



**Yrkes
Akademin**
Vi hjälper dig att lyckas!

Bluetooth

Communication Protocols

Bluetooth

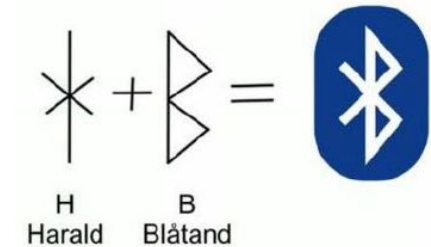
- ❖ A wireless technology used for exchanging data between devices
- ❖ One of the most popular short-range wireless communication standard
- ❖ Uses UHF radio waves in the ISM radio bands, from 2.400 GHz to 2.4835 GHz
- ❖ Used for building personal area networks (PANs)
- ❖ Originally developed as a wireless alternative to RS-232 data cables
- ❖ Initial development was done at Ericsson Mobile in Lund, in 1989
- ❖ The IEEE standardized Bluetooth as IEEE 802.15.1 in 2002
 - But no longer maintains the standard
- ❖ The [Bluetooth SIG](#) (Special Interest Group) maintains the development of Bluetooth
 - A global community of over 34,000 companies such as Ericsson, IBM, Intel, Nokia, and etc.



Bluetooth



- ❖ Named after the danish king Harald Blåtand (Bluetooth)
 - He was good at communication and was a king that united Denmark
 - The idea behind the technology was to unite communication
- ❖ There are different versions of Bluetooth

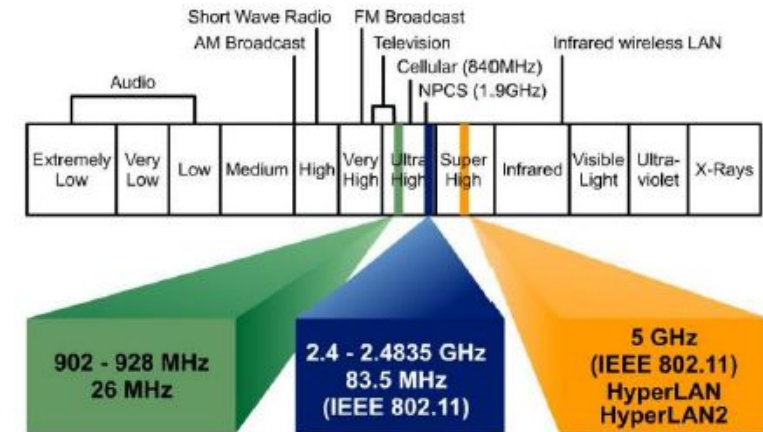


Bluetooth 1.x (1998-2003)	Bluetooth 2.x (2004 - 2007)	Bluetooth 3.0 + HS (2009)	Bluetooth 4.x (2010 - 2014)	Bluetooth 5.x (2016 - ...)
<ul style="list-style-type: none">- Base Rate: 1 Mbps- Max Range: 10 m- Latest version: v1.2	<ul style="list-style-type: none">- Enhanced Data Rate<ul style="list-style-type: none">- Up to 3 Mbps- Max range: 10 m- Secure Simple Pairing- Latest version: 2.1 + EDR	<ul style="list-style-type: none">- High Speed mode- Bluetooth v3.0: 3 Mbps- Max range: 10 m- HS Max rate: 24 Mbps- Transmission over WiFi (802.11) connection.- Bluetooth is only used to establish and manage a connection	<ul style="list-style-type: none">- Bluetooth v4.2: 1 Mbps- Up to 24 Mbps- Up to 50 m- BLE introduced- Improved privacy to prevent tracking- Almost a new technology- Categories: classic, high-speed, and low-energy- Latest version: v4.2	<ul style="list-style-type: none">- 2x speed, 4x range<ul style="list-style-type: none">- Up to 48 Mbps- Up to 200 m- Select bands with less interference- Forward Error Correction- Needs new hardware

Classic Bluetooth



- ❖ Uses ISM (Industrial, Science and Medical) radio bands
- ❖ Frequency ranges: 2400MHz – 2483.5MHz
 - Power Constrained
 - License free and free to use
 - Coexistence: WLAN(802.11), Zigbee(802.15.4), ...
 - Bluetooth divides the bandwidth into 79 channels
 - Each channel has a bandwidth of 1 MHz
 - Guard bands 2 MHz at the bottom end and 3.5 MHz at the top
 - Bluetooth divides data into packets, and transmits each packet on one of 79 channels
- ❖ Uses Frequency Hopping technology
 - A technology that spreads the signal over rapidly changing carrier frequencies
 - Data is sent on multiple radio spectrums

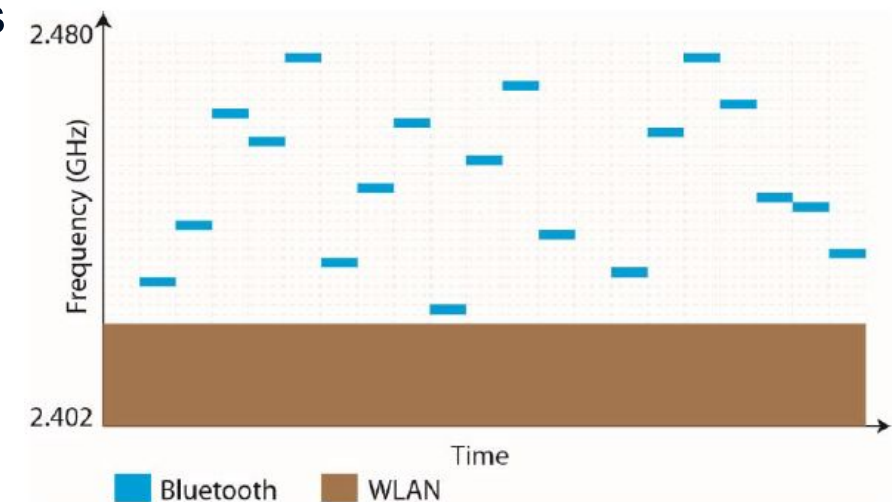


Classic Bluetooth



- ❖ Frequency Hopping / Adaptive Frequency Hopping and Time slots
 - Bluetooth changes the frequency of the data signal 1600 per second
 - Adaptive FH can detect the used spectrum bandwidth and avoid interference
 - Uses TDMA and each slot length is 625 μ s
- ❖ The transmit power, and range of a Bluetooth module is defined by its power class
- ❖ A module can operate in one or more power classes

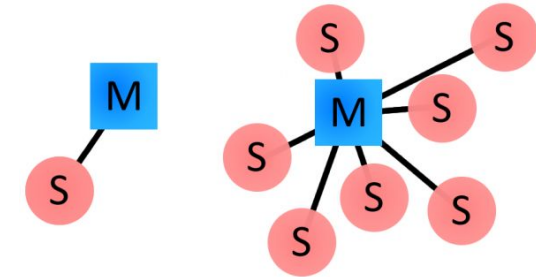
	Max. Output Power	Max. Range
Class 1	100 mw	100 m
Class 2	2.5 mw	10 m
Class 3	1 mw	1 m



Classic Bluetooth



- ❖ Is a packet-based protocol
 - Every packet is an independent transaction
- ❖ Master/slave architecture in classic Bluetooth
 - Any slave in the network can only be connected to a single master
 - The slaves can not communicate to each other
- ❖ A master can communicate with up to seven slaves in a network
 - Slaves get synchronized to the master clock
 - The master's transmission begins in even slots and the slave's in odd slots
- ❖ Every Bluetooth device has a unique 48-bit address (BD_ADDR)
 - Follows same pattern as LAN MAC addresses
- ❖ Bluetooth devices can also have user-friendly names (up to 248 bytes long)



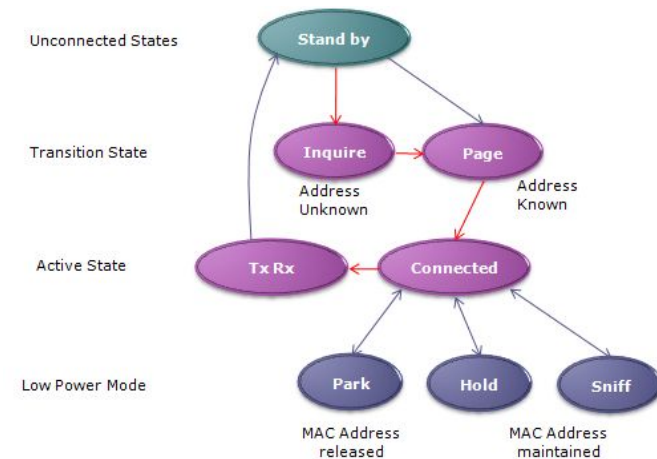
Classic Bluetooth



❖ Connection Process: A multi-step process involving three progressive states

- **Inquiry** - devices discover each other
- **Paging** (Connecting) - process of forming a connection
- **Connected** - After completing the paging process

- **Active Mode** - The normal mode
 - The device actively transmitting or receiving data
- **Sniff Mode** - A power-saving mode
 - The device sleeps and only listens to transmissions at a set interval (e.g. every 100ms)
- **Hold Mode** - A temporary power-saving mode
 - The device sleeps for a defined period and then returns back to active mode
 - The master can command a slave device to hold
- **Park Mode** - The deepest sleep mode
 - A master can command a slave to park
 - The slave will become inactive until the master command it to wake back up



❖ Bonding and Pairing

- Bonds are created through a one-time process called pairing
- Pairing is a form of information registration for connected devices
 - They share their addresses, names, and profiles, and usually store them in memory
 - They also share a common secret key, which allows them to bond in the future
- Pairing usually requires an authentication process; e.g. entering a PIN code
- Bonded devices automatically establish a connection whenever they're close enough

❖ Bluetooth Profiles

- Additional protocols, built upon the basic Bluetooth standard
- More clearly define what kind of data and application a Bluetooth module is transmitting
- For two Bluetooth devices to be compatible, they must support the same profiles
- E.g. Serial Port Profile (like RS-232 and UART), Human Interface Device (like keyboards), FTP ...

Classic Bluetooth - Summery



- ❖ Reliable - transmissions are based on connected link
- ❖ Relatively high speed, especially with EDR
 - Suitable for applications which require high data rate and stability
 - Music / File / Voice
- ❖ High Power Consumption
 - To perform high speed transmission
 - To maintain the Link
- ❖ Supports Asynchronous Connection-Less (ACL) transmission
 - Used for general data packets which are transmitted at irregular intervals
- ❖ Synchronous Connection-Oriented (SCO) transmission
 - Used for voice data. Each device transmits encoded voice data in the reserved timeslot.

Bluetooth Low Energy - Key Features

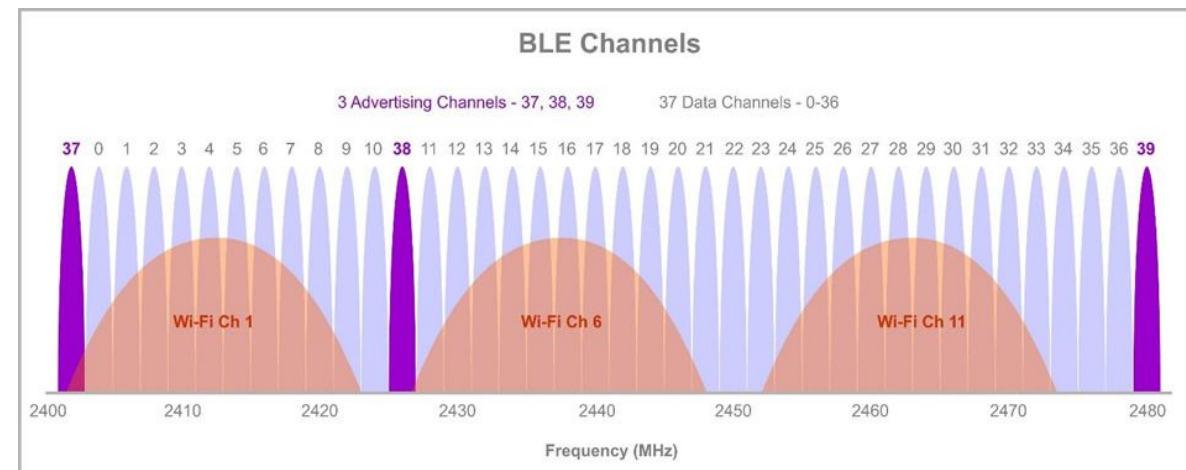


- ❖ A Wireless Personal Area Network technology
- ❖ Low power protocol (1 year on coin cell battery)
 - For applications with low power requirements; e.g. IoT, mobile phones, tablets and etc.
- ❖ Maintain connection for long time (3 ms vs. 0.625 ms)
- ❖ Stateless protocol (every request is an independent transaction)
- ❖ Shorter connecting time (6 ms vs. 100 ms)
- ❖ Max. Range: less than 100 m
- ❖ Max. data rate: 1 Mbps
- ❖ Small size and low cost
- ❖ Flexibel topology

Bluetooth Low Energy - Bands and Channels



- ❖ Uses ISM radio bands (2.400–2.4835 GHz)
 - Divided in 40 RF Channels with 2 MHz spacing
 - 3 Advertising Channels
 - Device discovery
 - Connection establishment
 - Broadcasts
 - Selected to minimize interference
 - 37 Data Channels
- ❖ Uses Adaptive Frequency Hopping
 - To detect used band to avoid interference
 - Regular Hopping Sequence with given intervals



Bluetooth Low Energy - GAP Roles



- ❖ All BLE devices use a GAP (Generic Access Profile) to
 - Define device roles, network topology, discovery process, device management, security and connection process between BLE devices.

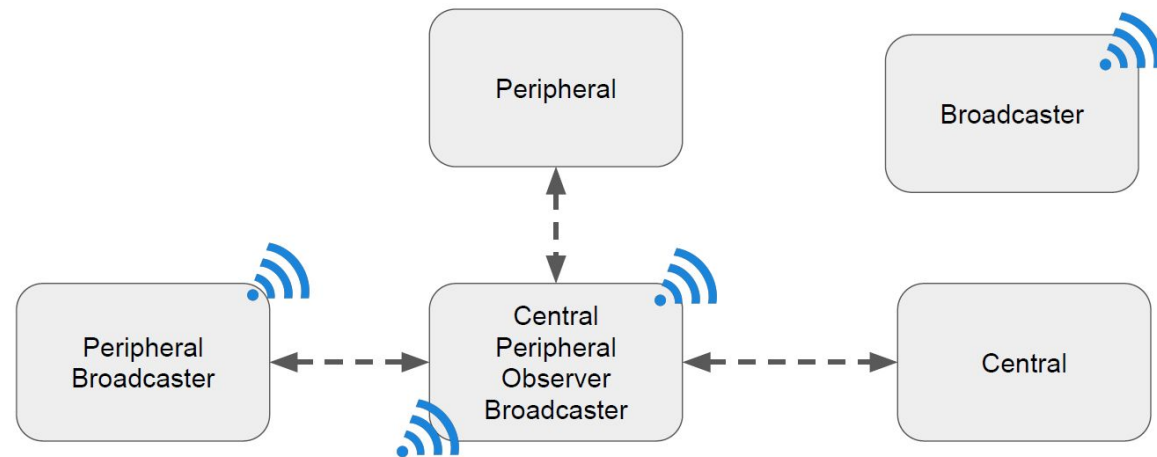
- ❖ The GAP defines four roles:

- **Broadcaster** (Transmitter only)

- Can only advertise
 - Sends only advertising packets
- Can be discovered by observers
- Cannot be connected

- **Observer** (Receiver only)

- Scans for broadcasters and reports the information to an application.
- Can only send scan requests, but cannot be connected.



Bluetooth Low Energy - GAP Roles



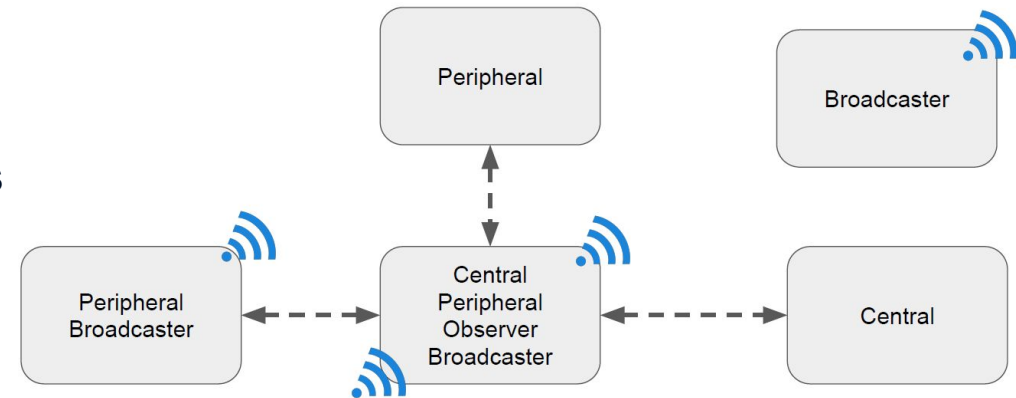
❖ The GAP defines four roles:

➤ **Peripheral** - A device that

- Advertises connectable advertising packets
- Becomes a slave once it gets connected.

➤ **Central** - A device that

- Initiates connections to peripherals
- Becomes master when connections are established
- Supports multiple connections



❖ A BLE device may support multiple roles

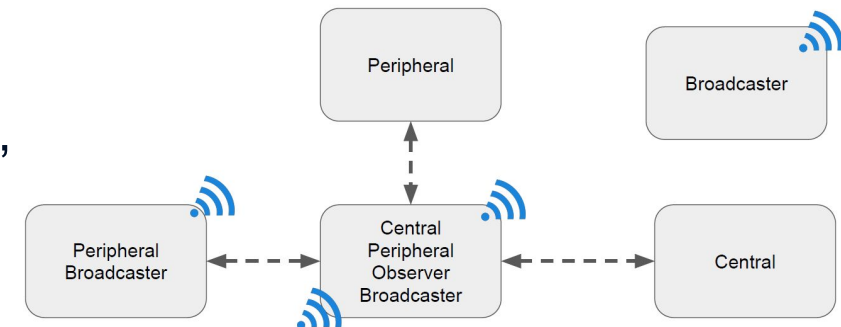
❖ Each BLE device has a unique 48 bit address which can be

- Private: Is static but can be changed after power cycle
- Public: Follows the same pattern as MAC addresses; Obtained from IEEE

Bluetooth Low Energy - Advertising (Broadcasting)



- ❖ Reporting data / advertisement
- ❖ There are three advertising channels
 - Transmit on all advertising channels each connection interval
- ❖ Configurable; channel / power / time interval
- ❖ A central node can request data via “Scan request”
 - Receives a “Scan response”
- ❖ Supports multiple Scan request - scan response
 - Request more data without initiating a new connection
- ❖ BLE devices are detected on broadcasting advertising packets
 - A scanner listens to the advertising channels intervally

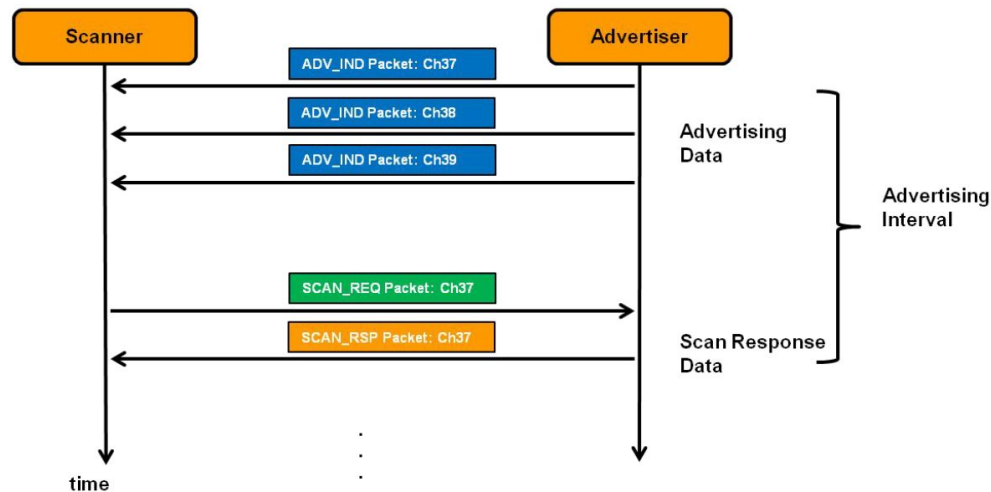


Bluetooth Low Energy - Scan and Discovery

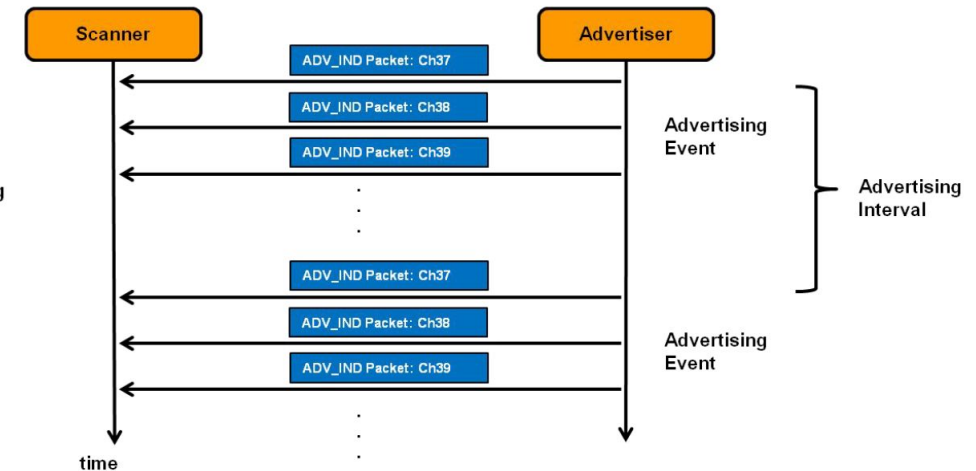


- ❖ Passive Scan
- ❖ Active Scan
 - SCAN_REQ: “I want more information”
 - SCAN_RSP: “More information as you wish”

BLE Active scanning



BLE Passive scanning

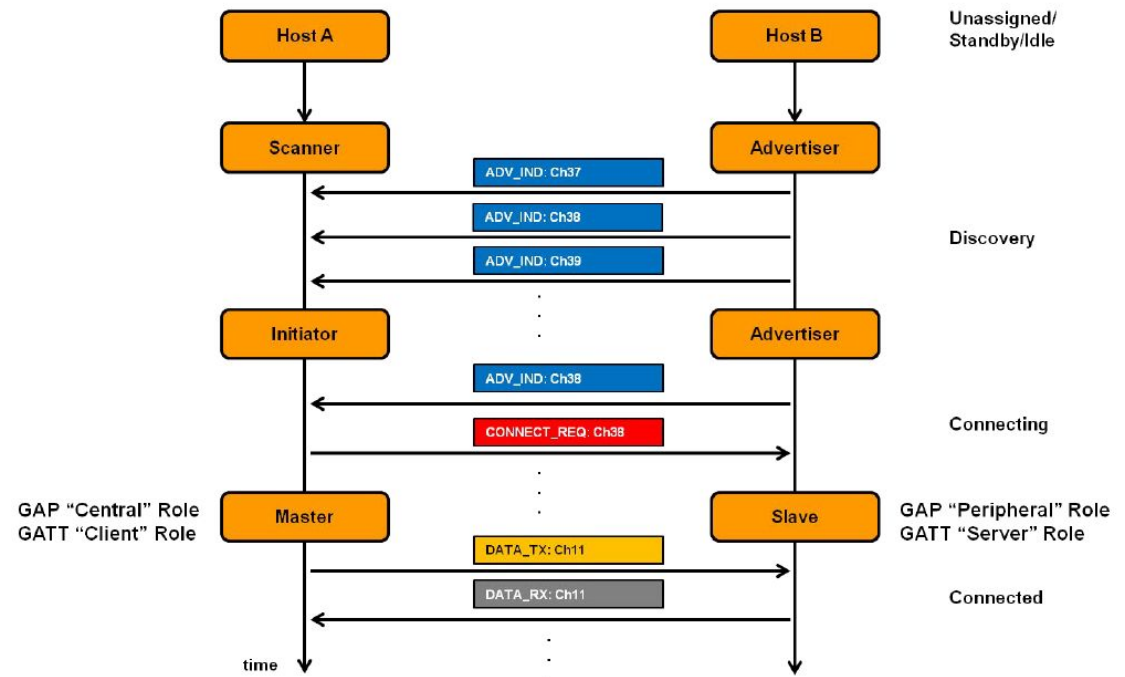


Bluetooth Low Energy



❖ Scan and Connect

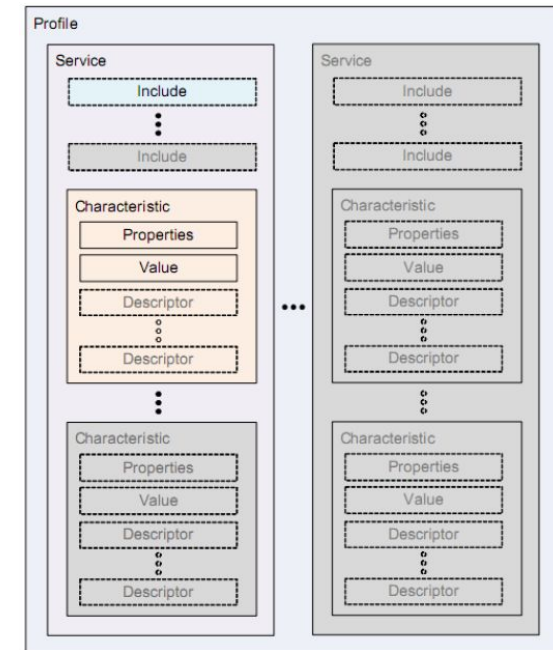
- CONNECT_REQ: “OK, let’s connect”
 - “Follow these parameters:”
- Connection Interval (7.5ms – 4s)
- Connection Timeout (100ms – 32s)



Bluetooth Low Energy - Software Model



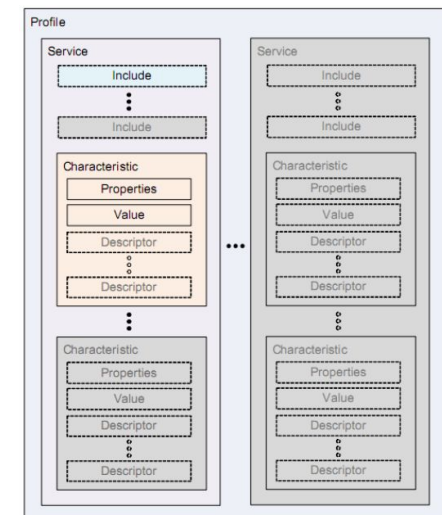
- ❖ BLE devices use Generic Attribute Profiles (GATT). A GATT
 - Describes an application
 - Is a collection of services; defined by Bluetooth SIG or the customer
- ❖ **Client:** A device that initiates GATT commands and requests, and accepts responses. For example, a computer or smartphone
- ❖ **Server:** A device that receives GATT commands and requests, and returns responses. For example, a temperature sensor
- ❖ **Characteristic:** A data value transferred between client and server
 - For example, the current temperature.
- ❖ **Service:** A collection of related characteristics, operate together to perform a particular function.
 - For example, the **Health Thermometer** service includes characteristics for a temperature measurement value, and a time interval between measurements.



Bluetooth Low Energy - Software model



- ❖ **Descriptor:** A descriptor provides additional information about a characteristic
 - For example, a temperature value characteristic may have
 - An indication of its units (e.g. Celsius), and
 - The maximum and minimum values which the sensor can measure.
 - Optional – each characteristic can have any number of descriptors.
- ❖ Services may also include other services as sub-functions;
 - The main functions of the device are so-called primary services
 - The auxiliary functions they refer to are secondary services
- ❖ BLE Identifying applications
 - Services, characteristics, and descriptors are collectively referred to as attributes, and identified by 128 bits UUIDs (Universal Unique Identifier)



Bluetooth Low Energy - Software model

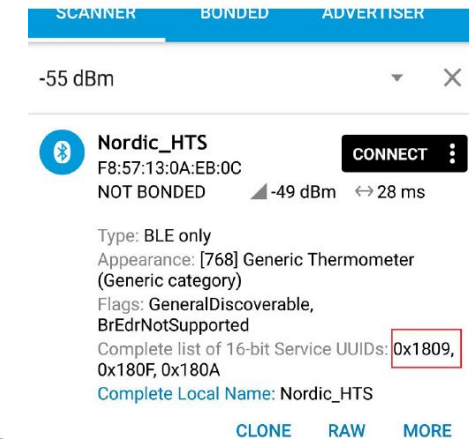


❖ BLE Identifying applications ...

- Broadcasted on advertising channels
- A random or pseudo random UUID can be used for private use
- The Bluetooth SIG have reserved a range of UUIDs (of the form xxxxxxxx-0000-1000-8000-00805F9B34FB) for standard attributes
 - For efficiency, these identifiers are represented as 16-bit or 32-bit values
- [Services defined by the Bluetooth SIG](#)
- E.g. UART over BLE (6E400001-B5A3-F393-E0A9-E50E24DCCA9E)
 - RX Characteristic (UUID: 6E400002-B5A3-F393-E0A9-E50E24DCCA9E)
 - TX Characteristic (UUID: 6E400003-B5A3-F393-E0A9-E50E24DCCA9E)

❖ Data exchange

- Read / write the value of characteristics; may need authentication



- ❖ GATT operations: The GATT protocol provides a number of commands
 - Discover UUIDs for all primary services
 - Find a service with a given UUID
 - Find secondary services for a given primary service
 - Discover all characteristics for a given service
 - Find characteristics matching a given UUID
 - Read all descriptors for a particular characteristic
 - Read (data transfer from server to client) and Write (from client to server) the values of characteristics
 - GATT offers notifications and indications:
 - The client may request a **notification** for a particular characteristic from the server.
 - The server can then send the value to the client whenever it becomes available.
 - An **indication** is similar to a notification, except that it requires a response from the client, as confirmation that it has received the message

❖ BLE Encryption

- AES128 encryption to protect the content

❖ Keys

- Temporary key: Used in pairing process
- Short term key: Used to encrypt connection during initial pairing
- Long term key: Replaces short term to encrypt connection
- Identity resolving key: Used to hide identities
- Connection signature key: Authentication key

❖ Higher level encryption

- Application level encryption

Bluetooth

❖ Some useful links

- [Bluetooth](#)
- [Bluetooth Core Specification v4.2](#)
- [Bluetooth Basics](#)
- [How Bluetooth Works](#)
- [Bluetooth 5: a concrete step forward towards the IoT](#)
- [ESP32 Bluetooth Classic with Arduino](#)
- [Getting Started with ESP32 Bluetooth Low Energy](#)
- [Bluetooth Low Energy App Development: The Basics](#)
- [All About Bluetooth - For the Layman](#)
- [What is Bluetooth 5? - Gary explains](#)