PHY + MAC for WPAN, WLAN, WMAN

Bluetooth, ZigBee, WiFi, WiMAX, LTE

Contents

wireless network technology options

Network definition	*standard*	*Known as*
Wireless personal area network (WPAN)	IEEE 802.15.1	Bluetooth
Low-rate WPAN (LR-WPAN)	IEEE 802.15.4	ZigBee
Wireless local area network (WLAN)	IEEE 802.11	WiFi
Wireless metroplitan area network (WMAN)	IEEE 802.16	WiMAX
Long Term Evolution (LTE)	IMT-Advaced/3GPP	LTE Advanced

ISM frequency bands

ISM (Industrial, Scientific and Medical) frequency bands:

- 900 MHz band (902 … 928 MHz)
- 2.4 GHz band (2.4 … 2.4835 GHz)
- 5.8 GHz band (5.725 … 5.850 GHz)
- 60 GHz band
- …

Anyone is allowed to use radio equipment for transmitting in these bands (provided specific transmission power limits are not exceeded) without obtaining a license.

ISM frequency band at 2.4 GHz

The ISM band at 2.4 GHz can be used by anyone as long as

Transmitters using FH (Frequency Hopping) technology:

- Total transmission power < 100 mW
- Power density < 100 mW / 100 kHz

Transmitters using DSSS technology:

- Total transmission power < 100 mW
- Power density < 10 mW / 1 MHz

Multiplexing / multiple access / duplexing

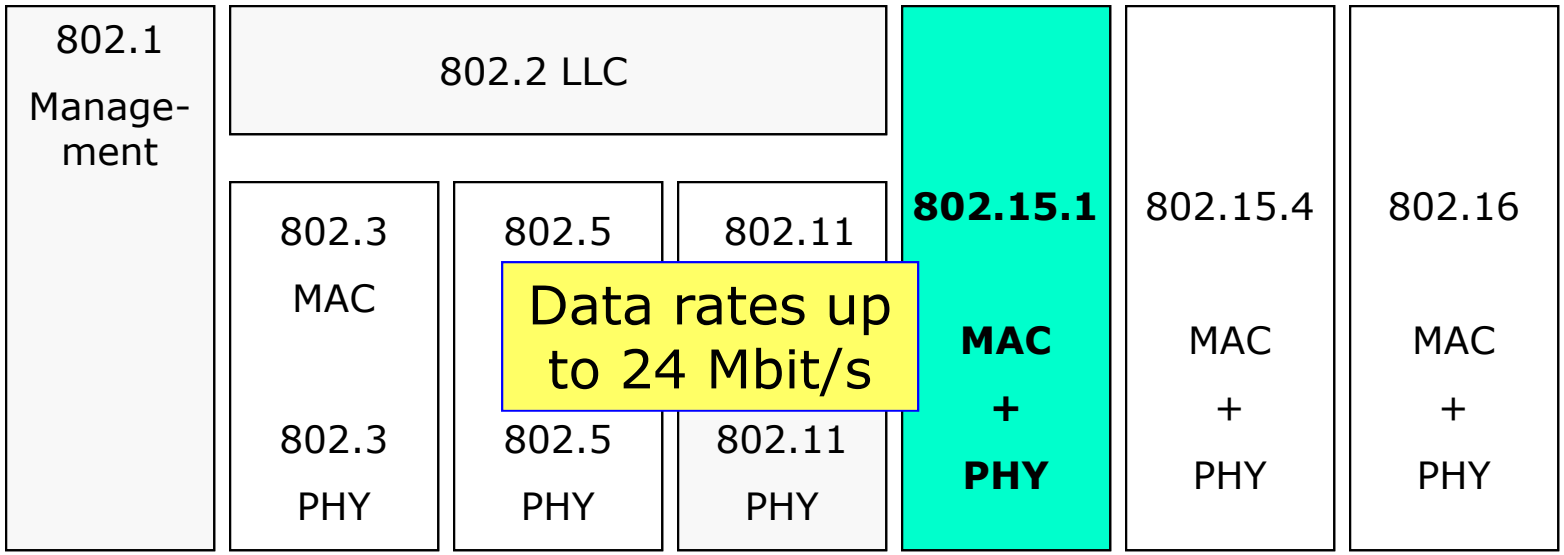
Multiplexing / multiple access

Signals to/from different users share a common channel using time division methods (TDMA), frequency division methods (FDMA), code division methods (CDMA), or random access methods (CSMA).

Duplexing:

The signals moving between two elements in opposite directions can be separated using time division duplexing (TDD) or frequency division duplexing (FDD). In the case of CSMA, duplexing is not relevant.

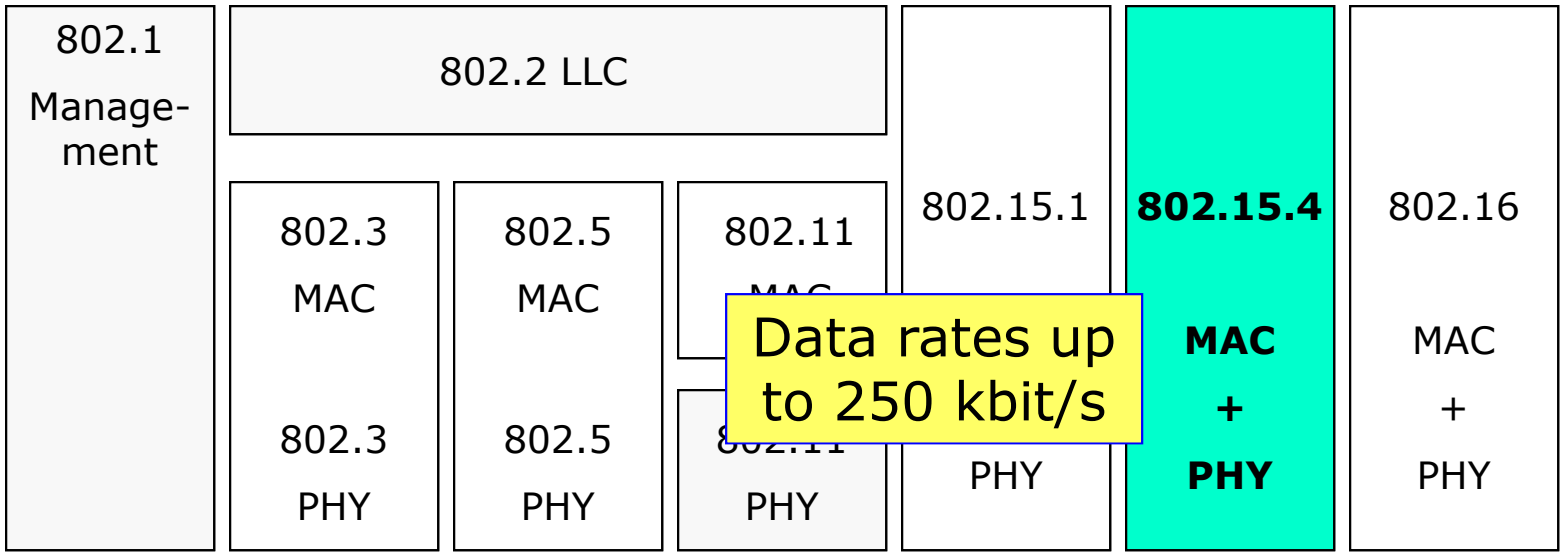
Wireless Personal Area Network (WPAN) ≈ 10m



ISM band: 2.4 … 2.4835 GHz

Bluetooth Special Interest Group (SIG)

Low-rate WPAN (LR-WPAN) ≈ 10m



ISM band: 2.4 … 2.4835 GHz

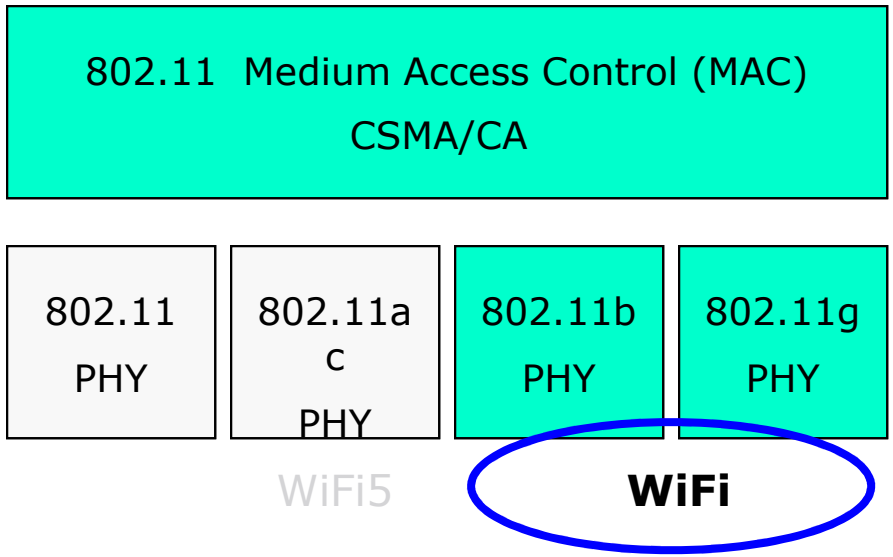
ZigBee Alliance

Wireless Fidelity (WiFi) ≈ 100m

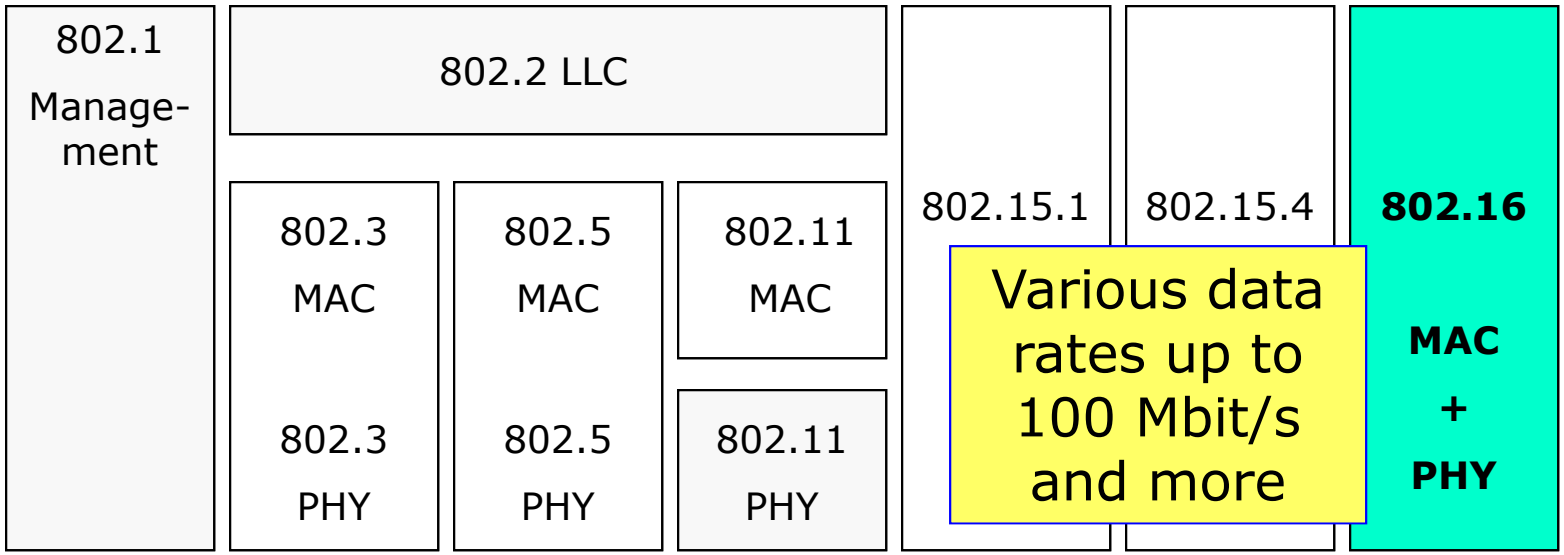
The WiFi certification program of the Wireless Ethernet Compatibility Alliance (WECA) addresses compatibility of IEEE 802.11 equipment

=>

WiFi ensures interoperability of equipment from different vendors.



Wireless Metropolitan Area Network (WMAN) ≈ 5km



Various frequency bands (not only ISM)

WiMAX, LTE-Advanced

Maximum channel data rates

Network	*Maximum data rate*
IEEE 802.15.1 WPAN (Bluetooth)	1 Mbit/s (Bluetooth v. 1.2) 24 Mbit/s (Bluetooth v. 4.0 for IoT)
IEEE 802.15.4 LR-WPAN (ZigBee)	250 kbit/s (ZigBee)
IEEE 802.11 WLAN (WiFi)	11 Mbit/s (802.11b) 54 Mbit/s (802.11g) 1 Gpbs (802.11ac/n)
IEEE 802.16 WMAN (WiMAX)	134 Mbps (WiMAX)
LTE-Advanced	DL 3 Gbps, UL 1.5 Gbps; 30 bps/Hz spectral efficiency

Modulation / Signal spreading

Network	*Modulation / spreading method*
IEEE 802.15.1 WPAN (Bluetooth)	Gaussian FSK / FHSS
IEEE 802.15.4 LR-WPAN (ZigBee)	Offset-QPSK / DSSS
IEEE 802.11 WLAN (WiFi)	DQPSK / DSSS (802.11b) 64-QAM / OFDM (802.11g)
IEEE 802.16 WMAN (WiMAX)	128-QAM / single carrier 64-QAM / OFDM
LTE-Advanced	64QAM / single carrier 64QAM / OFDM

Bluetooth

IEEE definition of WPAN

Wireless personal area networks (WPANs) are used to convey information over short distances among a private, intimate group of participant devices.

Unlike a wireless local area network (WLAN), a connection made through a WPAN involves little or no infrastructure or direct connectivity to the world outside the link. This allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices.

Bluetooth ≈ IEEE 802.15.1

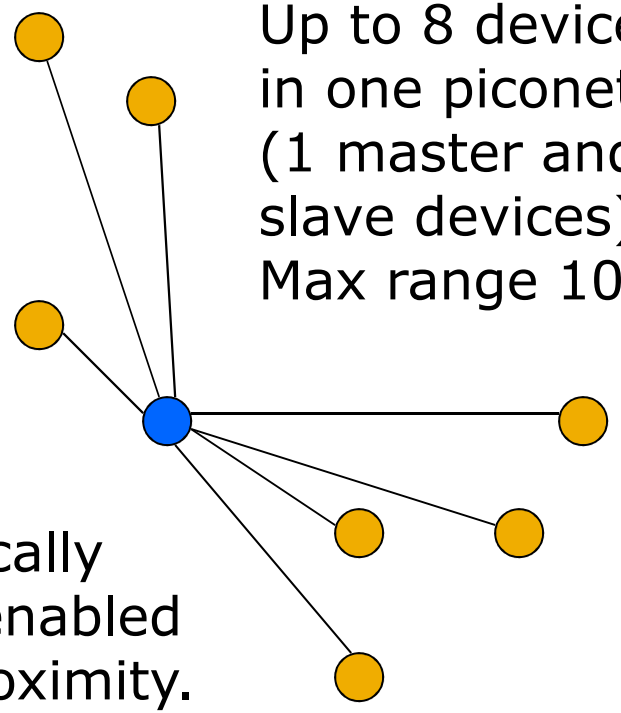
A widely used WPAN technology is known as Bluetooth (version 1.2 - version 4.0)

The IEEE 802.15.1 standard specifies the architecture and operation of Bluetooth devices, but only as far as physical layer and medium access control (MAC) layer operation is concerned (the core system architecture).

Higher protocol layers and applications defined in usage profiles are standardised by the Bluetooth SIG.

Piconets

Bluetooth enabled electronic devices connect and communicate wirelessly through short-range, ad hoc networks known as piconets.



Up to 8 devices in one piconet (1 master and 7 slave devices). Max range 10 m.

ad hoc => no base station

Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave radio proximity.

Piconet operation

The piconet master is a device in a piconet whose clock and device address are used to define the piconet physical channel characteristics. All other devices in the piconet are called piconet slaves.

At any given time, data can be transferred between the master and one slave. The master switches rapidly from slave to slave in a round-robin fashion.

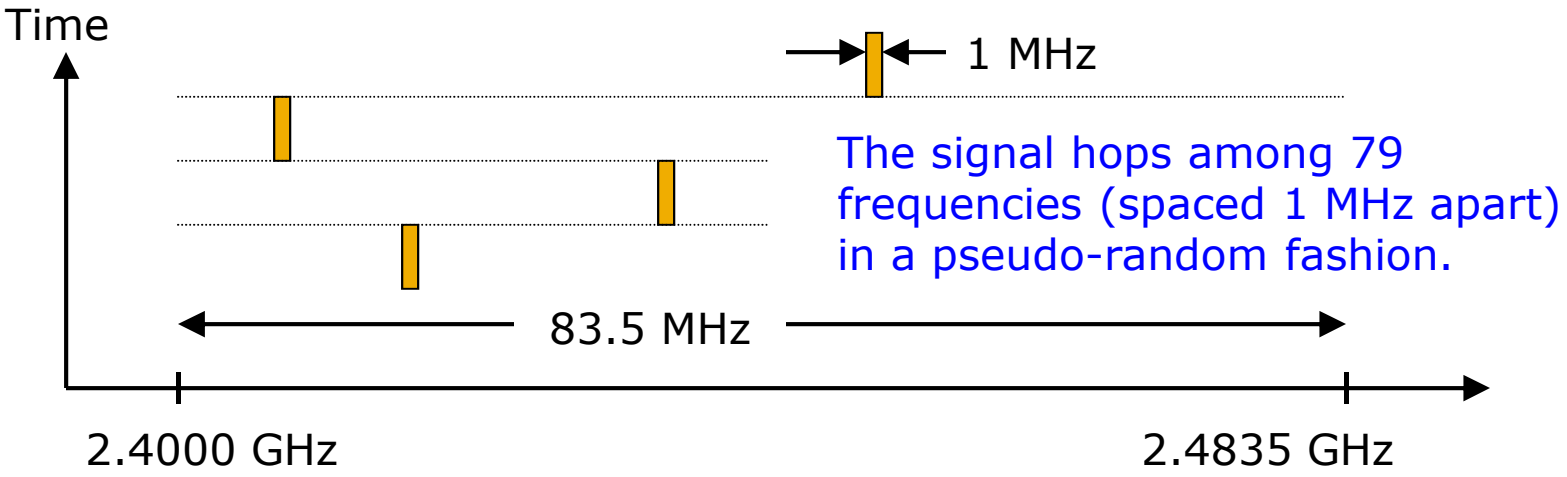
Any device may switch the master/slave role at any time.

Bluetooth radio and baseband parameters

Topology	Up to 7 simultaneous links
Modulation	Gaussian filtered FSK
RF bandwidth	220 kHz (-3 dB), 1 MHz (-20 dB)
RF band	2.4 GHz ISM frequency band
RF carriers	79 (23 as reduced option)
Carrier spacing	1 MHz
Access method	FHSS-TDD-TDMA
Freq. hop rate	1600 hops/s

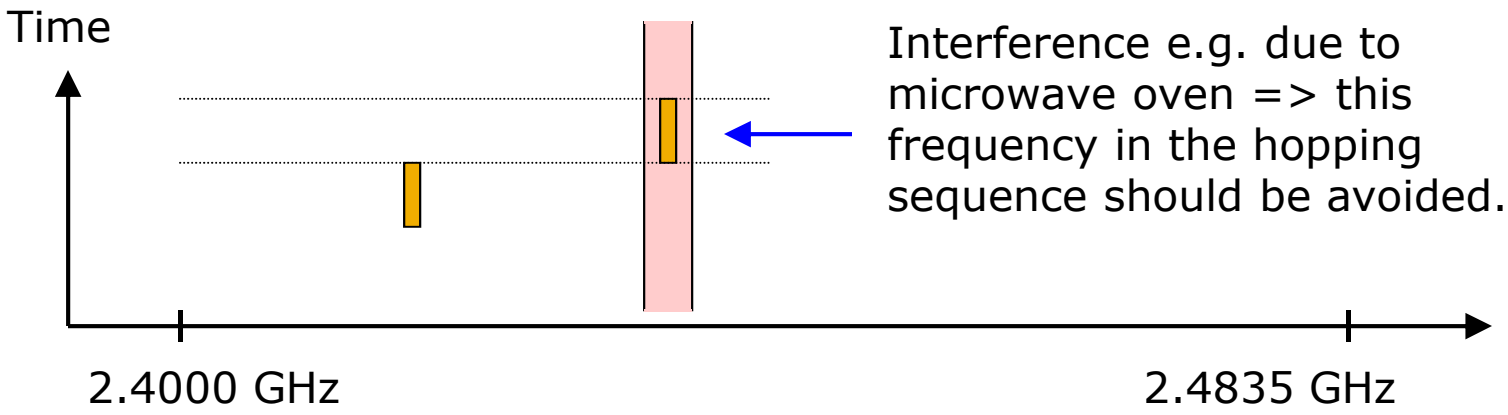
Frequency hopping spread spectrum (1)

Bluetooth technology operates in the 2.4 GHz ISM band, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/second.



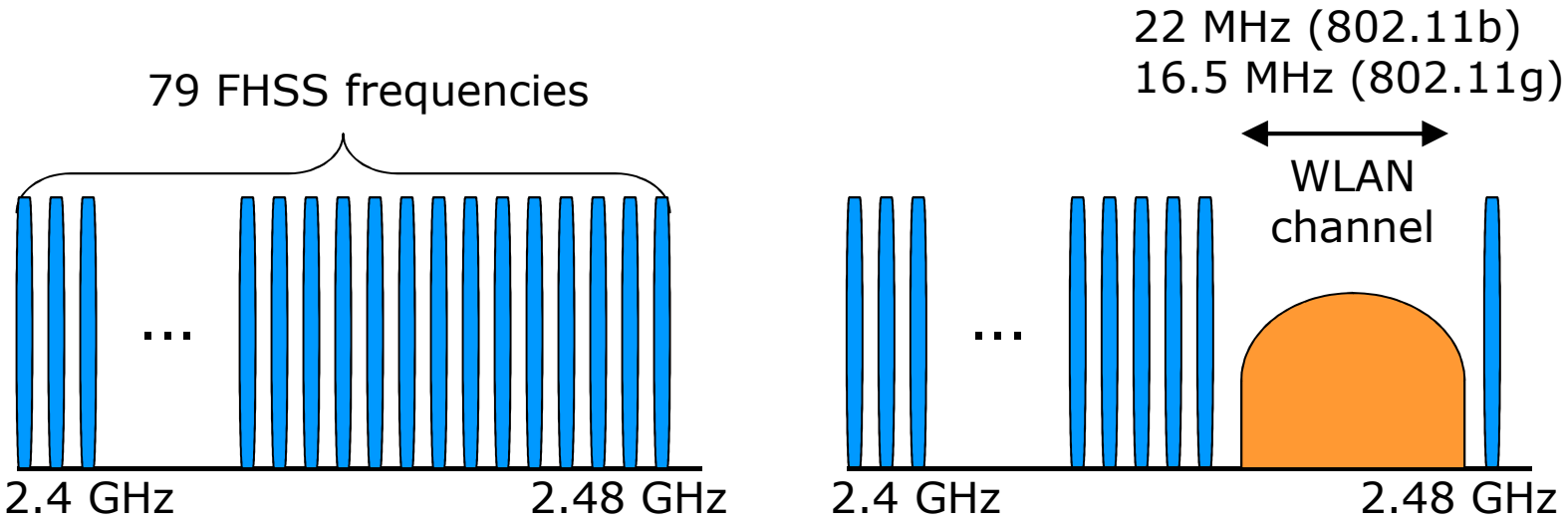
Frequency hopping spread spectrum (2)

The adaptive frequency hopping (AFH) feature (from Bluetooth version 1.2 onward) is designed to reduce interference between wireless technologies sharing the 2.4 GHz spectrum.



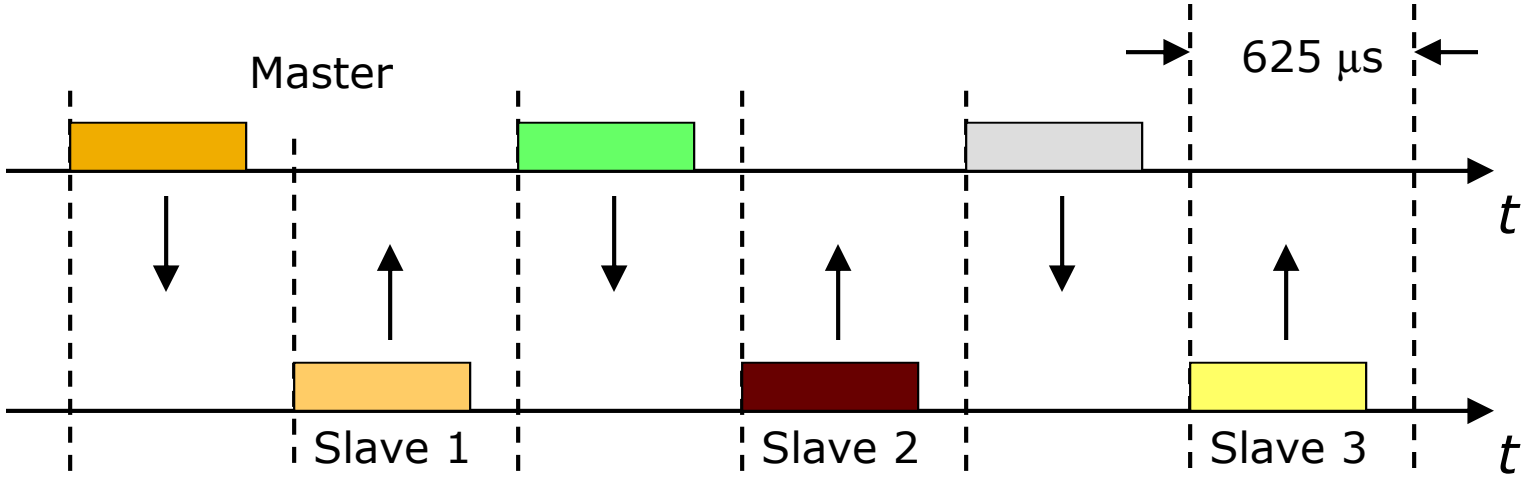
Frequency hopping spread spectrum (3)

In addition to avoiding microwave oven interference, the adaptive frequency hopping (AFH) feature can also avoid interference from WLAN networks:



Frequency hopping in action (1)

The piconet master decides on the frequency hopping sequence. All slaves must syncronise to this sequence. Then transmission can take place on a TDD-TDMA basis.



Link delivery services

Two types of links can be established between the piconet master and one or more slaves:

Synchronous connection-oriented (SCO) link allocates a fixed bandwidth for a point-to-point connection involving the piconet master and a slave. Up to three simultaneous SCO links are supported in a piconet.

Asynchronous connectionless or connection-oriented (ACL) link is a point-to-multipoint link between the master and all the slaves in the piconet. Only a single ACL link can exist in the piconet.

SCO links

SCO links are used primarily for carrying real-time data (speech, audio) where large delays are not allowed (so that retransmission cannot be used) and occasional data loss is acceptable.

The guaranteed data rate is achieved through reservation of slots. The master maintains the SCO link by using reserved slots at regular intervals. The basic unit of reservation is two consecuive slots - one in each transmission direction. An ACL link must be established (for signalling) before an SCO link can be used.

ACL link

The ACL link offers packet-switched data transmission. No bandwidth reservation is possible and delivery may be guaranteed through error detection and retransmission.

A slave is permitted to send an ACL packet in a slave-to-master slot only if it has been adressed in the preceeding master-to-slave slot.

For ACL links, 1-, 3-, and 5-slot packets have been defined. Data can be sent either unprotected (although ARQ can be used at a higher layer) or protected with a 2/3 rate forward error correction (FEC) code.

Connection Setup (Inquiry/Paging)

A connection between two devices occur in the following fashion:

- **Step 1:** The **inquiry procedure** enables a device to discover which devices are in range, and determine the addresses and clocks for the devices.
- **1.1:**The inquiry procedure involve the source sending out inquiry packets and then receiving the inquiry reply
- **1.2:**The destination that receives the inquiry packets, will hopefully be in the "**inquiry scan** state" to receive the inquiry packets.
- **1.3:**The destination will then enter the **"inquiry response** state" and send an inquiry reply to the source.

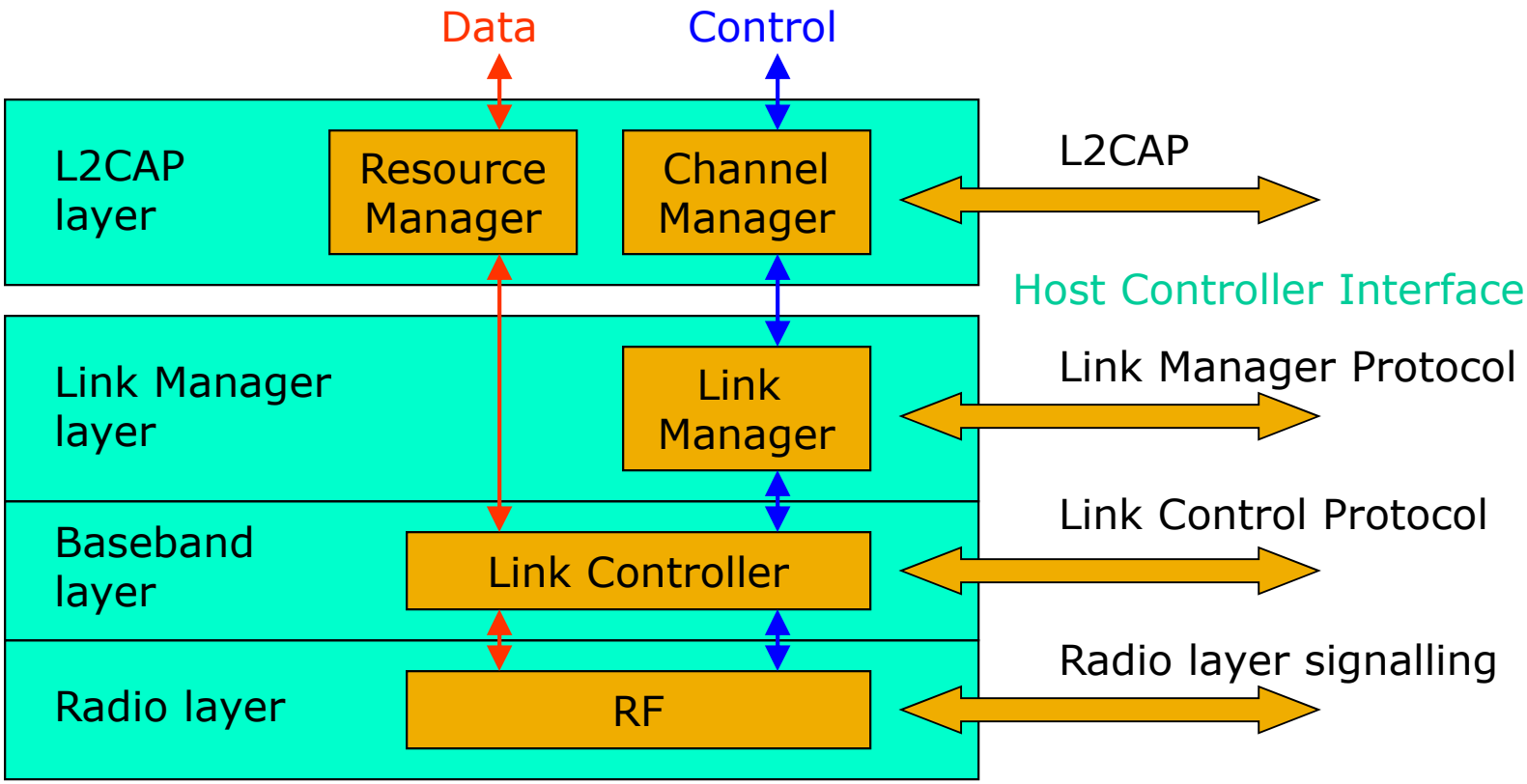
After the inquiry procedure has completed, a connection can be established using the paging procedure.

Connection Setup (Inquiry/Paging)

- With the **paging procedure**, an actual connection can be established. Only the Bluetooth device address is required to set up a connection. A unit that establishes a connection will carry out a page procedure and will automatically be the master of the connection. The procedure occurs as follows:

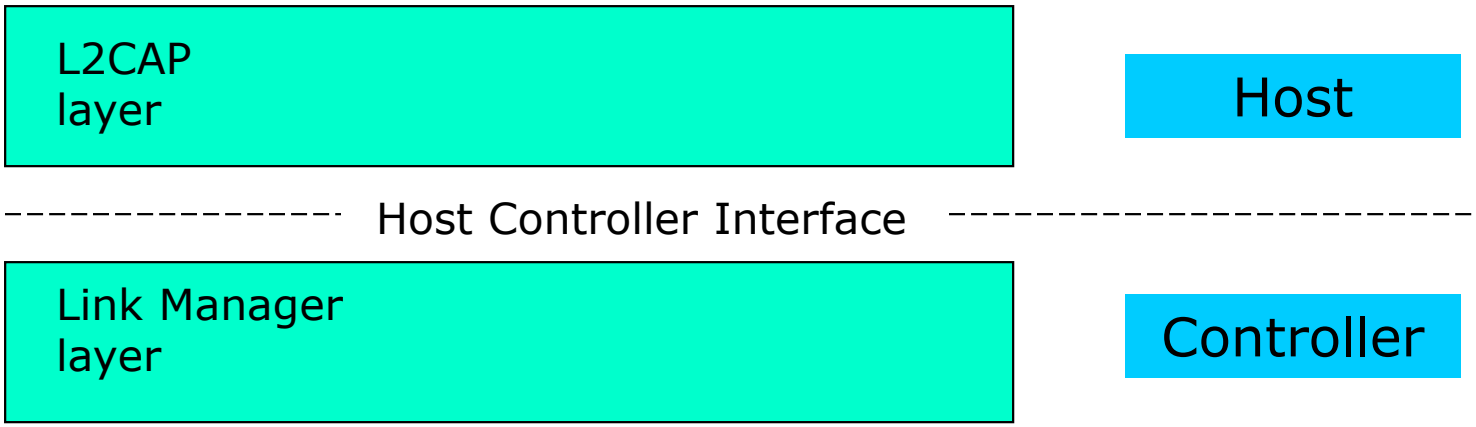
- **2.1:** The source device pages the destination device
- **2.2:**The destination receives the page while in the "**Page Scan** state"
- **2.3:**The destination sends a reply to the source
- **2.4:**The source sends an FHS packet to the destination.
- **2.5:**The destination sends it's second reply to the source.
- **2.6:**The destination & source then switch to the source channel parameters.
- The **Connection** state starts with a POLL packet sent by the master to verify that slave has switched to the master's timing and channel frequency hopping. The slave can respond with any type of packet.

Bluetooth core system architecture



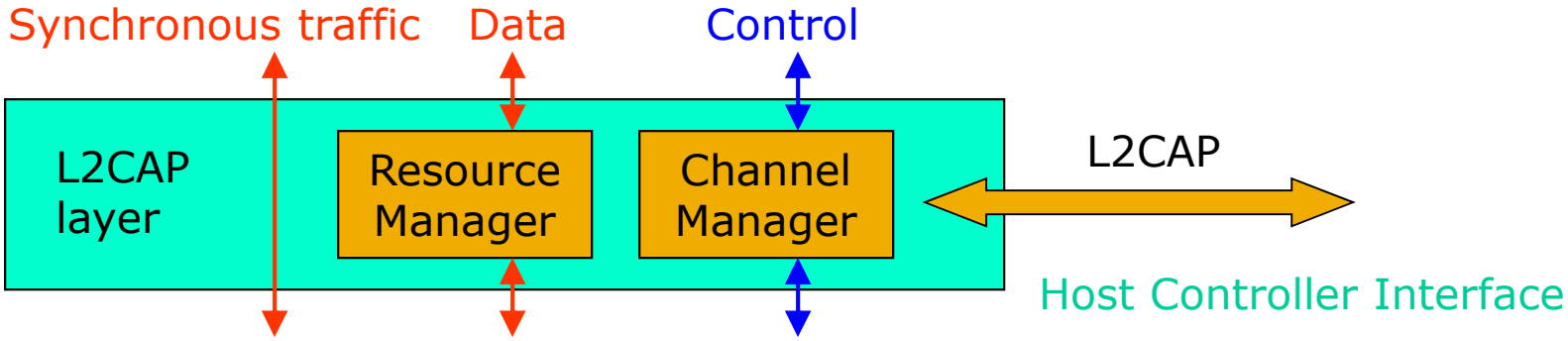
Host controller interface

The open host controller interface resides between the Bluetooth controller (e.g. PC card) and Bluetooth host (e.g. PC). In integrated devices such as Bluetooth-capable mobile devices this interface has little or no significance.



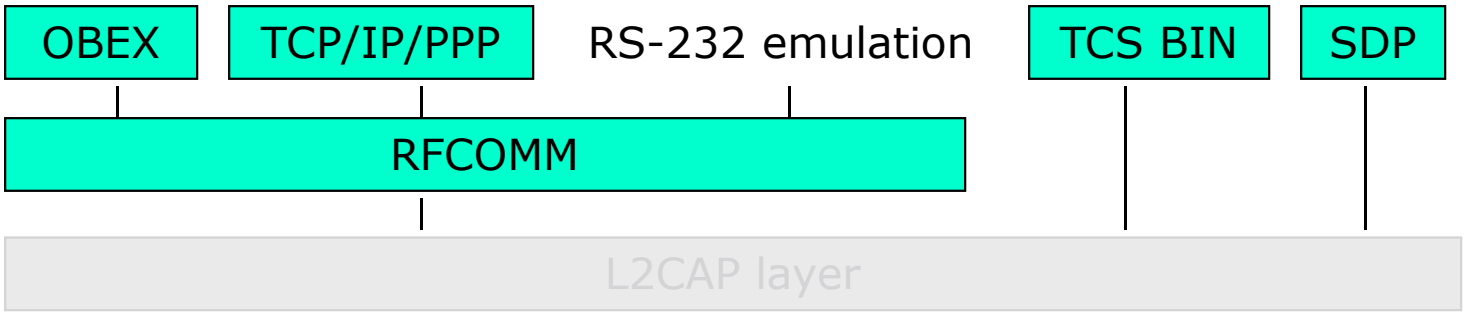
L2CAP layer

The Logical Link Control and Adaptation Protocol (L2CAP) layer handles the multiplexing of higher layer protocols and the segmentation and reassembly (SAR) of large packets. The L2CAP layer provides both connectionless and connection-oriented services.



Higher protocol layers (1)

The operation of higher protocol layers is outside the scope of the IEEE 802.15.1 standard (but included in the Bluetooth SIG standards). The usage of these protocols depends on the specific Bluetooth profile in question. A large number of Bluetooth profiles have been defined.



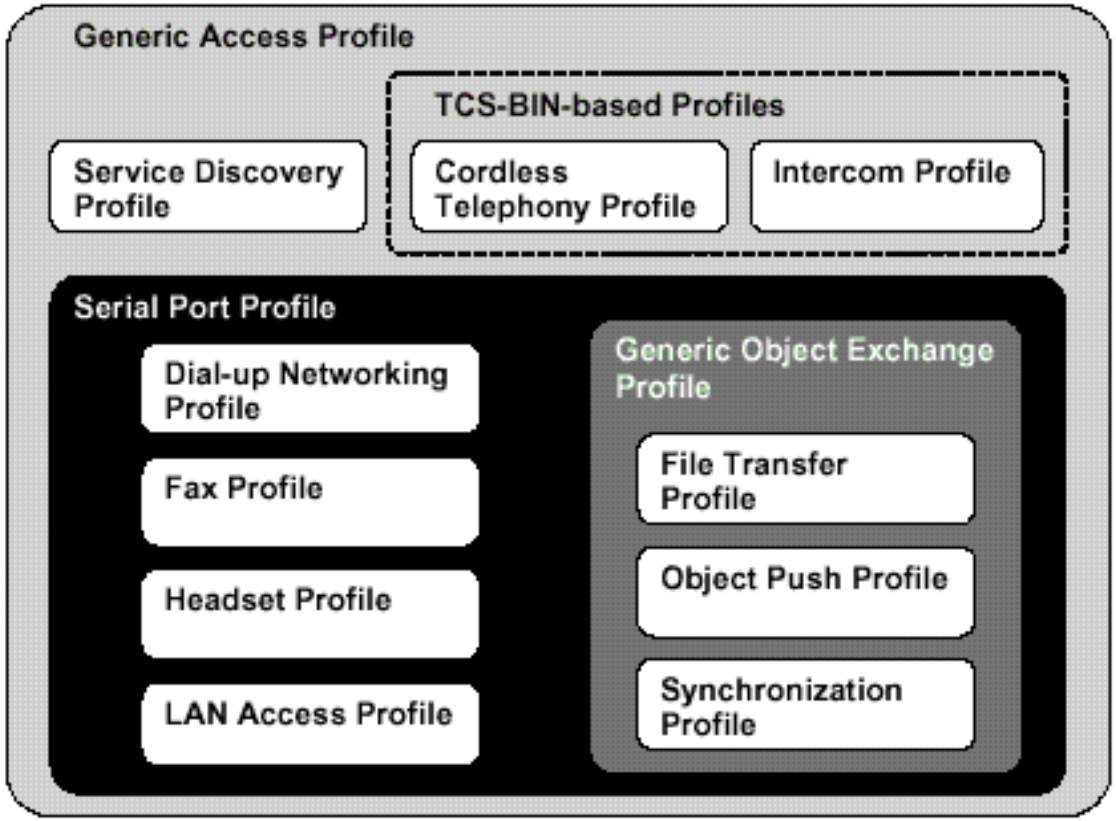
Other Bluetooth protocols

- RFCOMM: Provides emulation of serial ports over L2CAP.
- Service Discovery Protocol (SDP):
  - Provides attribute based searching of services.
  - Provides for browsing through available services.
  - Provides means of discovering new services.
  - Provides removal of unavailable services.

Bluetooth profiles

- Describe configuration of the Bluetooth stack for different types of applications.
- Specify minimum requirements from Bluetooth layers for each profile.
- The Generic Access Profile provides a basic level of functionality that all Bluetooth devices must implement.

Bluetooth profiles



ZigBee

IEEE 802.15.4 LR-WPAN (ZigBee)

ZigBee technology is simpler (and less expensive) than Bluetooth.

The main objectives of an LR-WPAN like ZigBee are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.

The raw data rate will be high enough (maximum of 250 kbit/s) to satisfy a set of simple needs such as interactive toys, but is also scalable down to the needs of sensor and automation needs (20 kbit/s or below) using wireless communications.

LR-WPAN device types

Two different device types can participate in an LR-WPAN network:

- Full-function devices (FFD) can operate in three modes serving as a personal area network (PAN) coordinator, a coordinator, or a device.
- Reduced-function devices (RFD) are intended for applications that are extremely simple.

An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD.

Network topologies (1)

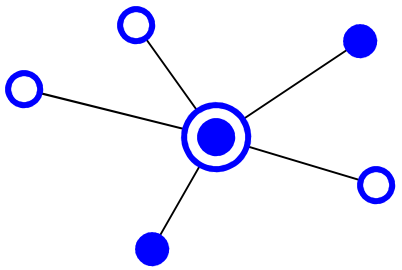
Two or more devices communicating on the same physical channel constitute a WPAN. The WPAN network must include at least one FFD that operates as the PAN coordinator.

The PAN coordinator initiates, terminates, or routes communication around the network. The PAN coordinator is the primary controller of the PAN.

The WPAN may operate in either of two topologies: the star topology or the peer-to-peer topology.

Network topologies (2)

Star topology



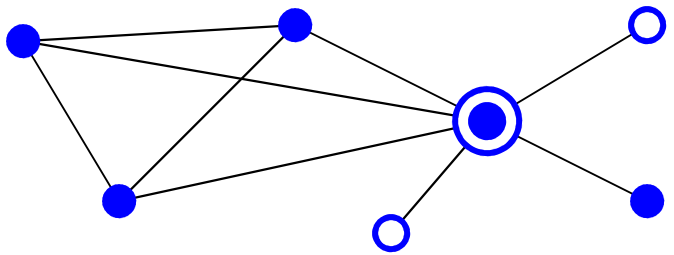
In a star network, after an FFD is activated for the first time, it may establish its own network and become the PAN coordinator.

The PAN coordinator can allow other devices to join its network.

Network topologies (3)

In a peer-to-peer network, each FFD is capable of communicating with any other FFD within its radio sphere of influence. One FFD will be nominated as the PAN coordinator.

Peer-to-peer topology



A peer-to-peer network can be ad hoc, self-organizing and self-healing, and can combine devices using a mesh networking topology.

ZigBee PHY and MAC parameters

Topology	Ad hoc (central PAN coordinator)
RF band	2.4 GHz ISM frequency band
RF channels	16 channels with 5 MHz spacing
Spreading	DSSS (32 chips / 4 bits)
Chip rate	2 Mchip/s
Modulation	Offset QPSK

Access method	CSMA/CA

CSMA/CA operation

Each time a device wishes to transmit data frames or MAC commands, it shall wait for a random period. If the channel is found to be idle, following the random backoff, the device shall transmit its data. If the channel is found to be busy, following the random backoff, the device shall wait for another random period before trying to access the channel again.

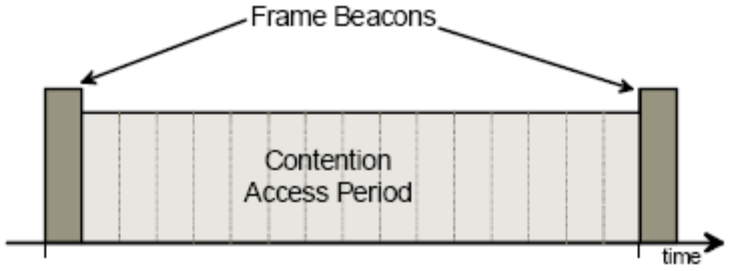
Acknowledgment frames shall be sent without using a CSMA-CA mechanism.

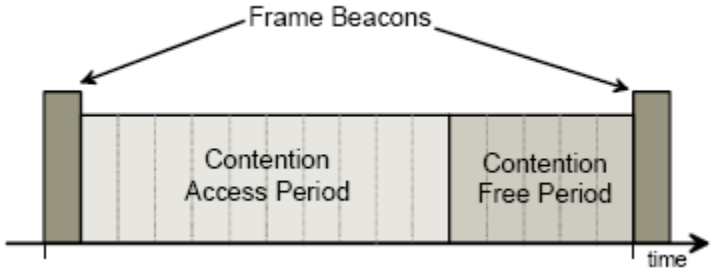
Types of ZigBee PANs

- Non-Beacon Enabled PAN
  - Un-slotted CSMA/CA
- Beacon Enabled PAN
  - Slotted CSMA/CA

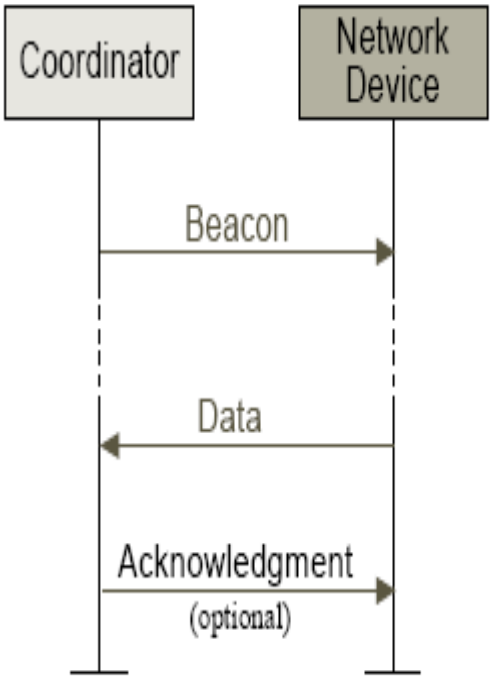
ZigBee SuperFrame Structures

- A superframe is formed by the PAN coordinator to synchronize network reception and transmission.

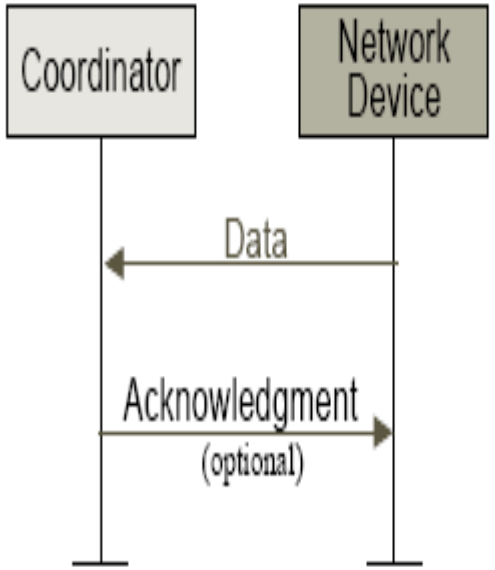




Communication to Coordinator

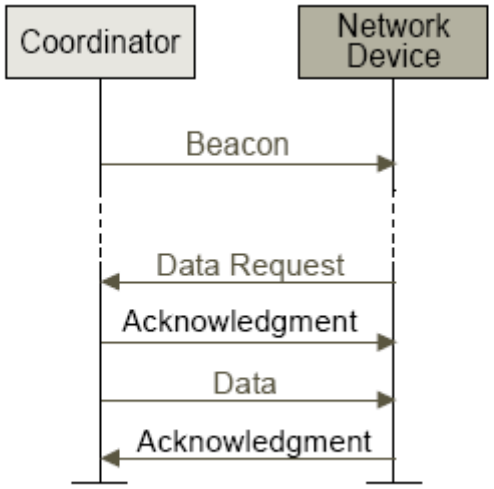


·Communication to a coordinator in a beacon-enabled network

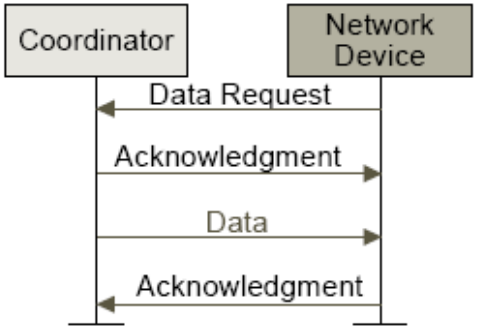


·Communication to a coordinator in a nonbeacon-enabled network

Communication from Coordinator



Communication from a coordinator a beacon-enabled network



Communication from a coordinator in a nonbeacon-enabled network