

Isolating Bluetooth Devices in Crowded Environments

Physical Optimization and Software Approaches - Best Practices

Introduction

Bluetooth technology is everywhere, enabling effortless wireless communication among a vast array of devices. With fitness trackers, smartwatches, headphones, and industrial sensors crowding the modern landscape, the number of Bluetooth signals in the air can be overwhelming.

In test and debug environments, like development labs and UPFs, Ellisys protocol analysis tools play a key role in characterizing, validating, and debugging Bluetooth devices and stacks. Here, engineers face challenges in finding and focusing on their devices amid the large number of devices typically present.



At a UPF, optimizing the physical setup and analysis configuration becomes essential to get the most out of your limited test time and keep the focus on your devices and the tasks at hand. There are bugs to clear, features to validate, and limited time slots in which to execute these efforts. Understanding the techniques available to drill down from huge amounts of traffic to very specific traffic is key to making the engineer's test time as efficient as possible.

In this Expert Note, we will outline a physical approach to desensitizing the capture process using attenuation and externalized, mobile antennas. This approach will “hide” device transmissions that are not very close, thus reducing the device clutter on the analyzer's user interface and creating an improved focus on your devices.

We will also provide some tips on software approaches that can be used to isolate your devices.

Physical Setup Optimizations for UPF

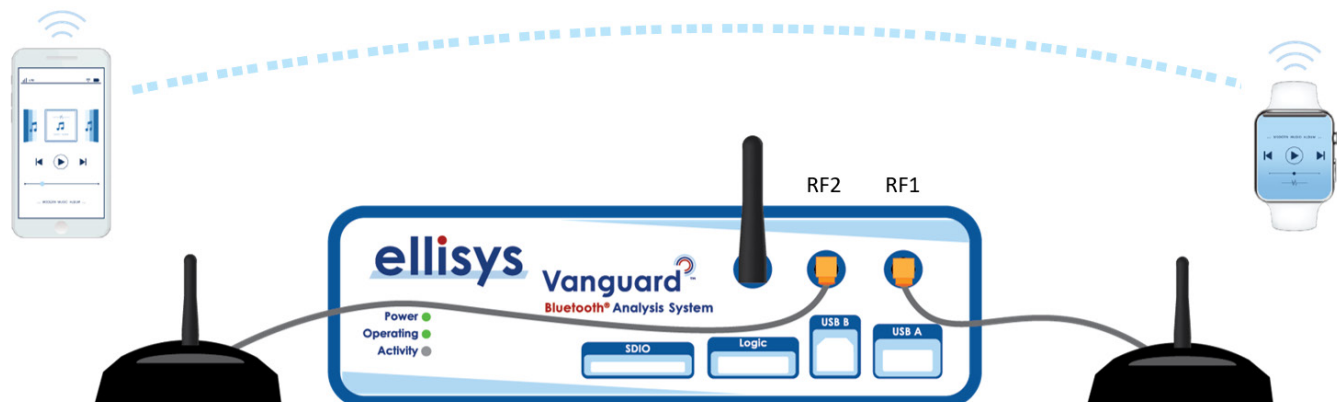
This is by far the most important step to get proper captures and ensure the most streamlined analyzer experience. The goal is to capture all traffic between the two devices of interest (your DUT and a partner's DUT) while minimizing everyone else's chatter. The trick is simple: put the antennas close to each DUT, add controlled attenuation, and make sure any **conducted** path between antennas (via cables/splitters) is weaker than the **over-the-air** path you want to test.

Two-Port Analyzers (Bluetooth Vanguard with Capture Diversity)

The setup is facilitated by the dual-port capability of the analyzer. Instead of connecting the antennas directly to the analyzer unit itself, typically on the RF1 and RF2 ports, coax cables are used to move the antennas close to the DUTs.

Procedure

- Use two coax cables from the analyzer's two RF ports to two separate antennas, one placed by each DUT.
- Set analyzer gain (Recording Options) to a nominal -15dB, to be fine-tuned depending on the DUTs TX power to get a reported High or Average RX quality (as shown in the Details view in the analyzer application).



Single-Port Analyzers (Bluetooth Explorer / Bluetooth Tracker)

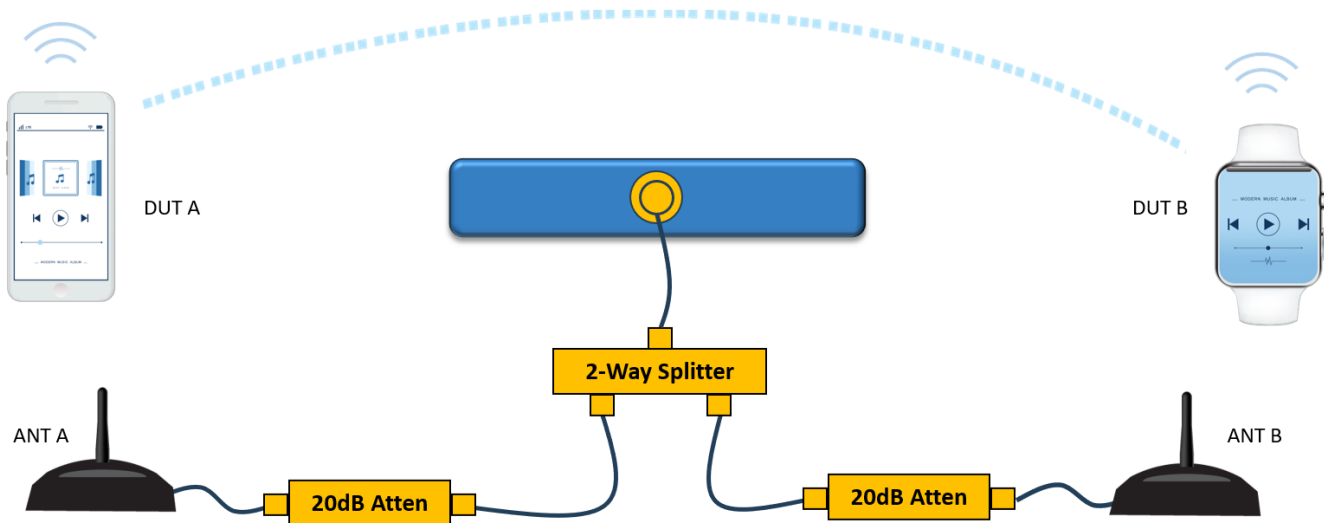
The setup is a bit more intricate but still workable with proper RF accessories. The two antennas need to be combined in this case, typically with a splitter. This alone isn't sufficient though, as this creates a low loss conducted path between antennas via the splitter, so DUTs "talk through the cable," not the air. This might be acceptable, but an added value of test events such as UPFs is that besides testing against other prototypes, the busy environment itself brings additional challenges which highlight certain bugs or inefficiencies that aren't seen otherwise.

To ensure devices communicate wirelessly, the conducted path shall have more attenuation than the wireless path. This can be achieved by adding a 20dB attenuator to each antenna, so the antennas will be isolated by 40dB, plus the splitter loss.

This approach is equivalent to about two meters wirelessly, so devices should be placed at less than 2 meters for this to be effective.

Procedure

- Place Antenna-A ~10–20 cm from DUT-A; same for Antenna-B to DUT-B.
- Add 20dB fixed attenuators at each antenna.
- Combine via a 2-way splitter.
- Set analyzer gain to a nominal +6dB, to be fine-tuned depending on the DUTs TX power to get a reported High or Average RX quality (as shown in the Details view in the analyzer application).



Software Filtering Strategies for Isolating Devices

The strategies covered in this section may not be needed if you're using the physical setup described above. The table below is a quick summary of these strategies, followed by more detail.

For a complete list of filter strategies, refer to Expert Note EEN_BT08 – Separating the Wheat from the Chaff, located in the Welcome view of the application.

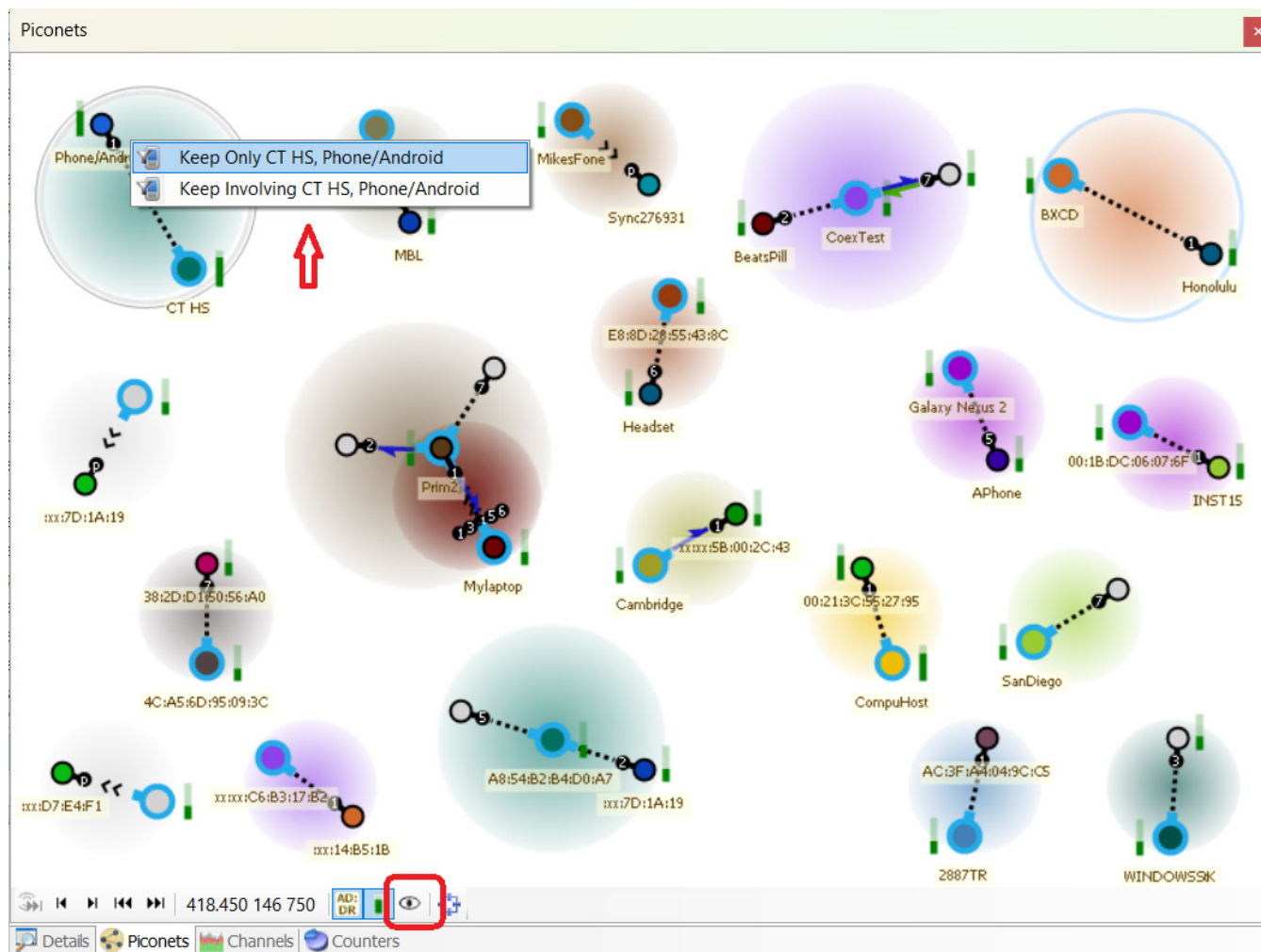
Function	Action
Piconets view	Hide Broadcast (toolbar)
Global filter menu	Hide Establishment traffic
Overview Communication Column	Right-click → Keep Only
Know only one BD_ADDR?	Use a Keep Involving, then refine
Know neither BD_ADDR? If no address: Service UUID	Device Database search by concatenated Name / Mfg Data
Still cluttered?	Packet-only view → RSSI ≥ -45 dBm → right-click Communication column

One of the simplest and quickest filters available is the Broadcast filter located in the Piconets view. This filter shows or hides broadcast traffic broadcast (e.g., advertising and non-connectable device traffic). Eliminating this ubiquitous traffic is often a good first step to removing device clutter.

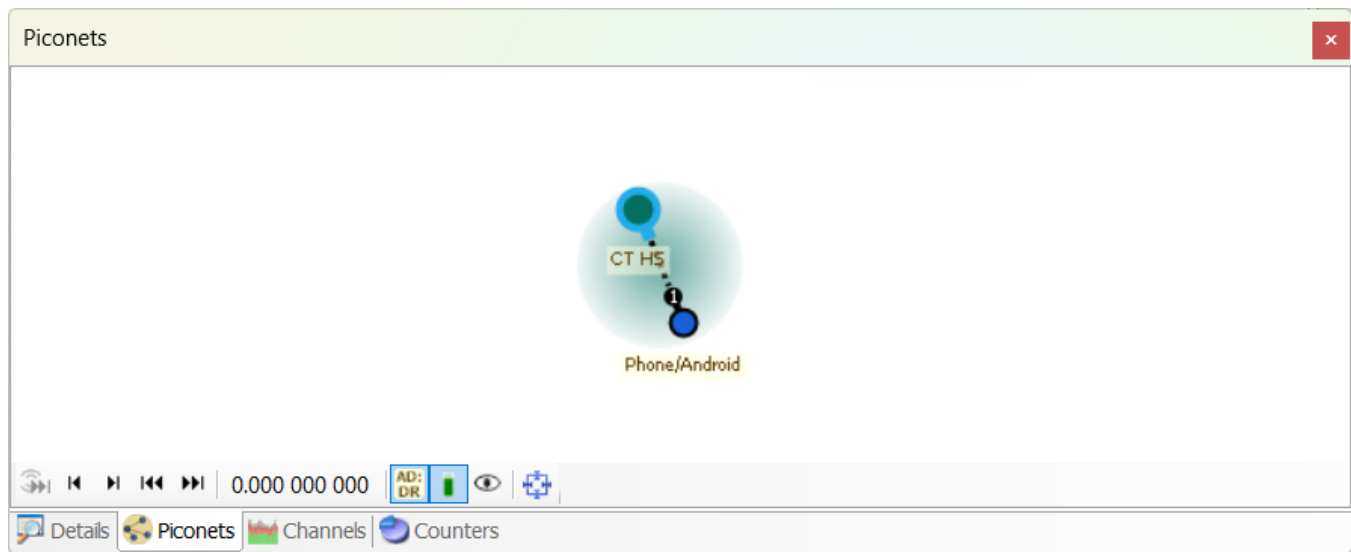
Device-based filtering can be enacted directly from the Piconets view. Below, we de-select the “Broadcast” icon on the toolbar.

The idea here is to find your piconet visually and quickly, and often this approach is the simplest.

Once the piconet of interest is located, right-click then select Keep Only.



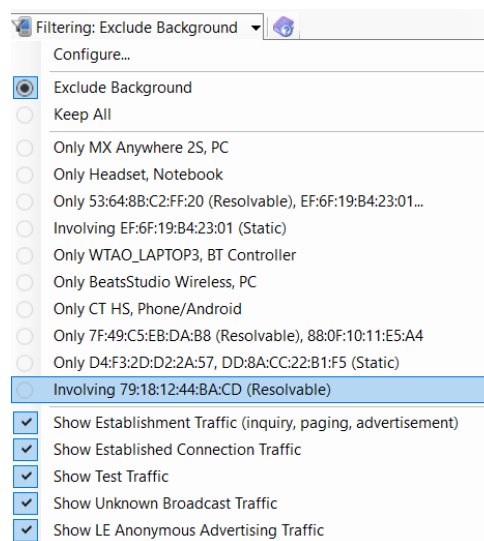
The result is shown below. With the device filter now enabled, all analyses and characterizations throughout the analyzer software are now focused solely on the devices subject to the filter criteria.



Tip: Once your device filter is applied, it's always a good idea to re-enable broadcast traffic (show), as you'll likely want to see any such traffic that is associated with your devices of interest.

Establishment Traffic Filter (Global)

This filter is accessible in the Filtering drop-down at the top of the user interface.



Security View

As devices pair, bond, and connect, the Security view will post an entry as shown below (green indicates a decrypted connection). Often, it is sufficient to connect your devices and watch for a corresponding entry as the first step in creating your filter. Right-click on your device pair in the Devices column to enact a global device filter.

Security					
Fill missing fields			Manage Mesh Security Manage ECDH Keys		
Time	Devices	PIN / TK	Key	ACO	IV
62.300 710 625 oo	"PC" A4:02:B9:CE:3A:B4~4C:FE:31:... "MX Anywhere 2S" D5:72:A9:6C:AA...	Just Works	50ABE204:FA941F78:8856136D:BE8CEF3A	Not applic...	4ADAF273:DDCE6EB3

Selecting the timestamp in the Security view's Time column synchronizes all views to the security exchange (Overview shown below).

Welcome

WiFi Overview

Low Energy Overview

Protocol: Single

All layers

7463 items displayed

4 selections / 900.371 ms

Device Database

The Device Database is located in the Devices dialog and is accessed from the Filtering drop-down menu located on the main toolbar, using the **Configure** selection. Use the Search Box here to search for your device's BD Address or other characteristics specific to your device. Search wildcards are available to ease the search. Add desired devices to the **Traffic Filtering Criteria**.

Devices

Traffic Filtering Criteria

Keep Only Selected Devices

Clear

Add

Name	Radio
<div><div></div>"BeatsStudio Wireless" 04:88:E2:76:16:51</div>	Classic
<div><div></div>"PC" A4:02:B9:CE:3A:B4</div>	Dual Mode

Device Database

New Device

Edit

Delete

Favorite

Search:

View: All Devices

194 devices

Name	Address	Address Type	Radio Cap...	Transmitted Name	Company ID
PC	A4:02:B9:CE:3A:B4	Public	Dual Mode	CHUCKHPLAPTOP[TA...	Intel Corporate
BeatsStudio Wireless	04:88:E2:76:16:51	Public	Classic	BeatsStudio Wireless	Beats Electronics LLC
PC	A4:02:B9:CE:3A:B4	Public	Dual Mode	CHUCKHPLAPTOP[TA...	Intel Corporate
SS18TPM Device	4C:35:AC:63:0F:57	Resolvable	Low Energy	SS18TPM Device	
A4:E4:B8:10:CE:E8	A4:E4:B8:10:CE:E8	Public	Classic		BlackBerry RTS
Gear S (63EE)	38:2D:D1:50:63:EE	Public	Dual Mode	Gear S (63EE)	Samsung Electronics ...
ALPS-03	16:34:56:55:2A:BC	Public	Classic	ALPS-03	
HSIAOKAI	0C:84:DC:DD:8D:...	Public	Classic	HSIAOKAI	Hon Hai Precision Ind...
OS-WIN-DL12	00:02:5B:02:DE:AD	Public	Classic	OS-WIN-DL12	Cambridge Silicon Ra...
xx:xx:E2:F7:15:EC	xx:xx:E2:F7:15:EC	Public	Classic		

OK

Cancel

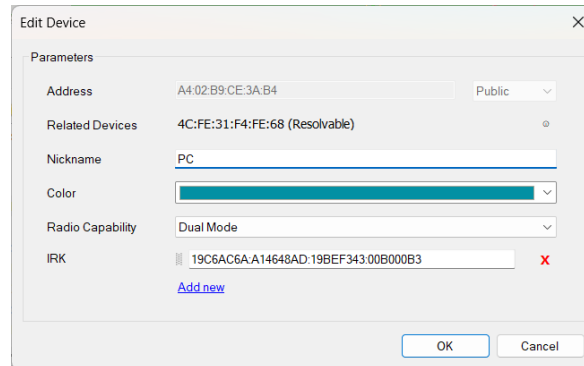
Apply

Device Database - Filtering by Concatenated NAME

The Device Database contains a list of all devices captured in the current trace, and historically, along with a collection of attributes. The **Name** column is a handy concatenation from multiple available sources, such as BD Address, Broadcast Name, transmitted name, custom name, etc.

Device Database - Resolvable Private Addresses

Add the IRK to when Resolvable Private Addressing (RPA) is in use. The user can add the IRK to the application to resolve to the Identity Address. The **Edit Device** dialog from the Device Database is below. If the IRK is captured via security exchanges, it is populated there automatically.

The image shows a screenshot of the 'Edit Device' dialog box. It has a title bar with a close button. The main area is titled 'Parameters' and contains several fields: 'Address' with the value 'A4:02:B9:CE:3A:B4' and a dropdown set to 'Public'; 'Related Devices' with the value '4C:FE:31:F4:FE:68 (Resolvable)' and a small circular icon; 'Nickname' with the value 'PC'; 'Color' with a blue color selection bar; 'Radio Capability' with a dropdown set to 'Dual Mode'; and 'IRK' with a text field containing '19C6AC6A:A14648AD:198EF343:00B000B3' and a red 'X' icon. Below the IRK field is a link that says 'Add new'. At the bottom right are 'OK' and 'Cancel' buttons.

Device Database - Adding the IRK in Advance

The IRK can also be manually added, in advance of the capture. The user can create a **New** device in the Device Database. Use the Identify Address if known, or use a place holder address, like DE:AD:C0:FF:EE. Give it a nickname (recommended). Any further RPA that can be resolved with this IRK will be associated with this added device.

Tip: Giving your device a Nickname can be helpful in visualizing your device throughout the software application and for search and filter functions.

Device Database - Filtering by Transmitted Name

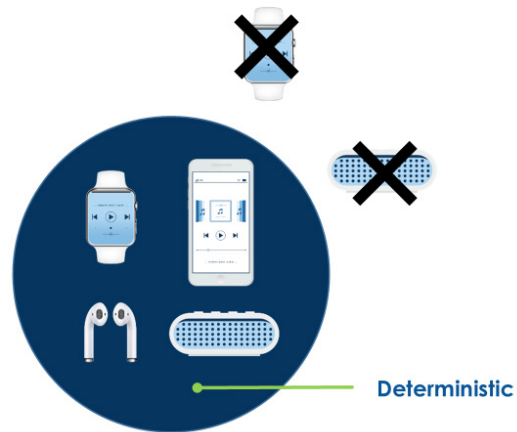
Device names (Transmitted Names) are helpful when BD Addresses are unavailable or randomized due to privacy features. Often, device names reflect the product or user.

Tip: Transmitted names may be truncated or absent in advertisements; sometimes a full GATT connection is needed for the complete name.

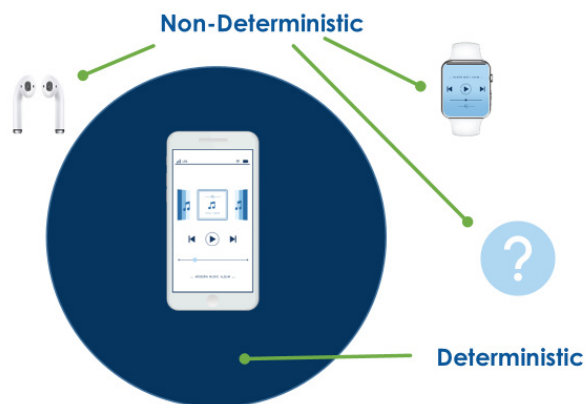
Keep Only and Keep Involving Filters

Keep Only and Keep Involving device filters are common options throughout the Ellisys software.

The **Keep Only** filter is fully deterministic and applies specifically to the selected devices (BD ADDR). Once enacted, all characterizations apply only to the devices subject to this filter.



The **Keep Involving** filter is *partially* deterministic and will show traffic that is likely addressed to the specified devices, but some unwanted traffic like broadcast might be displayed as it could be related. Use this when you know one BD address but not the other.



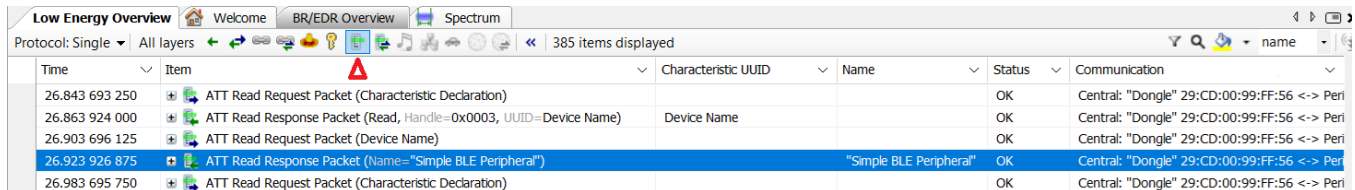
Tip: Start with Keep Involving on the known device's address (this declutters things nicely), then refine to a Keep Only filter once the paired device is found.

Filtering by Service UUIDs

Bluetooth LE devices advertise Service UUIDs to indicate their capabilities, such as “Heart Rate” or “Temperature.” You can use the Ellisys filtering tools to isolate devices advertising your expected Service UUIDs.

Below, the Low Energy Overview is opened and an ATT protocol filter is enabled. The Characteristic UUID and Name fields from the Details view have been dragged over to the Overview from Details. We see all Names advertised, in this case “Simple BLE Peripheral.”

Use the text Query filter in the Overview to show only lines populated in the Name field (use an asterisk), or you can specify a Name to show. Right click on the associated Communication field to enact a device filter.



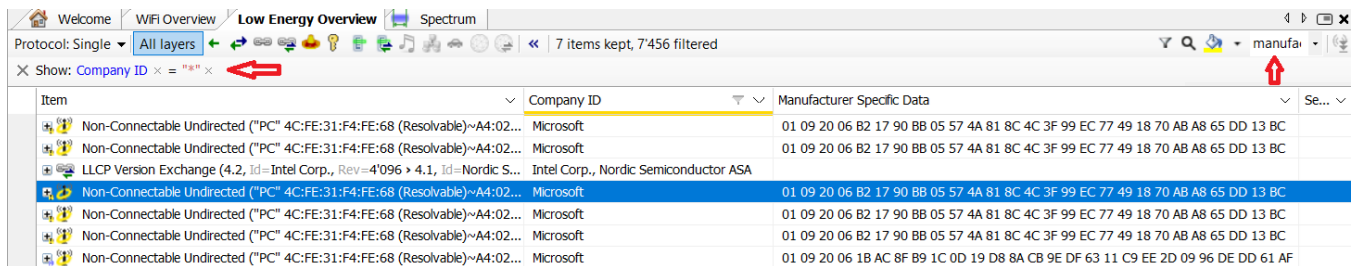
Time	Item	Characteristic UUID	Name	Status	Communication
26.843 693 250	ATT Read Request Packet (Characteristic Declaration)			OK	Central: "Dongle" 29:CD:00:99:FF:56 <-> Peri
26.863 924 000	ATT Read Response Packet (Read, Handle=0x0003, UUID=Device Name)	Device Name		OK	Central: "Dongle" 29:CD:00:99:FF:56 <-> Peri
26.903 696 125	ATT Read Request Packet (Device Name)			OK	Central: "Dongle" 29:CD:00:99:FF:56 <-> Peri
26.923 926 875	ATT Read Response Packet (Name="Simple BLE Peripheral")		"Simple BLE Peripheral"	OK	Central: "Dongle" 29:CD:00:99:FF:56 <-> Peri
26.983 695 750	ATT Read Request Packet (Characteristic Declaration)			OK	Central: "Dongle" 29:CD:00:99:FF:56 <-> Peri

Filtering by Manufacturer Specific Data

Capture and filter to show only specific information contained in Bluetooth LE advertisements to match the required data pattern to what you expect from your devices (e.g., first bytes for manufacturer, next bytes for model).

Manufacturer-specific fields provide detailed identification, such as model numbers, firmware version, or internal codes.

In the figure below, we are not using any protocol filters (having selected “All Layers”). The Company ID and Manufacturer Specific Data fields are added. A text Query (an asterisk) is used to show only lines where Company ID is populated. Right click on the associated Communication field to enact a device filter. Note that search, filter, and colorize functions can work whether the subject column(s) is/are in view.



Item	Company ID	Manufacturer Specific Data	Se...
Non-Connectable Undirected ("PC" 4C:FE:31:F4:FE:68 (Resolvable)~A4:02...	Microsoft	01 09 20 06 B2 17 90 BB 05 57 4A 81 8C 4C 3F 99 EC 77 49 18 70 AB A8 65 DD 13 BC	
Non-Connectable Undirected ("PC" 4C:FE:31:F4:FE:68 (Resolvable)~A4:02...	Microsoft	01 09 20 06 B2 17 90 BB 05 57 4A 81 8C 4C 3F 99 EC 77 49 18 70 AB A8 65 DD 13 BC	
Non-Connectable Undirected ("PC" 4C:FE:31:F4:FE:68 (Resolvable)~A4:02...	Microsoft	01 09 20 06 B2 17 90 BB 05 57 4A 81 8C 4C 3F 99 EC 77 49 18 70 AB A8 65 DD 13 BC	
Non-Connectable Undirected ("PC" 4C:FE:31:F4:FE:68 (Resolvable)~A4:02...	Microsoft	01 09 20 06 B2 17 90 BB 05 57 4A 81 8C 4C 3F 99 EC 77 49 18 70 AB A8 65 DD 13 BC	
Non-Connectable Undirected ("PC" 4C:FE:31:F4:FE:68 (Resolvable)~A4:02...	Microsoft	01 09 20 06 B2 17 90 BB 05 57 4A 81 8C 4C 3F 99 EC 77 49 18 70 AB A8 65 DD 13 BC	

Filtering by RSSI to Find a Nearby Device

RSSI values correlate to device proximity. Filtering on RSSI values can help isolate devices located near the analyzer's antenna(s). Use the Query filter. Flyover filter icons are above each column, fixed icons are at top-right of the Overview.

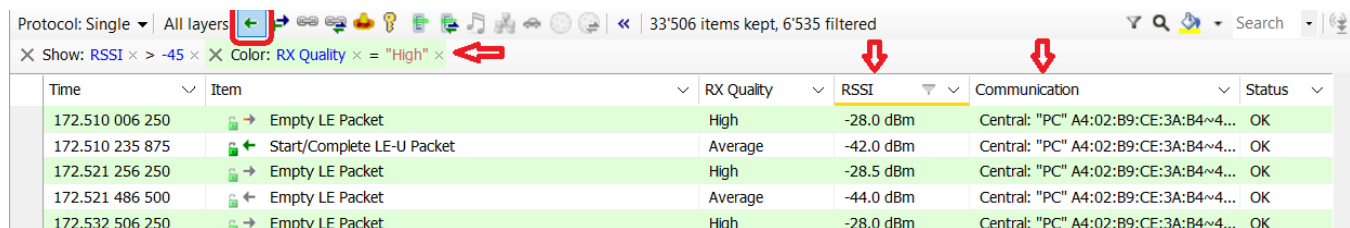
Enable packet-only view, implement the Query filter to show only packets stronger than a certain signal strength threshold. Colorize if helpful.

Right click on the associated Communication field to enact a device filter.

Below, packet-only view is enabled (single arrow icon). The filter will show only packets stronger than -45dBm. We added the RX Quality and RSSI columns (not absolutely needed for the filter to operate, but intuitive and can be selected for Query operations with a right-click on the column/row intersection).



Below, our "Greater than -45" RSSI filter is enabled. Lines with "High" RSSI are colorized.



Time	Item	RX Quality	RSSI	Communication	Status
172.510 006 250	Empty LE Packet	High	-28.0 dBm	Central: "PC" A4:02:B9:CE:3A:B4~4...	OK
172.510 235 875	Start/Complete LE-U Packet	Average	-42.0 dBm	Central: "PC" A4:02:B9:CE:3A:B4~4...	OK
172.521 256 250	Empty LE Packet	High	-28.5 dBm	Central: "PC" A4:02:B9:CE:3A:B4~4...	OK
172.521 486 500	Empty LE Packet	Average	-44.0 dBm	Central: "PC" A4:02:B9:CE:3A:B4~4...	OK
172.532 506 250	Empty LE Packet	High	-28.0 dBm	Central: "PC" A4:02:B9:CE:3A:B4~4...	OK

Conclusion

Effectively isolating specific Bluetooth devices in a crowded environment is crucial for modern wireless systems. At a UPF, the physical setup optimization outlined here is the first priority. By making use of the full set of filtering options—BD Address, device name, service UUIDs, manufacturer data, and RSSI—within the Ellisys Bluetooth Protocol Analyzer, developers and engineers can accomplish precise and reliable device selection. Combining filters, understanding platform constraints, and real-world testing ensure robust results. With thoughtful implementation, Bluetooth device isolation is both efficient and reliable, delivering secure and seamless wireless experiences.

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

Connect With Us

