

tw rev. 15.4.2024

Chapter 11: Wireless Communication

If you use or reference these slides or the associated textbook, please cite the original authors' work as follows:

Wilmshurst, T., Spink, T. & Toulson, R. (2024). Fast and Effective Embedded Systems Design – From Bits and Bytes to IoT, with the ARM Mbed (3rd edition), Newnes, Oxford, ISBN: 978-0323951975.

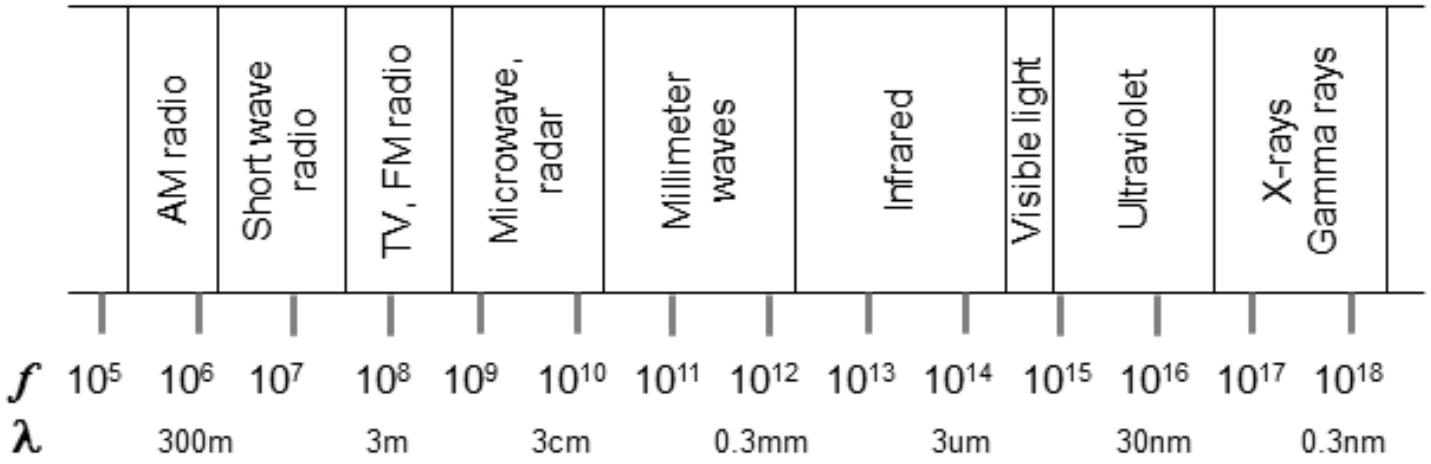
.

Some Wireless Preliminaries 1

The electromagnetic spectrum shows where various wireless activities sit. Any frequency on the spectrum, from the lowest frequency up to visible light, can be used for data communication. Almost all of this is very strictly regulated by national and international agencies.

Frequency and wavelength are related by $\boldsymbol{v = f\lambda}$. where *f* is the frequency, λ the wavelength, and *v* is the speed of radiation, known to be approximately 3 x 10^8 m/sec.

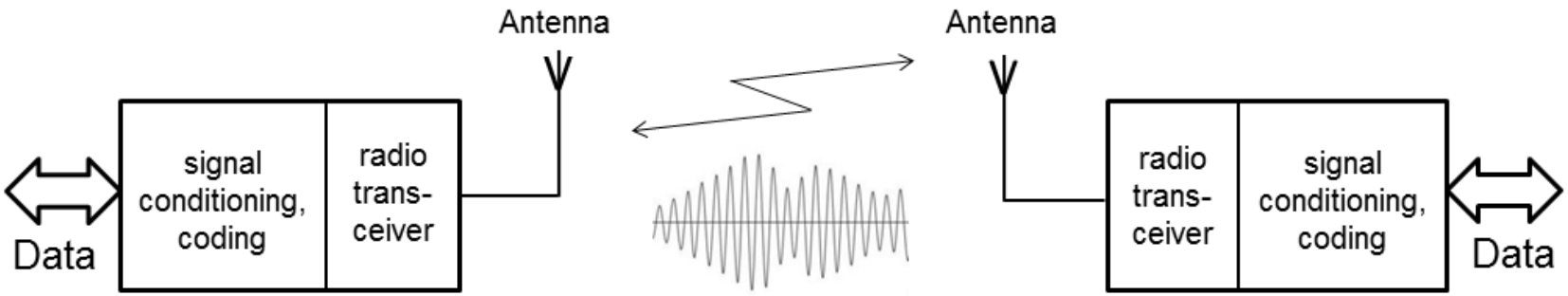
The International Telecommunication Union manages the allocation of the radio spectrum between different broadcasters and applications. It reserves certain frequency bands for Industrial, Scientific and Medical (ISM) applications. These are *unlicensed*, and some vary between countries. The 2.4 GHz band is however reserved for unlicensed use in all regions. It has become widely used, mainly for short-range, low power applications.



Some Wireless Preliminaries 2

While the spectrum represents the “pure” radio frequencies, they only become useful once they are carrying information. This is done by the process of *modulation*; the information to be carried is imprinted onto the carrier frequency, through one of a number of different techniques.

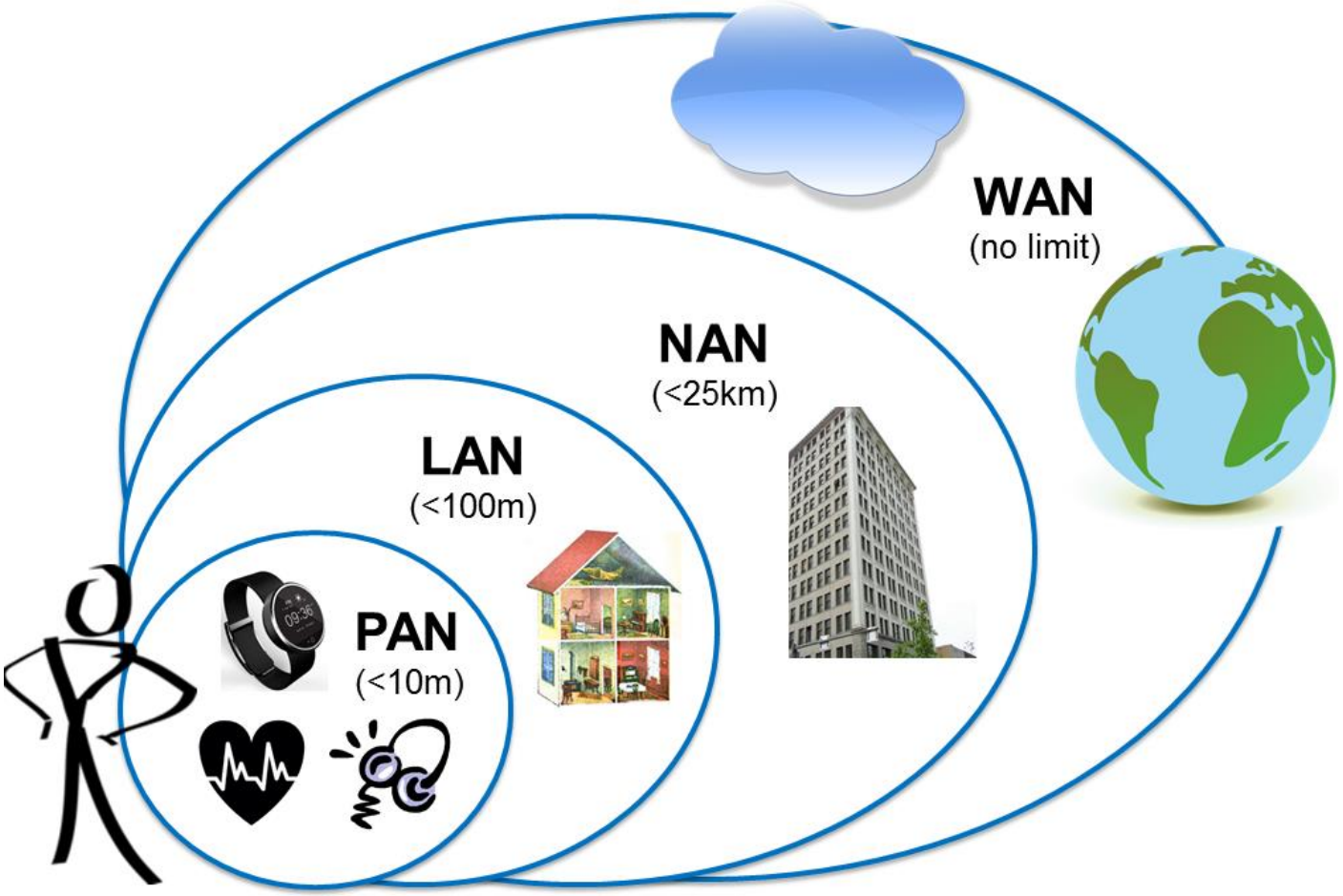
One effect of modulation is to cause fluctuations around the base frequency; thus if we say that a certain radio station can be found at the frequency of 103 MHz, in fact it is in a narrow band of frequencies centred on 103 MHz. The word *bandwidth* is used to define a range of frequencies, for example within which a particular transmission may be taking place.



Wireless Networks

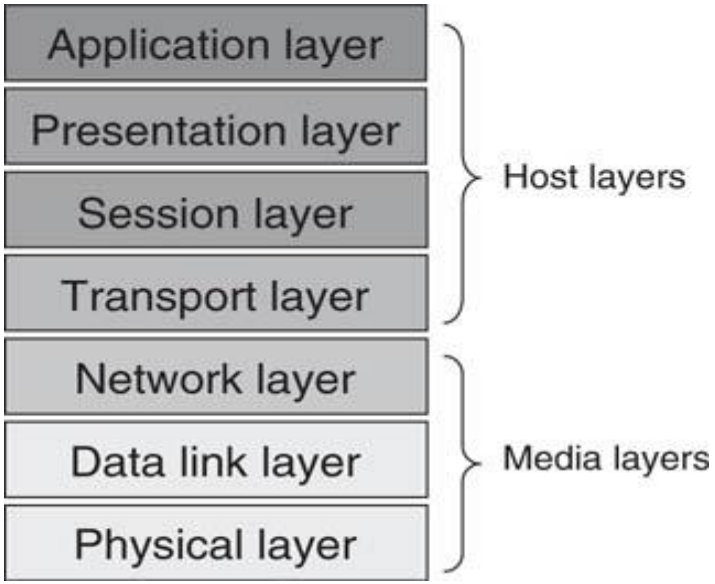
Networks can be divided into four categories:

- The Personal Area Network (PAN) usually relates to devices close to a person.
- The Local Area Network (LAN) typically applies to a single building.
- The Neighbourhood Area Network (NAN) could apply to a smart transport or smart energy system.
- The Wide Area Network (WAN) includes national or global systems, notably the Internet.



Protocols

With large networked systems, protocols can become very complicated, defining every aspect of the communication link. To aid in the process of defining a protocol, the International Organisation for Standardisation (ISO) devised a “protocol for protocols”, called the *Open Systems Interconnect* (OSI) model, as shown. Each layer of the OSI model provides a defined set of services to the layer above, and each therefore depends on the services of the layer below.



Protocols – IEEE Working Groups

The IEEE (the Institute of Electrical and Electronic Engineers) plays a major role in defining standards and protocols. It maintains a set of standards for Local Area Networks, allocated the number 802. A small number of these which are relevant to this and the next chapters are shown in the Table.

IEEE Working Group	Description
802.3	Ethernet
802.11	Wireless LAN, including Wi-Fi
802.15	Wireless PAN
802.15.1	Bluetooth
802.15.3	High-rate wireless PAN
802.15.4	Low-rate wireless PAN, e.g. Zigbee

Classic Bluetooth

Bluetooth is a digital radio protocol, meant for PAN applications, and operating in the 2.4 GHz radio band. It provides wireless data links between devices such as mobile phones, wireless audio headsets, computer interface devices like mice and keyboards, and remote sensors.

There are three Bluetooth classes, based on output power. Class 2 is the most common. The main characteristics are:

- The approximate communication range is up to 100 m for Class 1 Bluetooth devices, up to 10 m for Class 2 devices, and 1 m for Class 3.
- Bluetooth is relatively low power; devices of Classes 1 to 3 use around 100 mW, 2.5 mW and 1 mW respectively.
- Data rates up to 3 Mbps can be achieved. Recent higher data rate versions are being adopted.
- Up to 8 devices can be simultaneously linked, in a *piconet*. A Bluetooth device can belong to more than one piconet.
- Spread-spectrum frequency hopping is applied, with the transmitter changing frequency in a pseudo-random manner 1600 times per second.

Bluetooth Low Energy (BLE)

BLE was developed as a response to the emerging low-energy device market, which includes applications such as fitness trackers, sport, healthcare, and smart homes.

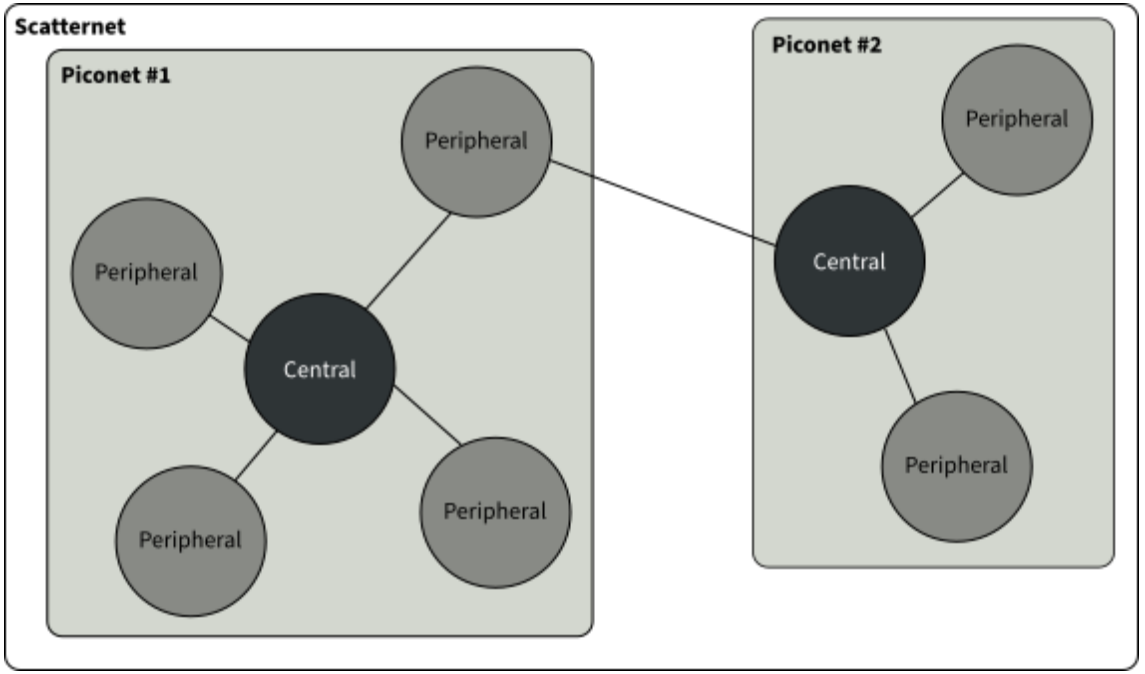
Power requirements can be in the 0.01 to 0.5 W range.

A range of factors can affect transmission range, but typically BLE can achieve ranges from 10m to 100m.

A BLE system comprises “central” and “peripheral” devices.

A central device can connect to many peripheral devices – forming a piconet.

A peripheral device can be connected to more than one central device – effectively connecting multiple piconets together and forming a scatternet.



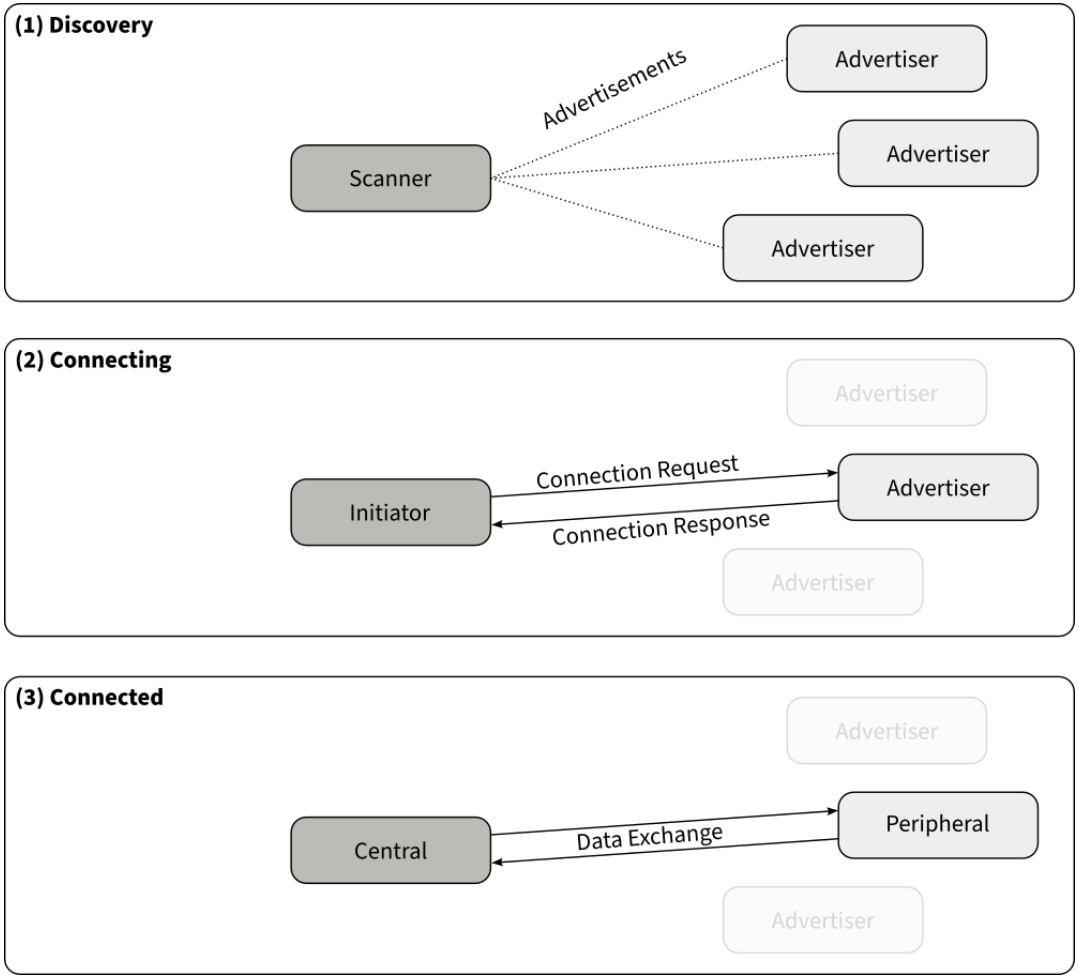
BLE: Establishing a Connection

The BLE Generic Access Profile (GAP) specification dictates how BLE devices can discover each other and establish connections.

BLE devices that want to be found (“advertisers”) periodically broadcast an “advertisement” packet, to let other devices in range (“scanners”) know of their presence.

The period of broadcast is called the “advertising interval”, a random delay of up to 10 ms is added to avoid interference between multiple advertisers.

The actual connection process between two devices takes place over three phases, summarised as shown.

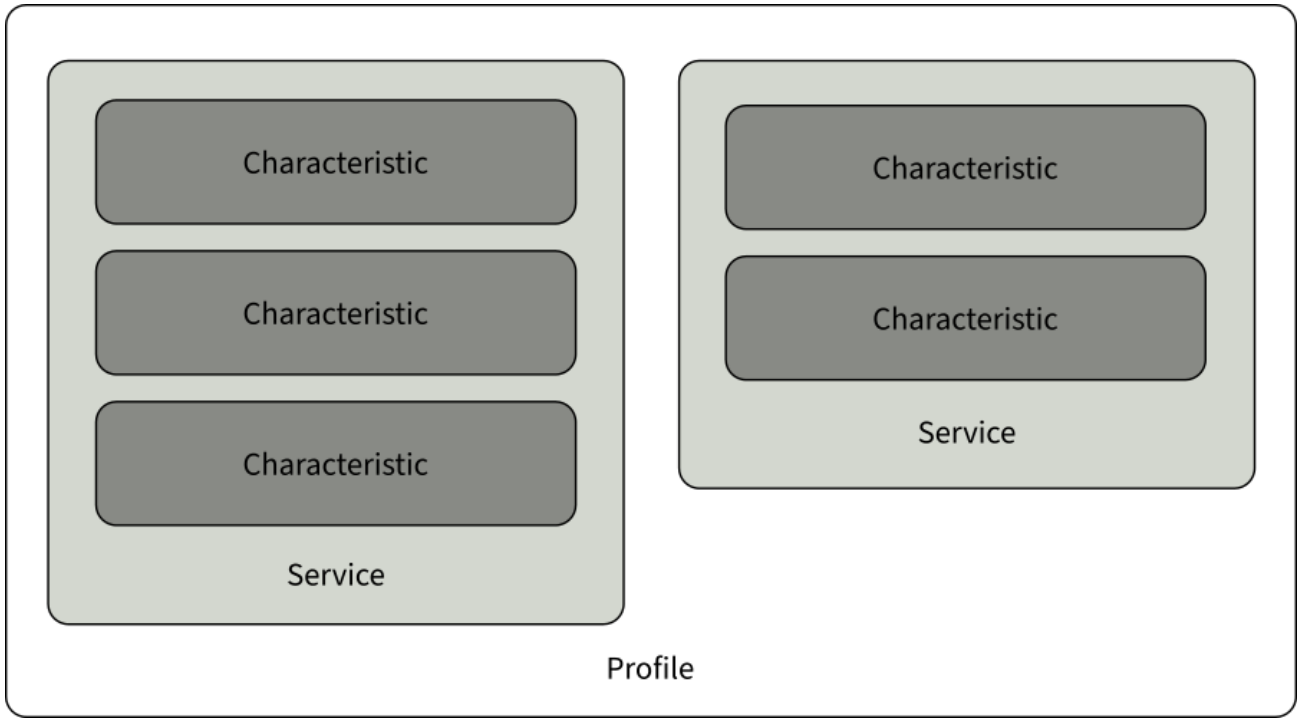


BLE: Exchanging Data

The BLE Generic Attribute (GATT) profile is used to describe one or more services offered by a device – such as a “blood pressure monitoring service”, or a “device information service”. A service is a collection of characteristics that represent the information offered and accepted by that service. This structure is shown.

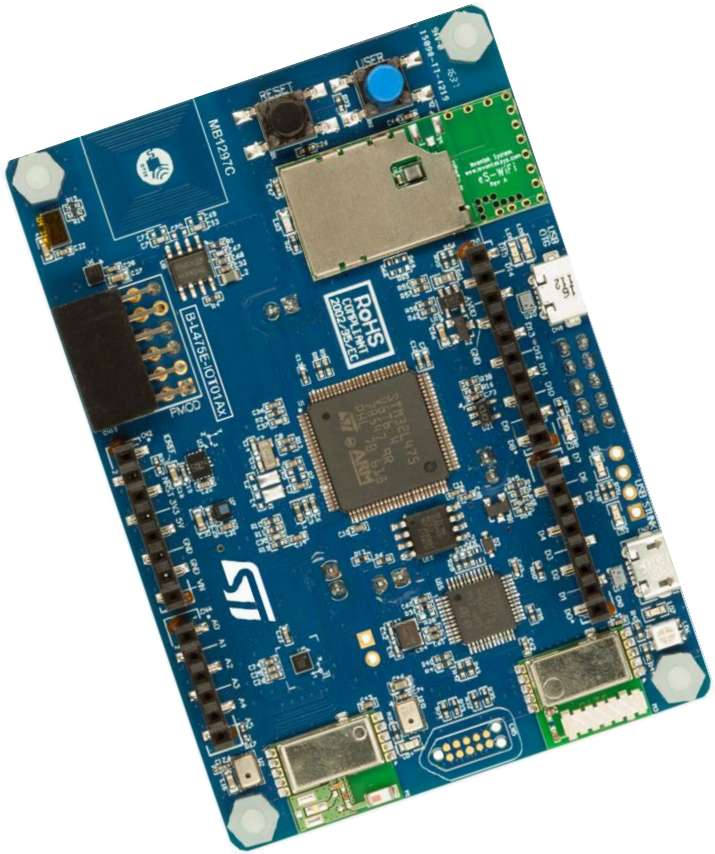
Characteristics are attribute types that have a name, a uniform type identifier, and an assigned Universally Unique Identifier (UUID) number. These are defined in the GATT Specification Supplement.

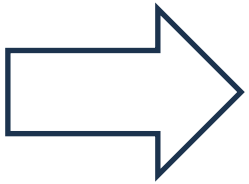
A characteristic offered by a service can be readable, writable, and/ or notifiable (which tells connected devices when the value of the characteristic changes – for example, a temperature change.)

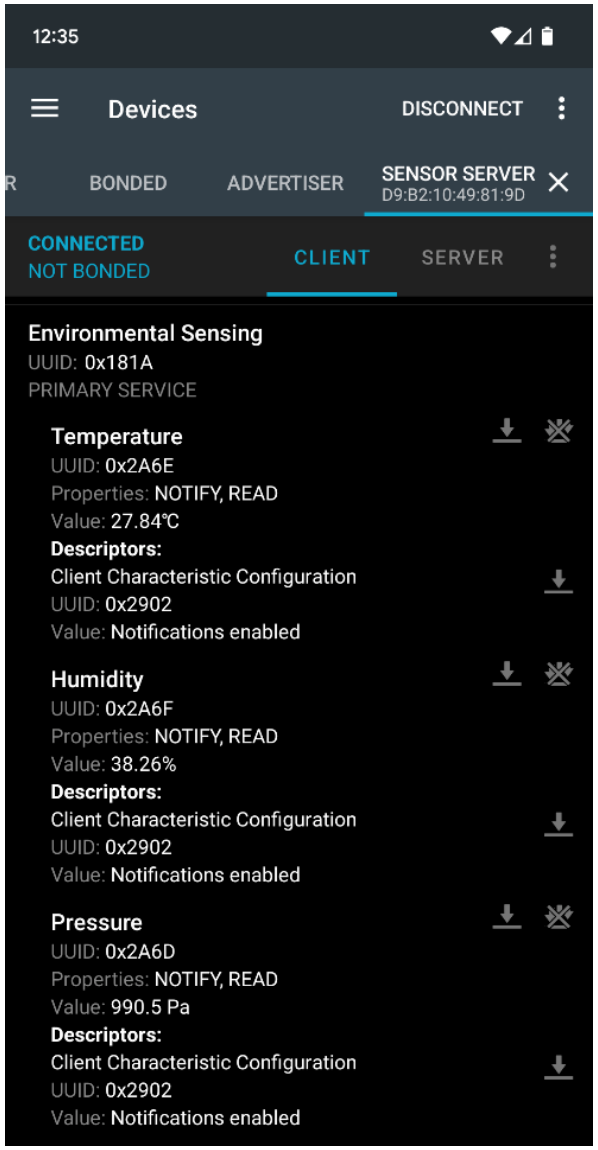


Simple BLE: Sending Data to a Smart Phone

The book BLE example (Program Examples 11.1-11.6) is too large to include in detail in this presentation. It initialises the BLE service on the IoT Discovery board and uses it periodically to transmit sensor data to a smart phone.







Evaluating BLE

Bluetooth Low Energy is an exciting technology that enables short range wireless communication. This has many valuable applications where wires are intrusive, expensive, or difficult/impossible to install.

The various software frameworks that are available (especially in the Mbed ecosystem) make interacting with BLE modules much easier than if trying to develop from scratch.

With lower energy comes a reduced transmission range, and a reduced data rate.

Operating in the 2.4 GHz ISM band means that the signal itself is subject to a lot of interference (given the relative “crowding” of this RF band), and that it is subject to physical limitations too. Higher frequencies are absorbed more easily by objects such as walls and the human body.

Introducing Zigbee

Zigbee is intended for extreme low power systems, with low data rates, even lower than BLE.

It applies and builds on the IEEE 802.15.4 Low-Rate WPAN standard. Like BLE it operates in the ISM bands of the radio spectrum.

Zigbee has some similarities to BLE, but aims to be simpler, cheaper, with smaller software overhead and with different target applications. Like BLE, Zigbee devices apply spread spectrum communication.

Zigbee is particularly appropriate for home automation, and other measurement and control systems, with the ability to use small, cheap microcontrollers.

Data rates vary from 20kbps (in 858 MHz band) to 250 kbps (in the 2.4 GHz band). Because of this low data rate expectation, Zigbee end devices are able to implement Sleep modes; power consumption can hence be minimal.

Zigbee Device Types

The end device: the simplest, able to undertake simple measurement actions and pass back the data. It can only do this to its “parent”, i.e. the router or coordinator which allows it to join. It may spend a large part of its time in the Sleep mode.

The router: After joining a Zigbee PAN, it can receive and transmit data, and can allow further routers and end devices to join the network. It can also exercise a useful function (e.g. measurement). It cannot sleep.

The coordinator: This is the most capable Zigbee device; there can be only one in a network. It launches a network by selecting a PAN ID, and a channel to communicate over. It can allow routers and end devices to join the network. It cannot sleep, so must normally be mains powered.

All Zigbee devices have a 16-bit and a 64-bit address. The latter – sometimes called the extended address - is assigned at manufacture and is unique.

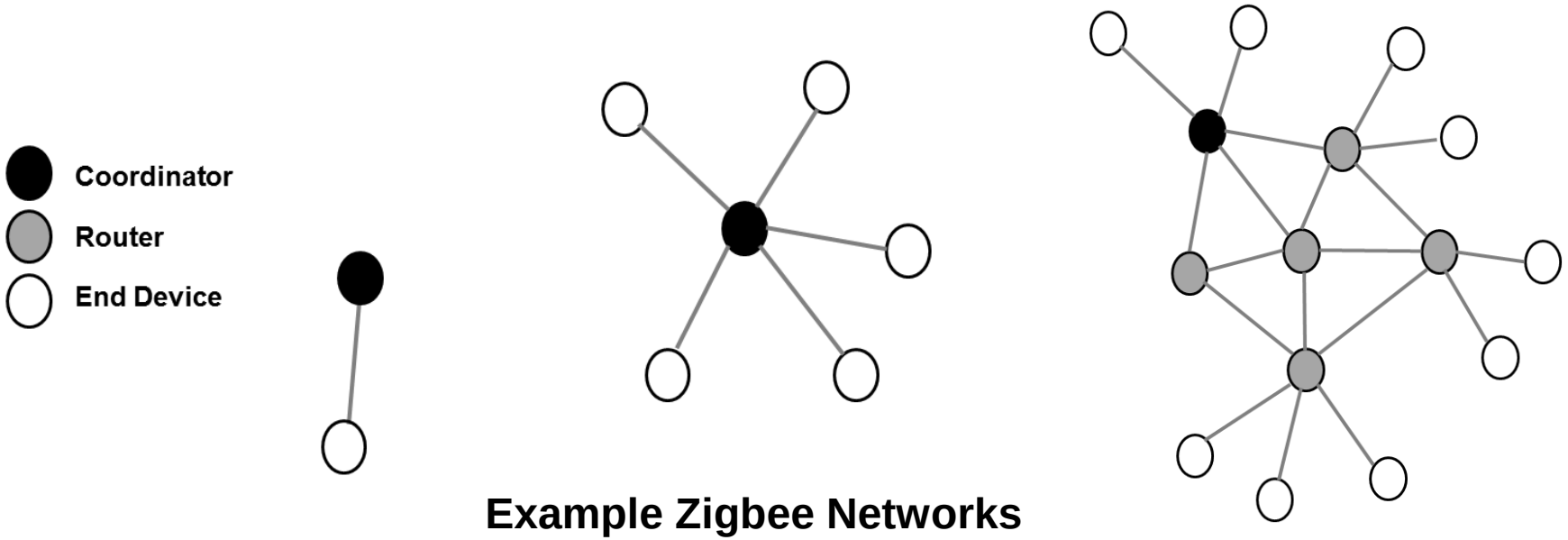
Zigbee Device Types

The Figure shows example Zigbee networks of increasing complexity, applying the three device types.

Each network, once established, is defined by a 64-bit (previously 16-bit) PAN ID (Personal Area Network identifier).

A device receives a 16-bit address as it joins a network, sometimes called the *network address*. This address is not permanent. If the device left the network and then re-joined, it would probably be assigned a different address.

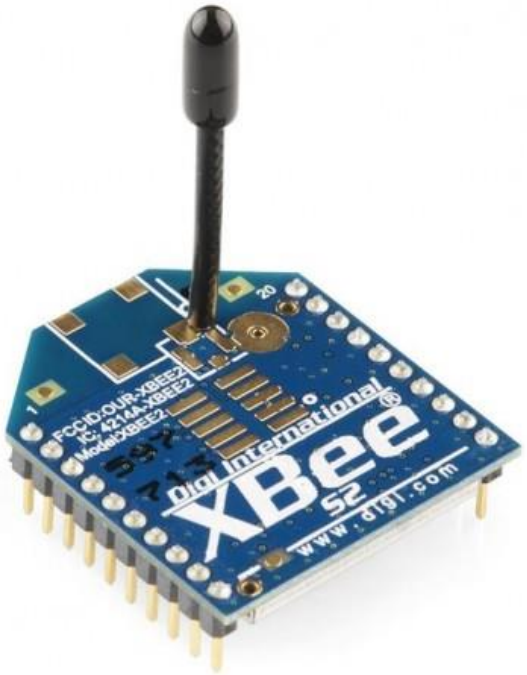
Zigbee data can be sent unicast (from one device to a specific target device) or broadcast (throughout the entire network).



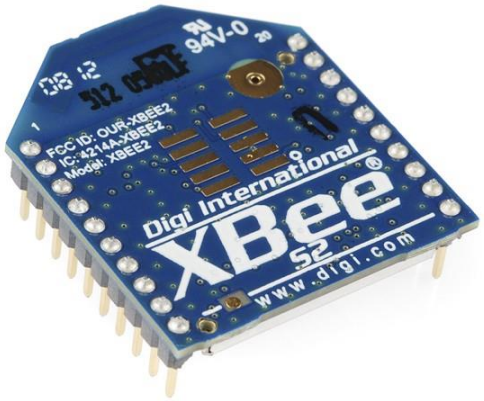
Example Zigbee Networks

Introducing XBee Wireless Modules

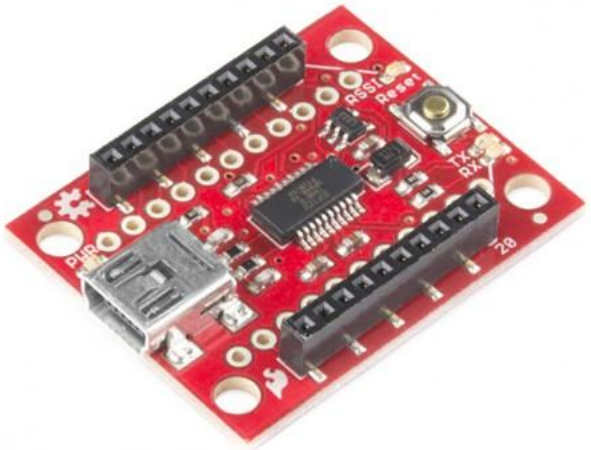
The XBee wireless modules, made by Digi International, can be used rapidly to configure Zigbee networks.



XBee with whip antenna



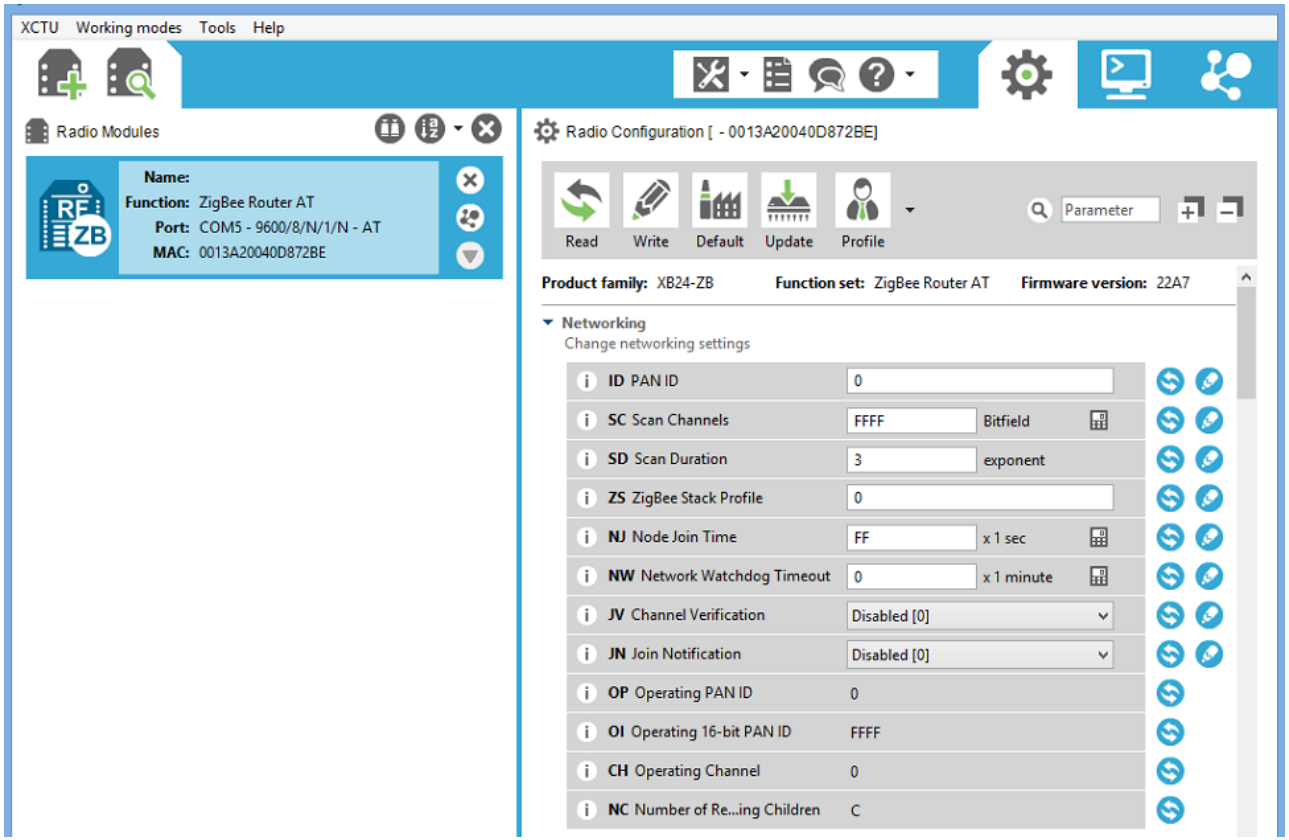
XBee with pcb antenna



XBee Explorer USB interface

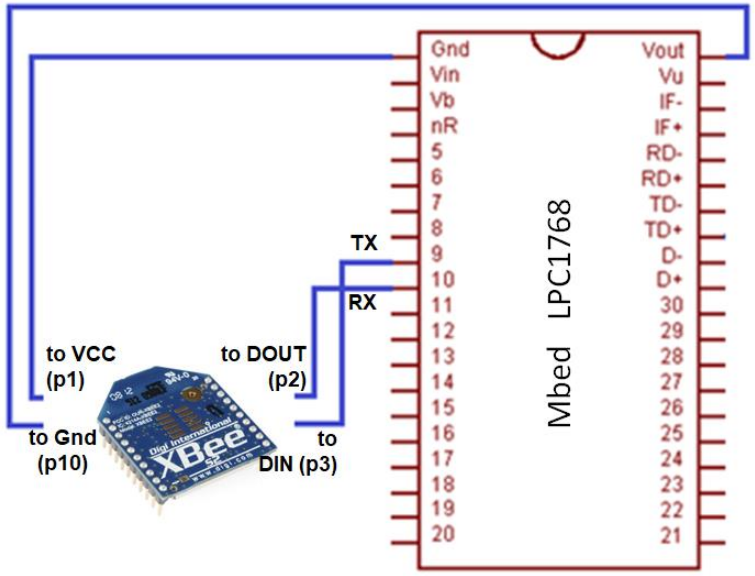
Linking to the XBee from a PC

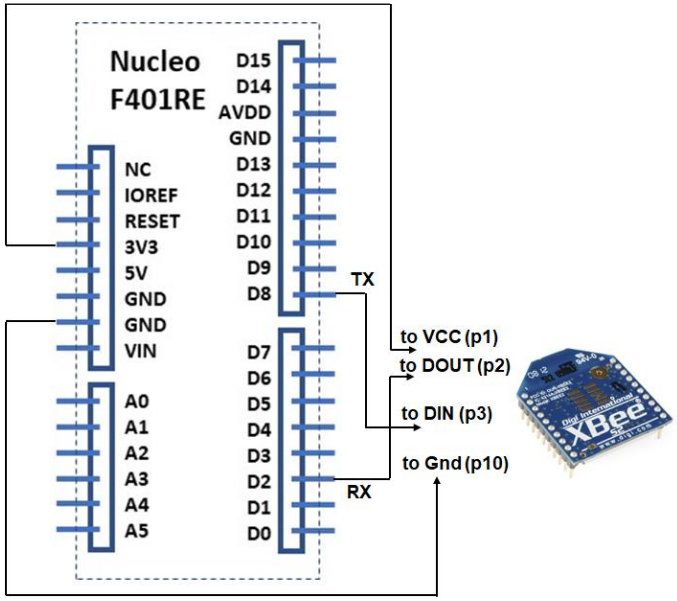
Zigbee to PC connectivity can be set up with two extra pieces of kit. The first is a USB interface such as the Explorer, shown earlier, providing a USB link from PC to XBee. The second is the official interface software from Digi, XCTU, downloaded from the Digi web site. This allows diagnostic testing of an XBee, downloading of new firmware, plus access to remote XBee devices by radio link. Using XCTU, the XBee device can be configured as coordinator, router or end device.



Implementing a Zigbee PC link to XBee and Mbed

Connect a preconfigured (wth XCTU) router XBee in one of the circuits shown. Compile and download the programme example on the next slide into the Mbed. A coordinator XBee is placed in the USB Explorer, plugged into the host PC. With Tera Term or CoolTerm running, the terminal should continuously count from 0 to 9, with the Mbed LEDs counting up in synchronism.





Implementing a Zigbee PC link to XBee and Mbed

```
/* Program Example 11.7: Zigbee serial test data program.
Data is transferred from Mbed to PC via Zigbee to Zigbee link.
Requires a set of "paired" XBee modules. The Zigbee coordinator connects with
the PC, the router with the Mbed.
Works with both LPC1768 and F401RE, with pin connections shown */

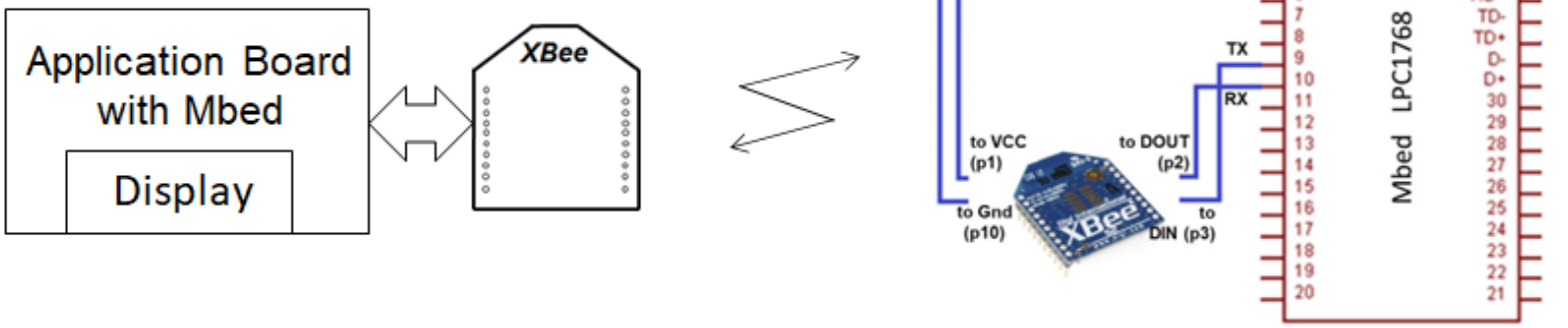
#include "mbed.h"

//name the serial port xbee
BufferedSerial xbee(p9,p10);      //Use D8,D2 for F401RE
BusOut leds(LED4,LED3,LED2,LED1);  //Use A1,A0,D12,D13 or own choice for F401RE
char buf[8] = {0};            //declare 8-byte buffer, initialise to 0

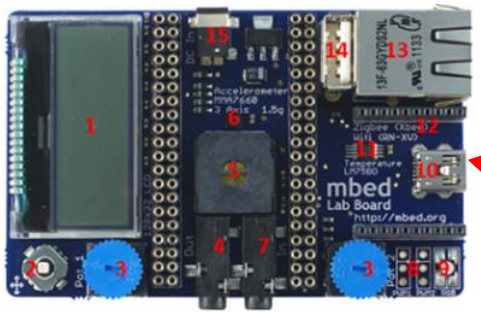
int main() {
  xbee.set_baud(9600);     // set baud rate for xbee
  while (true) {
    for (char x = 0x30;x <= 0x39;x++){  // ASCII numerical characters 0-9
      buf[0] = x;
      xbee.write(buf,1);    //transmit current value of x
      leds = x&0x0F;        // set LEDs to count in binary
      ThisThread::sleep_for(500ms);
    }
  }
}
```

Implementing a Zigbee Link Mbed to Mbed

It is a simple step to set up an XBee to XBee link, with no PC intervention. The Mbed app board has a very useful XBee socket. While the Mbed LPC1768 is shown here, the F401RE can equally be used. Full program details are given in the book.



Coordinator **Router**

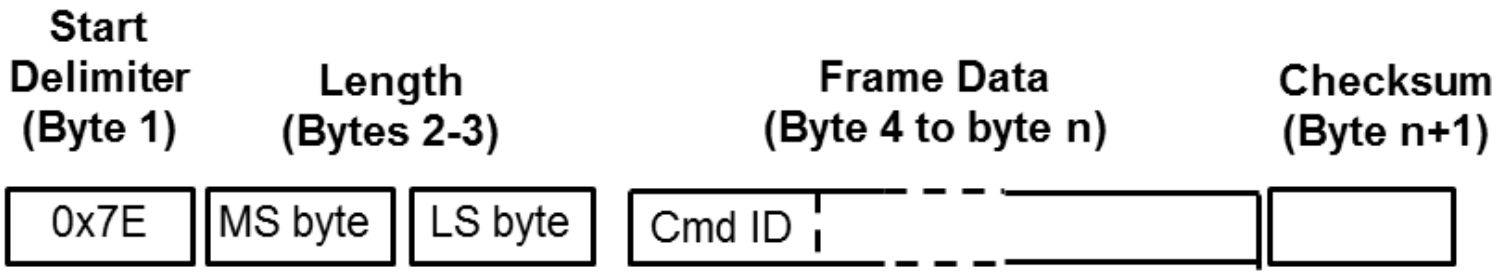


App board XBee socket

Introducing the XBee API

The XBee can operate in AT or API modes. It is the API mode which unlocks the power of Zigbee through the XBee. Using the API, the XBee can change the destination address dynamically, perform error checking, reconfigure remote radios, and exploit the remote XBee I/O capability.

In API mode all data is packaged into *frames,* which carry both the data itself, plus a range of ID, addressing, and error-checking capability.



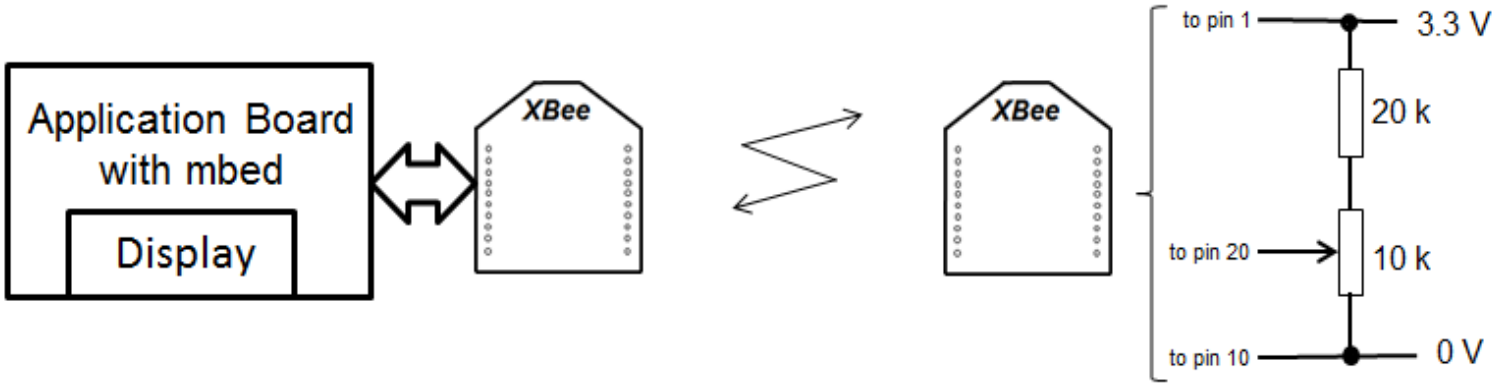
General XBee API data frame structure

Applying the XBee API

In this Zigbee link, one XBee is set up as a standalone device, configured as a router and making analog measurements. It remains in AT mode. Its pin 20, labelled ADO/DIO0, is configured as analog input. It periodically transmits data values to an XBee coordinator.

The coordinator can run in an Mbed App board, as pictured; alternative arrangements also work. The coordinator now runs in API mode.

The XBee ADC is a 10-bit device, and has an input range of 1.2 V. A potentiometer has been chosen to provide this simple analog source, as shown. This has itself been placed in a potential divider, through the addition of the 20 kΩ resistor, to match the ADC input range.



Diagnostic circuit for API trial

LoRa and LoRaWAN

LoRa (a contraction of “Long Range”), is one of a series of long-range, low data rate wireless communication technologies designed for power constrained embedded systems – especially those running on battery power.

LoRa supports data transfer rates in the 0.3 to 5.5 kilobits per second range. It claims a transmission distance of up to 16 km line of sight, or 5 km in built-up areas. It also claims good communication in “difficult” settings, for example through concrete and in tunnels.

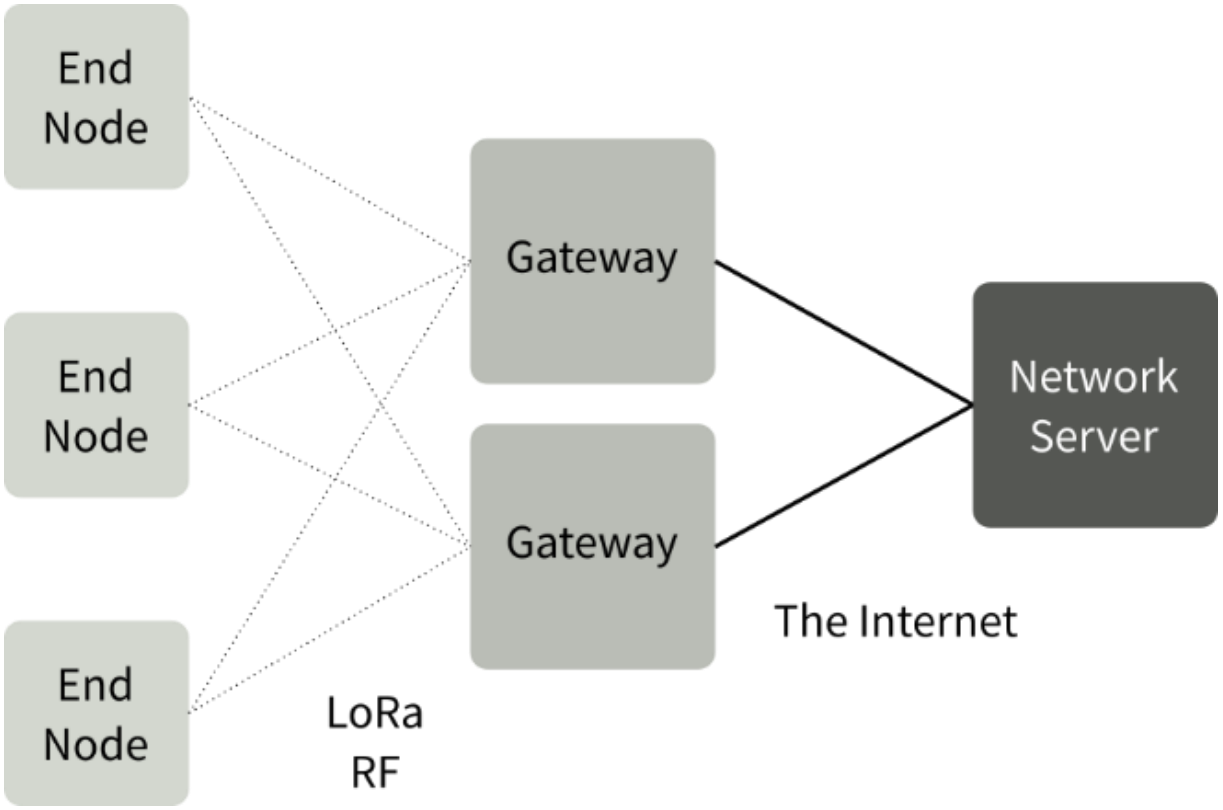
LoRa is a proprietary protocol, based on a chirp spread spectrum technique that defines the physical layer for long range communication, and on its own doesn’t dictate the actual communication protocol.

LoRaWAN is a protocol that defines an overall architecture, and specifies how devices communicate. As the name suggests, it uses LoRa for the physical layer, and overlays wide area networking capabilities.

LoRaWAN appears to offer the impossible – long range communication at extremely low power, albeit at the price of low data rate. It opens many doors to remote sensing opportunities, in areas without mobile phone, cable or fibre coverage.

LoRaWAN

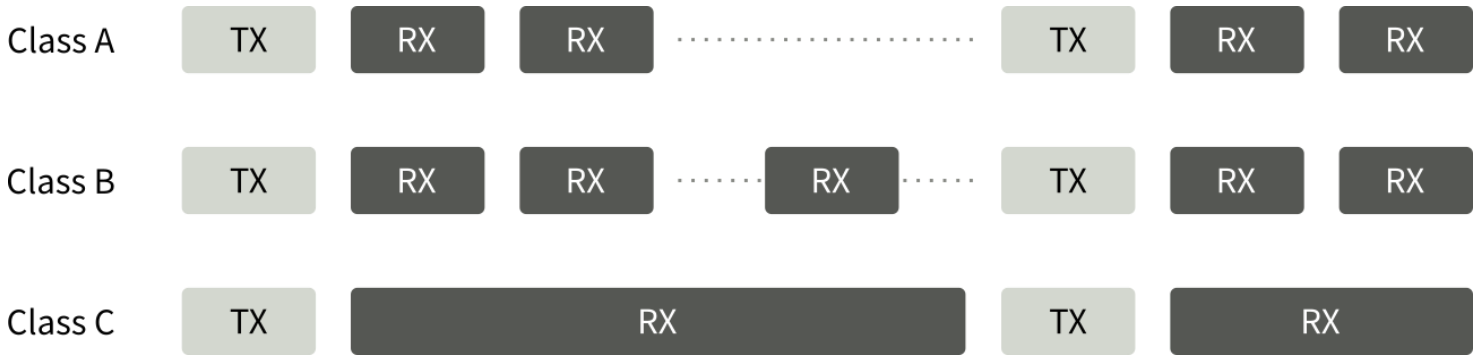
A typical LoRaWAN architecture is shown. It comprises “end nodes”, “gateways”, and “network servers”. The end node is the actual embedded device deployed in the field, which establishes an RF link with the gateway. This forwards data to the network server, usually over a WAN (such as the internet), which can then transfer it on as needed.



LoRaWAN

The LoRaWAN specification defines three classes of device, as illustrated:

- **Class A:** an end node initiates a transmission, which is immediately followed by two short receive windows where data can be received. All LoRaWAN devices must support Class A operation.
- **Class B:** operates as in Class A, but additional receive windows are available at scheduled times for non-device-initiated receives.
- **Class C:** the receive window is continuously open, except when transmitting. This imposes additional power requirements, i.e. the device must be continuously powered.



Transmit (TX) and Receive (RX) windows for different device classes

Chapter Review

- Wireless links exploit the characteristics of the electromagnetic spectrum, notably in radio, infra-red or visible light.
- A wide range of protocols and technologies exist to implement wireless data links across personal, local, neighbourhood and wide area networks.
- Bluetooth Low Energy is a complex, yet effective protocol defined within the IEEE 802 group, which allows Bluetooth-enabled devices to connect and transfer data wirelessly, with potentially high data rates.
- Zigbee is another important protocol defined within the IEEE 802 group, targeted towards low data rate, distributed measurement systems, and extreme low power.
- The XBee module provides Zigbee capability, which can be linked to an Mbed target. The XBee has its own on-board processing power and input/out capability, so can also readily act as a stand-alone device.
- LoRaWAN brings long transmission ranges to low-power communication, with the trade-off of lower data rates.