Capture and Security Challenges Relating to the LE Isochronous Physical Channel

The Benefits of tZERO™ Tracking Technology

Introduction

The release of Bluetooth 5.2 introduced several major features for Bluetooth, including LE Power Control, Enhanced Attributes (EATT), and the ability to transport audio over Bluetooth Low Energy, via the new LE Isochronous Physical Channel.

In this Expert Note, we will discuss the concept of Bluetooth LE physical channels, the fundamental operations of the two LE Isochronous logical transports, security approaches used by these transports, and how access addresses are used.

We will also look at challenges encountered by test equipment concerning capture, encryption and decryption of isochronous traffic carried over Bluetooth LE, and how these challenges are solved by unique and proprietary innovations from the Ellisys engineering team.

Bluetooth LE Physical Channels

Bluetooth LE devices communicate over a shared physical channel, which is defined by characteristics such as the channel map (e.g., hopping sequence), slot timings, and randomized access addresses.

In each of the four types of LE physical channels, communicating pairs of devices will tune their transceivers to the same PHY channel at the same time using the characteristics defined by the channel.

The four physical channels for Bluetooth LE physical channels are shown in **Table 1**.

The LE Isochronous physical channel, along with several new and emerging profiles and the high-performance, power friendly LC3 codec, enables new audio features for Bluetooth users that can be broadly categorized as follows:

- Multi-Stream Audio (connection-oriented)
- Broadcast Audio for Audio Sharing (connectionless)

Multi-Stream Audio involves the use of a source device that transmits independent, synchronized audio streams to audio sink devices, where the audio can be rendered at the same time across multiple sink devices.

To contrast, classic Bluetooth (BR/EDR) uses a single stream approach, which is relayed to get a TWS (True Wireless Stereo) result.

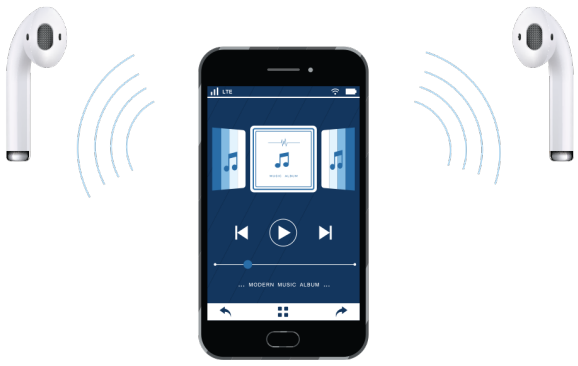


Figure 1 Multi-stream Audio Improves the True Wireless Stereo Experience.

Physical Channel	Purpose
Isochronous	Transfers isochronous data at regular intervals between connected devices in a piconet or unconnected devices (broadcast)
Piconet	Used for communication between specific devices within a piconet
Advertising	Used for broadcasting advertisements to devices
Periodic (Periodic Advertising)	Sends user data to scanner device at periodic intervals

Table 1 The Four Physical Channels Used by Bluetooth Low Energy.

The Audio Sharing feature enables a single audio source (an Isochronous Broadcaster) to broadcast one or more streams of audio to Synchronized Receivers (audio sinks).

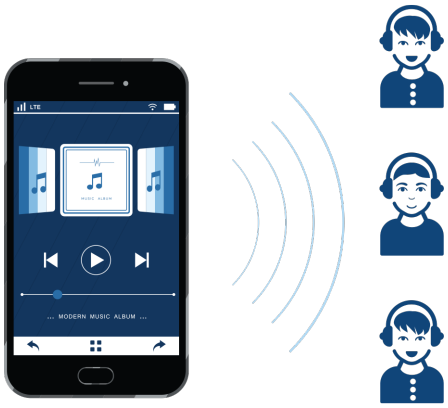


Figure 2 Broadcast (connectionless) Audio.
An Example of Personal Audio Sharing Shown Here.

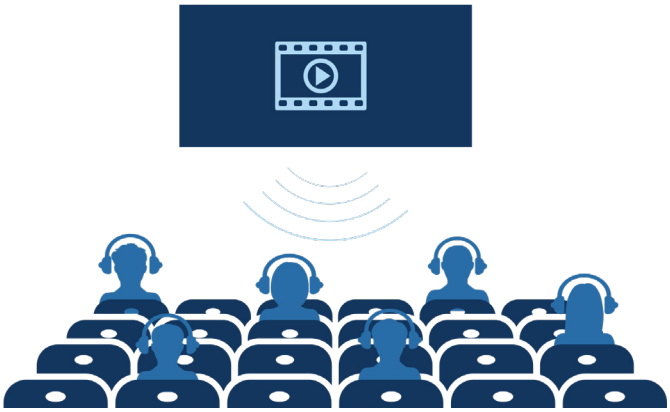


Figure 3 Broadcast Audio is Ideal for Use at Public Venues.
A Location-based Audio Sharing Example is Shown Here.

HELPFUL HINT: Ellisys Bluetooth analyzers include LC3 Auto-Detect, a proprietary Ellisys technology to detect and decode LC3 traffic, based on our test equipment-grade LC3 codec, even without capture of configuration parameters.

Figure 4 LC3 Auto-Detect.

Logical Transports for LE Audio

To support the various applications for LE Audio, two types of logical transports are defined:

Transport	Links
Connected Isochronous Stream (CIS)	LE-S (Streamed/Unframed Data) LE-F (Framed Data)
Broadcast Isochronous Stream (BIS)	LE-S (Streamed/Unframed Data) LE-F (Framed Data) LEB-C (Broadcast Control)

Table 2 Types of Logical Transports.

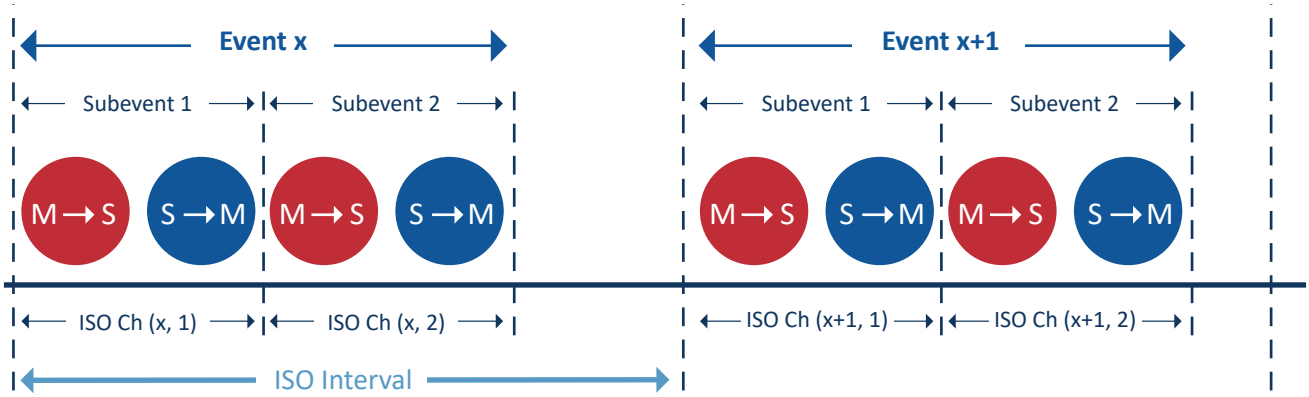
A CIS is established by LLCP commands sent over an LE-ACL (Asynchronous Connection Logical) connection, whereas a BIS is established using advertising packets.

A CIS uses acknowledgments to drive retransmissions and can be data-symmetric or data-asymmetric (data can be transferred in one or both directions). A single CIS is constructed of a Central device and a specific Peripheral device (1:1).

A BIS has no acknowledgment protocol (as the receivers do not respond); traffic is sent in one direction only, to an unlimited number of synchronized receivers (1:M). However, a BIS has an unconditional retransmission mechanism built in that can be used to improve reliability.

CISes and BISes are each comprised of “events” that occur at regular intervals, known as ISO_Intervals. CIS and BIS events consist of one or more sub-events. In a CIS sub-event, the Central and Peripheral devices each transmit once. In a BIS sub-event, the Broadcaster transmits an isochronous data packet.

CIS Events/Subevents



BIS Events/Subevents

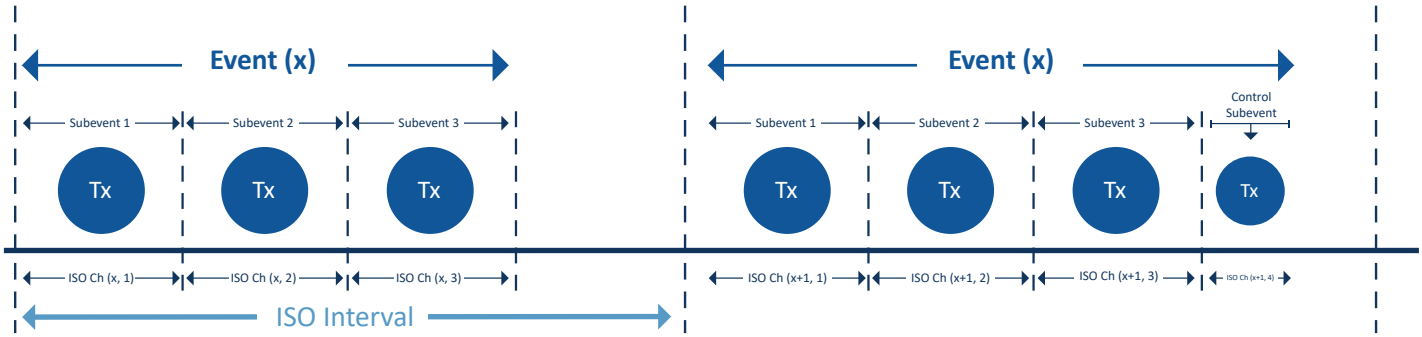


Figure 5 CIS and BIS Events and SubEvents.

A Connected Isochronous Group (CIG) consists of either one CIS, or two or more CISes with the same timing characteristics (ISO_Intervals) and an application layer relationship, up to 31 streams.

A Broadcast Isochronous Group (BIG), created by the Broadcaster, can contain one or more BISes, also up to 31 streams. **Table 3** Summarizes major CIS and BIS features.

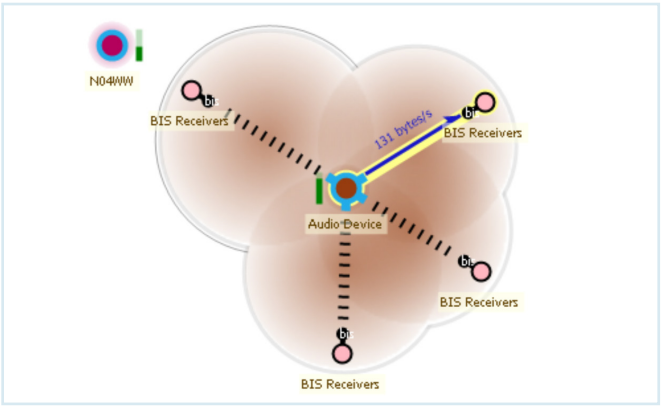


Figure 6 (Top) Instant Piconet View Showing Four BIS Streams (one BIG), Including an Active Audio PDU (and an Unrelated Broadcaster).

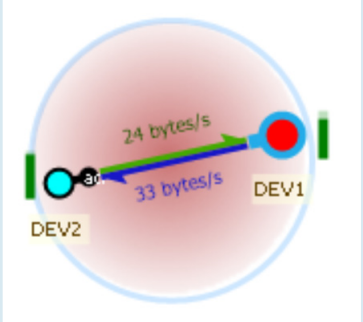


Figure 7 (Left) A Single CIS (Showing the 1:1 M-S Relationship). Note the Data is Going Both Ways in this Case.

Feature	CIS	BIS
Acknowledgement Protocol	Yes	No
Data Transfer	One or Both Directions	One Direction
Retransmissions	Yes, Driven by Ack Protocol	Yes, Sent Unconditionally
Streamed or Framed Logical Link	Both	Both
Control Logical Link	LLCP (Associated ACL)	LEB-C (Broadcast Control)
Number of Streams	31 per group (CIG)	31 per group (BIG)
Stream Topology	1:1	1:M
PHYs (1M, 2M, Coded S=2, Coded S=8)	All	All
Security Association	ACL	BIG

Table 3 Features Summary of Isochronous Transports.

Security Fundamentals for LE Isochronous Transports

If an ACL is encrypted, any constituent CISes must also be encrypted, using the same session key used by the ACL. If an ACL is not encrypted, any constituent CISes must not be encrypted. If a BIG is encrypted, all constituent BISes must be encrypted. Empty PDUs are not encrypted.

For encryption and decryption of a BIG, several parameters are involved:

Parameter	Length	Source	Notes
Broadcast Code	UI level: 16 octets maximum and 4 octets minimum All other levels: 128 bits	Provided by the host	Called the Bluetooth Privacy Code at the application (UI) level
Group Initialization Vector (GIV)	64 bits	Generated by the controller and transmitted via the BIGInfo field (in AUX_SYNC_IND)	Used as part of the calculation for the Initialization Vector (IV)
Group Session Key Diversifier (GSKD)	128 bits	Generated by the controller and transmitted via the BIGInfo field (in AUX_SYNC_IND)	Combined with Group LTK to create Group Session Key (GSK)
Group Long Term Key (GLTK)	128 bits	Provided by the host	Created from the Broadcast Code

Table 4 BIG Encryption Parameters.

To determine whether the BIG is encrypted, the link layer checks the length of the BIGInfo field. The length for a non-encrypted BIG is 33 octets and the length for an encrypted BIG is 57 octets (GIV + GSKD = 24 octets).

Users wishing to participate in a BIG must enter the Broadcast Code (Privacy Code) into their device. The Group Long-Term Key (GLTK) is created using the Broadcast Code. The Group Session Key, used for encrypting and decrypting, is calculated from the GLTK and the GSKD, which is broadcast in the BIGInfo field as part of extended advertising packets (AUX_SYNC_IND).

On an ACL, encryption can be initiated once the connection is established. Encryption is enabled before a CIS is assigned an access address, which adds complexities for test equipment, as the access address is needed for encryption *and decryption* of the CIS.

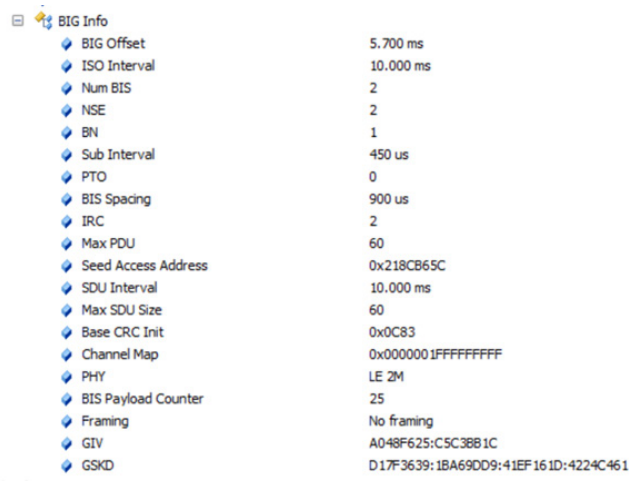


Figure 8 BIGInfo Field in AUX_SYNC_IND (with GIV and GSKD Fields Present).

To enable encryption, the IV (Initialization Vector) and SKD (Session Key Diversifier) parameters are exchanged between Central and Peripheral devices. These random numbers are exchanged using LL_ENC_REQ and LL_ENC_RSP PDUs. There is a Central part and a Peripheral part for each parameter.

For encryption and decryption of an ACL, several parameters are used, including:

Parameter	Length	Source	Notes
Initialization Vector, Central portion (IVm)	32 bits	Generated by the Link Layer and transmitted over the LLCP Encryption Request transaction	Concatenated with IVs to create IV
Initialization Vector, Peripheral portion (IVs)	32 bits	Generated by the Link Layer and transmitted over the LLCP Encryption Response transaction	Concatenated with IVm to create IV
Session Key Diversifier Central portion (SKDm)	64 bits	Generated by the Link Layer and transmitted over the LLCP Encryption Request transaction	Concatenated with SKDs to created SKD
Session Key Diversifier Peripheral portion (SKDs)	64 bits	Generated by the Link Layer and transmitted over the LLCP Encryption Response transaction	Concatenated with SKDm to created SKD

Table 5 ACL Encryption Parameters.

The Session Key Diversifiers are used to ensure a new session key is used for every new connection.

An Initialization Vector, sometimes called a Starting Variable (SV), is a block of bits used in an iterative process for randomizing encrypted traffic to prevent repeated patterns, i.e., to produce distinct ciphertexts from plaintext repetitions. The idea of randomization is that even if there is plaintext that repeats, like an email signature or fixed-location header fields, it will not result in the same ciphertext, which would make it easier for attackers to decrypt the traffic.

Note **Figure 9** below, depicting how an access address (CIS or BIS) is a direct input to the IV. The IV is created using the access address and an IVBASE. For a CIS, IVBASE is set to the value of the IV from the associated ACL and for a BIS, IVBASE is set to the value of GIV (Group IV), contained in the BIGInfo field of AUX_SYNC_IND.

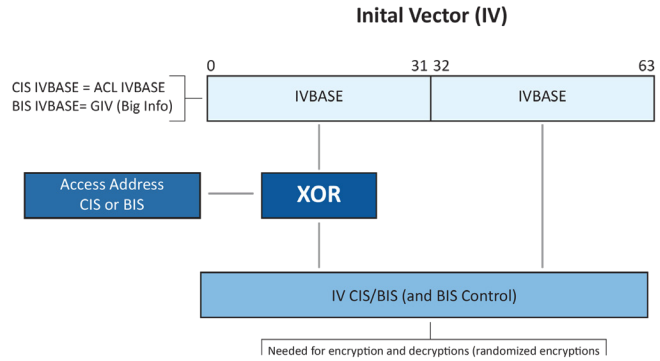


Figure 9 Creation of IV for CIS and BIS.

Access Addresses

As mentioned above, access addresses are used for physical channel access. They also play an important role in security for both Bluetooth LE Isochronous transports.

In **Figure 10**, the access address field is shown as part of an isochronous packet. It is 32-bits in length, follows the packet's preamble, and precedes the header.

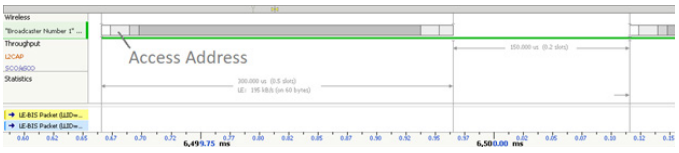


Figure 10 Broadcast Packet with Access Address Field Highlighted.

Table 6 summarizes how access addresses are generated on the four types of physical channels. Note that randomizing an access address produces a high number of addressable periodic advertising trains and active piconet devices.

Physical Channel	Access Address Generation
Isochronous	Randomly Generated (CIS and BIS)
Piconet	Randomly Generated
Advertising	Fixed (0x8E89BED6)
Periodic (Periodic Advertising)	Randomly Generated

Table 6 Generation of Access Addresses (Random and Fixed).

In **Figure 11**, using a filter to show LLCP traffic only, we see the LLCP_CIS_IND exchange occurring twice (colorized). Encryption is being used in this case and is established during the LLCP Encryption Start exchange.

The default ACL (AA = 0x364E99FB) is creating two CIS streams:

1. CIS1 AA = 0xEF14A8B1
2. CIS2 AA = 0x9F240CB3

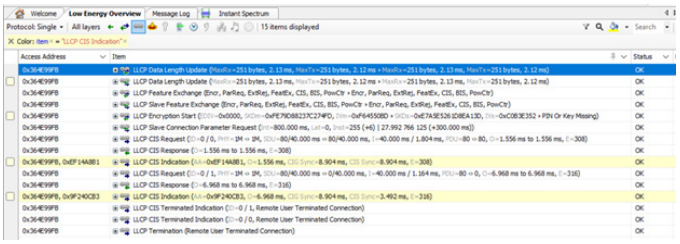


Figure 11 An ACL creating two CISes each with Unique, Randomized Access Addresses.

In **Figure 12**, the contents of the LLCP_CIS_IND packet are shown. In addition to the CIS access address, this packet also includes other important parameters to manage the isochronous transport.

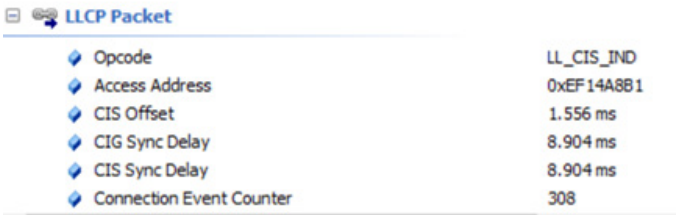


Figure 12 LLCP CIS IND Packet.

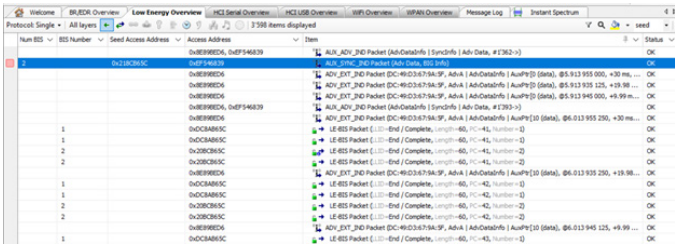


Figure 13 Advertising Sequences Showing BIG Seed Access Address and Two BIS Access Addresses.

In **Figure 13**, we see advertising packets (using the fixed AA of 0x8E89BED6) forming two BISes. The value of NumBIS in the BIGInfo field of the AUX_SYNC_IND packets = 2. These streams are created from a single BIG.

The Seed Access Address (SAA) for the BIG is 0x218CB65C (provided in AUX_SYNC_IND). This is used to create access addresses for each BIS:

1. BIS1 AA = 0xDC8AB65C
2. BIS2 AA = 0x20BCB65C

Solving Test Equipment Challenges with tzero Tracking Technology

Now that we have reviewed some fundamentals of the two isochronous transports, physical channels, encryption basics, and access addresses, we will examine what makes security for LE isochronous transports challenging for test equipment, and the benefits realized by engineers using Ellisys analyzer systems with tzero Tracking Technology.

Decrypting data carried over a CIS or a BIS requires solving several computational problems. To complicate matters, Isochronous data may begin very quickly once the link is encrypted. This requires that decryption by test equipment must be done very fast and without software intervention, to not miss any of the initial isochronous traffic.

In addition, there may be many BIGs present (public testing events, busy validation labs). Each BIG has many possible BISes (up to 31), each with their own unique access addresses and other critical data relating to security and data timings.

For a CIS, the LLCP_CIS_IND packet that contains the CIS access address may itself be encrypted. The ACL must be decrypted before the constituent CISes can be decrypted.

The challenge for capturing and decrypting a BIS (or BISes) is that the parameters of the BIG (or BIGs) must be collected, stored, and used by the analyzer system. As mentioned earlier, these parameters are provided in an AUX_SYNC_IND packet, in the BIGInfo field. Remember, these parameters include information for creation of the access addresses (the Seed Access Address), but other critical information as well, such as GIV and GSKD.

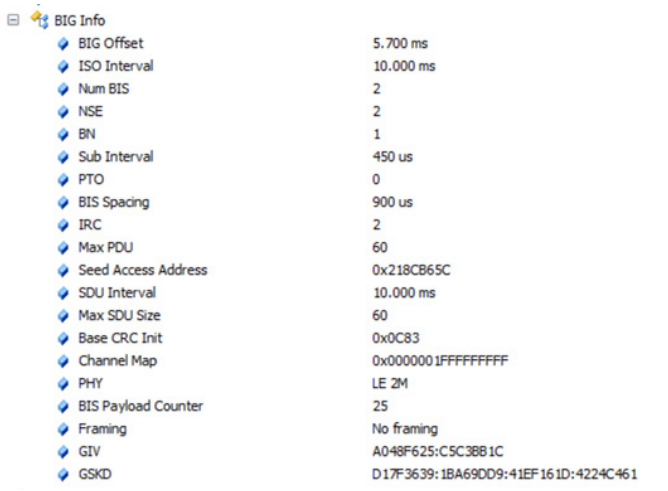


Figure 14 BigInfo Field from AUX_SYNC_IND Packet.

There are many other contextual items to be tracked by the analyzer, including codecs, capabilities, features, etc. The analyzer must manage various processes relating to each of these areas, and this cannot be easily done in hardware. If offloaded to the analyzer software, which consumes time, some BIS packets immediately following the BIS establishment will be missed.

Ellisys tzero Tracking Technology provides a method to track active BISes, in real time. With this technology, there is no need to load all possible access addresses into a table, which presents processing challenges and can lead to potential instabilities on test equipment, especially in very busy environments. There are no missed packets, no blind periods.

For CIS, the challenge is that the CIS access address is in an ACL link layer packet which can be encrypted. Test equipment hardware cannot begin decrypting CIS traffic until this access address is known.

Relying solely on security keys in hardware is limiting. There is also the processing challenge on a purely volume basis — there can be multiple CISes in a CIG, each with their own set of access addresses and other contextual information, and there can be multiple CIGs.

Without tzero, time-consuming software intervention is needed to decrypt the ACL traffic, determine various CIS/CIG parameters, and feed this back to the analyzer hardware. To decrypt this traffic live, the analyzer software must know the link key before starting the capture. If the capture is started without link key, the CIS / CIG connections cannot be determined and will be invisible to the sniffer.

With tzero, the CIS connections will actually be captured even if the link key is not known.

Summary

Audio remains one of the prime applications for Bluetooth Technology. While BR/EDR (Classic Bluetooth) implementations will surely continue to account for a substantial portion of Bluetooth audio products, new products that use applications made possible by LE Audio are now on the way. These new applications, built around the concepts of audio streaming, broadcast, and audio sharing, will bring on new consumer products, new test requirements for developers, and new approaches to how we all use Bluetooth technology.

Ensuring developers have the highest quality, most capable tools, at the earliest possible time is at the center of the Ellisys philosophy. Building tools that are extensible and can track developments in the Bluetooth specifications is also paramount. With Bluetooth 5.2 and the accompanying set of new audio features, this philosophy and the extensibility factor set the groundwork for new development for Ellisys Bluetooth analysis products to meet requirements for LE audio test and development.

With LC3 Auto-Detect and tZERO Tracking Technology, Ellisys engineers continue the spirit of innovation that has made Ellisys products the worldwide choice of engineers involved in wireless technology applications.

Other Interesting Reading

- EEN_BT02 - Analyzer Features Tour
- EEN_BT04 - Optimal Placement of Your Analyzer
- EEN_BT05 - Understanding Antenna Radiation Patterns

More Ellisys Expert Notes available at:
www.ellisys.com/technology/expert_notes.php

Feedback

Feedback on our Expert Notes is always appreciated. To provide comments or critiques of any kind on this paper, please feel free to contact us at expert@ellisys.com

Sales Contact:

USA: +1.866.724.9185
Asia: +852 3073 2033
Europe: +41 22 777 77 89

sales@ellisys.com

www.ellisys.com

Connect with us.