Bluetooth®
SPECIAL INTEREST GROUP

SPECIFICATION OF THE *BLUETOOTH* SYSTEM

Experience More

Bluetooth Core Specification Addendum 2

Adoption Date: 27 December 2011

Addendum 2

This addendum provides an optional update to the Bluetooth® Core Specification. When the addendum is applied to an allowed Core Specification, the following parts of the specification shall be replaced or appended with the revised versions:

Volume 1, Part D:
Mixing of Specification Versions

Volume 2, Part E
Host Controller Interface

Volume 3, Part C
Generic Access Profile

- Limited Discovery Time
- EIR and AD Data Types

Volume 4, Part B
USB

Volume 5, Part A
802.11 PAL

TABLE OF CONTENTS

MIXING OF SPECIFICATION VERSIONS

LIMITED DISCOVERY TIME CHANGES

EIR AND AD DATA TYPES IN GAP CHANGES

AUDIO ARCHITECTURE HCI CHANGES

AUDIO ARCHITECTURE USB CHANGES

802.11 PROTOCOL ADAPTATION LAYER FUNCTIONAL SPECIFICATION

Architecture & Terminology Overview

Part D

MIXING OF SPECIFICATION VERSIONS

CONTENTS

1 MIXING OF SPECIFICATION VERSIONS

This part describes how volumes, and parts within volumes, of different versions of the Core Specification may be mixed in Bluetooth implementations. The Core System consists of a BR/EDR Controller Package (see Volume 2), a Low Energy Controller Package (see Volume 6), a Host Package (see Volume 3) and AMP Protocol Adaptation Layers (see Volume 5).

A Core Specification Addendum contains one or more parts of a single volume or one or more parts in multiple volumes, changes on one or more parts, or a combination of parts and changes. Addend~~ums~~a ~~may be~~are used to supersede a part in a volume or may be used to add a part to a volume according to the rules in Section 1.2.

- All parts within a Primary Controller implementation shall be the same version of Volume 2 and Volume 6, and shall support at least one new Type 1, -2, or -3 feature from Table 1.2.
- All parts within a Host implementation of Volume 3 shall be the same version. An AMP Controller implementation shall contain parts of Volume 2 and Volume 5 from the same version and shall support at least one new Type 3 or Type 4 feature from Table 1.2.
- The Primary Controller, AMP Controller, and Host may be different versions within a single implementation.

In order to describe how these volumes and parts within volumes can be mixed, one needs to distinguish between four categories of features specified in the different specification versions. The four categories are:

Category	**Description**
Type 1	Feature that exists below HCI and cannot be configured/enabled via HCI
Type 2	Feature that exists below HCI and can be configured/enabled via HCI
Type 3	Feature that exists below and above HCI and requires HCI command/events to function
Type 4	Feature that exists only above HCI

Table 1.1: Feature type definitions

The outcome of mixing different core system packages are derived from the feature definitions in the table above:

- If an implementation contains features of type 1 or type 4, these features can function with any combination of Host Package and Controller Package or AMP Protocol Adaptation Layer (PAL) versions.
- If an implementation contains features of type 2, these features can only be used under a default condition if a Host Package of an older version is mixed with a Controller Package or AMP PAL of this version.

- In order to fully use the feature under all conditions, the Host Package, Controller Package, and AMP PAL must be of the same or later version.
- If an implementation contains features of type 3, these features can only function if the Host Package supports this version or a later version and if the Controller Package supports this version or a later version.

See the Bluetooth Brand Book for specification naming requirements.

1.1 FEATURES AND THEIR TYPES

The following table lists the features and their types.

Feature	**Version**	**Type**
Basic AFH operation	1.2	1
Enhanced inquiry	1.2	1
Configuration of AFH (setting channels and enabling/disabling channel assessment)	1.2	2
Enhanced synchronization capability	1.2	2
Interlaced inquiry scan	1.2	2
Interlaced page scan	1.2	2
Broadcast encryption	1.2	2
Enhanced flow specification and flush time-out	1.2	3
Extended SCO links	1.2	3
Inquiry Result with RSSI	1.2	3
L2CAP flow and error control	1.2	4
2 Mbps EDR	2.0 + EDR	2
3 Mbps EDR	2.0 + EDR	2
3 slot packets in EDR	2.0 + EDR	2
5 slot packets in EDR	2.0 + EDR	2
2 Mbps eSCO	2.0 + EDR	2[1]
3 Mbps eSCO	2.0 + EDR	2*[1]
3 slot packets for EDR eSCO	2.0 + EDR	2*[1]
Erroneous Data Reporting	2.1 + EDR	3
Extended Inquiry Response	2.1 + EDR	3
Encryption Pause and Resume	2.1 + EDR	1
Link Supervision Timeout Changed Event	2.1 + EDR	3

Table 1.2: Features and their types

Feature	Version	Type
Non-Flushable Packet Boundary Flag	2.1 + EDR	3
Sniff subrating	2.1+ EDR	3
Secure Simple Pairing	2.1.+ EDR	3
L2CAP Enhanced Retransmission Mode	Addendum 1/ 3.0 + HS	4
L2CAP Streaming Mode	Addendum 1/ 3.0 + HS	4
Enhanced Power Control	3.0 + HS	2
AMP Manager Protocol (A2MP)	3.0 + HS	4
L2CAP Enhancements for AMP	3.0 + HS	4
802.11 PAL	3.0 + HS	3
Generic Test Methodology	3.0 + HS	3
Unicast Connectionless Data	3.0 + HS	4
Low Energy (up through L2CAP)	4.0	3
Attribute Protocol	4.0	4
Generic Attribute Profile	4.0	4
Security Manager	4.0	3
Audio Architecture - HCI Changes	Addendum 2	2
Audio Architecture - USB Changes	Addendum 2	2
Limited Discovery Time	Addendum 2	4
Appearance Data Type	Addendum 2	4
802.11n Enhancements to the 802.11 PAL	Addendum 2	3

Table 1.2: Features and their types

1. The EDR eSCO options are marked as 2* because eSCO requires profile support, but if a product includes the eSCO option from V1.2, then EDR eSCO will be supported without any new support above HCI.

1.2 CORE SPECIFICATION ADDEND~~UMS~~A

~~The following table contains a list of Core Specification Addendums and Core Specification versions they are allowed to be used with.~~

A Core Specification Addendum contains one or more complete Parts and/or Changes of existing or new Parts.

Each part within an addendum is identified by a type indicating whether it may replace a part in an allowed ~~c~~Core ~~s~~Specification version or whether it may add to a package within a ~~c~~Core ~~s~~Specification version.

~~Type~~	~~Description~~
~~Replacement~~	~~The part in the addendum is used instead of the equivalent part in the allowed specification versions.~~
~~Addition~~	~~The Part in the Addendum is used in addition to the existing parts in the allowed specification versions.~~

Each Change may contain changes and/or additions to one or more parts of the Core Specification.

The following table lists adopted addend~~ums~~a and the Core Specification version they are allowed to be used with.

Addendum	Volume and Part or Change Name	Type	Allowed Versions	Mandatory / Optional / Conditional
1	Volume 3, Part A	Replacement	~~1.2,~~ 2.0 + EDR, 2.1 + EDR	O
2	Audio Architecture HCI Changes	Changes	2.1 + EDR, 3.0 + HS, 4.0	O
	Audio Architecture USB Changes	Changes	2.1 + EDR, 3.0 + HS, 4.0	O
	LE Limited Discovery Time Changes	Changes	4.0	C.1
	EIR and AD Data Types in GAP Changes	Changes	4.0	C.1
	EIR and AD Data Types Specification	Addition	4.0	C.1
	Volume 5, Part A	Replacement	3.0 + HS, 4.0	O

Table 1.3: Adopted core specification versions to use with addenda

C.1 Mandatory if either the Host Part of the Low Energy Core Configuration or the Host Part of the Basic Rate and Low Energy Combined Core Configuration is supported, otherwise Excluded.

LIMITED DISCOVERY TIME CHANGES

CONTENTS

1 CHANGE INSTANCES

1.1 CHANGE #1 – VOLUME 3, PART C (GAP), SECTION 13.1.2

A device in general discoverable mode shall follow the requirements for general discoverable mode for BR/EDR as defined in Section 4.1.3 and it shall follow the requirements for general discoverable mode for LE as defined in Section 9.2.4, except it shall not send connectable advertising events.

A device in limited discoverable mode shall follow the requirements for limited discoverable mode for BR/EDR as defined in Section 4.1.2 and it shall follow the requirements for limited discoverable mode for LE as defined in Section 9.2.3, except it shall not send connectable advertising events. The values for T_{gap}(104) and T_{gap}(lim_adv_timeout) shall be the same.

1.2 CHANGE #2 – VOLUME 3, PART C (GAP), SECTION 16, TABLE 16.1

Timer name	Value	Description	Requirement or Recommendation
T_{GAP}(lim_adv_timeout)	~~30.72~~180 s	Maximum time to remain advertising when in the limited discoverable mode	Required value

Table 1.1: Defined GAP timers

EIR AND AD DATA TYPES IN GAP CHANGES

CONTENTS

1 CHANGE INSTANCES

1.1 CHANGE #1 – VOLUME 3, PART C (GAP), SECTION 8

[Change in section 8, 2nd paragraph]

~~The extended inquiry response data types are specified in the Assigned Numbers document.~~The extended inquiry response data formats and meanings are defined in [Core Specification Supplement], Part A. The extended inquiry response data type values are defined in the Assigned Numbers document.

[Change in section 8, 5th paragraph]

The EIR data shall ~~always~~ be sent during inquiry response state. EIR data can contain device name, Tx power level, service class UUIDs, as well as manufacturers data, as defined in ~~Section 8.1~~[Core Specification Supplement], Part A. In selecting the packet type to be used, FEC (DM1 or DM3) should be considered to maximize the range.

[Delete all of sections 8.1 and 8.2 including all subsections]

1.2 CHANGE #2 – VOLUME 3, PART C (GAP), SECTION 9

[Change to section 9.1.1.2, 2nd paragraph]

The advertising data shall be formatted using the Advertising Data (AD) type format as defined in ~~Section 11~~[Core Specification Supplement], Part A, Section 1.3. A device in the broadcast mode shall not set the ‘LE General Discoverable Mode’ flag or the ‘LE Limited Discoverable Mode’ flag in the Flags AD Type as defined in ~~Section 11.1.3~~[Core Specification Supplement], Part A, Section 1.3.

[Change to section 9.2.2.2]

A device in the non-discoverable mode that sends advertising events shall not set the ‘LE General Discoverable Mode’ flag or ‘LE Limited Discoverable Mode’ flag in the Flags AD type (see [Core Specification Supplement], Part A, Section 1.3). A Peripheral device in the non-connectable mode may send non-connectable undirected advertising events or scannable undirected advertising events or may not send advertising packets.

[Change to section 9.2.3.2, starting at 3rd paragraph]

While in the limited discoverable mode the device shall send advertising event types with the advertising data including the Flags AD type as defined in ~~Section 11.1.3~~[Core Specification Supplement], Part A, Section 1.3 with all the following flags set as described:

- The LE Limited Discoverable Mode flag ~~shall be~~ set to one.

- The LE General Discoverable Mode flag ~~shall be~~ set to zero.
- For a~~A~~ device of the LE-only device type with all the following flags set as described:~~,~~
  - ~~shall set~~ T~~t~~he ‘BR/EDR Not Supported’ flag set to one.
  - T~~t~~he ‘Simultaneous LE and BR/EDR to Same Device Capable (Controller)’ flag set to zero~~, and~~.
  - T~~t~~he ‘Simultaneous LE and BR/EDR to Same Device Capable (Host)’ flag set to zero.

The advertising data should also include the following AD types to enable a faster connectivity experience:

- TX Power Level AD type defined in ~~Section 11.1.5~~[Core Specification Supplement], Part A, Section 1.5.
- Local Name AD type defined in ~~Section 11.1.2~~[Core Specification Supplement], Part A, Section 1.2.
- Service UUIDs AD type defined in ~~Section 11.1.1~~[Core Specification Supplement], Part A, Section 1.1. Slave Connection Interval Range AD type as defined in ~~Section 11.1.7~~[Core Specification Supplement], Part A, Section 1.9.

[Change to section 9.2.4.2, starting at 3rd paragraph]

While in general discoverable mode the device shall send advertising events with the advertising data including the Flags AD data type as defined in ~~Section 11.1.3~~[Core Specification Supplement], Part A, Section 1.3 with all the following flags set as described:

- The LE Limited Discoverable Mode flag set to zero.
- The LE General Discoverable Mode flag set to one.
- For a~~A~~ device of the LE-only device type with all the following fields set as described~~,~~:
  - ~~shall set~~ T~~t~~he ‘BR/EDR Not Supported’ flag set to one.
  - T~~t~~he ‘Simultaneous LE and BR/EDR to Same Device Capable (Controller)’ flag set to zero~~, and~~.
  - T~~t~~he ‘Simultaneous LE and BR/EDR to Same Device Capable (Host)’ flag set to zero.

The advertising data should also include the following AD types to enable a faster connectivity experience:

- TX Power Level AD type as defined in ~~Section 11.1.5~~[Core Specification Supplement], Part A, Section 1.5.
- Local Name AD type as defined in ~~Section 2~~[Core Specification Supplement], Part A, Section 1.2.

- Service UUIDs AD type as defined in ~~Section 11.1.1~~[Core Specification Supplement], Part A, Section 1.1**.**
- Slave Connection Interval Range AD type as defined in ~~Section 11.1.7~~[Core Specification Supplement], Part A, Section 1.9.

[Change to section 9.2.5.2, 4th paragraph]

The Host shall check for the Flags AD type in the advertising data. If the Flags AD type is present and the LE Limited Discoverable Flag is set to one then the Host shall consider the device as a discovered device, otherwise the advertising data shall be ignored. The Flag AD type is defined in ~~Section 11.1.3~~ [Core Specification Supplement], Part A, Section 1.3. The advertising data of the discovered device may contain data with other AD types, e.g. Service UUIDs AD type, TX Power Level AD type, Local Name AD type, Slave Connection Interval Range AD type. The Host may use the data in performing any of the connection establishment procedures.

[Change to section 9.2.6.2, 4th paragraph]

The Host shall check for the Flags AD type in the advertising data. If the Flags AD type (see [Core Specification Supplement], Part A, Section 1.3) is present and either the LE General Discoverable Mode flag is set to one or the LE Limited Discoverable Mode flag is set to one then the Host shall consider the device as a discovered device, otherwise the advertising data shall be ignored. The advertising data of the discovered device may contain data with other AD types, e.g. Service UUIDs AD type, TX Power Level AD type, Local Name AD type, Slave Connection Interval Range AD type. The Host may use the data in performing any of the connection establishment procedures as defined in Section 9.3.

1.3 CHANGE #3 – VOLUME 3, PART C (GAP), SECTION 11

[Add new paragraph to end of section 11]

The AD type data formats and meanings are defined in Core Specification Supplement Part A. The AD type identifier values are defined in the Assigned Numbers document.

[Delete all of sections 11.1 and 11.2 including all subsections]

1.4 CHANGE #4 – VOLUME 3, PART C (GAP), SECTION 13

[Change to section 13.1.1.2, list in 4th paragraph]

A device supporting both BR/EDR and LE physical links shall expose the capabilities of both physical links by performing the following steps:

a) The 'LE Supported (Controller)' and 'LE Supported (Host)' bits in the LMP features shall be set as defined in [Vol. 2], Part C Section 3.2.

b) The 'BR/EDR Not Supported' bit in the Flags AD type shall be set to ~~'0'~~zero as defined in ~~Section 18.1~~ [Core Specification Supplement], Part A, Section 1.3.

c) The 'Simultaneous LE and BR/EDR to Same Device Capable (Controller)' and 'Simultaneous LE and BR/EDR to Same Device Capable (Host)' bits in the Flags AD type shall be set to ~~'0'~~zero as defined in ~~Section 18.1~~ [Core Specification Supplement], Part A, Section 1.3.

[Change to section 13.2.3.1, 3rd paragraph]

If the procedure is performed on an LE physical channel:

> If the 'BR/EDR Not Supported' bit in the Flags AD type (see [Core Specification Supplement] Part A, Section 1.3) is set then the device type is LE-only, else the device type is BR/EDR/LE. The device type shall not change while the device is bonded with other devices.

1.5 CHANGE #5 – VOLUME 3, PART C (GAP), SECTION 18

[Delete all of section 18 including all subsections]

AUDIO ARCHITECTURE HCI CHANGES

CONTENTS

1 CHANGE INSTANCES

1.1 VOLUME 2, PART E (HCI)

[Insert the following rows to table 3.10 after Setup Synchronous Connection Command.]

Name	Vers.	Summary description	Supported Controllers
Enhanced Setup Synchronous Connection Command	CSA2	The Enhanced Setup Synchronous Connection command adds a new or modifies an existing synchronous logical transport (SCO or eSCO) on a physical link depending on the Connection_Handle parameter specified.	BR/EDR
Enhanced Accept Synchronous Connection Request Command	CSA2	The Enhanced Accept Synchronous Connection Request command is used to accept an incoming request for a synchronous connection and to inform the local Link Manager about the acceptable parameter values for the synchronous connection.	BR/EDR
Read Local Supported Codecs Command	CSA2	The Read Local Supported Codecs command is used for a host to query a controller’s supported codecs.	BR/EDR

[Add the following row to table 3.19 after the “Encryption Key Refresh Complete Event” row.]

Commands / Events	Group
Enhanced Accept Synchronous Connection Request Command	Synchronous Connections

[Add the following row to table 3.19 after the “Enhanced Flush Complete Event” row.]

Commands / Events	Group
Enhanced Setup Synchronous Connection Command	Synchronous Connections

[Add the following row to table 3.19 after the “Read Local Name Command” row]

Commands / Events	Group
Read Local Supported Codecs Command	Synchronous Connections

[Add the following rows to the table in Section 6.27 in order]

Octet	Bit	Command Supported
29	3	Enhanced Setup Synchronous Connection
29	4	Enhanced Accept Synchronous Connection
29	5	Read Local Supported Codecs

[NEW SECTION] 7.1.45 HCI Enhanced Setup Synchronous Connection Command

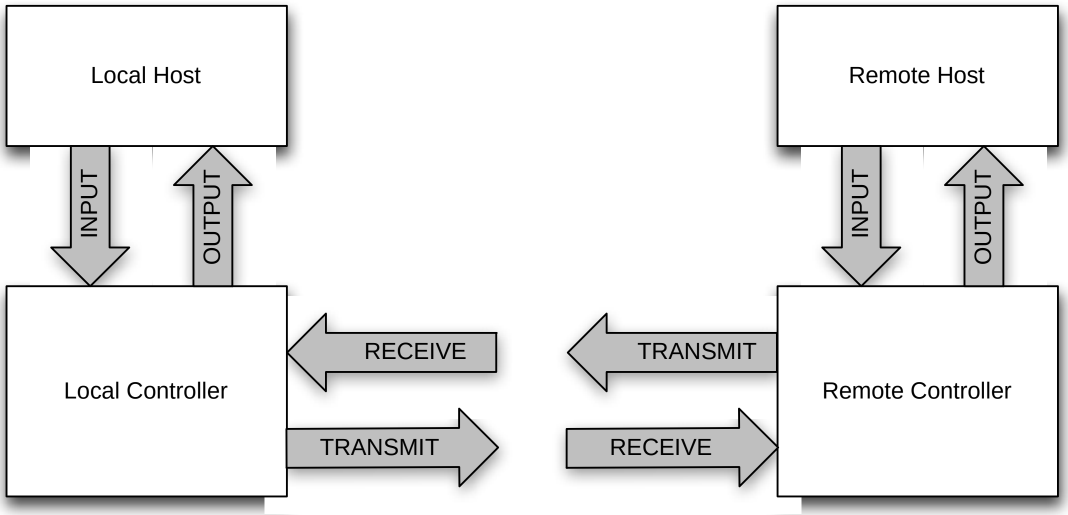
Command	OCF	Command Parameters	Return Parameters
HCI_Enhanced_Setup_Synchronous_Connection	0x003D	Connection_Handle, Transmit_Bandwidth, Receive_Bandwidth, Transmit_Coding_Format, Receive_Coding_Format, Transmit_Codec_Frame_Size, Receive_Codec_Frame_Size, Input_Bandwidth, Output_Bandwidth, Input_Coding_Format, Output_Coding_Format, Input_Coded_Data_Size, Output_Coded_Data_Size, Input_PCM_Data_Format, Output_PCM_Data_Format, Input_PCM_Sample_Payload_MSB_Position, Output_PCM_Sample_Payload_MSB_Position, Input_Data_Path, Output_Data_Path, Input_Transport_Unit_Size, Output_Transport_Unit_Size, Max_Latency, Packet_Type, Retransmission_Effort	

Description:

The Enhanced_Setup_Synchronous_Connection command adds a new, or modifies an existing, synchronous logical transport (SCO or eSCO) on a physical link depending on the Connection_Handle parameter specified. If the Connection_Handle refers to an ACL link, then a new synchronous logical transport shall be added. If the Connection_Handle refers to an existing synchronous logical transport (eSCO only), then this link shall be modified. The parameters are specified per connection. This synchronous connection can be used to transfer synchronous voice data or transparent synchronous data.

When used to setup a new synchronous logical transport, the Connection_Handle parameter shall specify an ACL connection with which the new synchronous connection shall be associated. The other parameters relate to the negotiation of the link, and may be reconfigured during the lifetime of the link.

The following terms are used to describe the four different audio paths: Transmit, Receive, Input and Output. The Transmit and Receive paths are from the perspective of the local Controller's radio. The Input and Output paths are from the perspective of the Controller.



The following parameters are used to describe the transmit and receive paths over the air:

- The Transmit_Bandwidth and Receive_Bandwidth parameters specify how much bandwidth shall be available for transmitting and for receiving data. The Host shall set the Transmit_Bandwidth and Receive_Bandwidth parameters to be equal or shall set one of them to be zero and the other non-zero.
- The Transmit_Coding_Format and Receive_Coding_Format parameters specify the coding format used for transmitted or received data. The Host shall set the Transmit_Coding_Format and Receive_Coding_Formats to be equal. Note: When the Transmit_Coding_Format and Receive_Coding_Format parameters are not equal to CVSD, A-law or u-law, the Link Manager shall map these to Transparent air mode.
- The Transmit_Codec_Frame_Size and Receive_Codec_Frame_Size parameters specify the frame size produced by the codecs in the context of over-the-air coding. The over-the-air packet size should have the following relationship with the codec frame size:

  Packet_Size = Frame_Size * N, or

  Packet_Size = Frame_Size / N

  where N is an integer.

The following parameters are used to describe the coding format used prior to encapsulating over the audio data transport path:

- The Input_Bandwidth and Output_Bandwidth specify the nominal rate at which the Host or Controller transfers data. Note: For HCI transports this excludes the HCI header. The Host shall either set the Input_Data_Rate and Output_Data_Rate to be equal, or shall set one of them to be zero and the other non-zero.
- The Input_Coding_Format and Output_Coding_Format parameters specify the coding format used over the transport. The Host shall set the Input_Coding_Format and Output_Coding_Format to be equal.
- The Input_Coded_Data_Size and Output_Coded_Data_Size specify the number of bits in each sample or frame of data. For CVSD, a frame of data shall be 8 bits.
- The Input_PCM_Data_Format and Output_PCM_Data_Format parameters specify the data format over the transport for linear samples. It is ignored when the data is encoded in any other way.
- The Input_PCM_Sample_Payload_MSB_Position and Output_PCM_Sample_Payload_MSB_Position parameters indicate, for linear samples, how many bit positions that the MSB of the sample is away from starting at the MSB of the data. It is ignored when the data is encoded in any other way. For example, if Input_Coded_Data_Size =16 and Input_PCM_Sample_Payload_MSB_Position = 3, then each sample is actually only 13 bits, the MSB (which is the sign bit for signed formats) is bit 12 (counting from the LSB at bit 0), and the contents of bits 13, 14, and 15 of each sample are ignored.

The following parameters describe the audio data transport path characteristics:

- The Input_Data_Path and Output_Data_Path parameters specify the audio data transport path. When set to 0x00, the audio data path shall be over the HCI transport. When set to 0xFF, audio test mode (see Vol 2, Part E, Section 7.6.2) is selected. Note: This is only applicable during test mode. When set to 0x01-0xFE, the audio data path shall use non-HCI transport data paths (e.g. PCM interface) with logical transport channel numbers. The meanings of these logical transport channel numbers are vendor specific.
- The Input_Transport_Unit_Size and Output_Transport_Unit_Size indicate how many bits are in each unit of data delivered by the audio data transport. Except for HCI, the meaning of “unit” depends on the host transport used and, therefore, is vendor specific (for example, on a PCM transport this should indicate the number of bits transported per sync pulse, and would normally be 8 or 16). The Host shall set the Input_Transport_Unit_Size and Output_Transport_Unit_Size to be equal. For HCI host transport the Host shall set them to 0.

The following parameters are used by the Link Manager to negotiate the synchronous transport:

- The Max_Latency parameter specifies an upper limit to the time in milliseconds between the eSCO (or SCO) instants, plus the size of the retransmission window, plus the length of the reserved synchronous slots for this logical transport.

- The Packet_Type parameter is a bitmap specifying which synchronous packet types may be used by the Link Manager in the negotiation of the link parameters. Multiple packet types are specified by bitwise OR of the packet type codes in the table. At least one packet type shall be specified for each negotiation. It is recommended to enable as many packet types as possible. Note: It is allowed to enable packet types that are not supported by the local device.
- The Retransmission_Effort parameter specifies the extra resources that are allocated to this connection if a packet may need to be retransmitted. The Retransmission_Effort parameter shall be set to indicate the required behavior, or to “Don’t care”.

The following restrictions shall apply:

- Either both the Transmit_Coding_Format and Input_Coding_Format shall be “transparent” or neither shall be. If both are “transparent”, the Transmit_Bandwidth and the Input_Bandwidth shall be the same and the controller shall not modify the data sent to the remote device.
- Either both the Receive_Coding_Format and Output_Coding_Format shall be “transparent” or neither shall be. If both are “transparent”, the Receive_Bandwidth and the Output_Bandwidth shall be the same and the Controller shall not modify the data sent to the Host.

A Connection_Handle for the new synchronous connection will be returned in the Synchronous Connection Complete event if the command is used to set up a new synchronous connection.

When used to modify an existing synchronous logical transport, only the Packet_Type, Retransmission_Effort and Max_Latency parameters may be modified.

Note: The Link Manager may choose any combination of packet types, timing, and retransmission window sizes that satisfy the parameters given. This may be achieved by using more frequent transmissions of smaller packets. The link manager may choose to set up either a SCO or an eSCO connection, if the parameters allow, using the corresponding LMP sequences.

Note: To modify a SCO connection, use the Change_Connection_Packet_Type command.

Note: If the lower layers cannot achieve the exact transmit and receive bandwidth requested subject to the other parameters, or cannot achieve the transcoding or resampling implied by the parameters, then the link creation or link modification shall be rejected. A synchronous connection may only be created when an ACL connection already exists and when it is not in Park state.

The data at the audio data transport interface shall be treated as a stream of bits. The bits in each unit of data delivered by the transport shall be taken LSB first, and the units shall be taken in the order of delivery. The samples, encoded samples, frames, or other entity to be transcoded for transmission, or that has been transcoded after reception, shall be taken in the order of transmission or reception, with each entity taken LSB first.

For example, if the audio data transport uses 16 bit units and the Input or Output coding format is A-law, each unit represents two samples with the first in the 8 least significant bits and the second in the 8 most significant bits. Similarly, if the audio data transport uses 8 bit units and the Input or Output coding format is linear PCM with a size of 16 bits, the 8 least significant bits of each sample are transmitted first.

Command Parameters:

Connection_Handle: *Size: 2 Octets (12 bits meaningful)*

Value	Parameter Description
0xXXXX	Connection Handle to be used to identify a connection. Range: 0x0000 – 0x0EFF (0x0F00 – 0x0FFF Reserved for future use)

Transmit_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0x00000000 – 0xFFFFFFFE	Transmit bandwidth in octets per second.
0xFFFFFFFF	Don’t care

Receive_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0x00000000 – 0xFFFFFFFE	Receive bandwidth in octets per second.
0xFFFFFFFF	Don’t care

Transmit_Coding_Format: *Size: 5 Octets*

Value	Parameter Description
Octet 0	See Assigned Numbers for Coding_Format
Octets 1-4	Octet 1-2: Company ID, see Assigned Numbers for Company Identifier. Octet 3-4: Vendor specific codec ID. Shall be ignored if octet 0 of Transmit_Coding_Format is not 0xFF.

Receive_Coding_Format: *Size: 5 Octets*

Value	Parameter Description
Octet 0	See Assigned Numbers for Coding_Format
Octets 1-4	Octet 1-2: Company ID, see Assigned Numbers for Company Identifier. Octet 3-4: Vendor specific codec ID. Shall be ignored if octet 0 of Receive_Coding_Format is not 0xFF.

Transmit_Codec_Frame_Size: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	Range: 0x0001-0xFFFF, the actual size of the over-the-air encoded frame in octets.
0x0000	Reserved

Receive_Codec_Frame_Size: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	Range: 0x0001-0xFFFF, the actual size of the over-the-air encoded frame in octets.
0x0000	Reserved

Input_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	Host to Controller nominal data rate in octets per second.

Output_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	Controller to Host nominal data rate in octets per second.

Input_Coding_Format: *Size: 5 Octets*

Value	Parameter Description
Octet 0	See Assigned Numbers for Coding_Format
Octets 1-4	Octet 1-2: Company ID, see Assigned Numbers for Company Identifier. Octet 3-4: Vendor specific codec ID. Shall be ignored if octet 0 of Input_Coding_Format is not 0xFF.

Output_Coding_Format: *Size: 5 Octets*

Value	Parameter Description
Octet 0	See Assigned Numbers for Coding_Format
Octets 1-4	Octet 1-2: Company ID, see Assigned Numbers for Company Identifier. Octet 3-4: Vendor specific codec ID. Shall be ignored if octet 0 of Output_Coding_Format is not 0xFF.

Input_Coded_Data_Size: Size: 2 Octets

Value	Parameter Description
0xXXXX	Size, in bits, of the sample or framed data

Output_Coded_Data_Size: Size: 2 Octets

Value	Parameter Description
0xXXXX	Size, in bits, of the sample or framed data

Input_PCM_Data_Format: Size: 1 Octet

Value	Parameter Description
0xXX	See Assigned Numbers for PCM_Data_Format

Output_PCM_Data_Format: Size: 1 Octet

Value	Parameter Description
0xXX	See Assigned Numbers for PCM_Data_Format

Input_PCM_Sample_Payload_MSB_Position: Size: 1 Octet

Value	Parameter Description
0xXX	The number of bit positions within an audio sample that the MSB of the sample is away from starting at the MSB of the data.

Output_PCM_Sample_Payload_MSB_Position: Size: 1 Octet

Value	Parameter Description
0xXX	The number of bit positions within an audio sample that the MSB of the sample is away from starting at the MSB of the data.

Input_Data_Path: Size: 1 Octet

Value	Parameter Description
0x00	HCI

Value	Parameter Description
0x01-0xFE	Logical_Channel_Number. The meaning of the logical channels will be vendor specific.
0xFF	Audio test mode

Output_Data_Path: *Size: 1 Octet*

Value	Parameter Description
0x00	HCI
0x01-0xFE	Logical_Channel_Number. The meaning of the logical channels will be vendor specific.
0xFF	Audio test mode

Input_Transport_Unit_Size: *Size: 1 Octet*

Value	Parameter Description
1 to 255	The number of bits in each unit of data received from the Host over the audio data transport.
0	Not applicable (implied by the choice of audio data transport)

Output_Transport_Unit_Size: *Size: 1 Octet*

Value	Parameter Description
1 to 255	The number of bits in each unit of data sent to the Host over the audio data transport.
0	Not applicable (implied by the choice of audio data transport)

Max_Latency: *Size: 2 Octets*

Value	Parameter Description
0x0000 – 0x0003	Reserved
0x0004 – 0xFFFE	The value in milliseconds representing the upper limit of the sum of the synchronous interval, and the size of the eSCO window, where the eSCO window is the reserved slots plus the retransmission window. (See Figure 8.7 in the Baseband specification)
0xFFFF	Don’t care.

Packet_Type: *Size: 2 Octets*

Value	Parameter Description
0x0001	HV1 may be used
0x0002	HV2 may be used

Value	Parameter Description
0x0004	HV3 may be used
0x0008	EV3 may be used
0x0010	EV4 may be used
0x0020	EV5 may be used
0x0040	2-EV3 shall not be used
0x0080	3-EV3 shall not be used
0x0100	2-EV5 shall not be used
0x0200	3-EV5 shall not be used
0x0400	Reserved for future use
0x0800	Reserved for future use
0x1000	Reserved for future use
0x2000	Reserved for future use
0x4000	Reserved for future use
0x8000	Reserved for future use

Note: 0x003F means all packet types may be used.

Retransmission_Effort: *Size: 1 Octet*

Value	Parameter Description
0x00	No retransmission
0x01	At least one retransmission, optimize for power consumption
0x02	At least one retransmission, optimize for link quality
0x03-0xFE	Reserved
0xFF	Don't care

Return Parameters:

None.

Event(s) generated (unless masked away):

When the BR/EDR Controller receives the Enhanced_Setup_Synchronous_Connection command, it shall send the Command Status event to the Host. In addition, when the LM determines that the connection is established, the local BR/EDR Controller shall send a Synchronous Connection Complete event to the local Host, and the remote Controller will send a Synchronous Connection Complete event or a Connection Complete event to the remote Host. The Synchronous Connection Complete event contains the Connection_Handle if this command is successful.

This command cannot be used to change the parameters of an SCO link.

Note: No Command Complete event will be sent by the local BR/EDR Controller to indicate that this command has been completed. Instead, the Synchronous Connection Complete event (for a new connection setup) or Synchronous Connection Changed event (for modifying an existing synchronous link) will indicate that this command has been completed.

[NEW SECTION] 7.1.46 HCI Enhanced Accept Synchronous Connection Request Command

Command	OCF	Command Parameters	Return Paramters
HCI Enhanced Accept Synchronous Connection Request	0x003E	BD_ADDR, Transmit_Bandwidth, Receive_Bandwidth, Transmit_Coding_Format, Receive_Coding_Format, Transmit_Codec_Frame_Size, Receive_Codec_Frame_Size, Input_Bandwidth, Output_Bandwidth, Input_Coding_Format, Output_Coding_Format, Input_Coded_Data_Size, Output_Coded_Data_Size, Input_PCM_Data_Format, Output_PCM_Data_Format, Input_PCM_Sample_Payload_MSB_Position, Output_PCM_Sample_Payload_MSB_Position, Input_Data_Path, Output_Data_Path, Input_Transport_Unit_Size, Output_Transport_Unit_Size, Max_Latency, Packet_Type, Retransmission_Effort	

Description:

The Enhanced_Accept_Synchronous_Connection_Request command is used to accept an incoming request for a synchronous connection and to present the local Link Manager with the acceptable parameter values for the synchronous connection. This command shall only be issued after a Connection_Request event, with link type SCO or eSCO, has occurred. A Connection_Request event contains the BD_ADDR of the device requesting the connection. The command to accept a connection must be received by the Controller before the connection accept timeout expires on the local device.

The parameter set of the Enhanced_Accept_Synchronous_Connection_Request command is the same as for the Enhanced_Setup_Synchronous_Connection command except for the Connection_Handle in the Enhanced_Setup_Synchronous_Connection command, which is replaced by the BD_ADDR in the Enhanced_Accept_Synchronous_Connection_Request command. Please refer to 7.1.45 for their descriptions.

If the Link Type of the incoming request is SCO, then the Retransmission Effort parameter shall be ignored.

If the Connection_Request event is masked away, the BR/EDR Controller will automatically reject it. A Controller shall not be configured to auto accept a synchronous connection.

Command Parameters:

BD_ADDR: *Size: 6 Octets*

Value	Parameter Description
0xXXXXXXXXXXXX	BD_ADDR of the device requesting the connection

Transmit_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0x00000000 – 0xFFFFFFFE	Transmit bandwidth in octets per second.
0xFFFFFFFF	Don't care

Receive_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0x00000000 – 0xFFFFFFFE	Receive bandwidth in octets per second.
0xFFFFFFFF	Don't care

Transmit_Coding_Format: *Size: 5 Octets*

Value	Parameter Description
Octet 0	See Assigned Numbers for Coding_Format
Octets 1-4	Octet 1-2: Company ID, see Assigned Numbers for Company Identifier. Octet 3-4: Vendor specific codec ID. Shall be ignored if octet 0 of Transmit_Coding_Format is not 0xFF.

Receive_Coding_Format: *Size: 5 Octets*

Value	Parameter Description
Octet 0	See Assigned Numbers for Coding_Format

Value	Parameter Description
Octets 1-4	Octet 1-2: Company ID, see Assigned Numbers for Company Identifier. Octet 3-4: Vendor specific codec ID. Shall be ignored if octet 0 of Receive_Coding_Format is not 0xFF.

Transmit_Codec_Frame_Size: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	Range: 0x0001-0xFFFF, the actual size of the over-the-air encoded frame in octets.
0x0000	Reserved

Receive_Codec_Frame_Size: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	Range: 0x0001-0xFFFF, the actual size of the over-the-air encoded frame in octets.
0x0000	Reserved

Input_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	Host to Controller nominal data rate in octets per second.

Output_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	Controller to Host nominal data rate in octets per second.

Input_Coding_Format: *Size: 5 Octets*

Value	Parameter Description
Octet 0	See Assigned Numbers for Coding_Format
Octets 1-4	Octet 1-2: Company ID, see Assigned Numbers for Company Identifier. Octet 3-4: Vendor specific codec ID. Shall be ignored if octet 0 of Input_Coding_Format is not 0xFF.

Output_Coding_Format: *Size: 5 Octets*

Value	Parameter Description
Octet 0	See Assigned Numbers for Coding_Format

Value	Parameter Description
Octets 1-4	Octet 1-2: Company ID, see Assigned Numbers for Company Identifier. Octet 3-4: Vendor specific codec ID. Shall be ignored if octet 0 of Output_Coding_Format is not 0xFF.

Input_Coded_Data_Size: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	Size, in bits, of the sample or framed data

Output_Coded_Data_Size: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	Size, in bits, of the sample or framed data

Input_PCM_Data_Format: *Size: 1 Octet*

Value	Parameter Description
0xXX	See Assigned Numbers for PCM_Data_Format

Output_PCM_Data_Format: *Size: 1 Octet*

Value	Parameter Description
0xXX	See Assigned Numbers for PCM_Data_Format

Input_PCM_Sample_Payload_MSB_Position: *Size: 1 Octet*

Value	Parameter Description
0xXX	The number of bit positions within an audio sample that the MSB of the sample is away from starting at the MSB of the data.

Output_PCM_Sample_Payload_MSB_Position: *Size: 1 Octet*

Value	Parameter Description
0xXX	The number of bit positions within an audio sample that the MSB of the sample is away from starting at the MSB of the data.

Input_Data_Path: *Size: 1 Octet*

Value	Parameter Description
0x00	HCI
0x01-0xFE	Logical_Channel_Number. The meaning of the logical channels will be vendor specific.

Value	Parameter Description
0xFF	Audio test mode

Output_Data_Path: *Size: 1 Octet*

Value	Parameter Description
0x00	HCI
0x01-0xFE	Logical_Channel_Number. The meaning of the logical channels will be vendor specific.
0xFF	Audio test mode

Input_Transport_Unit_Size: *Size: 1 Octet*

Value	Parameter Description
1 to 255	The number of bits in each unit of data received from the Host over the audio data transport.
0	Not applicable (implied by the choice of audio data transport)

Output_Transport_Unit_Size: *Size: 1 Octet*

Value	Parameter Description
1 to 255	The number of bits in each unit of data sent to the Host over the audio data transport.
0	Not applicable (implied by the choice of audio data transport)

Max_Latency: *Size: 2 Octets*

Value	Parameter Description
0x0000 – 0x0003	Reserved
0x0004 – 0xFFFE	The value in milliseconds representing the upper limit of the sum of the synchronous interval, and the size of the eSCO window, where the eSCO window is the reserved slots plus the retransmission window. (See Figure 8.7 in the Baseband specification)
0xFFFF	Don’t care.

Packet_Type: *Size: 2 Octets*

Value	Parameter Description
0x0001	HV1 may be used
0x0002	HV2 may be used
0x0004	HV3 may be used
0x0008	EV3 may be used

Value	Parameter Description
0x0010	EV4 may be used
0x0020	EV5 may be used
0x0040	2-EV3 shall not be used
0x0080	3-EV3 shall not be used
0x0100	2-EV5 shall not be used
0x0200	3-EV5 shall not be used
0x0400	Reserved for future use
0x0800	Reserved for future use
0x1000	Reserved for future use
0x2000	Reserved for future use
0x4000	Reserved for future use
0x8000	Reserved for future use

Note: 0x003F means all packet types may be used.

Retransmission_Effort: *Size: 1 Octet*

Value	Parameter Description
0x00	No retransmission
0x01	At least one retransmission, optimize for power consumption
0x02	At least one retransmission, optimize for link quality
0x03-0xFE	Reserved
0xFF	Don’t care

Return Parameters:

None.

Event(s) generated (unless masked away):

The Enhanced_Accept_Synchronous_Request command requests the local BR/EDR Controller to start setting up the connection. When this action commences, the Command Status event shall be sent by the BR/EDR Controller. When the link setup is complete, the BR/EDR Controller shall send a Synchronous Connection Complete event to its Host, and the remote BR/EDR Controller will send a Connection Complete event, or a Synchronous Connection Complete event, to its Host. The Synchronous Connection Complete will contain the Connection_Handle and the link parameters if the setup is successful.

Note: No Command Complete event will be sent by the local Controller as the result of this command. Instead, the Synchronous Connection Complete or Connection Complete event will indicate that this command has been completed.

[NEW SECTION] 7.4.8 HCI Read Local Supported Codecs Command

Command	OCF	Command Parameters	Return Parameters
HCI_Read_Local_Supported_Codecs	0x000B		Status, Number_of_Supported_Codecs, Supported_Codecs[i], Number_of_Supported_Vendor_Specific_Codecs, Vendor_Specific_Codecs[i]

Description:

This command reads a list of the Bluetooth SIG approved codecs supported by the Controller, as well as vendor specific codecs, which are defined by an individual manufacturer.

Command Parameters:

None.

Return Parameters:

Status: *Size: 1 Octet*

Value	Parameter Description
0x00	Read_Local_Supported_Codecs command succeeded.
0x01 – 0xFF	Read_Local_Supported_Codecs command failed. See Part D, Error Codes on page TBD for a list of error codes and descriptions.

Number_of_Supported_Codecs: *Size: 1 Octet*

Value	Parameter Description
0xXX	Total number of codecs supported

Supported_Codecs[i]: *Size : 1 * Number_of_Supported_Codecs Octets*

Value	Parameter Description
0xXX, 0xXX, …	An array of codec identifiers. Assigned Numbers for Codec_Type

Number_of_Supported_Vendor_Specific_Codecs: *Size: 1 Octet*

Value	Parameter Description
0xXX	Total number of vendor specific codecs supported

Vendor_Specific_Codecs[i]:Size: 4
*Number_of_Supported_Vendor_Specific_Codecs**

Value	Parameter Description
0xXXXXXXXX	Octets 0 and 1: Company ID, see Assigned Numbers for Company Identifier Octets 2 and 3: Vendor defined codec ID

Event(s) generated (unless masked away):

When the Read_Local_Supported_Codecs command has completed, a Command Complete event shall be generated.

[UPDATED SECTION] 7.7.35 Synchronous Connection Complete Event

Event	Event	Command Parameters
Synchronous Connection Complete	0x2C	Status, Connection Handle, BD_ADDR, Link Type, Transmit Interval, Retransmission Window, Rx_Packet_Length Tx_Packet_Length Air Mode

Description:

~~The Synchronous Connection Complete event indicates to both the Hosts that a new synchronous connection has been established. This event also indicates to the Host which issued the Setup_Synchronous_Connection, or Accept_Synchronous_Connection_Request or Reject_Synchronous_Connection_Request command and then received a Command Status event, if the issued command failed or was successful.~~

The Synchronous Connection Complete event is sent to indicate completion of any of the following commands:

- Setup_Synchronous_Connection
- Accept_Synchronous_Connection_Request
- Reject_Synchronous_Connection_Request
- Enhanced_Setup_Synchronous_Connection
- Enhanced_Accept_Synchronous_Connection_Request

This event returns the completion status for the command.

When the Synchronous Connection Complete event was triggered by the Enhanced_Setup_Synchronous_Connection or Enhanced_Accept_Synchronous_Connection_Request commands, the Controller shall set the Air Mode parameter to the Transmit Air Coding Format parameter of the original command.

[The rest of the text stays the same]

1.2 VOLUME 2, PART F (MESSAGE SEQUENCE CHARTS)

[NEW SECTION] 5.2 SYNCHRONOUS CONNECTION SETUP WITH ENHANCED SYNCHRONOUS COMMANDS

Using the HCI_Enhanced_Setup_Synchronous_Connection command, a Host can add a synchronous logical channel to the link. A synchronous logical link can be provided by creating a SCO or an eSCO logical transport.

Note: An ACL Connection must be established before a synchronous connection can be created.

Step 1a: Master device requests a synchronous connection with a slave device.

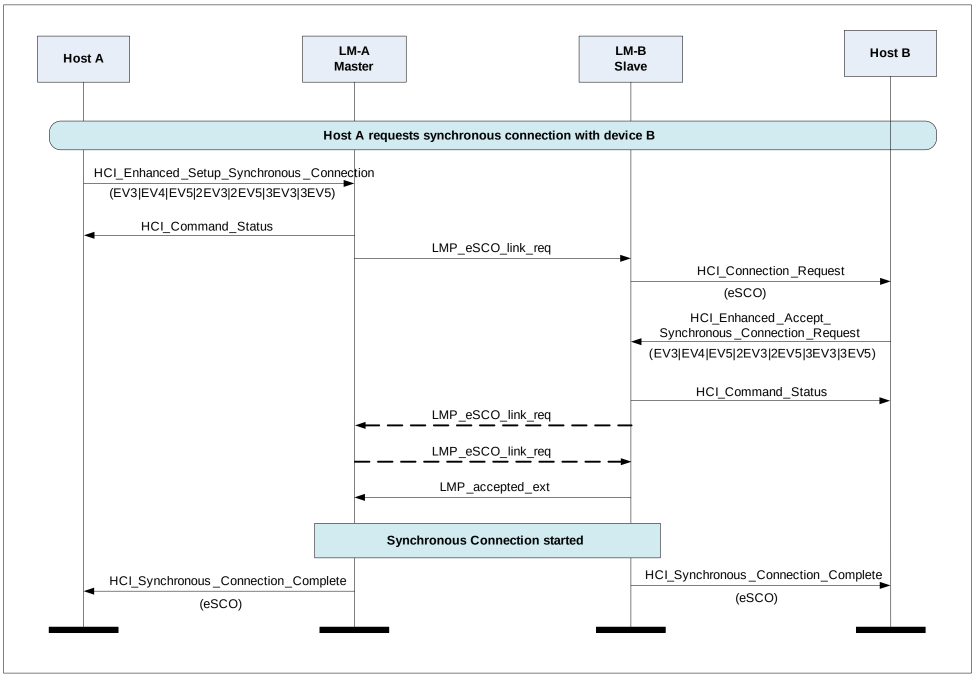

Host A
LM-A Master
LM-B Slave
Host B
Host A requests synchronous connection with device B
HCI_Enhanced_Setup_Synchronous_Connection
(EV3|EV4|EV5|2EV3|2EV5|3EV3|3EV5)
HCI_Command_Status
LMP_eSCO_link_req
HCI_Connection_Request
(eSCO)
HCI_Enhanced_Accept_ Synchronous_Connection_Request
(EV3|EV4|EV5|2EV3|2EV5|3EV3|3EV5)
HCI_Command_Status
LMP_eSCO_link_req
LMP_eSCO_link_req
LMP_accepted_ext
Synchronous Connection started
HCI_Synchronous_Connection_Complete
(eSCO)
HCI_Synchronous_Connection_Complete
(eSCO)

Figure 5.10: Master requests synchronous connection (EV3, EV4, EV5, 2-EV3, 2-EV5, 3-EV3, or 3-EV5)

Step 1b: Slave device requests a synchronous connection with a master device.

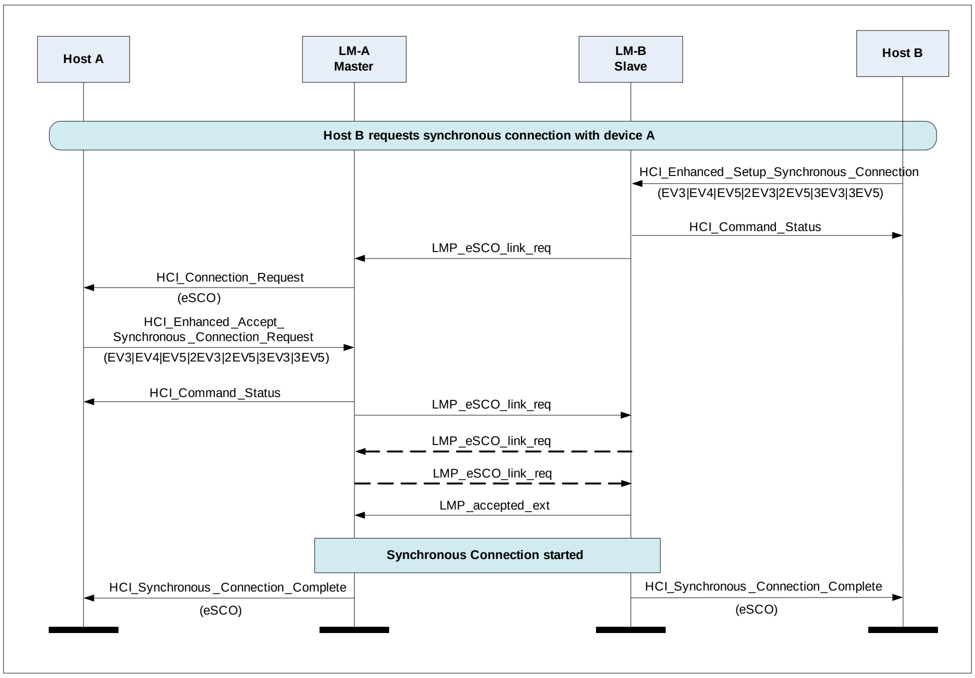

Host A
LM-A Master
LM-B Slave
Host B
Host B requests synchronous connection with device A
HCI_Enhanced_Setup_Synchronous_Connection
(EV3|EV4|EV5|2EV3|2EV5|3EV3|3EV5)
HCI_Command_Status
LMP_eSCO_link_req
HCI_Connection_Request
(eSCO)
HCI_Enhanced_Accept_Synchronous_Connection_Request
(EV3|EV4|EV5|2EV3|2EV5|3EV3|3EV5)
HCI_Command_Status
LMP_eSCO_link_req
LMP_eSCO_link_req
LMP_eSCO_link_req
LMP_accepted_ext
Synchronous Connection started
HCI_Synchronous_Connection_Complete
(eSCO)
HCI_Synchronous_Connection_Complete
(eSCO)

Figure 5.11: Slave requests synchronous connection (EV3, EV4, EV5, 2-EV3, 2-EV5, 3-EV3, or 3-EV5)

Step 1c: Master device requests a SCO connection with a slave device.

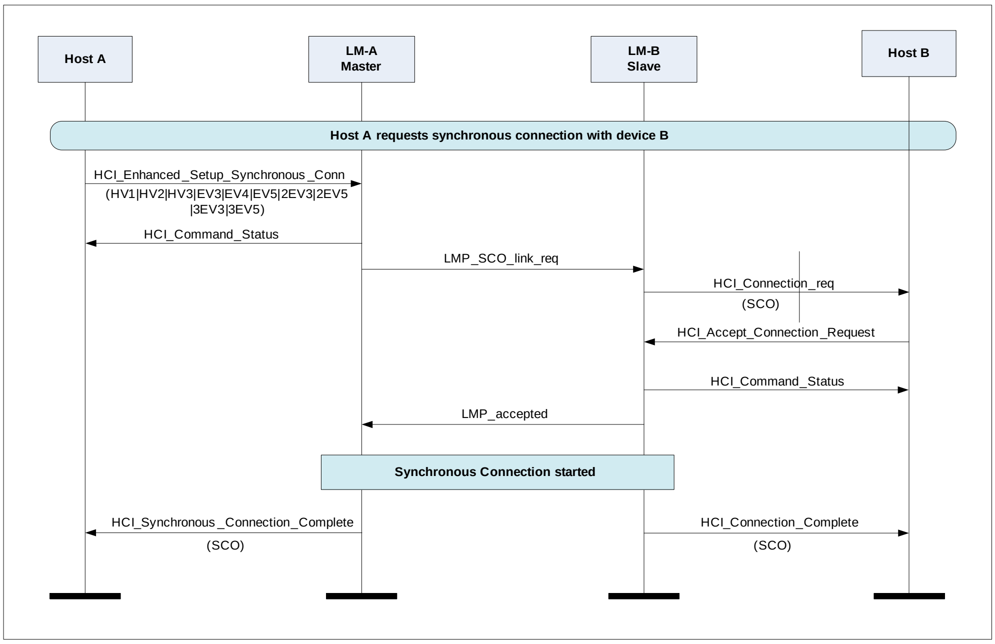

Host A
LM-A Master
LM-B Slave
Host B
Host A requests synchronous connection with device B
HCI_Enhanced_Setup_Synchronous_Conn
(HV1|HV2|HV3|EV3|EV4|EV5|2EV3|2EV5
|3EV3|3EV5)
HCI_Command_Status
LMP_SCO_link_req
HCI_Connection_req
(SCO)
HCI_Accept_Connection_Request
HCI_Command_Status
LMP_accepted
Synchronous Connection started
HCI_Synchronous_Connection_Complete
(SCO)
HCI_Connection_Complete
(SCO)

Figure 5.12: Master requests synchronous connection (HV1, HV2, or HV3)

Step 1d: Slave device requests a SCO connection with a master device.

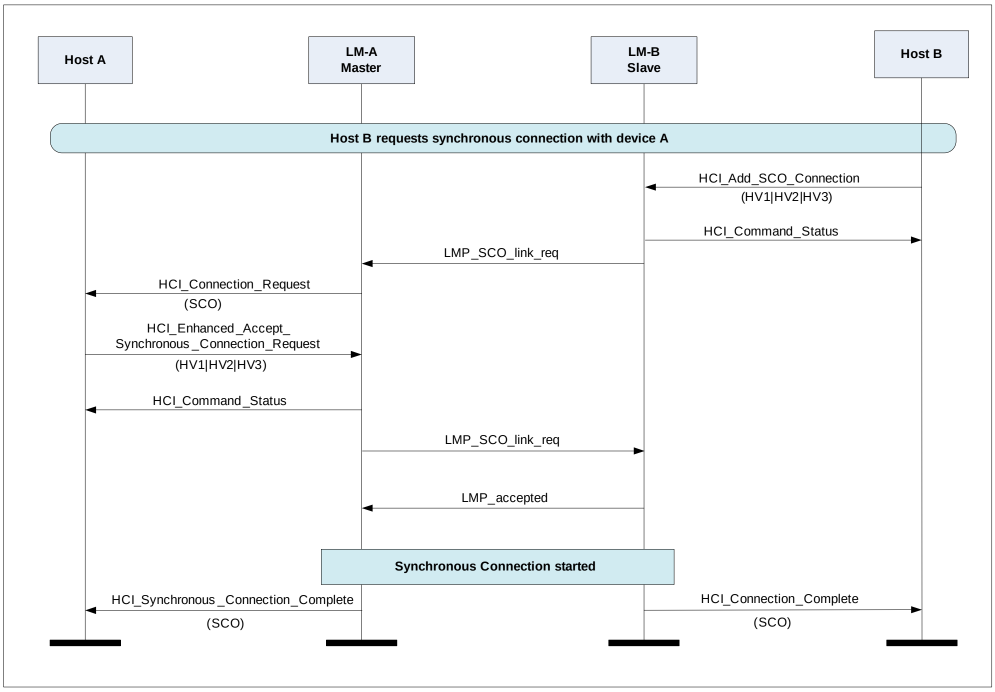

Host A
LM-A Master
LM-B Slave
Host B
Host B requests synchronous connection with device A
HCI_Add_SCO_Connection (HV1|HV2|HV3)
HCI_Command_Status
LMP_SCO_link_req
HCI_Connection_Request (SCO)
HCI_Enhanced_Accept_ Synchronous_Connection_Request (HV1|HV2|HV3)
HCI_Command_Status
LMP_SCO_link_req
LMP_accepted
Synchronous Connection started
HCI_Synchronous_Connection_Complete (SCO)
HCI_Connection_Complete (SCO)

Figure 5.13: Slave requests synchronous connection (HV1, HV2, or HV3)

Step 2a: Master renegotiates eSCO connection.

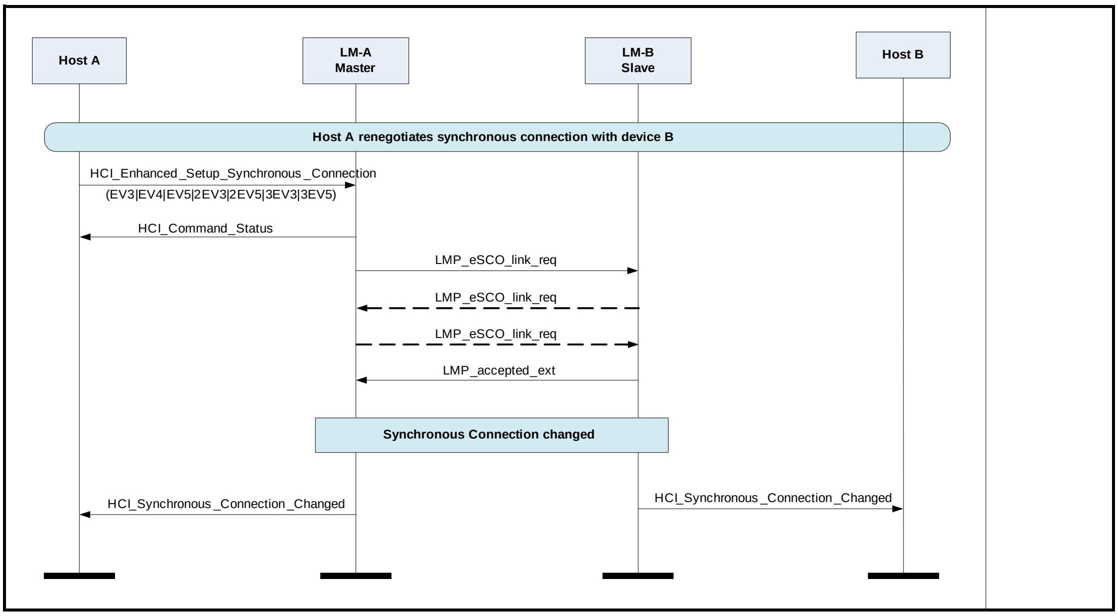

Host A
LM-A Master
LM-B Slave
Host B
Host A renegotiates synchronous connection with device B
HCI_Enhanced_Setup_Synchronous_Connection (EV3|EV4|EV5|2EV3|2EV5|3EV3|3EV5)
HCI_Command_Status
LMP_eSCO_link_req
LMP_eSCO_link_req
LMP_eSCO_link_req
LMP_accepted_ext
Synchronous Connection changed
HCI_Synchronous_Connection_Changed
HCI_Synchronous_Connection_Changed

Figure 5.14: Master renegotiates synchronous connection parameter change

Step 2b: Slave renegotiates eSCO connection.

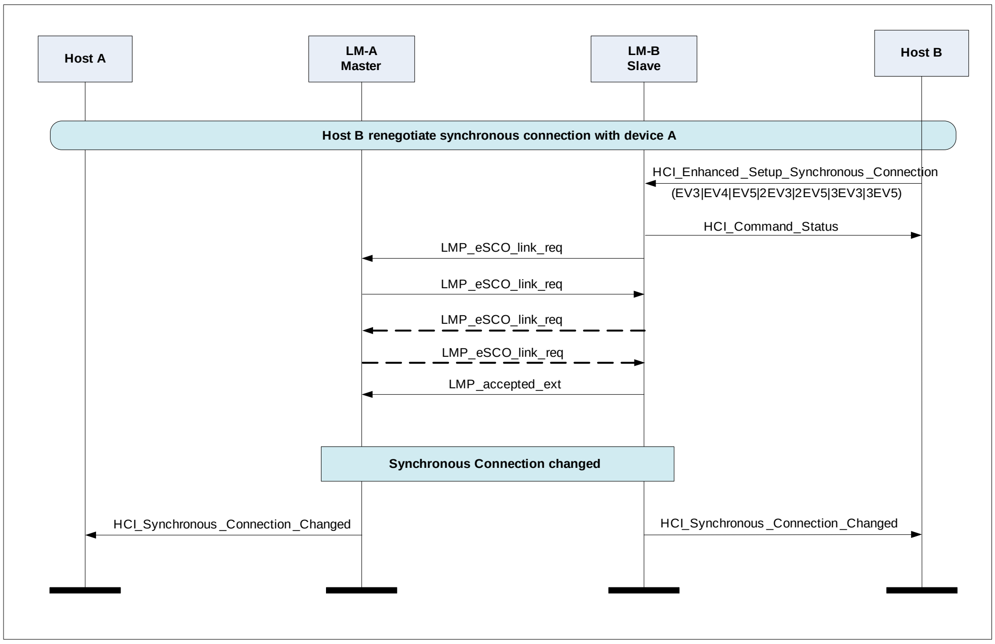

Host A
LM-A Master
LM-B Slave
Host B
Host B renegotiate synchronous connection with device A
HCI_Enhanced_Setup_Synchronous_Connection (EV3|EV4|EV5|2EV3|2EV5|3EV3|3EV5)
HCI_Command_Status
LMP_eSCO_link_req
LMP_eSCO_link_req
LMP_eSCO_link_req
LMP_eSCO_link_req
LMP_accepted_ext
Synchronous Connection changed
HCI_Synchronous_Connection_Changed
HCI_Synchronous_Connection_Changed

Figure 5.15: Slave renegotiates synchronous connection parameter change

AUDIO ARCHITECTURE USB CHANGES

CONTENTS

1 CHANGE INSTANCES

1.1 CHANGE #1 - VOLUME 4, PART B (USB), SECTION 2.1.1

The Primary Controller configuration consists of two interfaces. The first interface has no alternate settings and contains the bulk and interrupt endpoints. The second interface provides scalable isochronous bandwidth. The recommended configuration for the second interface has four alternate settings that provide different bandwidth. The default interface is empty so that the device is capable of scaling down to zero isochronous bandwidth.

An HCI packet consisting of an HCI header and HCI data shall be contained in one USB Transfer. A USB transfer is defined by the USB specification as one or more USB transactions that contain the data from one IO request. For example, an ACL data packet containing 256 bytes (both HCI header and HCI data) would be sent over the bulk endpoint in one IO request. That IO request will require four 64-byte full speed USB Transactions or a single 256-byte High-speed USB Transaction, and forms a Transfer. If the Maximum Packet Size for the endpoint on which the transfer is sent is 64 bytes, then that IO request will require four 64-byte USB transactions.

The endpoints are spread across two interfaces so that when adjusting isochronous bandwidth consumption (via select interface calls), any pending bulk and/or interrupt transactions do not have to be terminated or resubmitted.

Table 1.1 and the following example calculations illustrate recommended endpoint descriptor parameter values and how they are derived. The maximum packet sizes for control endpoints, interrupt endpoints and bulk endpoints may be any value allowed by the relevant USB core specifications. The maximum packet size for isochronous endpoints must be large enough to accommodate the maximum average traffic; they may be set to accommodate the largest HCI transfer, subject to the capabilities of the controller. In Table 1.1, the service interval is assumed to be 1 millisecond, for USB Full Speed (FS) frames.

Examples:

1. For a single 8 kHz audio channel with of 64 kbps CVSD audio the host may break HCI data into one USB transfers for each USB frame (e.g. 1 ms); in that case, the max packet size must be at least 11 = 3 octet HCI header + 8 octets of data. To reduce HCI header overhead, a common strategy (see Table 2.2) is to consolidate 3 ms of data into a 27 octet HCI packet of 24 octets of data + 3 octets of HCI header. These HCI packets can be exchanged as a single USB transfer on 3 ms intervals; this requires a max packet size of 27/3 = 9 octets per 1 millisecond USB Full Speed Frame.
2. For two 8 kHz audio channels of 64 kbps CVSD audio the host may double the payload size of each HCI packet, which would be 3 octets HCI header + 48 octets of data = 51 octets. Posting these at 3 ms intervals requires 51/3 = 17 octets of maximum packet size.

3. For one 16 kHz audio channel the HCI packets need to be large enough to accommodate single octet (128 kbps) or 2-octet (256 kbps) encoding. On 3 ms intervals, these would have to be (48+3)/3 = 17 octets or (96+3)/3 = 33 octets respectively.
4. For one mSBC compressed wideband audio channel the HCI packets will be 3 octets of HCI header + 60 octets of data. If the Controller can support a maximum packet size of 63 (or 64) octets, an entire mSBC frame may be exchanged in one USB transaction. If the maximum packet size is smaller than 63 octets, additional latency will be introduced. The USB Host Controller will reserve bandwidth that will only be used when the Bluetooth Host or Controller has data to transfer.
5. For combinations of audio channels, if the max packet size can accommodate the largest HCI packets, there is also sufficient bandwidth for the audio channels that have smaller HCI packets. See example 4 above.

The following table outlines ~~the~~a recommended configuration for a USB Full Speed device.

Interface Number	Alternate Setting	Suggested Endpoint Address	Endpoint Type	Suggested Max Packet Size	USB Polling Interval/HCI Packet Interval
HCI Commands					
N/A	N/A	0x00	Control	8/16/32/64	NA
HCI Events					
0	0	0x81	Interrupt (IN)	16	variable
ACL Data					
0	0	0x82	Bulk (IN)	32/64	variable
0	0	0x02	Bulk (OUT)	32/64	variable
No active voice channels (for USB compliance)					
1	0	0x83	Isoch (IN)	0	NA
1	0	0x03	Isoch (OUT)	0	NA
One 8 kHz voice channel with 8-bit encoding					
1	1	0x83	Isoch (IN)	9	1 ms/3 ms
1	1	0x03	Isoch (OUT)	9	1 ms/3 ms

Table 1.1: USB Primary firmware interface and endpoint settings

Interface Number	Alternate Setting	Suggested Endpoint Address	Endpoint Type	Suggested Max Packet Size	USB Polling Interval/HCI Packet Interval
Two 8 kHz voice channels with 8-bit encoding or one 8 kHz voice channel with 16-bit encoding					
1	2	0x83	Isoch (IN)	17	1 ms/3 ms
1	2	0x03	Isoch (OUT)	17	1 ms/3ms
Three 8 kHz voice channels with 8-bit encoding					
1	3	0x83	Isoch (IN)	25	1 ms/3ms
1	3	0x03	Isoch (OUT)	25	1 ms/3ms
Two 8 kHz voice channels with 16-bit encoding or one 16 kHz voice channel with 16-bit encoding					
1	4	0x83	Isoch (IN)	33	1 ms/3 ms
1	4	0x03	Isoch (OUT)	33	1 ms/3 ms
Three 8 kHz voice channels with 16-bit encoding or one 8 kHz voice channel with 16-bit encoding and one 16 kHz voice channel with 16-bit encoding					
1	5	0x83	Isoch (IN)	49	1 ms/3 ms
1	5	0x03	Isoch (OUT)	49	1 ms/3 ms
One mSBC voice channel					
1	6	0x83	Isoch (IN)	63	1 ms/7.5 ms
1	6	0x03	Isoch (OUT)	63	1 ms/7.5 ms

Table 1.1: USB Primary firmware interface and endpoint settings

802.11 PROTOCOL ADAPTATION LAYER FUNCTIONAL SPECIFICATION

This document specifies the Protocol Adaptation Layer for the IEEE 802.11 conformant Alternate MAC/PHY.

TABLE OF CONTENTS

1 INTRODUCTION

This Part of the Bluetooth Core Specification describes the operation of the Protocol Adaptation Layer (PAL) for a controller incorporating an 802.11 device compliant with the 2007 edition of the IEEE 802.11 Standard (see [1]) including support for High Throughput (HT) MAC and PHY extensions. In this Part, specific references in [1] will be given by clause number.

The 802.11 PAL defines the protocol state machines, data encapsulation methods, event triggers, and data structures in support of the use of an 802.11 AMP.

1.1 ORGANIZATION OF THE 802.11 PAL

To aid understanding of functional descriptions, Figure 1.1 shows the organization of the 802.11 PAL. This structure is informative.

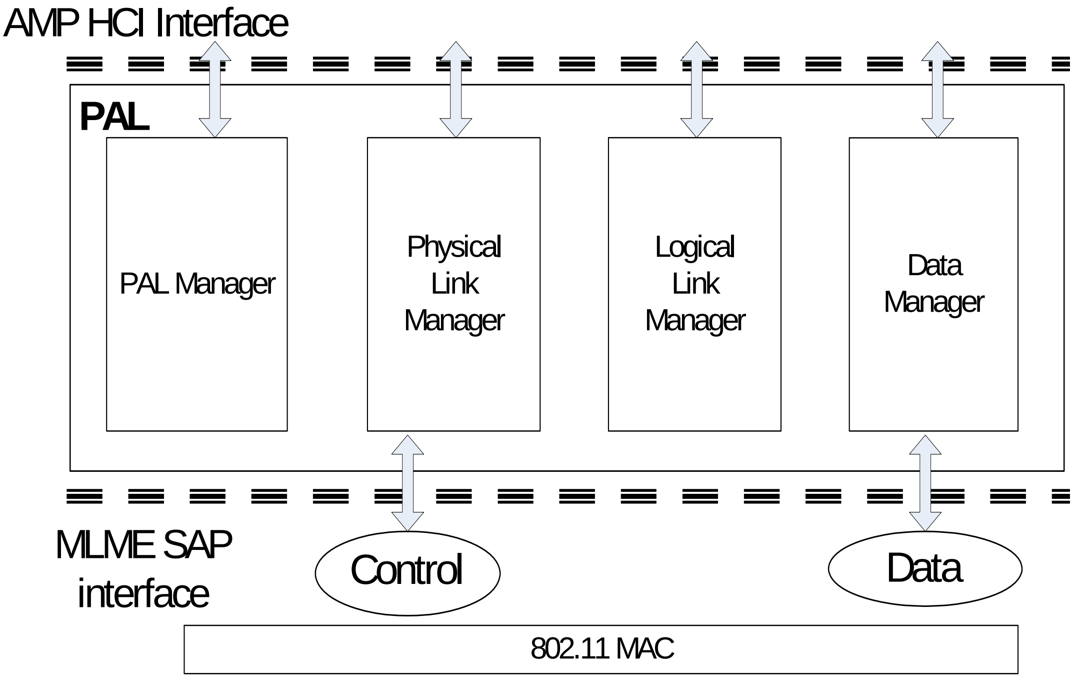


Figure 1.1: Internal structure of the 802.11 PAL

The upper edge of the 802.11 PAL provides a single instance of the logical HCI with AMP functionality. The behavior of the PAL is defined at this interface in terms of logical HCI operations. Implementations may optionally use a physical HCI transport.

For clarity of description, the lower edge of the PAL uses services including those defined in [1] clause 10.3.

The PAL Manager implements operations that are global to the PAL. This includes responding to host requests for AMP info and PAL version as well as performing PAL reset.

The Physical Link Manager implements operations on physical links. Physical link semantics are defined in Section 3. Supported operations include physical link creation and acceptance, and deletion of physical links. Supported operations at the MAC interface include PHY channel selection and security establishment and maintenance.

The Logical Link Manager implements operations on logical links. Logical link semantics are defined in Section 4. Each logical link exists with respect to a single physical link. Supported operations include creation and deletion of logical links and changes to QoS parameters for those logical links. At the MAC interface this includes the mapping of extended flow specifications to user priorities.

The Data Manager performs operations on data packets and is described in Section 5. Each data packet is associated with exactly one extended flow specification and therefore exactly one logical link. Supported operations include transmit, receive and buffer management operations such as flush events. At the MAC interface this includes interactions with the MAC transmit and receive operations and determination of the next packet to send on any particular link.

2 AMP HOST CONTROLLER INTERFACE

A number of elements used in HCI commands and events are defined to be AMP-type specific. This section describes the values to be used for the 802.11 PAL.

Octet ordering conventions for parameters and fields in this section shall be as defined in HCI, [Vol 2] Part E, Section 5.2.

2.1 READ LOCAL VERSION INFORMATION COMMAND

Two return parameter values from this HCI command are defined to be AMP-type specific. For the 802.11 PAL they shall be as follows.

PAL _Version *Size: 1 Octet*

Value	Parameter Description
0xXX	Version of the current PAL in the Controller. See Bluetooth Assigned Numbers.

PAL_Sub-version: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	In an 802.11 PAL this value is vendor specific.

2.2 READ LOCAL AMP INFO COMMAND

See [Vol 2] Part E, Section 7.5.7.

There are six return parameters for the Read Local AMP Info command which are 802.11 AMP specific.

Total_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	An upper bound on the total data rate that can be achieved by the AMP for applications. It accounts for the total bandwidth provided by the HCI transport. No sustained combination of transmit and receive operations shall exceed this value. This may be used to help in AMP selection and admission control. Expressed in kbps. For testing purposes, the achievable throughput deliverable to applications by an ERP or OFDM PHY shall be assumed to be no more than 30000 kbps and for the HT PHY shall be assumed to be no more than 50000 kbps.

Max_Guaranteed_Bandwidth: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	An upper bound on the maximum data rate as seen by the application that the AMP can guarantee for a logical channel. Any request made by an application above this level would be rejected. It accounts for any bandwidth limitations of the HCI transport. No sustained combination of transmit and receive operations shall exceed this value. This can be used to help in AMP selection and admission control. Expressed in kbps. The Max_Guaranteed_Bandwidth parameter value returned shall be no greater than the Total_Bandwidth parameter. This value is not a guarantee of bandwidth and should be interpreted as an upper bound on the sum of the bandwidths of all active flow specs.

Min_Latency: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	The Min_Latency parameter value is the practical lower bound on the service latency that can be provided by the 802.11 AMP. The lower bound of the service latency is the time from when a frame is issued to the AMP HCI until the MAC starts transmitting the frame with no contention window back off. This shall be equal to the AMP HCI minimum latency + DIFS + CWmin where the DIFS and CWmin are as given in [1] clause 9.2.10.

Max_PDU_Size: *Size: 4 Octets*

Value	Parameter Description
	An upper bound on the size of L2CAP PDU which may be provided for transmission or reception on this AMP. The Host shall not require the AMP to transport L2CAP PDUs larger than this value. Expressed in octets. The Maximum PDU Size parameter described in [[Vol 3] Part A, Section 5.4] for any connection over this AMP should not exceed this value. The Max_PDU_Size parameter returned shall be Max80211PALPDUSize.

Controller_Type: *Size: 1 Octet*

Value	Parameter Description
0x01	802.11 AMP

PAL_Capabilities: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	Bit 0: "Service Type = Guaranteed" is not supported by PAL = 0 "Service Type = Guaranteed" is supported by PAL = 1 Bits 15-1: Reserved (See L2CAP, [Vol 3] Part A, Section 5.6)

Bit 0 of the PAL_Capabilities parameter shall be set to 1 if the local 802.11 AMP device is capable of using the Enhanced Distributed Channel Access (EDCA) mechanisms (see [1] clause 9.9.1), otherwise it shall be set to 0.

AMP_ASSOC_Length: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	AMP_ASSOC maximum length for this AMP Controller.

The 802.11 PAL shall set this to Max80211AMPASSOCLen.

Max_Flush_Timeout: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	Maximum time period, in microseconds, which the AMP device may use to attempt to transmit a frame on a guaranteed logical link. This value is the sum of the durations of all 802.11 transmission attempts for a given frame. It should be chosen with the expectation that the 802.11 MAC may be denied access to the medium for a given transmission attempt. This may be due to interference from collocated radios, or otherwise. If the Controller is configured to retry frames for an unbounded time (there is no flushing at all), then the PAL shall set this value to 0xFFFFFFFF.

Best_Effort_Flush_Timeout: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	The typical time period, in microseconds, which the AMP device may use to attempt to transmit a frame on a best effort logical link. This value is the sum of the duration of all 802.11 transmission attempts for a given frame. It should be chosen with the expectation that the 802.11 MAC is usually able to access the medium for each attempt. The value shall not exceed the value given in Max_Flush_Timeout. If the Controller is configured to retry frames for an unbounded time (i.e. there is no flushing at all), then the PAL shall set this value to 0xFFFFFFFF.

2.3 RESET COMMAND

See [Vol 2] Part E, Section 7.3.2.

In addition to setting the HCI parameters to their default values, when the 802.11 PAL receives an AMP HCI_Reset command it shall ~~destroy~~delete all existing AMP physical links. ~~Informative n~~Note: Non AMP links should not be destroyed.

2.4 READ FAILED CONTACT COUNTER COMMAND

When the 802.11 PAL receives an HCI Read_Failed_Contact_Counter command it shall return the number of consecutive incidents in which the remote device didn't respond after the flush timeout had expired, and the L2CAP packet that was currently being transmitted was automatically flushed. The Failed Contact Counter is specific to each logical link.

2.5 READ LINK QUALITY COMMAND

See [Vol 2] Part E, Section 7.5.3.

The meaning of the Link_Quality parameter in the Read Link Quality command is as shown below.

Link_Quality: *Size: 1 Octet*

Value	Parameter Description
0xXX	In an 802.11 AMP this unsigned 8-bit value shall be the Link Quality Indicator value. It shall be 0 if the Link Quality Indicator value is not available. Range: 0x00 ≤ N ≤ 0xFF

2.6 READ RSSI COMMAND

See [Vol 2] Part E, Section 7.5.4.

The meaning of the RSSI parameter in the Read RSSI command is as shown below.

RSSI: *Size: 1 Octet*

Value	Parameter Description
0xXX	This value is a signed 8-bit value, and is interpreted as an indication of arriving signal strength at the antenna measured in dBm. The value shall be 0x81 (-127 dBm) if the signal strength indication is not available.

2.7 SHORT RANGE MODE COMMAND

When the Host determines that the AMP peers may have insufficient separation to obtain full AMP throughput, it may enable Short Range Mode in the PAL. The Short Range Mode command may be used by the Host to indicate to the PAL whether or not to operate in Short Range Mode.

When in Short Range Mode, the PAL shall limit to ShortRangeModePowerMax the transmit power in dBm (measured at the antenna) for all 802.11 AMP ERP-OFDM frames transmitted by the device on the given physical link, as necessary to prevent exceeding the maximum input signal level of the peer. If the Host does not enable Short Range Mode or if the Host sets Short Range Mode to disabled, the PAL shall assume it may set the maximum transmit power for the link as it deems appropriate, respecting regulatory limits. If the AMP device is not able to limit its transmit power due to other ~~extant~~existing connections then it may use a transmit power greater than ShortRangeModePowerMax in order to preserve those connections.

The meaning of the Short Range Mode parameter of the HCI_Short_Range_Mode command is as follows:

Short Range Mode: *Size: 1 Octet*

Value	Parameter Description
0xXX	0x00–Short range mode shall be disabled in the PAL (default) 0x01–Short range mode shall be enabled in the PAL. 0x02...0xFF - Reserved

When the AMP controller receives the Short_Range_Mode command, it shall indicate a Command Status event. Later, after the MAC programming is completed, the controller shall generate a Short_Range_Mode_Change_Completed event. See Section 2.13.

2.8 WRITE BEST EFFORT FLUSH TIMEOUT COMMAND

Best_Effort_Flush_Timeout: *Size: 4 Octets*

Value	Parameter Description
0xXXXXXXXX	0x00000000–0xFFFFFFFE: Best Effort Flush Timeout value in microseconds. 0xFFFFFFFF: No Best Effort Flush Timeout used. (default)

2.9 READ BEST EFFORT FLUSH TIMEOUT COMMAND

Best_Effort_Flush_Timeout: *Size: 4 Octets*

Value	**Parameter Description**
0xXXXXXXXX	0x00000000–0xFFFFFFFE: Best Effort Flush Timeout value in microseconds. 0xFFFFFFFF: No Best Effort Flush Timeout used (default)

2.10 PHYSICAL LINK LOSS EARLY WARNING EVENT

Implementation of this event is not required for 802.11 AMPs.

2.11 PHYSICAL LINK RECOVERY EVENT

Implementation of this event is not required for 802.11 AMPs.

2.12 CHANNEL SELECTED EVENT

See [Vol 2] Part E, Section 7.7.52.

When an HCI Channel Selected event is indicated by the PAL with successful status, it signifies the local 802.11 MAC has been configured to start operating on the selected channel.

Subsequent to the HCI Channel Selected event, the initiating AMP device shall create an AMP_ASSOC containing its MAC address TLV, ~~the 802.11 PAL capabilities,~~ and with only the selected channel in ~~its preferred channel list~~its PCL and/or PCLv2 TLV (see sections 2.14.4 and 2.14.7). Other TLVs may optionally be included. The host may obtain this AMP_ASSOC by issuing one or more HCI_Read_Local_AMP_ASSOC commands.

2.13 SHORT RANGE MODE CHANGE COMPLETED EVENT

See [Vol 2] Part E, Section 7.7.60.

After the PAL is notified of a change of state in Short Range Mode, it shall program the 802.11 device accordingly, unless the exceptions in Section 2.7 are in effect. When it has finished making such changes to the MAC configuration, or if the PAL has changed the state of the Short Range Mode autonomously, the PAL shall indicate this to the Host by indicating the Short_Range_Mode_Change_Event. The Short_Range_State parameter identifies the new configuration to the Host.

2.14 DATA STRUCTURES

2.14.1 AMP_ASSOC Structure

The AMP_ASSOC is an AMP type specific structure and appears in various HCI commands and events. The AMP_ASSOC structure used by the 802.11 PAL shall be composed of Type-Length-Value (TLV) triplets.

The general format of such a TLV, shown in Table 2.1, shall be a one-octet TypeID field, a two-octet Length field, and a variable length Value field. The length of the Value field in octets shall be exactly equal to the unsigned number represented by the Length field. A TLV with zero in its Length field shall contain no Value field. If an implementation does not have support for a triplet in a received AMP_ASSOC, it shall ignore the triplet and continue processing any remaining triplets.

The Length field is 2 octets in length and shall be ordered in the AMP_ASSOC according to Volume 2, [Part B] Section 6.2 on page 109. The Value field shall be interpreted as a stream of octets.

The TypeID of 0xFF shall be reserved for use in debugging.

TypeID	Length	Value
1 octet	2 octets	Variable number of octets

Table 2.1: TLV format

The set of defined TypeIDs is given in Table 2.2.

TypeID codepoint	Description	AMP_ASSOC inclusion
0x00	Reserved	NA
0x01	MAC ~~a~~Address	Mandatory
0x02	Preferred ~~c~~Channel List	Mandatory for Responder; Mandatory for Initiator if last HCI Write Remote AMP Assoc command did not include a PCLv2 (typeID 0x06), else Optional
0x03	Connected ~~c~~Channel List	Optional
0x04	802.11 PAL Capabilities List	Optional
0x05	802.11 PAL version	Mandatory
0x06	Preferred Channel List v2	Optional if PCL (typeID 0x02) is included in AMP_Assoc, else Mandatory
0x0~~6~~7 - 0xFE	Reserved	NA

TypeID codepoint	Description	AMP_ASSOC inclusion
0xFF	Reserved for use in debugging	NA

Table 2.2: ~~TypeIDs used for 802.11 AMP TLVs~~Requirements on contents of AMP_Assoc messages

2.14.2 MAC Address

The PAL shall use the following ~~format~~TLV to report the IEEE MAC address of its local 802.11 MAC. The bit ordering of the address is given in [1] clause 7.1.1.

MAC_Address_TypeID: *Size: 1 Octet*

Value	Parameter Description
0x01	MAC A~~a~~ddress TypeID

MAC_Address_Length: *Size: 2 Octets*

Value	Parameter Description
0x0006	MAC ~~a~~Address Length

MAC_Address_Specifier: *Size: 6 Octets*

Value	Parameter Description
0xXXXXXXXXXXXX	MAC A~~a~~ddress specifier

2.14.3 802.11 PAL Capabilities

The 802.11 PAL Capabilities is a bit field of supported capabilities of the sending device.

802.11_PAL_Capabilities_TypeID: *Size: 1 Octet*

Value	Parameter Description
0x04	802.11 PAL Capabilities TypeID

802.11_PAL_Capabilities_Length: *Size: 2 Octets*

Value	Parameter Description
0x0004	802.11 PAL Capabilities Length

802.11_PAL_Capabilities_Specifier: *Size: 4 Octets*

Bit format	Parameter Description
Bit 0	When set, signifies PAL capable of utilizing received Activity Reports

Bit format	**Parameter Description**
Bit 1	When set, signifies PAL is capable of utilizing scheduling information received in an Activity Report
Bit 2	HT Capability bit. When set, signifies 802.11 MAC and PHY is compliant with HT operation as specified in [1].
Bits ~~2~~3..31	Reserved

The 802.11 PAL Capabilities TLV is optional to include in the AMP_ASSOC. If an 802.11 PAL Capabilities TLV does not appear in an AMP_ASSOC, then the receiver shall interpret this as receiving an 802.11 PAL Capabilities TLV with a Value field containing the default value of all zeros.

2.14.4 Preferred Channel List

The Preferred Channel List (PCL) is a ~~non-empty list~~set of channels supported and usable by the ~~PAL~~sending device. The receiver of the ~~Preferred Channel List~~PCL shall interpret the contents of the list with the assumption that the list is arranged in order of most preferred channel to least preferred channel. The format of the list is identical to the 802.11 Country information element, excluding the 802.11 information, element identifier, length, and pad fields. See [1] clause 7.3.2.9.

Preferred Channel List TypeID: *Size: 1 Octet*

Value	**Parameter Description**
0x02	Preferred Channel List TypeID

Preferred_Channel_List_Length: *Size: 2 Octets*

Value	**Parameter Description**
0xXXXX	Length of Preferred Channel List

Preferred_Channel_List_Specifier: *Size: Variable*

Value	**Parameter Description**
0xXX..XX	List of preferred 802.11 channels. See Section 3.2.3 for details.

The channels are described by table entries in [1], Annex J, tables J-1, J-2, and J-3. For backward compatibility, the Preferred Channel List Specifier shall use table indices in the inclusive range [1-12] to describe US channels, [1-4] to describe EU country channels, and [1-32] to describe Japan channels.

2.14.5 Connected Channel List

The Connected Channel List (CCL) specifies the channels which may currently be in use by the sending device. If multiple channels are listed, the ordering gives no implied preference. The format of the list is the same as the ~~802.11 Country information element, without the element identifier, length, and pad fields. See [1] clause 7.3.2.9~~ PCL, see section 2.14.4.

The Connected Channel TLV is optional to include in the AMP_ASSOC. If it is not included, then the receiver shall assume there are no channels which are currently in use by the sending device.

Connected_Channel_List_TypeID: *Size: 1 Octet*

Value	**Parameter Description**
0x03	Connected Channel List TypeID

Connected_Channel_List_Length: *Size: 2 Octets*

Value	**Parameter Description**
0xXXXX	Length of Connected Channel List

Connected_Channel_List_Specifier: *Size: Variable*

Value	**Parameter Description**
0xXXXXXXXX	List of 802.11 channels currently in use by the sending device. See Section 3.2.3 for details.

For backward compatibility, the Connected Channel List Specifier shall use table indices in the inclusive range [1-12] to describe US channels, [1-4] to describe EU country channels, and [1-32] to describe Japan channels.

2.14.6 802.11 PAL Version

An AMP endpoint may need to discover the version of the remote PAL. The information in the 802.11 PAL Version TLV shall be composed of the PAL_Version from the HCI_Read_Local_Version_Information command, the Bluetooth SIG Company Identifier (see Assigned Numbers, [4]) for the provider of the PAL, and the PAL_Sub-version from the HCI_Read_Local_Version_Information command. The Company Identifier and PAL Sub-version parameters shall use the octet ordering as given in Volume 2, [Part B] Section 6.2 on page 109.

802.11_PAL_Version_TypeID: *Size: 1 Octet*

Value	Parameter Description
0x05	802.11 PAL Version TypeID

802.11_PAL_Version_Length: *Size: 2 Octets*

Value	Parameter Description
0x0005	Length of 802.11 PAL Version specifier

802.11_PAL_Version_Specifier: *Size: 1 Octet*

Value	Parameter Description
0xXX	PAL Version

802.11_PAL_Company_Identifier: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	SIG Company identifier of 802.11 PAL vendor

802.11_PAL_Sub_Version: *Size: 2 Octets*

Value	Parameter Description
0xXXXX	PAL Sub-version specifier

2.14.7 Preferred Channel List v2

The Preferred Channel List v2 (PCLv2) TLV specifies the channels supported and usable by the sending device. The format of the list is identical to the 802.11 Country information element syntax, excluding the 802.11 infor-mation element identifier, length, country string and pad fields. See [1] clause 7.3.2.9. The receiver of a PCLv2 TLV shall interpret the contents of the list with the assumption that the list is arranged in order of most preferred channel to least preferred channel.

The PCLv2 may include channels with 20 MHz width, 40 MHz width, or both. Channels are expressed as triplets of two types: the operating type contains a table index from Table 3.7 below, and the sub-band type contains a channel range. The PCLv2 shall contain at least one operating triplet. Country strings are not used in the PCLv2, so the operating triplet appears directly following the TLV length field. Sub-band triplets may be used to refine the list of channels expressed by the preceding operating triplet.

If a PCLv2 TLV is not included in the AMP Get AMP Assoc Request message from a responder, then the initiating PAL shall assume the responder may not have the ability to interpret PCLv2 TLVs. In this case the initiator shall include a PCL in the AMP_Assoc in the AMP Create Physical Link Request, and the PCLv2 TLV is optional. If an implementation supports PCLv2 TLVs and if it receives a PCLv2 from its peer, then it shall ignore any PCL it receives.

Preferred_Channel_Listv2_TypeID: *Size: 1 Octet*

Value	**Parameter Description**
0x06	Preferred Channel List v2 TypeID

Preferred_Channel_Listv2_Length: *Size: 2 Octets*

Value	**Parameter Description**
0xXXXX	Length of Preferred Channel Listv2.

Preferred_Channel_Listv2_Specifier: *Size: Variable*

Value	**Parameter Description**
0xXXXXXXXX	List of preferred channels, including 40 MHz channels if supported. See Section 3.2.3 for details.

2.15 CONNECTION ACCEPT TIMEOUT CONFIGURATION PARAMETER

See [Vol 2] Part E, Section 6.7.

The default value of the Connection Accept Timeout used by the 802.11 PAL shall be 5 seconds.

2.16 ENABLE DEVICE UNDER TEST MODE

If the device under test supports 40 MHz channels, the HCI Enable Device Under Test Mode command (see Vol 2, Part E, section 7.6.3) change the state of the PAL so that it will always utilize 40 MHz channel widths for connections if 40 MHz operation is supported by the AMP peer.

When an HCI Read Local AMP Assoc is issued following this command, the AMP ASSOC which is returned shall include at least one channel which is 40 MHz in width in the PCLv2 (see above). When an HCI Write Remote AMP

Assoc is issued following this command, and if the AMP ASSOC included in that Write Remote AMP ASSOC command contains 40 MHz channels, then the selected channel shall be a 40 MHz channel.

When the host issues the HCI Enable Device Under Test Mode command, the PAL shall advertise or choose 40 MHz channels, depending on its role. When serving as the Initiator, the PAL shall choose one of the 40 MHz channels offered by the Responder. When serving as the Responder, the PAL shall offer at least one 40 MHz channel in its PCLv2.

The described effect of the HCI Enable Device Under Test Mode is removed when the Host issues an HCI Reset command.

3 PHYSICAL LINK MANAGER

A physical link joins an initiating device and a responding device. The initiating device is the device on which the HCI_Create_Physical_Link command was issued. The responding device is the one on which the HCI_Accept_Physical_Link command was issued. Physical link creation collisions are resolved at a higher level, by the AMP Manager.

Support for the 802.11 ERP (see clause 19 of [1]) shall be mandatory for 802.11 AMP devices, but other PHY types may be supported. Channels 1 (2412 MHz) through 11 (2462 MHz) shall be supported for interoperability.

A physical link represents a transport between a single local 802.11 AMP device and a single remote device with a matching 802.11 AMP. The AMP may support multiple physical links (representing different remote devices) at one time. There is a unique binding between the 802.11 MAC addresses of the devices and the physical link.

For a physical link to exist in the CONNECTED state the two devices must have established a PTKSA as described in [1] clause 8.4.1.

3.1 PHYSICAL LINK STATE MACHINE

3.1.1 General rules

The behavior of the PAL with respect to physical links is described in terms of a finite state machine. The state machine describes the behavior of the PAL for an individual physical link; extension to multiple physical links is outside the scope of this document. The sequence of external stimulus and behavior at the logical HCI shall be as though this state machine is present in the implementation. Similarly, the sequence of stimulus and behavior at the 802.11 radio interface shall be as though this state machine is present in the implementation.

3.1.2 State Diagram

The possible state events and transitions are summarized in this diagram. The diagram itself is Informative.

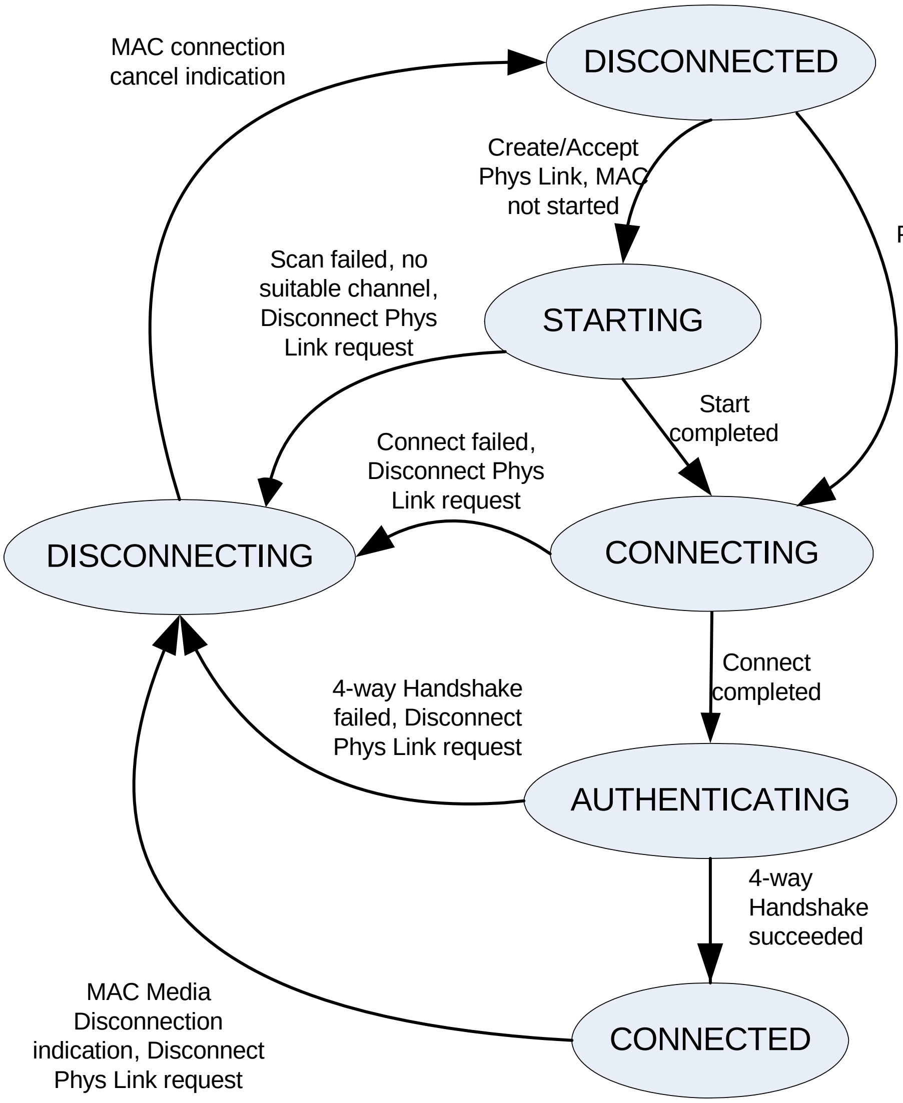

DISCONNECTED
STARTING
CONNECTING
DISCONNECTING
AUTHENTICATING
CONNECTED
MAC connection cancel indication
Create/Accept Phys Link, MAC not started
Create/Accept Phys Link, MAC on channel
Scan failed, no suitable channel, Disconnect Phys Link request
Start completed
Connect failed, Disconnect Phys Link request
Connect completed
4-way Handshake failed, Disconnect Phys Link request
4-way Handshake succeeded
MAC Media Disconnection indication, Disconnect Phys Link request

Figure 3.1: Physical Link finite state machine diagram

3.1.3 States

The following states have been defined to clarify the protocol. The states apply to an individual physical link. At power-up or reset, no physical links exist and the state is the DISCONNECTED state.

DISCONNECTED—The physical link is not active, and this is the initial state.

STARTING—Channel has been selected, the MAC is initializing.

CONNECTING—The initiating device waits for messages from the peer device; the responding device commences network connection operations.

AUTHENTICATING—The devices perform the security association process.

CONNECTED—A secure physical link has been established with the remote device.

DISCONNECTING—The PAL waits for the MAC to complete disconnection and return to the initial state.

3.1.4 Events

The following events may cause transitions in the state diagram.

Create/Accept Physical Link—HCI commands from the local host which affect the state of a physical link.

Connection Accept Timeout—The timeout for this physical link create/accept has expired.

MAC Start Completed—The MAC has started operation on the given channel. This includes beaconing and listening for connections.

MAC Start Failed—The MAC has failed to start on the specified channel for any reason.

MAC Connect Completed—The MAC has completed the process of connecting to a peer in a specified channel.

MAC Connect Failed—The MAC fails to connect on the selected channel for any reason

MAC Media Disconnection Indication—MAC has signaled an existing connection is lost to a remote device.

MAC Connection Cancel Indication—MAC has completed the request to cancel a prior connection.

HCI Disconnect Physical Link Request—The host has given a disconnect request to the PAL.

4-way Handshake Fails—The establishment of a secure link for this physical link has failed.

4-way Handshake Succeeds—The establishment of a secure link for this physical link has completed successfully.

3.1.5 Conditions

The following conditions are potential qualifiers for actions and state transitions to occur.

MAC not yet started in selected channel—The MAC is not beaconing in any PHY channel, or is beaconing in a different channel than the one specified.

MAC already in selected channel—The MAC is already beaconing in the selected PHY channel.

No suitable channel—No suitable channel can be selected, or the selected channel cannot be joined for any reason.

Device is initiator—Role of device is physical link initiator due to reception of Physical Link Create command.

Device is responder—Role of device is physical link responder due to reception of Physical Link Accept command.

3.1.6 Actions

In some cases, a state transition causes one or more of the following actions to occur. The actions for a state transition shall occur in their entirety before any subsequent state transition occurs, as follows.

Determine selected channel—Using information from the AMP_ASSOC of the remote device and preferences from the local device, select a channel

Set or clear Connection Accept Timeout —Start or stop the timer for the current physical link.

Set or clear NeedPhysLinkCompleteEvent, DiscRequested —Set or clear state variables which control subsequent behavior.

Set or PhysLinkCompleteStatus—Sets command status to be indicated to Host.

Signal MAC to start on channel—Command the MAC to start the process of connection on the specified channel.

Issue MAC connection command—Command the MAC to attempt to connect to the remote device.

Initiate 4-way handshake—Command the authenticator to send the first security message.

Send HCI event—send the indicated HCI event to the local Host.

Cancel MAC connect operation—This physical link no longer needs to be present on this channel. The PAL signals the MAC to delete the connection.

Signal MAC to disconnect peer—Command MAC to send disconnection frame to peer.

3.1.7 DISCONNECTED State

This is the initial state. No timers shall be active.

Event	Condition	Action	Next State
HCI_Create_ Physical_Link command	MAC not yet in selected channel	Determine selected channel Request MAC to start on channel Set Connection Accept timeout Set NeedPhysLinkCompleteEvent Set PhysLinkCompleteStatus to 0x00 (no error)	STARTING
HCI_Create_ Physical_Link command	MAC already in selected channel	Determine selected channel Send HCI Channel Select event Set Connection Accept Timeout Set NeedPhysLinkCompleteEvent Set PhysLinkCompleteStatus to 0x00 (no error)	CONNECTING
HCI_Create_ Physical_Link command	No suitable channel	Determine selected channel Send HCI Physical Link Complete event with Status set to [E3474]~~Connection Rejected due to Limited Resources~~No~~-~~Suitable Channel Found (0x~~0D~~39)	DISCONNECTED
HCI_Accept_ Physical_Link command	MAC not yet in channel	Signal MAC to start on channel Set Connection Accept Timeout Set NeedPhysLinkCompleteEvent Set PhysLinkCompleteStatus to 0x00 (no error)	STARTING
HCI_Accept_ Physical_Link command	MAC already in that channel	Set Connection Accept Timeout Issue MAC connection command Set NeedPhysLinkCompleteEvent Set PhysLinkCompleteStatus to 0x00 (no error)	CONNECTING
HCI_Accept_ Physical_Link command	No suitable channel	Send HCI Physical Link Complete event with Status set to [E3474]~~Connection Rejected due to Limited Resources (0x0D)~~NoSuitable Channel Found (0x39)	DISCONNECTED

Table 3.1: DISCONNECTED State event table

3.1.8 STARTING State

This state is used to begin MAC operation, if required.

Event	Condition	Action	Next State
Connection Accept Timeout		SetPhysLinkCompleteStatus to Connection Accept Time-out (0x10)	DISCONNECTED
HCI_ Disconnect_ Physical_Link command		Indicate HCI Disconnection Physical Link Complete event with Status set to Success (0x00) and Reason set to Connection Terminated By Local Host (0x16) Clear Connection Accept Timeout Cancel MAC connect operation Set PhysLinkCompleteStatus to Unknown connection identifier (0x02)	DISCONNECTED
MAC Start Completed	Device is link originator	Issue HCI Channel Select event	CONNECTING
MAC Start Completed	Device is link responder	Issue MAC connection command	CONNECTING
MAC Start Failed		Clear Connection Accept Timeout Set PhysLinkCompleteStatus to MACConnection Failed(0x3F)	DISCONNECTED

Table 3.2: STARTING State event table

3.1.9 CONNECTING State

This state is used to cause the devices to start communication with each other, over the 802.11 media.

Event	Condition	Action	Next State
Connection Accept Time-out		Cancel MAC connect operation Set PhysLinkCompleteStatus to 0x10 (Connection Accept timeout)	DISCONNECTING
MAC Connect Completed	Device is responder		AUTHENTICATING

Table 3.3: CONNECTING State event table

Event	Condition	Action	Next State
MAC Connect Completed	Device is initiator	Initiate four way handshake	AUTHENTICATING
HCI_ Disconnect_ Physical Link command		Indicate HCI Disconnection Physical Link Complete event with Status set to Success (0x00) and Reason set to Connection Terminated By Local Host (0x16) Set PhysLinkCompleteStatus to Unknown connection identifier (0x02) Clear Connection Accept Timeout Cancel MAC connect operation	DISCONNECTING
MAC Connect Failed		Cancel MAC connect operation Set PhysLinkCompleteStatus to MAC Connection Failed (0x3F)	DISCONNECTING

Table 3.3: CONNECTING State event table

3.1.10 AUTHENTICATING State

The AUTHENTICATING state is entered when the two devices have established an unsecured connection.

While in the AUTHENTICATING state the two devices shall perform the 802.11 RSN 4-way handshake as described in Section 3.5, establish a PTKSA, and insert key material into the MAC.

Event	Condition	Action	Next State
Connection Accept Timeout		Set PhysicalLinkCompleteStatus to 0x10 (MAC Connection Failed)	DISCONNECTING
HCI_ Disconnect_Physical Link command		Indicate HCI Disconnection Physical Link Complete event with Status set to Success (0x00) and Reason set to Connection Terminated By Local Host (0x16) Set PhysLinkCompleteStatus to Unknown connection identifier (0x02 Clear Connection Accept Timeout Signal MAC to disconnect peer	DISCONNECTING

Table 3.4: AUTHENTICATING State event table

Event	Condition	Action	Next State
4-way Handshake Failed		Signal MAC to disconnect peer Set PhysLinkCompleteStatus to 0x05 (Authentication failure) Clear Connection Accept Timeout	DISCONNECTING
4-way Handshake Succeeded		Send HCI Physical Link Complete event with Status set to Success (0x00) Configure MAC with Link Supervision Timeout Clear Connection Accept Timeout Clear NeedPhysLink CompleteEvent	CONNECTED

Table 3.4: AUTHENTICATING State event table

3.1.11 CONNECTED State

The CONNECTED state is the operational state for the physical link.

Event	Condition	Action	Next State
HCI_ Disconnect_ Physical Link command		Indicate HCI Disconnection Physical Link Complete event with Status set to Success (0x00) and Reason set to Connection Terminated By Local Host (0x16) Clear Connection Accept Timeout Signal MAC to disconnect peer	DISCONNECTING
MAC Media Disconnection Indication		Indicate HCI Disconnection Logical Link Complete event for each logical link, with Status set to Success (0x00) and Reason set to Connection Terminated by remote host Cancel MAC connect operation	DISCONNECTING

Table 3.5: CONNECTED State event table

3.1.12 DISCONNECTING State

This is a transit state to the DISCONNECTED state and is used to prevent the PAL from preparing to accept or create new connections while a given connection is being deleted by the PAL and the MAC. The PAL shall exit from this state when the MAC is ready to accept new connections.

Event	Condition	Action	Next State
MAC Connection Cancel Indication	PhysLinkCompleteEvent is set	Send HCI Physical Link Complete with status set to PhysLinkCompleteStatus	DISCONNECTED
MAC Connection Cancel Indication	PhysLinkCompleteEvent is clear		DISCONNECTED

Table 3.6: DISCONNECTING State event table

3.2 CHANNEL SELECTION

3.2.1 Overview

Peer to peer networks in 802.11 can incur long connection latency unless there is out of band coordination. Also, one or both of the AMP devices may already be connected to an external network and may therefore need to remain on a given channel. To solve these problems, the data structures and algorithms specified here may be used to provide a coordination service during the creation of the physical link.

An 802.11 channel should be chosen based on up-to-date dynamic information obtained from both AMP peers. The channel selection process is outside the scope of this document but the selected channel shall meet the following criteria:

- ~~S~~The channel shall be legally permitted for use according to local regulatory agencies. If no locale is known, then a common mode configuration shall be used. See Section 3.2.2.
- ~~S~~The channel shall not use a 40 MHz channel width in the 2.4 GHz ISM band.
- ~~S~~If the channel width is 20 MHz, then the channel shall be ~~present~~included in the ~~Preferred Channel List~~PCL TLV and in the PCLv2 TLV, if present, in the AMP_ASSOC ~~given in the HCI Write Remote AMP ASSOC command~~ provided by the initiator in connection establishment. If the channel width is 40 MHz, then the channel shall be present in the PCLv2 TLV.
- ~~S~~"The channel selection process should avoid forcing either AMP device to move its channel.
- ~~S~~"The channel selection process should favor channels with least impact on BR/EDR operation.

The initiating PAL may not be able to select a suitable channel or the responding PAL may reject the selected channel. If the selection process cannot identify a channel, then the physical link establishment shall be aborted.

The selected channel is transmitted to the responding AMP manager as a field in the AMP_ASSOC parameter in the AMP Create Physical Link message, and given to the responding PAL via the HCI Write Remote AMP ASSOC command.

3.2.2 Regulatory

Even though IEEE 802.11 devices operate in unlicensed spectral bands, the unlicensed bands and the limits of allowable behavior in each band is specific to a country and is enforced by spectrum regulatory bodies. ~~See annex I of [1] for example regulations and references to relevant documents.~~ There is a consistent set of rules for operation in the 2.4 GHz ISM band, as described in the following text.

802.11 AMP equipment providers interpret these rules in independent ways and meet the regulations with independent mechanisms so specification of an algorithm to implement regulatory compliance for all situations is beyond the scope of this document.

If an implementation has knowledge of local regulatory constraints then such an implementation may be able to improve certain characteristics of the AMP link, for example by selecting a 5 GHz channel of operation to provide better performance with the collocated BR/EDR radio.

3.2.3 Specification of Channel Identifiers

~~The format of Preferred Channel Lists and Connected Channel Lists is specified by the 802.11 Country information element in [1] clause 7.3.2.9.~~ Tables ~~including~~specifying regulatory class identifiers, channel ~~lists~~frequencies, ~~and required behaviors~~widths and descriptors are given for three regulatory domains in [1] normative annex J. ~~From this it is seen that to~~ When using these tables, to resolve all ambiguity of channel identification in construction of a PCL TLV, the country string as specified in [4] and the regulatory class are needed. To support channel descriptions for countries not included in tables J-1, J-2, or J-3, the country string may be distinct from the locale known by the implementation, if any. The country string is only used to select a specific table from the set of tables listed above and is only used in the PCL TLV.

AMP devices may utilize 40 MHz channel width in the 5 GHz UNII band. As described in [1], 40 MHz channels are specified as two adjacent 20 MHz channels, one with a role of the primary channel and the other with a role of the extension channel. The role and relative positioning of the primary and extension channels are given in Table 3.6a. The operating index is contained within an operating triplet.

Operating index	Channel Starting Frequency (GHz)	Channel Spacing (MHz)	Channel Set	Behavior Limits Set
1 – 80	NA	Reserved	Reserved	Reserved
81	2.407	25	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	
82	NA	Reserved	Reserved	Reserved
83	NA	Reserved	Reserved	Reserved
84	NA	Reserved	Reserved	Reserved
85-114	NA	Reserved	Reserved	Reserved
115	5	20	36, 40, 44, 48	IndoorOnlyBehavor
116	5	40	36, 44	IndoorOnlyBehavior, PrimaryChannelLowerBehavior
117	5	40	40, 48	IndoorOnlyBehavior, PrimaryChannelUpperBehavior
118	5	20	52, 56, 60, 64	
119	5	40	52, 60	PrimaryChannelLowerBehavior
120	5	40	56, 64	PrimaryChannelUpperBehavor
121	5	20	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	
122	5	40	100, 108, 116, 124, 132	PrimaryChannelLowerBehavior
123	5	40	104, 112, 120, 128, 136	PrimaryChannelUpperBehavior

Table 3.6a: Channel set descriptions for PCLv2

124	5	20	149, 153, 157, 161	NomadicBehavior
125	5	20	149, 153, 157, 161, 165, 169	LicenseExemptBehavior
126	5	40	149, 157	PrimaryChannelLowerBehavior
127	5	40	153, 161	PrimaryChannelUpperBehavior
128-191	NA	Reserved	Reserved	Reserved
192-253	NA	Vendor Specific	Vendor Specific	Vendor Specific
254	2.407	25	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	Operating index for Bluetooth, 20 MHz operation only
255	NA	Reserved	Reserved	Reserved

Table 3.6a: Channel set descriptions for PCLv2

Multiple ~~regulatory~~operating triplets may be given in the same ~~Country information element~~PCL, PCLv2, or CCL TLVs. If sub-band triplets are given then they are to be assumed to modify the ~~immediately prior regulatory~~nearest preceding operating triplet. Sub-band triplets may be specified in any order, but they must not contain overlapping channel sets, as noted in [1] clause 7.3.2.9.

The ~~Preferred Channel List shall~~PCL may be included in messages containing AMP_ASSOC fields exchanged over the BR/EDR link during construction of the physical link. The ~~Preferred Channel List~~PCL shall contain exactly one country string and one or more ~~regulatory~~operating triplets. If the current locale is unknown, then the non-country designator of 'XXX' (see definition of dot11CountryString in [1] normative Annex D) and regulatory class of 254 shall be used. The set of channels preferred when using this designator and regulatory ~~class~~index shall be channels 1 through 11 in the 2.4 GHz ISM band, with channel 1 the most preferred of the set. Supporting examples ~~follow~~are given below.

The PCLv2 may be included in messages containing AMP_ASSOC fields exchanged over the BR/EDR link during construction of the physical link. The PCLv2 does not contain a country string. It shall contain one or more operating triplets and zero or more sub-band triplets. Note: For the channel descriptions given in Table 3.6a, for a given operating index, not every associated channel may be legal to use in a given locale. It is up to each AMP implementation to maintain compliance with local regulatory rules. If the current locale is unknown, then the PCLv2 shall not be included in any AMP_ASSOC sent over the BR/EDR link.

The PCLv2 is included by the sender to describe both 20 MHz and 40 MHz channels and also contains the same 20 MHz channels as described in the required PCL TLV. However, the channels in the PCLv2 are specified using operating indices as given in Table 3.6a, not the specific regulatory domain identifiers used in the PCL.

The CCL is used to inform the peer of the current channel usage of the sending AMP.

3.2.4 Channel List Examples

In the first example ~~preferred channel list~~PCL, we assume the ~~PAL~~device does not know its locale and it prefers operation on channel 1 in the 2.4 GHz ISM band, although operation on channels 2 through 11 is acceptable. The absence of a specific sub-band triplet implies all channels 1 through 11 are acceptable.

Field	Value	Comments
Country String	'XXX'	Applies to entire table. Signifies non-country (mobile applications).
Regulatory Extension Identifier	201	
Regulatory Class	254	In context of Country String. Signifies 2.4 GHz ISM band channels 1 through 11 unless modified by specific channel list.
Coverage Class	0	Not used by AMPs.

Table 3.7: Simple preferred channel list

In the next example, assume the PAL again does not know its locale, but it prefers operation only on channels 6, 7 and 11, with 11 the most preferred.

Field	Value	Comments
Country String	'XXX'	Applies to entire table. Signifies non-country (mobile applications)
Regulatory Extension Identifier	201	
Regulatory Class	254	In context of Country String. Signifies 2.4 GHz ISM band channels 1 through 11 unless modified by specific channel list.
Coverage Class	0	Not used by AMPs.
First Channel	11	First sub-band triplet
Number of channels	1	
Maximum transmit power level	20	

Table 3.8: Preferred channel list with non-contiguous channels

Field	Value	Comments
First Channel	6	Second sub-band triplet
Number of channels	2	
Maximum transmit power level	20	

Table 3.8: Preferred channel list with non-contiguous channels

In the ~~final~~next example, assume the PAL knows that it is operating in the US and it has determined that all channels in the 2.4 GHz ISM band and 2 channel s of 20 MHz width, 36 and 40, in the 5 GHz U-NII I band should be communicated to the other peer. It is also assumed that the PAL has determined that channels in the 2.4 GHz band are preferred to the 5 GHz channels. The PAL would use the following ~~Preferred Channel List~~PCL.

Field	Value	Comments
Country String	'US'	Applies to entire table.
Regulatory Extension Identifier	201	First ~~regulatory~~operating triplet.
Regulatory Class	12	In context of Country String, specifies channels 1 through 11, inclusive, in 2.4 GHZ ISM band. Absence of specific channel list signifies all channels in this (FCC) regulatory class are available to the AMP.
Coverage Class	0	Not used by AMPs.
Regulatory Extension Identifier	201	Second ~~regulatory~~operating triplet.
Regulatory Class	1	In context of Country String, specifies 20 MHz channel spacing. Presence of subsequent channel list signifies not all channels in the regulatory class are available to the AMP.
Coverage Class	0	Not used by AMPS.
First channel	36	First sub-band triplet.
Number of channels	2	Channels 36 and 40 are included, with channel 36 more preferred than channel 40.
Maximum transmit power level	20	Units in context of Country String (dBm, mW, etc).

Table 3.9: Mixed band preferred channel list example

In the next example consider the case of a PCL for Canada with 20 MHz channel numbers 36 and 40 and a PCLv2 with 40 MHz channel widths for channel pairs (36, 40) and (44, 48), as well as the 20 MHz channels in the PCL.

Assume for this example that Canada uses the same channel descriptions as the US for the channels referenced. A country string of 'US ' is used in the PCL in order to indicate we are drawing the channel descriptions from Table J-1 in [1]. The channel descriptor in the PCLv2 for the former channel pair shows that 36 is the primary channel, while the descriptor for the latter pair shows that 48 is the primary channel. The operating indices will be from the set {115, 116}. Note: 2.4 GHz channels are not included at all in this example, implying that only 5 GHz band channels will be used if any connection is made.

The PCL TLV and PCLv2 TLV are shown in the tables 3.9a and 3.9b below. In the PCLv2 TLV the 40 MHz pairs are shown first and the 20 MHz channels follow.

Field	**Value**	**Comments**
Country String	'US'	Applies to entire PCL
Regulatory Extension Identifier	201	First operating triplet
Regulatory Class	1	Specifies channels 36 - 48 inclusive, 20 MHz width. Will be further restricted by sub-band triplet
Coverage Class	0	Not used by AMPs
First channel	36	First sub-band triplet
Number of channels	2	Denotes channels 36, 40
Transmit power	20	

Table 3.9a: *Example preferred channel list TLV for Canada*

Field	**Value**	**Comments**
Operating Extension Identifier	201	First operating triplet
Operating index	116	Specifies channels 36 and 44, inclusive, are to be considered primary channels with extension channels at the higher adjacent frequencies, i.e. channels 40 and 48 are extension channels.
Coverage Class	0	Not used by AMPs
First Channel	36	First sub-band triplet. Specifies 36 is primary and 40 is upper extension.
Number of Channels	1	There is one 40 MHz channel specified.

Table 3.9b: *PCLv2 example*

Field	Value	Comments
Transmit power	20	
Operating Extension Identifier	201	Operating triplet for the 20 MHz channels
Operating index	115	Specifies channels 36 – 48 inclusive, 20 MHz width.
Coverage Class	0	Not used by AMPs
First channel	36	Sub-band triplet
Number of channels	2	Denotes channels 36, 40
Transmit power	20	

Table 3.9b: PCLv2 example

3.3 802.11 LINK CREATION

3.3.1 Starting the AMP Network

After the initiator has selected a channel of operation, the initiating PAL shall instruct the MAC to commence network operation, including beaconing. The 802.11 AMP devices shall use probe responses and/or beacons (respecting regulatory restrictions) to advertise MAC capabilities.

AMP devices shall use beacons to enable effective coexistence with neighboring 802.11 networks. For example, non-AMP devices can discover the existence of AMP networks and such devices can also determine the EDCA characteristics of the network. In regulatory domains where DFS operation is required, an AMP device may need to passively observe the channel to check for radar, as described in [1] clause 11.9, before it may start to beacon. For AMP operation, the maximum beacon period shall be Max80211BeaconPeriod.

The SSID information element for AMP devices shall be of the form 'AMP-xx-xx-xx-xx-xx-xx' (with no null termination and no quotes) where the "x" characters are replaced by the lowercase hexadecimal characters of the MAC address of the local 802.11 device. This is referred to here as the AMP SSID. For example, if the MAC address of a device is 00:01:02:0A:0B:0C, then the AMP SSID would be 'AMP-00-01-02-0a-0b-0c'.

AMP beacons shall be indicated as ESS-style beacons in the capability information field as described in [1] clause 7.3.1.4 and shall include the AMP SSID. Beacons shall be sent with standard beacon channel access semantics as given in [1] clause 11.1.2.1. The contents of the Address2 and Address3 fields for beacons and probe responses shall be the MAC address of the transmitting AMP node. Probe requests sent to AMP peers shall use the MAC address of the intended recipient as the content of the Address1 and Address3 fields. In

[1] clause 7.2.3.1 contains the details of the format of 802.11 beacon frames and [1] clause 7.2.3.9 contains the details of the format of 802.11 probe response frames, including a list of the required information elements is specified.

3.3.1.1 HT Operation

The AMP peers shall maintain the HT protection field in the HT operation information element in their beacons according to [1]. When communicating with the initiator, the responder shall use the protection mechanism dictated by the initiator's beacon.

The HT features of Greenfield, Reduced Inter-Frame Space (RIFS), dual Clear to Send (CTS) protection and Phased Coexistence Operation (PCO) shall not be used in AMP links. The respective fields in the 802.11 HT operation information element shall be set to zero in transmitted MMPDUs and ignored in received MMPDUs.

When using a DFS channel, the AMP responder shall monitor the field which indicates Overlapping BSS (OBSS) non-HT stations are present in the HT operation element of the AMP initiator's beacon and adhere to the requirements in [1]. The AMP initiator shall be responsible for setting this field.

3.3.2 Establishing the 802.11 Link

AMP devices may choose to obtain the timebase of their peer through the timestamp field in 802.11 beacons and probe responses. The respective Target Beacon Transmission Time (TBTT) of the peers may be independent and occur at different times with respect to one another. The beacon period of the devices may be different from one another.

AMPs shall use RSN security. RSN security requires the use of 802.11 open authentication as specified in [1] clause 8.2.2.2. The AMP responder shall send the first frame of the 802.11 authentication transaction sequence with transaction ID of 1. Address fields Address1 and Address3 shall contain the initiator's address.The AMP initiator shall respond with an 802.11 authentication frame with transaction ID of 2. Address fields Address2 and Address3 shall contain the initiator's address.

AMPs shall use 802.11 (re)association frames to select features advertised by their peer. The AMP responder shall send an (re)association request frame. Address fields Address1 and Address3 shall contain the initiator's address.

The AMP initiator shall reply with an (re)association response frame. Address fields Address2 and Address3 shall contain the initiator's address. The frame body contents of both the (re)association request and response are given in [1] clause 7.2.3.4 and [1] clause 7.2.3.5, respectively.

After successful 802.11 (re)association, unencrypted security frames may be transmitted on the physical link.

3.3.3 Address Fields of Data Frames

The 802.11 AMP shall support the use of four address field frame format for all data frames after (re)association.

To use data frames with four address fields the AMP shall set the ToDS and FromDS bits in the FrameControl field equal to one. The addresses used for such frames shall be arranged as shown in Table 3.10. Because there is no frame forwarding by AMPs, the RA is the same as the DA and the TA is the same as the SA.

Field	Value
Address1	Receiver Address (RA)
Address2	Transmitter Address (TA)
Address3	Receiver Address (RA)
Address4	Transmitter Address (TA)

Table 3.10: Four address frame address fields

3.3.4 Admission Control

AMP devices should respond to probe requests with a probe response.

If Address2 of an 802.11 association request does not match the MAC address from the AMP Assoc received during construction of the current physical link or if the SSID in the association request does not match the AMP SSID of the receiving AMP device, then the receiving AMP device shall not transmit an 802.11 association response with a status code of 0 (success).

3.4 PHYSICAL LINK MAINTENANCE

After a physical link is created, an AMP device shall monitor the state of the link and provide an indication of link failure to the Host if no frames are received from the AMP physical link peer for a period of Link Supervision Timeout (LSTO). Correctly decrypted data frames received from the peer shall be evidence of an existing physical link, but this is not true for 802.11 ACK and CTS control frames.

If the PAL has not received a correctly decrypted data frame for a period less than LSTO, then it shall solicit a response from its peer in an attempt to receive the response before the expiration of LSTO. For this purpose, link supervision request/response protocol identifiers are given in Table 5.2 and may be used to construct link supervision data frames. When a PAL receives a data frame with a protocol identifier of Link Supervision Request, it shall reply by transmitting a data frame with a protocol identifier of Link Supervision Reply.

3.5 PHYSICAL LINK SECURITY

3.5.1 Obtaining Key Material

The Host provides key material for use with a physical link as the Dedicated_AMP_Link_Key parameter of the HCI_Create_Physical_Link or HCI_Accept_Physical_Link command. See [Vol 2] Part E, Section 5.2 for octet ordering of multi-octet HCI parameter values. The Dedicated_AMP_Link_Key parameter shall be interpreted by the PAL as a 256 bit integer and used directly as a Pairwise Master Key (PMK) by the two devices to create a PTK. Further key material is derived from the PTK.

3.5.2 Creating a PTK

The 802.11 4-way handshake is used to create a PTK from the PMK. See [1] clause 8.5.3.

Entities known as authenticator and supplicant are used to exchange security information in the 802.11 security architecture. Since the responding AMP device receives the 802.11 (re)association response frame, it shall serve the role of supplicant; the initiating AMP device shall serve the role of authenticator. The authenticator sends the first and third messages of the 4-way handshake and the supplicant sends the second and fourth messages. Only a single instance of the 4-way handshake is run by the 802.11 AMP to establish its secure connection.

If a 4-way handshake fails then the PAL physical link state machine shall transition to the DISCONNECTING state as described in Section 3.1.10.

The supported security configurations of the peers are given in the RSN information element in beacons or probe responses exchanged by the AMP devices. The PAL shall enforce the following restrictions:

- UseGroup (00:0F:AC:00), WEP-40 (00:0F:AC:01), TKIP (00:0F:AC:02), and WEP-104 (00:0F:AC:05) shall not be allowed as valid pairwise cipher suites.
- The group cipher shall be CCMP (00:0F:AC:04)
- The only valid AKMP shall be PSK (00:0F:AC:02) or a vendor-specific AKMP.
- The NoPairwise bit (B1) of the RSN Capabilities field shall ~~not be allowed as a valid selection~~be set to zero.
- ~~The group cipher shall be CCMP (00:0F:AC:04)~~The Management Frame Protection Required (MFPR) bit (B6) of the RSN Capabilities field shall be

set to zero. Note: This does not prevent the use of Management Frame Protection.

The supplicant shall ensure a proper intersection of capabilities exists subject to the constraints above. It may also choose a set according to its policy requirements and may ~~decide to~~ terminate a connection attempt if no policy match is found. Either the supplicant or the authenticator may ~~choose to~~ terminate a connection after AMP Create Physical Link Response is sent by indicating an HCI Physical Link Complete event with an unsuccessful status code.

The AMP key received from the host may be marked with a Link_Type of debug. If it is, then the local PAL may choose to use the key, or it may choose to refuse to establish the link, according to its own policy. The management of this debug key policy is outside the scope of this document.

The PAL shall use the AMP key as a Pairwise Master Key (PMK) according to the 802.11 key hierarchy described in [1] clause 8.5.1.2 and shall exchange nonces (as part of a 4-way handshake) to add liveness in the derivation of a Pairwise Transient Key (PTK). The PTK shall be derived specifically for a session started by the HCI_Create_Physical_Link_Request command and shall be destroyed when the session is terminated by the HCI_Disconnect_Physical_Link command. The construction of the AAD used with CCMP shall include Address4 in the manner illustrated in [1] clause 8.3.3.3.2, Figure 8-17.

3.5.3 Using Encryption

Encryption keys are derived from the PTK and are inserted into the 802.11 MAC after the 4-way handshake has successfully completed. All data frames after this point are encrypted and this state persists until the physical link is destroyed.

3.5.4 Refreshing a PTK

The PTKSA, if any, shall be discarded when the physical link to which it applies enters the DISCONNECTED state. At this point the Host may reestablish the connection which will cause the creation of a new PTKSA.

The PTKSA shall be discarded in the event its receive sequence counter becomes exhausted. Since this is a 48 bit counter, this is an unlikely event.

To establish a new PTK, the physical link shall be torn down and re-established.

3.5.5 Transporting Security Handshake Messages

Security handshake messages shall be sent after the physical link is created, but before any logical link is created between the two devices.

The SNAP header composed of the OUI of the Bluetooth SIG and the protocol identifier given in Table 5.2 shall be used to distinguish AMP 4-way handshake messages from external security traffic.

3.6 PHYSICAL LINK SUPPORT FOR QOS

3.6.1 QoS Advertisement

If an AMP device supports 802.11 EDCA and is configured to use it, then it should indicate this to the host by setting the Guaranteed_Service_Type_Supported field of the PAL_Capabilities parameter included in the HCI_Read_Local_AMP_Info command.

If QoS is offered by an AMP device, it shall advertise EDCA in beacon and probe response frames by including the EDCA Parameter Set information element, as given in [1] clause 7.3.2.29. Note: The EDCA Parameter Set information element is also included in (re)association response frames. For AMP devices, the use of the EDCA parameter set shall be as follows. The QoS Info field shall be zero. The ACI, AIFSN, and TXOPlimit values of the AC parameter record shall be as given in [1] Table 7-37. The ECWmin and ECWmax values are specific to the 802.11 PHY type and are documented in their appropriate clauses in [1] The Admission Control Mandatory (ACM) bit should be zero.

The QoS Capability information element is described in [1] clause 7.3.2.35. The QoS Info field (see [1] clause 7.3.1.17) is contained in the QoS Capability information element as well as the first field of the EDCA Parameter Set information element. AMP devices shall not include the QoS Capability information element in beacons or probe responses.

The [E3764] interpretation of the content of the QoS Info field is different depending on if the enclosing frame is a beacon or probe response, or if it is a (re)association request. ~~The QoS Info field is not included in (re)association response frames~~.

802.11 Information element	Frame(s) contained in
QoS Capability information element	Association Request, Reassociation Request
EDCA Parameter Set information element	Beacon, Probe Response, Association Response, Reassociation Response

Table 3.11: EDCA advertisement and negotiation

The EDCA AC parameters shall not change unless the physical link is torn down and re-established. Therefore the EDCA Parameter Set Update Count subfield of the QoS Info field in beacons and probe responses shall be zero.

3.6.2 Negotiation

To request the use of EDCA on the physical link an AMP device shall include a QoS Capability element in its (re)association request. If the AMP peer rejects the EDCA negotiation then the (re)association response frame shall have no EDCA Parameter Set element included. If the (re)association response frame has a status code of successful and the EDCA Parameter Set element is included, then the link shall be considered to support EDCA.

4 LOGICAL LINK MANAGER

A logical link provides a (possibly) bidirectional path for in-order delivery of L2CAP PDUs, with a specified set of traffic characteristics. Each logical link exists with respect to a specific physical link in the CONNECTED state.

A logical link is characterized by a pair of Extended Flow specification parameter sets, as described in [1]. An Extended Flow specification parameter set is referred to simply as a flow spec here.

Each logical link is classified as either Best Effort or Guaranteed. The logical link is known as Best Effort if either of its flow specs indicates Best Effort in its Service Type field. Otherwise, it is known as Guaranteed.

Support for Guaranteed links is optional; the PAL may reject any guaranteed flow spec. If 802.11 QoS (see Section 3.6.1) is not supported by both endpoints, then there is no traffic prioritization in the MAC.

4.1 LOGICAL LINK CREATION

Creation of a logical link is initiated by the HCI_Create_Logical_Link or HCI_Accept_Logical_Link command. If the physical link is not in state CONNECTED, the PAL shall send the HCI Logical Link complete event with status set to Command Disallowed (0x0C). The Controller shall indicate successful completion of the logical link creation using the HCI Logical Link Complete event, with Status set to Success (0x00).

4.1.1 Logical Link Handles

When a Logical Link is created or accepted the PAL shall create a Logical Link handle, or logical handle. The logical handle is included in HCI ACL data packets received from the HCI in the Handle field; the PAL may use the logical handle to help it select the egress physical link. If the Host delivers an HCI ACL data packet to the AMP Controller with an invalid Handle field, then the AMP shall discard the ACL data packet and the PAL may indicate a Number of Completed Blocks or Number of Completed Packets event (depending on the configuration of the Flow Control setting) using the Host-supplied logical handle.

When the PAL receives data frames from the MAC, it may use the source address to determine the physical link. It shall place the physical link handle corresponding to that link into the Handle field of the HCI ACL data packet before the packet is indicated to HCI. Note: the PAL is not required to determine a logical handle for frames it receives from the MAC.

4.1.2 Null Traffic Logical Links

Data frames may be discarded if attempted on a No Traffic flow.

4.1.3 Best Effort Logical Links

There is a single logical link used to transport all Best Effort traffic.

If EDCA was successfully negotiated during the physical link creation, the PAL shall map all egress frames marked with the Best Effort logical handle to a UP of either BEUserPrio0 or BEUserPrio1, inclusive. Otherwise, if EDCA is not used, no mapping is required and the UP shall be set to zero by the PAL.

4.1.4 Guaranteed Logical Links

Flow specs requesting guaranteed service may be accepted by the PAL if the physical link was negotiated with 802.11 QoS.

EDCA shall be used by the 802.11 AMP devices if supported and available for use by both devices. The PAL shall provide a priority field associated with each egress 802.11 frame. The priority field is interpreted by the MAC as a User Priority (UP) and is mapped to access category as specified in [1] clause 9.1.3.1.

If the 802.11 link was negotiated with QoS, then on receiving an HCI_Create_Logical_Link or HCI_Accept_Logical_Link command specifying a Guaranteed transmit flowspec the PAL shall use a UP with a value between MinGUserPrio and MaxGUserPrio, inclusive. The determination of precisely which UP to use is outside of the scope of this specification. A flow spec expresses maximum bandwidth as the product of inter-SDU arrival time and maximum SDU size. The PAL may use the specified maximum bandwidth or latency requirements from the flow spec to establish mappings of logical handles to UPs.

If a request for a guaranteed link cannot be mapped to a UP in the range specified above, it may be rejected.

The PAL shall reject all requests to establish a guaranteed logical link with a flow spec expressing a maximum bandwidth which is greater than the Total_Bandwidth parameter of the Read Local AMP Info command minus the sum of the requested maximum bandwidths of all existing guaranteed logical links.

The transmitter shall store the logical channel to UP mapping for application to future frame transmissions. The receiver shall create an HCI ACL data header and insert the physical link handle into the Handle field of the packet before indication to the Host.

4.2 LOGICAL LINK UPDATES

The Host may indicate a change of traffic requirements on a logical link by using the HCI_Flow_Spec_Modify command. An HCI_Flow_Spec_Modify command will not change the Service Type of the flow specs for a logical link.

When the PAL receives an HCI_Flow_Spec_Modify command, it should validate that the new flow spec requirements can be met with the available resources. If not, then the PAL should reject the command.

4.3 LOGICAL LINK DELETION

The PAL shall rely on upper layers to flush any frames before a logical link is destroyed. See explicit flush in Section 5.3. The PAL may choose to re-use the same logical link identifier for new logical links even on the same physical link.

The PAL should recover any allocated QoS resources when the logical link is deleted. In particular, when deallocating resources for a flow spec which expressed a maximum bandwidth, the PAL should subtract that parameter from the total allocated bandwidth.

5 DATA MANAGER

5.1 ENCAPSULATION

The PAL shall advertise a maximum PDU length of Max80211PALPDUSize octets and each L2CAP PDU is transmitted by the MAC as a single MSDU. The MSDU boundary determines the L2CAP PDU boundary for the receiver.

Before transmission, the PAL shall remove the HCI header, add LLC and SNAP headers and insert an 802.11 MAC header. The LLC/SNAP frame format used by the 802.11 AMP is shown in Table 5.1.

	DSAP	SSAP	Control	OUI	Protocol	Frame Body
Value	0xAA	0xAA	0x03	00:19:58	XX:XX	
Octets	1	1	1	3	2	0-1492

Table 5.1: 802.11 AMP LLC/SNAP encapsulation

The protocol identifiers shall be as shown in Table 5.2:

Value	Protocol Description	Logical Link
0x0000	Reserved	N/A
0x0001	L2CAP ACL data	AMP-U
0x0002	Activity Report	AMP-C
0x0003	Security frames	AMP-C
0x0004	Link supervision request	AMP-C
0x0005	Link supervision reply	AMP-C
0x0006-0xFFFF	Reserved	N/A

Table 5.2: Protocol Identifiers

All 802.11 data frames on the AMP link shall be sent with ToDS and FromDS bits in the Frame Control field both set to one. For a description of the Frame Control field, see [1] clause 7.1.3.1. If QoS was negotiated on the physical link between the peers then the QoS Control field shall be included in the MAC header, otherwise it shall not be included.

The receiving device can determine the physical link identity from the TA of the received frame. The receiving PAL shall decapsulate the frame from 802.11 and into the HCI ACL data encapsulation.

5.2 COEXISTENCE AND LOCAL INTERFERENCE

5.2.1 Interference from Collocated Radios

The BR/EDR radio, LE PHY and the ERP of 802.11 AMP operate in the 2.4GHz ISM band and mechanisms are required to help mitigate potential interference. The BR/EDR and LE radio subsystems on an 802.11 AMP capable device should employ AFH to attempt to avoid interference of overlapping transmissions on the medium.

Protocols specified in [1] are designed to mitigate interface from non-collocated radios.

On systems where the devices are collocated such that radio isolation is insufficient to mitigate interference, the use of the shared medium should be time-division multiplexed to ensure only one of the interfering radios will gain access to the medium. In the case of the BR/EDR radio and the 802.11 radio operating in the 2.4GHz band, the PAL should ensure that local high priority BR/EDR traffic such as SCO, eSCO and ACL packets carrying A2DP information have higher priority over potentially interfering local 802.11 AMP packets. The PAL may ensure this prioritization through many ways including employing the methods described in [3] but the exact methods are outside the scope of this document.

Interference can also arise between the 802.11 AMP radio and collocated licensed band radios (LBRs) operating in adjacent bands to the ISM spectrum. Due to 802.11 AMP transmissions, the collocated LBR may not be able to receive transmissions from its peer LBR. Again the use of the medium should be time-division multiplexed to ensure only one of the radios will gain access to the medium at one time. In the case of the 802.11 AMP radio and an LBR, the PAL should ensure that the local LBR packets have higher priority over potentially interfering local 802.11 AMP packets. Although the exact methods are outside the scope of this document, similar collocated radio interference mitigation mechanisms as described above may be used.

5.2.2 Unavailability of Remote Peer

Distributed AMP devices may experience 802.11 performance degradation due to simultaneous BR/EDR activity occurring at one of the AMP peers. Local interference mitigation schemes (see Section 5.2.1) employing time-divided access to the medium will result in the 802.11 radio being periodically unavailable to its peer. The PAL attempting to transmit to a periodically unavailable AMP device may employ techniques to allow its transmissions to consume minimal airtime and power while still achieving acceptable performance for its own transmissions and those of neighboring networks.

When a physical link is created, the PAL shall configure the 802.11 MAC to use RTS/CTS signaling by default. This behavior may be modified by using Activity Reporting as given in Section 5.2.3.

5.2.3 Activity Reports

AMP Activity Reports provide an optional mechanism for the 802.11 PAL to inform its 802.11 AMP peer of events which may result in the 802.11 device being unavailable to receive 802.11 traffic. Activity Reports may also be used to inform a peer of the absence of local interference thereby allowing the remote peer to disable its RTS/CTS signaling.

Examples of simultaneous traffic include, but are not limited to:

1. BR/EDR SCO/eSCO streams
2. 802.11 traffic required to maintain an external 802.11 connection
3. Traffic from other collocated radios such as LBRs in the 2.3 or 2.5 GHz band (including WiMax, LTE, and UMB)

When Activity Reports are used, it is the PAL which is aware of its unavailability which may generate the interference information. The PAL can determine the information to include in the Activity Report through methods including, for example, the PTA model described in [3]. In many systems with collocated radios there are PTA signals between the BR/EDR and 802.11 controllers which may be used to generate this information.

The information shall be transferred between the communicating 802.11 PALs using a PAL Activity Report PDU encapsulated in an 802.11 data frame. The frame body of the Activity Report PDU following the LLC/SNAP header is shown in Table 5.3. It has a variable length.

Activity Report *Size: Variable*

Value	Octets	Description
ScheduleKnown	1	Bit 0: 1 if the sender knows the schedule of interference 0 if the sender does not know the schedule of interference
NumReports	1	The number of traffic reports in this PDU
StartTime	4	The absolute time of the start of possible unavailability of the peer, expressed as the least significant 32 bits of the 802.11 TSF of the transmitter of the PDU.
Duration	4	Duration of the active phase of the traffic in microseconds.
Periodicity	4	Periodicity of traffic in microseconds. May be zero to indicate aperiodic traffic.

Table 5.3: Activity Report

Processing of received Activity Reports is optional and support for it is advertised in the 802.11 PAL Capabilities field.

The ScheduleKnown field shall indicate to the receiver of the Activity Report whether or not the sender is aware of the schedule of subsequent data traffic.

- If the ScheduleKnown is set to zero, this shall signify the sender is aware of the presence of traffic but not its schedule, and the receiving PAL shall configure the MAC with RTS/CTS signaling for all traffic on the physical link to the sender.
- If the ScheduleKnown is set to one, the sender shall describe the schedule of interference in the subsequent fields; the receiver of the report may either schedule all 802.11 AMP traffic around this schedule, configure the MAC with RTS/CTS signaling, or both.

If a PAL knows there is no interference from collocated radios before or during establishment of a physical link, an Activity Report conveying this state should be sent at the earliest possible opportunity after the physical link is established.

The StartTime, Duration and Periodicity form an Activity Report triplet. The difference between the StartTime and the current TSF of the peer shall be interpreted as a signed 32 bit value. A negative value shall denote a time in the past. The NumReports value indicates the number of Activity Report triplets which follow. The Duration shall specify the amount of time (in microseconds) the PAL is in the mode specified. If the ScheduleKnown field is zero, there shall be no Activity Report triplets and the NumReports field shall be zero. If the Periodicity is non-zero, it shall be a value greater than the Duration.

An Activity Report may be created to describe a burst of interfering traffic by setting ScheduleKnown to one, NumReports to one, StartTime to the time the burst is predicted to start, Duration to the duration of the burst, and Periodicity to zero.

The PAL may inform its peer that interference is no longer present by sending an Activity Report with a ScheduleKnown field set to one, and a NumReports field set to zero. Upon reception of such an Activity Report frame, a receiving PAL may configure the MAC without RTS/CTS signaling.

The PAL may transmit an Activity Report frame periodically in order to correct clock drift between its TSF and the schedule of unavailability caused by the collocated radio. The most recent Activity Report shall supersede all others received.

5.3 EXPLICIT FLUSH

Explicit flush may be initiated at the HCI on any logical link by using the HCI_Enhanced_Flush command. Explicit flush discards all data frames for transmit on the indicated logical link.

5.4 AUTOMATIC FLUSH

If guaranteed logical links are supported, then automatic flush timeouts shall be supported by the 802.11 PAL.

5.5 QUALITY OF SERVICE VIOLATIONS

The PAL may generate a HCI QoS Violation event when it is determined that the parameters of the flow spec are not being met. This may occur for instance when a data packet has been queued for transmission on a Guaranteed logical link for longer than the Access Latency in the flow spec for transmitted traffic on that link. It can also occur when a data packet fails to receive an acknowledgement before the specified flush timeout.

6 CONSTANTS

Name	Value	Units	Description
Max80211PALPDUSize	1492	Octets	Maximum PDU size
Max80211AMPASSOCLen	672	Octets	Maximum length of AMP_ASSOC for this AMP
MinGUserPrio	4	N/A	Minimum value of user priority for guaranteed link
MaxGUserPrio	7	N/A	Maximum value of user priority for guaranteed link
BEUserPrio0	0	N/A	Best effort User Priority
BEUserPrio1	3	N/A	Best effort User Priority
Max80211BeaconPeriod	2000	milliseconds	Maximum value of AMP dot11BeaconPeriod MIB variable
ShortRangeModePowerMax	4	dBm	Maximum transmit power for ERP-OFDM frames when in Short Range Mode

Table 6.1: 802.11 PAL Constants

7 MESSAGE SEQUENCE CHARTS

The MSCs necessary to show the creation and deletion of physical and logical links can be found in the HCI specification (see [Vol 2] Part E), as the sequencing of steps is determined by the logical HCI. However, an overview MSC for physical link creation is given in Figure 7.1.

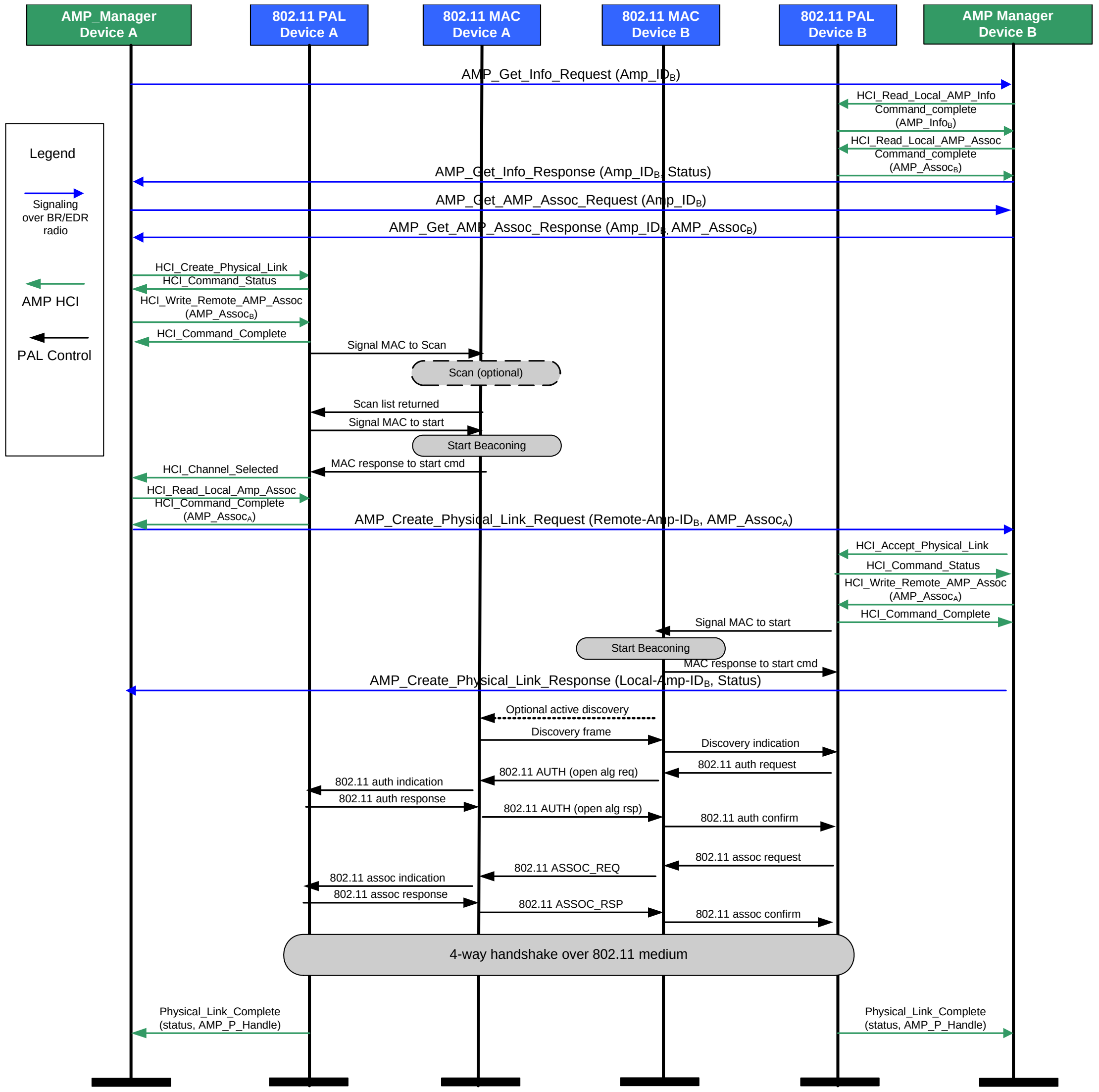

AMP_Manager Device A
802.11 PAL Device A
802.11 MAC Device A
802.11 MAC Device B
802.11 PAL Device B
AMP Manager Device B
Legend
Signaling over BR/EDR radio
AMP HCI
PAL Control
AMP_Get_Info_Request (Amp_ID$_B$)
HCI_Read_Local_AMP_Info
Command_complete (AMP_Info$_B$)
HCI_Read_Local_AMP_Assoc
Command_complete (AMP_Assoc$_B$)
AMP_Get_Info_Response (Amp_ID$_B$, Status)
AMP_Get_AMP_Assoc_Request (Amp_ID$_B$)
AMP_Get_AMP_Assoc_Response (Amp_ID$_B$, AMP_Assoc$_B$)
HCI_Create_Physical_Link
HCI_Command_Status
HCI_Write_Remote_AMP_Assoc (AMP_Assoc$_B$)
HCI_Command_Complete
Signal MAC to Scan
Scan (optional)
Scan list returned
Signal MAC to start
Start Beaconing
MAC response to start cmd
HCI_Channel_Selected
HCI_Read_Local_Amp_Assoc
HCI_Command_Complete (AMP_Assoc$_A$)
AMP_Create_Physical_Link_Request (Remote-Amp-ID$_B$, AMP_Assoc$_A$)
HCI_Accept_Physical_Link
HCI_Command_Status
HCI_Write_Remote_AMP_Assoc (AMP_Assoc$_A$)
HCI_Command_Complete
Signal MAC to start
Start Beaconing
MAC response to start cmd
AMP_Create_Physical_Link_Response (Local-Amp-ID$_B$, Status)
Optional active discovery
Discovery frame
Discovery indication
802.11 auth request
802.11 AUTH (open alg req)
802.11 auth indication
802.11 auth response
802.11 AUTH (open alg rsp)
802.11 auth confirm
802.11 assoc request
802.11 ASSOC_REQ
802.11 assoc indication
802.11 assoc response
802.11 ASSOC_RSP
802.11 assoc confirm
4-way handshake over 802.11 medium
Physical_Link_Complete (status, AMP_P_Handle)
Physical_Link_Complete (status, AMP_P_Handle)

Figure 7.1: Overview MSC for physical link create/accept

8 APPENDIX A: TEST SUPPORT

This section provides the details of the AMP test commands and events described in [Vol 2] Part E.

8.1 AMP TEST COMMAND

Command	OCF	Command Parameters	Return Parameters
HCI_AMP_Test	0x0009	Test Parameters	Status

Description:

This command is used to configure and start a test. This command shall be only valid in AMP Test Mode.

When a test scenario has completed or on receiving a HCI_AMP Test_End command the AMP shall send a HCI AMP Test End event and the AMP returns to an idle state with the RX and TX off.

Test Parameters: *Size: 18 octets*

Value	Parameter Description
0xXX	Test Scenario 0x01 - Transmit single frames with following parameters 0x02 - Receive frames with following parameters 0x03 – 0xFF Reserved
0xXX	Preamble 0x00 – ERP-OFDM preamble 0x01 - Short Preamble 0x02 - Long preamble 0x03 – 0xFF Reserved
0xXX	Payload 0x00 – All Zeros payload 0x01 – All ones payload 0x02 - PRBS9. The PRBS9 sequence is reinitialized for every frame. Each PRBS9 payload is the same. 0x03 - PRBS15. The PRBS15 sequence is reinitialized for every frame. Each PRBS15 payload is the same. 0x04 – 0xFF Reserved

0xXXXXXX	Country	Channel Descriptor For AMP type 802.11, the channel is completely described by a four-tuple of {Country, ~~Regulatory~~Operating Extension Identifier, Regulatory class, Channel number}. The Country identifier is an ISO/IEC-3166 three-octet field and the ~~Regulatory~~ Extension Identifier is equal to 201. If the locale is unknown to the EUT, then it shall only allow channel numbers as given in Ref [2] Clause 18.4.6.2. Valid values are from 1 to 11. All other values are reserved
0xC9	~~Regulatory~~Operating Extension Identifier	
0xXX	~~Regulatory~~Operating Class	
0xXX	Channel Number	
0xXX	Modulation 0x00 ERP-DSSS 0x01 ERP-CCK 0x02 ERP-OFDM 0x03 ERP-PBCC 0x04 DSSS-OFDM 0x05 OFDM All other values are reserved	
0xXX	Rate (Mb/s) Transmission data rate of PSDU. See Ref [2] Clause 19.8.2 PHY MIB dot11SupportedDataratesTxValues The allowed data rates are dependent on the modulation selected. Ref [2] Table 19.1 Clause 19.2 and Clause 17.2.3.3. All other values reserved	
0xXXXX	Payload length 1 to 1500. All other values reserved.	
0xXX	Transmit Power Control (TPC) Valid values are 1 to 8 as defined in the Ref [2] implementation dependent. All other values reserved.	
0xXX	Duty Cycle 10 to 99% (default 50%) All other values reserved.	
0xXXXX	Frame count 1 to 65525 - Number of frames to be transmitted. When the defined frame count has been transmitted the system returns to the idle state and the AMP Test End event is returned to the tester. On receiving the Test End command the AMP returns to idle state.	

0xXX	Scramble state 0x00 – OFF 0x01 – ON All other values reserved.

Return Parameters:

Status: *Size: 1 Octet*

Value	Parameter Description
0x00	AMP Test command succeeded
0x01-0xFF	Test command failed. See “Error Codes” on page 339 [Part D].

Event(s) Generated (unless masked away):

When the AMP receives the HCI_AMP_Test command, the AMP shall send the Command_Status event to the AMP Test Manager which shall be routed to the tester.

The HCI AMP Start Test event shall be generated when the HCI_AMP_Test command has completed and the first data is ready to be sent or received.

The HCI Command Complete event shall not be sent by the AMP to indicate that this command has been completed. Instead the HCI AMP Start Test event shall indicate that this command has been completed.

When in a transmitter test scenario and the frames/bursts count have been transmitted the HCI AMP Test End event shall be sent.

8.1.1 Test Scenarios

All test mode frames shall be test mode data frames.

Single Frame Transmission

When the test scenario is set to transmit single frames the format shall be as defined by the parameters in the rest of the test configuration parameters. The interval between frames shall be as defined by the transmission interval time.

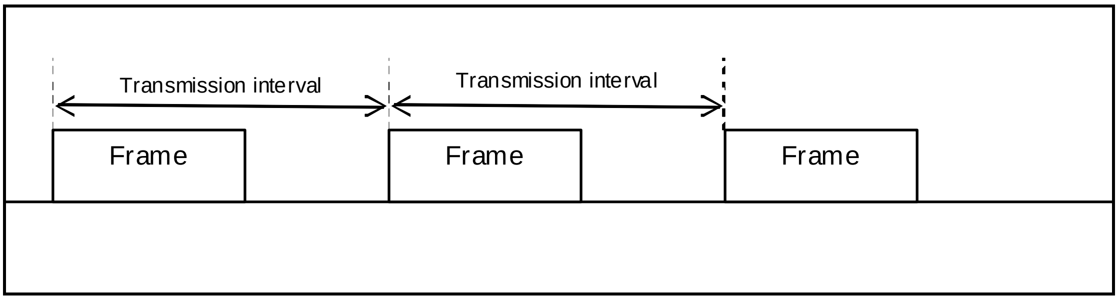


Figure 8.1: Single Frame test transmission

The transmissions shall continue until the frame count is reached or a test end command is received; when a HCI AMP Test End event shall be sent to the tester via the AMP Test Manager.

The requirements of the frames are described in the Test mode data frame format section.

Receive Frames

When the test scenario is set to receive frames the AMP shall receive the frames defined in the other test scenario parameters and, when AMP receiver reports are configured, return receiver reports as defined to the tester via the AMP Test Manager.

8.1.2 Test Mode Data Frame Format

The frames transmitted in test mode are not super frames. All frames shall be Data frames. The format of the frame agrees with the PHY frames in [2] section 19 with non connection test mode fixed fields.

Source and Destination Address

When performing the AMP PHY non connection tests these fields are fixed according to the direction of the message. The AMP shall use a fixed address AMP_TEST_ADDRESS and shall expect to receive frames with an AMP_TESTER_ADDRESS.

Parameter	Address
AMP_TEST_ADDRESS	0x5555 (0101010101010101 binary)
AMP_TESTER_ADDRESS	0xAAAA (1010101010101010 binary)

These are fixed addresses for testing purposes only.

The AMP shall transmit frames in the transmit test scenarios with the SrcAddr set to the AMP_TEST_ADDRESS and the DestAddr set to the AMP_TESTER_ADDRESS.

The AMP shall receive test frames in the receiver test scenarios with the SrcAddr set to AMP_TESTER_ADDRESS and the DestAddr set to the AMP_TEST_ADDRESS.

8.2 AMP START TEST EVENT

Event	Event Code	Event Parameters
HCI_AMP_Start_Test	0x49	Status Test Scenario

Description:

The HCI AMP Start Test event shall be generated when the HCI_AMP_Test command has completed and the first data is ready to be sent or received.

Event Parameters:

Status: *Size: 1 Octet*

Value	Parameter Description
0x00	Test command succeeded
0x01-0xFF	Test command failed. See “Error Codes” on page 339 [Part D].

Test Scenario: *Size: 1 Octet*

Value	Parameter Description
0xXX	0x01 - Transmit single 0x02 – Receive frames 0x00 and 0x03 – 0xFF Reserved

8.3 AMP TEST END EVENT

Event	Event Code	Event Parameters
HCI_AMP_Test_End	0x4A	Status Test Scenario

Description:

The HCI AMP Test End event shall be generated to indicate that the AMP has transmitted or received the number of frames/bursts configured.

If the Receiver reports are enabled an HCI_AMP Receiver Report event shall be generated.

Event Parameters:

Status: *Size: 1 Octet*

Value	Parameter Description
0x00	AMP Test command succeeded
0x01-0xFF	Test command failed. See “Error Codes” on page 339 [Part D].

Test Scenario: *Size: 1 Octet*

Test Scenario for which the test end event has been generated.

Value	Parameter Description

0xXX	0x01 - Transmit single 0x02 – Receive frames 0x03 – 0xFF Reserved

9 REFERENCES

[1] IEEE 802.11-2007 Standard and the following amendments: Amendment 1 (Radio Resource Measurement), Amendment 2 (Fast BSS Transition), Amendment 3 (3650 MHz - 3700 MHz Operation in US), Amendment 4 (Protected Management Frames), and Amendment 5 (Enhancements for Higher Throughput)

[2] ISO/IEC 3166-2

[3] IEEE 802.15.2 Recommended Practice: Coexistence of WPAN with other wireless devices operating in unlicensed frequency bands

[4] Bluetooth SIG Company Identifiers https://www.bluetooth.org/Technical/AssignedNumbers/identifiers.htm

10 LIST OF FIGURES

11 LIST OF TABLES