Personal Area Networks (PANs)

- A PAN technology provides communication over a short distance
- It is intended for use with devices that are owned and operated by a single user. For example
  - between a wireless headset and a cell phone
  - between a computer and a nearby wireless mouse or keyboard
- Several standards
  - Frequencies dedicated to Industrial, Scientific and Medical (ISM) band
  - Bluetooth, Near Field Comms(NFC)

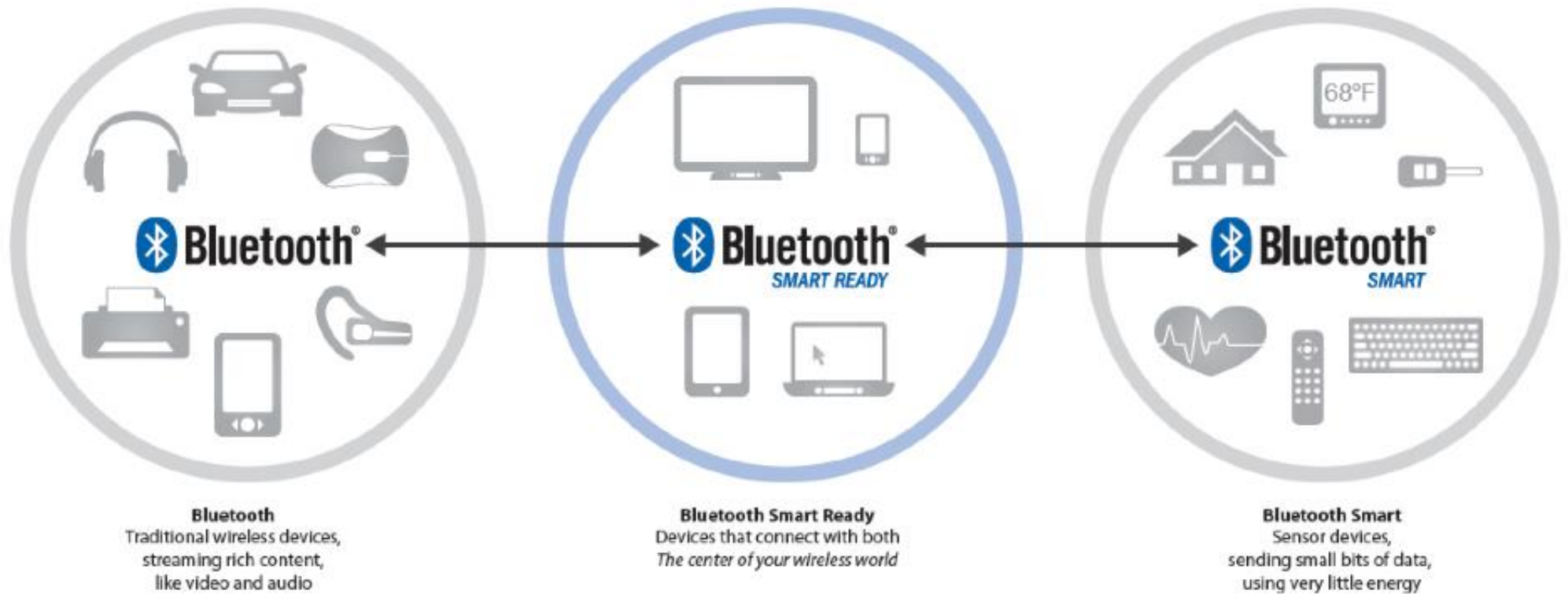A typical personal network or PAN connecting devices. (Bluetooth shown)

Bluetooth

- Used for short distance data exchanging, such as Personal Area Network
- RF from 2.4 to 2.485 GHz
- Originally invented by Ericsson (a telecom vendor) in 1994
- Now managed by the Bluetooth Special Interest Group (SIG)
- Frequency hopping spread spectrum (FHSS)
- 16000+ SIG member companies
- Billions of products shipped

Bluetooth Classification

Bluetooth
Traditional wireless devices,
streaming rich content,
like video and audio

Bluetooth Smart Ready
Devices that connect with both
The center of your wireless world

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

Bluetooth "classic"

- The "conventional" Bluetooth
- Operates in 2.4GHz
- Range: 1m - 100m (10m typical)
- Connection-oriented: audio, file transfer, networking
- Reasonably fast data rate: **2.1** Mbps
- Power consumption:
    - < Wifi < 3G

Bluetooth Low Energy

- "Bluetooth Smart"

- Light-weight subset of classic Bluetooth
  - Operates in same freq. Range, 2.4GHz
  - introduced as part of the Bluetooth 4.0 core specification

- Target Apps:
  - Wireless battery-powered sensors eg. heart rate, thermometer, wearables
  - Low bandwidth (you won't be streaming video)
  - Not always on, constrained devices

All good for IoT devices!

BLE vs Classic

- Bluetooth and Bluetooth Low Energy are used for different purposes
- Bluetooth Classic
  - can handle a lot of data
  - consumes battery quickly
- BLE
  - used for applications that do not need to exchange large amounts of data
  - cheap
  - Marginally further range

Bluetooth History

- Bluetooth 1.1
  - Published in 2002
  - Data rate: 1 Mbit/s
  - First widely implemented version
- Bluetooth 2.0 + Enhanced Data Rate (EDR)
  - Published in 2004
  - Data rate: 3 Mbit/s
- Bluetooth 3.0 + High Speed (HS)
  - Published in 2009
  - Data rate: 24 Mbit/s
- Bluetooth 4.0 +
  - Published in 2010
  - Data rate: 24 Mbit/s
  - Also called Bluetooth Smart
  - Includes Classic Bluetooth, Bluetooth high speed and Bluetooth low energy protocols
  - Bluetooth 4.2 (2014) - Introduces some key features for IoT

BLE Roles

- Broadcaster
  - Transmitter only
- Observer
  - Receiver only
- Peripheral(Slave)
- Central(Master)
  - Can take multiple connections
  - Initiates connection to peripheral
- One Device can have multiple roles
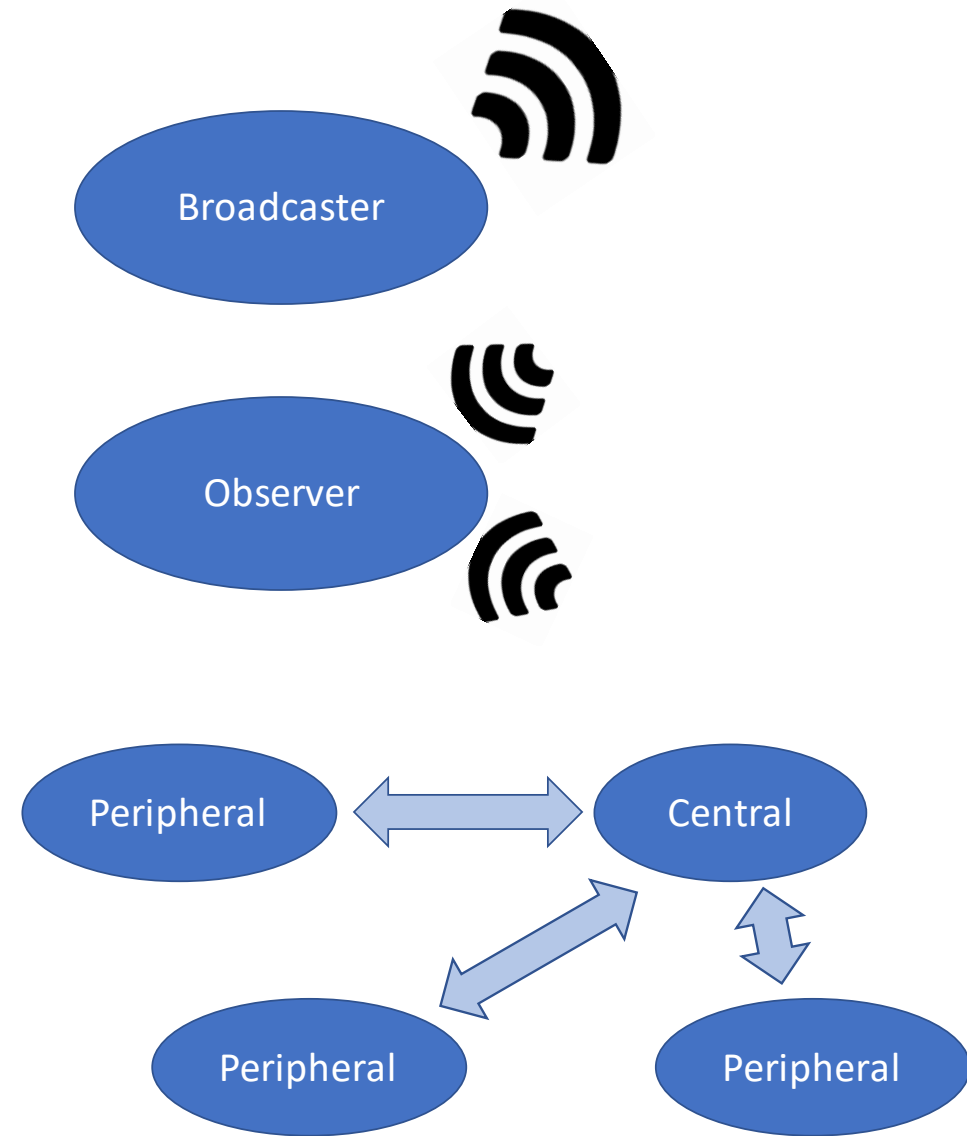
BLE Operation Modes

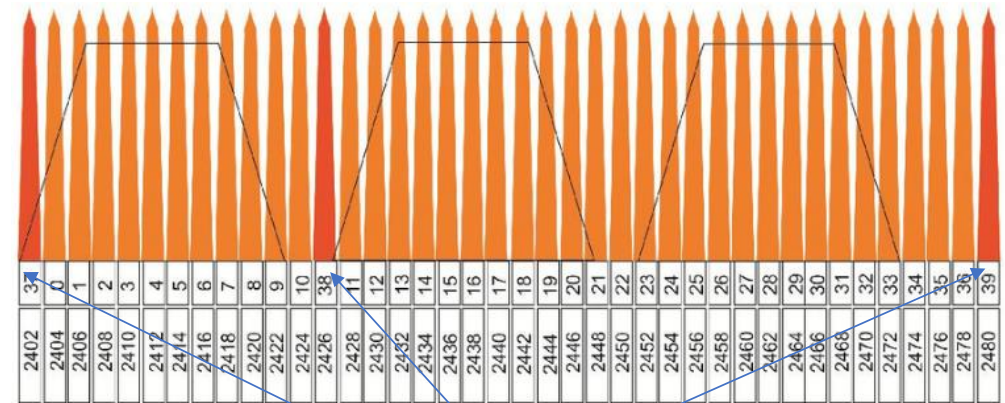| Peripheral and Central Devices	**Master/central :** will typically have more computing resources and available energy - a computer or a tablet, for example.
	Slave/peripheral : an embedded device - will be constrained in both computing resources and energy.
Servers and Clients	**Server :** the device that has information it wishes to share, and in BLE that is typically the peripheral (the embedded device).
	Client : the device that wants information and services, and in BLE that is typically the central device - the phone

BLE Connections

- Initiating Connections
  - The central is free to establish or terminate a connection
  - The peripheral (the BLE device) cannot force the central to scan for BLE devices
- The two modes BLE uses are:
  - Advertising mode : the peripheral sends out Generic Access Profile (GAP) that any device in the area can pick up; this is how central devices know that there are peripherals around.
  - Connected mode : the peripheral and a central device establish a one-to-one conversation. This is how they can exchange complex information.

Advertising mode   Connected mode
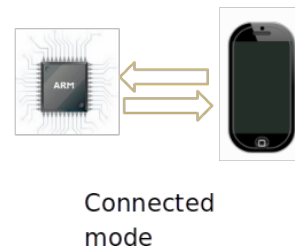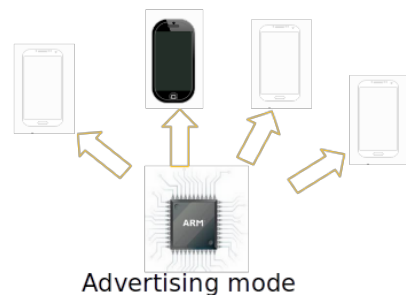
Advertising process

- Operates in 2.4 GHz Band

- Peripheral sets a specific advertising interval and transmit advertising packet
  - longer delays saves power but less responsive

- Transmits on all advertising channels in each interval(channel 37/38/39)

- A listening device interested in the scan response payload can optionally request the scan response payload, and the peripheral will respond with the additional data.
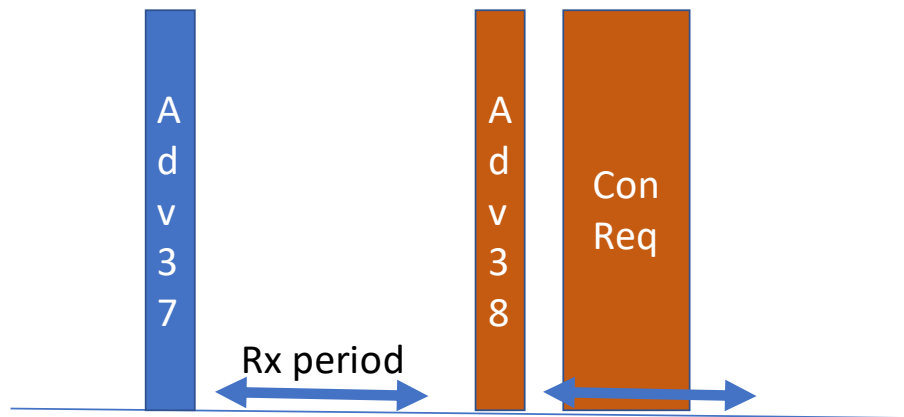

Advertising channels
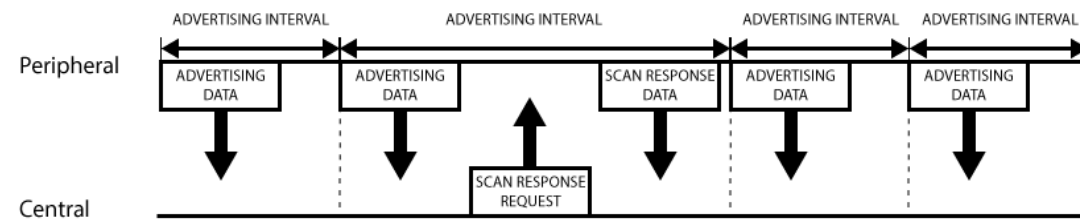
Connection Process

- Initiated by central device in a specific response period
- Central can issue connection request after receiving advertisement


- Peripheral stops advertising after connection request (becomes a slave)
- Slave waits for packets from Master.
  - When received, connection established

Bluetooth LE Device Address

- The Bluetooth **Device Address** is a 48-bit (6-byte) number uniquely identifies a device among peers.
  - Similar to an Ethernet Media Access Control (MAC) address
- Think of it as a unique address of a device
- There are two types of device addresses and one or both can be set on a device:
  - Random Address:
    - Random number according to the Bluetooth SIG. Can be static(can only change on power cycle) or Private(resolvable/non-resolvable)
  - Public Address:
    - Calculated just like IEEE Ethernet LAN address

GAP and GATT for BLE

- Generic Access Profile (GAP) or Advertising
  - Information advertised to central before connection
  - Name of peripheral
  - Is it connectable?
  - Supported features (services)
- Generic Attribute Profile (GATT)
  - How to exchange data once connected
 - Identifies Services, Characteristics and Descriptors

GAP	GATT
SMP	ATT

L2CAP
Link Layer
LE PHYSICAL
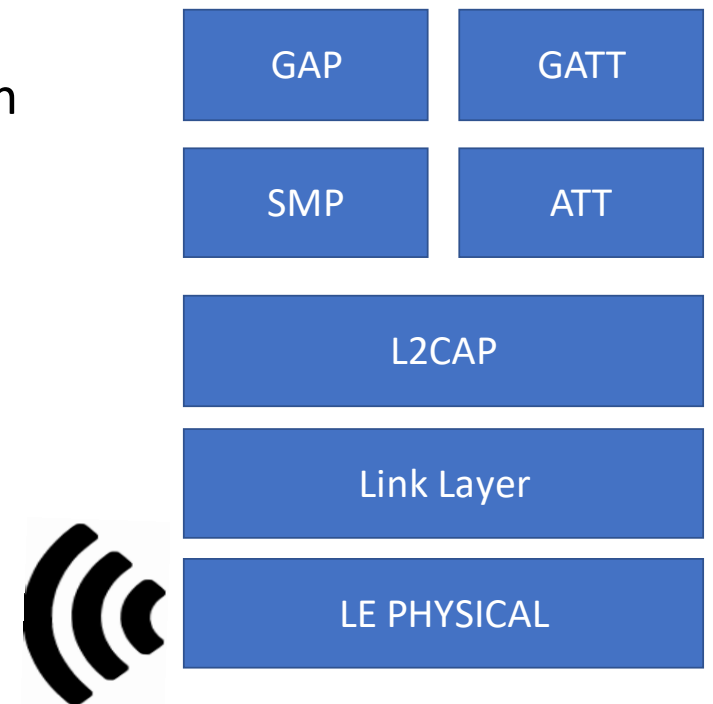
Generic Access Profile (GAP)

- GAP responsible for "device visibility."
- Determines how two devices can (or can't) interact with each other.
- 2 ways for a device to advertise with GAP
  - *Advertising Data* payload
  - *Scan Response* payload.
- Advertising data payload is mandatory
- Scan response payload is optional
  - allows device designers to fit more information in the advertising payload such a strings for a device name, etc.

Broadcast Network Topology

- Some devices/apps only require advertise data.
  - E.g. app requires peripheral to send data to more than one device at a time.

- Can include small amount of custom data in **31** byte advertising or scan response payloads.

- In this way, BLE peripheral can send data one-way to any devices in listening range
 - BLE Beacons
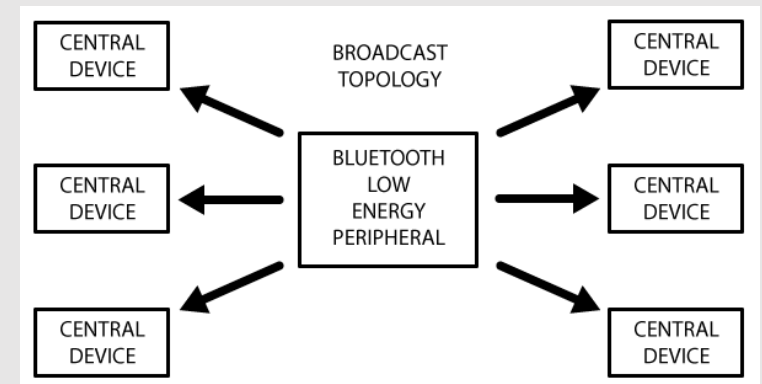
Bluetooth Connection

- Establishing a connection between a peripheral and a central device results in 1 to 1 communication
  - the advertising process will stop
  - no longer be able to send advertising packets
- Communication in both directions
- Must use GATT services and characteristics to communicate

Generic Attribute Profile - GATT

- A pre-defined collection of Services that has been compiled by either the Bluetooth Special Interest Group or by the peripheral designers.
  - E.g. The Heart Rate Profile
  - combines the Heart Rate Service and the Device Information Service.
- Complete list of GATT-based profiles can be found here: Profiles Overview
- Defines the way that two Bluetooth Low Energy devices transfer data back and forth
- Uses **Services** and **Characteristics**.
- With GATT, a BLE peripheral can only be connected to one central device (e.g. a mobile phone, etc.)
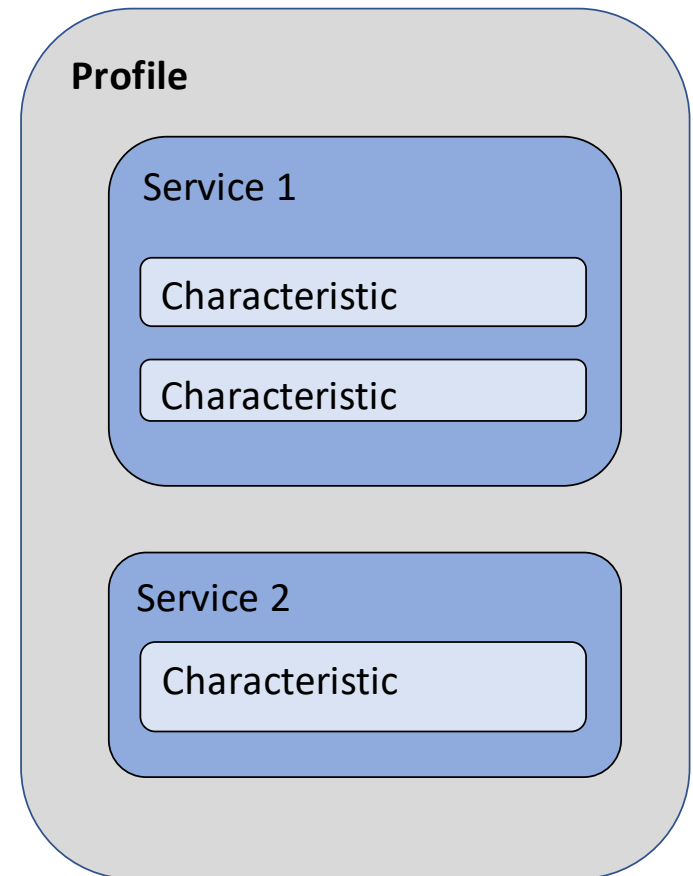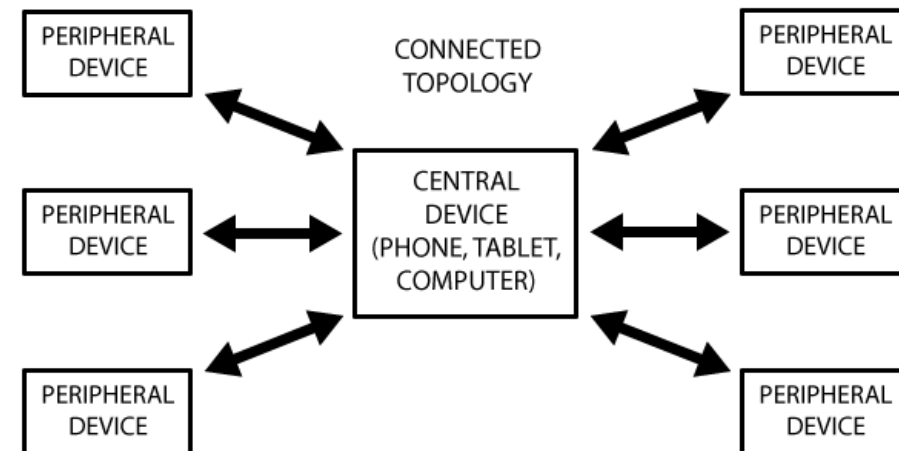
GATT Transactions
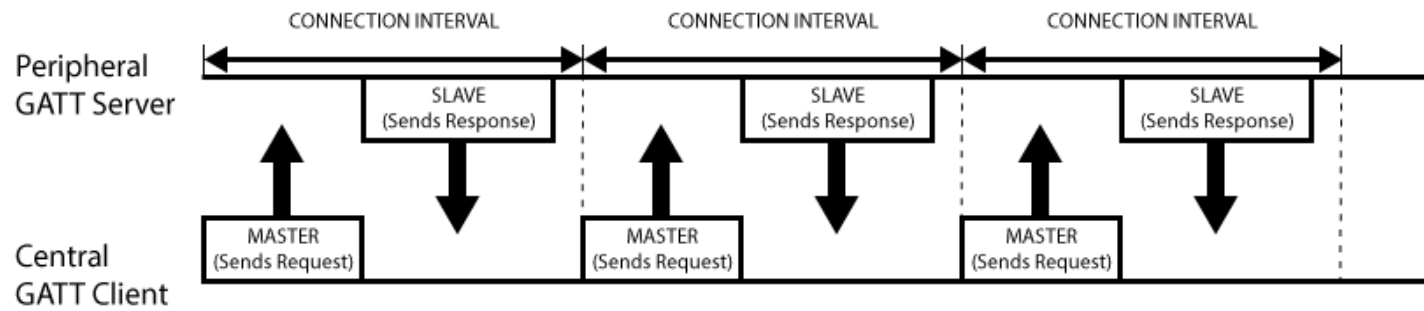
BLE Connected Network Topology

- A peripheral can only be connected to one central device

- Communication is **2** -way

- Central device can be connected to multiple peripherals.

- If data needs to be exchanged between two peripherals, a custom messaging system will need to be implemented
  - all messages pass through the central device.

PERIPHERAL DEVICE

CONNECTED TOPOLOGY

PERIPHERAL DEVICE

PERIPHERAL DEVICE

CENTRAL DEVICE (PHONE, TABLET, COMPUTER)

PERIPHERAL DEVICE

PERIPHERAL DEVICE

PERIPHERAL DEVICE

GATT Services

- Breaks data up into logic entities

- Contains one or more **characteristics**

- Each service distinguished by unique numeric ID called a UUID
  - 16 bit

- Set of officially adopted BLE services can be seen on the [Services](#)

- E.g. official Heart rate service
  - service has a 16-bit UUID of 0x180D
  - contains up to 3 characteristic
    - *Heart Rate Measurement, Body Sensor Location* and *Heart Rate Control Point.*

GATT Characteristics

- Represents a single data point
- Similarly to Services, each Characteristic distinguishes itself via a pre-defined UUID
  - Also use standard characteristics defined by the Bluetooth SIG
- E.G Heart Rate:
  - the Heart Rate Measurement characteristic is mandatory for the Heart Rate Service
  - Heart rate measurement has UUID of 0x2A37
- If you write apps that use BLE, **characteristics** are what you will be after with your BLE peripheral

BLE Power consumption

Chipset	Advertising Interval	Est. Battery Life CR2032	Est. Battery Life CR2045	Est. Battery Life CR2477
Gimbal	100ms	n/a	n/a	n/a
Gimbal	645ms	1 month	2.5 months	4.1 months
Gimbal	900ms	n/a	n/a	n/a
Nordic Semiconductors	100ms	1.2 months	3.1 months	5.1 months
Nordic Semiconductors	645ms	7.0 months	18.19 month	29.3 months
Nordic Semiconductors	900ms	11.1 months	28.7 months	46.29 months
Bluegiga	100ms	0.9 months	2.4 months	3.8 months
Bluegiga	645ms	5.9 months	15.4 months	24.8 months
Bluegiga	900ms	9.3 months	23.9 months	38.5 months
Texas Instruments	100ms	0.7 months	1.8 months	2.9 months
Texas Instruments	645ms	4.1 months	10.6 months	17.1 months
Texas Instruments	900ms	5.6 months	14.4 months	23.1 months

Aislelabs