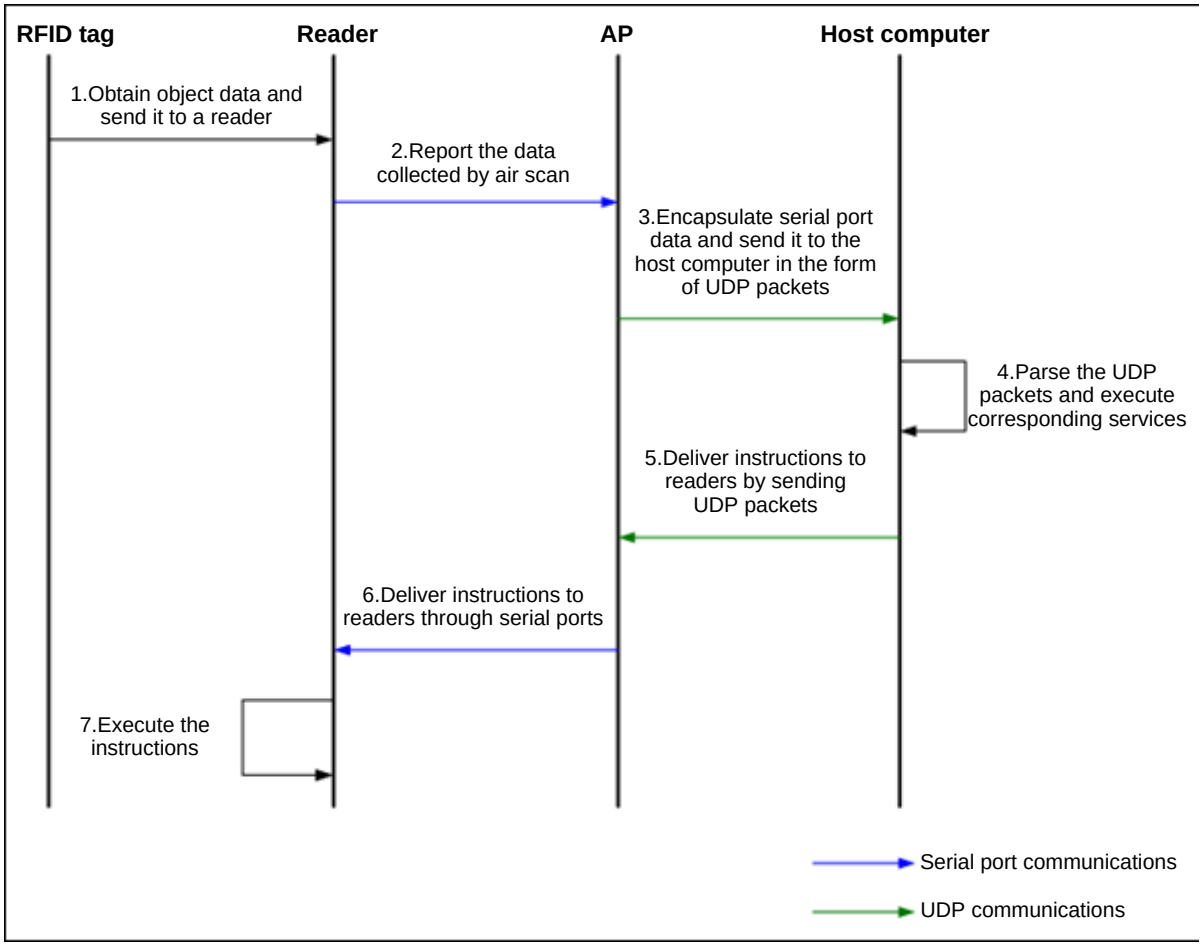
functions. IoT APs offer RFID reader slots and serve as information backhaul channels for readers. Additionally, the APs function as Wi-Fi APs and provide Wi-Fi access.

Figure 2-10 Architecture of the infant protection system based on RFID



On IoT APs, readers communicate with APs through standard Mini-PCI-E ports. IoT APs communicate with the host computer through Ethernet ports. Figure 12 shows the communications process for the tags, readers, APs, and host computer.

Figure 2-11 Communications process for RFID tags, readers, APs, and host computer



1. A tag obtains object data and sends it to a reader.
2. The reader reports the data collected by air scan to an AP through serial ports.
3. The AP encapsulates parameters into packets based on serial ports and sends the packets to the host computer in the form of UDP.
4. After receiving the packets sent by the AP, the host computer parses the packets and executes corresponding services.
5. The host computer delivers instructions to readers by sending UDP packets.
6. After receiving the UDP packets sent by the host computer, the AP extracts the data, differentiates slots based on the destination port numbers of Ethernet packets, and delivers instructions to readers through serial ports.
7. The reader executes the instructions delivered by the host computer.

3 Customer Benefits

1. Integrated access

   During wireless network deployment, the issues such as wireless site address selection, wired backhaul, and site power supply must be considered. When IoT networks using different wireless technologies coexist in one physical scenario, each wireless technology may configure the site address, backhaul, and power supply separately. This brings great challenges to deployment costs and workloads, as well as landscape works. Huawei IoT APs provide Wi-Fi coverage and other IoT connections, such as Bluetooth, RFID, and ZigBee, implementing integrated access of different technologies. In this solution, multiple wireless technologies can share the same site address, backhaul network, and power supply, significantly reducing costs, construction workloads, and damage to surrounding environments.

2. Unified management

   IoT APs gain benefits of unified management for users from the following aspects:

   (1) IoT and Wi-Fi can be implement on the same backhaul network through built-in Bluetooth modules of IoT APs or RFID/ZigBee modules connected to Mini PCI-E slots of the IoT APs. Only one wired network needs to be deployed and managed.

   (2) Unified site management: IoT sites can be unified by built-in Bluetooth modules of IoT APs and RFID/ZigBee modules connected to Mini PCI-E slots of the IoT APs. Only one physical site needs to be managed and maintained for different wireless technologies, including Wi-Fi, Bluetooth, RFID, and ZigBee.

   (3) Unified device management: Huawei eSight enables unified management on APs and IoT wireless modules. For example, in the Bluetooth location scenario, eSight manages and maintains APs and Bluetooth Beacons (including parameter configurations, power information, and online status monitoring) simultaneously.

3. Scalability

   In addition to Wi-Fi coverage and built-in Bluetooth modules, an IoT AP also provides various external ports, including one Ethernet port supporting the PoE out function, one USB port, and three Mini-PCI-E ports. These ports make networks scalable at various network construction phases. For example, in the early phase of network construction, only Wi-Fi coverage needs to be provided. When the number of users increases and new APs need to be added, an Ethernet port supporting the PoE out function can be used to connect to a new AP without deploying additional access switches. When the network develops to the IoT phase, the built-in Bluetooth module, external USB port, and three Mini-PCI-E ports on an AP provide multiple options on network technologies and scales. The physical ports on IoT APs have already been configured. However, due to the discrepancy in IoT modules between different vendors, software must be configured accordingly to achieve compatibility between different IoT modules.

4 Typical Applications

The IoT AP is a new AP type designed by Huawei for IoT scenarios. This type of APs realizes integrated access and unified management on different IoT technologies, and is also scalable. It applies to shopping mall IoT, healthcare IoT, and mining IoT scenarios.

4.1 Shopping Mall IoT

The iBeacon technology has been widely applied since it was released by Apple in September 2013. It is especially popular in the retail industry. When customers go shopping, they can receive discount information about commodities around them. In addition to message pushing, location and navigation applications of iBeacon are also emerging. Now Wi-Fi access has become a necessity of people's lives and is ubiquitous in shopping malls and supermarkets. If the two separate iBeacon and Wi-Fi networks can be combined, benefits such as integrated access and unified management are noticeable and construction workloads and damages to surrounding environments will be reduced.

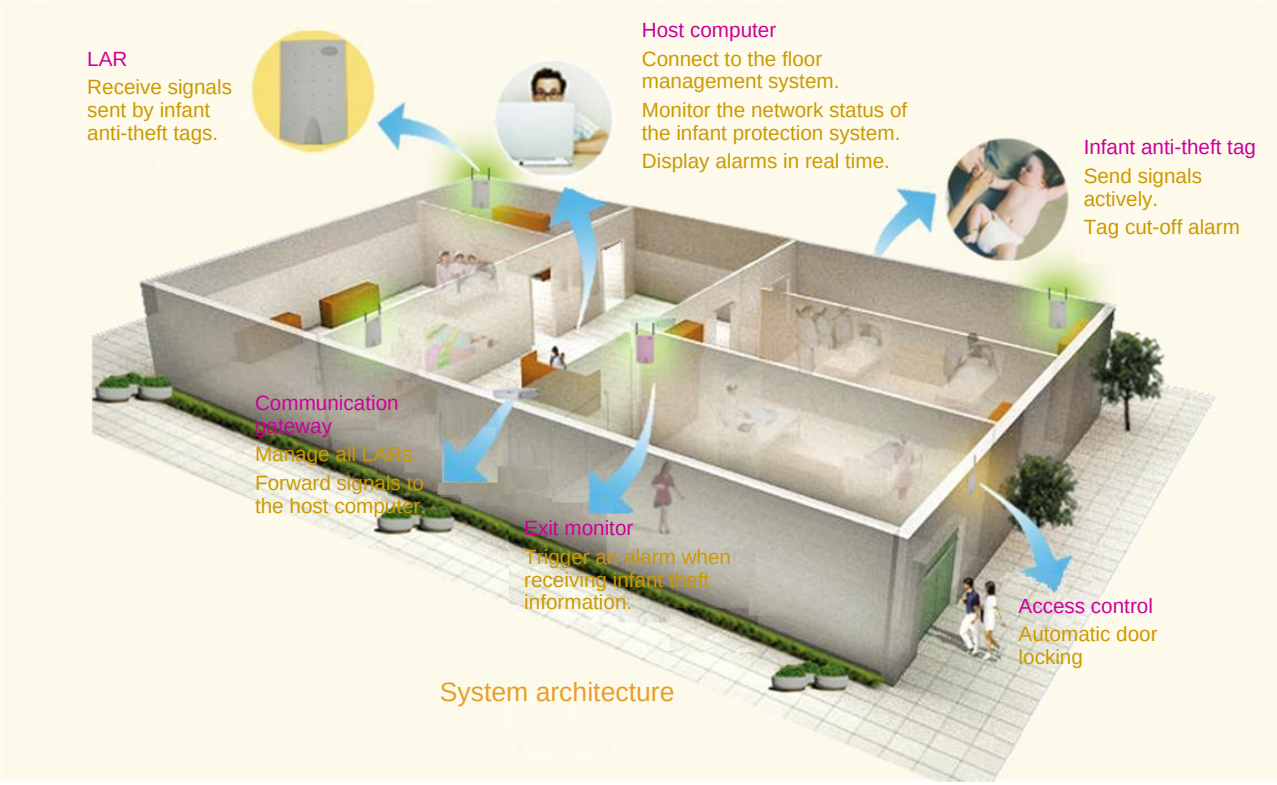
Figure 4-1 Vision of the shopping mall Beacon solution

IoT APs are the best choice to integrate these two networks. IoT APs provide 2.4 GHz/5 GHz Wi-Fi coverage for users to access Wi-Fi. Additionally, their built-in Bluetooth modules can be used as Beacons or used to manage other Bluetooth Beacons.

4.2 Healthcare IoT

Healthcare IoT is the core of future smart healthcare. Healthcare IoT combines all types of information sensing devices such as RFID devices, infrared sensors, global positioning system (GPS), laser scanners, and medical sensors with the Internet to achieve smart usage, information sharing, and interconnection of resources.

Figure 4-2 Enjoyor infant protection system



The infant protection system is a typical application of the healthcare IoT. In this system, infants wear RFID tags that are harmless to human bodies, and RFID signal receivers are installed in the area to be controlled. A signal receiver constantly receives RF signals sent by the tags worn by infants and determines the tag status based on the received signals. Therefore, infant locations can be monitored and tracked in real time, and an alarm can be generated immediately if an infant is taken away by strangers. In conjunction with access control, the system is capable of preventing infant theft more efficiently.

In the infant protection system, the external readers of IoT APs receive the RF signals sent by RFID tags. In addition, IoT APs provide 2.4 GHz/5 GHz Wi-Fi coverage, satisfying work requirements of hospitals. In the healthcare scenario, IoT APs bring benefits to customers through integrated access and unified management, as well as reduce the construction workloads and damages to surrounding environments.