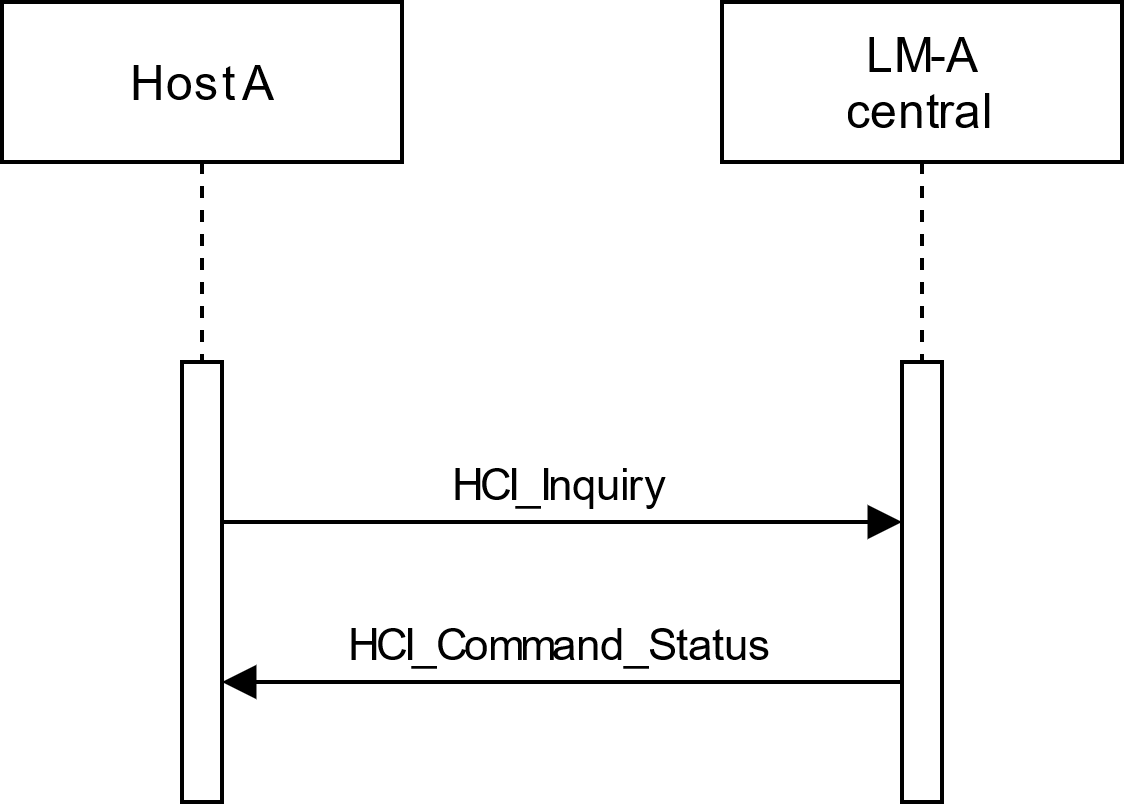
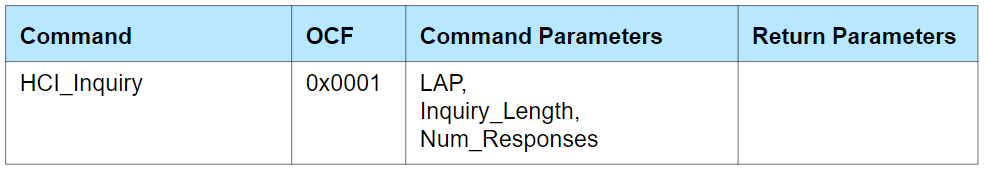
# ACL Connection SetUp

本文档描述ACL连接的建立，从Inquiry到连接建立分为10个步骤。

## Step 0. Inquiry



在准备建立连接之前，Host A首先会检测和收集邻近的设备的信息，通过给LM-A发送一个**HCI\_Inquiry**命令（P1846），来使得Controller进入Inquiry Mode。

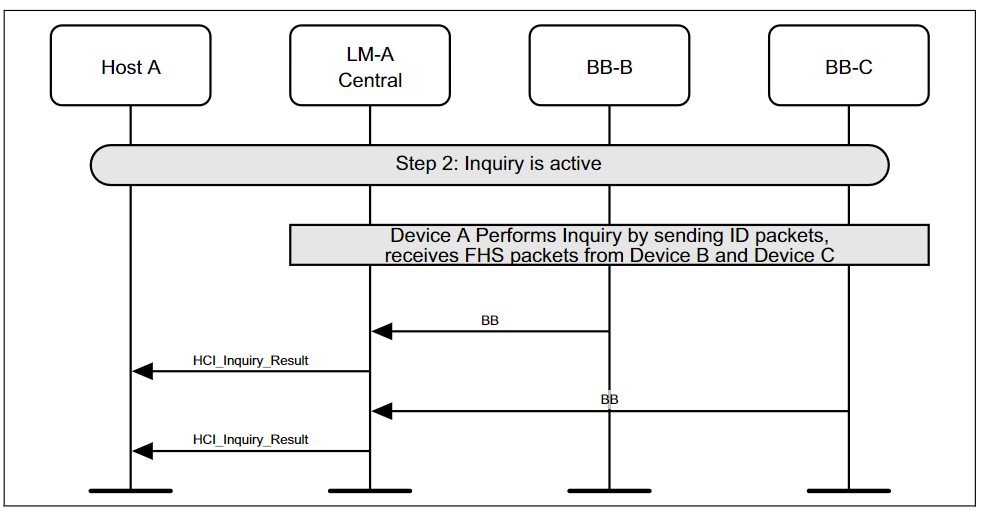


**LAP**：查询程序进行查询时应从中导出查询访问码的LAP

**Inquiry\_Length**：添加到Extended\_Inquiry\_Length中的Inquiry\_length参数指定查询模式的总持久性，并且当此时间到期时，查询将停止。

**Num\_Responses**：指定在停止查询之前可以收到的响应数量。

在LM-A开启Inquiry过程之后会给Host A发送HCI\_Command\_Status事件。

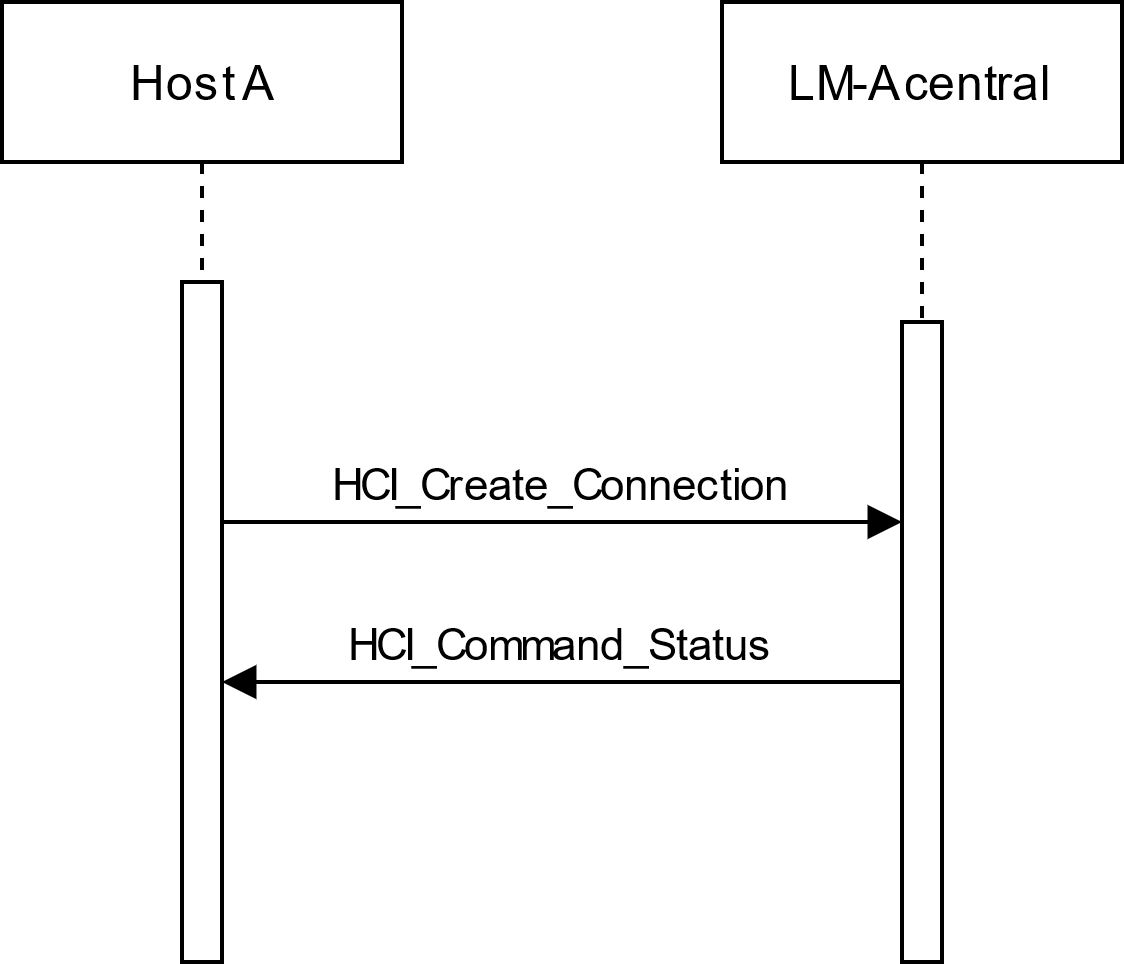


控制器LM-A在使用指定的Inquiry Access code和Inquiry Length启动basebond查询过程，在接收到了Inquiry response之后，LM-A将会提取所需的信息，使用一个或者多个事件将所查询到的周围的设备的信息返回给主机，这个event为**HCI\_Inquiry\_Result**（P）。

同功能的事件还有：HCI\_Inquiry\_Result\_with\_RSSI和HCI\_Extended\_Inquiry\_Result。

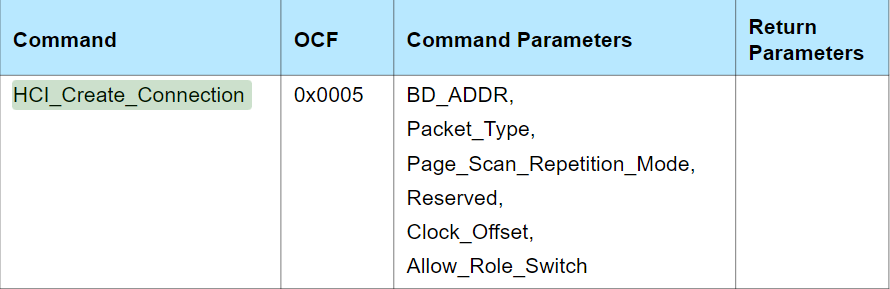
## Step 1. Create Connection（Page）

**Host A requests a connection to Device B**



(1）希望和外设B建立连接的device A的Host端会首先向A的Controller发送一个命令：

**HCI\_Create\_Connection命令**（P1853），之后Controller A会进入**Page**状态。



**BD\_ADDR**：请求连接的远程device的地址

**Packet\_Type: Link Manager：**可以使用的包类型

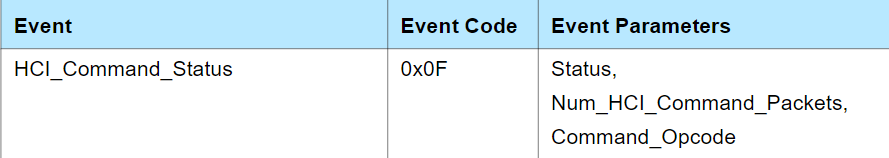
**Page\_Scan\_Repetitio\_Mode**：使用BD\_ADDR的远端设备所支持的Page Scan Repetition模式，此模式信息可以从之前的inquiry过程中获取，也可以从事件event：HCI\_Page\_Scan\_Repetition\_Mode\_Change中获取。

**Clock\_Offset：**远程BD\_ADDR设备与本设备的clock之间的offset。

**Allow\_Role\_Switch：**接受/拒绝远端设备的角色切换请求（在Controller 返回一个连接完成事件：HCI\_Connection\_Complete之前）

(2) 当BR/EDR控制器接收到HCI\_Create\_Connection命令时，BR/EDR控制器会发送event：HCI\_COMMAND\_STATUS到主机。

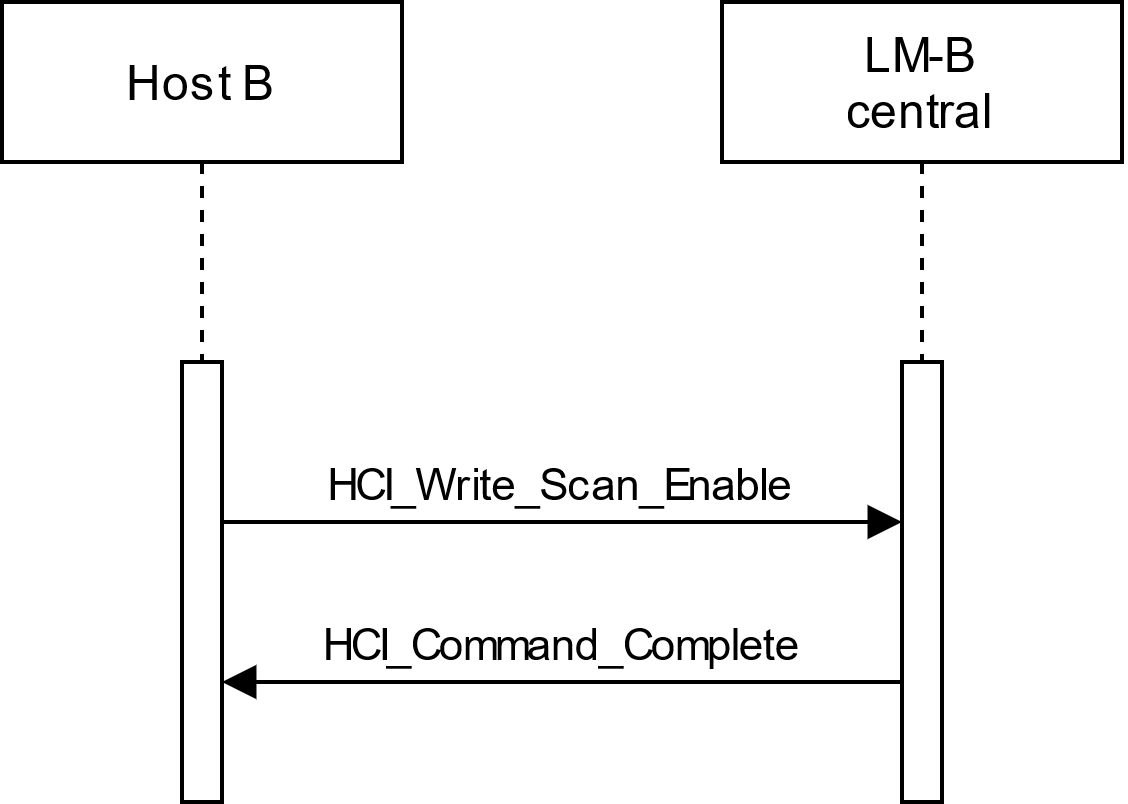
**HCL\_Command\_Status**  事件 (P2190)



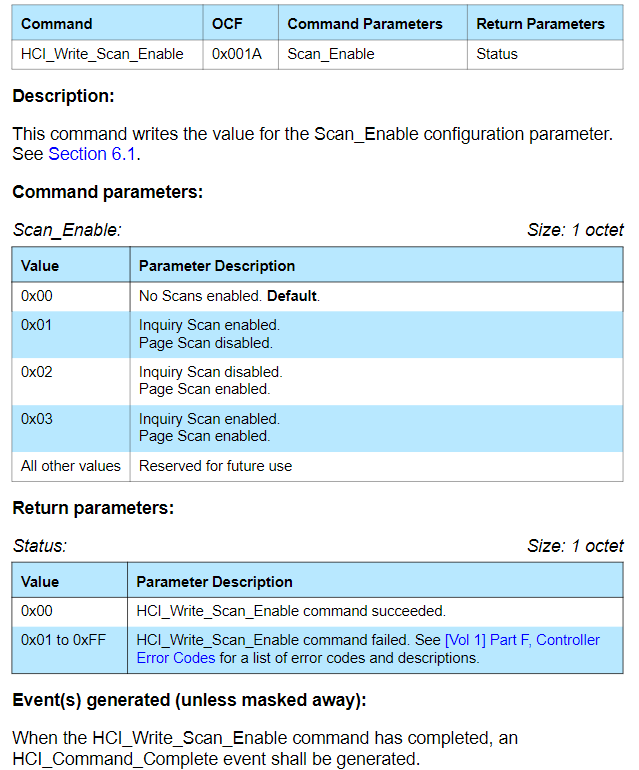
HCI\_COMMAND\_STATUS事件用于指示命令Command\_Opcode参数所描述的命令已接收到，并且控制器当前正在执行此命令的任务。需要此事件来提供异步操作的机制，这避免了主机等待命令完成的需求。

如果命令不能开始执行(可能发生了参数错误，或者命令当前不允许)，Status事件参数将包含相应的错误代码，并且没有完整的事件将跟随，因为命令没有启动。

## Page Scan



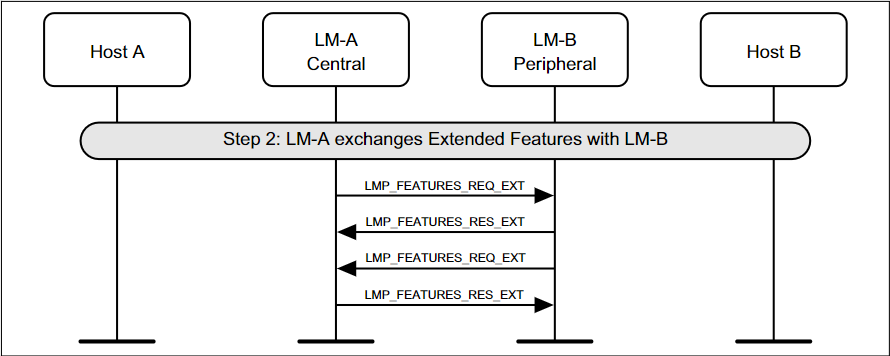
在触发而来Page Scan流程之后，Host B会向Controller B发送**HCI\_Write\_Scan\_Enable**（P1997）命令。



这个命令写入Scan\_Enable配置参数，参数Scan\_Enable可以选择Inquiry Scan和Page Scan的enable 或者 disable。返回参数表明这个命令执行的成功与否。

## Step 2. Features exchange (optionally)

**Link Mangaer可能会决定交换一些特性，此步骤为可选，非必须步骤**。



LM-A向LM-B发送LMP\_FEATURES\_REQ\_EXT

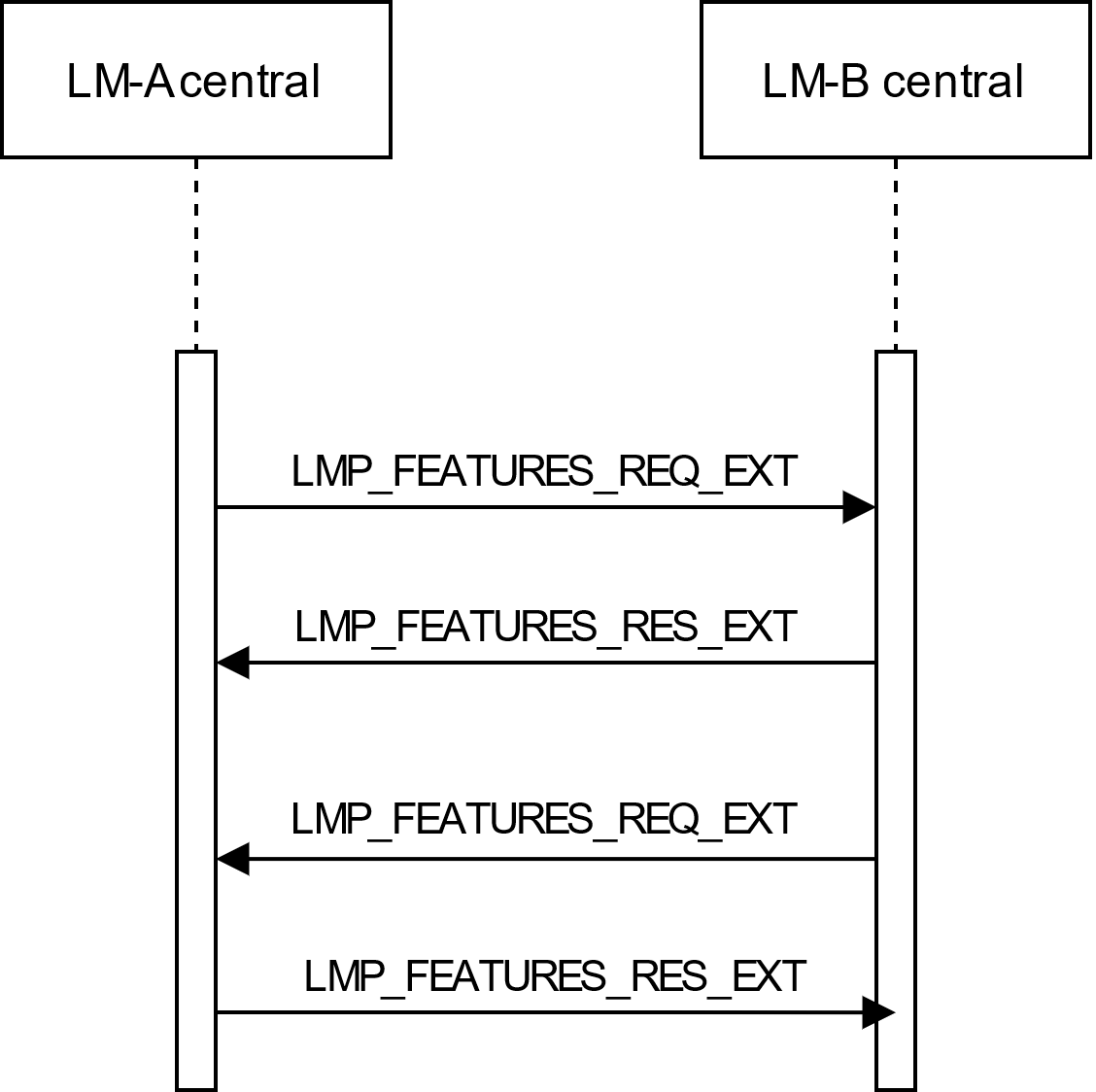
LM-B向LM-A返回LMP\_FEATURES\_RES\_EXT 和LMP\_FEATURES\_REQ\_EXT

最后LM-A发送LMP\_FEATURES\_RES\_EXT 给 LM-B。

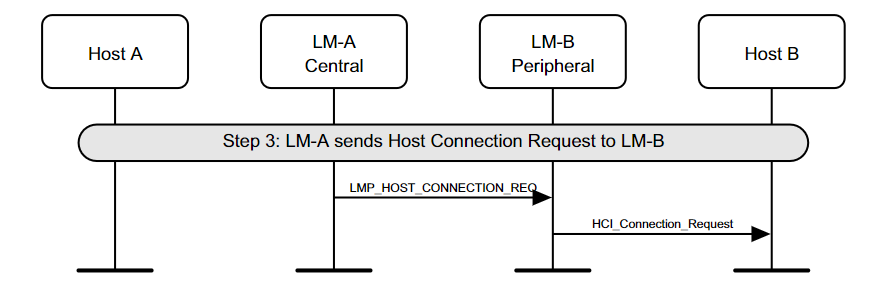
(P662)

Request for extended features：通过发送LMP\_Features\_REQ\_PDU，可以在成功的基带Page过程之后的任何时候请求受支持的特性。

接收设备接收到LMP\_FEATURES\_REQ\_PDU后，应返回LMP\_FEATURES\_RES\_PDU。

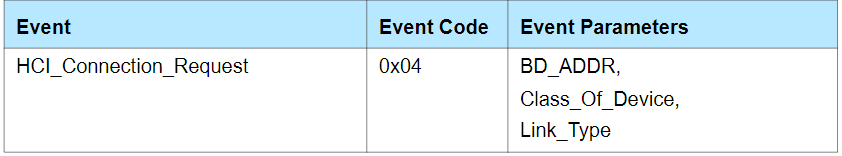


## Step 3. Connection Request



在step2之后，LM-A会发送PDU请求给LM-B，表示HostA想和HostB建立连接，这类PDU叫做**LMP\_HOST\_CONNECTION\_REQ** （P599）**。**

LM-B收到了之后会给HostB发送一个事件：**HCI\_Connection\_Request**（P2172），指示一个新的传入BR/EDR连接正在尝试建立。



**BD\_ADDR**：请求连接的远程device的地址

**Class\_Of\_Device：**请求连接的设备的类型

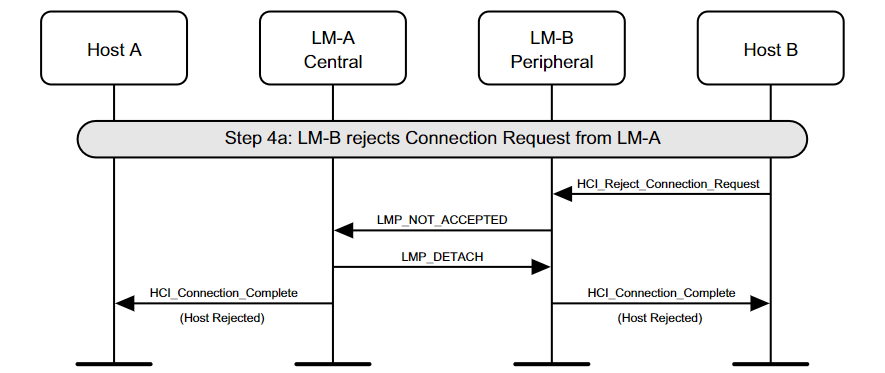
**Link\_Type: 1）0x00 : SCO；2）0x01：ACL；3）0x02：eSCO; 4）others：reserved**

然后，外围设备LM-B将确认连接是正常的，如果是的话，判断选择哪个角色更好。

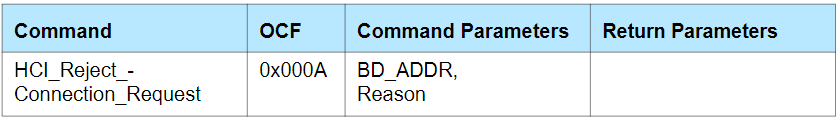
## Step 4. Role Switch (optionally)

### Step 4a. Host B rejects this connection

情况a：Host B 拒绝了Host A的Host连接请求，此时连接将会终止。



首先Host B会发送一个拒绝连接的命令：**HCI\_Reject\_Connection\_Request。**（P1862）

****

**BD\_ADDR**：拒绝的请求连接的远程device的地址

**Reason：** 主机拒绝错误代码error codes

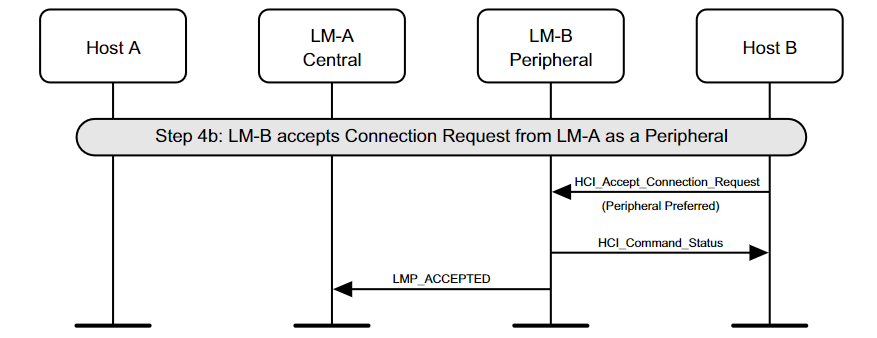
在控制器B接收到来自Host的**HCI\_Reject\_Connection\_Request**后，会将事件HCI\_COMMAND\_STATUS发送到Host。之后，将**HCI\_Connection\_complete**事件发送到Host B表示连接结束。

同时，LM-B将向LM-A发送**LMP\_NOT\_ACCEPTED** （P584）PDUs作为对之前从LM-A那里收到的PDU（step 3）：**LMP\_HOST\_CONNECTION\_REQ**的respond message。当然，**LMP\_NOT\_ACCEPTED**中包含操作码(opcode)表示将要拒绝哪个message，同时还包含error\_code表示拒绝原因。

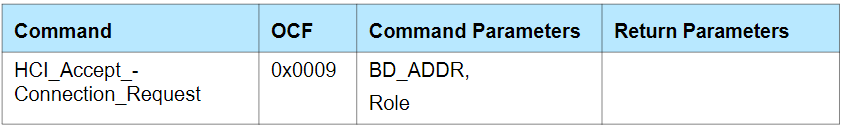
LM-A在收到**LMP\_NOT\_ACCEPTED** PDU后会发送PDU：**LMP\_DETACH**给LM-B，指示蓝牙设备A和蓝牙设备B的连接断开，其中包含的内容是error\_code错误码参数，用于通知另一方断开连接的原因。之后，LM-A将**HCI\_Connection\_complete**事件发送到HostA表示连接结束。

### Step 4b. Host B accepts this connection

情况b：Host B 同意了Host A的Host连接请求，此时连接将会建立。



HostB将向LM-B发送同意连接的命令：**HCI\_Accept\_Connection\_Request**（P1860）。



**BD\_ADDR**：同意的请求连接的远程device的地址

**Role：**想要在连接中成为的角色

1）0x00：成为Central，之后LM会进行Role Switch

2）0x01：成为Peripheral，之后LM不会进行Role Switch

之后链接管理器LM-B将决定如何建立新连接。这将由设备的当前状态、其piconet和要连接设备的状态决定。Role命令参数允许主机指定链接管理器是否需要请求角色切换并成为此连接的central。这是首选项，而不是要求。如果角色切换失败，那么连接仍将被接受，并且HCI\_Role\_Discovery命令将反映当前的角色设定。

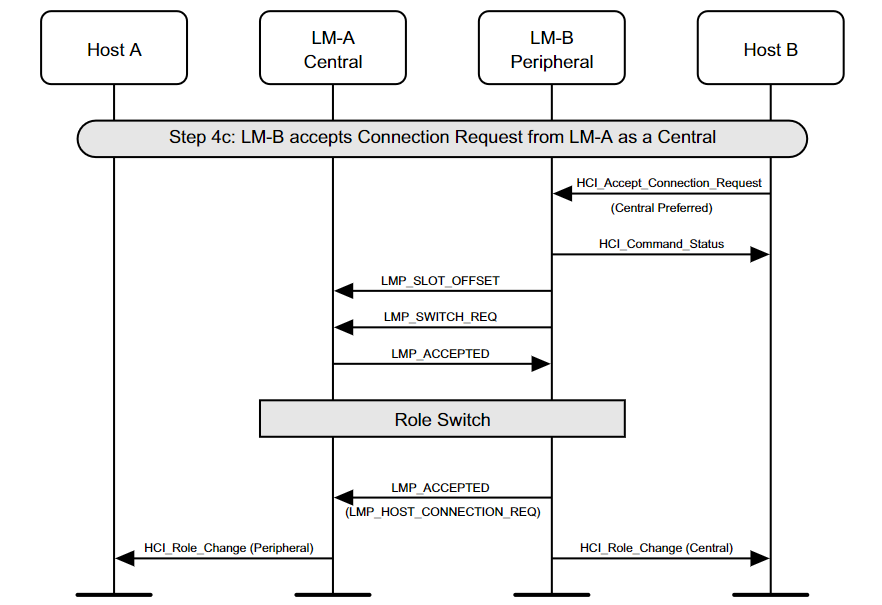
如果角色切换失败，资源不足，则链接管理器可以终止连接。接受连接的决定应该在本地蓝牙模块上的连接接受超时之前完成。

BR/EDR的Controller开始**设置连接**时，发送HCI\_COMMAND\_STATUS事件到Host端。

同时，LM-B将向LM-A发送**LMP\_ACCEPTED** （P584）PDUs作为对之前从LM-A那里收到的PDU（step 3）：**LMP\_HOST\_CONNECTION\_REQ**的respond message。当然，**LMP\_ACCEPTED**中包含操作码(opcode)表示将要接受哪个message。

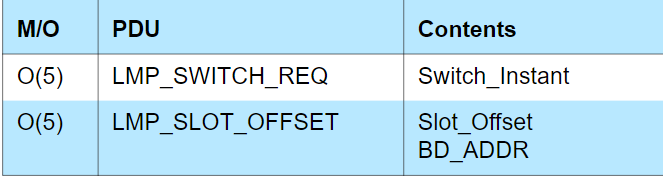
### Step 4c. Host B preference of being a Central (optionally)

情况c：在情况b中，设备B想要进行Role Switch，即**在此次连接中成为central**。

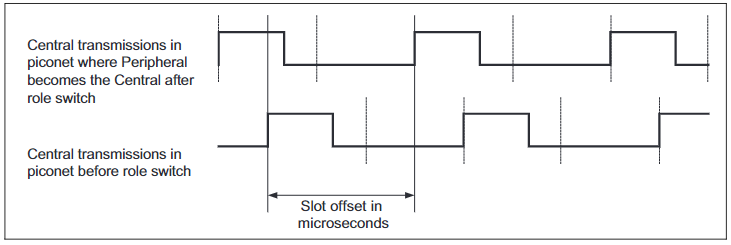


当LM-B收到的**HCI\_Accept\_Connection\_Request**命令中参数Role值是0x00时，表示Host B想要进行role switch，会给LM-A发送PDU：

**LMP\_SLOT\_OFFSET。**（P664） 和 **LMP\_SWITCH\_REQ**。



Slot\_Offset是指从当前微微网（A是central）的中心传输开始到下一个微微网(B成为central)的中心传输开始的时间(以微秒为单位)，BD\_ADDR为B的地址。



只有当ACL逻辑传输处于Active模式、加密被停止或暂停、同一物理链路上所有同步逻辑传输被禁用时，才会发送LMP\_SWITCH\_REQ，参数Switch\_Instant指定TDD switch的瞬间。为central的clock值（A的），对两个设备都可用，此讯息由B发送，且在未来必须是一个至少max{ 2\*, 32 slots }的值。这个瞬变应在当前时钟值的12小时内，避免clock wrap。

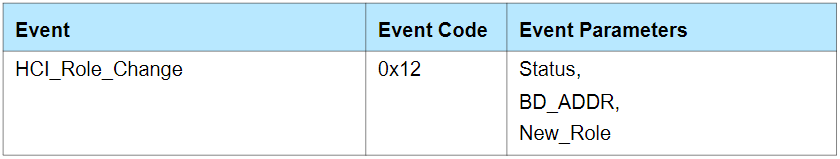
如果响应的设备A作为central接受这个角色转换，就会响应 **LMP\_ACCEPTED** PDU，且开始BaseBond 角色切换过程。如果不接受，则会发送**LMP\_NOT\_ACCEPTED** PDU。

具体操作：当LM-A在接收到LMP\_SWITCH\_REQ时，将Switch\_Instant与中央时钟的当前值进行比较。如果它在过去，那么表示交换瞬间已经过去，就返回一个LMP\_NOT\_ACCEPTED PDU，错误码为Error\_Code Instant Passed (0x28)。如果是在未来(即还没发生)，则返回一个LMP\_ACCEPTED PDU，假设角色切换被接受，并在切换瞬间开始一个计时器。当该定时器到点时，角色切换将被启动。

注：角色切换，无论成功还是失败，都不会影响链路管理器以及ACL-C和ACL-U逻辑链路的状态，除非有明确的说明。

在角色转换完成之后，LM-B会给LM-A发送**LMP\_HOST\_CONNECTION\_REQ**，即step 3。

同时LM-A和LM-B分别给Host A和Host B发送 **HCI\_Role\_Change** 事件(P2194)。



**HCI\_Role\_Change**事件用于指示与特定连接有关的当前BR/EDR控制器**角色已更改**。

**Status**：

1）0x00 ： Role changed successed

2）0x01 – 0xFF：Role change failed

**BD\_ADDR**：已经完成角色变更的那个设备的地址

**New\_Role**：

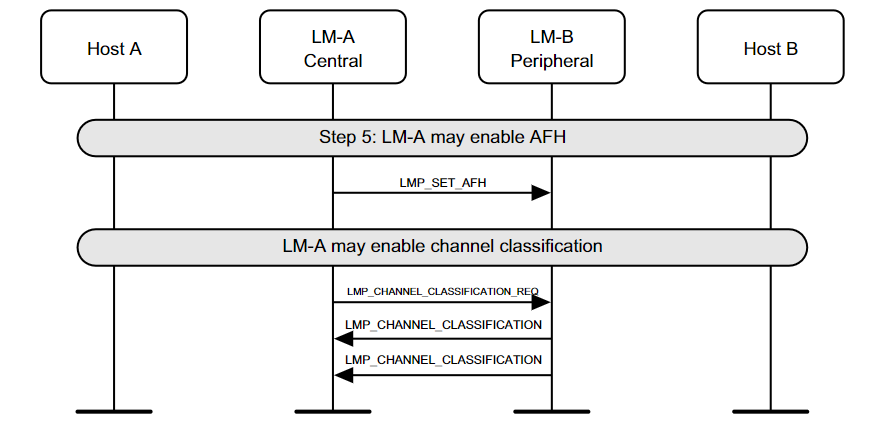
1）0x00 ： 目前是BD-ADDR设备的central

2）0x01 ： 目前是BD-ADDR设备的peripheral

当HCI\_Switch\_Role命令完成时，该事件还会在本地控制器上生成，因为没有要求更改或发生错误。如果尝试了基带角色开关但失败了，则控制器可能会生成事件。

## Step 5. Adaptive Frequency Hopping(AFH) (optionally)

**开启自适应跳频（可选，非必须操作）**

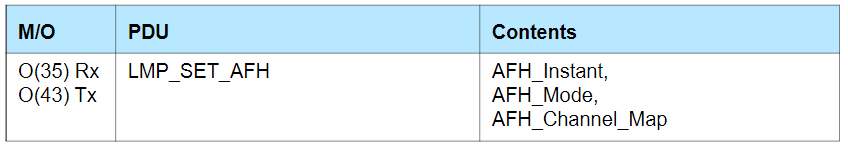


在特征交换完成且确定AFH支持之后，central可以enable AFH 和 channel classification。

LM-A通过发送 **LMP\_SET\_AFH** PDU，来enable AFH。

AFH用于提高物理链路在存在干扰时的性能，同时减少物理链路对ISM频段内其他设备的干扰。AFH只能在连接状态下使用。

LMP\_SET\_AFH (P604)



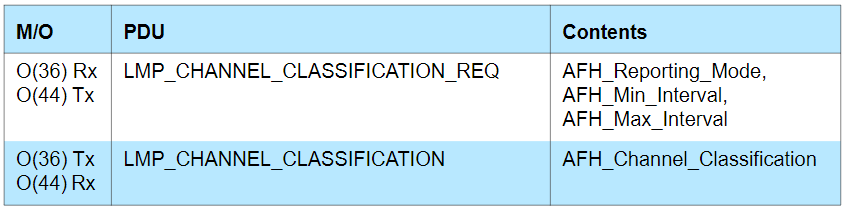
**AFH\_Instant**：指定AFH生效的时间瞬间，为central的clock值（已经sync），由Central选择，且在未来必须是一个至少max{ 6\*, 96 slots }的值。AFH瞬变应在当前时钟值的12小时内。

**AFH\_Mode**：指定启用或者禁用AFH。

**AFH\_Channel\_Map**：指定启用AFH时应使用的信道集合。

同时，central可以通过PDU：**LMP\_CHANNEL\_CLASSIFICATION\_REQ**控制AFH\_reporting\_mode，peripheral也将使用PDU：**LMP\_CHANNEL\_CLASSIFICATION**报告自身的信道分类和情况。

（P607）



**AFH\_Reporting\_Mode**：确定外设处于启用或禁用状态。

**AFH\_Min\_Interval**：定义从发送上一个**LMP\_CHANNEL\_CLASSIFICATION**命令到发送下一个LMP\_CHANNEL\_CLASSIFICATION PDU的最小时间间隔。

**AFH\_Max\_Interval**：定义从外设检测到的信道分类变化到它生成LMP信道分类PDU之间的最大时间。同时AFH最大间隔应等于或大于AFH最小间隔。

当发生下列任何一种情况时，AFH\_reporting\_mode隐式设置为禁用状态：  
• Establishment of a connection at the Baseband level  
• Role switch  
• Entry to Hold mode operation

当发生以下任何情况时，AFH\_reporting\_mod隐式恢复到以前的值：

• Exit from Hold mode  
• Failure of role switch

**AFH\_Channel\_Classification：uint2 [40]** 表示信道质量的好、坏或未知

The value of each element indicates:

0 = unknown

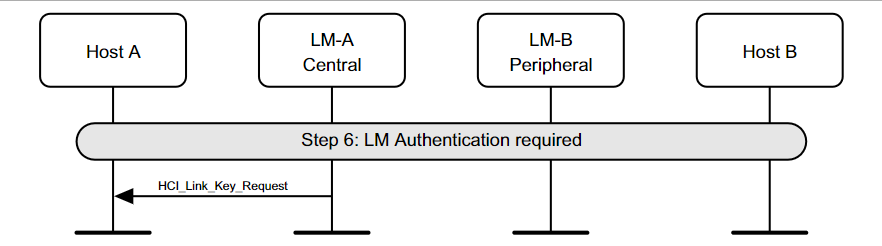
1 = good

2 = reserved for future use

3 = bad

## Step 6. Security (optionally)

**开启安全认证，可选，非必须操作。**



LM-A可以开启认证请求，向Host A发送 **HCI\_Link\_Key\_Request** 事件（P1764）。

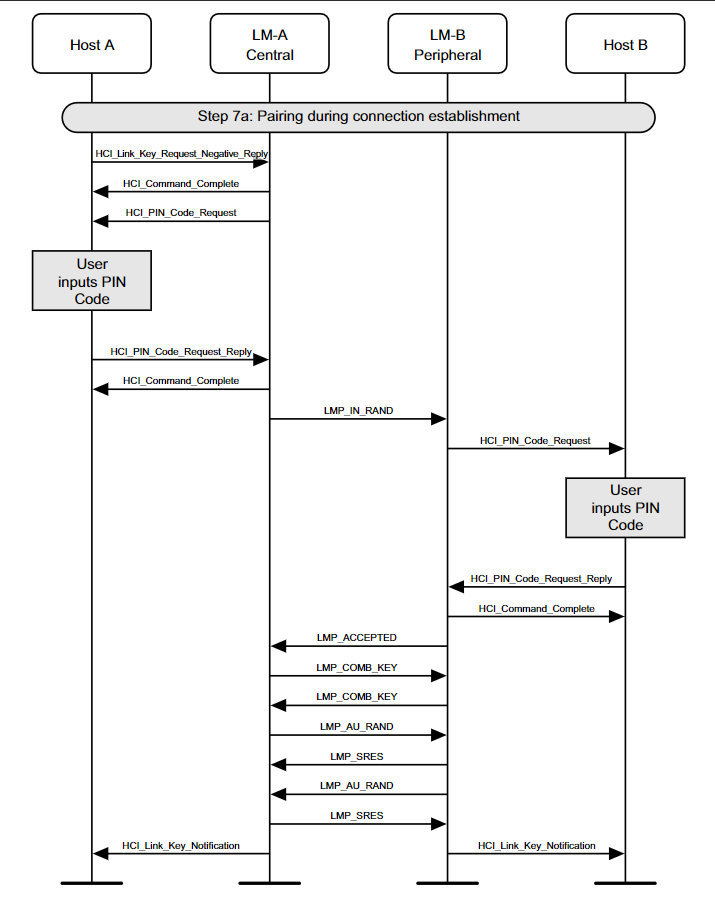
HCI\_Link\_Key\_Request事件用于标识与BD\_ADDR中指定的设备的连接需要Link Key。

## Step 7. Two work (Optionally)

### Step 7a. Pairing (Optionally)

如果高层控制要求认证，且待连接的设备没有统一的link key，则采用pairing过程。

**配对过程，可选，非必须操作**

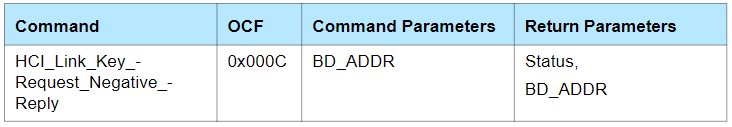


LM-A将通过**HCI\_Link\_Key\_Request** 的event向Host A请求此连接的link key，如果得到了否定的答复（**HCI\_Link\_Key\_Request\_Negative\_Reply**），那么将要求一个PIN码。

这个PIN码将在连接的两边被请求，并根据这个PIN码进行身份验证。

最后一步是将这个连接的新link key传递给主机，以便它可以存储它以备将来的连接。

**HCI\_Link\_Key\_Request\_** **Negative\_Reply**（P1865）



**BD\_ADDR**： Link Key所在设备的地址

返回值：

**Status**：0x00表示**HCI\_Link\_Key\_Request\_** **Negative\_Reply**命令成功，其他表示失败。

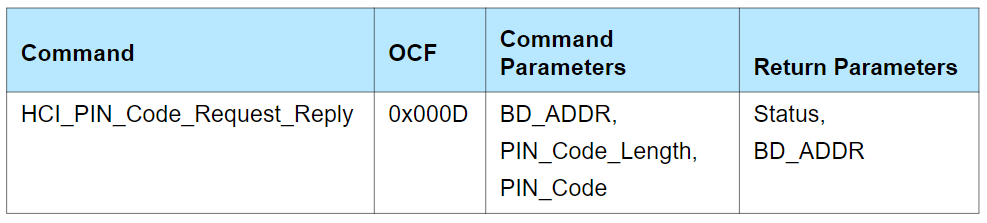
**BD\_ADDR**：执行HCI\_Link\_Key\_Request\_Negative\_Reply命令后设备的地址。

在得到否定的答复之后。LM-A会发起一个请求PIN码的事件：**HCI\_PIN\_Code\_Request**

（P1766）。表示请求一个PIN code，为了连接来创建一个新的link key。

那么对于这个请求PIN码的事件，Host A当然也有回应，不管是回应成功还是回应不成功。

1）回应成功：**HCI\_PIN\_Code\_Request\_Reply** 命令 （P1867）



此命令回应Controller的事件，同时指定连接使用的PIN码。

**BD\_ADDR**：PIN码所在的设备地址。

**PIN\_Code\_Length**：要使用的PIN码的长度（单位是字节）0x01 to 0x10

**PIN\_Code**：待连接设备的PIN码，为字符串，最大128bits。

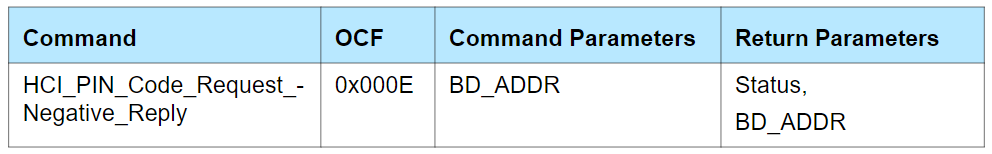
返回值：

**Status**：表示本命令成功与否。

**BD\_ADDR**：执行HCI\_PIN\_Code\_Request\_Reply命令后设备的地址。

同时，**HCI\_PIN\_Code\_Request\_Reply**命令完成后，将生成HCI\_COMMAND\_COMPLETE事件。

2）回应不成功：**HCI\_PIN\_Code\_Request\_Negative\_Reply** 命令 （P1869）



当主机无法指定用于连接的PIN代码时，使用此命令回复，当然地此命令将导致远程设备的配对（Pairing）请求失败。

**BD\_ADDR**：PIN码所在的设备地址。

返回值：

**Status**：表示本命令成功与否

**BD\_ADDR**：执行HCI\_PIN\_Code\_Request\_Negative\_Reply命令后设备的地址。

同时，在HCI\_PIN\_Code\_Request\_Negative\_Reply命令完成后，controller将生成HCI\_COMMAND\_COMPLETE事件。

获得了PIN码之后，配对过程开始：

（1）首先LM-A向LM-B发送 **LMP\_IN\_RAND PDU**，此时设备A被称为启动器（initiator）或者初始LM（initiating LM）。设备B被称为响应器（responder）或者响应LM（responding LM）。

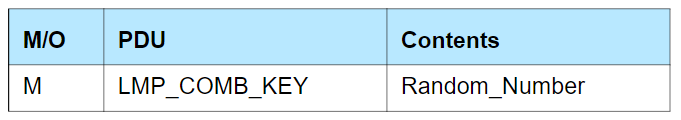
**LMP\_IN\_RAND PDU**中包含随机数。

（2）LM-B在接收到**LMP\_IN\_RAND** 的PDU之后，会向Host B发送事件请求，这个事件和之前LM-A向Host A发送的事件是同一类型的事件**HCI\_PIN\_Code\_Request，**请求PIN码。

（3）如果响应器B接受这次配对且从Host B那里得到了一个可变的PIN，则会回复启动器A一个LMP\_ACCEPTED PDU。

（4）此时，配对的双方都会向对方发送PDU：**LMP\_COMB\_KEY**，配对的过程中创建的link key将是一个组合key。任何配置为使用组合键的设备都应存储link key。

**LMP\_COMB\_KEY** （P631）



LMP\_COMB\_KEY的内容受到当前link key的位XOR保护。

新的link key被保存下来，旧的link key被丢弃掉。

新的link key作为两个设备后续所有连接的link key，直到其再被改变。

当创建新的链路密钥时，需要进行相互验证，以确认两台设备创建了相同的链路密钥。在双方认证后，如果开启加密，启动设备应暂停并立即恢复加密，生成新的加密密钥

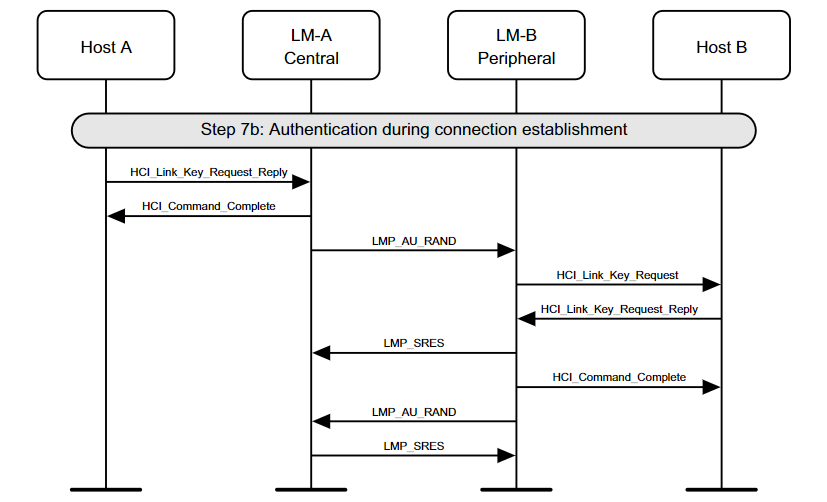
一旦安全简单配对完成，就可以从DHKey计算出链接密钥，这应该用作标准的相互身份验证的输入。一旦完成，将生成一个HCI链接键通知事件：**HCI\_Link\_Key\_Notification** （P1764）

HCI\_Link\_Key\_Notification事件用于向主机指示与BD\_ADDR中指定的BR/EDR控制器的连接创建了新的链接密钥。

### Step 7b. Authentication (Optionally)

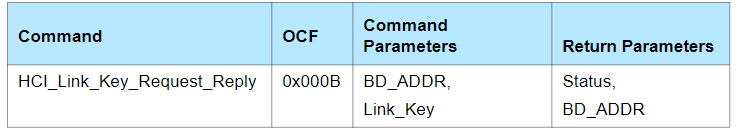
如果高层要求认证，且待连接的设备已经有了统一的link key，则不需要pairing过程。

可以直接认证。可选，非必须操作。



LM-A将通过**HCI\_Link\_Key\_Request** 的event向Host A请求此连接的link key，如果得到了肯定的答复（**HCI\_Link\_Key\_Request\_Reply**），那么此link key将用于身份认证。

**HCI\_Link\_Key\_Request\_Reply**（P1863）



**BD\_ADDR**： Link Key所在设备的地址

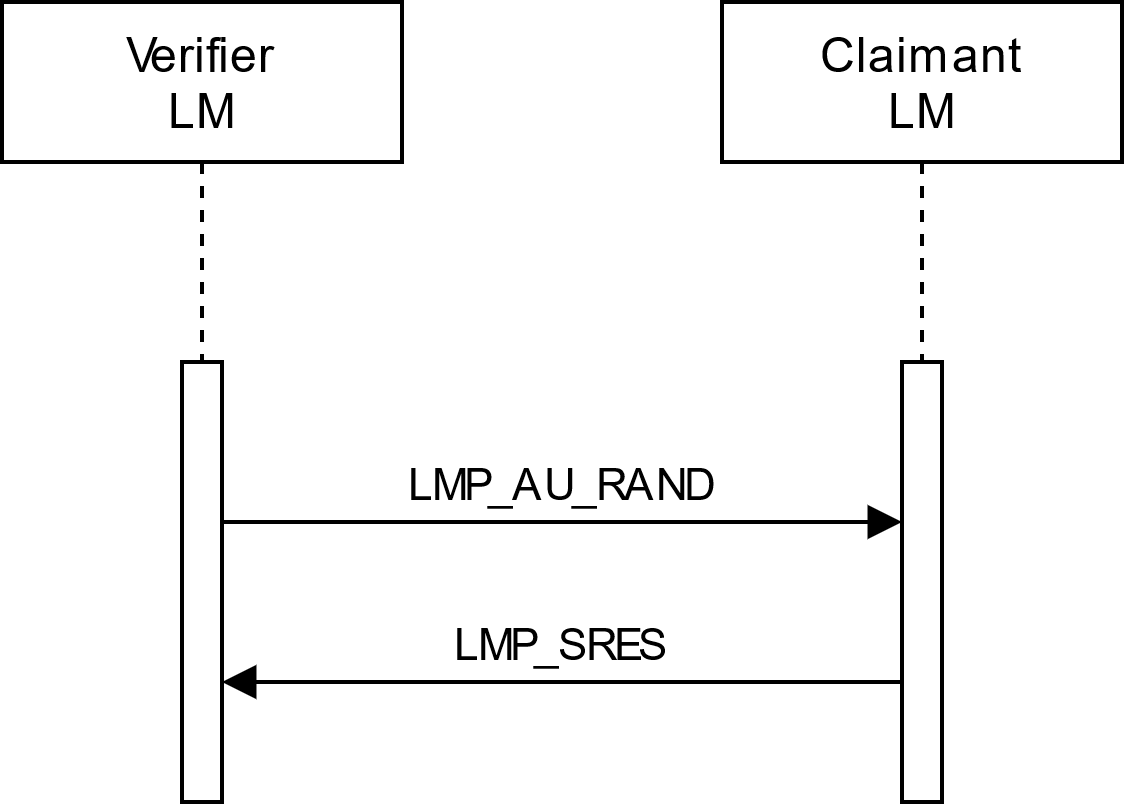
**Link\_Key**：关联的BD\_ADDR的Link Key

返回值：

**Status**：0x00表示命令成功，其他表示失败。

**BD\_ADDR**：Link Key请求应答完成设备的地址

HCI\_LINK\_KEY\_REQUEST\_REPLY命令完成后，LM-A会生成HCI\_COMMAND\_COMPLETE事件，之后LM-A将会发送PDU：**LMP\_AU\_RAND**，包含一个随机数。在之后LM-B将会提供另一个**LMP\_AU\_RAND**，其中也包含一个随机数。两个链路管理器都使用h4函数计算设备认证密钥。

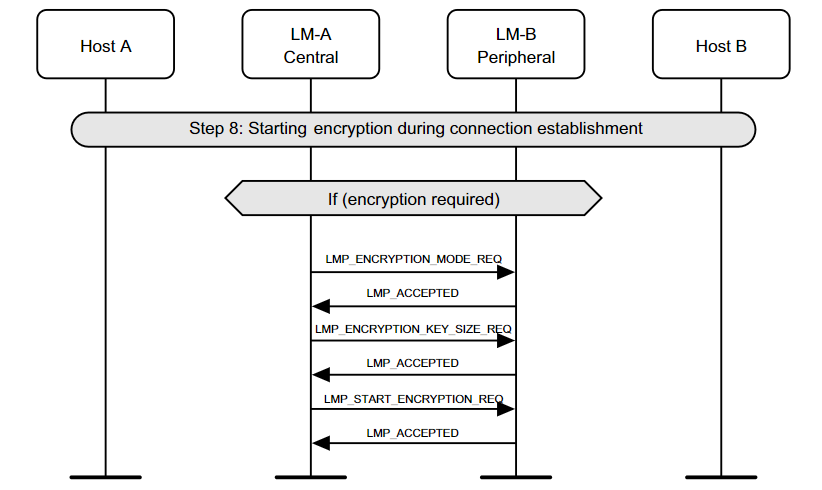


如果Verifier有与claimant相关联的link key，Verifier应检查response并通过LMP\_SRES（包含识别码）发送给claimant。

在claimant检查response之后。如果发现response不正确，Verifier可以发送一个终止连接的LMP\_DETACH 的PDU (Error Code Authentication Failure (0x05))。

## Step 8. Encryption (optionally)

**配对或身份验证过程成功就可以启动加密过程。可选，非必须操作。**



**MSC只显示加密的点对点连接的设置**

如果需要加密过程，LM-A 向LM-B发送 PDU：**LMP\_ENCRYPTION\_MODE\_REQ.**（P635）

这个PDU包含来自Encryption\_Mod加密模式和ID，ID将会用来开始和停止加密序列。

在接收到来自LM-B的 **LM\_ACCEPTED** PDU之后，LM-A发送一个包含建议的Key\_Size的PDU：**LMP\_ENCRYPTION\_KEY\_SIZE\_REQ。**

如果peripheral回送一个**LMP\_ENCRYPTION\_KEY\_SIZE\_REQ**的PDU，则Central根据peripheral的建议进行相应的测试。这个过程重复进行，直到达成一个关键大小的协议，或者很不能达成这样的协议。

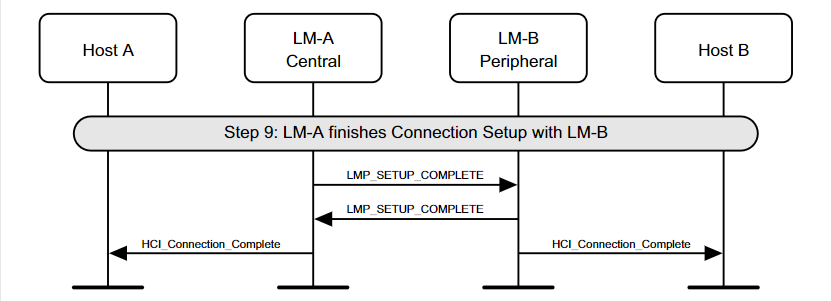
如果达成了协议，则peripheral会发送一个 **LM\_ACCEPTED** 的PDU，之后central发送一个

**LMP\_ENCRYPTION\_KEY\_SIZE\_REQ** 标志最后使用的Key\_size。

在商定了密钥大小之后，LM-A发送LMP\_START\_ENCRYPTION\_REQ的PDU，其中包含EN\_RAND，标志了加密过程的开始。当接收到此消息时，peripheral将计算加密密钥，并使用LMP\_ACCEPTED的PDU进行确认。

## Step 9. Setup Complete

**连接建立完成**

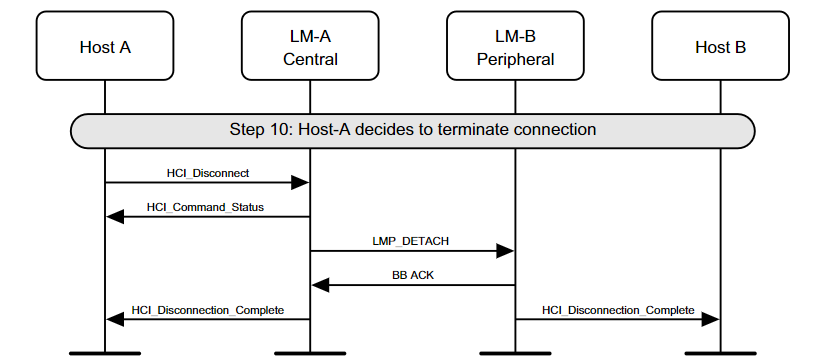


在LM-A不再打算发起安全程序时，会分别向对方发送**LMP\_SETUP\_COMPLETE** PDU（P599）。

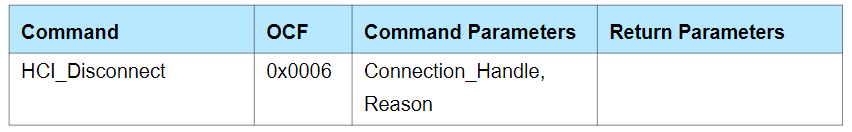
当两个设备都发送LMP\_SETUP\_COMPLETE PDU时，就可以在BR/EDR ACL逻辑传输上传输流量了。

当链接管理器确定连接已建立时，构成连接的BR/EDR控制器将**HCI\_Connection\_Complete**事件发送给每个主机。如果此命令成功，则Connection\_handle将会通知Host，此连接可能用来传输高层的数据例如L2CAP数据。

## Step 10. Disconnection



一旦不再需要连接，任何一个设备都可以使用**HCI\_Disconnect**命令和终止连接。断开连接过程是单方面的，不需要来自远程LM的显式确认。使用来自基带的ARQ确认表示远程LM已经收到LMP DETACH PDU。



HCI\_Disconnect（P1856）命令用于终止已存在的连接。

**Connection\_Handle:** 要断开哪个连接。（0x0000 to 0x0EFF）

**Reason**：断开的原因。

当控制器LM\_A接收到HCI\_Disconnect命令时，它将向主机发送HCI\_Command\_Status事件，并向LM\_B发送**LMP\_DETACH**消息PDU。指示蓝牙设备A和蓝牙设备B的连接断开，其中包含的内容是error\_code错误码参数，用于通知另一方断开连接的原因。之后，LM-A将**HCI\_Connection\_complete**事件发送到Host A表示连接结束。

最后，HCI\_Disconnection\_Complete事件会发送给各自的主机，表示断连完成。