WPAN: IEEE802.15

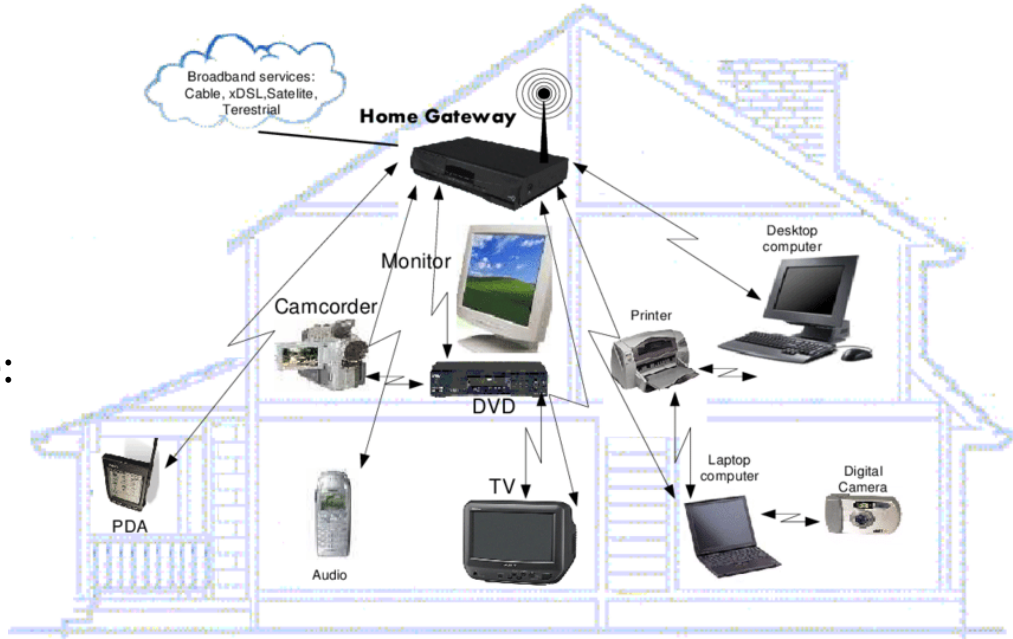
Wireless Personal Area Network

A **Wireless Personal Area Network** (**WPAN**) is a **low-range wireless network** which covers an area of only a few dozen meters. This sort of network is generally used for **linking peripheral devices** (like printers, cellphones, and home appliances), a **PDA** to a computer or just two nearby computers, without using a hard-wired connection. There are **several kinds of technology** used for WPAN.

Why WPAN?

WPAN can gain many benefits to eliminate wires in various applications:

- Home control systems (smart home)
- Home automation: control washing machine, air condition etc..
- Portable device data exchange
- Sharing a number of photos
- Connecting audio and video devices to computers. For example: Headphone with music player.
- Industrial control systems.
- Mobile and Wireless Computing



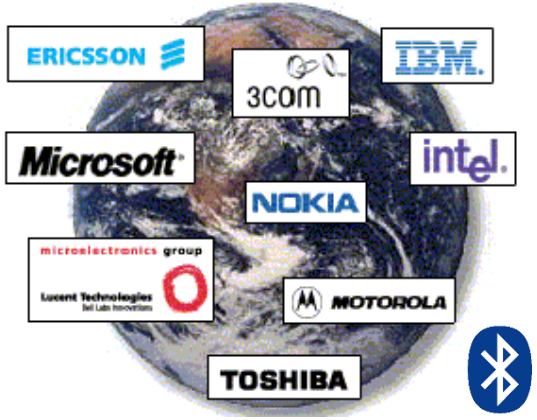
There are different technologies used in WPAN which are listed below:-

- **Infrared (IR):** the transmission is done in a direct way, whereby the devices must remain close together and in the same position during data transmission. Nowadays, it is rarely used. IrDA(Infrared Data Association) was formed in 1995.
- **802.15 WPAN Task Group 1: WPAN/Bluetooth.** The WPAN Task Group 1 (TG1) has created the WPAN 802.15.1 standard based on the Bluetooth v1.1 specification.
- **802.15 WPAN Task Group 2: Coexistence Mechanisms.** The 802.15 WPAN Task Group 2 (TG2) is developing the recommended practices to facilitate the coexistence of WPAN (802.15) and WLAN (802.11) technologies. Part of this task involves developing a coexistence model to quantify the mutual interference of a WPAN and a WLAN.
- **802.15 WPAN Task Group 3: High Rate WPAN.** The 802.15 WPAN Task Group 3 (TG3) is chartered to publish a new standard for high-rate (20 Mbps or higher) WPANs. In addition to high data rates, 802.15.3 also has to provide a means for low-power and low-cost solutions to address the needs of portable consumer electronics, digital imaging, and multimedia applications. **Example: UWB.**
- **802.15 WPAN Task Group 4: Low Rate-Long Battery Life.** The 802.15 WPAN Task Group 4 (TG4) is chartered to establish a low-data-rate (200 Kbps maximum) solution with long battery life (many months to many years) and low complexity. It is intended to operate in an unlicensed international frequency band and is targeted at sensors, interactive toys, smart badges, home automation, and remote controls. **Example: ZigBee**
- **IEEE 802.15.5: Mesh Networking**
- **IEEE 802.15.6: Body Area Networks**
- **IEEE 802.15.7: Visible Light Communication**

IrDA – Infrared Data Association

- Medium: Infrared light
- Range: Approximately 1m.
- Wavelength 875nm
- Direction: Directed within at least ±15 degrees.
- Data rate: 2.4 kb/s to 16 Mb/s
- Point-to-point
- Requires line-of-sight. IrDA was popular on laptops and some desktops during the late 90s through the early 2000s. Replaced by Bluetooth and WiFi.

Bluetooth


ERICSSON
3com
IBM
Microsoft
intel
NOKIA
microelectronics group
Lucent Technologies
MOTOROLA
TOSHIBA

- The word "Bluetooth" is named by the tenth-century king Harald I of Denmark who united dissonant Danish tribes into a single kingdom (Denmark and Norway).
- Created by Ericsson in 1994
- February 1998: The Bluetooth SIG is formed
  - promoter company group: Ericsson, IBM, Intel, Nokia, Toshiba
- May 1998: The Bluetooth SIG goes “public”

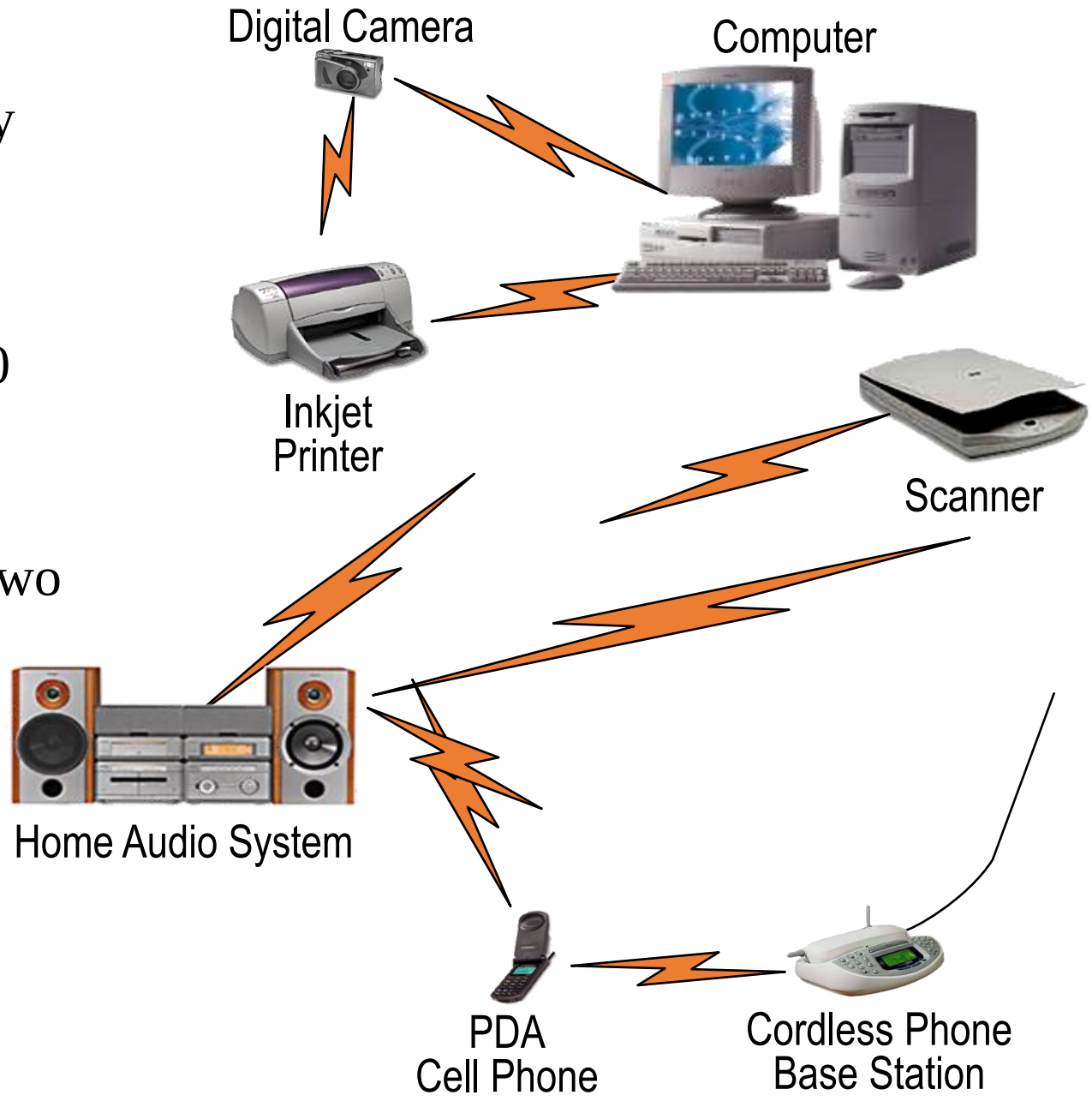
* The stone’s inscription (“runes”) says:
  * Harald had dark hair
  * Harald united Denmark & Norway
  * Harald believed that devices should seamlessly communicate [wirelessly]

Bluetooth®

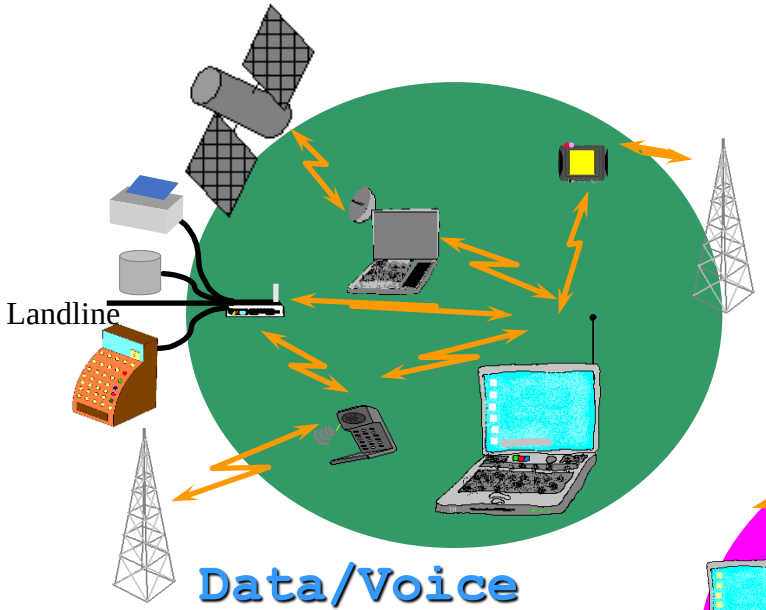
H (ᚼ hagall) and B (ᛒ berkanan)

Overview

- Universal short-range wireless capability
- Uses 2.4-GHz band
- Available globally for unlicensed users
- Devices within 10 m can share up to 720 kbps of capacity
- Bluetooth provides
  - point-to-point connection (only two Bluetooth units involved), or
  - point-to-multipoint connection.
- Synchronous & asynchronous data channels
- Supports open-ended list of applications
  - Data, audio, graphics, video

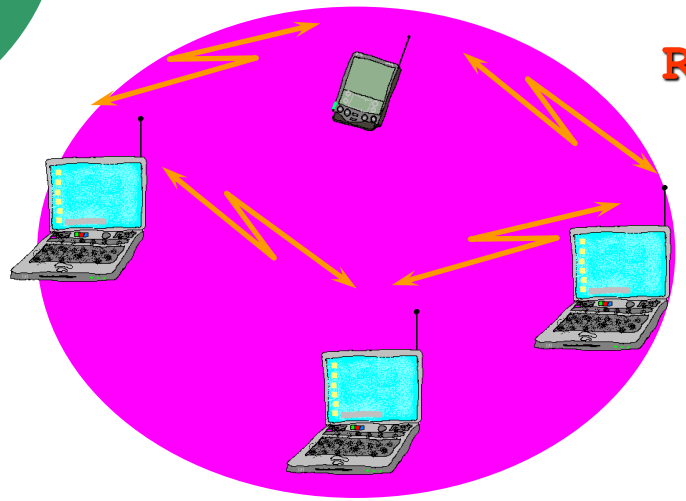


What does Bluetooth do for you?



Data/Voice
Access Points

Cable
Replacement



Personal Ad-hoc
Networks

Bluetooth Application Areas

- Data and voice access points
  - Real-time voice and data transmissions
- Cable replacement
  - Eliminates need for numerous cable attachments for connection
- Ad hoc networking
  - Device with Bluetooth radio can establish connection with another when in range

Why not use Wireless LANs?
- power
- cost

Bluetooth Standards Documents

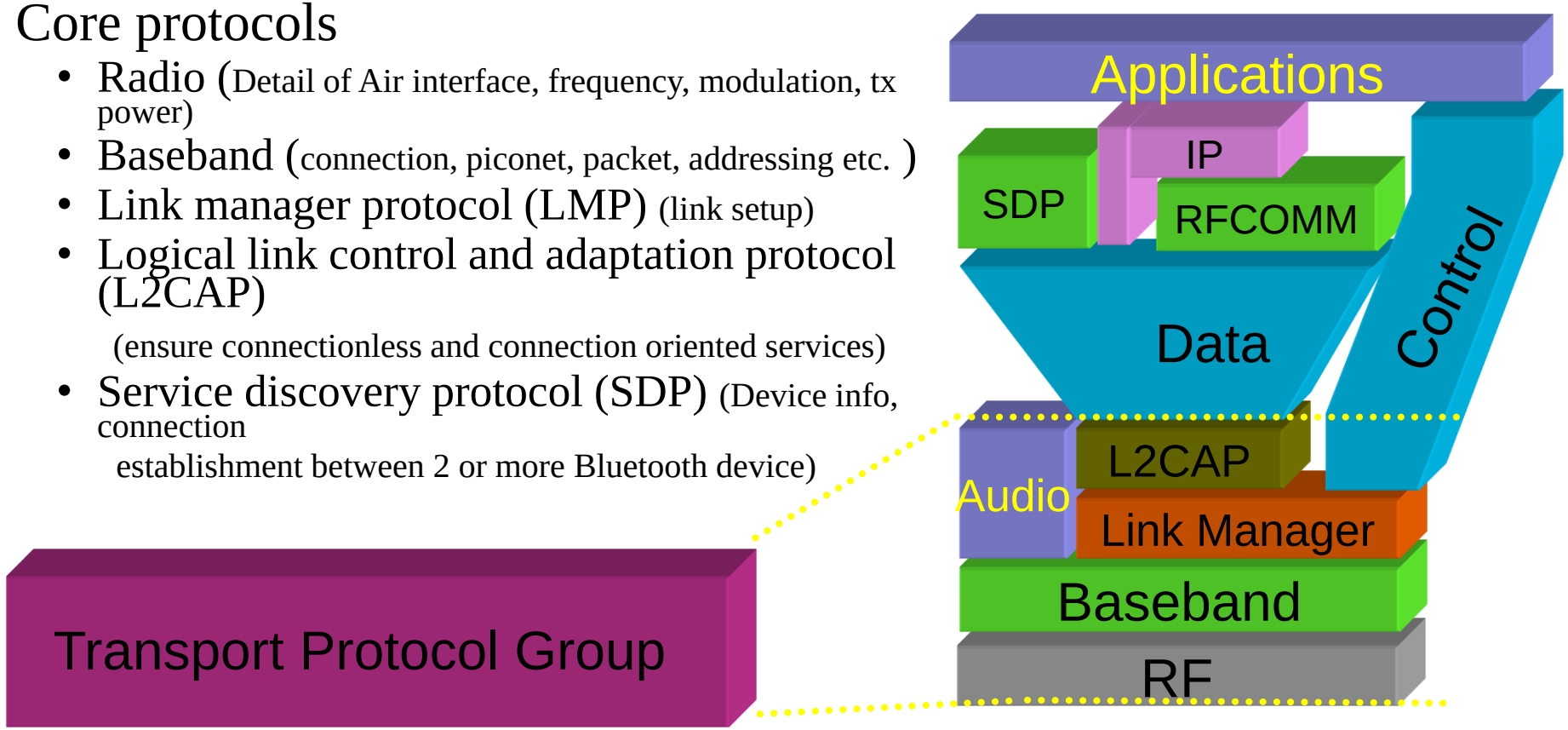
- Core specifications
  - Details of various layers of Bluetooth protocol architecture
- Profile specifications
  - Use of Bluetooth technology to support various applications

Protocol Architecture

- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio (Detail of Air interface, frequency, modulation, tx power)
  - Baseband (connection, piconet, packet, addressing etc.)
  - Link manager protocol (LMP) (link setup)
  - Logical link control and adaptation protocol (L2CAP)

    (ensure connectionless and connection oriented services)
  - Service discovery protocol (SDP) (Device info, connection

    establishment between 2 or more Bluetooth device)



Protocol Architecture

- Cable replacement protocol
  - RFCOMM(Use of Virtual serial port)
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols
  - PPP
  - TCP/UDP/IP
  - OBEX (same functionality as http, but simpler form)
  - WAE/WAP

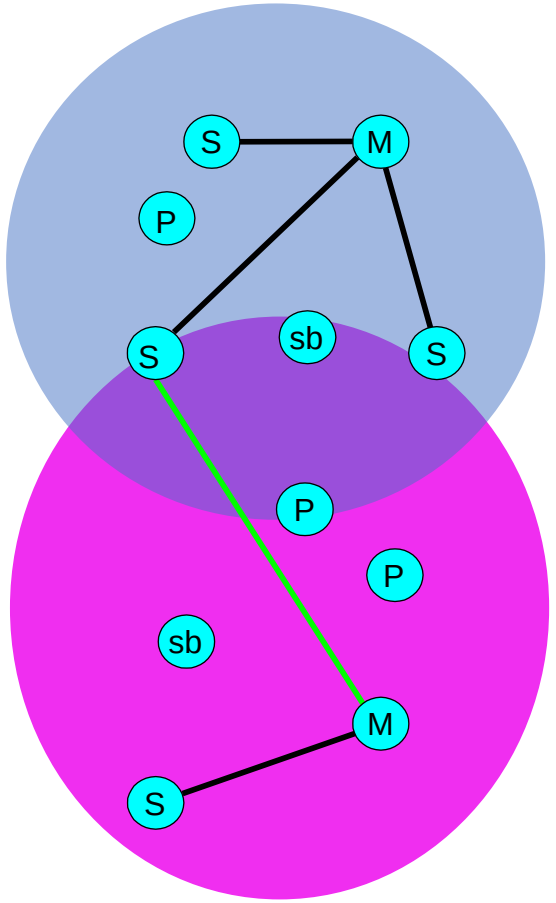
Usage Models

- File transfer
- Internet bridge
- LAN access
- Synchronization (device to device sync of PIM and IrDA)
- Three-in-one phone (act as a cordless connected to a voice BS as intercom and connecting to other tel and as a cell ph.)
- Headset (remote device for audio I/O)

Piconets and Scatternets

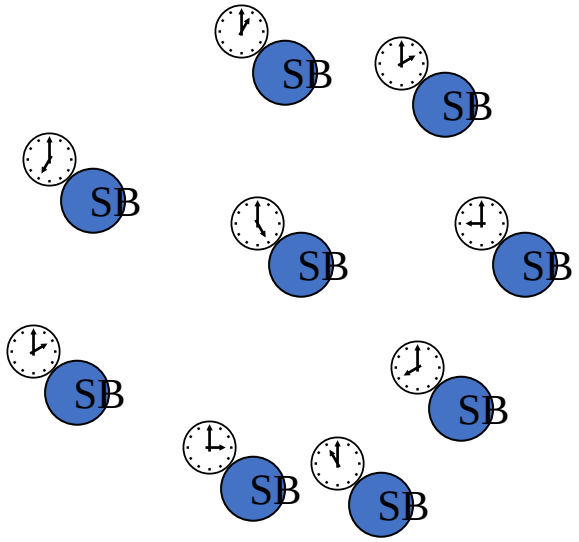
- Piconet
  - Basic unit of Bluetooth networking
  - Master and one to seven slave devices
  - Master determines channel (freq hopping) and phase (timing)

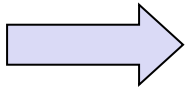
- Scatternet
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth

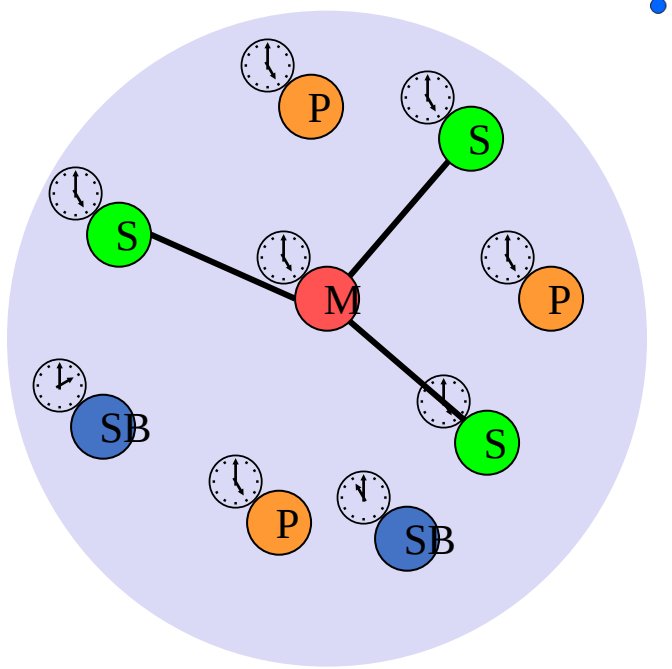


Forming a piconet

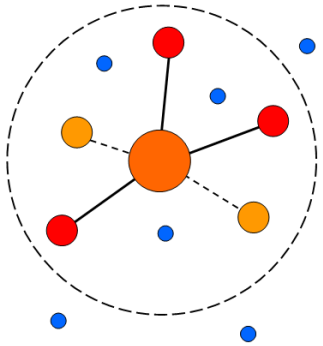
- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit, 8 nodes) for all active nodes
  - Parked Member Address (PMA, 8 bit, 256) for parked nodes
  - SB devices do not need address







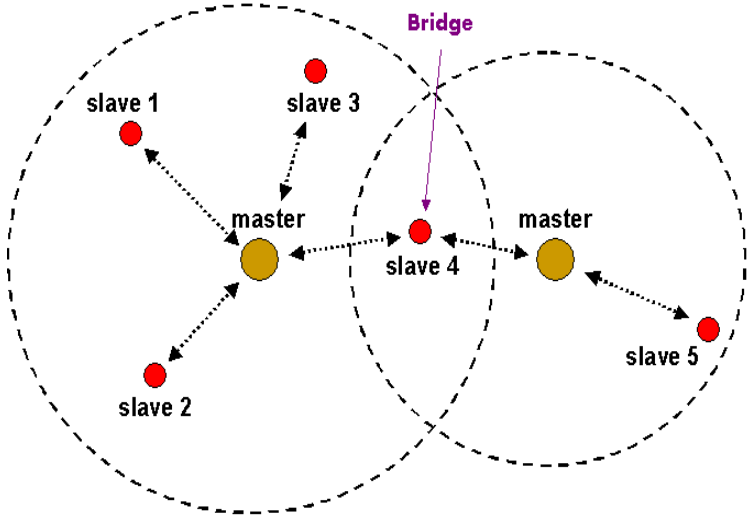
Different roles in a piconet

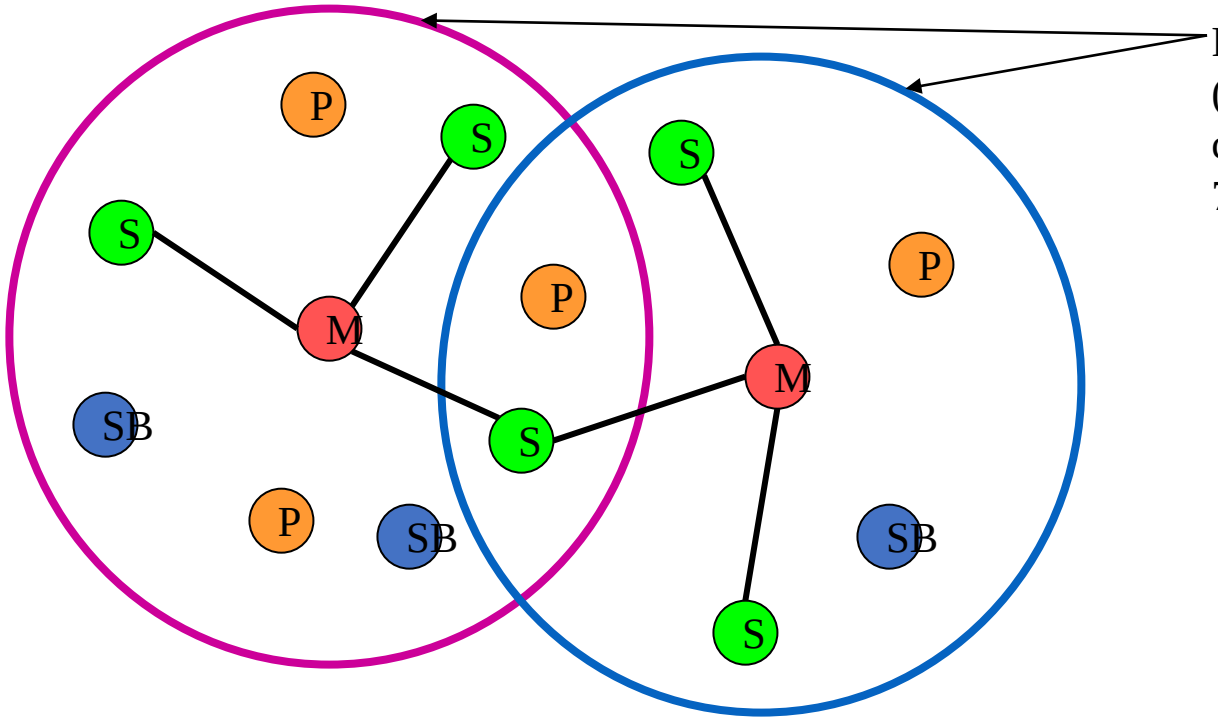


Master
Active slave
Parked slave
Standby

Scatternet

- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
  - Master-slave can switch roles
- Communication between piconets
  - Devices jumping back and forth between the piconets
- Overlapping piconets experience collisions

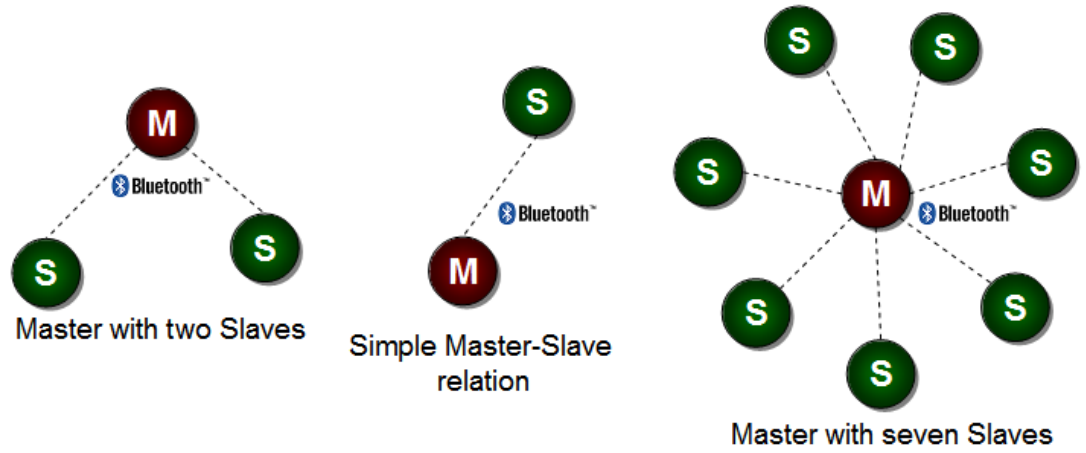


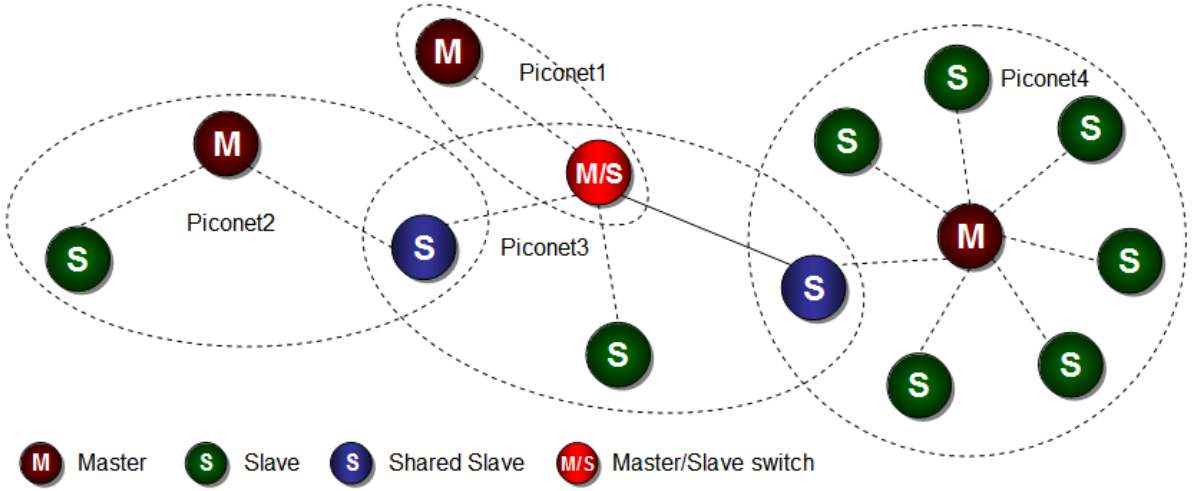


Piconets (each with a capacity of 720 kbit/s)

M=Master
S=Slave
P=Parked
SB=Standby

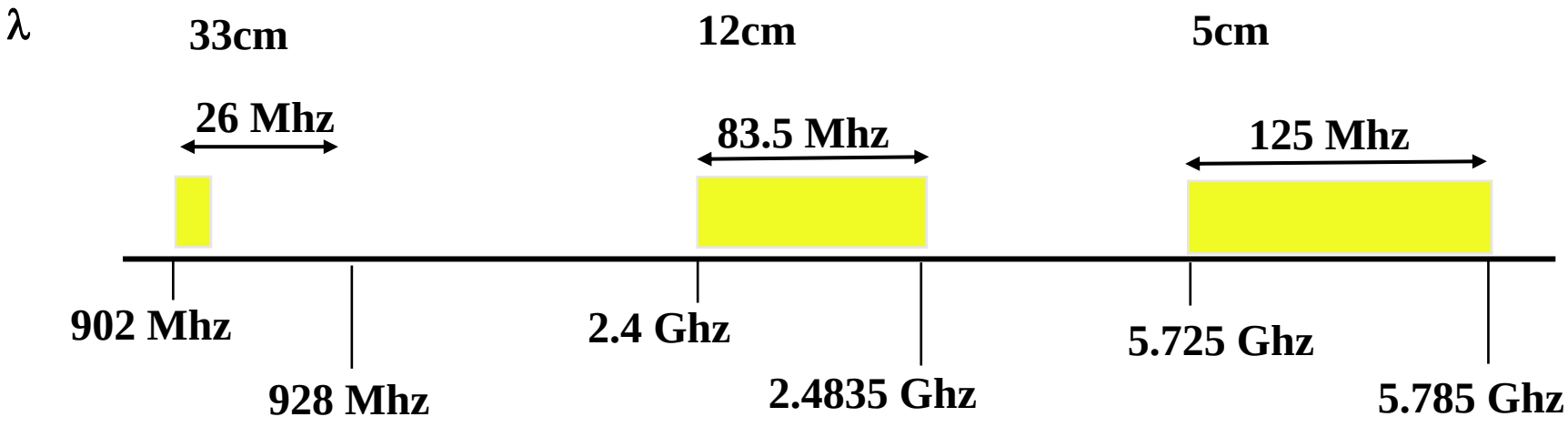
Bluetooth Network Architecture





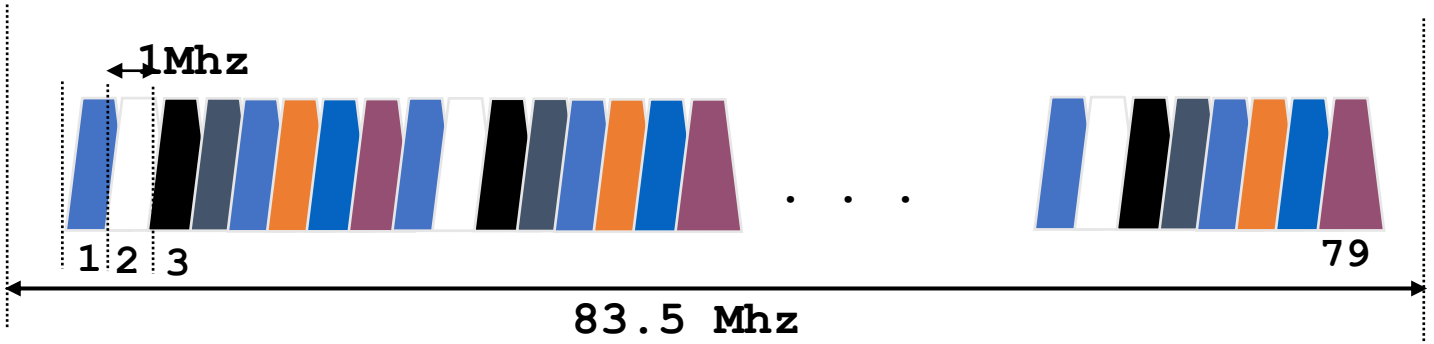
Radio Specification

- Classes of transmitters
  - Class 1: Outputs 100 mW for maximum range
    - Power control mandatory
    - Provides greatest distance
  - Class 2: Outputs 2.4 mW at maximum
    - Power control optional
  - Class 3: Nominal output is 1 mW
    - Lowest power



cordless phones	802.11	unused
baby monitors	Bluetooth	
Wireless LANs	Microwave oven	

Bluetooth Radio Link



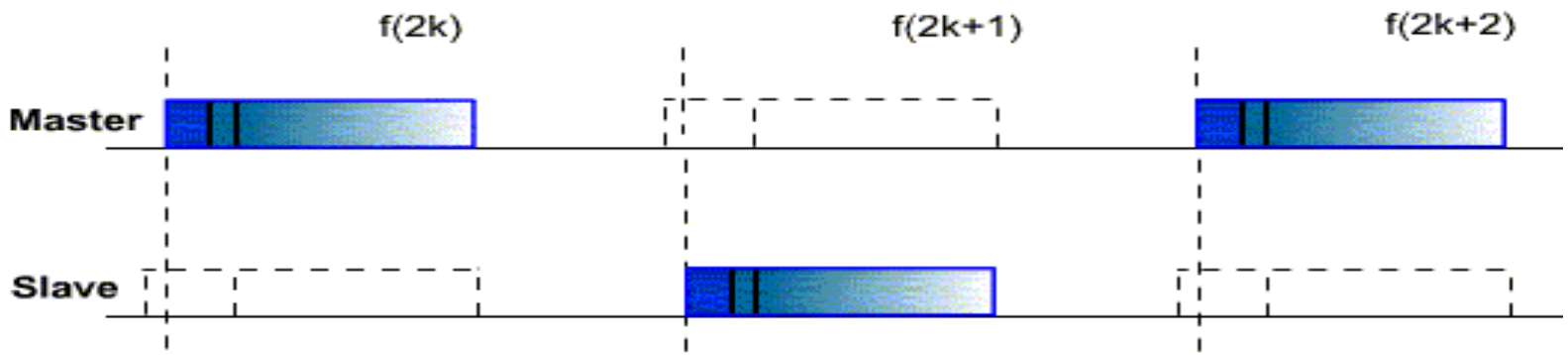
- MA scheme: Frequency hopping spread spectrum.
  - 2.402 GHz + k MHz, k=0, …, 78
  - 1,600 hops per second.
  - 1 Mb/s data rate.

Frequency Hopping in Bluetooth

- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets
- Total bandwidth divided into 1MHz physical channels, hope rate 1600hps. Per ch 0.625 ms.
- FH occurs by jumping from one channel to another in pseudorandom sequence
- Hopping sequence shared with all devices on piconet
- Piconet access:
  - Bluetooth devices use time division duplex (TDD)
  - Access technique is TDMA
  - FH-TDD-TDMA

Frequency Hopping

* Bluetooth devices use a Time-Division Duplex (TDD) scheme
* Channel is divided into consecutive slots (each 625 μs)
* One packet can be transmitted per slot
* Subsequent slots are alternatively used for transmitting and receiving
  * Strict alternation of slots b/t the master and the slaves
  * Master can send packets to a slave only in EVEN slots
  * Slave can send packets to the master only in the ODD slots

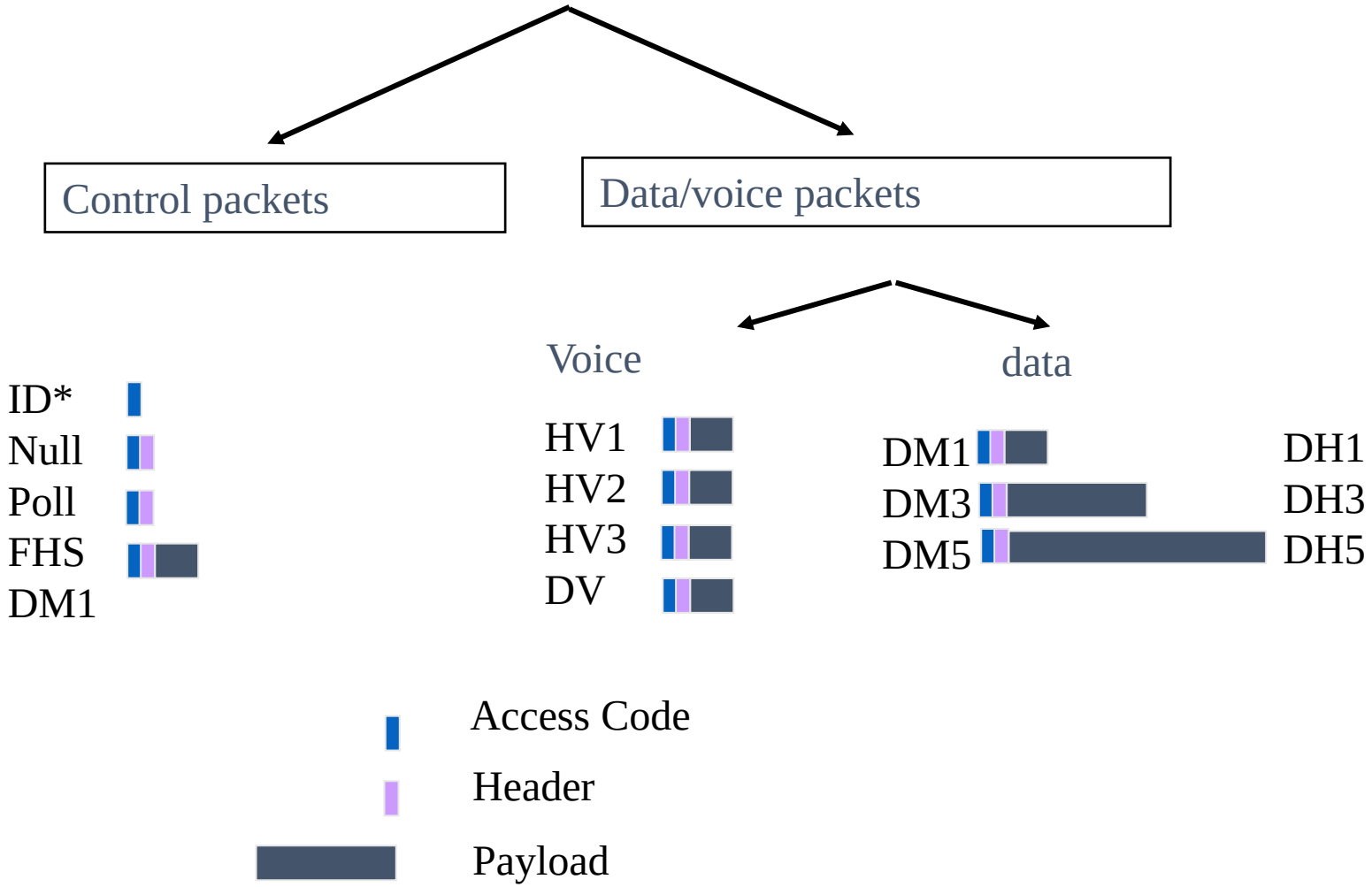


Physical Links between Master and Slave

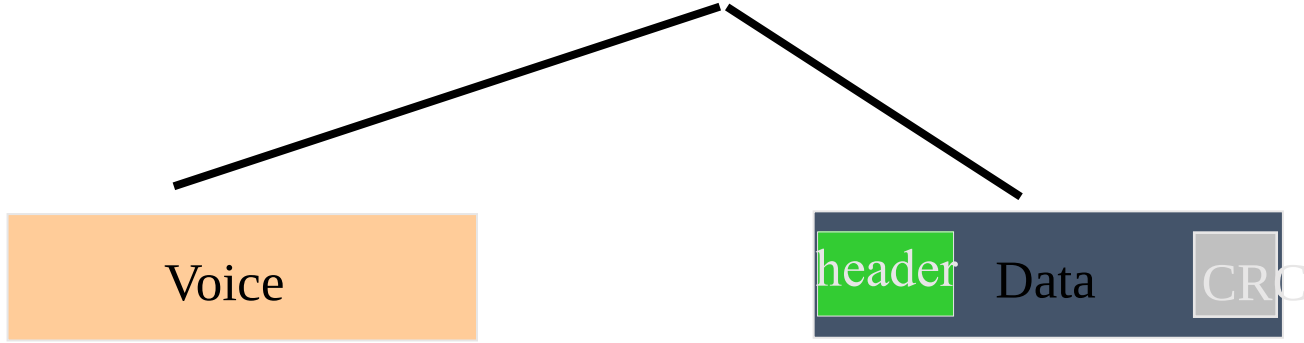
- Synchronous connection oriented (SCO)
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
- Asynchronous connectionless (ACL)
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist

Bluetooth Packet Fields

- **Access code** – used for Controlling such as timing synchronization, paging, and inquiry
- **Header** – used to identify packet type and carry protocol control information
- **Payload** – contains user voice or data and payload header, if present

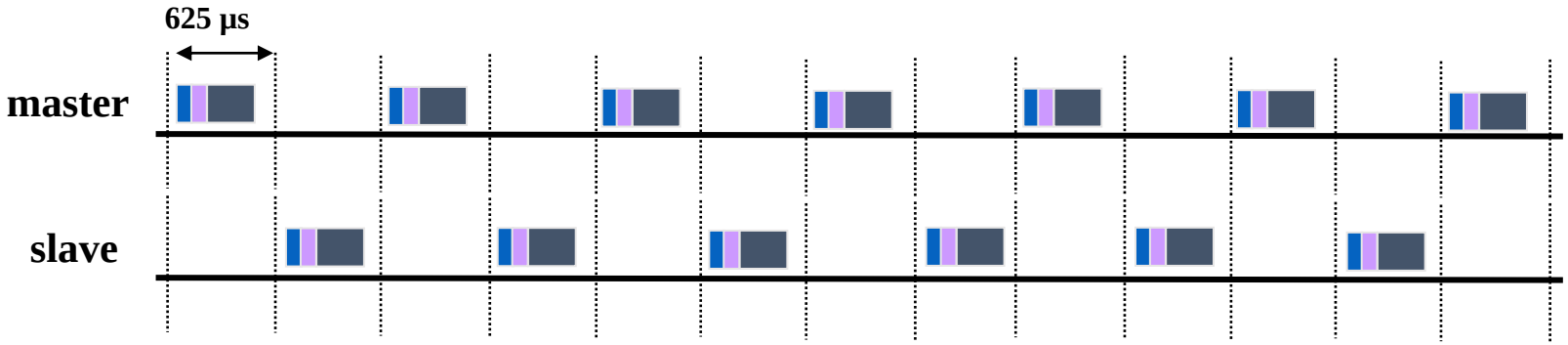


Packet Structure



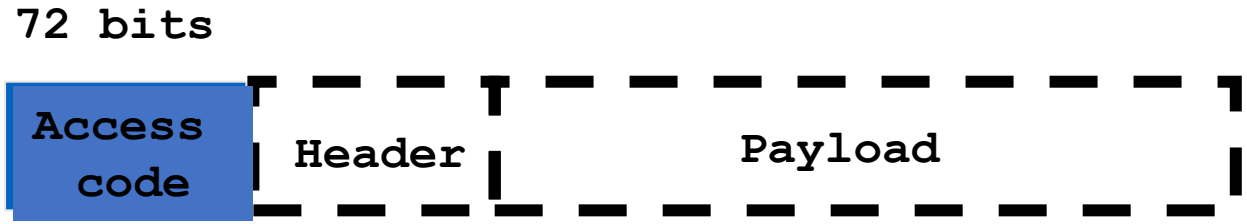
No CRC
No retries
FEC (optional)

ARQ
FEC (optional)

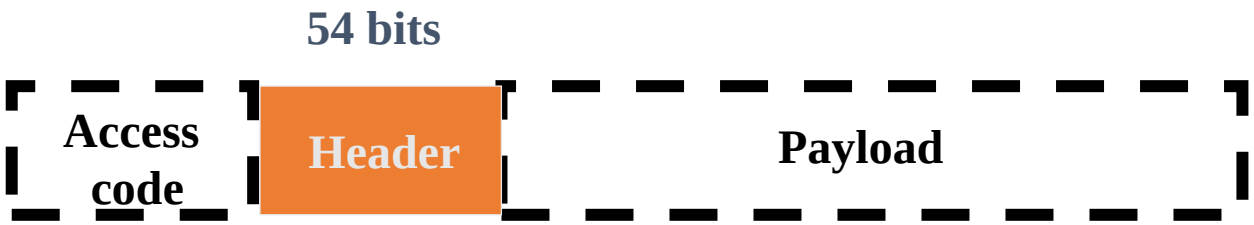


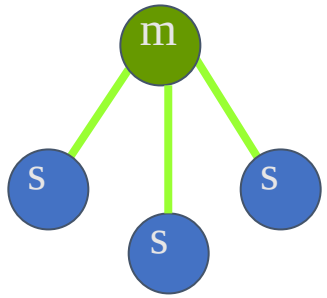
Types of Access Codes

- Address of piconet master
- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – used for paging and subsequent responses
- Inquiry access code (IAC) – used for inquiry purposes



Packet Header





Purpose

* Addressing	(3)	→ Max 7 active slaves
* Packet type	(4)	→ 16 packet types (some unused)
* Flow control	(1)	→ Used to stop flow on ACL link.
* 1-bit ARQ	(1)	→ Broadcast packets are not ACKed
* Sequencing	(1)	→ For filtering retransmitted packets
* HEC	(8)	→ Verify header integrity
total	**18 bits**	

➢The entire header is protected by 1/3 rate FEC.

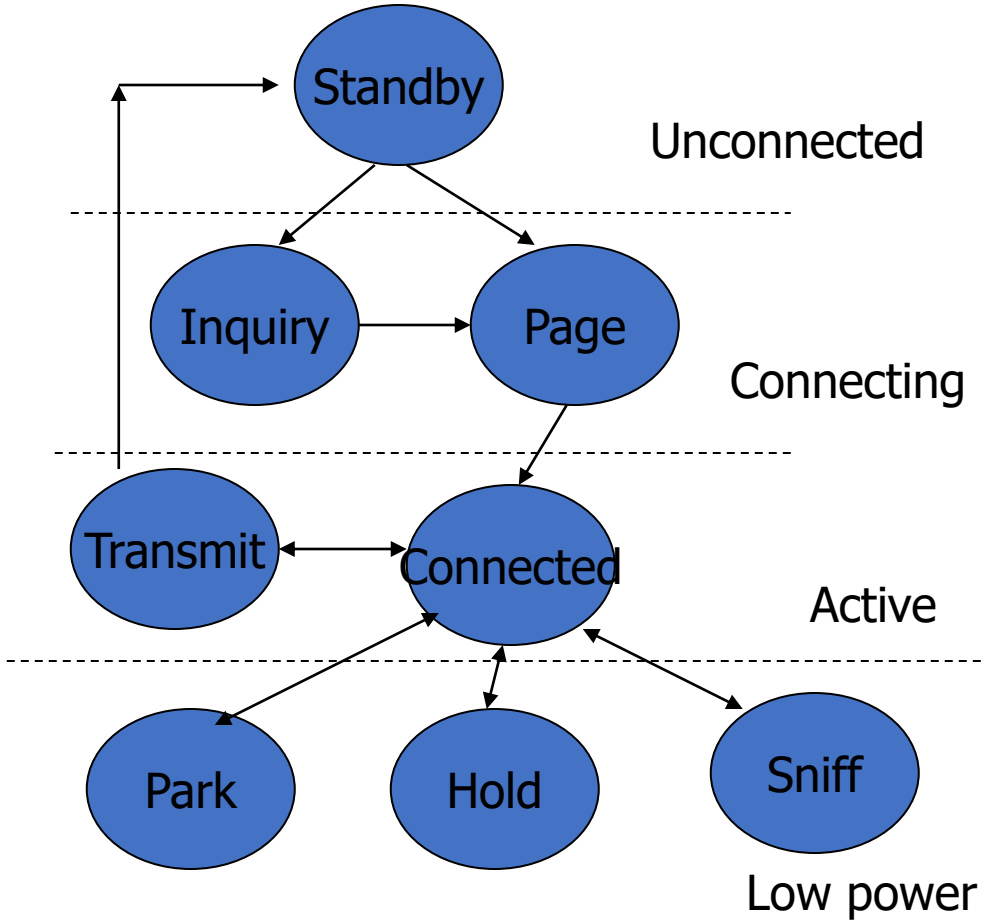
Bluetooth packet types		
TYPE	**NAME**	**DESCRIPTION**
Common	DM1	To support control messages in any link type. can also carry regular user data. Occupies one slot.
SCO	HV1	Carries 10 information bytes. Typically used for voice transmission. 1/3 FEC encoded. Occupies one slot.
SCO	HV2	Carries 20 information bytes. Typically used for voice transmission. 2/3 FEC encoded. Occupies one slot.
SCO	HV3	Carries 30 information bytes. Typically used for voice transmission. Not FEC encoded. Occupies one slot.
SCO	DV	Combined data-voice packet. Voice field not protected by FEC. Data field 2.3 FEC encoded. Voice fiels is never retransmitted but data field can be.
ACL	DM1	Carries 18 information bytes. 2/3 FEC encoded. Occupies one slot.
ACL	DH1	Carries 28 information bytes. Not FEC encoded. Occupies one slot.
ACL	DM3	Carries 123 information bytes. 2/3 FEC encoded. Occupies three slots.
ACL	DH3	Carries 185 information bytes. Not FEC encoded. Occupies three slots.

Channel Control

- States of operation of a piconet during link establishment and maintenance
- Major states
  - Standby – default state
  - Connection – device connected

Channel Control

- Interim sub-states for adding new slaves
  - Page – device issued a page (used by master)
  - Page scan – device is listening for a page
  - Master response – master receives a page response from slave
  - Slave response – slave responds to a page from master
  - Inquiry – device has issued an inquiry for identity of devices within range
  - Inquiry scan – device is listening for an inquiry
  - Inquiry response – device receives an inquiry response



Initially, all nodes in standby. Node (master) can begin inquiry to find nearby devices. Piconet is then formed. Devices join by paging.

Example (without security)

- A Person in a hotel wants to access her email over a BT enabled PDA. The device will automatically carry out the following steps
  1. Inquiry
     - The device initiate an inquiry to find out access points (Masters) within its range
     - All nearby access points respond with their addresses
     - The device picks one out of the responding devices
  2. Paging
     - The device will invoke paging procedure
     - It synchronizes with the access point in terms of clock, phase and frequency hop
  3. Link establishment
     - The LMP will establish a link with the master
     - ACL link will be used (email)

Slave Connection State Modes

- Active – participates in piconet
  - Listens, transmits and receives packets
- Sniff – only listens on specified slots
- Hold – does not support ACL packets
  - Reduced power status
  - May still participate in SCO exchanges
- Park – does not participate on piconet
  - Still retained as part of piconet

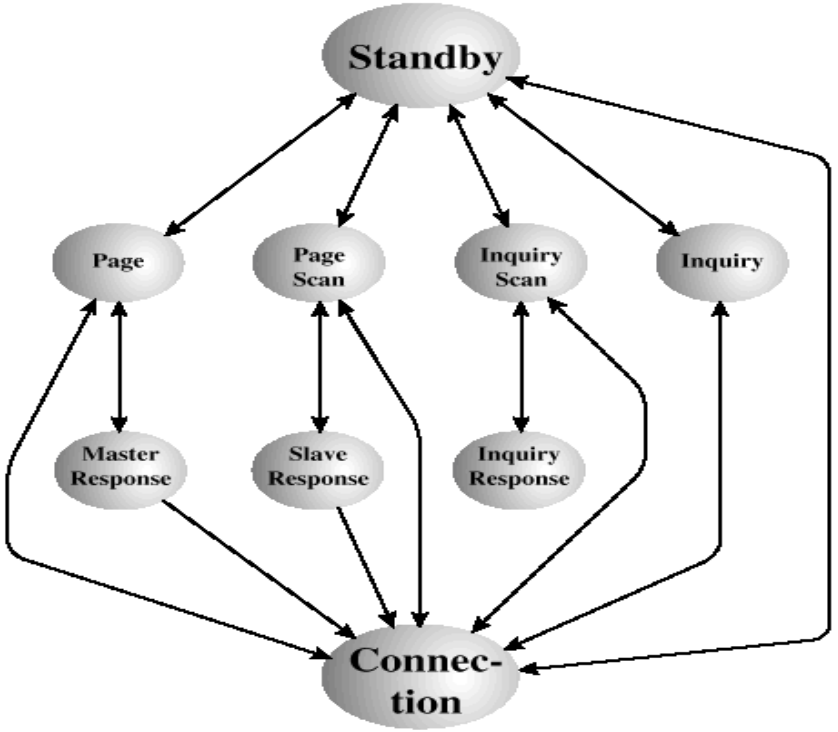
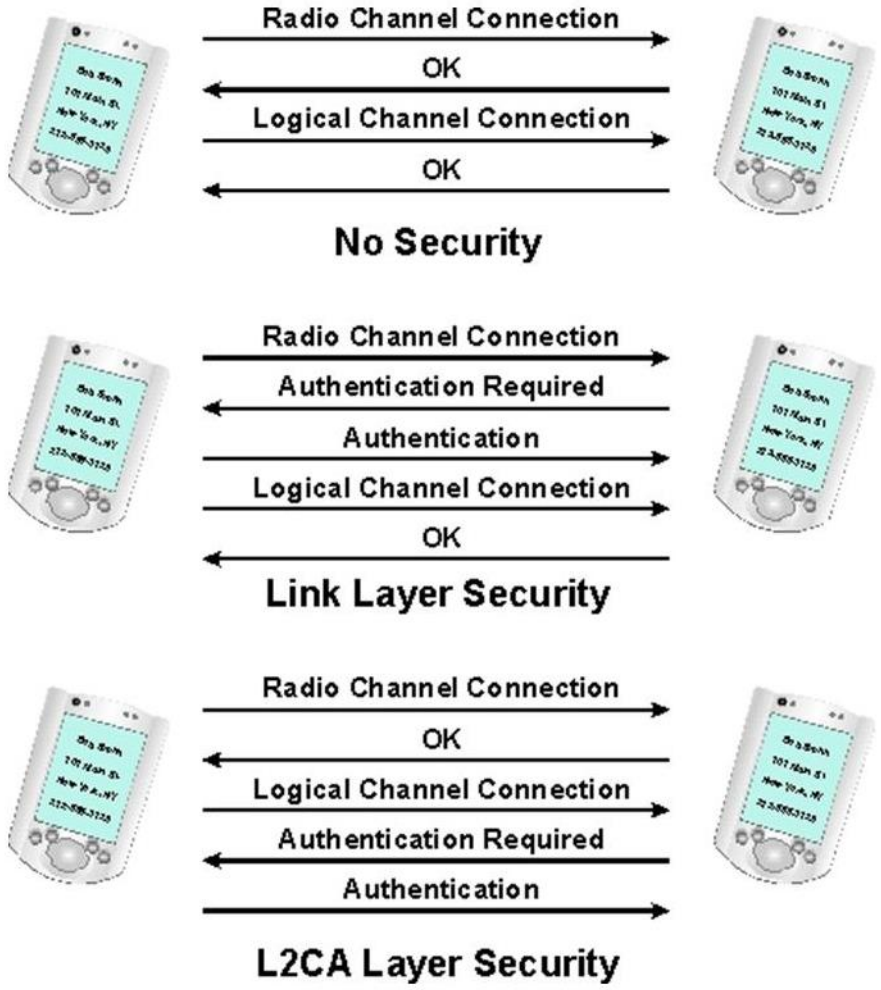


Figure 15.12 Bluetooth State Transition Diagram

Bluetooth Link Security

- Elements:
  - Authentication – verify claimed identity
  - Encryption – privacy
  - Key management and usage
- Security algorithm parameters:
  - Unit address
  - Secret authentication key
  - Secret privacy key
  - Random number



Bluetooth on the market

PC cards, Cell phones, Head sets, Chip sets,…

Company	Features	Applications	Cost
Toshiba, Motorola, Digianswer	20 dBm (~100 m) Point-to-multipoint No Scatternet	File Transfer, Dial-Up Networking LAN access, Fax, …	169 $ --- 200 $
IBM, TDK	0 dBm (~10 m) Point-to-multipoint No Scatternet	File Transfer, Dial-Up Networking LAN access, Fax, …	169 $ ---
3COM	10 m user-user; 100 m user-Base Station Point-to-multipoint SW- & FW-upgradeable	File Transfer, Dial-Up Networking LAN access, Fax, E-mail Unconscious connection	149 $
Nokia	10 m user-user; Point-to-point Connectivity Battery for the cell phone	File Transfer, Dial-Up Networking LAN access, Fax, E-mail Unconscious connection	149 $
Ericsson, Sigma	10 m user-user; Point-to-point; ARM processor; USB; RFCOMM ports	Basic BT Radio stack Embedded or Host stack Programmable	500 $ 1500$

Summary

- Advantages of Bluetooth
  - Low power consumption
  - Low price on Bluetooth components
  - Non line-of-sight
- Disadvantages of Bluetooth
  - Wireless LANs offer faster data rates and larger communication ranges
  - Possibility of interference on 2.4GHz frequency band

IEEE 802.15.4: Zigbee Overview

General Characteristics

Data rates of 250 kb/s, 40 kb/s and 20 kb/s.

Star or Peer-to-Peer operation.

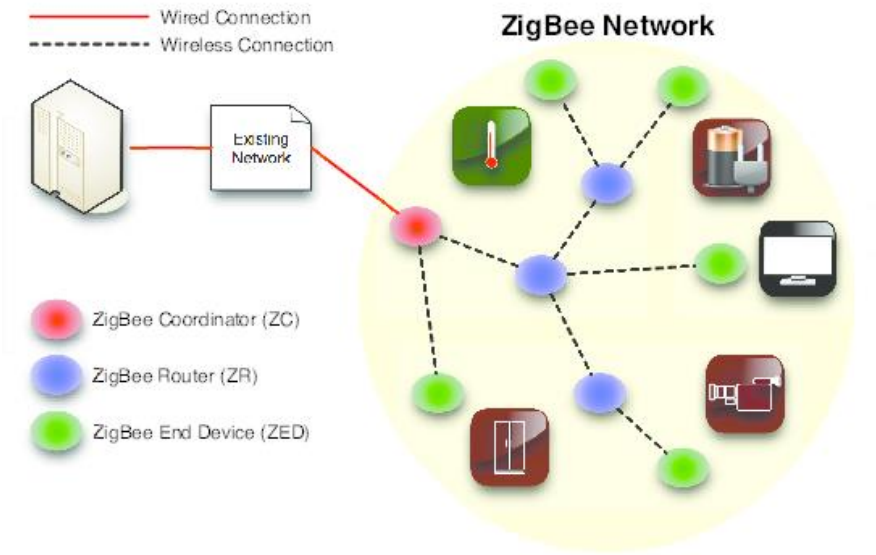
Support for low latency devices.

Fully handshake protocol for transfer reliability.

Low power consumption.

Frequency Bands of Operation

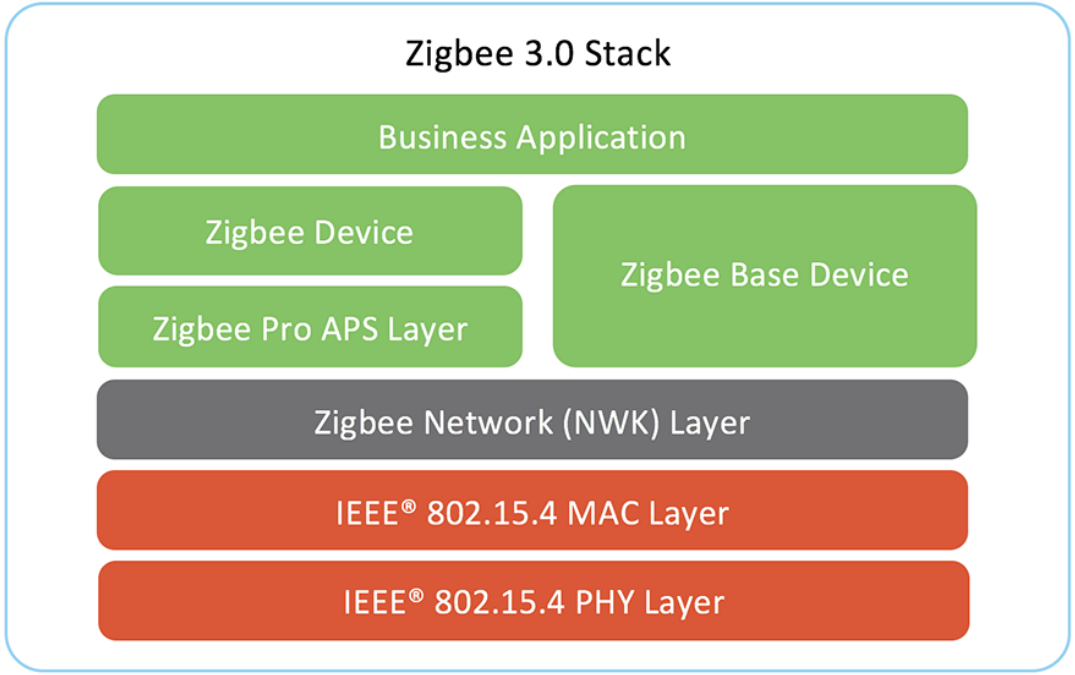
- 16 channels in the 2.4GHz ISM* band
- 10 channels in the 915MHz ISM band
- 1 channel in the European 868MHz band.



*** ISM: Industrial, Scientific, Medical**

Zigbee protocol features include:

•Support for multiple network topologies such as point-to-point,
point-to-multipoint and mesh networks
•Low duty cycle – provides long battery life
•Low latency
•Direct Sequence Spread Spectrum (DSSS)
•Up to 65,000 nodes per network
•128-bit AES encryption for secure data connections
•Collision avoidance, retries and acknowledgements

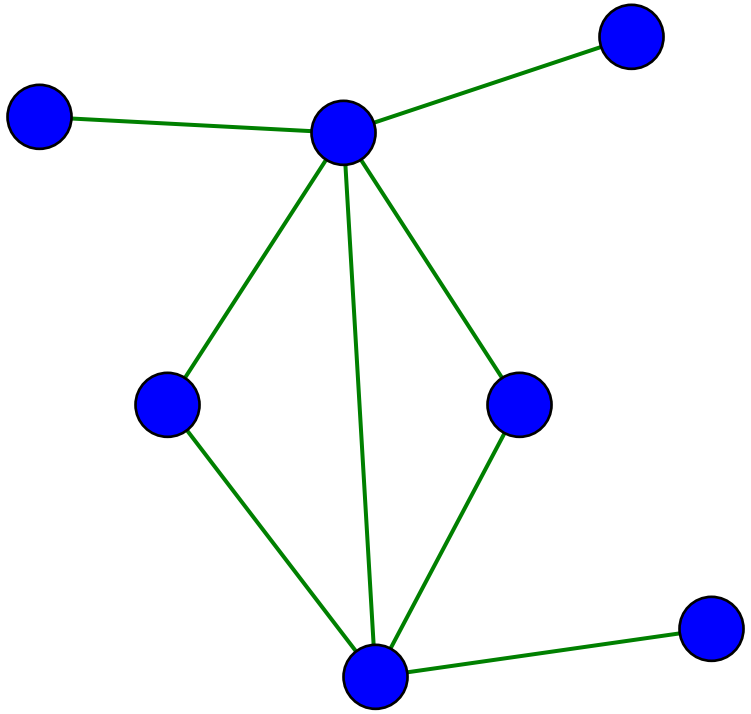


Typical Network Topologies

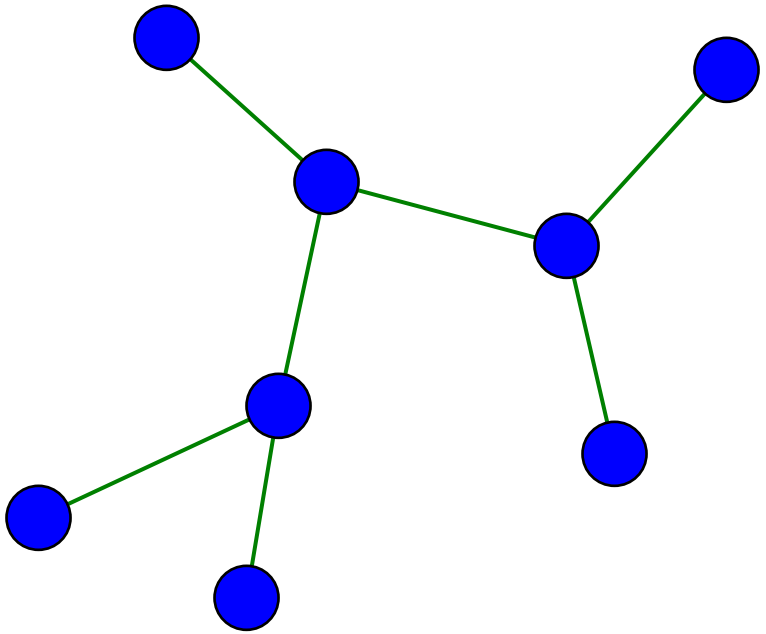
Star Topology

Peer-Peer Topology

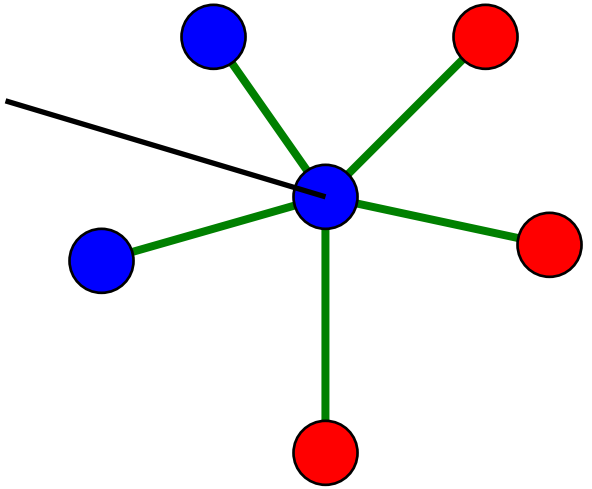
PAN
Coordinator



Point to point

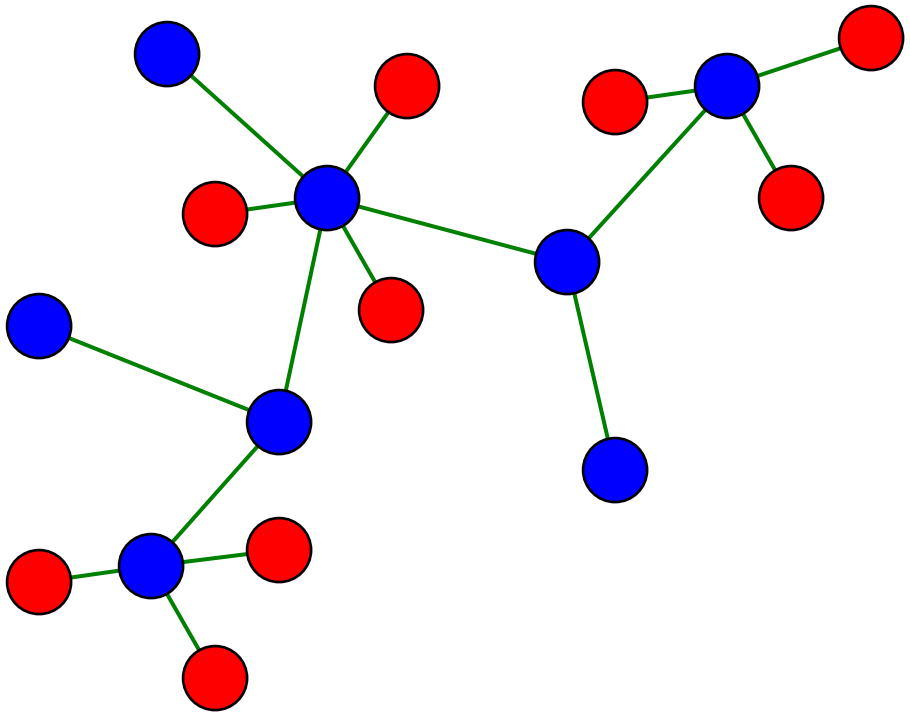


Cluster tree



Master/slave

Combined Topology



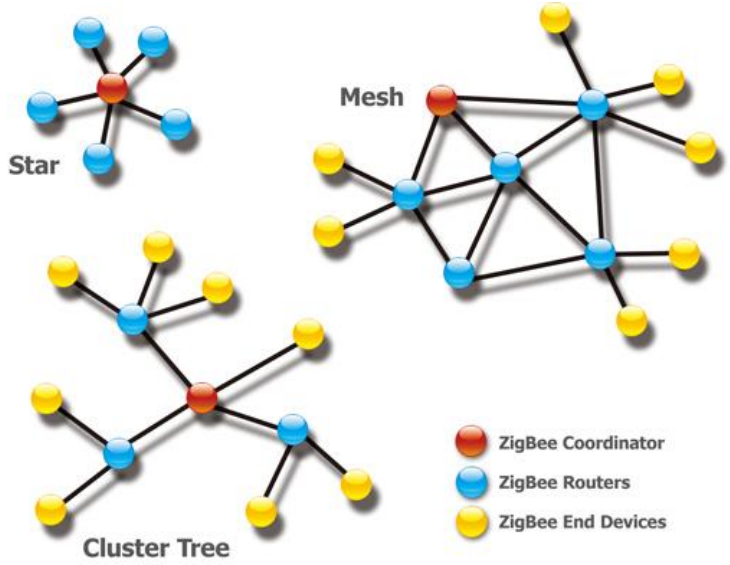
Full function device

Reduced function device

Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

A key component of the Zigbee protocol is the ability to support mesh networking. In a mesh network, nodes are interconnected with other nodes so that multiple pathways connect each node. Connections between nodes are dynamically updated and optimized through sophisticated, built-in mesh routing table. The characteristics of mesh topology and ad-hoc routing provide greater stability in changing conditions or failure at single nodes.

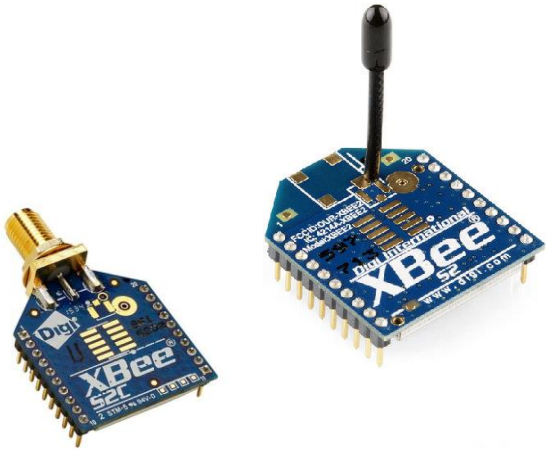
How Zigbee Works?



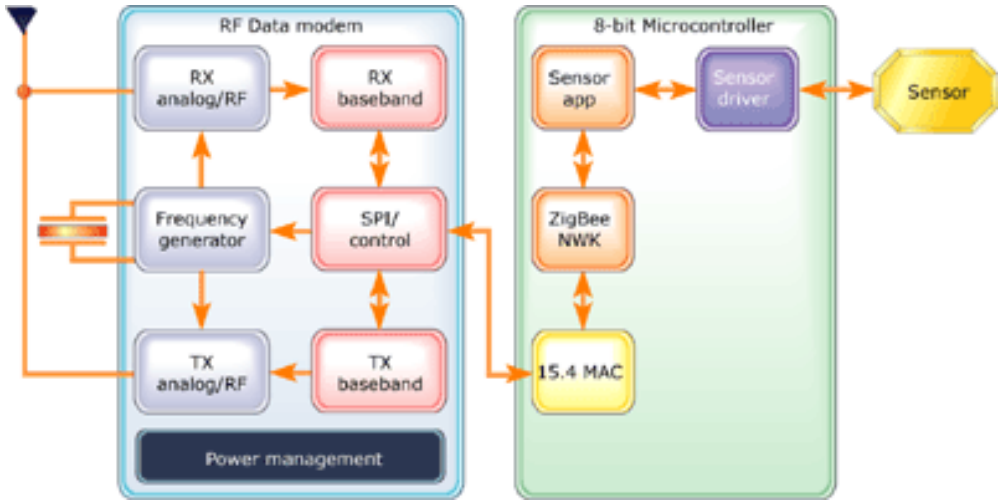
- A typical Zigbee network contains three different types of devices: **Coordinator, routers, and end devices**.
- The coordinator is the most capable device and sits at the root of the network. There is only one coordinator per network, and it is responsible for performing several tasks.
- They select an appropriate channel by performing a channel scan and finding the most suitable one with the least amount of interference, assign a unique ID to the network, allocate a unique address to each device within the network, and initiate and transfer the messages, or instructions, within the network.
- Routers sit in between the coordinator and end devices and are responsible for routing the messages between the different nodes. They receive messages from the coordinator and then store them until their children, the end devices, are in a position to receive them. Routers can also allow other routers and end devices to join the network; they take this responsibility off the coordinator.
- End devices control a very small amount of information; just enough to communicate with the parent node which could be the coordinator or a router depending on the type of Zigbee network.
- They often go to sleep (standby node) which makes battery operate devices ideally suited as an end device.
- End devices don’t communicate directly with each other, so one light bulb doesn’t talk directly to another, for example.
- All traffic is first routed to the parent node, which is usually the router. The router holds on to this data until the receiving end device is in a position to receive it by being awake.
- End devices are also responsible for requesting any messages that are pending from the parent.

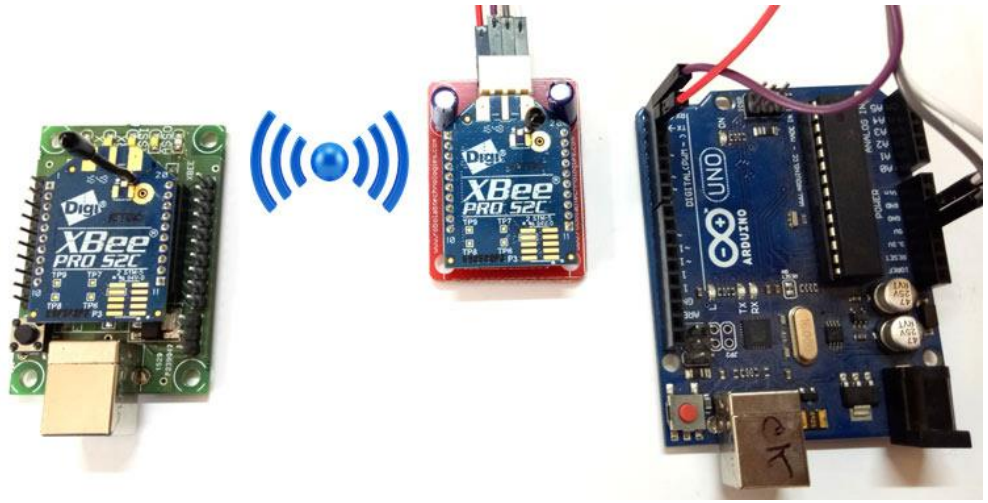
Traffic Types

- Periodic data
  - Application defined rate (e.g. sensors)
- Intermittent data
  - Application/external stimulus defined rate (e.g. light switch)
- Repetitive low latency data
  - Allocation of time slots (e.g. mouse)



Typical ZigBee-Enabled Device Design





Typical design consist of RF IC and 8-bit microprocessor with peripherals connected to an application sensor or actuators

ZigBee Application Profiles

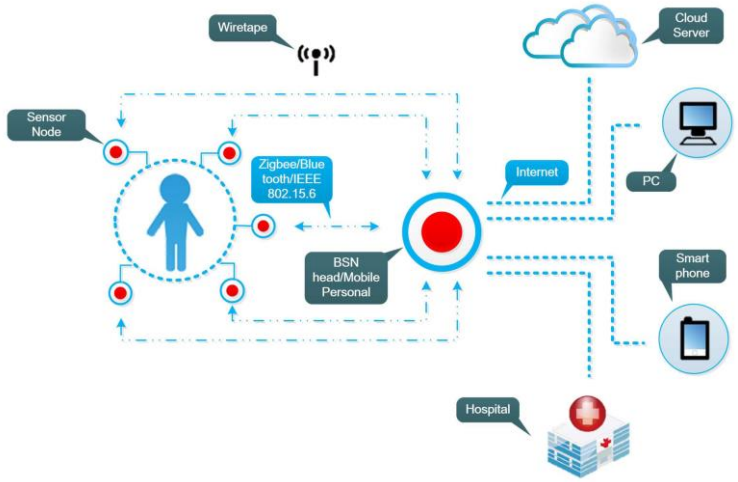
- ZigBee Building Automation (Efficient commercial spaces)
- ZigBee Remote Control (Advanced remote controls)
- ZigBee Telecom Services (Value-added services)
- ZigBee Retail Services (Smarter shopping)
- ZigBee Light Link (LED lighting control)
- ZigBee Input Device (Easy-to-use touchpads, mice, keyboards, wands)
- ZigBee Home Automation (Smart homes)
- ZigBee Health Care (Health and fitness monitoring)
- ZigBee Smart Energy (Home energy savings)
- Smart Energy Profile 2 (IP-based home energy management)

WBAN IEEE 802.15.6

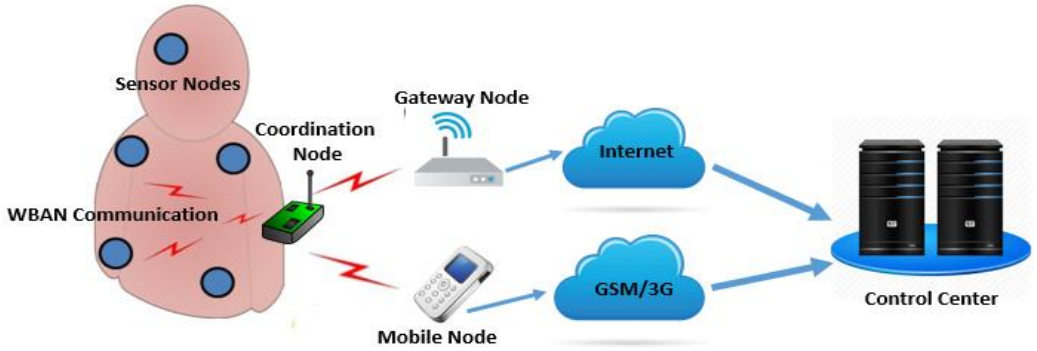
Wireless Body Area Network (WBAN) is becoming a special application of such technique. WBAN differs with other wireless sensor networks (WSN) with some significant points. First difference between a WBAN and WSN is mobility. In WBAN user can move with sensor nodes with same mobility pattern whereas WSN is generally used to be stationary. Energy consumption is much less in WBAN than other WSNs.

There are several wireless technologies such as Low power WiFi, Bluetooth, ZigBee and IEEE 802.15.6. In this paper we have discussed about the general architecture of WBAN, adopted technologies and its possible applications in different areas.

WBAN is designed with special purpose sensor which can autonomously connect with various sensors and appliances, located inside and outside of a human body.



WBAN network architecture is classified into four sections. The first section is the WBAN part which consists of several numbers of sensor nodes. These nodes are cheap and low-power nodes with inertial and physiological sensors, strategically placed on the human body. All the sensors can be used for continuous monitoring of movement, vital parameters like heart rate, ECG, Blood pressure etc.



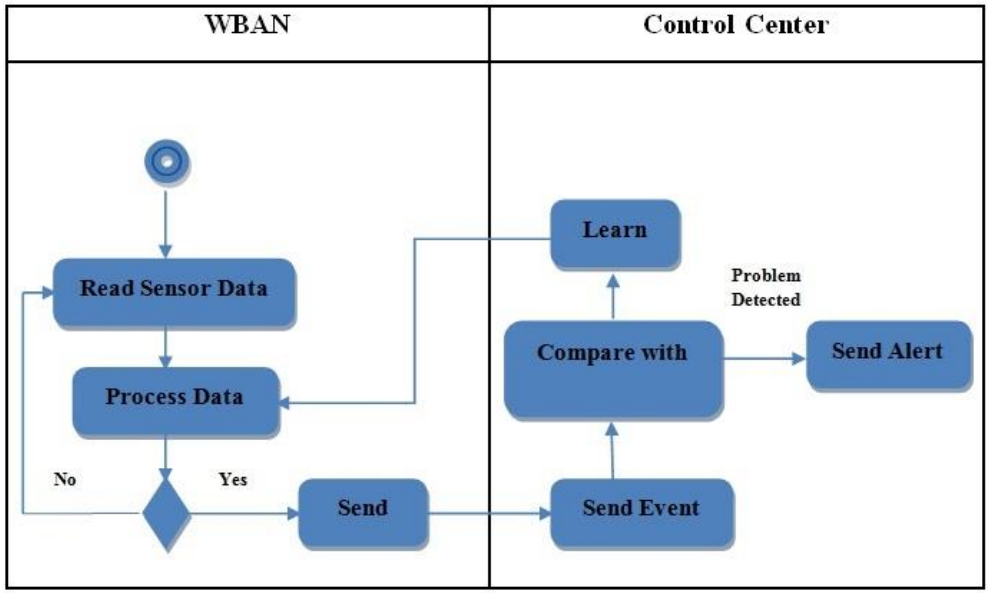
The next section is the coordination node where the entire sensor nodes will directly connected with a coordination node known as Central Control Unit (CCU). CCU takes the responsibility to collect information from the sensor nodes and to deliver to the next section.

The third section is the WBAN communication which will act as a gateway to transfer the information to the destination. A mobile node can be a gateway to a remote station to send Mobile Message to a cellular network using GSM/3G/4G. A router or a PC can be a remote node to communicate via email or other service using Ethernet

The last section is the control center consists of end node devices such as Mobile phone for message, PC for monitoring and email and server for storing the information in the database.

How WBAN works?

- The workflow is divided into two sections. First section is the WBAN where all the sensors devices will collect data and process them to the control center. While processing if any error occurs then it will read data again from the sensor and will forward for processing.



- The control center will send the data to the desired location. If any problem occurs then it will generate an error where resend option should be needed again.

WBAN Application Areas