Logical Link Control and Adaptation Protocol
Outline

• Introduction
• General Operation
• State Machine
• Data Packet Format
• Signaling
• Summary
Introduction

• L2CAP is layered over the Baseband Protocol and resides in the data link layer.

• L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstraction.

• L2CAP permits higher level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.
• The Baseband Protocol defines two link types:
  – Synchronous Connection-Oriented (SCO) links
    • SCO links support real-time voice traffic using reserved bandwidth.
  – Asynchronous Connection-Less (ACL) links:
    • ACL links support best effort traffic.

• The L2CAP specification is defined for only ACL links and no support for SCO links is planned.
L2CAP in Bluetooth Protocol Architecture
L2CAP Functional Requirements

The functional requirements for L2CAP include:

- Protocol Multiplexing
- Segmentation and Reassembly (SAR)
- Group Management
- Quality of Service
Protocol Multiplexing

- L2CAP must support protocol multiplexing because the Baseband Protocol does not support any “type” field identifying the higher layer protocol being multiplexed above it.

- L2CAP must be able to distinguish between upper layer protocol such as the Service Discovery Protocol, RFCOMM, and Telephony Control.

- Protocol multiplexing is supported by defining logical channels.

- Each L2CAP packet received on a channel is directed to the appropriate higher level protocol.
Channel Type

- **Signalling channel:**
  - This channel is used to create and establish connection-oriented data channels and to negotiate changes in the characteristics of these channels.

- **Connection-oriented channel:**
  - Unicast, reliable or unreliable
  - Bi-directional.
  - QoS

- **Connectionless channel:**
  - Multicast, unreliable.
  - Unidirectional.
  - Best effort
  - The channel is used to support a channel ‘group’ where the CID on the source represents one or more remote devices.
General Operation

- **Channel Identifier**
  - Channel identifier (CIDs) are local names representing a logical channel end-point on the device.
  - The same CID is not reused as a local L2CAP channel endpoint for multiple simultaneous L2CAP channels between a local device and some remote device.
CID assignment is relative to a particular device and a device can assign CIDs independently from other devices (unless it need to use any of the reserved CIDs).

<table>
<thead>
<tr>
<th>CID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>Null identifier</td>
</tr>
<tr>
<td>0x0001</td>
<td>Signalling channel</td>
</tr>
<tr>
<td>0x0002</td>
<td>Connectionless reception channel</td>
</tr>
<tr>
<td>0x0003-0x003F</td>
<td>Reserved</td>
</tr>
<tr>
<td>0x0040-0xFFFF</td>
<td>Dynamically allocated</td>
</tr>
</tbody>
</table>

Table 2.1: CID Definitions
### Table: Channel Type and CID Configuration

<table>
<thead>
<tr>
<th>Channel Type</th>
<th>Local CID</th>
<th>Remote CID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection-oriented</td>
<td>Dynamically allocated</td>
<td>Dynamically allocated</td>
</tr>
<tr>
<td>Connectionless data</td>
<td>Dynamically allocated</td>
<td>0x0002 (fixed)</td>
</tr>
<tr>
<td>Signalling</td>
<td>0x0001 (fixed)</td>
<td>0x0001 (fixed)</td>
</tr>
</tbody>
</table>
Group Management

- Group management provides the abstraction of a group of units allowing more efficient mapping between groups and members of the Bluetooth piconet.

- Group communication is connectionless and unreliable.

- Data sent to the ‘group’ channel is sent to all members of the group in a best-effort manner.

- The L2CAP group service interface provides basic group management mechanisms including creating a group, adding members to a group, and removing members from a group.
Segmentation and Reassembly

- The L2CAP maximum transmission unit (MTU) will be exported using an implementation specific service interface.
- It is the responsibility of the higher layer protocol to limit the size of packets sent to the L2CAP layer below the MTU limit.
- Largest Baseband payload is 341 bytes.
- Large L2CAP packets must be segmented into multiple smaller Baseband packets prior to their transmission over air.
- Similarly, multiple received Baseband packets may be reassembled into a single larger L2CAP packet.
Segmentation

- The two L_CH bits defined in the first byte of Baseband payload are used to signal the start and continuation of L2CAP packets.

- L_CH shall be “10” for the first segment in an L2CAP packet and ’01’ for a continuation segment.
Reassembly

- L2CAP implementation must use the length field in the header of L2CAP packets as consistency check and discard any L2CAP packets that fail to match the length field.

- If channel reliability is not needed, packets with improper lengths may be silently discarded.

- For reliable channels, L2CAP implementations must indicate to the upper layer that the channel has become unreliable.
SAR Service in a unit with an HCI
Quality of Service

- The L2CAP connection establishment process allows the exchange of information regarding the quality of service (QoS) expected between two Bluetooth units.

- L2CAP conveys QoS information across channels and provides some admission control to prevent additional channels from violating existing QoS contracts.

- L2CAP implementations are only required to support “Best Effort” service, support for any other service type is optional.
State Machine

• L2CAP Layer Interactions

[Diagram showing the interactions between L2CAP, Upper Protocol Layer, and Lower Protocol (LP) Layer for both Client and Server.]
Event & Action

- The Events causing state transitions, and the actions to be performed in response to events.

- **Connection:**
  - To create a channel between two devices.

- **Configuration:**
  - To establish an initial logical channel transmission contract between two L2CAP entities and also to re-negotiate this contract whenever appropriate.

- **Disconnection:**
  - To terminate an L2CAP channel.
**Timer Event**

- **RTX:**
  - The Response Timeout expired (RTX) timer is used to terminate the channel when the remote endpoint is unresponsive to signaling requests.
  
  - The value of this timer is implemented-dependent but the minimum initial value is *1 second* and the maximum initial value is *60 seconds*.

- If the initial timer expires, a duplicate Request message may be sent or the channel identified in the request may be disconnected.

- If a duplicate Request message is sent, the RTX timeout value must be reset to a new value at least double the previous value.
Timer Event

- **ERTX:**
  - The Extended Response Timeout expired (ERTX) timer is used in place of the RTX timer when it is suspected the remote endpoint is performing additional processing of a request signal.
  
  - This timer is started when the remote endpoint responds that a request is pending.
  
  - The value of this timer is implementation-dependent but the minimum initial value is 60 seconds and the maximum initial value is 300 seconds.
Channel Operational States

- CLOSED
- W4_L2CAP_CONNECT_RSP
- W4_L2CA_CONNECT_RSP
- CONFIG
- OPEN
- W4_L2CAP_DISCONNECT_RSP
- W4_L2CA_DISCONNECT_RSP
• **CLOSED**
  
  - In this state, there is no channel associated with this CID.
  
  - This is the only state when a link level connection (Baseband) may not exist.
  
  - Link disconnection forces all other states into the CLOSED state.
• **W4_L2CAPCONNECT_RSP**
  - In this state, the CID represents a local end-point and an L2CAP_ConnectReq message has been sent referencing this endpoint and it is now waiting for the corresponding L2CAP_ConnectRsp message.

• **W4_L2CACONNECT_RSP**
  - In this state, the remote end-point exists and an L2CAP_ConnectReq has been received by the local L2CAP entity. An L2CAP_ConnectInd has been sent to the upper layer and the part of the local L2CAP entity processing the received L2CAP_ConnectReq waits for the corresponding response.
- **CONFIG**
  - In this state, the connection has been established but both sides are still negotiating the channel parameters.
  - The Configuration state may also be entered when the channel parameters are being renegotiated.
  - Prior to entering the CONFIG state, all outgoing data traffic should be suspended since the traffic parameters of the data traffic are to be renegotiated. Incoming data traffic must be accepted until the remote channel endpoint has entered the CONFIG state.
• **OPEN**
  – In this state, the connection has been established and configured, and data flow may proceed.

• **W4_L2CAP_DISCONNECT_RSP**
  – In this state, the connection is shutting down and an `L2CAP_DisconnectReq` message has been sent. This state is now waiting for the corresponding response.

• **W4_L2CA_DISCONNECT_RSP**
  – In this state, the connection on the remote endpoint is shutting down and an `L2CAP_DisconnectReq` message has been received. An `L2CAP_DisconnectInd` has been sent to the upper layer. This state is now waiting for the corresponding response from the upper the layer.
Data Packet Format

• Connection-Oriented Channel

• Length:
  – Indicates the size of information payload in bytes.
  – The length of an information payload can be up to 65535 bytes.

• Channel ID:
  – The channel ID identifies the destination channel endpoint of the packet.

[Diagram of L2CAP Header with fields for Length, Channel ID, and Information (payload)]
• **Connectionless Data Channel:**

  ![Connectionless Data Channel Diagram]

  - **Length**
    - Indicates the size of information payload plus the PSM field in bytes, excluding the length of the L2CAP header.

  - **Channel ID**
    - (0x0002) reserved for connectionless traffic.
• The PSM (Protocol/Service Multiplexer) value definitions are specific to L2CAP and assigned by the Bluetooth SIG.

• The dynamically assigned values may be used to support multiple implementations of a particular protocol, e.g., RFCOMM, residing on top of L2CAP or for prototyping an experimental protocol.

<table>
<thead>
<tr>
<th>PSM value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0001</td>
<td>Service Discovery Protocol</td>
</tr>
<tr>
<td>0x0003</td>
<td>RFCOMM</td>
</tr>
<tr>
<td>0x0005</td>
<td>Telephony Control Protocol</td>
</tr>
<tr>
<td>&lt;0x1000</td>
<td>RESERVED</td>
</tr>
<tr>
<td>[0x1001-0xFFFF]</td>
<td>DYNAMICALLY ASSIGNED</td>
</tr>
</tbody>
</table>

*Table 5.4: Defined PSM Values*
Signaling

- This section describes the signalling commands passed between two L2CAP entities on remote devices.
- All signalling commands are sent to CID 0x0001.
- Multiple commands may be sent in a single (L2CAP) packet.
Command Format

- **Code:**
  - Identifies the type of command.

- **Identifier:**
  - Helps matching a request with the reply.
  - Identifiers should not be recycled until a period of 360 seconds has elapsed from the initial transmission of the command using the identifier.
## Signaling Command Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>RESERVED</td>
</tr>
<tr>
<td>0x01</td>
<td>Command reject</td>
</tr>
<tr>
<td>0x02</td>
<td>Connection request</td>
</tr>
<tr>
<td>0x03</td>
<td>Connection response</td>
</tr>
<tr>
<td>0x04</td>
<td>Configure request</td>
</tr>
<tr>
<td>0x05</td>
<td>Configure response</td>
</tr>
<tr>
<td>0x06</td>
<td>Disconnection request</td>
</tr>
<tr>
<td>0x07</td>
<td>Disconnection response</td>
</tr>
<tr>
<td>0x08</td>
<td>Echo request</td>
</tr>
<tr>
<td>0x09</td>
<td>Echo response</td>
</tr>
<tr>
<td>0x0A</td>
<td>Information request</td>
</tr>
<tr>
<td>0x0B</td>
<td>Information response</td>
</tr>
</tbody>
</table>
**Command Reject (Code 0x01)**

- A Command Reject packet is sent in response to a command packet with an *unknown command code* or when sending the corresponding is inappropriate.

- **Reason:** describes why the Request packet was rejected.

<table>
<thead>
<tr>
<th>Reason value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>Command not understood</td>
</tr>
<tr>
<td>0x0001</td>
<td>Signalling MTU exceeded</td>
</tr>
<tr>
<td>0x0002</td>
<td>Invalid CID in request</td>
</tr>
<tr>
<td>Other</td>
<td>Reserved</td>
</tr>
</tbody>
</table>
• **Data:** (depends on the Reason Code)

<table>
<thead>
<tr>
<th>Reason value</th>
<th>Data Length</th>
<th>Data value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>0 octets</td>
<td>N/A</td>
</tr>
<tr>
<td>0x0001</td>
<td>2 octets</td>
<td>Actual MTU</td>
</tr>
<tr>
<td>0x0002</td>
<td>4 octets</td>
<td>Requested CID</td>
</tr>
</tbody>
</table>

• If the Reason code is
  – 0x0000: No data field is used.
  – 0x0001: the 2-octet Data field represents the MTU that the sender of this packet can accept.
  – 0x0002: the 4-octet data field on the command reject will contain the local and remote channel endpoints of the disputed channel.
Connection Request (Code 0x02)

- Connection Request packets are sent to create a channel between two devices.

- Source CID (SCID):
  - Represents a channel endpoint on the device sending the request and receiving the response.

<table>
<thead>
<tr>
<th>Code=0x02</th>
<th>Identifier</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSM</td>
<td>Source CID</td>
<td></td>
</tr>
</tbody>
</table>
Connection Response (Code 0x03)

- When a unit receives a Connection Request packet, it must send a Connection Response packet.

- **Destination Channel Identifier (DCID):**
  - Represents the channel end-point on the device sending this Response packet.

- **Source Channel Identifier (SCID):**
  - Represents the channel end-point on the device receiving this Response packet.
Connection Response (Code 0x03)

- **Result:** This field indicates the outcome of the connection request.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>Connection successful.</td>
</tr>
<tr>
<td>0x0001</td>
<td>Connection pending</td>
</tr>
<tr>
<td>0x0002</td>
<td>Connection refused – PSM not supported.</td>
</tr>
<tr>
<td>0x0003</td>
<td>Connection refused – security block.</td>
</tr>
<tr>
<td>0x0004</td>
<td>Connection refused – no resources available.</td>
</tr>
<tr>
<td>Other</td>
<td>Reserved.</td>
</tr>
</tbody>
</table>

- **Status:** Only defined for Result = Pending.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>No further information available</td>
</tr>
<tr>
<td>0x0001</td>
<td>Authentication pending</td>
</tr>
<tr>
<td>0x0002</td>
<td>Authorization pending</td>
</tr>
<tr>
<td>Other</td>
<td>Reserved</td>
</tr>
</tbody>
</table>
Configuration Request (Code 0x04)

- Configuration Request packets are sent to establish an initial logical link transmission contract between L2CAP entities and also to renegotiated this contract whenever appropriate.

- Each configuration parameter is one-directional.

- Even if all default values are acceptable, a Configuration Request packet with no options MUST be sent.
• **Flags:**

  - C - More configuration requests will follow when set to 1.
  - The flag indicates the the remote device should not enter OPEN state after agreeing to these parameters because more parameter negotiations are being sent.

• **Options:**

  - The list of the parameters and their values to be negotiated.
  - Configuration Request may contain no options
Configuration Response (Code 0x05)

- Each configuration parameter value in a Configuration Response reflects an ‘adjustment’ to a configuration parameter value that has been sent.

- **Flags:**
  - More configuration responses will follow when set to 1
Configuration Response (Code 0x05)

- **Result:**

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>Success</td>
</tr>
<tr>
<td>0x0001</td>
<td>Failure – unacceptable parameters</td>
</tr>
<tr>
<td>0x0002</td>
<td>Failure – rejected (no reason provided)</td>
</tr>
<tr>
<td>0x0003</td>
<td>Failure – unknown options</td>
</tr>
<tr>
<td>Other</td>
<td>RESERVED</td>
</tr>
</tbody>
</table>

- **Configuration Options:**
  - This field contains the list of parameters being negotiated.
  - On an unacceptable parameters failure, the rejected parameters should be sent in the response with the values that would have been accepted if sent in the original request.
**Configuration Parameter Options**

- Options are transmitted in the form of information elements comprised an option type, an option length, and one or more option data fields.
Maximum Transmission Unit (MTU)

- This option specifies the payload size the sender is capable of accepting. (the largest L2CAP packet payload)

- The remote device in its positive Configuration Response will include the actual MTU to be used on this channel for traffic flowing into the local device which is minimum \{MTU in Config Req, outgoing MTU capability of remote device\}. 
Flush Timeout Option

- This option is used to inform the recipient of the amount of time the original’s link controller/link manager will attempt to successfully transmit an L2CAP segment before giving up and flushing the packet.

**Flush Timeout:**
- This value represents units of time measured in milliseconds.
- The value of 1 implies no retransmission at the Baseband level should be performed since the minimum polling interval is 1.25ms.
- The value of all 1’s indicates an infinite amount of retransmissions.
- When included in a Configuration Request, this option describe the outgoing traffic flow from the device sending the request to the device receiving it.
- When included in a positive Configuration Response, this option describes the incoming traffic flow agreement as seen from the device sending the response.
• **Flags:**
  – Reserved for future use and must be set to 0.

• **Service type:**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>No traffic</td>
</tr>
<tr>
<td>0x01</td>
<td>Best effort (Default)</td>
</tr>
<tr>
<td>0x02</td>
<td>Guaranteed</td>
</tr>
<tr>
<td>Other</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

– L2CAP implementations are only required to support ‘Best Effort’ service, support for any other service type is optional.
Disconnection Request (Code 0x06)

- Terminating an L2CAP channel requires that a disconnection request packet be sent and acknowledged by a connection response packet.

- Once a Disconnection Request is issued, all incoming data in transit on this L2CAP channel will be discarded and any new additional outgoing data is not allowed.
Disconnection Response (Code 0x07)

- Disconnection responses should be sent in response to each disconnection request.

- The DCID and the SCID (which are relative to the sender of the request), and the Identifier fields must match those of the corresponding disconnection request command.

- If the CIDs do not match, the response should be silently discarded at the receiver.
ECHO Request (Code 0x08)

- Echo request are used to solicit a response from a remote L2CAP entity. These requests may be used for testing the link or passing vendor-specific information using the optional data field.
• The optional and implementation-dependent data field may contain the contents of the data field in the Request, different data, or no data at all.
Information Request (Code 0x0A)

- Information requests are used to solicit implementation-specific information from a remote L2CAP entity.

- **InfoType:**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0001</td>
<td>Connectionless MTU</td>
</tr>
<tr>
<td>Other</td>
<td>Reserved</td>
</tr>
</tbody>
</table>
Information Response (Code 0x0B)

- Info Type: Same value sent in the request.
- Result:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>Success</td>
</tr>
<tr>
<td>0x0001</td>
<td>Not supported</td>
</tr>
<tr>
<td>Other</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

- Data:

<table>
<thead>
<tr>
<th>InfoType</th>
<th>Data</th>
<th>Data Length (in octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0001</td>
<td>Connectionless MTU</td>
<td>2</td>
</tr>
</tbody>
</table>
Summary

- The Logical Link Control and Adaptation Protocol (L2CAP) is one of two link level protocols running over the Baseband.

- L2CAP is responsible for higher level protocol multiplexing, segmentation and reassembly, group management, and conveying quality of service information to link level.