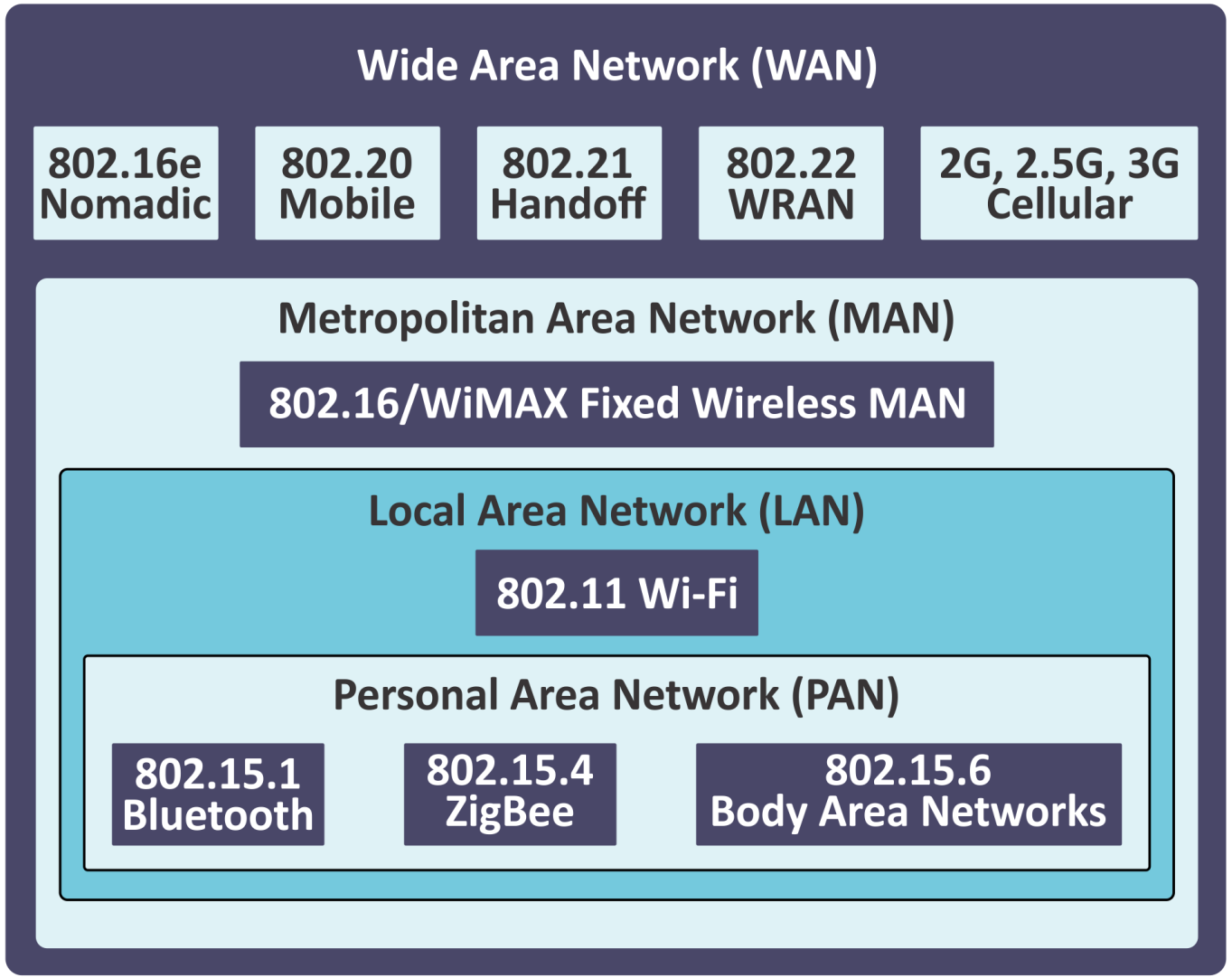
Affordable Custom BLE Target

Nishant Sharma & Jeswin Mathai
www.PentesterAcademy.com

Index

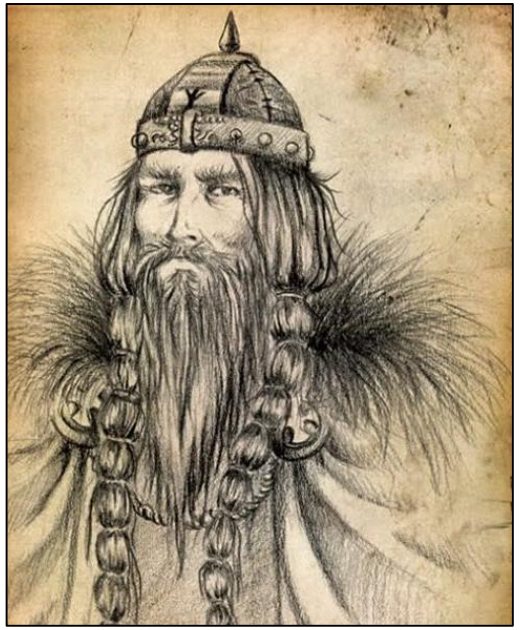
Introduction to BLE

WPAN



Bluetooth

- Named after Danish king Herald Blatand (AD 940-981)

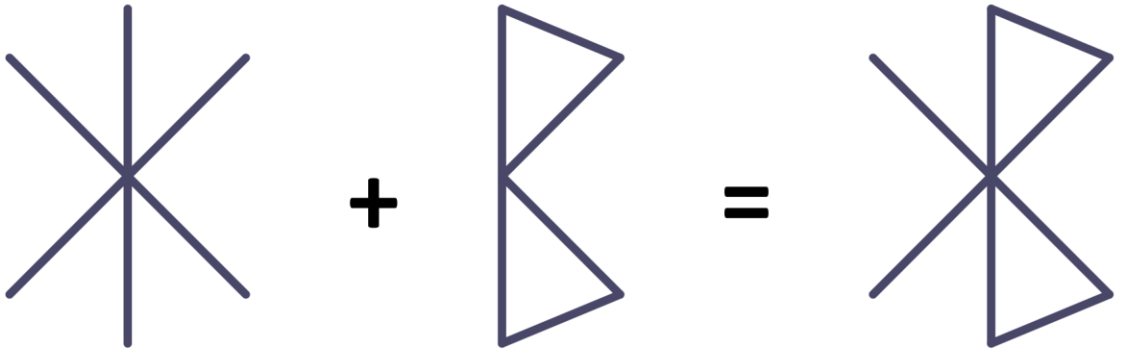


Important historical events

- 1994: Started by Ericsson.
- 1998: Bluetooth SIG formed
- 1999: Version 1.0A specs released
- 2002: 802.15.1 approved

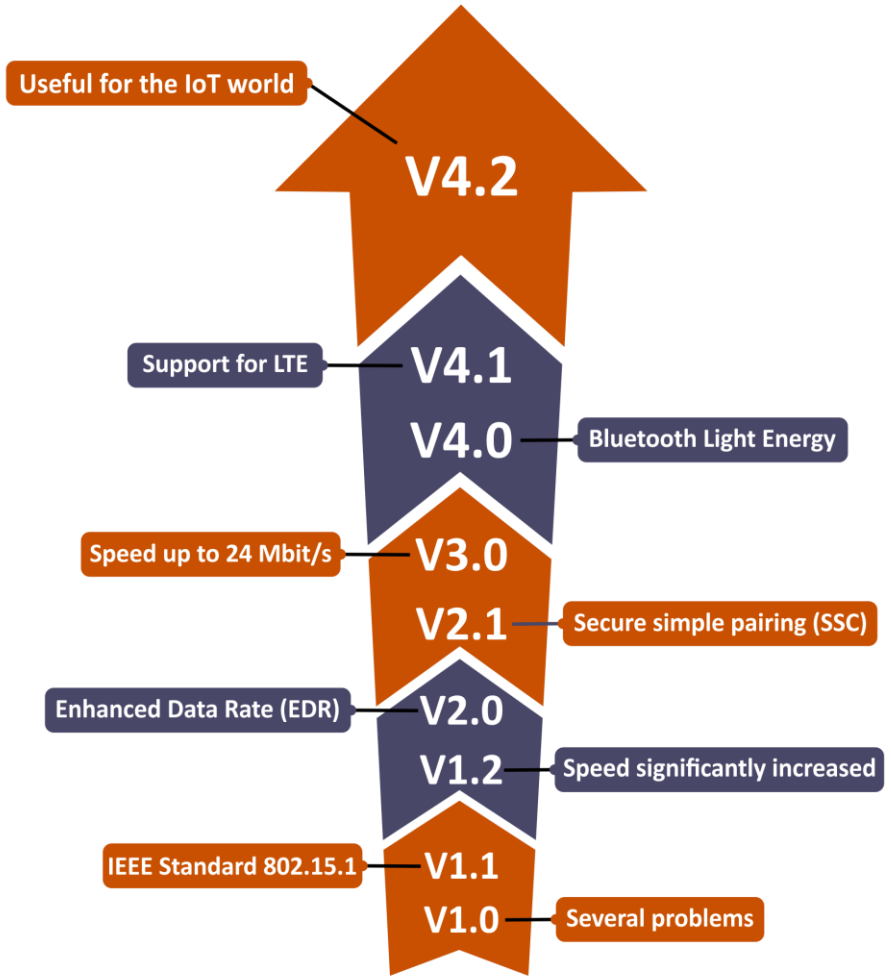
Source: http://media2.intoday.in/indiatoday/images/stories/2017July/king-harald-bluetooth_071717051504.jpg

Bluetooth Naming and Logo



“H” “B”

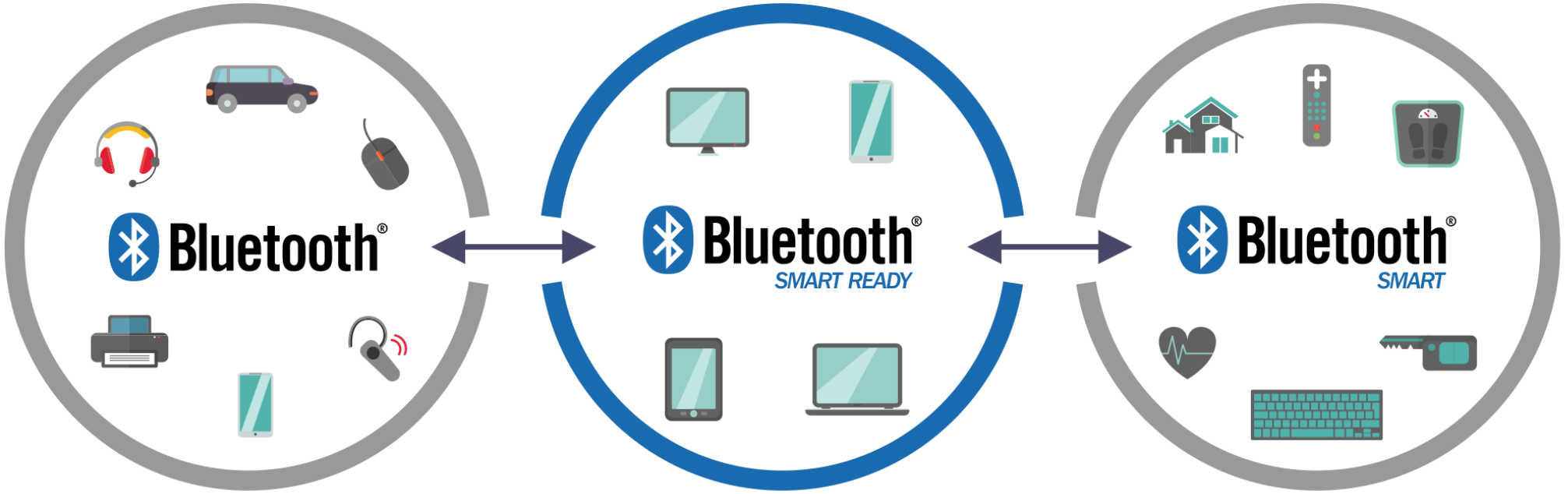
History



Bluetooth Low Energy (BLE)

- Wireless technology standard, designed from ground up
- Simple and easy to use model
- Small bursts of data
- Impressive battery life
- Low cost
- 2.4 GHz band
- Ideal for sensors/ IoT

Naming Bluetooth 4.0



Wireless devices streaming rich content like video and audio

Devices that connect with both

Sensor devices sending small bits of data, using very little energy

BLE Working

BLE Device Roles

Peripheral

Advertise

Connect

Fetch information

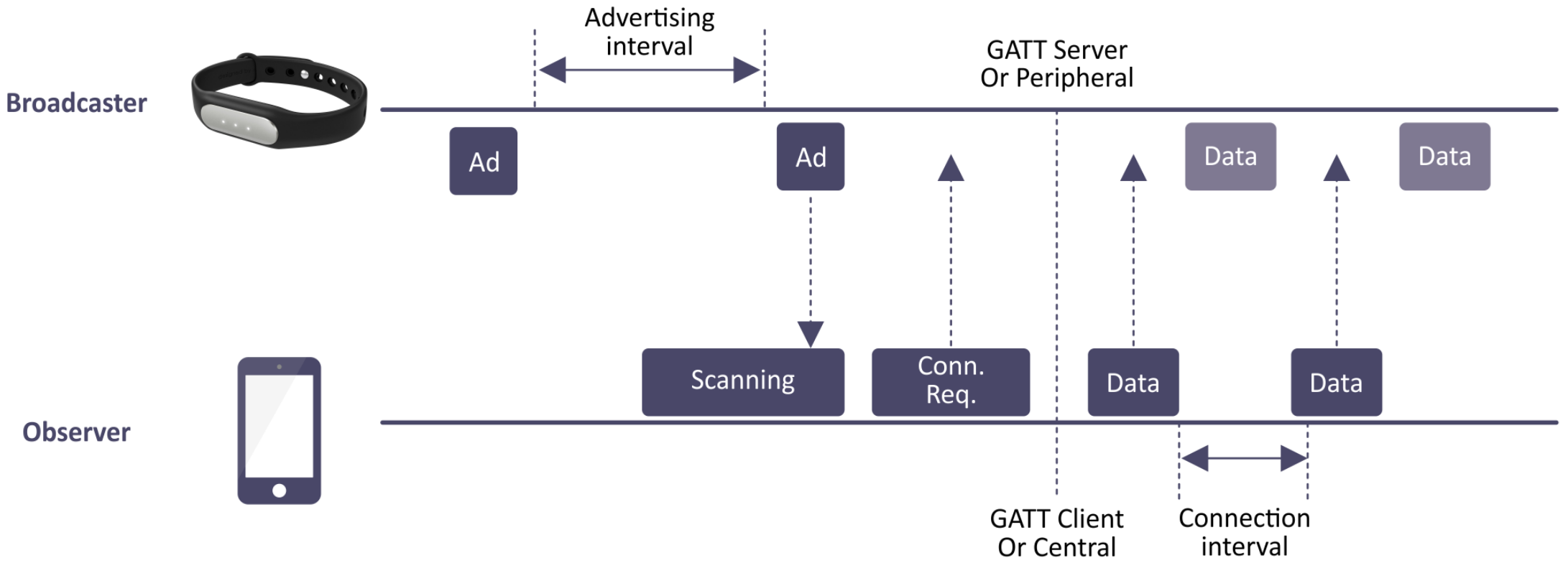
Central

Broadcaster

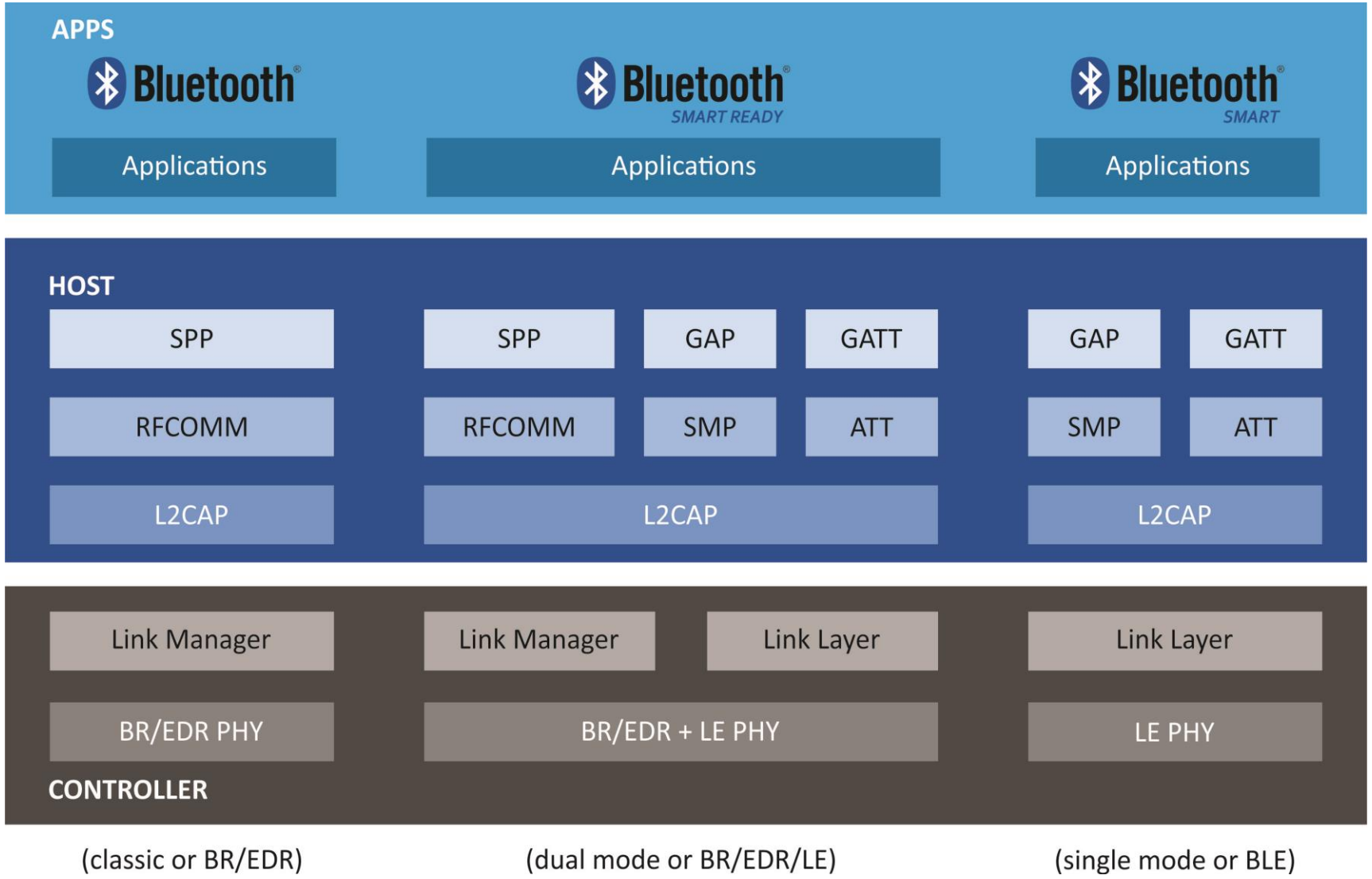
Broadcasting information

Observer

Working



Protocol Stack



GAP Profile

Assigned numbers are used in GAP for inquiry response, EIR data type values, manufacturer-specific data, advertising data, low energy UUIDs and appearance characteristics, and class of device.

EIR Data Type, Advertising Data Type (AD Type) and OOB Data Type Definitions

Data Type Value	Data Type Name	Reference for Definition
0×01	«Flags»	Bluetooth Core Specification:Vol. 3, Part C, section 8.1.3 (v2.1 + EDR, 3.0 + HS and 4.0)Vol. 3, Part C, sections 11.1.3 and 18.1 (v4.0)Core Specification Supplement, Part A, section 1.3
0×02	«Incomplete List of 16-bit Service Class UUIDs»	Bluetooth Core Specification:Vol. 3, Part C, section 8.1.1 (v2.1 + EDR, 3.0 + HS and 4.0)Vol. 3, Part C, sections 11.1.1 and 18.2 (v4.0)Core Specification Supplement, Part A, section 1.1
0×03	«Complete List of 16-bit Service Class UUIDs»	Bluetooth Core Specification:Vol. 3, Part C, section 8.1.1 (v2.1 + EDR, 3.0 + HS and 4.0)Vol. 3, Part C, sections 11.1.1 and 18.2 (v4.0)Core Specification Supplement, Part A, section 1.1
0×04	«Incomplete List of 32-bit Service Class UUIDs»	Bluetooth Core Specification:Vol. 3, Part C, section 8.1.1 (v2.1 + EDR, 3.0 + HS and 4.0)Vol. 3, Part C, section 18.2 (v4.0)Core Specification Supplement, Part A, section 1.1
0×05	«Complete List of 32-bit Service Class UUIDs»	Bluetooth Core Specification:Vol. 3, Part C, section 8.1.1 (v2.1 + EDR, 3.0 + HS and 4.0)Vol. 3, Part C, section 18.2 (v4.0)Core Specification Supplement, Part A, section 1.1

GAP Profile: https://www.bluetooth.com/specifications/assigned-numbers/generic-access-profile

GATT Profile

- Defines data formats/interfaces with Attribute Protocol
- Type-Length-Vlaue(TLV) encoding
- Each attribute has a 16bit Universally Unique ID (UUID) assigned by Bluetooth SIG or 128-bit UUID assigned by manufacturer
- Allows client to find server and read/write data

GATT Profile

Periferal

Service
Heart rate service

Characteristic
Heart rate measurement

Characteristic
Body sensor location

Profile

Service
Characteristic
Descriptor
Characteristic
Descriptor

Service
Characteristic
Descriptor
Characteristic
Characteristic

Services

Services are collections of characteristics and relationships to other services that encapsulate the behavior of part of a device.

All Service Assigned Numbers values on this page are normative. All other materials contained on this page is informative only. Authoritative compliance information is contained in the applicable *Bluetooth*® specification.

Name	Uniform Type Identifier	Assigned Number	Specification
Generic Access	org.bluetooth.service.generic_access	0x1800	GSS
Alert Notification Service	org.bluetooth.service.alert_notification	0x1811	GSS
Automation IO	org.bluetooth.service.automation_io	0x1815	GSS
Battery Service	org.bluetooth.service.battery_service	0x180F	GSS
Blood Pressure	org.bluetooth.service.blood_pressure	0x1810	GSS
Body Composition	org.bluetooth.service.body_composition	0x181B	GSS
Bond Management Service	org.bluetooth.service.bond_management	0x181E	GSS
Continuous Glucose Monitoring	org.bluetooth.service.continuous_glucose_monitoring	0x181F	GSS
Current Time Service	org.bluetooth.service.current_time	0x1805	GSS

GATT Services: https://www.bluetooth.com/specifications/gatt/services

Services Components

- UUID
- Name
- Type
- Start Handle
- End Handle
- Characteristics

Characteristics

Characteristics are defined attribute types that contain a single logical value. All Assigned Numbers values on this page are normative.

Name	Uniform Type Identifier	Assigned Number	Specification
Aerobic Heart Rate Lower Limit	org.bluetooth.characteristic.aerobic_heart_rate_lower_limit	0x2A7E	GSS
Aerobic Heart Rate Upper Limit	org.bluetooth.characteristic.aerobic_heart_rate_upper_limit	0x2A84	GSS
Aerobic Threshold	org.bluetooth.characteristic.aerobic_threshold	0x2A7F	GSS
Age	org.bluetooth.characteristic.age	0x2A80	GSS
Aggregate	org.bluetooth.characteristic.aggregate	0x2A5A	GSS
Alert Category ID	org.bluetooth.characteristic.alert_category_id	0x2A43	GSS
Alert Category ID Bit Mask	org.bluetooth.characteristic.alert_category_id_bit_mask	0x2A42	GSS

GATT Characteristics: https://www.bluetooth.com/specifications/gatt/characteristics

Characteristics Components

- UUID
- Name
- Start Handle
- Value
- Value Handle
- Properties
- Descriptors

GATT Operation

- Central device can
  - Enumerate services and characteristics as per permissions
  - Interact (read/write value) with characteristics as per permissions

- Peripheral device
  - Notify central device of changes

Need?

BLE devices

Smart Lock

https://www.amazon.ca/Fingerprint-Bluetooth-Biometric-Smart-Keyless/dp/B01IXZ10FW

Smart Bottle

https://www.mbreviews.com/best-smart-water-bottle/

Smart watch/Heart Rate monitor

https://www.walmart.com/ip/Tagital-Smart-Watch-Fitness-Tracker-Waterproof-Activity-Tracker-with-Heart-Rate-Monitor-Sleep-Monitor-Pedometer-Calorie-Counter/535823786

BLE devices (contd.)

Smart Scale

https://store.getqardio.com/products/qardiobase?variant=49488491028

Smart Anti Lost (Theft)

https://www.walmart.com/ip/Wireless-Bluetooth-4-0-Anti-lost-Anti-Theft-Alarm-Device-Tracker-GPS-Locator-Key-Dog-Cat-Kids-Wallets-Finder-Tracer-w-Camera-Remote-Shutter-Recording/769561218

Smart Temperature Sensor

https://www.bestbuy.com/site/nest-temperature-sensor-white/6221357.p

Problems for a Pentester/Learner

- Expensive to get all devices
- Can’t carry all devices with him for demos/training
- Can’t design custom device profiles/challenges

Solution

BLE MYSTIQUE

- Transform ESP32 to different BLE profiles
- Take a template and modify it as per your need
- Thanks for X-Men for name

Why ESP32?

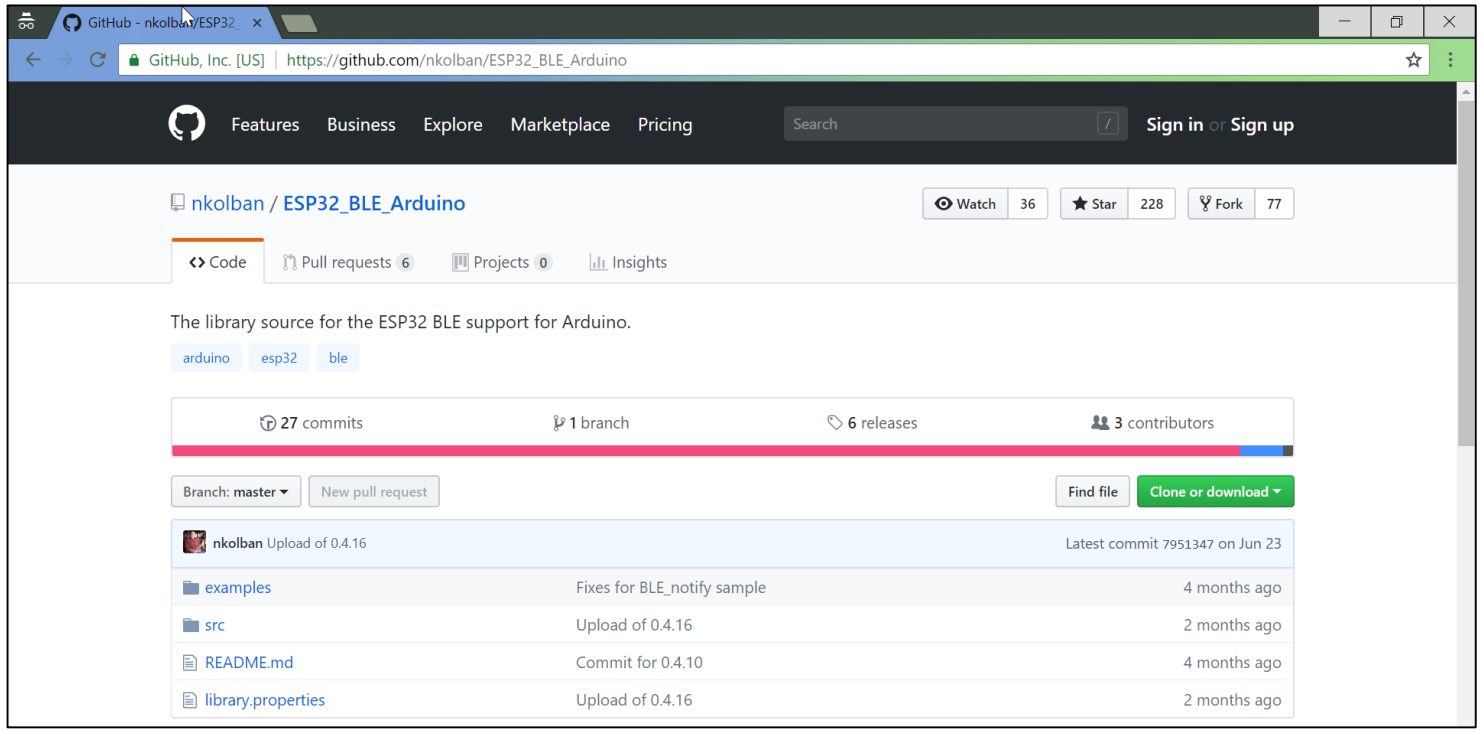
- Affordable WiFi-BLE SoC (< $5)
- Can be operated on power bank or USB connection
- Cab be used with mobile phone/laptop
- Easily available, comes in multiple variations
  - https://www.aliexpress.com/item/ESP32-development-board-WIFI-Bluetooth-IoT-smart-home-ESP-WROOM-32-ESP-32-ESP-32S/32849567377.html
  - https://www.mouser.com/ProductDetail/Espressif-Systems/ESP32-WROOM-32D

How it work?

How it work?

- Host GATT services on ESP32

- BLE Library: https://github.com/nkolban/ESP32_BLE_Arduino



How to use?

- Clone from GitHub: https://github.com/pentesteracademy/blemystique
- Flash to your ESP32
- Connect to mobile or power bank (and take it with you)

What can be imitated

Services are collections of characteristics and relationships to other services that encapsulate the behavior of part of a device.

All Service Assigned Numbers values on this page are normative. All other materials contained on this page is informative only. Authoritative compliance information is contained in the applicable *Bluetooth*® specification.

Name	Uniform Type Identifier	Assigned Number	Specification
Generic Access	org.bluetooth.service.generic_access	0x1800	GSS
Alert Notification Service	org.bluetooth.service.alert_notification	0x1811	GSS
Automation IO	org.bluetooth.service.automation_io	0x1815	GSS
Battery Service	org.bluetooth.service.battery_service	0x180F	GSS
Blood Pressure	org.bluetooth.service.blood_pressure	0x1810	GSS
Body Composition	org.bluetooth.service.body_composition	0x181B	GSS
Bond Management Service	org.bluetooth.service.bond_management	0x181E	GSS
Continuous Glucose Monitoring	org.bluetooth.service.continuous_glucose_monitoring	0x181F	GSS
Current Time Service	org.bluetooth.service.current_time	0x1805	GSS

GATT Services: https://www.bluetooth.com/specifications/gatt/services

Code Walk and Demo: Heart Rate Monitor

What's Next?

What's Next?

- I don't want to write or modify code or even JSON? ☹
- Service list is long for my device of interest. ☹
- Want something which just works.

Solution

Cloner (BLE Mystique 2.0 feature)

- Search and locate the device
- Select the target device
- Clone it
- Save the profile for future use.

Demo: Cloner

Q & A

Thanks!