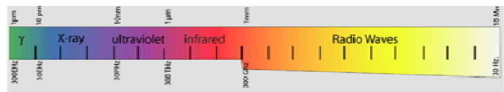
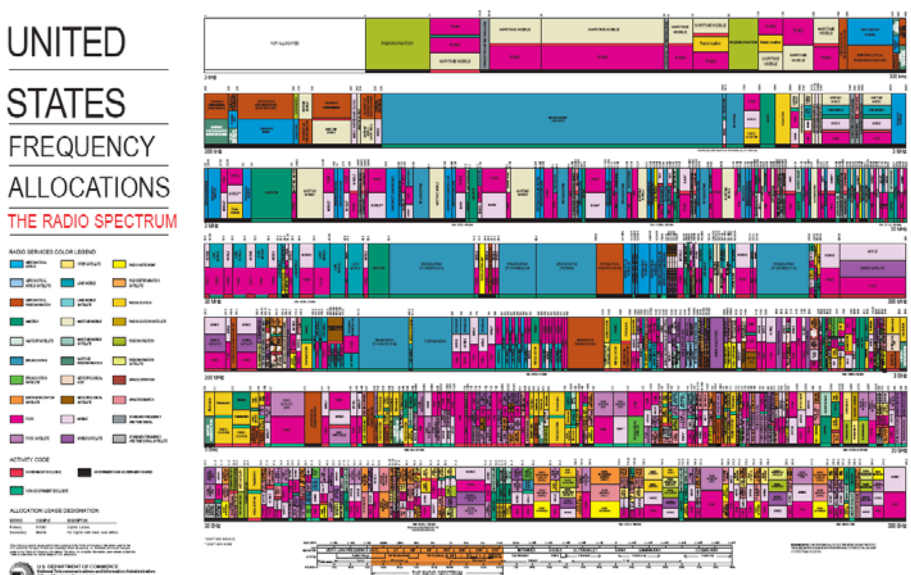
Wireless Communication

- Serial communication
- Allocated a frequency of operation
  - Could be a range of frequencies
  - Regulated by FCC (Federal Communications Commission) in US
  - Unfortunately, allocations are not world-wide
- Dominant forms
  - Infrared
  - VHF (very-high-frequency)
  - UHF (ultra-high-frequency)
  - Microwave
  - UWB (ultra-wide-band)



Electromagnetic Spectrum (3kHz – 300GHz)



How wireless frequencies are allocated

- Garage door openers, alarm systems, etc. – 40MHz
- Cordless phones: 40-50MHz, 900MHz, 2.4GHz, 5.8GHz
- Baby monitors: 49MHz
- Radio controlled toys: 27-75MHz
- Wildlife tracking collars: 215-220MHz
- MIR space station: 145-437MHz
- Cell phones: 824-849MHz, 869-894MHz, 1850-1990MHz
- Public safety (fire, police, ambulance): 849-869MHz
- Air traffic control radar: 960MHz-1.215GHz
- Global Positioning System: 1.227-1.575MHz
- Satellite radio: 2.3GHz
- WiFi/802.11b/g and Bluetooth: 2.4GHz
- Zigbee/802.15.4: 868MHz, 915MHz, 2.4GHz
- Microwave ovens: 2.4Ghz
- TV: 54-216 (VHF 2-13), 470-806MHz (UHF 14-69)
- Ultra-wide-band: 3.1-10.6GHz
- ISM (industrial, scientific, medical): 900MHz, 1.8GHz, 2.4GHz, 5.8GHz

Considerations in choosing a carrier frequency

- Carrier frequency
  - Signal that is modulated to carry data
  - Frequency is not equal to bandwidth
- Ability to carry data (modulation rate)
- Availability of devices to transmit and receive signals
- Interference from other devices in same band
  - ISM bands limit power output
- Interactions of radiation with environment
  - absorption by water, metal, building materials, foliage
- Reflection and multi-path properties
  - constructive/destructive interference patterns (e.g., nulls)

Radio Protocols for Wireless Networks

- UHF (300-1000Hz)
  - Mote radio
- WiFi (2.4GHz)
  - Wireless LAN
- Bluetooth (2.4GHz)
  - Common in many consumer devices (PDAs, cell phones, etc.)
- Zigbee (850-930MHz)
  - Next generation radio for sensor networks and consumer devices

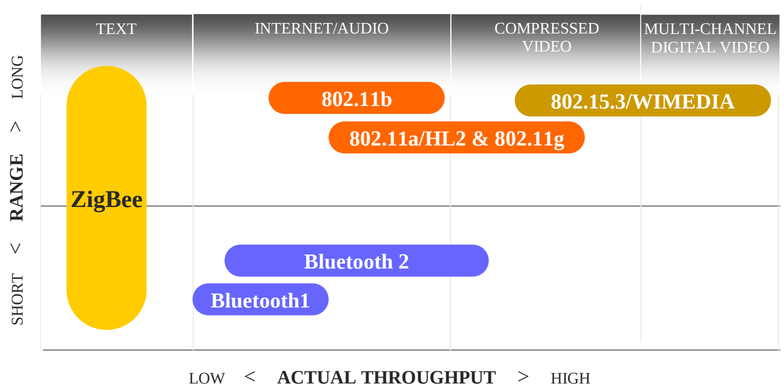
Wireless Network Evolution

- Point-to-point
  - Simple wire replacement (Virtual Wire, Bluetooth)
- Star pattern (single base-station)
  - Centralized routing and control point (WiFi, GSM)
- Multi-hop/Mesh (wireless sensor networks)
  - Multiple paths for data
  - Self-configuring

Comparison of Major Protocols

Feature(s)	IEEE 802.11b	Bluetooth	ZigBee
Power Profile	Hours	Days	Years
Complexity	Very Complex	Complex	Simple
Nodes/Master	32	7	64000
Latency	Enumeration upto 3 seconds	Enumeration upto 10 seconds	Enumeration 30ms
Range	100 m	10m	70m-300m
Extendability	Roaming possible	No	YES
Data Rate	11Mbps	1Mbps	250Kbps
Security	Authentication Service Set ID (SSID)	64 bit, 128 bit	128 bit AES and Application Layer user defined

The Wireless Market



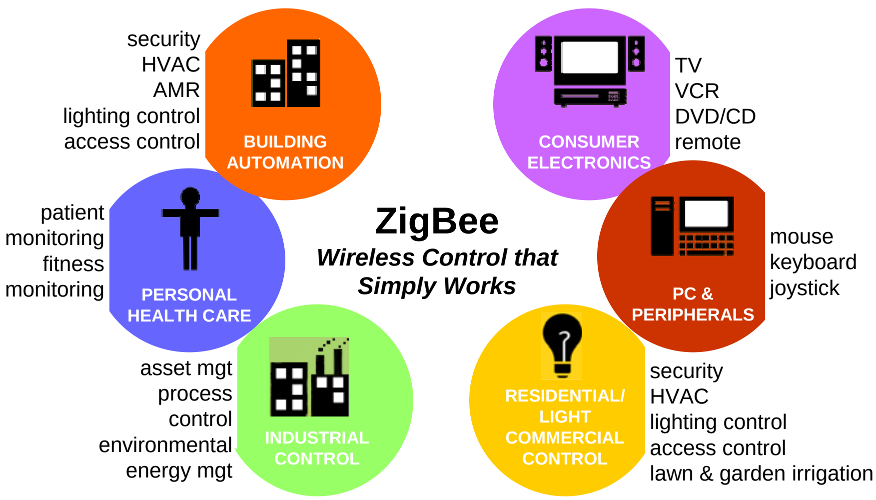
Zigbee (adapted from www.zigbee.org)

- Simple protocol (small memory footprint for protocol stack)
- Broadcast support (unlike Bluetooth)
- Full network support (up to 64-bit addresses)
- Very low power (batteries that last years)
- Consumer device networks
  - Remote monitoring and control
  - Low-cost, low-complexity
  - Support ad-hoc and mesh networking
- Industry consortium
- Builds on IEEE standard 802.15.4 physical radio standard – OQSK encoding (offset quadrature phase shift keyed)
  - Adds logical network, security and application software
- 250Kb/sec bandwidth – 128Kb/sec effective, 30m range at 2.4GHz
  - 40Kb/sec at 915MHz

Why is low power important

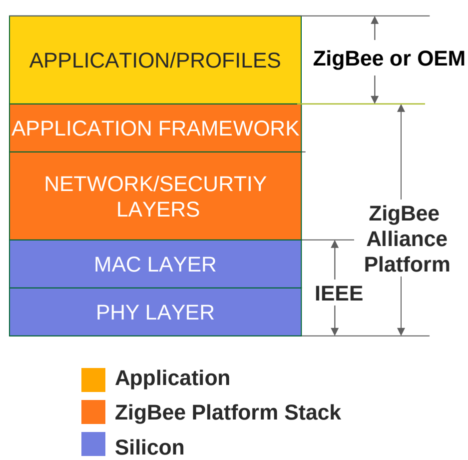
- Always need to be conscious of energy
- Consider a future home with 100 wireless control/sensor devices and 50K homes in a city
  - Case 1: 802.11 Rx power is 667 mW (always on) = 3.33MW
  - Case 2: 802.15.4 Rx power is 30 mW (always on) = 150KW
  - Case 3: 802.15.4 Rx power cycled at .1% (typical) = 150W

Applications



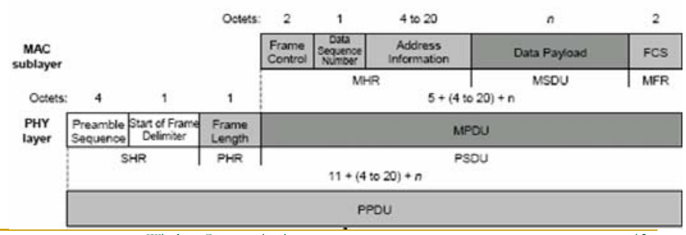
Protocol Stack Features

- 8-bit microcontroller
- Compact protocol stack <32KB
- Supports even simpler slave-only stack <4KB
- Coordinator requires extra memory for storing association tables



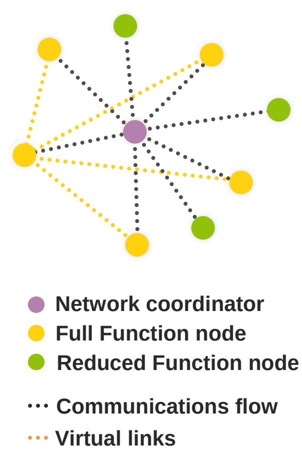
802.15.4 Packet Format

- Physical Protocol Data Unit
  - Preamble Sequence 4 Octets
  - Start of Frame Delimiter 1 Octet
  - Frame Length 1 Octet
- Physical Service Data Unit
  - Frame Control 2 Octets
  - Data Sequence Number 1 Octet
  - Address Information 4 – 20 Octets
  - Frame Check Sequence 2 Octets

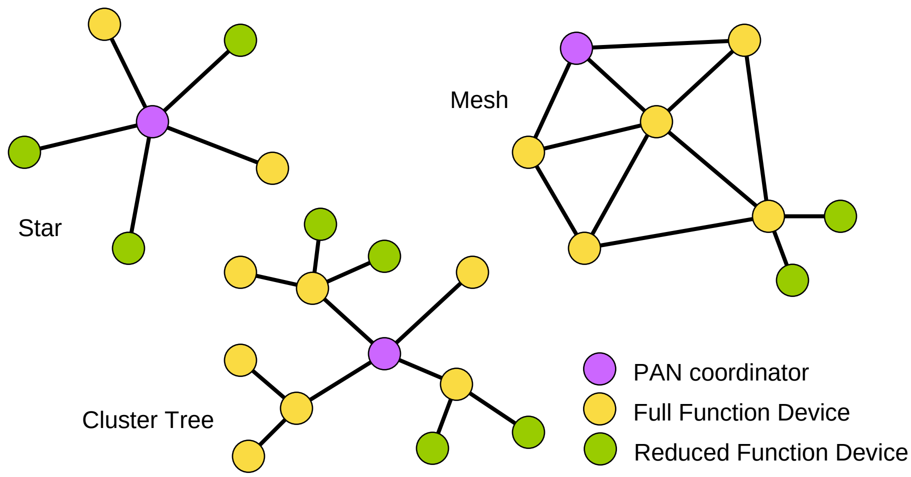


Zigbee Networks

- 64-bit address, 16-bit network address
- Optimized for timing-critical applications
  - Network join time: 30 ms (typ)
  - Sleeping slave changing to active: 15 ms (typ)
  - Active slave channel access time: 15 ms (typ)
- Traffic types
  - Periodic data (e.g., sensor)
  - Intermittent data, event (e.g., light switch)
  - Low-latency, slotted (e.g., mouse)



Zigbee Networks (cont'd)



Lighting Control

[Philips Lighting]

- Advance Transformer
  - Wireless lighting control
    - Dimmable ballasts
    - Light switches anywhere
    - Customizable lighting schemes
    - Energy savings on bright days
    - Dali [or other] interface to BMS
  - Extendable networks
    - Additional sensors
    - Other networks

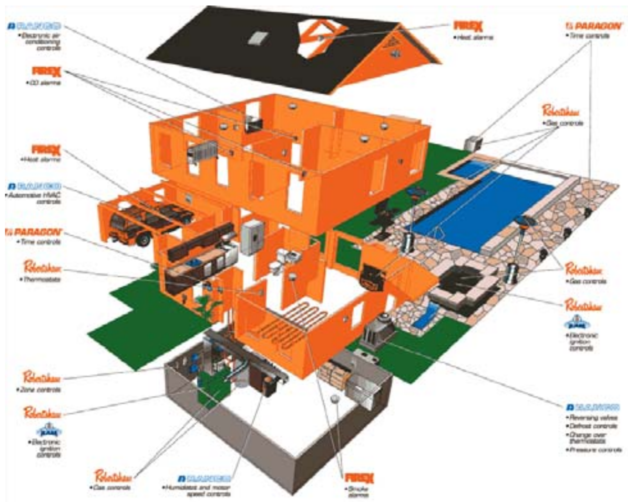
HVAC Energy Management

- Hotel energy management
  - Major operating expense for hotel
    - Centralized HVAC management allow hotel operator to make sure empty rooms are not cooled
  - Retrofit capabilities
  - Battery operated thermostats can be placed for convenience
  - Personalized room settings at check-in

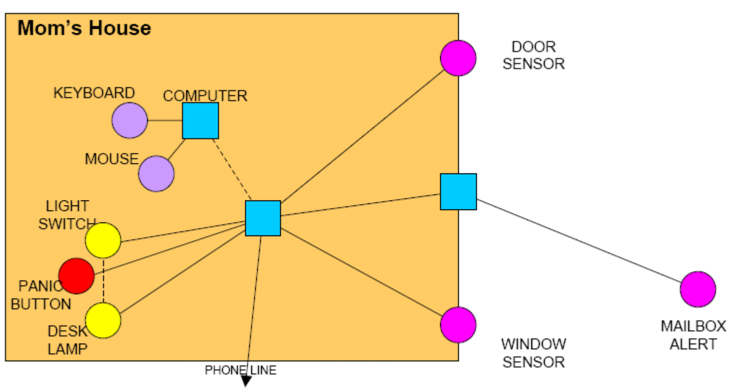
Asset Management

- Within each container, sensors form a mesh network.
- Multiple containers in a ship form a mesh to report sensor data
- Increased security through on-truck and on-ship tamper detection
- Faster container processing. Manifest data and sensor data are known before ship docks at port.

Residential Control



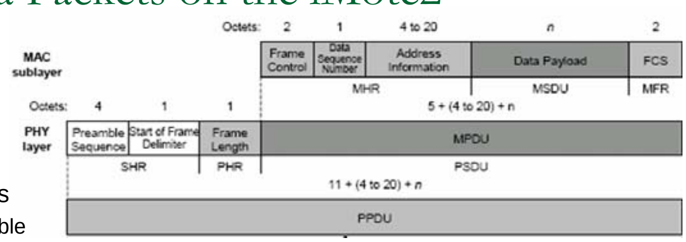
Residential Example



Wireless radio on iMote2

- Chipcon 2420
  - Low-cost transceiver at 2.4GHz (unlicensed ISM band)
  - Compliant with IEEE 802.15.4 (ZigBee physical layer)
- Key features
  - Low current consumption (RX: 19.7 mA, TX: 17.4 mA)
  - Low supply voltage with internal voltage regulator (2.1 V - 3.6 V)
  - Programmable output power
  - Few external components
  - Packet handling with 128 byte (RX) + 128 byte (TX) data buffering
  - Digital RSSI/LQI support
  - Hardware MAC encryption and authentication (AES-128)

Radio Data Packets on the iMote2



- Packet contents
  - 4 byte preamble
  - 1 byte frame delimiter (hex 7A – 01111010)
  - 1 byte frame length (all that follows: 39)
  - 2 byte frame control (defaults: see Fig 19 of data sheet)
  - 1 byte sequence number (increments for every packet sent)
  - 6 byte address
    - 2 byte dest. network (fixed to a default value)
    - 2 byte dest. node (1^{st} byte is group number, 2^{nd} byte is group's iMote (1 or 2))
    - 1 byte packet type (used to indicate handler to use)
    - 1 byte packet group (not used)
  - 28 byte data payload
  - 2 byte frame check sequence

Basic data transfer

- 44 total bytes sent by CC2420
- User-level program provides 34 bytes (address, payload)
- CC2420 sends fully-formed packet
- Awaits acknowledgement from receiving CC2420
- Acknowledgement frame automatically sent
  - 4 byte preamble
  - 1 byte frame delimiter
  - 1 byte frame length
  - 2 byte frame control
  - 1 byte data sequence number (same as received packet)
  - 2 byte frame check sequence
- For “broadcast” packets, drivers turns off acknowledgement required bit in frame control field

API to user-level program

- Yet another character-based device
- Open device
- Create packet (referred to as ToS message)
- Write to file descriptor (provide struct)
- Close file

ToS message struct

```
struct __TOS_Msg
{
        __u8 length;
        __u8 fcfhi;
        __u8 fcflo;
        __u8 dsn;
        __u16 destpan;  // destPAN
        __u16 addr;     // destAddr
        __u8 type;
        __u8 group;
        __s8 data[MAX_TOSH_DATA_LENGTH + 6];
        __u8 strength;
        __u8 lqi;
        __u8 crc;
        __u8 ack;
        __u16 time;
};
```

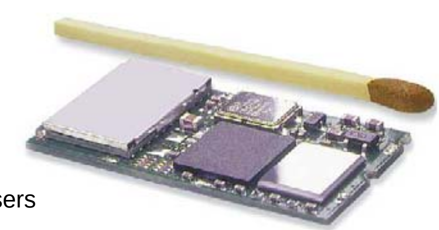

Sending a packet

```
int tosmac_dev;
TOS_Msg recv_pkt;
TOS_Msg send_pkt;

tosmac_dev = open(TOSMAC_DEVICE, O_RDWR);
msg_init(&send_pkt);
send_pkt.addr = 99;
memcpy(send_pkt.data, "0000000000000", 14);
send_pkt.length = 14;
write(tosmac_dev, (TOS_Msg*)&send_pkt, sizeof(TOS_Msg));
close(tosmac_dev);
```

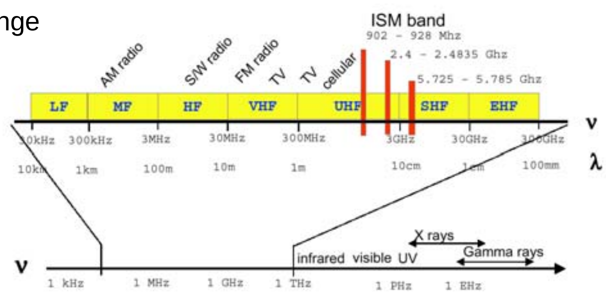
Receiving a packet

```
int tosmac_dev;
TOS_Msg recv_pkt;
TOS_Msg send_pkt;

// open as blocking mode
tosmac_dev = open(TOSMAC_DEVICE, O_RDWR);
read(tosmac_dev, &recv_pkt, sizeof(TOS_Msg));
printf("length is %d\n", recv_pkt.length);
printf("data is %s\n", recv_pkt.data);
close (tosmac_dev);
```


Bluetooth



- Short-range radio at 2.4GHz
  - Available globally for unlicensed users
  - Low-power
  - Low-cost
  - Cable replacement
  - Devices within 10m can share up to 1Mb/sec – 700Kb/sec effective
  - Universal short-range wireless capability



Bluetooth Application Areas

- Data and voice access points
  - Real-time voice and data transmissions
  - Cordless headsets
  - Three-in-one phones: cell, cordless, walkie-talkie
- Cable replacement
  - Eliminates need for numerous cable attachments for connection
  - Automatic synchronization when devices within range
- Ad hoc networking
  - Can establish connections between devices in range
  - Devices can “imprint” on each other so that authentication is not required for each instance of communication
  - Support for object exchange (files, calendar entries, business cards)

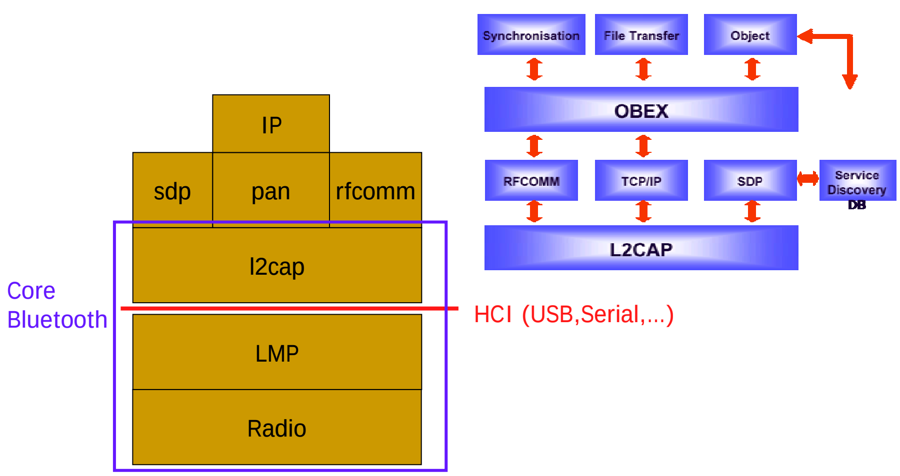
Bluetooth Standards Documents

- Core specifications
  - Details of various layers of Bluetooth protocol architecture
  - Emphasis on physical and transport layers
- Profile specifications
  - Use of Bluetooth technology to support various applications
  - Examples include point-to-point audio and local area network

Protocol Architecture

- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
  - Baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)

Bluetooth Stack Overview



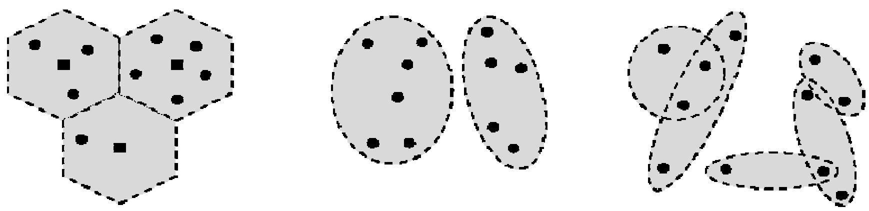
Protocol Architecture

- Cable replacement protocol
  - RFCOMM
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols
  - PPP
  - TCP/UDP/IP
  - OBEX
  - WAP
- Profiles – vertical slide through the protocol stack
  - Basis of interoperability
  - Each device supports at least one profile
  - Defined based on usage models
    - e.g., headset, camera, personal server, etc.

Piconets and Scatternets

- Piconet
  - Basic unit of Bluetooth networking
  - Master and up to 7 slave devices
  - Master determines channel and phase
- 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

Wireless Network Configurations



(a) Cellular system (squares represent stationary base stations)   (b) Conventional ad hoc systems   (c) Scatternets

Radio Specification

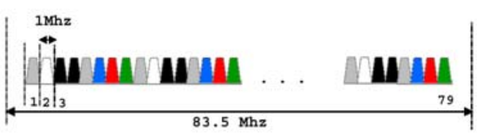
- Classes of transmitters
  - Class 1: Outputs 100 mW for maximum range
    - Power control mandatory
    - Provides greatest distance
  - Class 2: Outputs 2.4 mW at maximum
    - Power control optional
  - Class 3: Nominal output is 1 mW
    - Lowest power

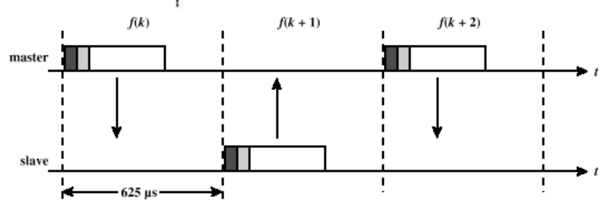
Frequency Hopping in Bluetooth

- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets

Frequency Hopping

- Total bandwidth divided into 1MHz physical channels
- Frequency hopping occurs by moving transmitter/receiver from one channel to another in a pseudo-random sequence
- Hopping sequence shared with all devices in the same piconet so that they can hop together and stay in communication





Physical Links between Master - 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
  - timing synchronization, offset compensation, paging, and inquiry
- Header
  - identify packet type and carry protocol control information
- Payload
  - contains user voice or data and payload header, if present

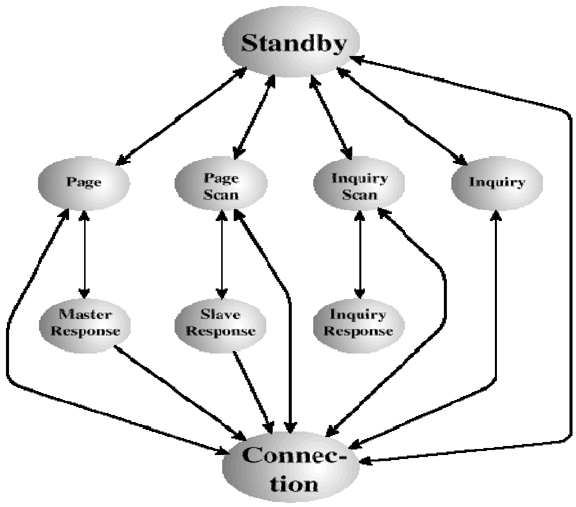
Channel Control

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

Channel Control

- Interim substates 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

State Transition Diagram



Scenario steps

- Master device (e.g., PDA) pages for nearby devices
- Receives response from 0, 1, or more devices
  - Slave device (e.g., headphone) responds to page
- Determines which it "knows" – established connections
- L2CAP establishes Bluetooth connection assigning paging device to be master
- Devices exchange profiles they both support
- Agree upon profile (e.g., audio streaming)
- Master sends audio data
  - Two devices synchronize their frequency hopping
- Keep-alive packets used to maintain connections
- Connections dropped if keep-alive packets are not acknowledged

Limitations/Issues

- Discovery time on the order of 10sec for unknown devices
- Interaction with user required to connect to unknown devices or if multiple masters
- Can connect 8 devices at a time, more need to be multiplexed radically lowering throughput
- Doesn't support simple broadcast – need to be on same frequency hopping schedule
- Effective bandwidth closer to 500Kbps (within one scatternet, order of magnitude lower if between two)