The Many Communication Modes of Bluetooth® LE

ADVB$_E$ – Extended Advertising

Understanding Extended Advertising (ADVB$_E$)

Advertising is one of the fundamental communication capabilities of Bluetooth Low Energy (LE). It's used for device discovery, beaconing, and for general purpose connectionless communication. It's also one of the foundations of Bluetooth mesh networking[1].

Since the initial release of Bluetooth LE in V4.0 of the core specification, advertising has evolved significantly, and there are now a number of distinct advertising types that are defined.

Sharing the same logical transport, Advertising Broadcast (ADVB), are two variants, one called **legacy advertising**, or ADVB$_L$ for short, and the other called **extended advertising**, abbreviated ADVB$_E$ in this article.

Note: *Before reading this article, it is recommended that the previous article in this series (Legacy Advertising) be read first.*

The concept of extended advertising doesn't map cleanly to one Link Layer logical transport, however. The term refers to a collection of advertising capabilities and properties which concern the way the LE radio channels are used, the Protocol Data Units (PDUs) that are involved and the way different PDU types can be used together. Sometimes extended advertising involves the ADVB logical transport, but the term also applies to advertising based on two other logical transports called **Periodic Advertising Broadcast** (PADVB) and **Periodic Advertising with Responses** (PAwR). In this article we'll focus solely on extended advertising as used with the ADVB logical transport.

[1] *The current version of Bluetooth Mesh (V1.1) uses legacy advertising as a bearer.*

Overview

Extended advertising made its debut in V5.0 of the Bluetooth Core Specification. It was introduced because of a number of issues relating to what we now know as legacy advertising. For example:

- Legacy advertising only uses the 3 primary advertising channels and with the rapidly growing number of Bluetooth devices in the world, there was a risk that they would become congested and that this would affect user experience.
- The amount of application data that can be transported using legacy advertising is constrained by very small PDUs and fields.
- The uncoordinated, independent transmit and receive behaviors of advertising devices and scanners have pros and cons but can lead to slower application data transfer rates, lower reliability in getting application data to its destination, and poor energy efficiency.

These issues gave rise to a number of design goals for a better form of advertising which included:

1. Reduce dependency on the three primary advertising channels for connectionless communication.
2. Make it easier for applications to transfer larger application data payloads.
3. Allow devices wishing to receive advertising data to synchronize their scanning schedule with the transmission schedule of the advertising device.

The third of these goals was addressed by a special form of extended advertising known as *periodic advertising* and this will be the subject of another article in this series.

The first two goals and the impact they had on the design of extended advertising are of relevance to both extended advertising as used with the ADVB logical transport and the special periodic variants.

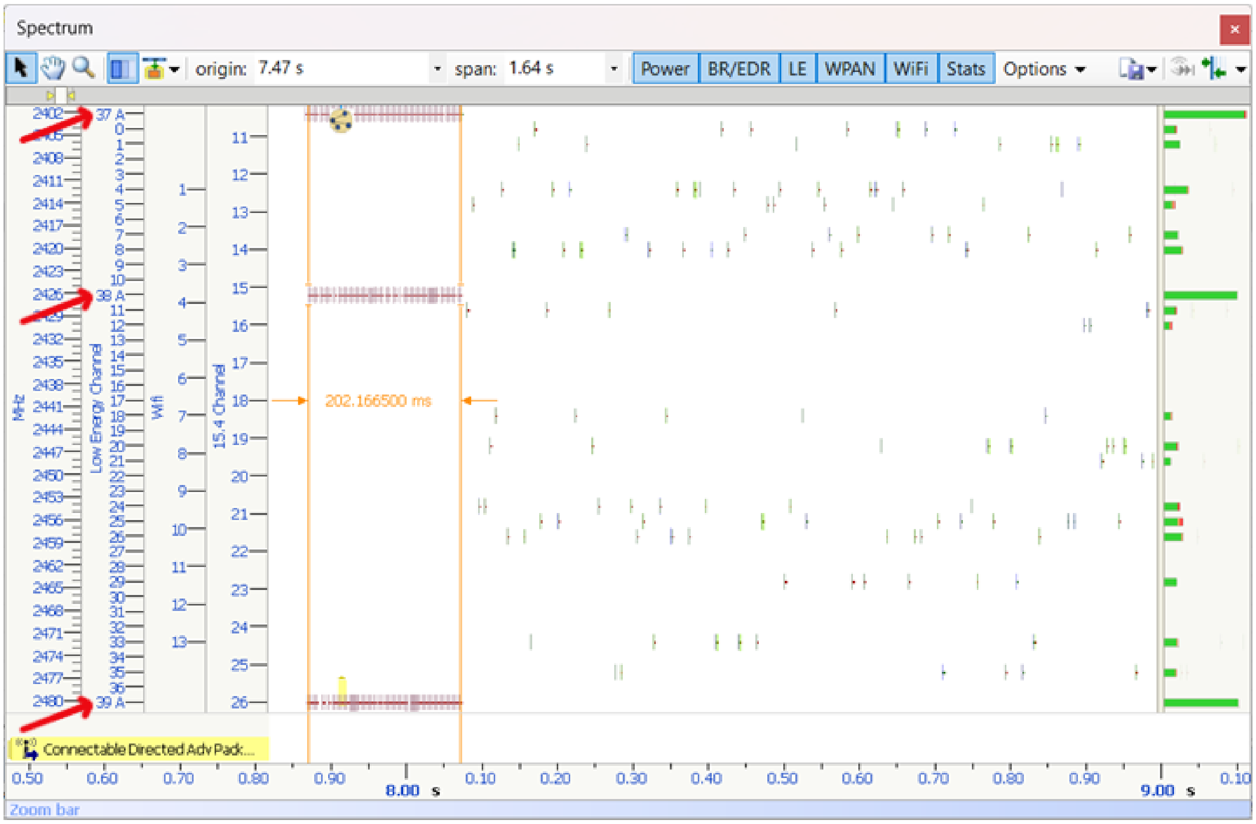

Figure 1 The Spectrum View of the Ellisys Bluetooth Analysis Software showing ADV packets in the three primary advertising channels.

Advertising Modes

In legacy advertising, a number of different advertising PDUs are defined and each is synonymous with a particular advertising mode. For example, the ADV_IND PDU is associated with the *connectable and scannable undirected* mode.

In extended advertising, the advertising mode is indicated directly using a field called AdvMode in conjunction with the presence or absence of a target device address field (TargetA) whose presence means that *directed* advertising is being performed and absence that the mode is using *undirected* advertising.

Connectable advertising can be performed in either low duty cycle mode or (e.g. to enable rapid reconnections) high duty cycle mode.

The advertising modes and the variants supported by $ADVB_E$ are:

Advertising Mode	Undirected	Directed	High Duty Cycle Mode Available?
Non-connectable and non-scannable	Yes	Yes	No
Connectable	Yes	Yes	Yes
Scannable	Yes	Yes	No

Table 1 Advertising modes and the variants supported by $ADVB_E$

Note that extended advertising cannot be both connectable *and* scannable.

The concept of being *discoverable* (or not) applies to $ADVB_E$ just as it does to $ADVB_L$ and is indicated in the same way using bits in an AD Type called *Flags*. Application data is accommodated differently though, as we shall soon learn.

Device Roles

The device roles that are assumed when using $ADVB_E$ are the same as those used with legacy advertising. They were covered in the previous article in this series. They're repeated here for convenience:

- **Broadcaster** - In this role, a device transmits but does not receive packets. As such, a Broadcaster cannot be connected to it.
- **Observer** - An Observer is the counterpart to the Broadcaster. It receives advertising packets, may reply to request more information but cannot initiate a connection with the Broadcaster.
- **Peripheral** - A GAP Peripheral device transmits advertising packets and can receive packets such as connection requests or scan requests, depending on the advertising event type in use.
- **Central** - A GAP Central is the counterpart to the GAP Peripheral. It receives advertising packets by scanning and may reply with transmitted connection or scan requests depending on the advertising event type in use.

Packets, PDUs, and Radio Channels

$ADVB_E$ uses the same Link Layer packet format as $ADVB_L$ but uses a completely different set of PDUs. All $ADVB_E$ PDUs share the same payload format, and the Bluetooth Core Specification calls it the *Common Extended Advertising Payload Format (CEAPF)*. Not all fields in the CEAPF are relevant to all advertising modes (as indicated by the AdvMode field) and the Link Layer specification tabulates the rules for inclusion or omission of each CEAPF field for each advertising mode.

$ADVB_E$ also uses radio channels differently as shall be explained in the following sections.

Channel Offload

Legacy advertising involves transmission of packets on one, two or all three of the primary advertising channels which have channel indices 37, 38 and 39. There are four different advertising PDUs and three of them can accommodate up to 31 bytes of application data (including type and length subfields) in the AdvData field. Packets containing the largest possible AdvData field are 47 bytes or 376 bits long, and at a symbol rate of 1 per microsecond require 376 µs of airtime. This might not sound like much time but with copies of the same PDU typically transmitted on three channels in close succession and advertising intervals potentially as short as 20 ms, this can soon add up to a significant amount of airtime and channel occupancy.

Extended advertising defines a PDU type called ADV_EXT_IND. This type of PDU can only be transmitted on the primary advertising channels and so is comparable to the legacy advertising ADV_IND PDU in that respect.

$ADVB_E$ does not support the transmission of application data on the primary advertising channels though and so ADV_EXT_IND does not include the AdvData. This reduces the demand for airtime on the primary advertising channels. Instead, application data is delivered in other types of PDU that are transmitted on the 37 general-purpose channels.

Scanning devices always start their hunt for advertising packets on the primary advertising channels, and as stated, it's on these channels that they will receive ADV_EXT_IND PDUs. And here's where it starts to get interesting because ADV_EXT_IND PDUs include a field called **AuxPtr** which points to a separate but related packet containing a type of PDU called AUX_ADV_IND. AUX_ADV_IND PDUs are transmitted on the 37 general purpose channels and can include the AdvData field.

AuxPtr contains several sub-fields and between them they tell the scanning device which radio channel the related AUX_ADV_IND PDU will be transmitted on and when it will be transmitted, this timing information expressed as an offset from the time the start of the ADV_EXT_IND PDU containing the AuxPtr field was received.

The naming of these PDUs hints at some further terminology. Any extended advertising PDU that is referenced by AuxPtr in another PDU is called an *auxiliary PDU* and the packet containing the referencing AuxPtr field is called a *superior PDU*.

Figure 2 illustrates the relationship between ADV_EXT_IND PDUs and AUX_ADV_IND PDUs.

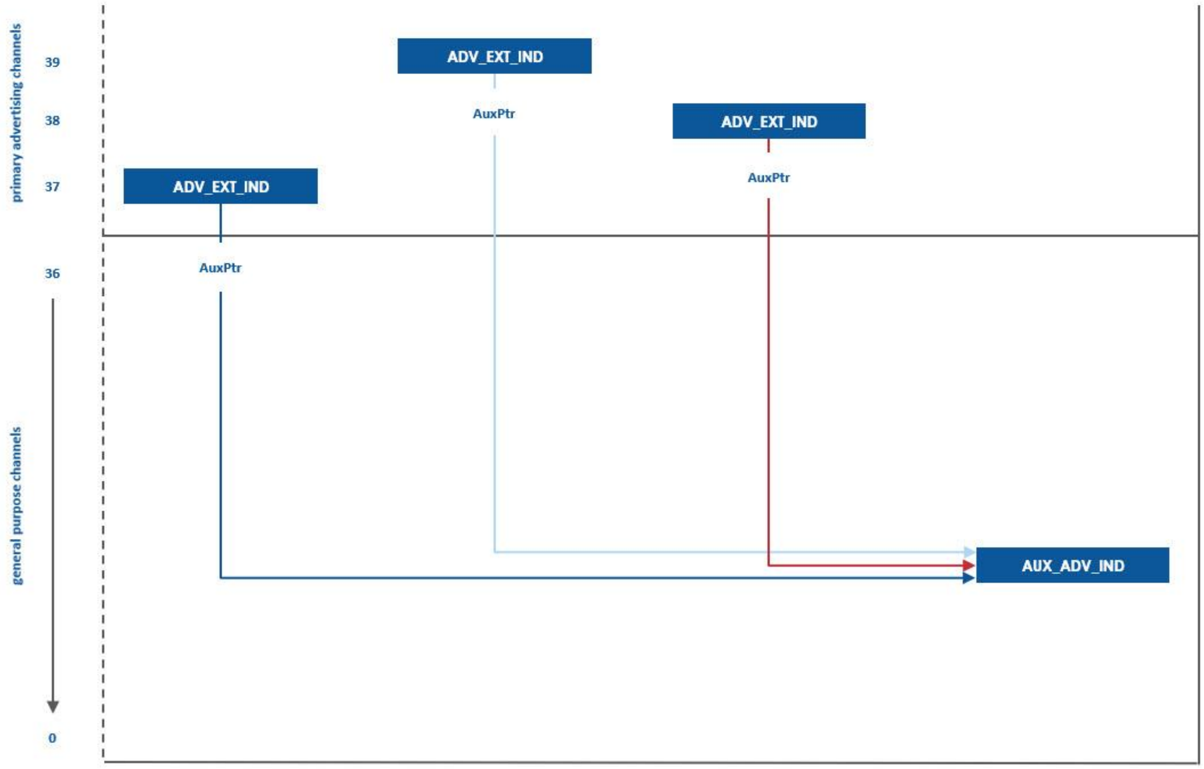

Figure 2 ADV_EXT_IND PDUs linked to an AUX_ADV_IND PDU by the AuxPtr field

In the illustration above, three ADV_EXT_IND PDUs are transmitted in the same advertising event, one on each of the primary advertising channels. All three ADV_EXT_IND PDUs point to the same AUX_ADV_IND PDU which is transmitted a little later on one of the general-purpose channels.

Extended advertising reduces the demand for airtime on the primary advertising channels by offloading AdvData to a single PDU transmitted on the general-purpose channels instead of transmitting three copies of the same data in three different PDUs on the primary advertising channels as would be the case if legacy advertising was used.

Larger Application Data Capacity

Extended advertising makes it possible for applications to communicate **much larger amounts of data** than is possible using legacy advertising and up to 1,650 bytes can be transferred in an advertising event (depending on Controller capabilities). Two features contribute to this significant improvement.

Maximum AdvData Size

The Common Extended Advertising Payload Format is depicted in Figure 3.

PAYLOAD			
Extended Header Length (6 bits)	AdvMode (2 bits)	Extender Header (0-63 octets)	AdvData (0-254 octets)

Figure 3 The Common Extended Advertising Payload Format

AdvData has a maximum size of 254 octets, but it is a variable length field, and its maximum length depends on how large the variable length Extended Header field is. When performing non-connectable, non-scannable, undirected extended advertising over the LE 1M PHY the rules regarding the inclusion of the fields in the Extended Header make it only three octets long which leaves a maximum of 251 bytes available for the AdvData field. This is much larger than the 31 bytes maximum size of AdvData with legacy advertising.

Fragmentation and PDU Chaining

Extended advertising goes further in enabling larger amounts of application data to be accommodated than simply increasing the size of the AdvData field. Application data up to 1,650 bytes can be fragmented and transmitted in one AUX_ADV_IND PDU followed by **a series of linked AUX_CHAIN_IND PDUs**. The AUX_ADV_IND PDU is linked to the first AUX_CHAIN_IND PDU using the AuxPtr field and each AUX_CHAIN_IND PDU is linked to the next in the series in the same way.

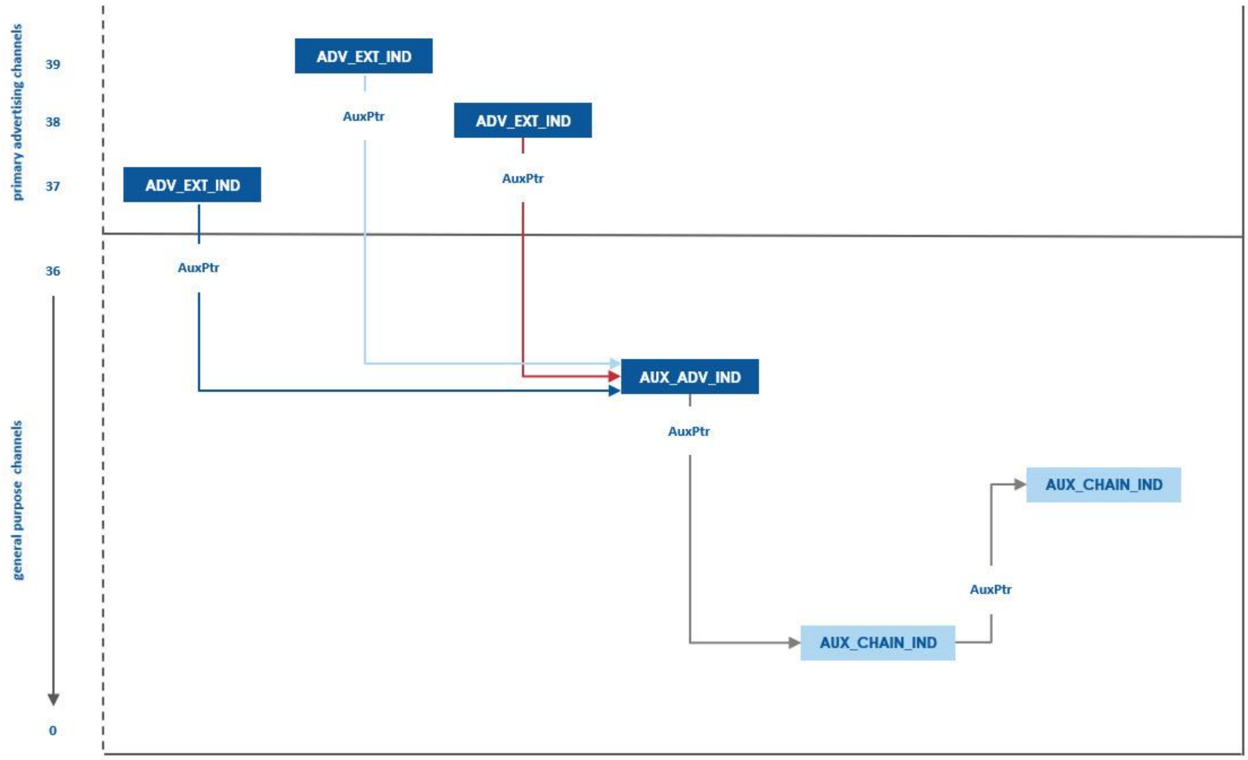

Figure 4 Extended Advertising PDU Chaining

The first AUX_CHAIN_IND PDU in Figure 4 is both an auxiliary PDU of the AUX_ADV_IND that points to it and the superior PDU of the second AUX_CHAIN_IND PDU to which its AuxPtr field points.

Scheduling and Channel Selection

The scheduling rules for $ADVB_E$ include the concept of an *extended* advertising event as well as the standard advertising event. Advertising events relate to transmissions on the primary advertising channels only and are defined in the same way as for legacy advertising whereas extended advertising events span both the transmission of packets on the primary channels and the transmission of auxiliary PDUs on the general-purpose channels. An extended advertising event starts at the same time as the related advertising event and ends when the last auxiliary PDU (e.g. AUX_ADV_IND or AUX_CHAIN_IND) has been transmitted.

The selection of general-purpose channels is left to the implementation, but the Bluetooth Core Specification recommends that *"that sufficient channel diversity is used to avoid collisions"*.

Advertising

An example of an extended advertising event is shown in Figure 5.

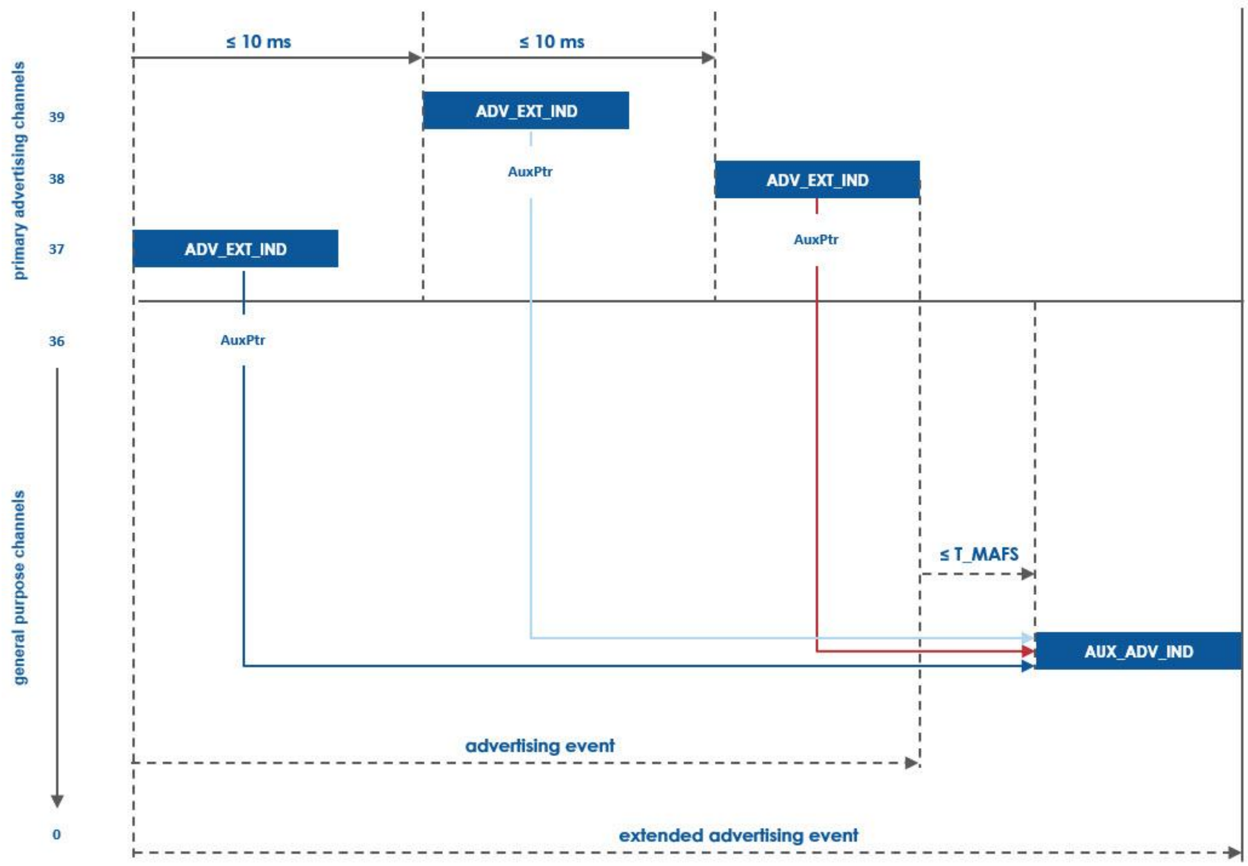

Figure 5 Advertising event and extended advertising event

The transmission of successive ADV_EXT_IND PDUs takes place at intervals of no more than 10 ms. The ordering of primary channels can be randomized at each event. The transmission of the first auxiliary PDU such as the AUX_ADV_IND PDU shown in Figure 5, takes place a short time after the end of the last superior ADV_EXT_IND PDU. This time has a symbolic name of *T_MAFS* in the Bluetooth Core Specification and stands for Minimum AUX Frame Space. T_MAFS has a default value of 300 µs.

Scanning

The concept of active scanning is the same regardless of whether extended advertising or legacy advertising is being performed. The only difference concerns the types of PDU and the channels used.

If a scannable form of extended advertising is being performed, after transmitting an AUX_ADV_IND PDU on one of the general-purpose channels, the advertising device must listen for scan request PDUs (AUX_SCAN_REQ) on the same channel. If a scan request is received, the advertiser replies with further data in an AUX_SCAN_RSP PDU, also on the same channel.

Scan request and response PDUs are separated by a frame spacing which by default (currently) is 150 µs.

Initiating

If a connectable form of advertising is being performed, a scanner can request a connection by responding to an AUX_ADV_IND PDU with an AUX_CONNECT_REQ PDU after a short frame space period which by default is 150 µs. After the same frame space period, the advertiser responds with AUX_CONNECT_RSP.

Advertising Sets

Extended advertising defines a feature known as the *advertising set*. Advertising sets allow a device to have up to 16 instances of advertising running at a time, with each set governed by its own set of parameters such as its own advertising interval. A field in the extended header called AdvDataInfo includes a sub-field, Advertising Set ID (SID) which identifies the set that a PDU belongs to.

The Physical Layer

Legacy Advertising PDUs may only be transmitted using the LE 1M PHY. In contrast, ADV_EXT_IND PDUs which are only ever transmitted on the primary advertising channels, may use either LE 1M, or the LE Coded PHY which potentially increases range by a factor of 4.

Extended advertising PDUs transmitted on the general-purpose channels may use the LE 1M, LE 2M or LE Coded PHYs.

Application Concerns

Configuration

The Host Controller Interface (HCI) defines the *LE Set Extended Advertising Parameters* command which can be used to set the parameters that govern how an advertising set will behave. The parameters that can be specified include an advertising set ID (SID) so that multiple distinct sets can be created, each with a different SID.

Additional parameters that can be specified by the host include properties of the required type of advertising events (e.g. whether connectable and/or scannable), a minimum to maximum range for the advertising interval, and a primary channel map that controls which of these channels ADV_EXT_IND PDUs will be transmitted on. The PHY to be used for primary advertising channel transmissions and a potentially different PHY for general purpose channel transmissions can also be specified.

APIs may or may not provide direct access to all aspects of the HCI *LE Set Extended Advertising Parameters* command. The device's scheduler will select an advertising interval from within the suggested range of values if possible.

Application Data

Applications make one or more calls to the HCI *LE Set Extended Advertising Data* command to provide the data for an advertising set. As with legacy advertising, data must be encapsulated within a series of AD Type containers each consisting of a type identifier, length and value field.

Each call to the HCI command can provide up to 251 bytes of data only but applications can fragment larger application data payloads and make multiple calls to the command, indicating in a parameter called *Operation* whether the data provided in each call is the first fragment, an intermediate fragment or the last fragment of the full payload. Developers may find that APIs are designed to hide the fact that multiple HCI calls are required from application code by providing a higher-level abstraction which allows the full payload to be passed in a single function call.

Compatibility

Devices wishing to be discoverable by older devices that support only legacy advertising should interleave legacy advertising and extended advertising.

Reliability

The lack of coordination between the scheduling of advertising and scanning by devices using $ADVB_E$ presents the same challenges as legacy advertising and thought must go into the values chosen for advertising intervals and scanning intervals. The Ellisys Expert Education Series article on legacy advertising says more about this. That said, the offset information in the AuxPtr field means that scanning on general purpose channels for auxiliary packets can be precisely scheduled.

$ADVB_E$ uses more radio channels than $ADVB_L$ but is still dependent on scanning devices successfully receiving packets transmitted on the primary advertising channels. Extended advertising ADV_EXT_IND PDUs contain no application data and when associated with an auxiliary PDU that does contain application data using the LE 1M PHY, the largest such packet will be 192 bits in length and require only 192 µs of primary advertising channel airtime. This reduces the probability of packet loss due to collisions.

Security

Confidentiality of Data

The Encrypted Advertising feature introduced in version 5.4 of the Bluetooth Core Specification may be used with extended advertising. This involves the advertising device encrypting all data fields that it wishes to protect from eavesdropping as a single composite sequence of AD Types and then placing the resultant cipher text in an AD Type called Encrypted Data.

The feature includes the definition of a secure method for the sharing of encryption key material with trusted devices. Only those scanning devices that have obtained the encryption key parameters can decrypt the value of the Encrypted Data field within the AdvData PDU field.

Privacy

Link Layer PDUs used for advertising, scanning and other purposes often include a field in which the address of the transmitting device might be placed (e.g. AdvA in advertising PDUs). Sometimes the inclusion of the device's address is mandatory and sometimes it is optional. A device address is an identifier and to work as such, it needs to be static.

Devices which repeatedly transmit static, unchanging data are vulnerable to being tracked. In security circles this is classified as a *privacy issue*.

To mitigate this issue as it applies to Bluetooth device addresses, a special type of address called a *private address* is defined in the specification. A private address automatically changes at intervals. How often depends on the implementation but the core specification recommends an interval of about 15 minutes.

If it's necessary to both protect the privacy of a device and allow it to be reliably identified by *trusted* devices, a special type of private address, the *resolvable private address* (RPA) is defined. If an RPA is used, then a device also has a hidden *identity address* which acts as a reliable and unchanging identifier for the device. When used along with an RPA, the identity address is never revealed but devices can translate or *resolve* an RPA into its identify address if and only if the two devices have been paired.

Note that whenever a private address changes, one of the inputs to the encrypted advertising data encryption procedure, known as a *nonce*, also changes and therefore so does the value of the encrypted data. This too helps protect the privacy of the device.

Ellisys Bluetooth Analyzer Examples

Bluetooth extended advertising is a little complicated. Using an Ellisys Bluetooth Analyzer system makes life a lot simpler. Consider the trace in Figure 6.

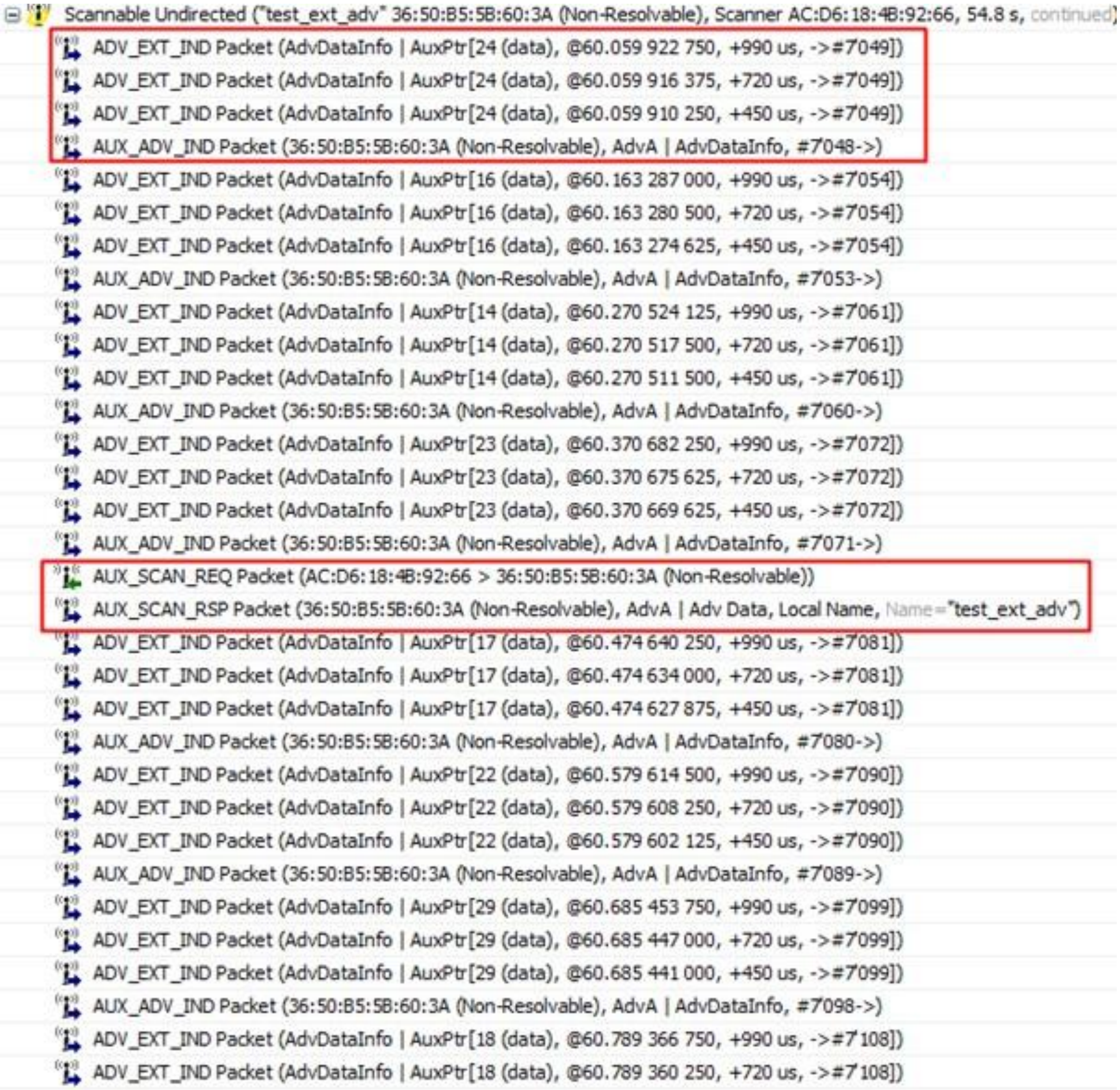

Figure 6 Extended advertising in Ellisys Bluetooth Analyzer software

Figure 6 above shows a trace captured with the Ellisys Bluetooth® Vanguard™ system. It contains a series of PDUs transmitted by the advertiser[2] during extended scannable advertising. There are groups of three ADV_EXT_IND PDUs, each transmitted on one of the three primary advertising channels, followed by a single AUX_ADV_IND auxiliary PDU.

The information shown for each ADV_EXT_IND PDU includes a breakdown of the AuxPtr field. In the first group (highlighted), we can see that an auxiliary PDU is expected on channel 24. We can also see the timing offset which, as expected, reduces for each of the ADV_EXT_IND PDUs as we approach the end of the advertising event and get closer to the expected transmission time for the auxiliary packet.

---

[2] *Extended advertising packets were generated using a Nordic Semiconductor nRF54L15DK.*

On selecting one of the ADV_EXT_IND PDUs from this group, the Ellisys system provides even more information, as shown in Figure 7 below.

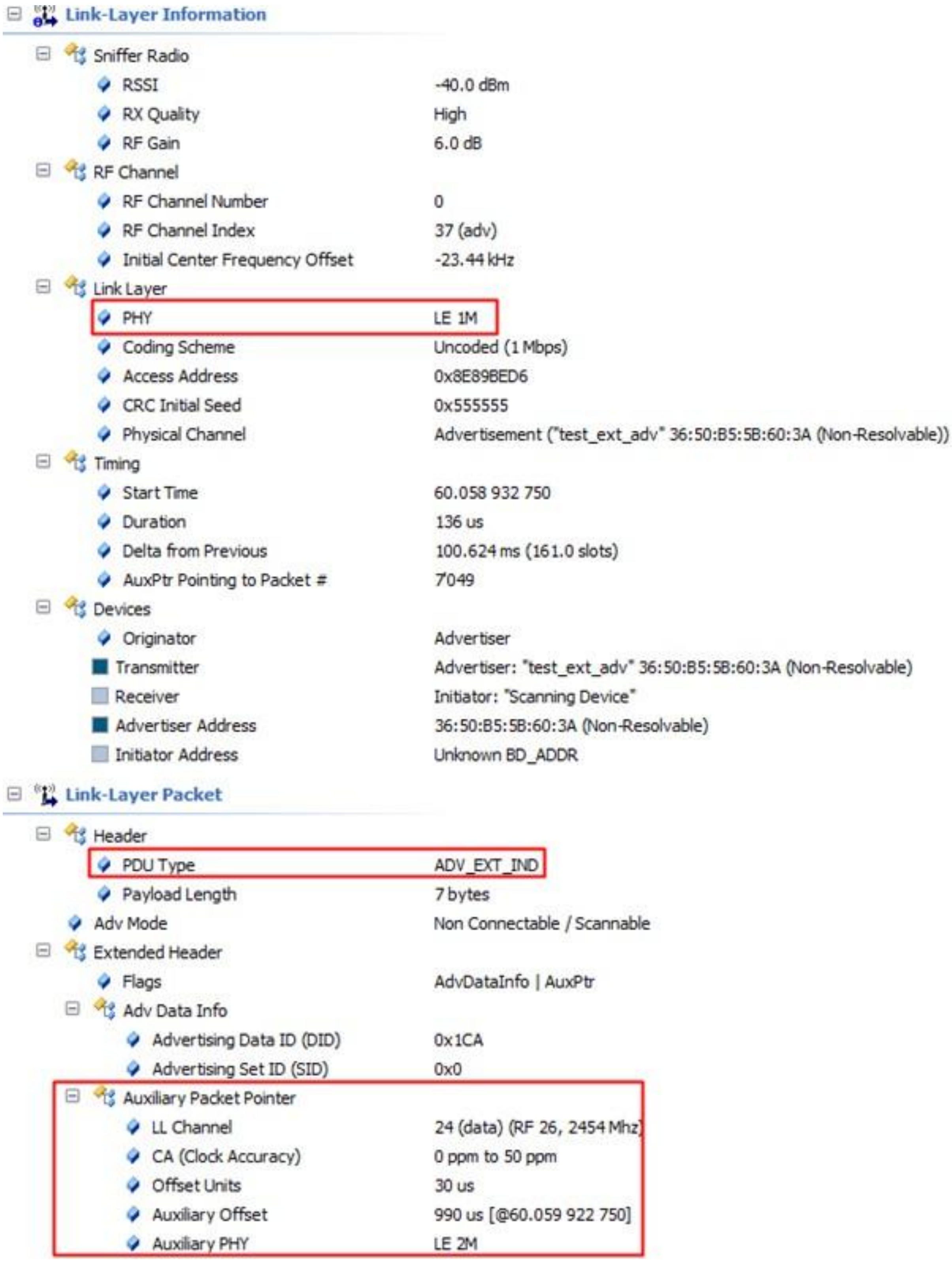

Figure 7 ADV_EXT_IND PDU in Ellisys Bluetooth Analyzer software

Figure 7 above reveals that the ADV_EXT_IND PDUs are using the LE 1M PHY but the AuxPtr field indicates that auxiliary PDUs will use the LE 2M PHY.

Selecting the AUX_ADV_IND PDU, the Ellisys analyzer provides its details as shown in Figure 8 below.

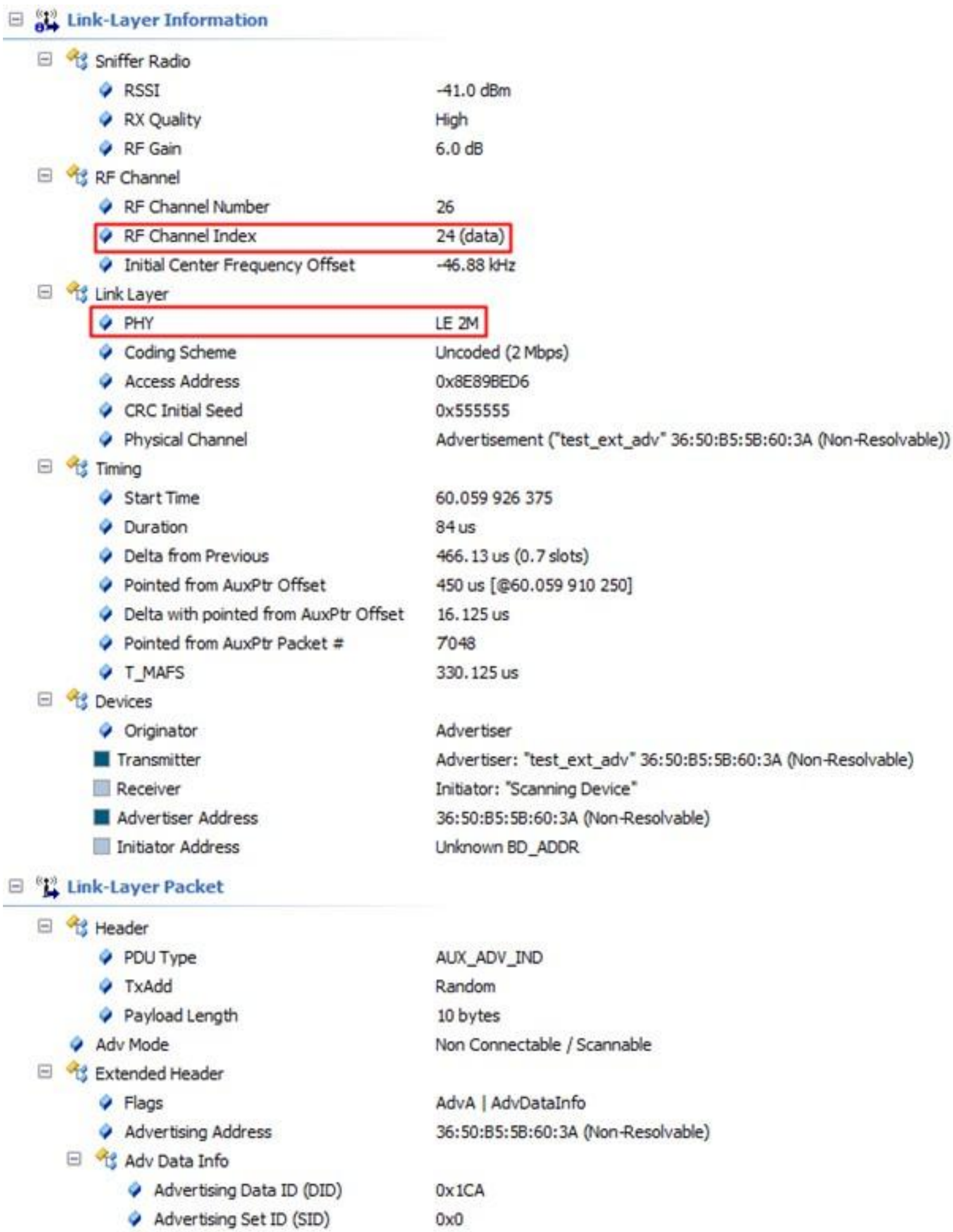

Figure 8 An AUX_ADV_IND PDU in Ellisys Bluetooth Analyzer software

As expected, we can see that the PDU was transmitted using LE 2M on channel 24.

Returning to Figure 6, we can also see that a scanner is performing active scanning and that the advertising device is responding. The series of 6 PDUs that relate to this activity are shown in Figure 9 below.

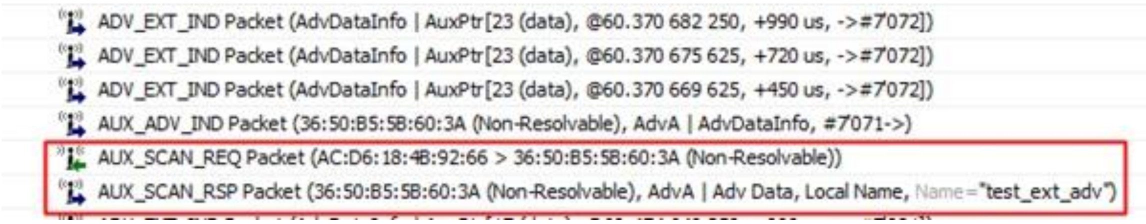

Figure 9 Active scanning in Ellisys Bluetooth Analyzer software

From the ADV_EXT_IND PDUs, we can see that auxiliary PDUs will use channel index 23.

Selecting the AUX_SCAN_REQ and AUX_SCAN_RSP PDUs in the Ellisys tool confirms that this is the case.

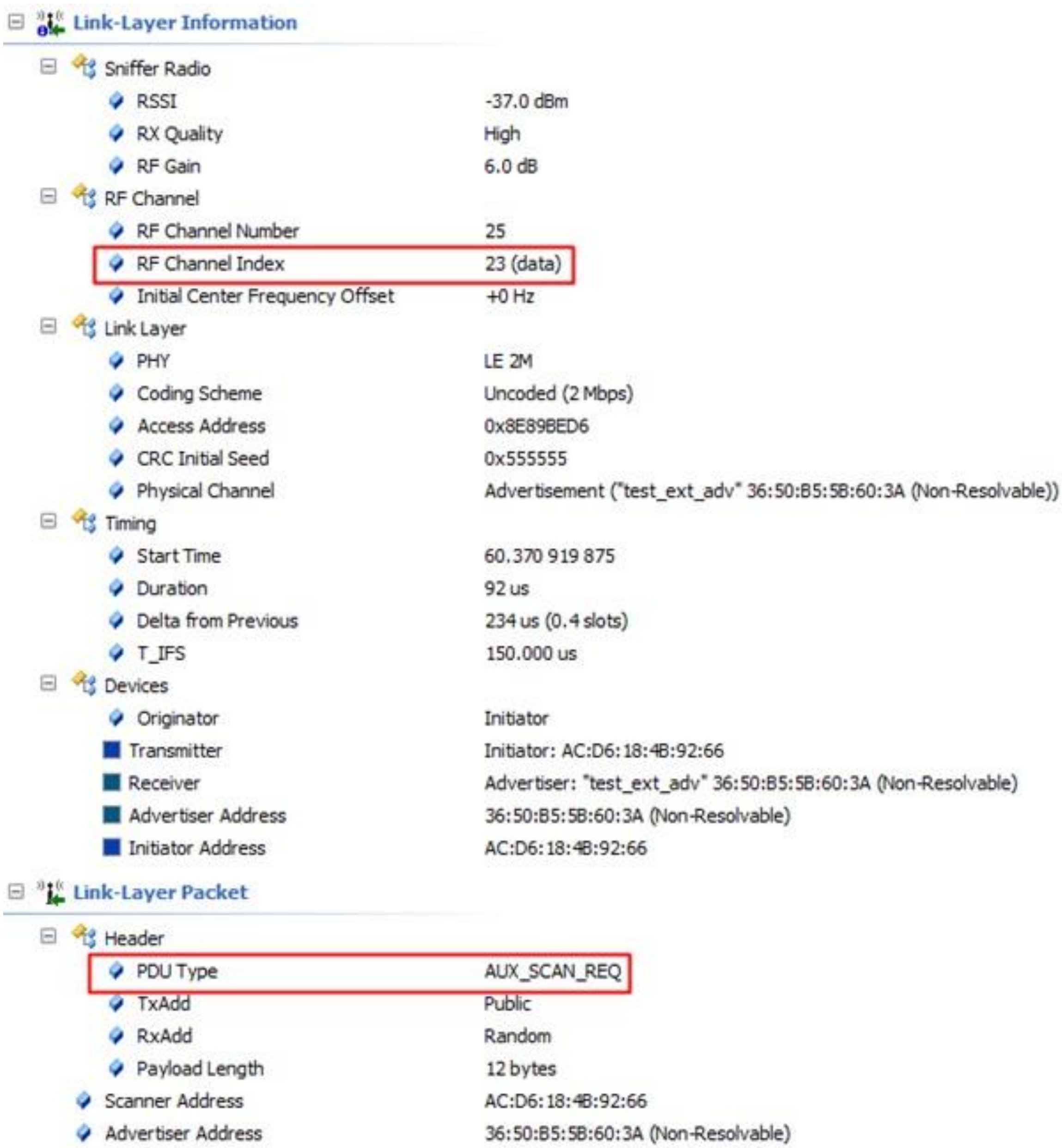

Figure 10 AUX_SCAN_REQ on the expected channel in Ellisys Bluetooth Analyzer software

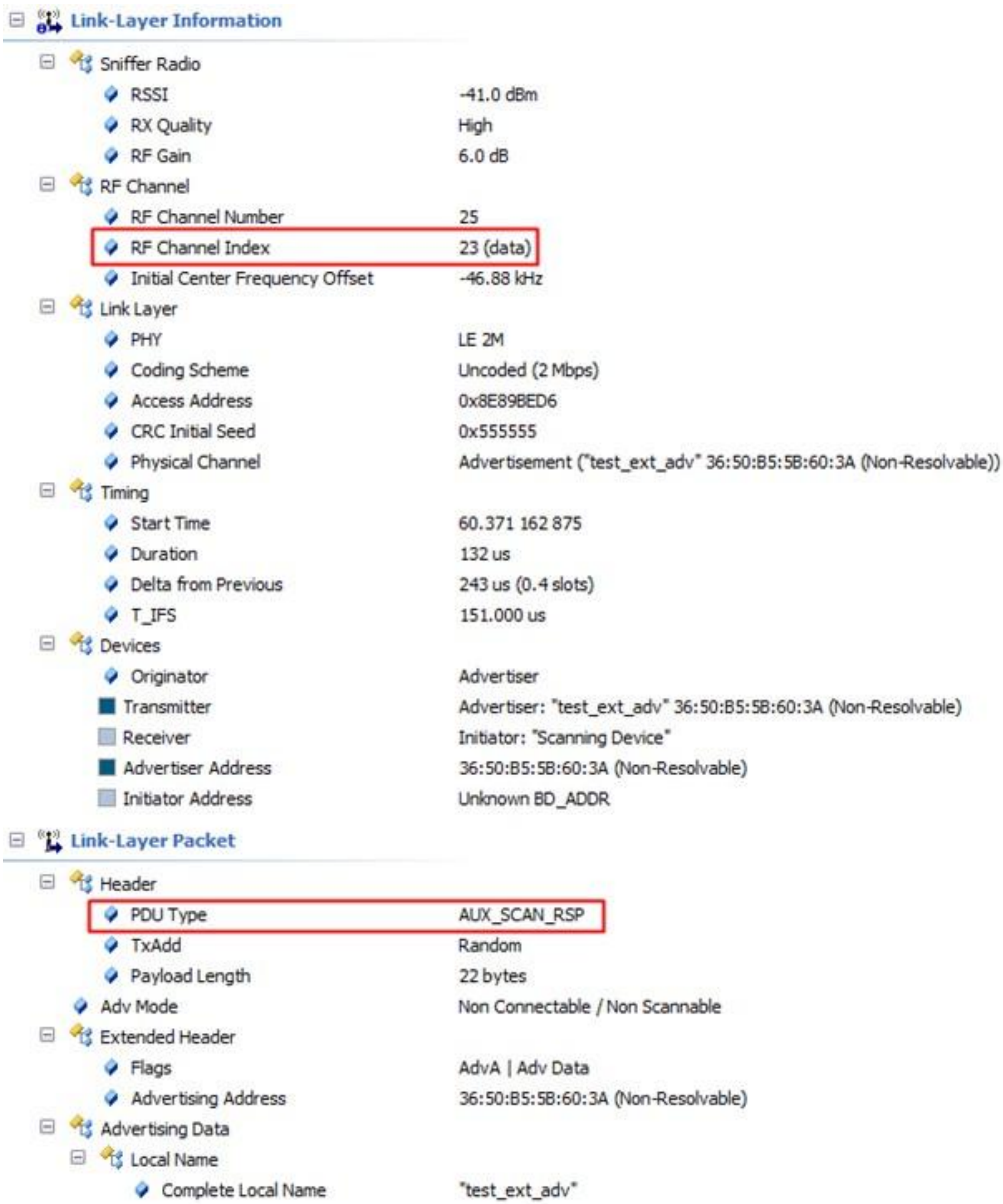

Figure 11 AUX_SCAN_RSP on the expected channel in Ellisys Bluetooth Analyzer software

Communication Mode Properties

The first article in this series, *The Many Communication Modes of Bluetooth LE*, introduced a set of properties that can be useful in comparing one communication mode with another. Below is the table of properties for extended advertising ($ADVB_E$).

Property	Comment
Topology	Undirected: one-to-many (1:m) or Directed: one-to-one (1:1)
Transmitters vs Receivers	This depends on the advertising event type and device role(s) in use. *See Device Roles section above.*
Application Data Direction	One-way. Application data can be transmitted only from the advertising device to scanning devices.
Connected or Connectionless?	Connectionless.
Data and Time	Asynchronous.
Receiver Concurrency	An unlimited number of scanning devices can receive undirected advertising packets at the same time. Directed advertising means transmitted packets are only relevant to one scanning device.
Radio Channels	All 40 Bluetooth LE channels are used by $ADVB_E$.
Scalability	Undirected advertising can reach a theoretically unlimited number of devices so in this respect, $ADVB_E$ is highly scalable. $ADVB_E$ allows significantly more application data to be transmitted per advertising event than $ADVB_L$.
Choice of PHY	Packets transmitted on the primary advertising channels may use LE 1M or the longer range LE Coded PHY. Packets transmitted on the general purpose channels may use LE 1M, LE 2M or LE Coded.

Table 2 $ADVB_E$ Properties

Did You Know?

As we approach the end of this article we'll close with a series of interesting and useful additional points about extended advertising.

Did you know that a new feature called Decision-Based Advertising Filtering (DBAF) was introduced in version 6.0 of the Bluetooth Core Specification?

Extended advertising PDUs transmitted on the primary advertising channels (ADV_EXT_IND) do not contain application data. To receive application data associated with a received ADV_EXT_IND PDU, a device must next scan on the general-purpose channel indicated by the AuxPtr field. But there's a chance that having spent time and energy scanning for the associated auxiliary PDU, the application data it contains is not of interest. This phenomenon is known as a distraction.

While scanning on the general-purpose channel for a packet that might transpire is not relevant; the scanning device is also not scanning on the primary advertising channels and therefore may miss an ADV_EXT_IND PDU as a result.

Distractions can have a negative impact on latency, reliability and energy efficiency.

DBAF addresses these issues by introducing Decision PDUs, which are named ADV_DECISION_IND in the core specification. Decision PDUs are transmitted on primary advertising channels as an alternative to ADV_EXT_IND PDUs and allow the advertising device to provide some information about the contents of auxiliary advertising packets. An enhanced form of scanning filter policy allows the Controller in scanning devices to make informed decisions about whether to scan the channel indicated by AuxPtr or not. In this way, distractions can be avoided and more time spent scanning the primary advertising channels.

Did you know that since version 5.4 of the Bluetooth Core Specification, it has been possible to select the coding parameter "S" for use with the LE Coded PHY when advertising?

The LE Coded PHY increases the range of transmissions and is used with a parameter called S, which has a value of either 2 or 8. This parameter is important as it determines by how much the range is likely to be improved, relative to the LE 1M PHY. With S=2, range will be approximately doubled and with S=8, it will be approximately quadrupled. This comes at a cost, however. S=2 may double range, but the application data transfer rate will be halved. With S=8, application data will be transferred at an eighth of the rate of LE 1M.

Before v5.4 of the core specification it was not possible to indicate the value of S to use when the LE Coded PHY was used for advertising. That all changed with the Advertising Coding Selection feature which makes this possible, giving advertising applications control over the tradeoff between range and application data transfer rates.

Did you know that the Monitoring Advertisers feature, introduced in v6.0 of the Bluetooth Core Specification applies to extended advertising as well as legacy advertising?

Well, it does! Extended advertising benefits in exactly the same way as legacy advertising to this feature. A scanning filter policy can be set to drop duplicate advertising packets, but the monitoring advertisers feature can be used to ensure the scanner is informed when a device of interest moves in and out of range.

Next in the Series

In this article we've explored the extended advertising ($ADVB_E$) communication mode of Bluetooth LE.

In the next article in this series, we'll explore the periodic advertising (PADVB) communication mode.
View the PDF here: https://ellisys.com/technology/edu_bt01_lecomm_ch05_padvb.pdf