Overview

- Introduction
- Software/Interface Stack
- Device Description
  - Radio Specification
  - Baseband Specification
  - Link Management and Control
- Service Discovery
- Emulation/Telephony Protocols
- Integration with other wireless services
- Available hardware
Introduction

• Named after a medieval Danish king
• Intended as a replacement for short-range cables
  – Inexpensive
  – Flexible
  – Robust

Bluetooth SIG

• Over 1500 companies
  – Started by Ericsson, Nokia, IBM, Intel, and Toshiba
• Assembled specifications
  – Functional descriptions
  – Leaves several implementation details open to the developer
Market Estimates

- Number of units expected to reach 260 Million by 2003
- Worldwide sales market expected to exceed $3 Billion by 2005
  - Market figure for devices only
  - Does not include applications

General Market Goal

- Single-chip solution
  - Around $5 per device
- Risks of current marketing
  - Success of devices a function of
    - Engineering/Manufacturing
    - Marketing
  - Danger of hype over-selling technology
Device Usage

• (almost) Stand-alone wireless connection
  – Needs external application to drive services

Device Communications

• Client/Server (Master/Slave) configuration
  – Devices are inherently equal
  – Application determines identity
Software/Interface Stack

- Bluetooth Host
  - Host Controller Interface driver
  - Physical Bus driver
- Physical Bus
  - Physical Bus Firmware
- Bluetooth Hardware
  - Host Controller Interface firmware
  - Baseband controller

Connecting to Device

- Host Controller Interface
  - Allows control interaction with Bluetooth hardware
- Transport layer
  - Physical connection between host and Bluetooth hardware
Host Controller Interface

• Uniform interface to access Bluetooth hardware capabilities
• Contains sets of commands for hardware
• Contains handle to possible events
• Contains access to error codes

Transport Layer

• Transport layer between host controller driver and host controller
• Intended to be transparent
  – Host controller does not care whether it is running over USB or PC card
  – Allows upgrade of HCI without affecting transport layer
Transport Options

- Standard describes three basic transport formats
  - USB Transport
    - Universal Serial Bus
  - RS232 Transport
  - UART Transport
    - Universal Asynchronous Receiver/Transmitter
    - Serial interface
      - Can be set to RS232 settings

Current Point in Presentation

- Reviewed basic device usage
  - Interfacing to the “outside world”
- Next sections cover
  - RF and baseband description
  - Link management
  - Services
  - Device/kit availability
Bluetooth is more than a radio

• Forms ad hoc networks
  – Piconet: up to 7 devices can be actively connected to a master station
  – Additional devices can be connected in a parked or hold mode
  – Piconets can form Scatter Nets for almost unlimited connectivity

• Software Stack
Bluetooth Networking

• **Piconet formed by up to seven active Bluetooth devices**
  – Master/Slave configuration
  – Additional slaves can be placed in a “parked” state
    Devices are not active but remain synchronized
  – Connection, synchronization, parked/active controlled by master
  – All devices connected in a piconet share timing and frequencies

• **Scatternet formed by two or more Piconets**
  – One master per piconet but a master in one piconet can participate
    as a slave in a different piconet
  – Slaves are time division multiplexed into more than one piconet
  – Piconets not time or frequency synchronized

Establishing a connection

Bluetooth units transmit inquiry message to find other Bluetooth units
Master/Slave Piconet

- One unit becomes the master and the others slaves.
- Master/slave relationship establishes timing.
- A slave can become a master in another Piconet. This connects two Piconets into a Scatter Net.

Bluetooth Pico and Scatter Nets

- Master in one piconet can be a slave in another.
- Addressing limits number of active devices in a piconet to 7.
- An indefinite number of parked devices remain synchronized with the piconet but are not active.
Bluetooth Radio

- **Radio specification**
  Goal is a single chip radio
  Relaxed RF specifications reduce cost

- **Operation under unlicensed international rules**
  US: FCC Part 15
  Europe: ESTI 300-328

- **2.4 GHz ISM band radio**
  Frequency Hop (FH) spread spectrum: 1600 hops/sec
  Time Domain Duplex (TDD)
Bluetooth Radio

Bluetooth is a 2.4 GHz ISM band spread spectrum radio

- 2400 - 2483.5 MHz allows worldwide (almost) operation
- 1600 hops/sec (625 µsec) frequency hopper
- 79 One MHz channels (23 in France, Japan)
- Time Division Duplex
- Tx power 0 dBm to 20 dBm
- Range 10 cm to 10 m at low power (0dBm)
- Data rates: from 108/108 kbps symmetric channel
to 723/57 kbps asymmetric channel
- Isosynchronous (circuit switched) or asynchronous (packet)

Bluetooth International Allocations

<table>
<thead>
<tr>
<th>Geography</th>
<th>Regulatory Allocation</th>
<th>Blue Tooth Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>2.400 – 2.4835 GHz</td>
<td>f = 2402 + k MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>k = 0…78</td>
</tr>
<tr>
<td>Europe</td>
<td>2.400 – 2.4835 GHz</td>
<td>f = 2402 + k MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>k = 0…78</td>
</tr>
<tr>
<td>Spain</td>
<td>2.445 – 2.475 GHz</td>
<td>f = 2449 + k MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>k = 0…22</td>
</tr>
<tr>
<td>France</td>
<td>2.4465 – 2.4835 GHz</td>
<td>f = 2454 + k MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>k = 0…22</td>
</tr>
<tr>
<td>Japan</td>
<td>2.471 – 2.497 GHz</td>
<td>f = 2473 + k MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>k = 0…22</td>
</tr>
</tbody>
</table>

- FCC Part 15 in the US
- ETSI 300-328 in the European Union,
  Africa, and Eastern Europe
- Harmonization efforts currently under way
BT Power Levels

<table>
<thead>
<tr>
<th>Power Class</th>
<th>Maximum Power</th>
<th>Nominal Power</th>
<th>Minimum Power (at Max Pwr setting)</th>
<th>Power Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100 mW (20 dBm)</td>
<td>N/A</td>
<td>0 dBm</td>
<td>4 dBm – 20 dBm -30 dBm - 0 dBm (optional)</td>
</tr>
<tr>
<td>2</td>
<td>2.5 mW (4 dBm)</td>
<td>0 dBm</td>
<td>0.25 mW (-6 dBm)</td>
<td>-30 dBm - 0 dBm (optional)</td>
</tr>
<tr>
<td>3</td>
<td>1 mW (0 dBm)</td>
<td>N/A</td>
<td>N/A</td>
<td>-30 dBm - 0 dBm (optional)</td>
</tr>
</tbody>
</table>

Power control required for high powered Bluetooth devices to minimize interference

Power control requires receiver RSSI function

BT Link Budget

TX power of 0 dBm
C/I = 21 dB
NF = 23 dB

Results in a radio with very relaxed specifications
Bluetooth Modulation

- Modulation: Gaussian filtered FSK (GFSK) \( BT=0.5 \)
- Modulation Index: 0.28 - 0.35
- Deviation: \( F_{\text{min}} > 115 \text{ KHz} \)
- \( F_t - F_{\text{min}} = \text{“0”} \quad F_t + F_{\text{min}} = \text{“1”} \)
- Symbol Timing: 20 ppm

Bluetooth Spectrum Mask

- Adjacent Channel
- Adjacent Channel 2 & 3
- Adjacent Channel > 3
- Span = 10 MHz
Bluetooth Baseband

SOFTWARE STACK

APPLICATIONS

TCP/IP  HIC  RFCOMM

DATA

L2CAP

LINK MANAGER

BASEBAND

RADIO

Baseband Controller

- **Baseband**: baseband protocols and low level link routines

- **Link Manager**: Link Layer messages for setup and link control
Bluetooth Baseband

- **Frequency Hop Time Division Duplex Channel**
  Channel based on a 625 µsec time slot (1600 hop/sec)
  220 µsec of the slot lost to PLL settling

- **Bluetooth uses both circuit and packet switched channels, supports:**
  - Up to 3 simultaneous 64 kbps synchronous voice channels
  - Simultaneous synchronous voice and asynchronous data channel
  - Asynchronous data channel:
    - 721/57.6 kbps asymmetric
    - 432.6 kbps symmetric

Bluetooth Packet Format

![Bluetooth Packet Format Diagram](image_url)
Access Codes

- **Channel Access Code (CAC):** Identifies a piconet, this code is used with all traffic exchanged on a piconet.

- **Device Access Code (DAC):** Used for signaling, e.g. paging and response to paging.

- **Inquiry Access Code (IAC):**
  - General Inquiry Access Code (GIAC)
    Common to all Bluetooth devices
  - Dedicated Inquiry Access Code (DIAC)
    Common to a class of Bluetooth devices
  - Inquiry process “finds” BT devices in range

Packet Header

- **AM_ADDR:** 3 bit member address defines active members of a piconet.

- **Data Type:** Defines various types of packets and their length. Allows non-addressed slaves to determine when they can transmit.

- **Flow Control**

- **Acknowledgement:** ACK/NAK field

- **HEC:** header error check, if an error is found, the entire packet is discarded.
TDD and Packet Timing

- Bluetooth is time division duplex (TDD)
- About 220 µsec of the time slot is left for synthesizer settling
  Allows simple single loop synthesizers for frequency hop
- Master transmits in even number slots
  Slave transmits in odd number slots

Multi-slot Packets (Master Transmit)
Packet Types: System

- **ID**: Contains Device Access or Inquiry Access Code
  Used for paging, inquiry, and response

- **NULL**: Channel Access Code and Packet Header
  Used for acknowledgement and buffer flow control

- **POLL**: Similar to NULL packet but a slave response is required upon reception

- **FHS**: Contains Bluetooth device address and the clock information of sender, used in piconet set up and hop synchronization

High Quality Voice Packets

- **HV1 Packet**
  - 1/3 rate FEC protected, no retransmission, no CRC
  - 10 data bytes 1.25 msec of 64 kbps speech
  - Retransmitted every two time slots

- **HV2 Packet**
  - 2/3 rate FEC protected, no retransmission, no CRC
  - 20 data bytes 2.5 msec of 64 kbps speech
  - Retransmitted every 4 time slots

- **HV3 Packet**
  - No FEC, no retransmission, no CRC
  - 30 data bytes 3.75 msec of 64 kbps speech
  - Retransmitted every 6 time slots
Medium Rate Error Protected Data Packets

- **DM1: Data Medium rate**
  - 18 data bytes and occupies 1 time slot
  - 2/3 FEC plus 16 bit CRC
- **DM3**
  - 123 data bytes and occupies 3 time slots
  - 2/3 FEC plus 16 bit CRC
- **DM5**
  - 226 data bytes and occupied 5 time slots
  - 2/3 FEC plus 16 bit CRC

High Rate Data Packets No Error Protection

- **DH1: Data High rate**
  - 28 data bytes and occupies 1 time slot
  - 16 bit CRC, no FEC
- **DH3**
  - 185 data bytes and occupies 3 time slots
  - 16 bit CRC, no FEC
- **DH5**
  - 341 data bytes and occupied 5 time slots
  - 16 bit CRC, no FEC
Other Packets

- **DV**: Combined voice data packet, Transmitted as SCO packet
  - Voice: 80 bits  No FEC and no retransmission
  - Data: up to 150 bits  2/3 FEC but retransmission permitted

<table>
<thead>
<tr>
<th>Access Code</th>
<th>Header</th>
<th>Voice Field</th>
<th>Data Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>72 bits</td>
<td>54 bits</td>
<td>80 bits</td>
<td>32 - 150 bits</td>
</tr>
</tbody>
</table>

- **AUX1**: Similar to DH1 packet but 30 bytes, no CRC

---

Bluetooth Data Rates

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Symmetric</th>
<th>Asymmetric</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM1</td>
<td>108.8 kbps</td>
<td>108.8 kbps</td>
</tr>
<tr>
<td>DH1</td>
<td>172.8 kbps</td>
<td>172.8 kbps</td>
</tr>
<tr>
<td>DM3</td>
<td>258.1 kbps</td>
<td>172.8 kbps</td>
</tr>
<tr>
<td>DH3</td>
<td>390.4 kbps</td>
<td>585.6 kbps</td>
</tr>
<tr>
<td>DM5</td>
<td>286.7 kbps</td>
<td>477.8 kbps</td>
</tr>
<tr>
<td>DM5</td>
<td>433.9 kbps</td>
<td>723.2 kbps</td>
</tr>
</tbody>
</table>
Bluetooth ARQ

Physical Links

- Bluetooth supports synchronous and asynchronous physical connections

- Asynchronous Connectionless (ACL) Link
  - Master exchanges packets with any slave on a per slot basis
  - Packet switched connections to all active slaves in the piconet
  - Only a one ACL link per slave
  - ACL packets not addressed to a particular slave are broadcast packets and are read by all slaves
Physical Links

- **Synchronous Connection Oriented (SCO) Link**
  - Point to point synchronous symmetric link between the master and a particular slave
  - Circuit switched: time slots are reserved for time bounded information like voice
  - Master can support up to three SCO links with the same or different slaves
  - A slave can support up to three SCO links with one master or two with different masters
  - Link Manager (LM) establishes SCO link through LM protocol messages

Multiple Links with Mixed Packets
**Bluetooth Addressing**

- **Bluetooth Device Address (BD_ADDR)**
  - Uniquely identifies a Bluetooth device
  - 48 bit IEEE 802 address

- **Active Member Address (AM_ADDR)**
  - 3 bit address identifies active piconet slave
  - All zero address for broadcast

- **Parked Member Address (PM_ADDR)**
  - 8 bit address identifies an packed slave

**Synchronization**

- Hopping sequence is established by the master device address, each Bluetooth device has a unique address
- Timing takes place in the Baseband layer
- Specification for NATIVE CLK is only ± 20 ppm
Clock Offsets Established

Each slave calculates an time offset from its local clock.

Link Manager

SOFTWARE STACK

APPLICATIONS
TCP/IP  HCI  RFCOMM
DATA
L2CAP
BASEBAND
RADIO

Link Manager
Link Manager Protocol (LMP)

• **Link Configuration**
  – Supported features
  – Quality of Service, packet types
  – Security and Authentication
  – Establishes Logical Channels
    Beacon, Paging, Broadcast

• **Security Functions**
  – Authentication
  – Encryption and Key Management

Link Manager Protocol (LMP)

• LMP runs between Link Managers

• LMP sets up, terminates, and manages baseband connections

• **LMP Functionality**
  – Attach and detach slaves
  – Control Master-Slave switch
    Used when a Slave/Master participates in another piconet as Master/Slave
  – Establish ACL and SCO links
  – Control low power modes: Park, Hold and Sniff
Bluetooth Connection States

Link Manager Controls BT operational modes

- **Active Mode**
  - BT can accommodate only 7 active slaves
  - AM_ADDR: 3 bit address given to each active slave

- **Hold Mode**
- **Park Mode**
- **Sniff Mode**

**Hold Mode**

- **ACL slave placed on Hold mode**
  - ACL packets no longer supported
  - SCO packets can still be exchanged
- **Frees Slave**
  - When master has no data, goes to low-power sleep
  - To attend another piconet
  - Scanning, inquiry, paging
    - Slave finds or is found by another piconet
- **Slave keeps AM_ADDR**
- **Master assigns hold time**
  - After hold time slave wakes up and synchronizes with traffic on the channel
Park Mode

- **Low activity, low power mode**
  - “Deeper Sleep” than Hold Mode
  - Devices wake up periodically to resynchronize and check for broadcast messages

- **Parked Device**
  - Gives up AM_ADDR
  - Remains synchronized
  - Receives:
    - PM_ADDR: 8 bit Park Member Address
    - AR_ADDR: 8 bit Access Request Address

- **Allows multiple slaves to be connected to a Master**

---

Park Mode

- **Parked Member Address**
  Used in Master initiated reconnection

- **Access Request Address**
  Used in Slave initiated reconnection

- **Special all zero PM_ADDR**
  - Device must be unparked using 48 bit BM_ADDR
  - Allows almost an unlimited number of parked devices
Park Mode Beacon Channel

- Master establishes a Beacon Channel when a device is parked
  - Maintains packed member synchronization
  - Communication via broadcast Link Manager messages
Sniff Mode

- **Sniff Mode much like Hold Mode**
  - Device remains active
  - Low power active mode

- **Slave retains AM_ADDR and goes to sleep**
  - Wakes up at assigned Sniff Interval to exchange packets

Sniff Mode

<table>
<thead>
<tr>
<th>Sniff Interval</th>
<th>Nsniff</th>
<th>Ntimeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic reduced to periodic Sniff slots: Nsniff</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slave listens for traffic with Slave AM_ADDR or Nsniff which ever is longer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>After traffic ceases, Slave continues to listen for Ntimeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LMP sets Sniff Mode parameters</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ACL Link Setup Under LMP

Overview of LMP

Piconet Management
- ACL Link setup and detach
- SCO Link setup and detach
- Master/Slave Switch
- Low Power Modes
  - Hold
  - Sniff
  - Park

Link Configuration
- Power Control
- FEC Control
- QoS Control
- Link Timers
- Multi slot packet

Link Information
- LMP Version
- LMP supported features
- Clock and Timing
Bluetooth and Interference

Unlicensed Part 15 devices
- Must take interference from unlicensed/licensed services
- Must not give interference
- No interference protection

Acknowledgement Scheme
- R&R: Rude and Robust
  - Robust: retransmits until message gets through
  - Rude: keeps retransmitting, may negatively impact throughput of listen before transmit devices (IEEE802.11)
- Frequency Hop will avoid some interference
- Will retransmitting lead to the Tragedy of the Commons with multiple devices in a Bluetooth enabled space?
Logical Link Control

- Logical Link Control and Adaptation Layer Protocol (L2CAP)
  - Layered over baseband protocol
  - Supports services
    - Protocol multiplexing
    - Segmentation/reassembly
    - Quality-of-Service (QoS)
    - Group abstractions

Protocol Multiplexing

- Baseband protocol treats all data packets equally
  - L2CAP needs to distinguish multiple protocols
    - Service Discovery Protocol
    - RFCOMM
    - Telephony Control
Segmentation/Reassembly

- Baseband packets are size-limited
  - Large packets need to be segmented by L2CAP into smaller baseband packets
  - Multiple baseband packets need to be reassembled into single, large packet
    - Integrity check performed on data
      - 16-bit CRC
      - Leverages ARQ mechanism used by baseband protocol

Quality-of-Service (QoS)

- L2CAP supports QoS message between Bluetooth devices
  - Only required to support “Best Effort” service
    - No guarantees
  - Other QoS services are optional
    - Token Rate
    - Token Bucket Size
    - Peak Bandwidth
    - Latency
    - Delay Variation
Group Abstraction

- Piconet supported by baseband protocol
  - Group Abstraction allows mapping of protocol groups to piconets
- Prevents higher-level protocols from needing to interact with baseband protocol or link manager

Service Discovery Protocol (SDP)

- Means for application to:
  - Discover services available on device
  - Determine characteristics of services available
- Single SDP server per device
- Device may contain both SDP Client and Server
SDP Requirements

• Ability to search services based on attribute
• Service discovery based on service class
• Allow browsing of services without apriori knowledge of service characteristics
• Allow for dynamic service discovery
  – Allows for device to enter or exit coverage area
• Uniquely-identified service/service classes

SDP Requirements

• Client on one device able to determine the services on another device without consulting a third device
• Simple enough for use by simple devices
• Allow for gradual service discovery
• Allow caching of service discovery
SDP Requirements

• Functions while using L2CAP as transport protocol
  – QoS info, segmentation, and protocol multiplexing
• Allows the usage of other service discovery protocols
• Support creation of new services without registration with central authority

SDP Basic Functionality

• SDP Client requests information from SDP Server
  – Information from Service Record returned
    • Contains list of Service Attributes
• Separate connection needs to be establish to initiate service
  – SDP connection used only to determine service availability
Sample Service Attributes

- ServiceName (human-readable)
- ServiceID (identifier for unique service instance)
- ServiceClassIDList (list of classes in which a service is an instance)
  - Example of color printer ServiceClassIDList
    - DuplexColorPostscriptPrintServiceClassID
    - ColorPostscriptPrinterServiceClassID
    - PostscriptPrinterServiceClassID
    - PrinterServiceClassID

SDP Wrap-up

- SDP allows the search and browsing of services available through nearby devices
- SDP allows an application to interface with the Bluetooth device to establish who is out there and what type of services are supported
RFCOMM

- Emulation of serial port over L2CAP protocol
  - Supports up to 60 simultaneous connections between two Bluetooth devices
    - Actual maximum of supported devices is implementation-specific
  - Bluetooth acts as a replacement for the serial cable

Telephony Control Protocol

- Call Control
  - Establishment and release of speech or data calls between Bluetooth devices
- Group Management
  - Ease handling of groups of Bluetooth devices
- ConnectionLess
  - Exchange signaling information not related to on-going call
IrDA Interoperability

• Infrared Data Association (IrDA)
• Support development of applications that operate well over both short-range RF and IR
  – Achieve technology overlap with IrOBEX
    • Protocol defined by IrDA
    • Used also by Bluetooth
    • Mapped over RFCOMM and TCP/IP (optional)

Bluetooth IrOBEX (OBEX)

• Uses only connection-oriented OBEX
  – Mapped over connection-oriented Bluetooth architecture
• Enables exchange of data objects
• Simple commands
  – Connect, Disconnect, Put, Get, SetPath, Abort
WAP Interoperability

- Bluetooth used to communications between WAP client and server
  - Physical layer and link control
- In general, support communications between any two WAP-enabled Bluetooth devices

WAP Integration

- Provide ability for WAP applications to use Bluetooth device
  - Application-controlled communications
- Supported through PPP/RFCOMM
  - Also support SDP
- WDP Management Entity needed
  - Out-of-band mechanism for controlling protocol stack
    - Used to support detection of nodes and other events
First Commercial Bluetooth Product

- Hands free headset for cellular phone
- Introduced by Ericsson
  Fall 1999

Getting Started in Bluetooth

- Bluetooth technical specification is openly available
  - www.bluetooth.com
  - Current news and hype!

- Palo Pacific Technology
Bluetooth Development Kits

- Development Kits for Bluetooth
  - Ericsson: www.ericsson.se
  - Digianswer
    - Danish, owned by Motorola
    - www.digianswer.com
  - Cambridge Silicon Radio
    - English
    - www.cambridgesiliconradio.com

Ericsson Radio Module

Operates as
- USB device
- UART
Ericsson Development Kit

- Starter kit available 1Q 2000
  - $3000
- Full kit available

Cambridge Silicon Radio
CSR: BlueCore

CSR Development Kit

- Motherboard and software to interface with PC
- Contains BlueCore 01
- Cost: $8K
- Availability: now
- www.cambridgesiliconradio.com
Conclusion

- Bluetooth provides robust, short-range communications
- Flexible configuration can support multiple applications
  - Layers capable of supporting significant application variety growth
- Standard’s loose implementation guidelines allow for introduction of new technology

Final Thoughts

- A single-chip solution is the ultimate goal
  - Around $5/chip
  - Several players have begun developing implementations
- Success of device depends on
  - The supplier’s ability to deliver implementation at a low price point
  - Application development that is easily integrated with today’s infrastructure
  - Ability of Bluetooth to meet market’s expectations