

Tech Talks LIVE Schedule – Presentation will begin shortly



How to Measure and Debug Network Performance - Using Silicon Labs Network Analyzer	Thursday, May 7
RF Regulatory and Qualification Testing for Bluetooth, Zigbee & Z-Wave	Tuesday, May 12
Simplicity Studio Tips & Tricks: Our FAEs Know All The Tricks - Improve Your Life in Simplicity Studio	Thursday, May 14
Wireless Module vs Wireless SoC Tradeoffs and Decision Making Criteria	Tuesday, May 19
Thunderboard BG22 Unboxing. You Have Our Kit... What Can You Do With It?	Thursday, May 21
Designing in Bluetooth using Bluetooth Xpress Modules with Minimal Code Writing	Tuesday, May 26
Overview of Silicon Labs Wi-Fi Solutions (Including Redpine Signals Wi-Fi Solutions)	Thursday, May 28

Please take the 3 question poll while waiting and be entered to receive a BG22 Starter Kit.



Find Past Recorded Sessions at:
<https://www.silabs.com/support/training>



WELCOME



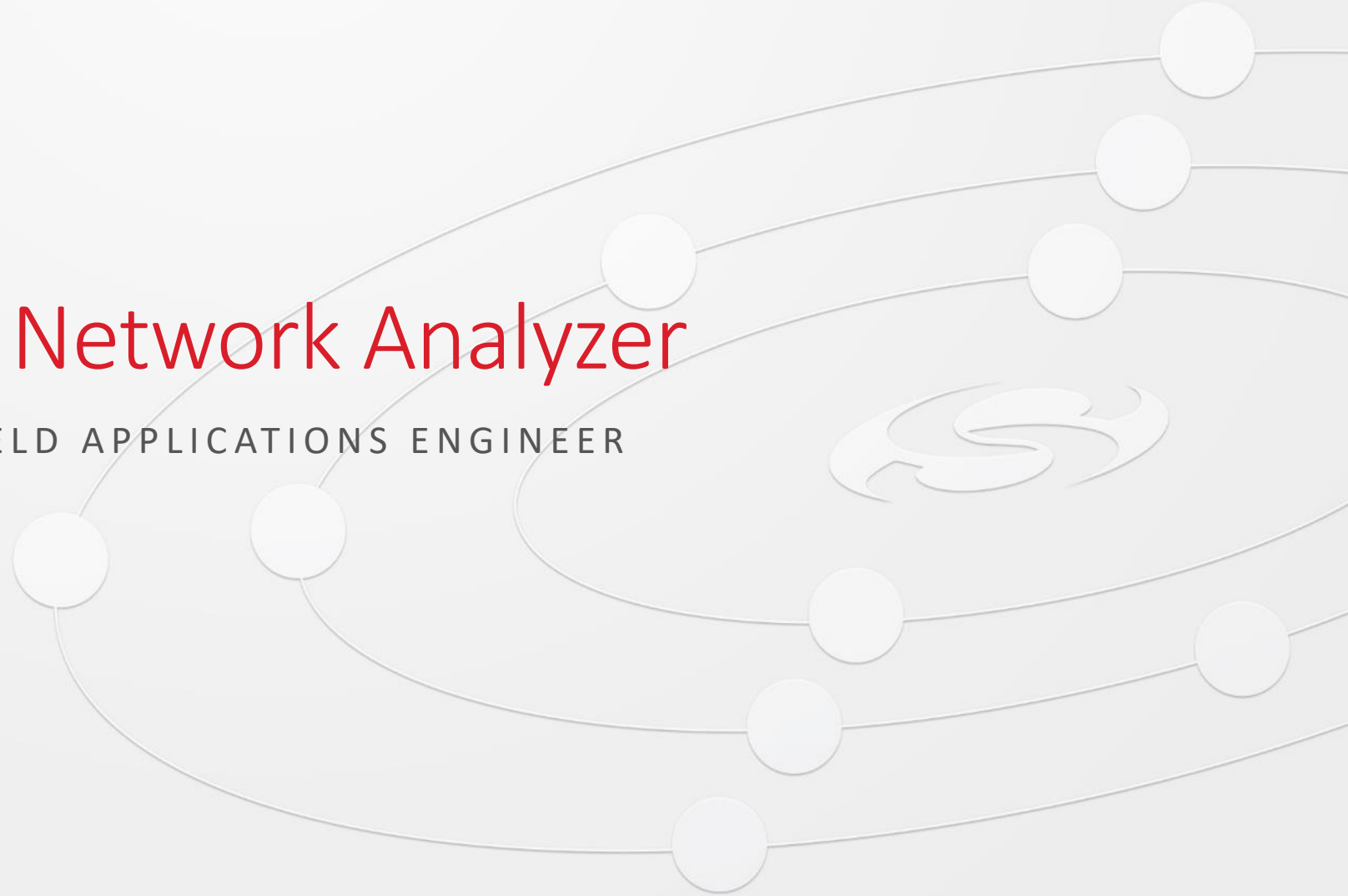
Silicon Labs LIVE:
Wireless Connectivity
Tech Talks

A blue background with a pattern of white circuit board traces and code snippets. The code includes comments like '/* Bluetooth connection */' and '/* UART connection */', and function names like 'BTTL_Init()', 'BOARD_Init()', 'BUTTON_Init()', 'void Init()', and 'cb_InitGetCircularBuf()'. There are also some numbers like '100' and '4'.



Simplicity Studio - Network Analyzer

MAY 2020 – JAKE JOHNSON, FIELD APPLICATIONS ENGINEER



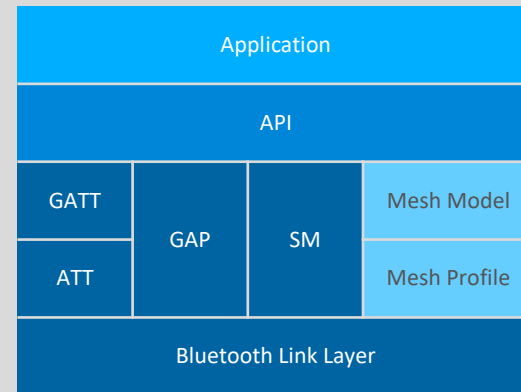
A Complete Solution for Enabling Wireless Products

SoCS AND MODULES



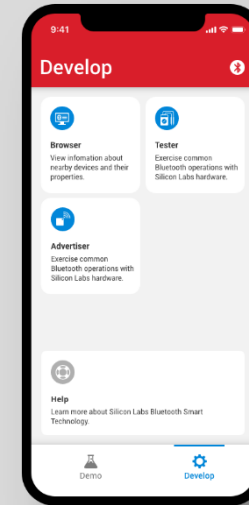
Industry leading Zigbee, Thread, Bluetooth 5.2, and proprietary SoCs and pre-certified modules

STACK SOFTWARE



In-house developed stacks with latest Zigbee, Thread, Bluetooth 5.2 and mesh features

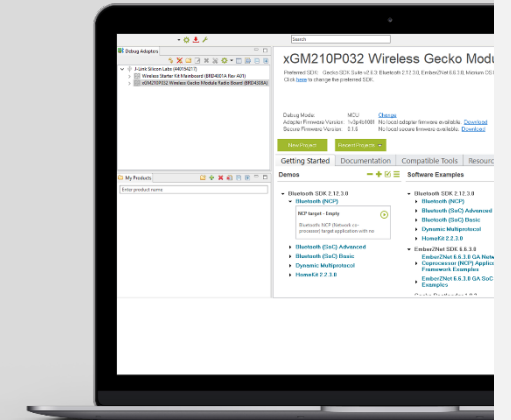
MOBILE APPLICATIONS



Reference applications and source code for iOS and Android





Phone interoperability test program

DEVELOPMENT TOOLS



Free-of-charge development and protocol analysis tools to boost productivity

A Common Platform

	 Bluetooth®	 THREAD	 zigbee	FLEX SDK  Proprietary		
Application	Customer Application		Customer Application	Customer Application		
	GATT (profiles / services)	Mesh Models (e.g. lighting)	Application Layer (e.g. dotdot, CoAP)		Application Profile (e.g. HA1.2, ZLL, dotdot)	
Network / Transport	Bluetooth LE Core	Bluetooth Mesh Core	UDP	Zigbee Core Stack	Connect Stack	
			IPv6, Mesh Routing			Customer Proprietary Stack
			6LoWPAN			
Link	Bluetooth Link Layer		IEEE 802.15.4 MAC	IEEE 802.15.4 like MAC		
Physical	Bluetooth PHY (2.4 GHz)		IEEE 802.15.4 PHY (2.4 GHz)	IEEE 802.15.4 PHY (2.4 GHz)	Proprietary PHY (2.4 GHz or Sub-GHz)	
Platform	RAIL		RAIL	RAIL	RAIL	
	Common Bootloader		Common Bootloader	Common Bootloader	Common Bootloader	

The Right Tool Set – Simplicity Studio™

Wireless and MCU design made simple



- Cross platform development environment for MCU and Wireless products
- Eclipse-based IDE
- Complete Documentation
- Demos / Software Examples
- Advanced Tools
 - AppBuilder
 - Radio Configurator
 - Commander
 - Energy Profiler
 - Network Analyzer

Single Tool for Development

Overview

Network Analyzer

- Radio packet tracing in real time
- Simultaneous capture from multiple nodes
- Debug Multiple wireless protocols
- Debug Multiprotocol networks (Zigbee & BLE)
- Developed by our own networking engineers to develop and debug our stacks

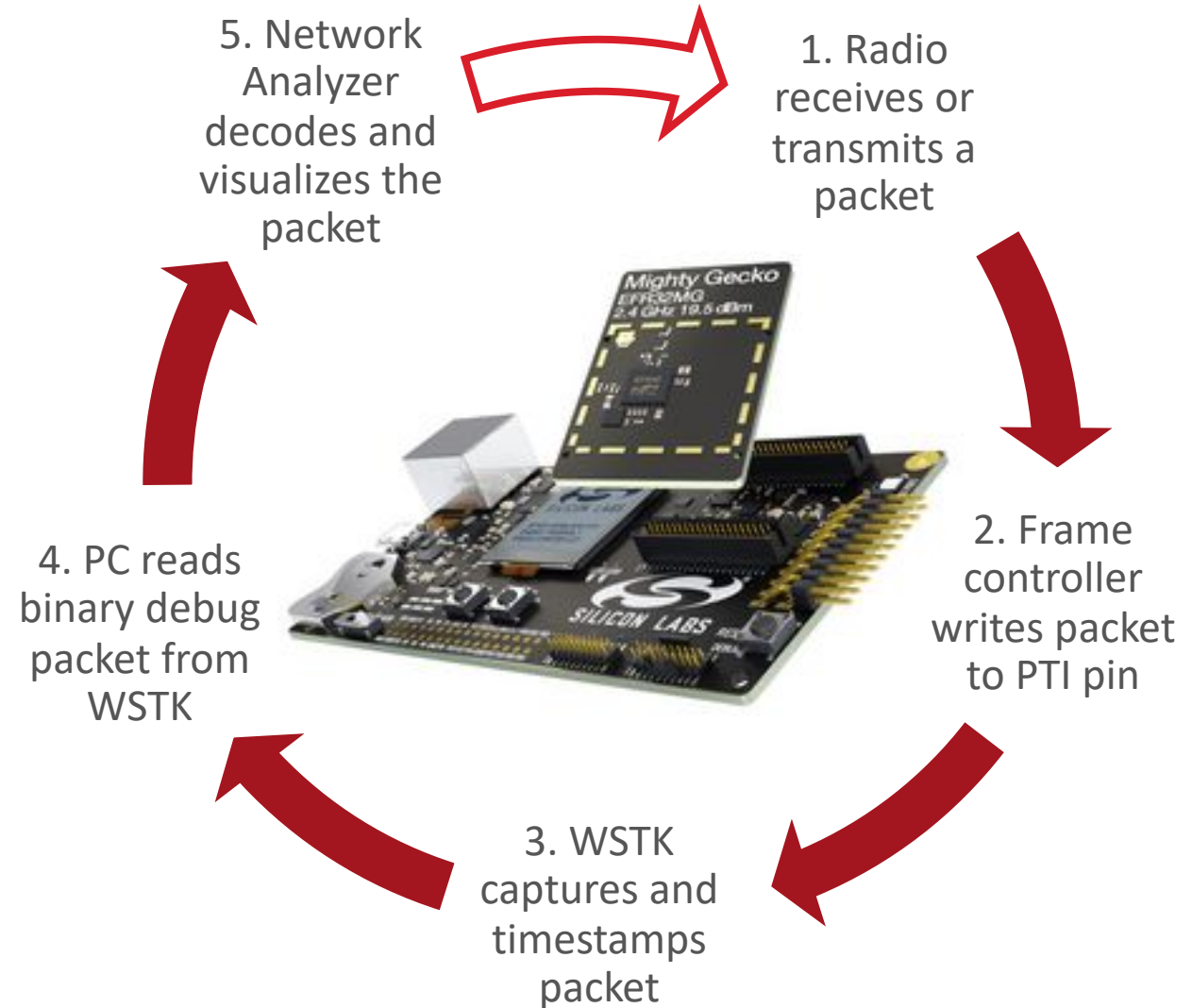
The screenshot displays the Network Analyzer software interface. The top window shows a network diagram with nodes and their connections. The middle window shows a list of transactions with columns for Time, Duration, Summary, NWK Src, NWK Dest, P#, M#, E#, and Status. The bottom window shows event details, including IEEE 802.15.4 packet information and a hex dump.

Time	Duration	Summary	NWK Src	NWK Dest	P#	M#	E#	Status
13.181.052000	0.289	ZCL: QueryNextImageRequest	9CAA	0000	4			
13.181.347000	0.024	ZCL: QueryNextImageResponse	0000	9CAA	4			
13.213.839000	1.045	Many-to-One Route Discovery	0000	FFFC	23			
13.224.076000	0.927	Many-to-One Route Discovery	0000	FFFC	24			
13.226.434000	0.014	Rejoin Request	7652	91DE	4			
13.226.449000	0.006	Route Record	91DE	0000	2			
13.226.488000	0.006	Update Device	91DE	0000	2			

Time	Type	Summary	MAC Src	MAC Dest	Status
13.181.052000	Packet	ZCL: QueryNextImageRequest	9CAA	0000	
13.181.058000	Packet	802.15.4 Ack	0000	9CAA	
13.181.202000	Packet	Link Status	1589	FFFF	
13.181.332000	Packet	Data Request	9CAA	0000	
13.181.335000	Packet	802.15.4 Ack	0000	9CAA	
13.181.336000	Packet	APS Ack	0000	9CAA	
13.181.341000	Packet	802.15.4 Ack	9CAA	0000	

Packet Trace Interface (PTI)

- Direct feedback from baseband radio
 - Raw TX and RX packet
 - Timestamp, RSSI, channel, protocol, etc.
- Implemented in hardware and radio sequencer
 - Dedicated UART/SPI interface
 - Zero overhead to Cortex code
- Captured and timestamped by Wireless Starter Kit (WSTK)



Development Hardware

Radio pin access headers for prototyping

Radio card header for easy swapping

Integrate J-Link debugger
Connect via USB or Ethernet
Virtual Com Port support
Packet Trace
Energy Profiler

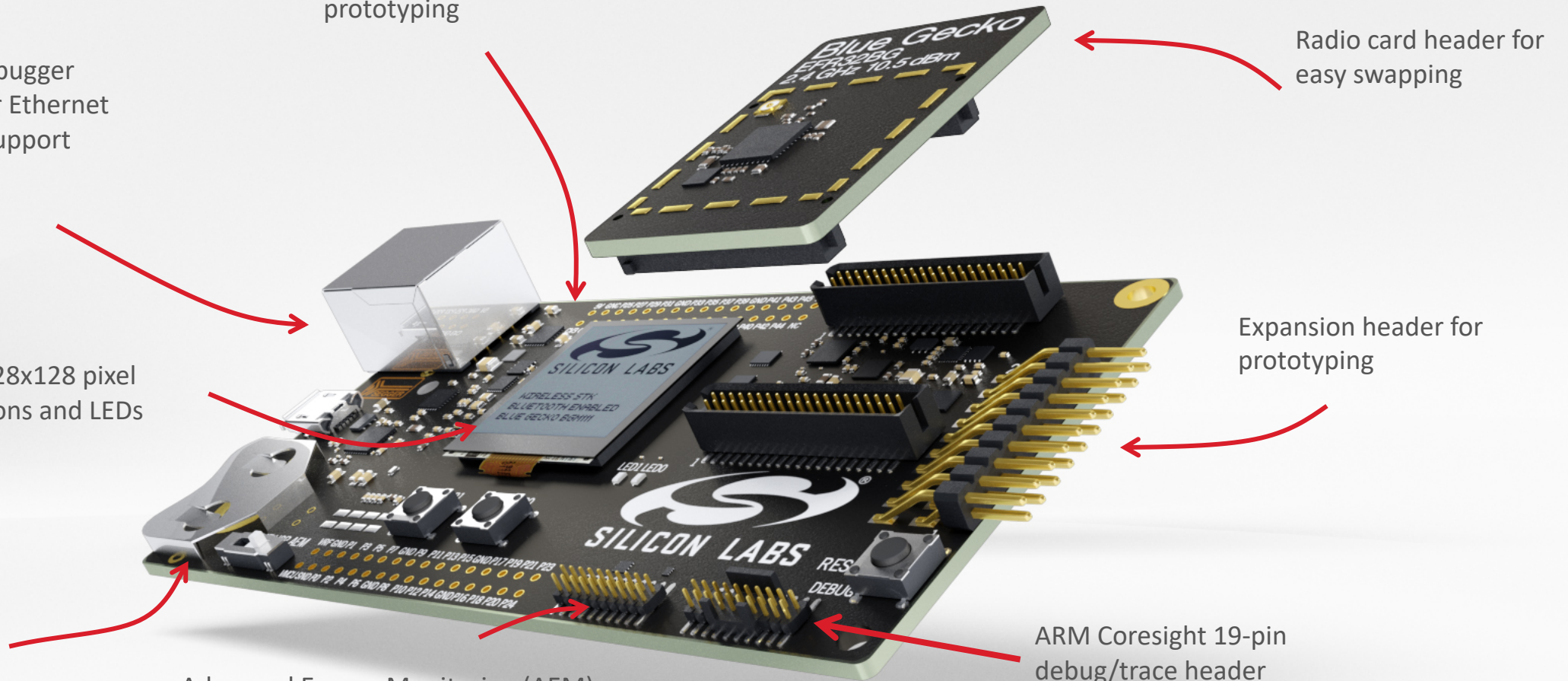
Ultra-low power 128x128 pixel
memory LCD, buttons and LEDs

Expansion header for
prototyping

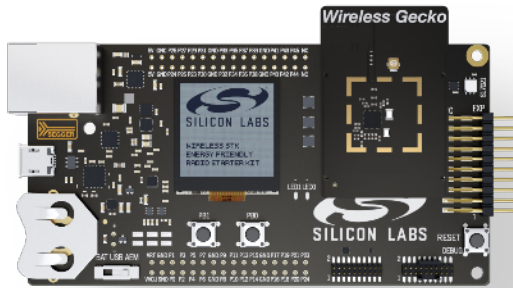
USB Power or
Battery Power

Advanced Energy Monitoring (AEM)
USB Serial Port
Packet Trace Port

ARM Coresight 19-pin
debug/trace header



Getting Started with BG22 SoCs



BG22 SoC Starter Kit
SLWSTK6120A



Thunderboard BG22
SLTB010A

SLWSTK6120A

1x WSTK main boards
1x SLWRB4182A radio boards (QFN40)
1x SLWRB4183A radio boards (QFN32)

SLWRB4182A

BG22 +6 dBm radio board (QFN40)

SLWRB4183A

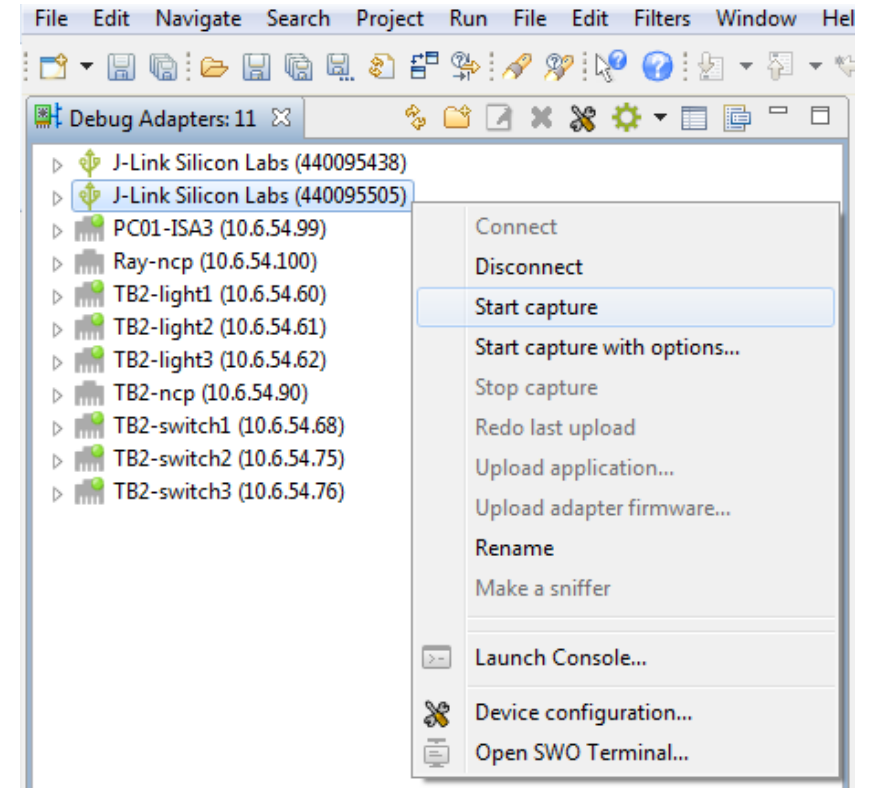
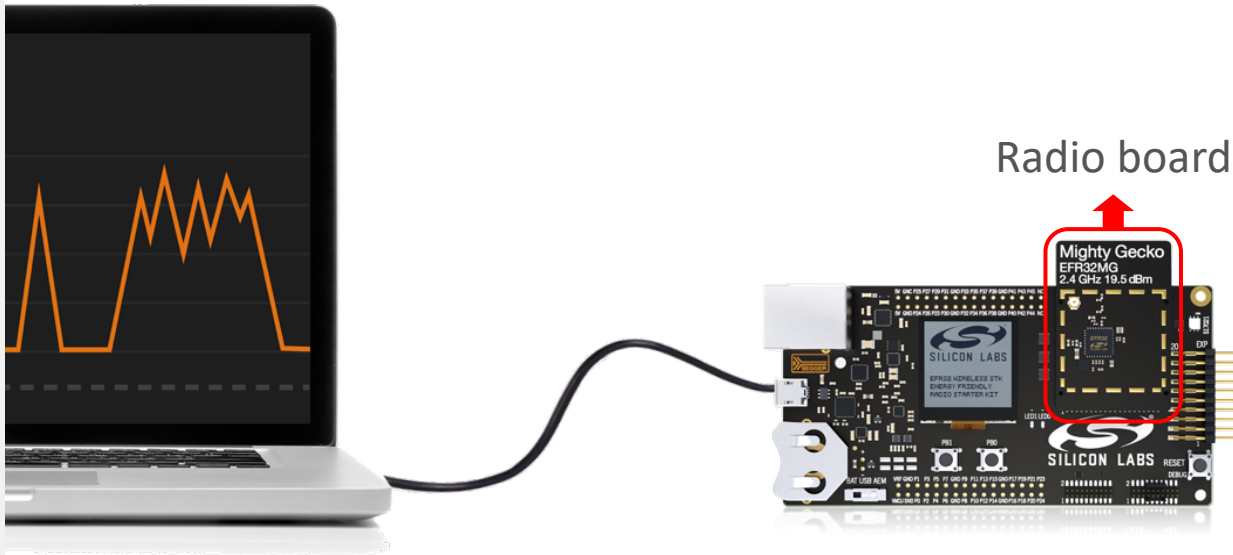
BG22 +6 dBm radio board (QFN32)

SLTB010A

Thunderboard BG22 kit

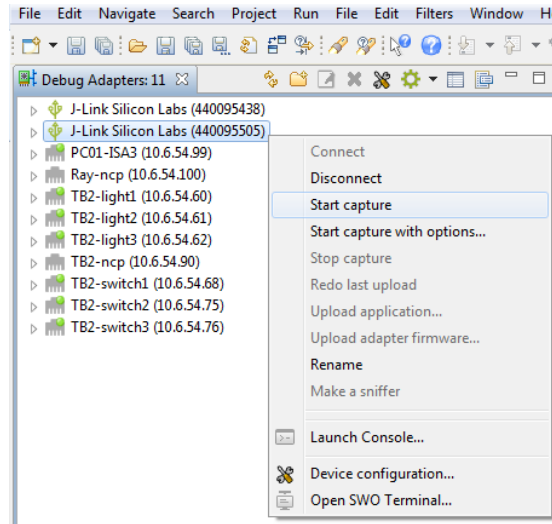
How to capture packet trace on demo boards - Hardware connection

- Capture packet trace on WSTK Kit
 - WSTK main board + Radio board, debug mode set to 'MCU'
 - USB/Ethernet cable
 - Running Network Analyzer on PC
 - Click "Start capture" on adapter



How to capture packet trace - Hardware connection

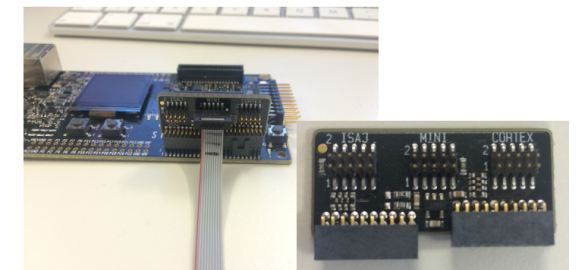
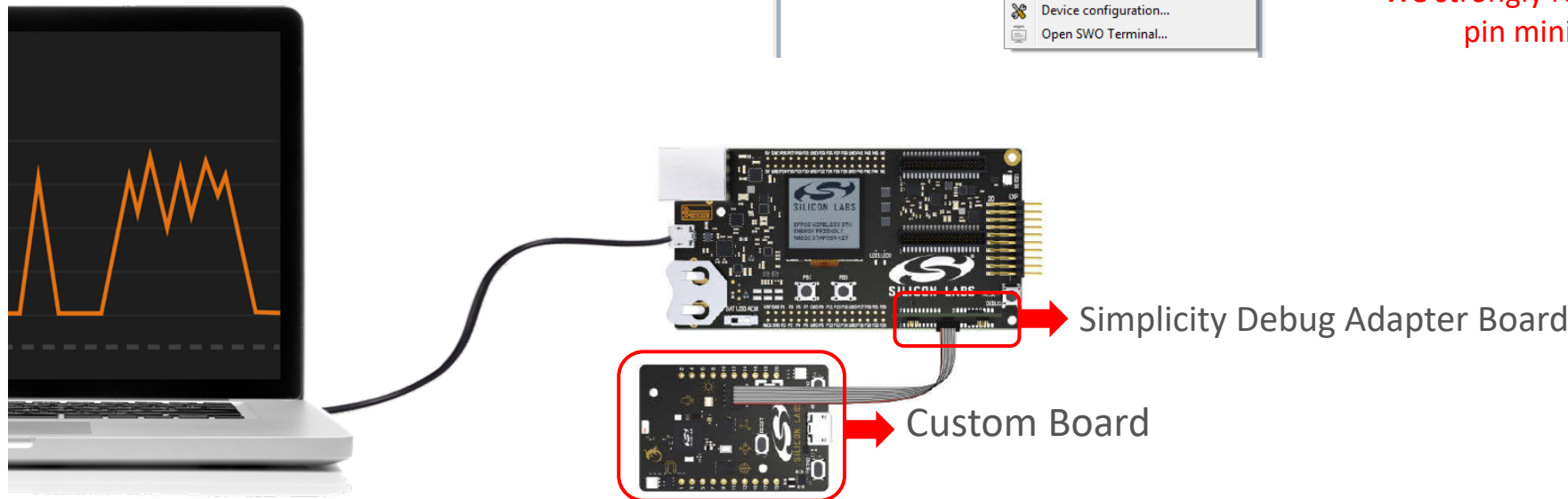
- Capture packet trace on Custom Board
 - WSTK main board, debug mode set to 'OUT'
 - Simplicity Debug Adapter Board
 - 10-Pin ribbon cable
 - USB/Ethernet cable
 - Running Network Analyzer on PC
 - Click "Start capture" on adapter



Pin #	Pin Name	Pin Function	EFR32 Functionality
1	VAEM	Target Advanced Energy Monitor Voltage Net	VDD
2	GND	Target Ground	VSS
3	RST	Target Reset (Active Low)	RESETn
4	VCOM_RX	Target Pass-through UART/Virtual COM Port Receive	US0_RX
5	VCOM_TX	Target Pass-through UART/Virtual COM Port Transmit	US0_TX
6	SWO	Target Serial Wire Output	SWO
7	SWDIO	Target Serial Wire Data Input/Output	SWDIO
8	SWCLK	Target Serial Wire Clock	SWCLK
9	PTI_FRAME	Target Packet Trace Interface Frame Signal	FRC_DFRAME
10	PTI_DATA	Target Packet Trace Interface Data Signal	FRC_DOUT

VAEM	1	2	GND
RST	3	4	VCOM_RX
VCOM_TX	5	6	SWO
SWDIO	7	8	SWCLK
PTI_FRAME	9	10	PTI_DATA

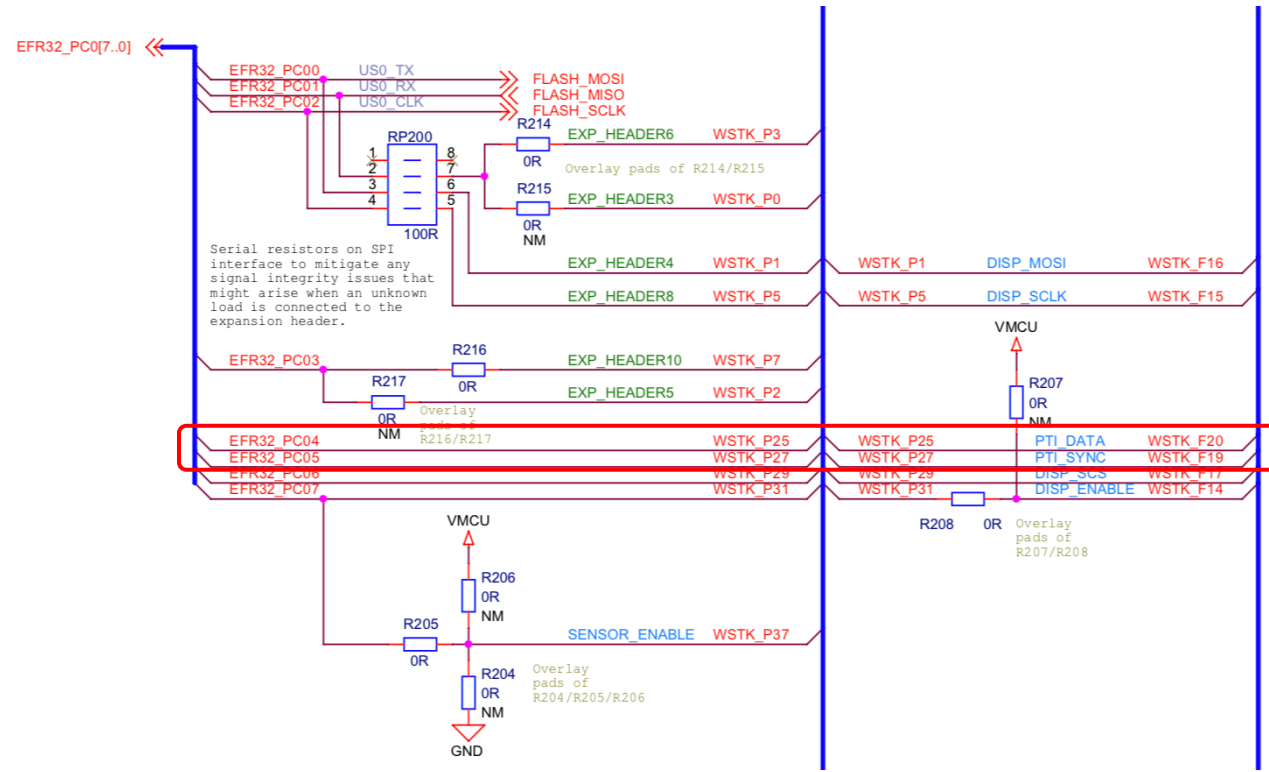
We strongly recommend that customers include 10-pin mini simplicity connector pin-out on development hardware



How to capture packet trace – Software configuration for Bluetooth

■ Bluetooth - Configure PTI in hal-config-app-common.h

```
#define HAL_PTII_ENABLE  
#define HAL_PTII_MODE  
#define HAL_PTII_BAUD_RATE  
(1)  
(HAL_PTII_MODE_UART)  
(1600000)
```



How to capture packet trace – Software configuration in App Builder

- App Builder Projects - Configure PTI in .hwconfig file
 - PTI_FRAME
 - PTI_DATA

The screenshot displays the App Builder software configuration interface for a project named 'brd4182a_efr32mg22c224f512im40.hwconf'. The main window is titled 'DefaultMode Peripherals' and is divided into several sections:

- Peripherals:** A grid of checkboxes for various hardware components. The 'PTI' checkbox is checked and highlighted with a tooltip that reads 'Packet Trace Interface'. Other checked components include CMU, DCDC, GPIO, PA, and WDOG.
- HAL:** A grid of checkboxes for hardware abstraction layer components. The 'LED' checkbox is checked.
- NCP:** A grid of checkboxes for Network Co-Processor components. 'SPI NCP' and 'UART NCP' are unchecked.
- Radio:** A grid of checkboxes for radio-related components. 'Antenna Diversity', 'Coexistence', 'EZRadioPro', and 'External FEM' are unchecked.
- Serial:** A grid of checkboxes for serial communication components. All are unchecked.

On the right side, there are three panels:

- Outline:** A tree view showing the project structure, including 'DefaultMode', 'Peripherals', and 'Port I/O'.
- Properties:** A panel titled 'Properties of PTI' showing a table of properties for the selected PTI component.
- Port I/O Mapping:** A panel showing 'No valid mapping selection'.

At the bottom, there is a 'Problems' and 'Console' panel, which is currently empty.

Property	Value
Owned by	
mode	Asynchronous (UART)
PTI baud rate	1600000 (0x186A00)
DFRAME pin	PC05
DOUT pin	PC04

How to capture packet trace – Software configuration, peripheral routing

- GPIO LOCATION
 - FRC_DFRAME
 - FRC_DOUT

Table 6.6. DBUS Routing Table

Peripheral.Resource	PORT			
	PA	PB	PC	PD
CMU.CLKIN0			Available	Available
CMU.CLKOUT0			Available	Available
CMU.CLKOUT1			Available	Available
CMU.CLKOUT2	Available	Available		
EUART0.CTS	Available	Available	Available	Available
EUART0.RTS	Available	Available	Available	Available
EUART0.RX	Available	Available	Available	Available
EUART0.TX	Available	Available	Available	Available
FRC.DCLK			Available	Available
FRC.DFRAME			Available	Available
FRC.DOUT			Available	Available

Network Analyzer Perspective

- Editor Panes
 - Adapters
 - Map
 - Transactions
 - Events
 - Event Details
 - Hex Dump
 - Filters
 - Tools

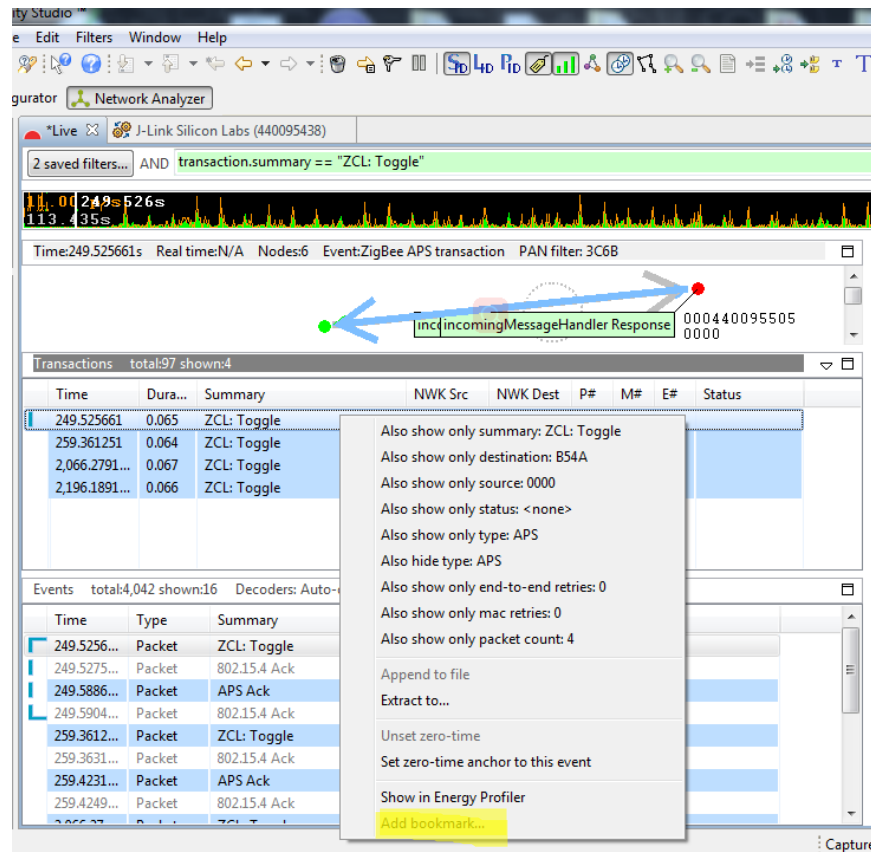
The screenshot displays the Network Analyzer interface with several panes highlighted by red boxes:


- Debug Adapters:** A tree view on the left showing the capture source: J-Link Silicon Labs (440095438) and its sub-devices like PC01-ISA3, Ray-ncp, and various TB2 devices.
- Transactions:** A table showing network transactions. The selected transaction at 94.689971s is a 'Device joined' event.
- Events:** A table showing event details for the selected transaction, including 'Match Description Request' and 'Route Record'.
- Event Detail:** A pane on the right showing the decoded data for the selected event, including NWK crypto, IEEE 802.15.4, ZigBee Network, and ZigBee Application Support.
- Hex Dump:** A pane on the right showing the raw hex data of the selected event, with ASCII characters visible on the right side.

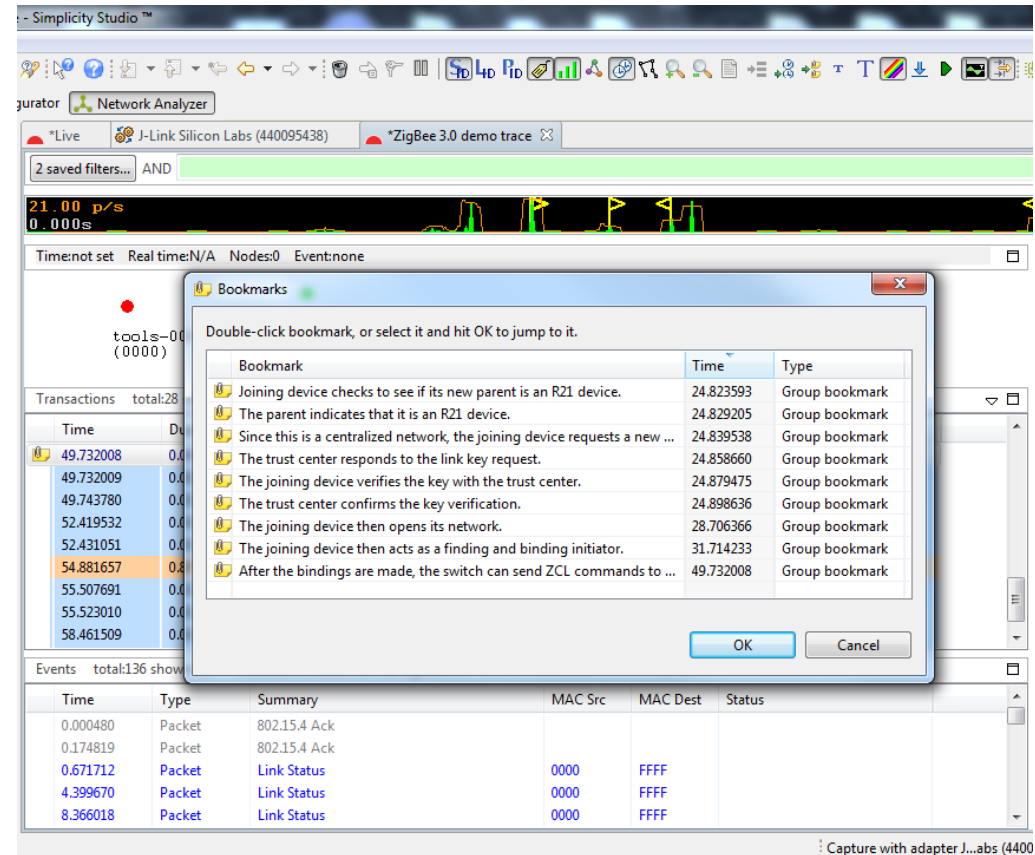
At the top, a toolbar contains various analysis tools like filters, zoom, and replay. A central map pane shows a network topology with nodes and connections.

Tools in Network Analyzer - Bookmark

- Add bookmark
 - Right click on the transaction or event
 - Choose “Add bookmark”



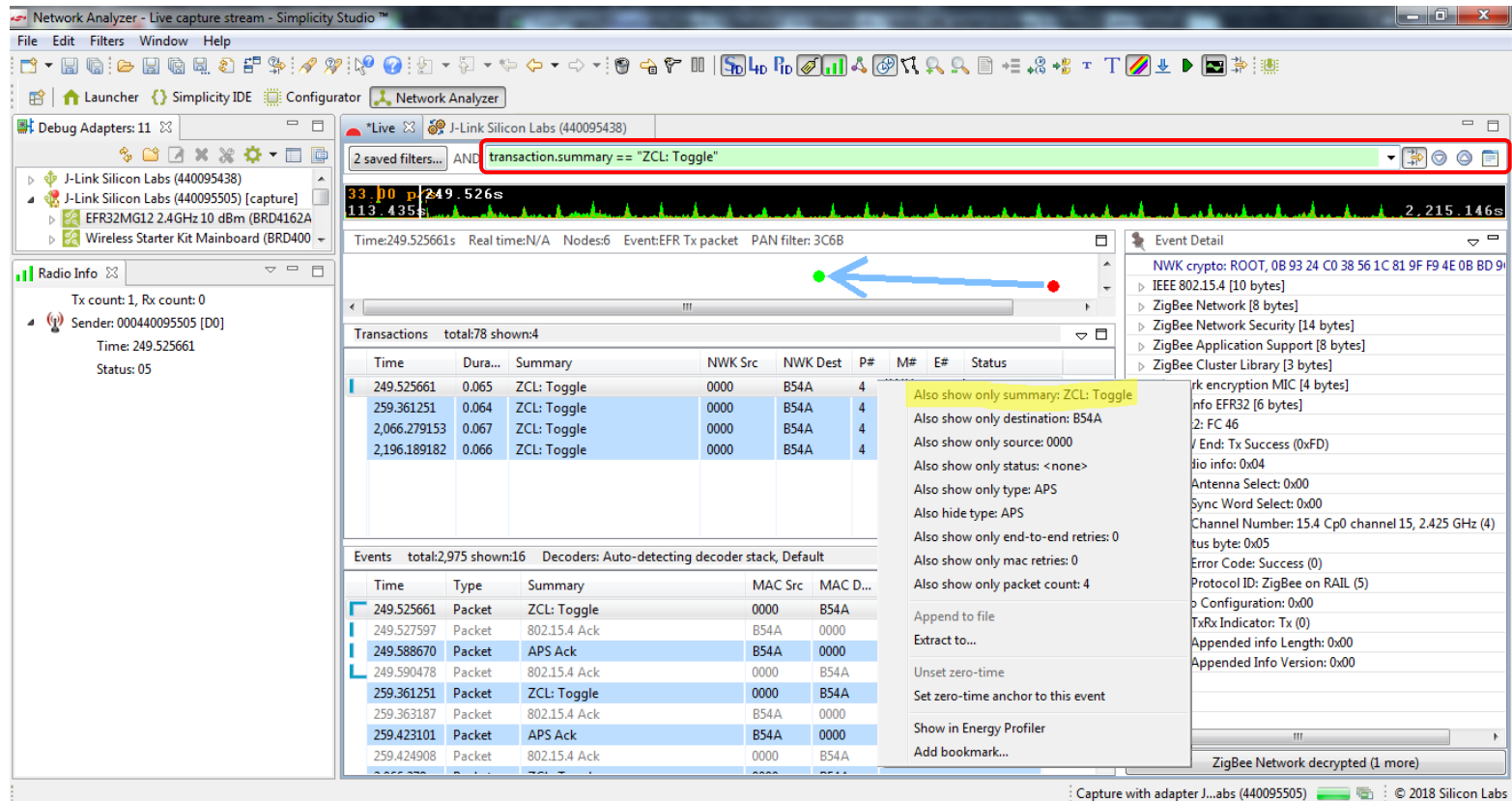
- Go to bookmark
 - Click  on toolbar



Tools in Network Analyzer - Filters

- Filters

- Right click on the transaction or event and choose "Also show only xxx"
- Edit filters with regular expression (&& or ||)



Tools in Network Analyzer - Event difference

- Simplicity Studio->Windows->Show View-> Event Difference

The screenshot displays the Simplicity Studio Network Analyzer interface. The 'Event Difference' window is highlighted with a red circle and shows a comparison of two events. The 'Transaction' window shows a list of transactions with columns for Time, Duration, Summary, NWK Src, NWK Dest, P#, M#, E#, and Status. The 'Event Detail' window shows the structure of a ZigBee APS transaction, including fields like NWK crypto, IEEE 802.15.4, PHY Header, Packet Length, Frame Control, Frame Type, Security Enabled, Frame Pending, Ack Required, Intra Pan, Frame Version, and Reserved. The 'Hex Dump' window shows the raw data of the transaction.

Field	2,763.746817	2,805.322130
originator	000440095505	000440095505
▶ fifteenFour	present	different
▶ zigbeeNetwork	present	different
▶ zigbeeSecurity	present	different
▶ zigbeeApplicationSupport	present	different
frameControl	40	40
frameType	0	0
deliveryModeV2	0	0
indirectAddressMode	0	0
securityEnabled	false	false
ackRequired	true	true
extHeaderPresent	false	false
destEndpoint	1	1
clusterIdV2	6	6
profileId	104	104
sourceEndpoint	1	1
apsCounter	6	7
▶ zclPayload	present	different
zclFrameControl	1	1
zclFrameType	1	1
manufSpecific	false	false
direction	0	0
disableDefResp	false	false

Time	Dur...	Summary	NWK Src	NWK Dest	P#	M#	E#	Statu
2,763.74...	0.066	ZCL: Toggle	0000	4459	4			
2,763.76...	0.003	Route Record	4459	0000	2			
2,763.76...	0.003	Route Record	4459	0000	2			
2,763.80...	0.013	ZCL: DefaultResponse	4459	0000	4			
2,780.73...	1.070	Many-to-One Route Discovery	0000	FFFC	7			
2,786.19...	29.9...	ZCL: global clustId 141 (0x&d), cmdId...	0F00	0100	30			Miss
2,801.85...	0.001	Data	0F00	00FF	1			
2,805.32...	0.066	ZCL: Toggle	0000	4459	4			
2,805.33...	0.003	Route Record	4459	0000	2			
2,805.33...	0.003	Route Record	4459	0000	2			
2,805.38...	0.011	ZCL: DefaultResponse	4459	0000	4			
2,817.15...	29.9...	ZCL: global clustId 141 (0x&d), cmdId...	0F00	0100	30			Miss

Time	Type	Summary	MAC S...	MAC ...	Status
2,805.3...	Packet	ZCL: Toggle	0000	4459	
2,805.3...	EZSP	sendUnicast Command	0004...		
2,805.3...	APITrace	Send unicast	0004...		
2,805.3...	EZSP	sendUnicast Response	0004...		

Tools in Network Analyzer - Radio Info

■ Simplicity Studio->Windows->Show View-> Radio Info

The screenshot displays the Network Analyzer interface in Simplicity Studio. The main window shows a signal capture with a time cursor at 15.809025s. The 'Radio Info' panel on the right is highlighted with a red circle, showing details for a BLE transaction. The 'Transactions' table below the signal capture lists various BLE packets, and the 'Events' table at the bottom shows the underlying protocol events.

Radio Info (Highlighted):

- Corrupt: field length overflow: 1 [at field: txPhys]
- BLE Data [2 bytes]
- BLE Control [9 bytes]
- Op Code: Length Request (0x14)
- Maximum Rx Octets: 0x00FB
- Maximum Rx Time: 0x4290
- Maximum Tx Octets: 0x00FB
- Maximum Tx Time: 0x4290
- Radio info EIR32 [11 bytes]
- Crc3: 47 C7 38
- HW End: Tx Success (0xFD)
- Sync Word: EA A3 D5 E8
- Radio info: 0x24
- Antenna Select: 0x00
- Sync Word Select: 0x00
- Channel Number: RF-channel 36, 2474 MHz
- Status byte: 0x03
- Error Code: Success (0)
- Protocol ID: BLE (3)
- Info Configuration: 0x20
- TxRx Indicator: Tx (0)
- Appended info Length: 0x04
- Appended info Version: 0x00

Transactions Table:

Time	Duration	Summary	NWK Src	NWK Dest	P#	M#	E#	Error Status	Warning Status
15.479321	0.001	BLE Adv - Scan Request/Response	54 80 88 E6 CD 9E	58 8E 81 A5 47 75 2					
15.806672	0.001	BLE LL Control - Feature Exchange Procedure	58 8E 81 70 27 1A	58 8E 81 A5 47 75 1				Missing packets	
15.807277	0.001	BLE ATT: MTU Request	58 8E 81 70 27 1A	58 8E 81 A5 47 75 1				Missing packets	
18.106797	0.052	BLE ATT - Read By Group Type Request/Response	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					
18.206802	0.052	BLE ATT - Read By Group Type Request/Response	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					
18.306809	0.052	BLE ATT - Read By Type Request/Response	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					
18.406813	0.052	BLE ATT - Read By Type Request/Error	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					
18.506819	0.052	BLE ATT - Read By Type Request/Response	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					
18.606824	0.052	BLE ATT - Read By Type Request/Error	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					
18.706829	0.052	BLE ATT - Read By Type Request/Response	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					
18.806835	0.052	BLE ATT - Read By Type Request/Error	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					
18.906841	0.052	BLE ATT - Read By Type Request/Response	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					
19.006846	0.052	BLE ATT - Read By Type Request/Error	58 8E 81 70 27 1A	58 8E 81 A5 47 75 2					

Events Table:

Time	Type	Summary	MAC Src	MAC Dest	Event error status	Event warning status
15.807277	Packet	BLE ATT: MTU Request	58 8E 81 70 27...	58 8E 81 A5 4...		
15.807761	Packet	BLE LL Control: Slave Feature Request	58 8E 81 A5 4...	58 8E 81 70 27...	Packet Out of Sync...	
15.807849	Packet	BLE LL Control: Feature Response	58 8E 81 70 27...	58 8E 81 A5 4...	Packet Out of Sync...	
15.808350	Packet	BLE ATT: MTU Request	58 8E 81 A5 4...	58 8E 81 70 27...	Packet Out of Sync...	
15.808452	Packet	BLE ATT: MTU Response	58 8E 81 70 27...	58 8E 81 A5 4...	Packet Out of Sync...	
15.808937	Packet	BLE LL Control: Feature Response	58 8E 81 A5 4...	58 8E 81 70 27...	Packet Out of Sync...	
15.809025	Packet	BLE LL Control: Length Request	58 8E 81 70 27...	58 8E 81 A5 4...	field length overflo...	
15.809525	Packet	BLE ATT: MTU Response	58 8E 81 A5 4...	58 8E 81 70 27...	Packet Out of Sync...	
15.810112	Packet	BLE LL Control: Length Request	58 8E 81 A5 4...	58 8E 81 70 27...	field length overflo...	
15.856675	Packet	BLE LL Control: Length Response	58 8E 81 70 27...	58 8E 81 A5 4...	field length overflo...	
15.857763	Packet	BLE LL Control: Length Response	58 8E 81 A5 4...	58 8E 81 70 27...	field length overflo...	
15.906677	Packet	BLE LL - Empty PDU	58 8E 81 70 27...	58 8E 81 A5 4...		
15.907694	Packet	BLE LL - Empty PDU	58 8E 81 A5 4...	58 8E 81 70 27...		
15.956680	Packet	BLE LL - Empty PDU	58 8E 81 70 27...	58 8E 81 A5 4...		

Tools in Network Analyzer - Network Key

- Corrupt: NWK decryption failed
 - Missing Network Key in packet trace

The screenshot displays a network analyzer interface with the following components:

- Filter:** 2 saved filters... AND
- Timeline:** 3.50740s to 0.000s, 388.858s. Time: 5.739840s, Real time: Jul 17, 10:27:59, Nodes: 6, Event: ZigBee unicast transaction.
- Transactions Table:**

Time	Durati...	Summary	NWK Src	NWK Dest	P#	M#	E#	Status
5.739840	0.002	Data	5325	0000	2			
5.742958	0.002	Data	5325	0000	2			
5.751840	0.002	Data	5325	0000	2			
5.754473	0.002	Data	5325	0000	2			
5.759440	0.002	Data	5325	0000	2			
7.343840	0.002	Data	5325	0000	2			
7.351262	0.002	Data	5325	0000	2			
- Events Table:**

Time	Type	Summary	MAC Src	MAC Dest	Status
5.739840	Packet	Data	5325	0000	NWK decryption failed
5.740000	Packet	802.15.4 Ack	0000	5325	
5.742958	Packet	Data	5325	0000	NWK decryption failed
5.744990	Packet	802.15.4 Ack	0000	5325	
5.751840	Packet	Data	5325	0000	NWK decryption failed
5.752000	Packet	802.15.4 Ack	0000	5325	
5.754473	Packet	Data	5325	0000	NWK decryption failed
5.756505	Packet	802.15.4 Ack	0000	5325	
5.759440	Packet	Data	5325	0000	NWK decryption failed
- Event Detail:**
 - Corrupt: NWK decryption failed
 - IEEE 802.15.4 [10 bytes]
 - PHY Header: 0x34
 - Packet Length: 52
 - Frame Control: 0x8861
 - Frame Type: Data (1)
 - Security Enabled: false
 - Frame Pending: false
 - Ack Required: true
 - Intra Pan: true
 - Frame Version: 2003 (0)
 - Reserved: 0x00
 - Destination Address Mode: Short (2)
 - Source Address Mode: Short (2)
- Hex Dump [59 bytes]:**

```
F8 34 61 88 83 A3 .4a...
47 00 00 25 53 08 G...%S.
02 00 00 25 53 1E ...%S.
FD 28 30 63 0E 00 .(0c...
2D E1 F4 FE FF 5E .....
CF D0 00 25 EB B5 ...%..
F6 81 8C 47 8E BC ...G..
A4 E9 A5 BC 03 64 .....d
39 FC 71 AE 43 C3 9.q.C.
F9 BE 09 05 48 ....H
```

Tools in Network Analyzer - Get Network Key

- Get Network Key
 - Print “keys print” CLI on console
 - Read it from packet trace

```
ep 2 [endpoint enabled, device enabled] nwk [0] profile [0x0104] devId [0x010D] ver [0x00]
  in (server) cluster: 0x0000 (Basic)
  in (server) cluster: 0x0003 (Identify)
  in (server) cluster: 0x0004 (Groups)
  in (server) cluster: 0x0005 (Scenes)
  in (server) cluster: 0x0006 (On/off)
  in (server) cluster: 0x0008 (Level Control)
  in (server) cluster: 0x0300 (Color Control)
  out(client) cluster: 0x1000 (ZLL Commissioning)
  in (server) cluster: 0x1000 (ZLL Commissioning)
ep 242 [endpoint enabled, device enabled] nwk [0] profile [0xA1E0] devId [0x0061] ver [0x00]
  out(client) cluster: 0x0021 (Green Power)
Nwk cnt: 1
nwk 0 [Primary (pro)]
  nodeType [0x02]
  securityProfile [0x05]
Z3LightSocZDOTesting>EMBER_SECURITY_LEVEL: 05
NWK Key out FC: 00015B02
NWK Key seq num: 0x00
NWK Key: 0B 93 24 C0 38 56 1C 81 9F F9 4E 0B BD 9C 8A F5
Link Key out FC: 00004002
TC Link Key
- (>)000B57FFFE648DD3 00025005 L y 7A 0B AA D5 29 FF 57 5A 06 27 80 B9 78 0F C6 A3
Link Key Table
0/0 entries used.
Z3LightSocZDOTesting>
```

keys print

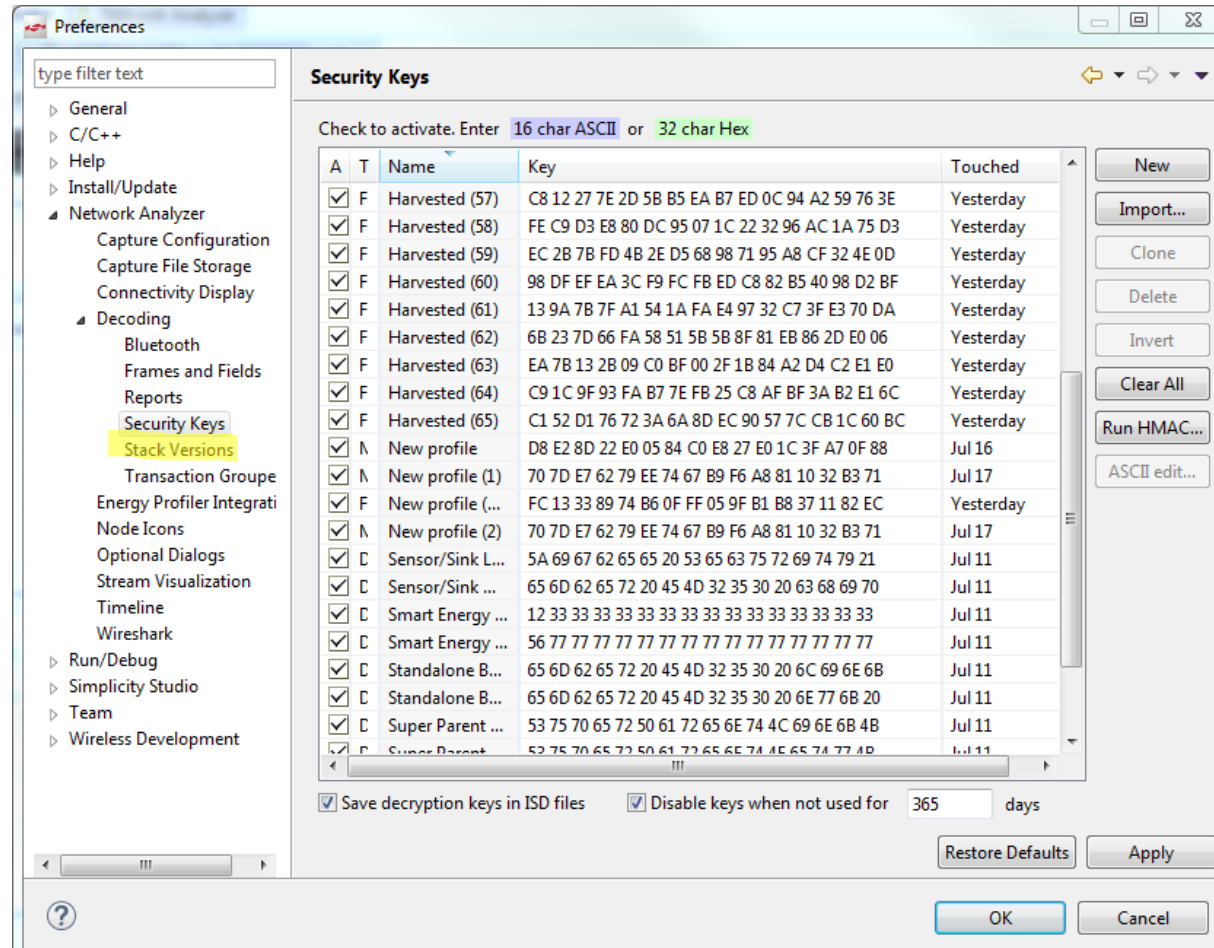
Event Detail

NWK crypto: ROOT, 0B 93 24 C0 38 56 1C 81 9F F9 4E 0B BD 9C 8A F5

- ▶ IEEE 802.15.4 [10 bytes]
- ▶ ZigBee Network [8 bytes]
- ▶ ZigBee Network Security [14 bytes]
- ▶ ZigBee Application Support [8 bytes]
- ▶ ZigBee Device Profile V2 [3 bytes]
- ▶ Network encryption MIC [4 bytes]
- ▶ Radio Info EFR32 [6 bytes]

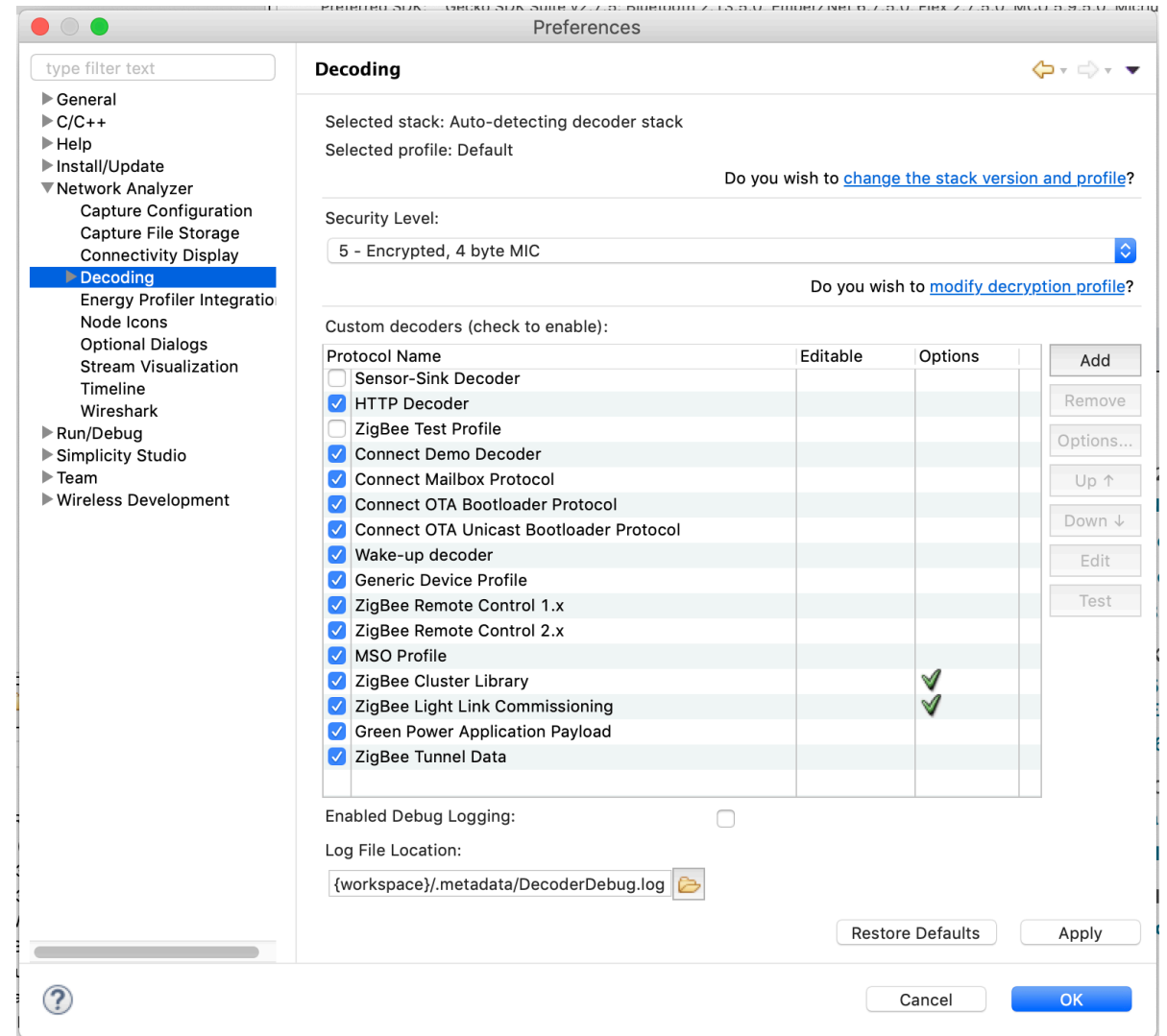
Tools in Network Analyzer - Import Network Key

- Simplicity Studio->Windows->Preferences->Network Analyzer->Decoding->Security keys



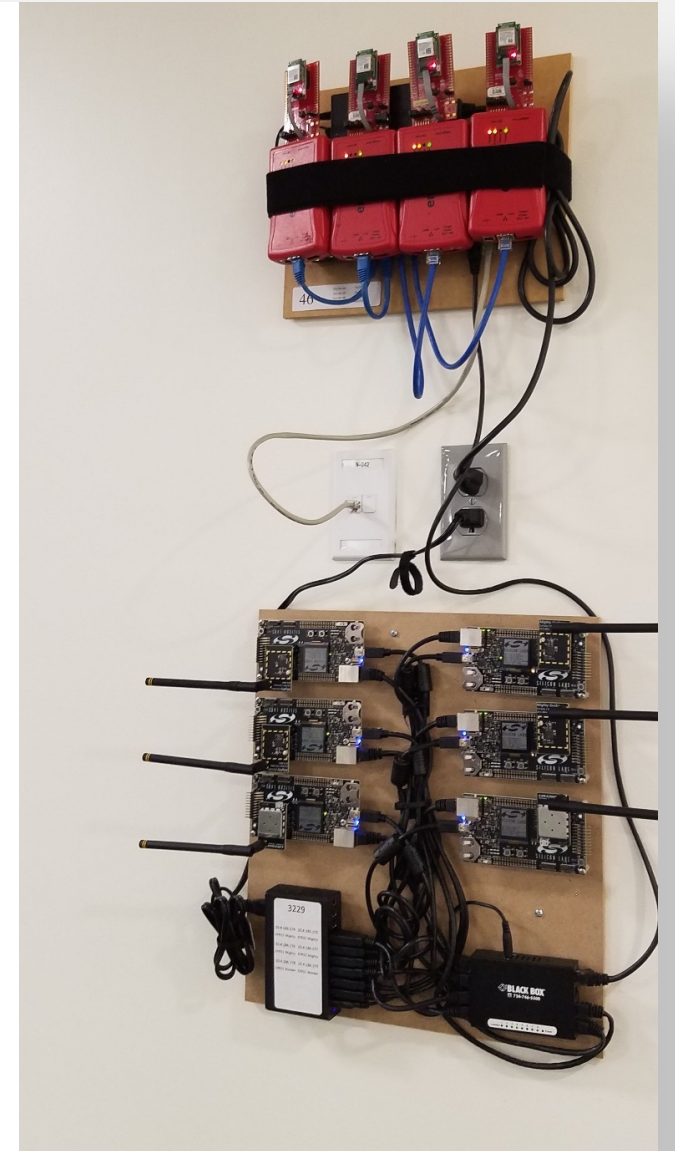
Protocol Decoding

- Usually auto detected but can be manually configured
- Possible to implement your own decoders for proprietary protocols

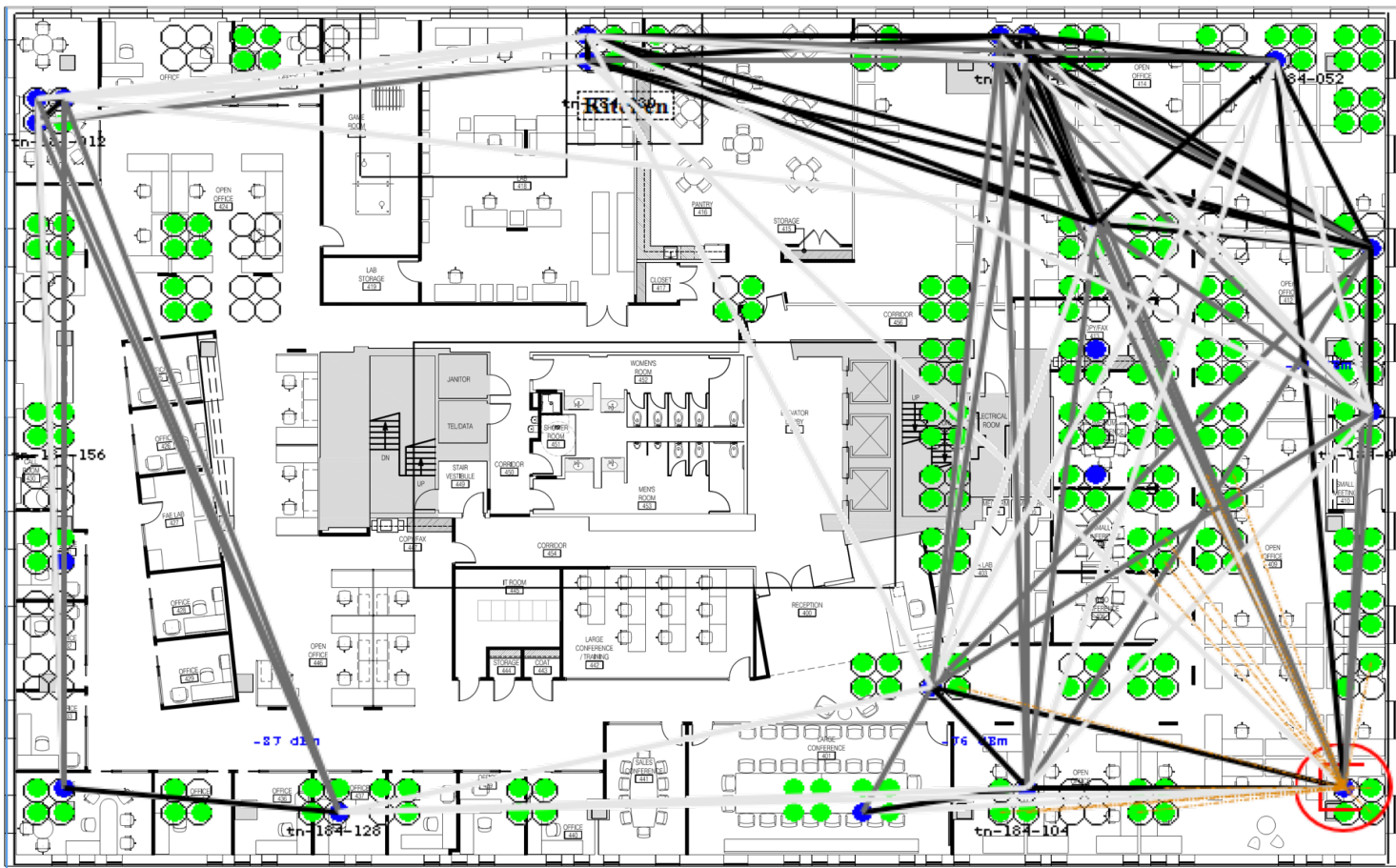


Silicon Labs Test Network

- 500+ node test network for QA and performance testing
- Ability to configure various network topologies
- Consists of device clusters spaced over entire office
- Controlled over Ethernet backchannel to allow
- Learn more at www.silabs.com/mesh-peformance or check out the following application notes:
 - AN1138: Zigbee Mesh Network Performance
 - AN1141: Thread Mesh Network Performance
 - AN1142: Mesh Network Performance Comparison



Silicon Labs Test Network



Energy Profiler

- Key Features
 - Multi-node support allowing analysis of power consumption of entire network
 - Code correlation support for all monitored nodes
 - Integration with Network Analyzer
 - Complex searches are supported
 - Configurable capture triggers
 - Color coding of code sections to highlight relevant areas on graphs

Energy Profiler – Single Node



Energy Profiler – Multi Node

The screenshot displays the Energy Profiler Multi-Node interface. At the top, there are controls for 'Single-Node' and 'Multi-Node' modes, along with a 'Scope View' button. The main area shows two current traces for different nodes, each with a corresponding RX/TX event timeline. The bottom panel shows a table of function contributions to the energy profile.

Function	Energy	Contribution (%)
RTCCSYNC_PostWakeUp	7.52 μ Wh	7.926%
0x0E000000-0x0E000FFF	3.67 μ Wh	3.866%
BUS_RegBitRead	2.82 μ Wh	2.974%
RTCCSYNC_PreSleep	2.37 μ Wh	2.497%
SystemHFClockGet	1.35 μ Wh	1.423%
I2C_Transfer	1.22 μ Wh	1.28%

```
uint32_t tmp;
uint32_t pending;
I2C_Transfer_TypeDef *transfer;
I2C_TransferSeq_TypeDef *seq;

EFM_ASSERT(I2C_REF_VALID(i2c));

/* Support up to 2 I2C buses. */
if (i2c == I2C0) {
    transfer = i2cTransfer;
}
#if (I2C_COUNT > 1)
else if (i2c == I2C1) {
    transfer = i2cTransfer + 1;
}
#endif
#if (I2C_COUNT > 2)
else if (i2c == I2C2) {
    transfer = i2cTransfer + 2;
}
#endif
else {
    return i2cTransferUsageFault;
}

seq = transfer->seq;
for (; ) {
    pending = i2c->IF;

    /* If some sort of fault, abort tr
    if (pending & I2C_IF_ERRORS) {
        if (pending & I2C_IF_ARBLOST) {
            /* If an arbitration fault, in
            /* not responding as expected,
            /* supported by this software.
            transfer->result = i2cTransfer
        } else if (pending & I2C_IF_BUSE
        /* A bus error indicates a mis
        /* not occur in master mode co
        transfer->result = i2cTransfer
    }

    /* If an error occurs, it is diff
    /* an exact cause and how to res
    /* to determine how to handle a
    transfer->state = i2cStateDone;
    goto done;
}

->state) {
    *****
    rst start+address
    *****
```

Network Analyzer – Energy Traces

The screenshot displays a network analyzer interface with several key components:

- Top Panel:** Shows a time-domain energy trace with a green signal and a yellow envelope. The time range is from 61.048s to 67.656s. Below the trace, a timeline shows a sequence of events with a red arrow pointing to a specific event at 67.656205s.
- Event Detail Panel (Right):** Provides metadata for the selected event:
 - BLE Data [2 bytes]
 - Radio Info EFR32 [12 bytes]
 - Crc3: FC DC 7B
 - HW End: Rx Success (0xF9)
 - RSSI: -38 dBm (0xDA)
 - Sync Word: 50 65 73 18
 - Radio info: 0x0A
 - Antenna Select: 0x00
 - Sync Word Select: 0x00
 - Channel Number: RF channel 10, 2422
 - Status byte: 0x03
 - Error Code: Success (0)
 - Protocol ID: BLE (3)
 - Info Configuration: 0x68
 - TxRx Indicator: Rx (1)
 - Appended info Length: 0x05
 - Appended Info Version: 0x00
- Transactions Table (Middle):** Lists 109 transactions. The selected transaction at 67.700565s is:

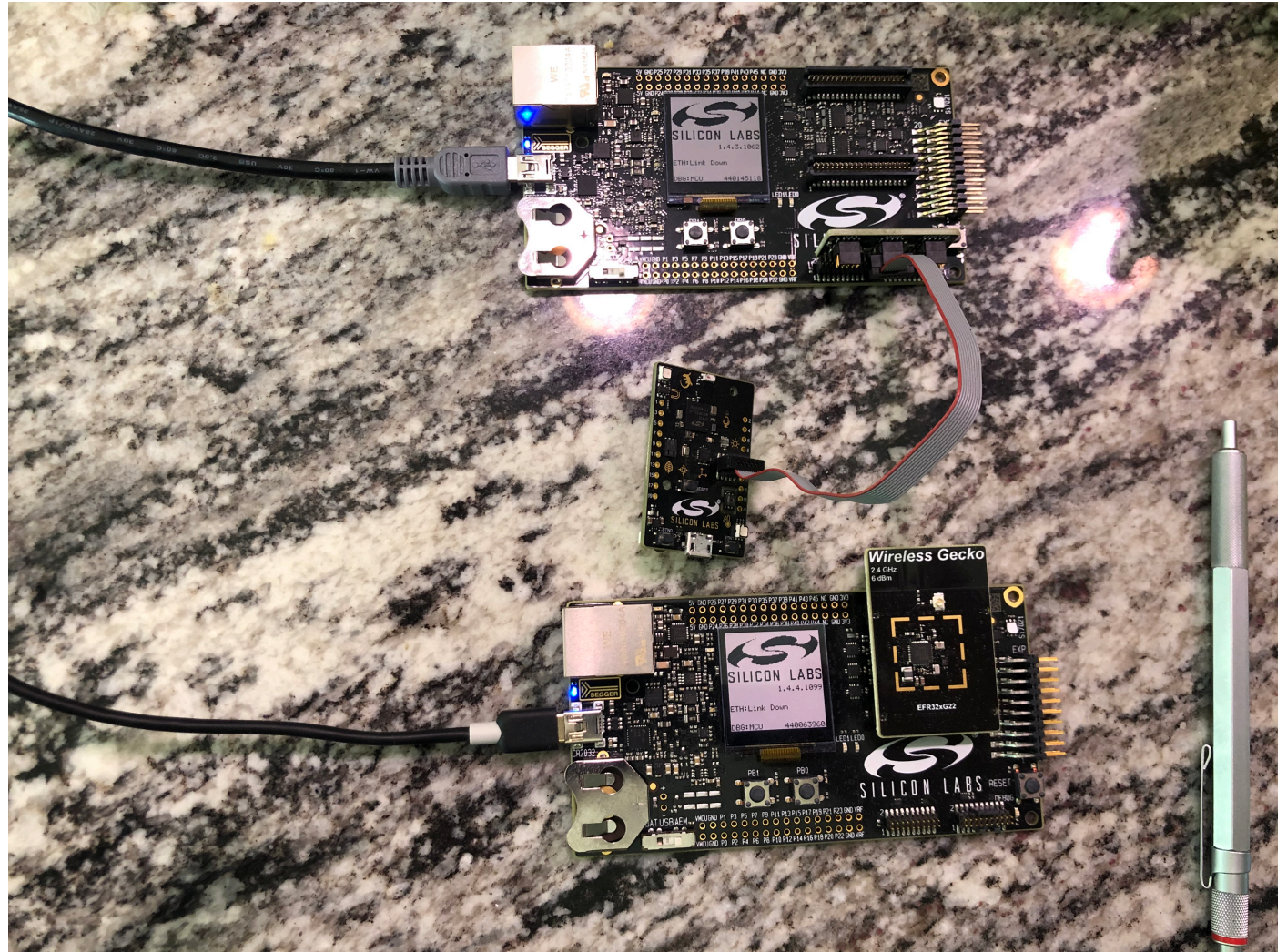
Time	Duration	Summary	NWK Src	NWK Dest	P#	M#	E#	Status
67.700565	0.001	BLE Adv - Scan Request/Response	7A EB C9 EF 9C 63	00 0B 57 18 19 40	2			
- Radio Info Panel (Left):** Shows statistics for the selected event:
 - Tx count: 0, Rx count: 1
 - Receiver: 000440062893 [9246]
 - Time: 67.656205
 - Raw RSSI: 218
 - Scaled RSSI: -38 dBm
 - Status: 03
- Events Table (Bottom):** Lists 4,190 events. The selected event at 67.656205s is:

Time	Type	Summary	MAC Src	MAC Dest	Status
67.656205	Packet	BLE LL - Empty PDU	48 4B 85 E2 59...	00 0B 57 18 18...	
- Hex Dump Panel (Bottom Right):** Shows the raw data for the selected event:


```
F8 0D 00 FC DC 7B ... {
F9 DA 18 73 65 50 ... seP
0A 03 68 ... h
```

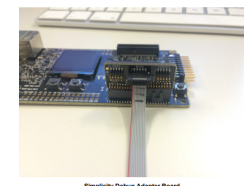
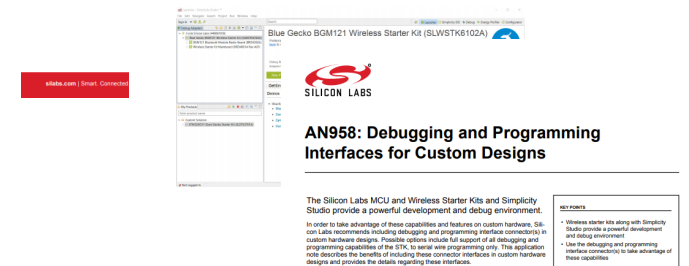
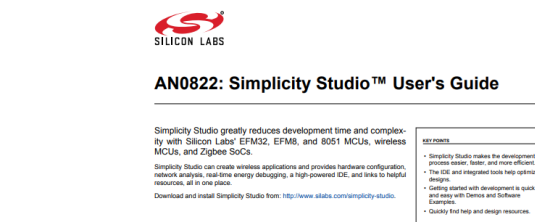
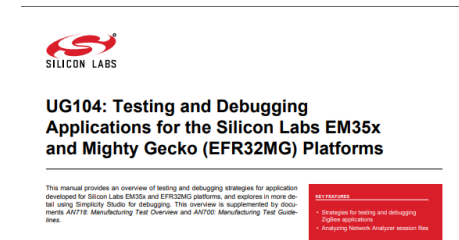

Demo – Bluetooth advertising and connections, Zigbee 3.0

- WSTK with BG22 radio card in NCP mode
 - BGTool used to graphically scan, connect, read attributes, disconnect
- WSTK with BG22 Thunderboard advertising multiple advertising sets
 - One iBeacon
 - One connectable advertisement
 - Simple GATT



Additional documentation

- Main documentation link – docs.silabs.com
- Application Notes
 - [AN0822 - Simplicity Studio User Guide.pdf](#)
 - [AN958 - Debugging and Programming Interfaces for Custom Designs](#)
 - [UG343 - Multi Node Energy Profiler](#)
 - [UG104 - Testing and Debugging Applications for the Mighty Gecko](#)
- KBAs
 - [Can I examine captured packet/event data outside of Network Analyzer?](#)
 - [How to open large *.isd\(packet trace\) file with Network Analyzer?](#)



BG22 Virtual Workshop



Learn how to develop and deploy more powerful, efficient, and secure IoT products with your own BG22 Thunderboard – free for all registrants!

North America: May 19th–21st, May 12th-14th, 2020

10:00AM –11:30 AM CST

(Other sessions available for Asia Pacific and Europe)

We have added new workshops in AMER for May 26-28, June 2-4, June 9-11, June 23-25 and June 30-July 2. We'll soon be adding new dates for APAC and EMEA.

Register today! <https://www.silabs.com/about-us/events/virtual-bluetooth-workshop>

Thank You | Questions and Answers

Webinar will be available soon at:

<https://www.silabs.com/about-us/events/tech-talks>

Previous webinars on CHIP, Bluetooth and Security are already posted