Examining the Changes with Bluetooth™ Core Specification Version 1.1

Tom Siep, Texas Instruments
siep@ti.com

Bluetooth is a trademark Telefonaktiebolaget L M Ericsson, Sweden
Topics

◆ Overview of Specification 1.1
◆ The general nature of the changes in the specification
◆ Changes in:
  ■ Radio
  ■ Baseband
  ■ LMP
  ■ L2CAP
  ■ HCI
  ■ Other
◆ Summary
My Involvement with Bluetooth

◆ TI Short Distance Wireless Business Unit formed
◆ Chief Technical Editor, IEEE802.15
◆ Lead Technical Editor, IEEE802.15.1
◆ Editorial interface between BSIG and 802.15.1
◆ Author

"An IEEE Guide: How to Find What You Need in the Bluetooth Spec"


◆ Bluetooth Specification Section Owner, L2CAP
Bluetooth Architecture

- Applications
  - Other
  - TCS
  - RFCOMM
  - SDP
- Data
- Control
- Audio
- L2CAP
- Link Manager
- Baseband
- RF
Bluetooth Architecture
How Does IEEE 802.15.1 Relate to Bluetooth?
How the Bluetooth Spec Changes

- Discovery of problem during:
  - Reading the Spec
  - Implementation
  - Usage

- Submission to Errata system
  - Critical
  - Recommended

- Debate/Resolution by Section members
- Integration into proposed revision of Spec
- Approval by Bluetooth Architecture Review Board
- Approval by Promoters → Associates → Adopters
- Publication of new Specification
What Changed?

Lots of edits

but

Not a lot of fundamental changes
A Little More Detail on v1.1

◆ In general
  ■ Clarifications
  ■ Corrections
  ■ Little or no “new” features

◆ Specifically
  ■ Radio – Regulatory domain changes
  ■ Baseband – Connection issues in the channel
  ■ LMP – Link Control issues clarified/corrected
  ■ L2CAP – Corrections to a few complex interactions
Radio

Radio (RF) Defines Bluetooth radio front-end (IEEE calls this a PHY)

- 2.4GHz ISM band
- 1Mbps
- 1,600 hops/sec
- 0dBm (1mW) radio, up to 20dBm
Radio Critical Errata

- Harmonisation (or in the US, Harmonization) of frequency bands
  - France
  - Spain
  - Japan
Baseband

- Baseband (BB)
  - Piconet/Channel definition
  - “Low-level” packet definition
  - Channel sharing
Baseband Critical Errata

- Master Slave switch – clarification
- ACO Correction – generation of an encryption key is optional
- Audio – text clarifying the order of the CVSD encoded bit stream when sent over air
- Sniff Mode – Inactive connection modes HOLD and SNIFF do not affect the ARQN scheme
- Sniff Mode – Alignment with LMP
Link Management Protocol

- Link Management Protocol (LMP) – Defines link properties
  - encryption/authentication
  - polling intervals set-up
  - SCO link set-up
  - low power mode set-up
LMP Critical Errata

- Stopping encryption
- Allowed PDUs on host_connection_req
- Link setup procedure
- Mutual authentication on Kinit
- Slave needs to control slots in uplink
- TransactionID in LMP_setup_complete
- Change link key problems
- Temporary link keys
- LMP/BB inconsistency for encryption restart
- AM address position in unpark command
- Counting sniff slots
- No text describing master initiating sniff mode
- Handling disallowed PDUs
- LMP version
- Dynamically enabling encryption
- Definition of Transaction
- Synchronisation
  - detach
  - hold
  - park
  - switch
- LC level timings.
- Timeouts between transactions
- slot offset definition
- ACO mismatch fix
- Flow control lag feature
Logical Link Control & Adaptation Protocol (L2CAP)

- A simple data link protocol on top of the baseband
  - connection-oriented & connectionless
  - protocol multiplexing
  - segmentation & reassembly
  - QoS flow specification per connection (channel)
  - group abstraction
L2CAP Critical Errata

- Actions on timer expiration
- Configuration request sent to invalid CID
- Continue flag sequencing on lost packets
Host Controller Interface (HCI)

- Provides a common interface between a Bluetooth host and a Bluetooth module
  - Physical Interfaces – USB; UART; RS-232
  - Control Interface
HCI Critical Errata

No critical Errata
Other Critical Errata

◆ Service Discovery Protocol
  ■ Base UUID incorrect
  ■ UUID error in PublicBrowseRoot
  ■ MaximumAttributeCount ambiguous

◆ RF Comm
  ■ Multiple multiplexer control messages
  ■ DLC parameter negotiation
  ■ Message Sequence Chart (MSC) command clarification
  ■ Mandatory requirements unnecessary
Other Critical Errata (profiles)

◆ Cordless Telephone Profile
  ■ Ordering ServiceClass UUIDs
  ■ CTP with optional PARK mode

◆ Intercom Profile
  ■ ServiceClass UUID ordering
  ■ SCO establishment initiator

◆ Headset Profile
  ■ Service Record for the Audio Gateway
  ■ Definition of "gain"
  ■ RING not always necessary
  ■ Bonding should be optional

◆ Dial-up Networking Profile and FAX Profile
  ■ Ordering ServiceClass UUIDs
  ■ General/Limited Discoverable modes should match GAP

◆ LAN Access Profile
  ■ PinCode
Summary

◆ Process of change of 1.x continues

◆ Evolutionary not Revolutionary

◆ Continuity and backward compatibility is considered to be a critical success factor