Bluetooth Privacy feature

Bluetooth LE supports a feature that reduces the ability to track a LE device over a period of time by changing the Bluetooth device address on a frequent basis.

In order for a device using the privacy feature to reconnect to known devices, the device address, referred to as the private address, must be resolvable by the other device. The private address is generated using the device’s resolving identity key (IRK) exchanged during the bonding procedure.

**resolution:** means a process used by a device to calculate the device identity address from the received private address and the IRK, while the state resolved is the successful result of a resolution

**There are two variants of the privacy feature:**

(1).In the first variant, private addresses are resolved and generated by the Host.

(2).In the second variant, private addresses are resolved and generated by the Controller without involving the Host after the Host provides the Controller device identity information.

identity information consists of the peer’s identity address and a local and peer’s IRK pair.

**There are two modes of privacy:**

device privacy mode: A device in device privacy mode is only concerned about the privacy of the device and will accept advertising packets from peer devices that contain their identity address as well as ones that contain a private address, even if the peer device has distributed its IRK in the past.

当一个device处于device privacy mode时，device只关注自己的privacy，不关心peer device是否开启privacy或者开启了privacy但并没有使用privacy feature.所以，device可以接受来自peer device的advertising packages(无论这个package里面带有identity address或者private address)。即使peer device以及分发了自己的IRK，但是发出的advertising packages里面可以也包含identify address。

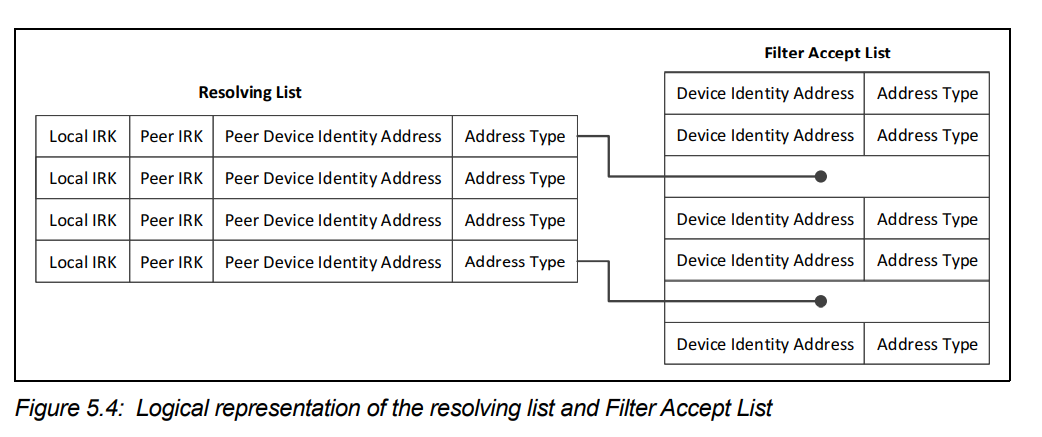
network privacy: device shall not accept advertising packets containing the Identity Address of peer devices that have distributed their IRK. By default, network privacy mode is used when private addresses are resolved and generated by the Controller.

当一个device处于network privacy时，device只接受来自peer device的带有private address的advertising packages。如果device接收到了带有identity address的packages，controller将不会上报至host，直接丢弃。

**Device Filtering and Privacy:**

Device filtering becomes possible when address resolution is performed in the Controller because the peer’s device Identity Address can be resolved prior to checking whether it is in the Filter Accept List.

Figure 5.4 shows a logical representation of the relationship between the Controller resolving list and the Controller Filter Accept List. Actual implementations of the resolving list and Filter Accept List are not required to follow this model. The resolving list may be independent of the Filter Accept List.



**Bluetooth-Address (Public Address/Random Address)**

A Bluetooth device must use one of these types of addresses, and in some cases, it contains both types.

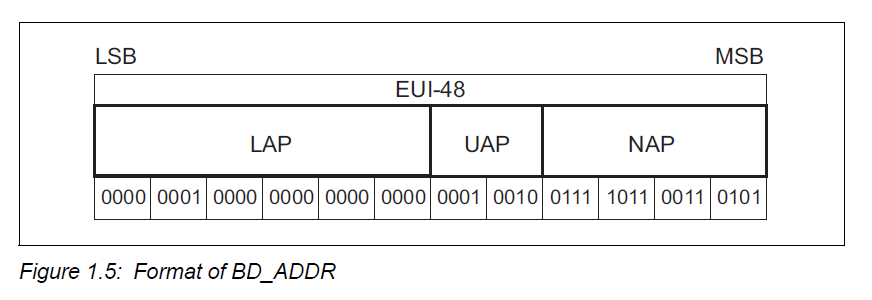
1. **Public Address**

A Bluetooth Public address is a global fixed address that must be registered with the IEEE. It follows the same guidelines as MAC Addresses and shall be a 48-bit extended unique identifier (EUI-48).

The creation of a valid EUI-48 requires one of the following MAC Address Block types to be obtained from the IEEE Registration Authority:

* MAC Address Block Large (MA-L)
* MAC Address Block Medium (MA-M)
* MAC Address Block Small (MA-S)

This address never changes and is guaranteed to be unique for a Bluetooth device.



To learn more about the details of IEEE-assigned MAC address blocks, refer to the following links:

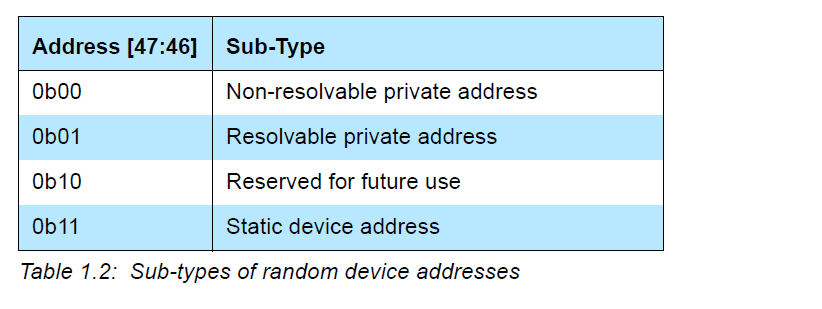
* <https://standards.ieee.org/products-programs/regauth/>
* [https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf](https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf" \t "_blank)

1. **Random Address**

Random addresses are more popular than Public addresses since they do not require registration with the IEEE. A Random address is an identifier that’s either:

The two subtypes of Random addresses are:

* Static Address
* Private Address



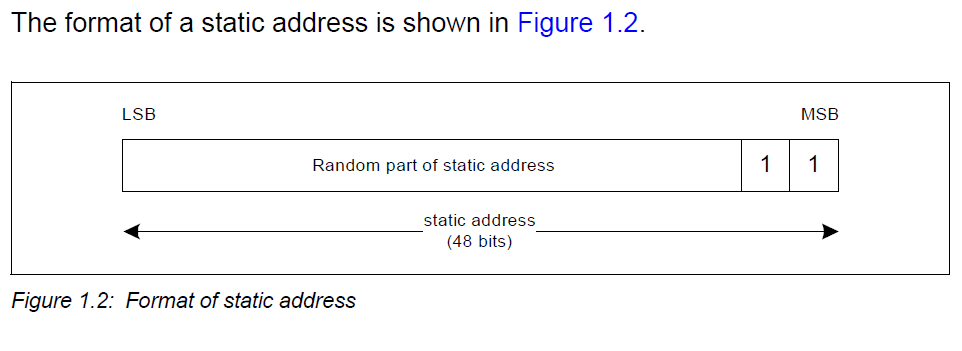
* 1. **Static Address**

A static address is a 48-bit randomly generated address and shall meet the

following requirements:

• At least one bit of the random part of the address shall be 0

• At least one bit of the random part of the address shall be 1



A device may choose to initialize its static address to a new value after each

power cycle. A device shall not change its static address value once initialized

until the device is power cycled.

* 1. **Random Private Address**

The private address may be of either of the following two sub-types:

• Non-resolvable private address

• Resolvable private address.

* + 1. **Resolvable Random Private Address**

To generate a resolvable private address, the device must have either the

Local Identity Resolving Key (IRK) or the Peer Identity Resolving Key (IRK).

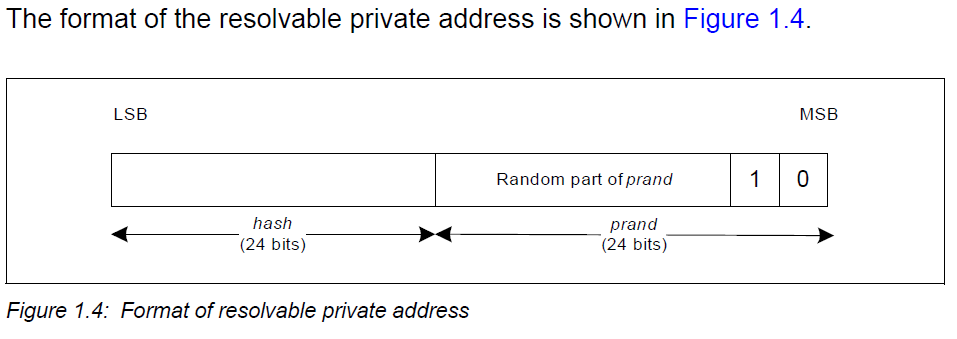
The resolvable private address shall be generated with the IRK and a randomly

generated 24-bit number. The random number is known as prand and shall

meet the following requirements:

• At least one bit of the random part of prand shall be 0

• At least one bit of the random part of prand shall be 1



First, calculate the hash value:

hash = ah(IRK, prand)

Then, the prand and hash are concatenated to generate the random address (randomAddress) in the following manner:

randomAddress = prand || hash

The least significant octet of hash becomes the least significant octet of randomAddress and the most significant octet of prand becomes the most significant octet of randomAddress.

The Host shall set a timer equal to TGAP(private\_addr\_int). The Host shall generate a new resolvable private address or non-resolvable private address when the timer TGAP(private\_addr\_int) expires.

* + 1. **Non-resolvable Random Private Address**

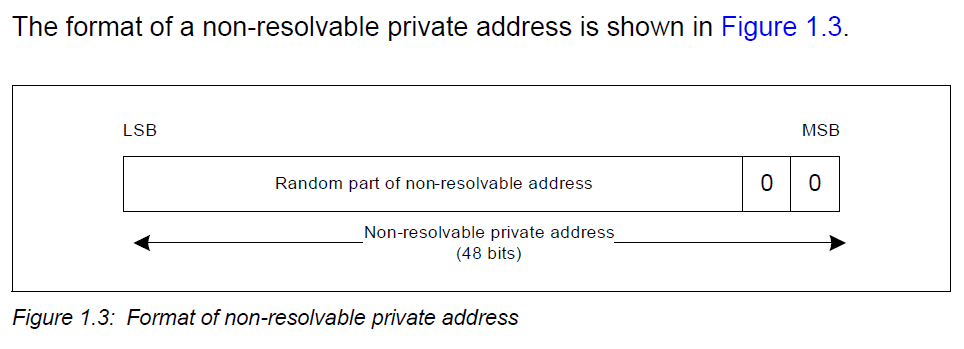
To generate a non-resolvable address, the device shall generate a 48-bit

address with the following requirements:

• At least one bit of the random part of the address shall be 1

• At least one bit of the random part of the address shall be 0

• The address shall not be equal to the public address



**Private device address resolution**

A resolvable private address may be resolved if the corresponding device’s IRK is available using this procedure. If a resolvable private address is resolved, the device can associate this address with the peer device.

The resolvable private address (RPA) is divided into a 24-bit random part(prand) and a 24-bit hash part (hash). The least significant octet of the RPA becomes the least significant octet of hash and the most significant octet of RPA becomes the most significant octet of prand. A localHash value is then generated using the random address hash function ah:

localHash = ah(IRK, prand)

The localHash value is then compared with the hash value extracted from RPA. If the localHash value matches the extracted hash value, then the identity of the peer device has been resolved.

**Message Chart of BLE Privacy**

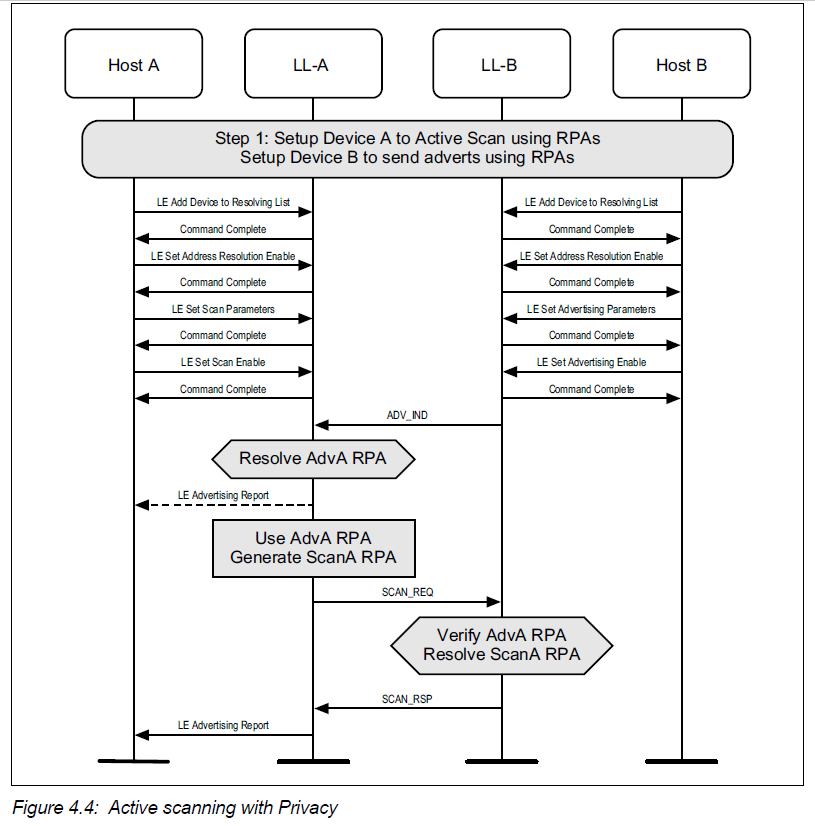
1. **Active scanning with privacy**

A device may use active scanning to obtain more information about devices

that may be useful to populate a user interface. Privacy may be used during

active scanning to make it more difficult to track either device during active

Scanning.(Location: Corespec V5.3-vol6-PartD-4.4)

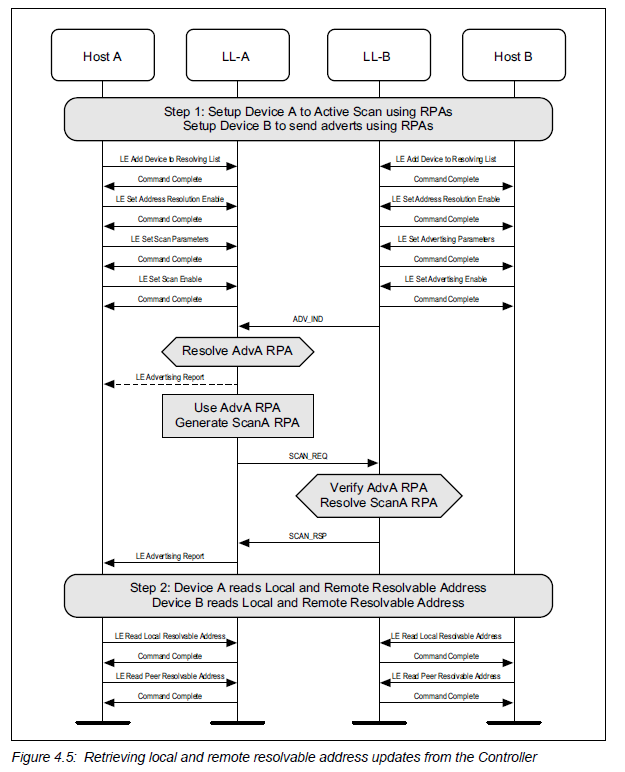


1. **Active scanning with privacy and controller based**

A device may use active scanning on the secondary advertising physical

channel in order to obtain more information about devices that may be useful to

populate a user interface. (Location: Corespec V5.3-vol6-PartD-4.5)



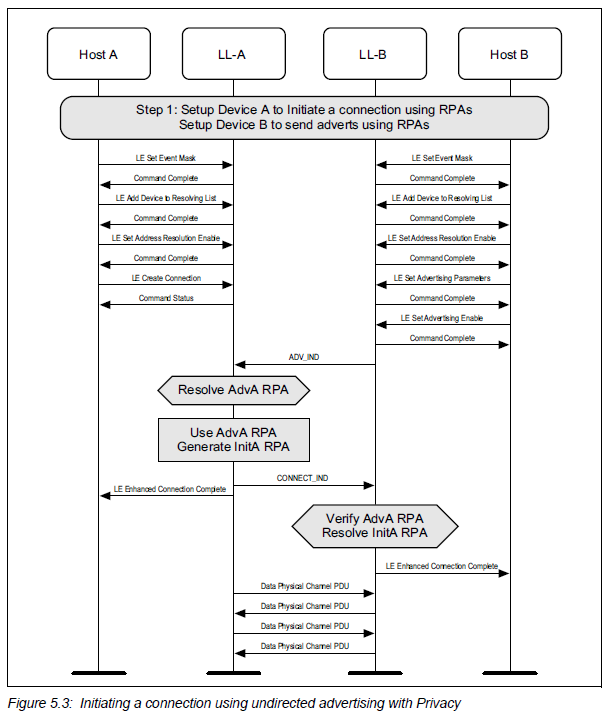
1. **Initiating a connection using undirected advertising with privacy**

A device can initiate a connection to an advertiser. Privacy may be used during

connection initiation to make it more difficult to track either device during

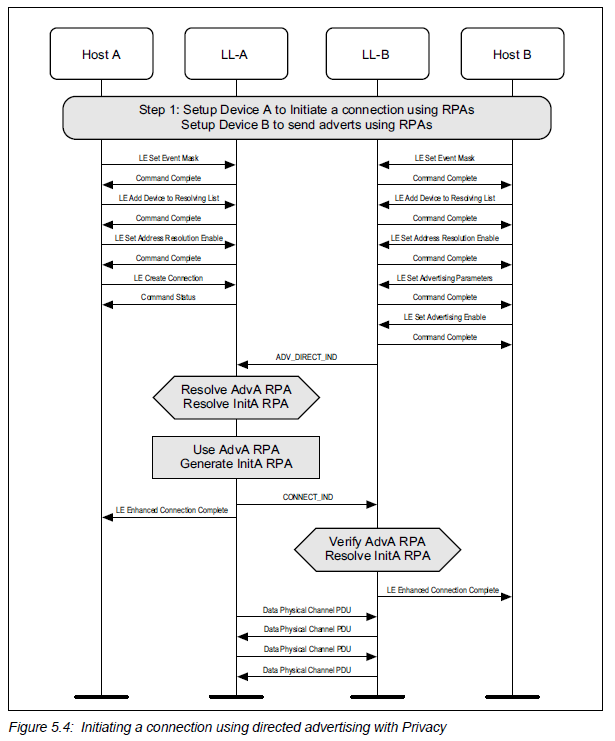
connection setup. The example shows a successful initiation, resulting in both

devices able to send application data(Location: Corespec V5.3-vol6-PartD-5.3)



1. **Initiating a connection using directed advertising with privacy**

A device can initiate a connection to an advertiser who is using Directed Advertising. Privacy may be used during connection initiation to make it more difficult to track either device during connection setup as well as target a single initiator. The example shows a successful initiation, resulting in both devices able to send application data(Location: Corespec V5.3-vol6-PartD-5.4)



Reference:

1. <https://blog.csdn.net/wenbo13579/article/details/126409399>
2. <https://www.anquanke.com/post/id/204177>