Bluetooth® SIG Liaison Report May 2009

Date: 2009-05-12

Authors:

Name	Affiliations	Address	Phone	email
John R. Barr	Motorola, Inc.	21939 Old Farm Road, Deer Park, IL 60010	+1-847-962-5407	barr@ieee.org

Abstract

Overview of recent activities of the Bluetooth SIG to inform IEEE 802.15 and 802.11 about developments concerning use of IEEE 802.11 standards by the Bluetooth SIG.

Bluetooth® Wireless Technology

- **Most recognized wireless brand world wide.**
- **Over 2 Billion *Bluetooth* enabled devices shipped:**
  - 600M Bluetooth devices shipped in 2006 (12 million per week)
  - 833M shipped in 2007 (16 million per week)
  - Over 1B shipped in 2008 (19 million per week)
  - Target of 2B devices shipped in 2012 (38.5 million per week)
- **81% of the current *Bluetooth* device market centered around mobile phones**
  - 75% are mobile phones and headsets (mono and stereo)
  - 6% are PCs, printers, and dongles that support mobile phones
- **9% of market is gaming devices:**
  - 91M *Bluetooth* devices shipped for Wii and PS3 remotes
- **The only wireless specifications that provide a complete end-to-end experience for end consumer.**
- **True Personal Area Networking between Peer devices.**

Current Status

- **3.0 + HS Specification Adopted on April 21, 2009**
  - High Speed Transport
  - Other performance enhancements
- **Bluetooth Low Energy Scheduled for Early 2010**
  - Low Energy radio suitable for products that run on button batteries (Sensors and Watches)
  - Health & Fitness applications

Bluetooth Core Specification Version 3.0 High Speed (HS)

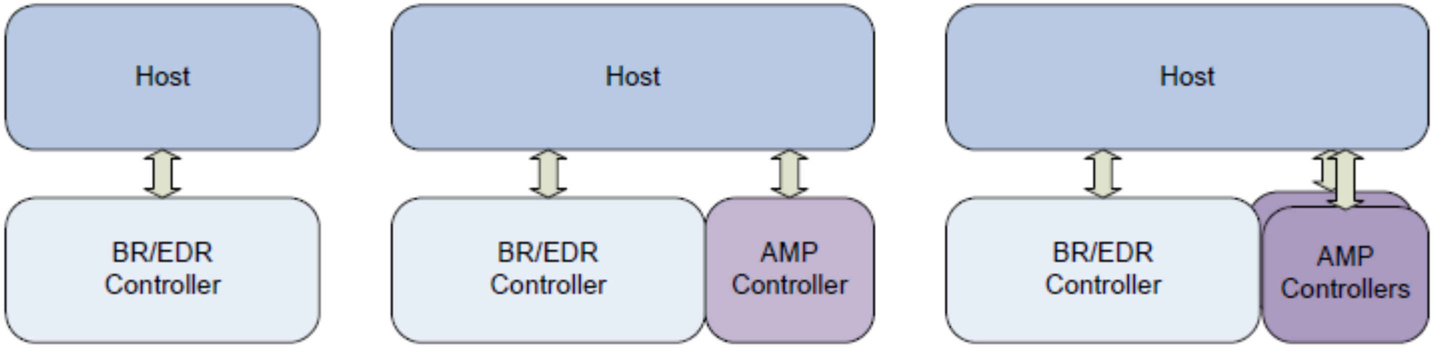
- **High Speed Bluetooth Specification Adopted 21April09**
- **“High Speed” achieved by using IEEE 802.11-2007 as an Alternate MAC/PHY with ERP mode mandatory.**
- **Designed so that operation does not interfere with connection to an AP.**
- **Demonstrated on existing net book with updated software for Bluetooth 3.0 + HS implementation.**
  - No hardware changes required for existing certified Wi-Fi device with Bluetooth 2.1 chip sets.

Features of 3.0 + HS

Feature	Benefits	Core Part
Generic Alternate MAC/PHY (AMP)	Improvements to the Host to enable high speed and to support multiple radios	Host
802.11 Protocol Adaptation Layer (PAL)	Enables the use of the 802.11b/g/a MAC/PHY as a high speed radio	AMP Controller
HCI Transport Updates (USB and SDIO)	Support for multi-function devices and other improvements required to support PALs	All
Generic Test Methodology	Provides a common method for testing AMPs without requiring a standardized HCI transport	Host
Unicast Connectionless Data	Enables 50-100ms shorter latency for sending small amounts of data	Host
Enhanced Power Control	Faster and more responsive power control	BR/EDR Controller
Read Encryption Key Size	Enables the Host to read the encryption key size for a given connection. Important for profiles that require high levels of security (e.g. SIM Access Profile)	BR/EDR Controller

CONFIGURATIONS

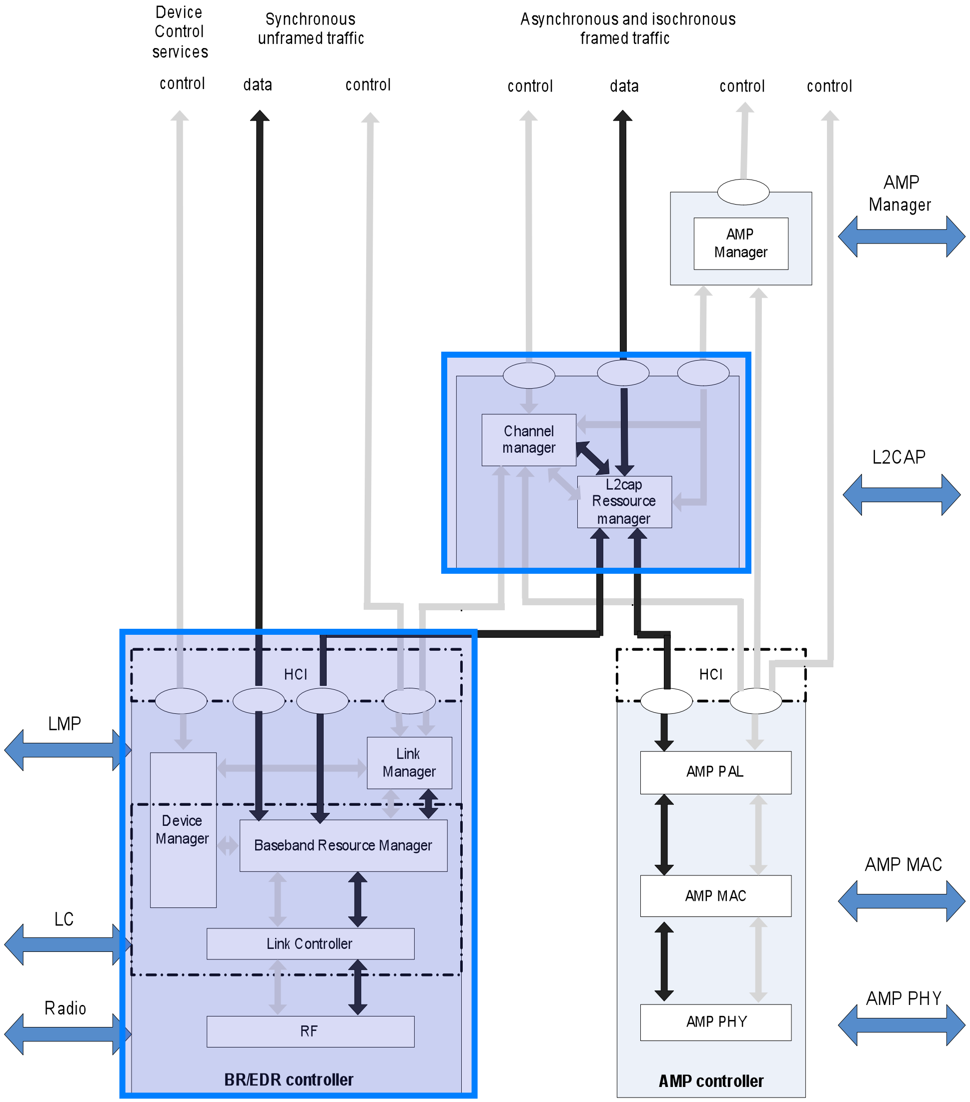
- Prior to 3.0 + HS, there were two main parts to the *Bluetooth* Core architecture: *Bluetooth* Host and *Bluetooth* Controller
- 3.0 + HS adds a third part, the AMP Controller, and also renames the "*Bluetooth* Controller" as the "Basic Rate / Enhanced Data Rate" (BR/EDR) Controller"



DISCOVERY AND CONNECTION SETUP

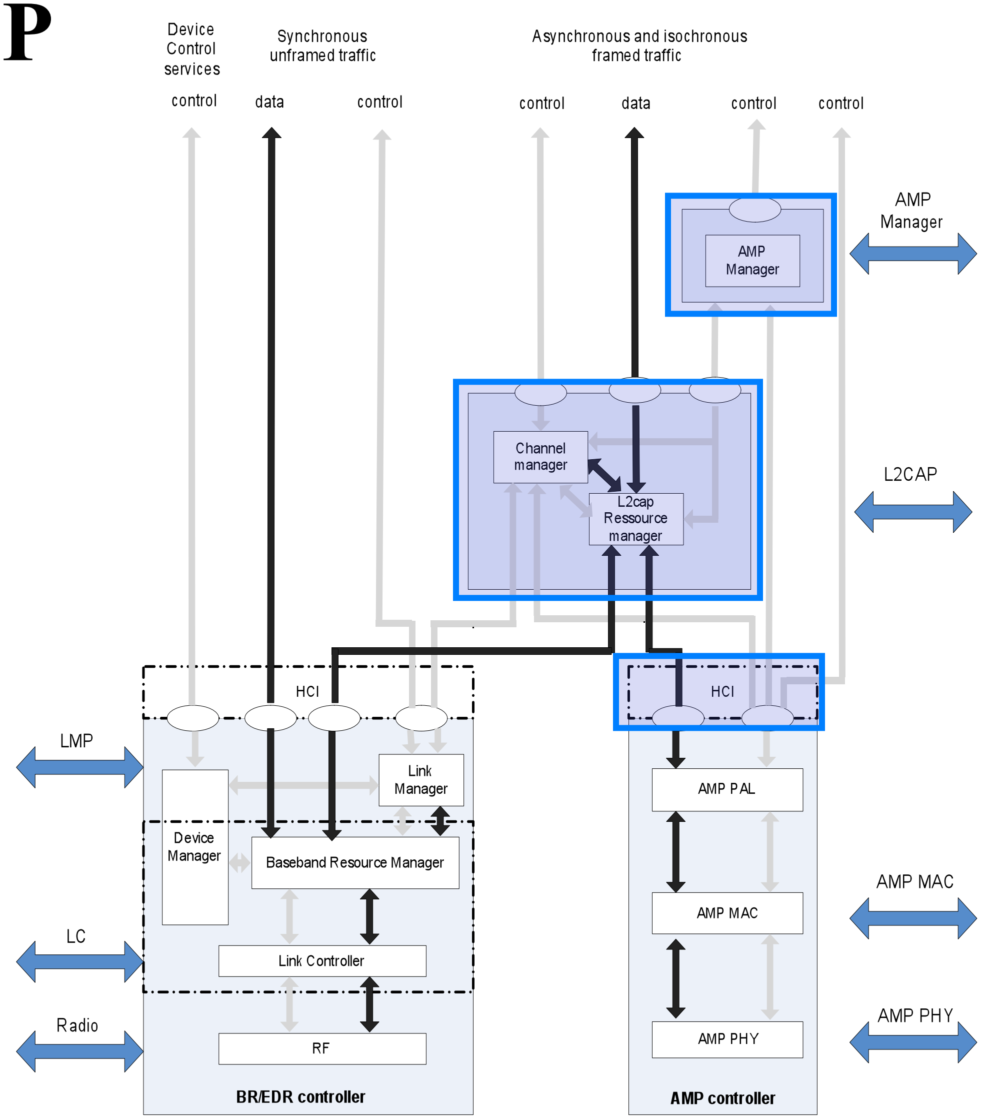
- **A key aspect of the AMP architecture is that discovery, association and initial connection setup is identical to *Bluetooth* 2.1**

- **Benefits**
  - These mechanisms do not have to be replicated over each new high speed radio
  - Ensures backwards compatibility with the almost 2B deployed base of *Bluetooth* products



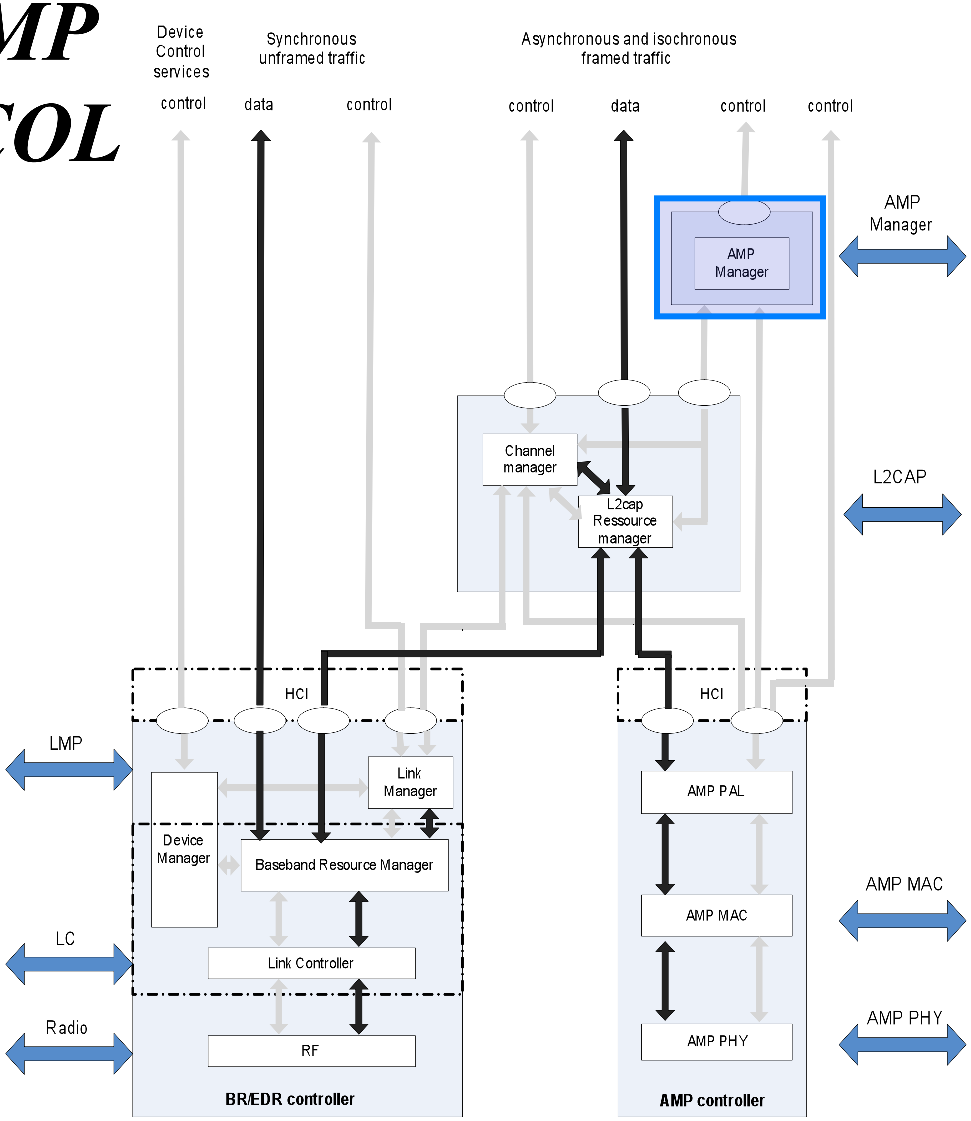
GENERIC AMP

- **"Generic AMP" is the infrastructure for utilizing Alternate MAC/PHYs including**
  - AMP Manager Protocol (A2MP)
  - L2CAP changes
  - Security
  - HCI updates



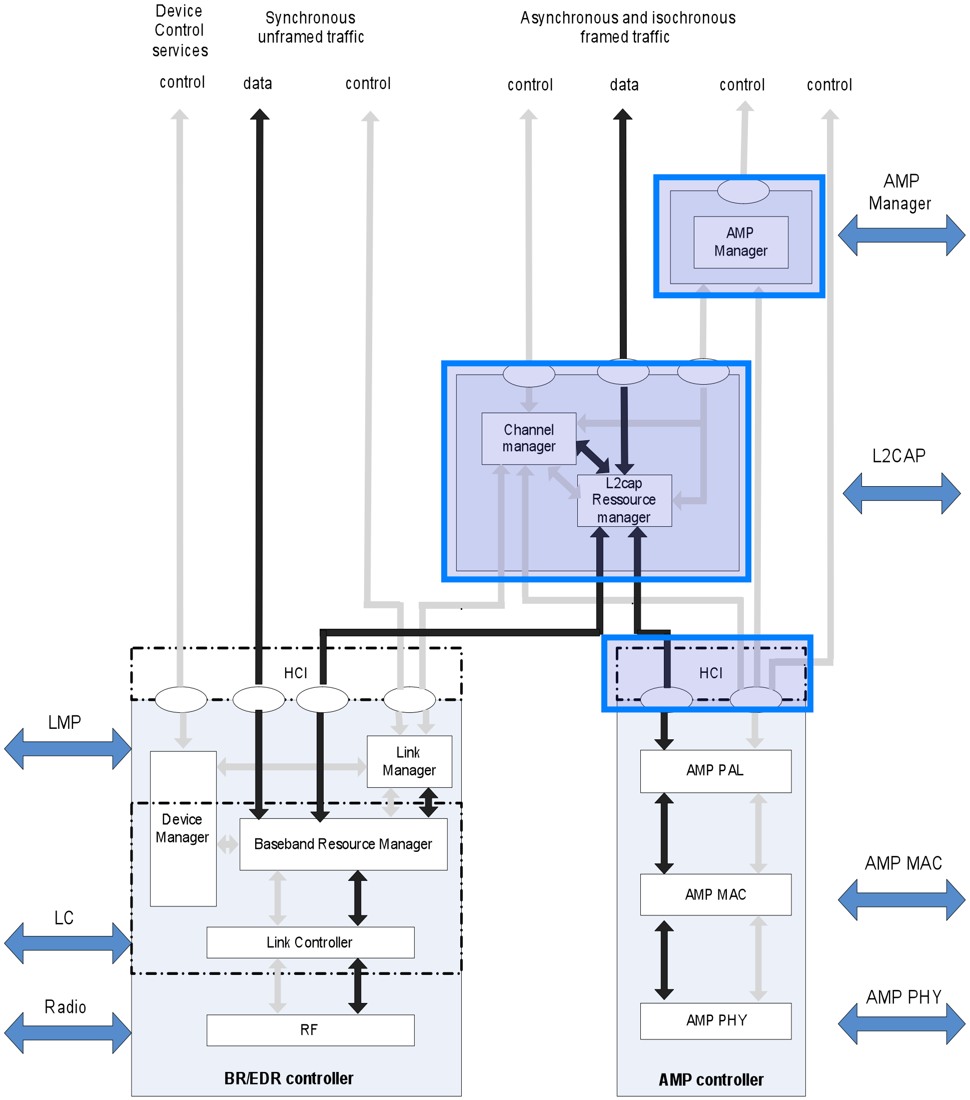
GENERIC AMP: *AMP MANAGER PROTOCOL*

- **The AMP Manager Protocol (A2MP) is responsible for**
  - Discovering remote AMP Managers and Controllers
  - Querying remote AMP Controller information
  - Managing AMP physical links
  - Creating dedicated AMP keys
- **The AMP Manager Protocol runs exclusively over BR/EDR**
- **A2MP uses a fixed L2CAP channel**
  - "Fixed" L2CAP channels have pre-defined characteristics, so negotiation isn't required and channel setup is immediate



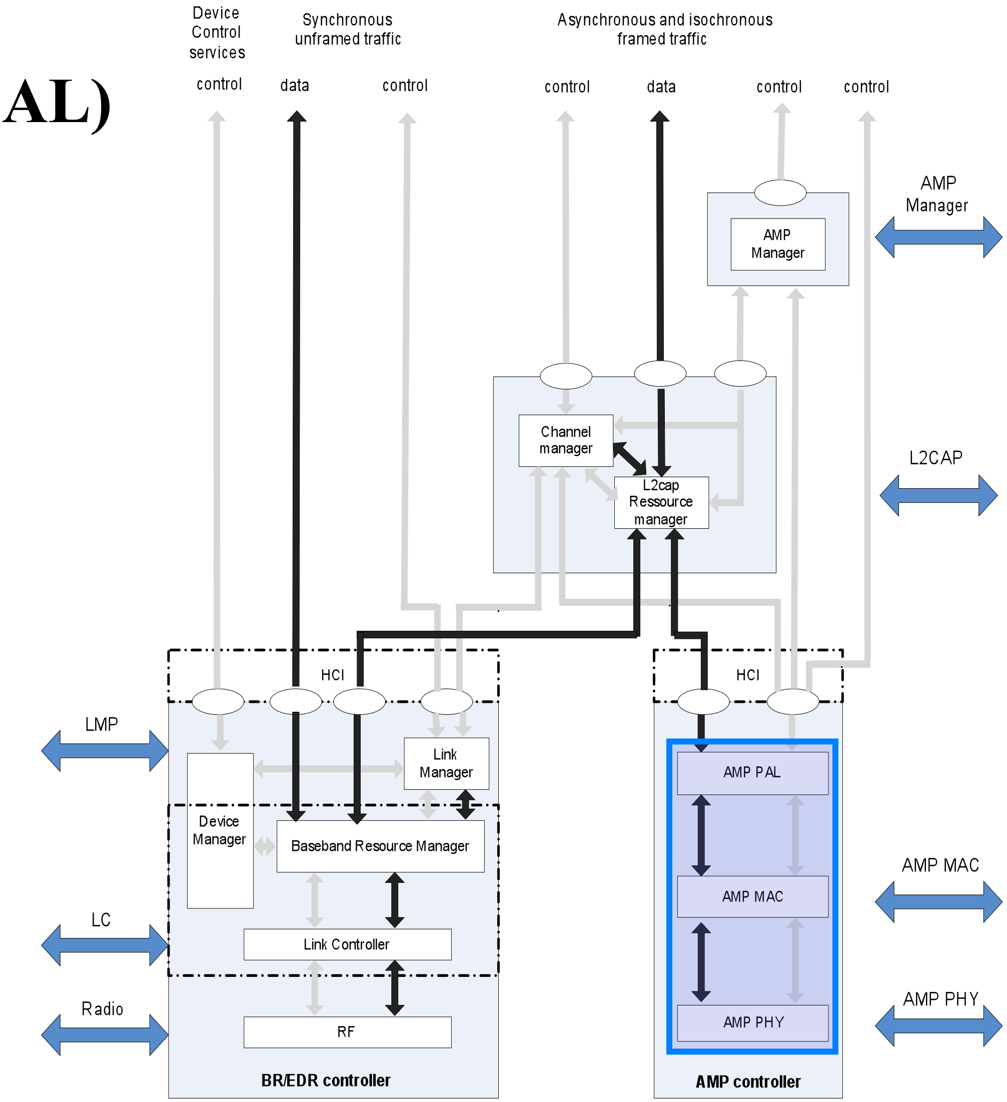
GENERIC AMP: *SECURITY*

- Pairing and Link Key generation for the BR/EDR Controller remains the same as in version 2.1
- Generic AMP derives a key from the BR/EDR link key using the h2 function with keyID="gamp"
- Dedicated link keys are then derived for each AMP also using the h2 function and a keyID specific to the AMP (e.g. "802b" for 802.11)
- Each AMP uses the dedicated link key for authentication during physical link setup



802.11 PROTOCOL ADAPTATION LAYER (PAL)

- **The 802.11 PAL is the Protocol Adaptation Layer that translates between HCI and the 802.11 MAC**
  - 802.11-2007 plus amendment 1 is the referenced standard
  - Once 802.11n is ratified, the specification may be updated to include it
- **The 802.11 MAC utilizes the 802.11 four address frame format in order to support simultaneous ad-hoc and infrastructure operation**
- **Target performance requirements**
  - >24Mbps stand alone
  - >12Mbps with SCO
  - >15Mbps when connected to an Access Point



MANDATORY COMPONENTS

- **802.11 physical link requires BR/EDR as control channel**
- **Devices shall implement 802.11 Enhanced Rate PHY (ERP, aka 802.11g)**
  - Specified by IEEE 802.11-2007 and Amendment 1
  - Devices may implement 802.11 OFDM PHY (aka 802.11a)
- **Devices shall send beacons**
- **RTS/CTS signaling shall be used unless non-interference indicated with Activity Report messages**

PAL PROTOCOLS

- **Physical Link establishment**
- **Security**
  - RSNA
  - 4-way handshake
- **Link supervision protocol**
- **Activity Reports**

PHYSICAL LINK ESTABLISHMENT OUTLINE (1)

- **A2MP Discovery**
- **Responder supplies its AMP Assoc to initiator**
  - Allows deterministic channel selection
- **Initiator**
  - Selects 802.11 channel
  - Starts its MAC if not already done
  - Supplies AMP Assoc to responder
- **Responder**
  - Reads 802.11 channel from initiator’s AMP Assoc
  - Starts its MAC if not already done

PHYSICAL LINK ESTABLISHMENT OUTLINE (2)

- **Both use 802.11 open authentication**
- **Both use 802.11 association**
- **Both use RSN-PSK**
  - Dedicated AMP Link Key used as PMK
  - AES-CCMP used as pairwise cipher
  - Encapsulated with Security Frame protocol ID (not EAPOL)

QUALITY OF SERVICE

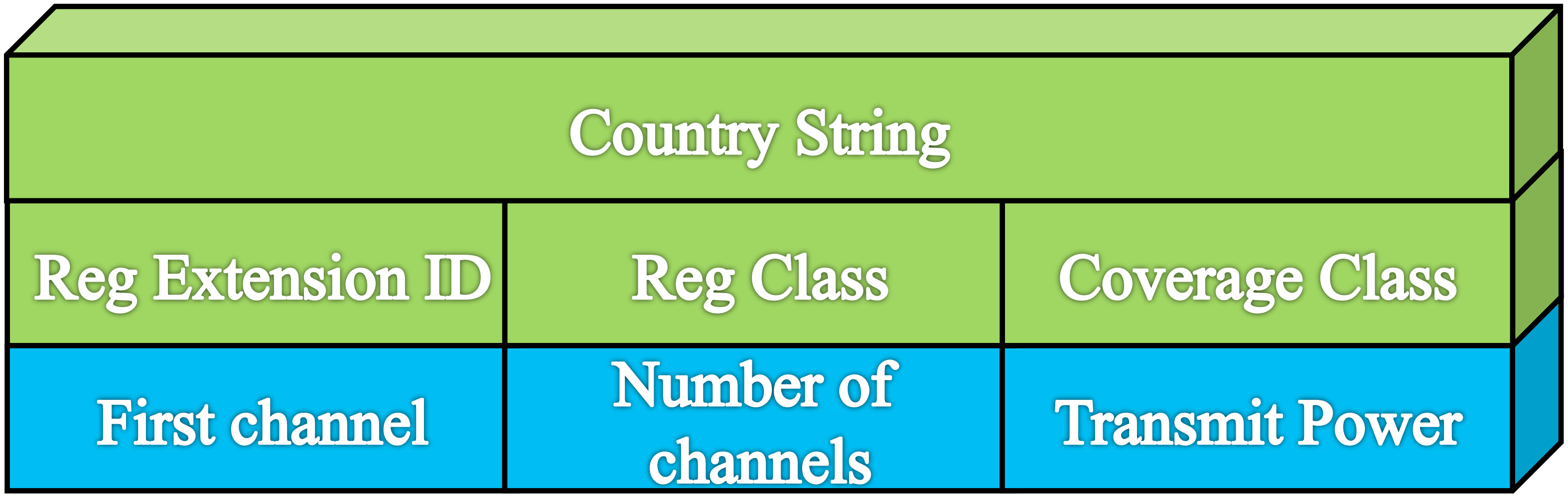
- **802.11 AMP QoS implemented with EDCA**
- **Use of IEEE 802.11 EDCA is optional**
  - Availability advertised in AMP discovery phase
    - Remote: PAL Capabilities parameter of the AMP GetInfoResponse packet
    - Local: PAL Capabilities parameter of the HCI Read Local AMP Info
  - If both peers advertise Guaranteed service type, Host may attempt to create a Guaranteed logical link
- **If it is to be used, then devices must:**
  - Advertise EDCA Parameter Set element in beacons and probe responses
  - Include the QoS Capability element in association requests

CHANNEL SELECTION

- **Both initiator and responder may scan before advertising channel list (responder) or selecting operational channel (initiator)**
- **Preferred Channel List uses syntax similar to IEEE 802.11 Country Information element**
  - Channels inserted in order of preference
  - Absence of sub-band triplet implies no preference in band
- **No requirement to determine or advertise current locale, but performance may be improved**
- **Country String 'XXX' used for 'non-country' identifier**

PREFERRED CHANNEL LIST

- Country String – required
- Regulatory triplet {Regulatory Extension ID, Regulatory Class, Coverage Class} – required
- Sub-band triplet {First channel number, Number of Channels, Tx Power} - optional



Country String

Reg Extension ID | Reg Class | Coverage Class

First channel | Number of channels | Transmit Power

ACTIVITY REPORTS

- **PAL to PAL messages sent over 802.11 medium**
- **Notification to peer of:**
  - Absence of interference
  - Presence of interference, with schedule if known
- **May include multiple schedules**
- **802.11 TSF (clock) of sender used as reference**
- **Activity Reports are optional to send**

INTER-OPERATION WITH 802.11 NETWORKS

- **802.11 PAL specification does not require any features or services which prevent *Bluetooth* devices from concurrently communicating with an 802.11 Access Point (AP) and another *Bluetooth* device using the 802.11 PAL**
- **802.11 AMP devices may refuse to establish a physical link when the same channel between AP and AMP peer is not available**
- **Beacons and probe responses are used to signal AMP operation to other devices and networks, including QoS parameters**
- **802.11 AMP devices use same channel access procedures as non-AMP 802.11 devices**

SHORT RANGE OPERATION

- **As an ad-hoc personal area wireless technology, *Bluetooth* products tend to work closer to each other than Wi-Fi products using an infrastructure network**
  - For example, you may place your cell phone very close (less than 12 inches) to your laptop while making a data transfer
- **Consumers are used to data rates decreasing as devices get further apart. They are not used to the data rate decreasing as the devices get closer together.**
- **To ensure that *Bluetooth* devices retain high throughputs at both short and long range, *Short Range Mode* (the ability to reduce the TX power to +4dBm) was included**

802.11 PAL SUMMARY

- **Supports transfer rates as high as 24 Mbps**
- **Supports AMP connections concurrently with non-AMP connections**
- **Supports 2.4 GHz and 5 GHz spectral bands**
- **Supports Quality of Service**

References

- http://www.bluetooth.com/Bluetooth/Press/SIG/iBLUETOOTHi_TECHNOLOGY_GETS_FASTER_WITH_iBLUETOOTHi_30.htm
- http://www.bluetooth.com/Bluetooth/Products/Bluetooth_High_Speed_Technology.htm
- http://www.bluetooth.com/Bluetooth/Technology/Works/Core_Specification_v30.htm
- http://bluetooth.com/NR/rdonlyres/298BE70B-4353-4492-9A91-160549463612/10885/Core_V30__HS.zip