Bluetooth:
Technology and Applications

Yang Bo,
CTTL-SYS, CAICT
2017.10.31

Course Objectives

Upon completion of this course, you will be able to

- Know what the Bluetooth technology is and its evolution
- Know some technology basics about Bluetooth
- Know the application scenarios of the Bluetooth
- Know the basic regulations in the test of the Bluetooth products

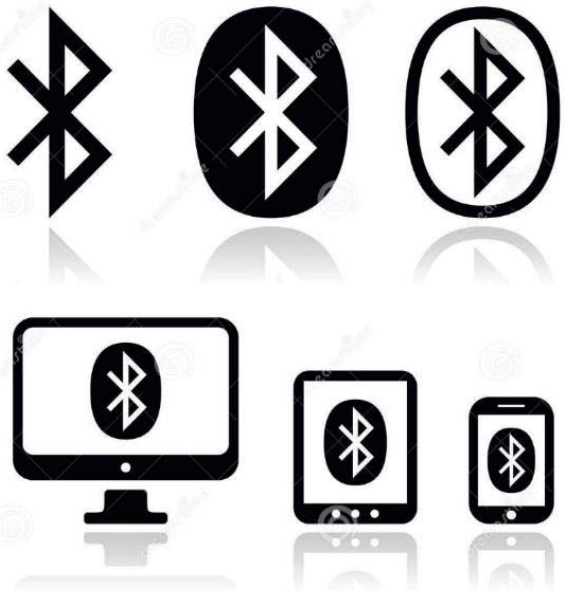
Main Contents

1. Bluetooth : What/When/Where
2. Technology basics of Bluetooth
3. Applications and Innovations
4. Test and Authentication

Bluetooth: What / Where

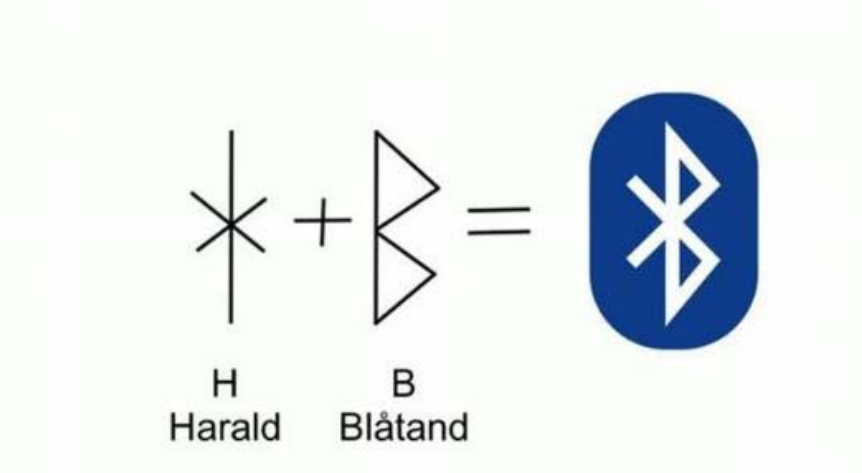
- Bluetooth
  - One of the most popular short-range wireless communication standard
  - Known as IEEE 802.15.1, now maintained by SIG (Special Interest Group)

- Bluetooth is everywhere
  - How many Bluetooth devices are there in the room?
  - Cellphones, wireless mouse/keyboard, smart watch/bracelet, earphone, ibeacon, …



Bluetooth: The Name

- The name: Bluetooth
  - Harald Gormsson (935-985/6)
  - Aka. Harald Blåtand (Harald Bluetooth)
  - Likes to eat blueberries
  - King of Denmark and Norway



  - Unites the Norway, Sweden and Denmark
  - Eloquent, good at communication

Bluetooth: Born

- Invention
  - 1994
  - Erission
  - a wireless alternative to RS-232 cable
- Development
  - 1997-1998
  - Erission, Nokia, Toshiba, IBM, Intel
  - Ver 0.7, 0.8 proposed
- Publish
  - 1999
  - SIG (Special Interest Group) is founded
  - Microsoft, Motorola, Samsung, Lucent with SIG
  - Bluetooth 1.0 published

Bluetooth: The chronicle

Bluetooth 1.0

1998.10 – 2003. 11
"Base Rate"
- 1Mbps data rate
- V1.0 - Draft
- V1.0A - published on 1999.7
- V1.0B Enhanced the Interoperability
- V1.1 - IEEE 802.15.1
- V1.2 Enhanced the compatibility

Bluetooth 2.0 + EDR

2004. 11 – 2007. 7
"Enhanced Data Rate"
- Higher ordered modulation for data payload
- 2Mbps or 3Mbps physical data rate

- V2.0
- V2.1

Bluetooth 3.0 + HS

2009. 4
"HS Mode"
- AMP Alternative MAC/PHY
- Implement high data rate by using 802.11 protocols.
- Facing the Challenge from Wi-Fi

- V3.0

Bluetooth 4.0

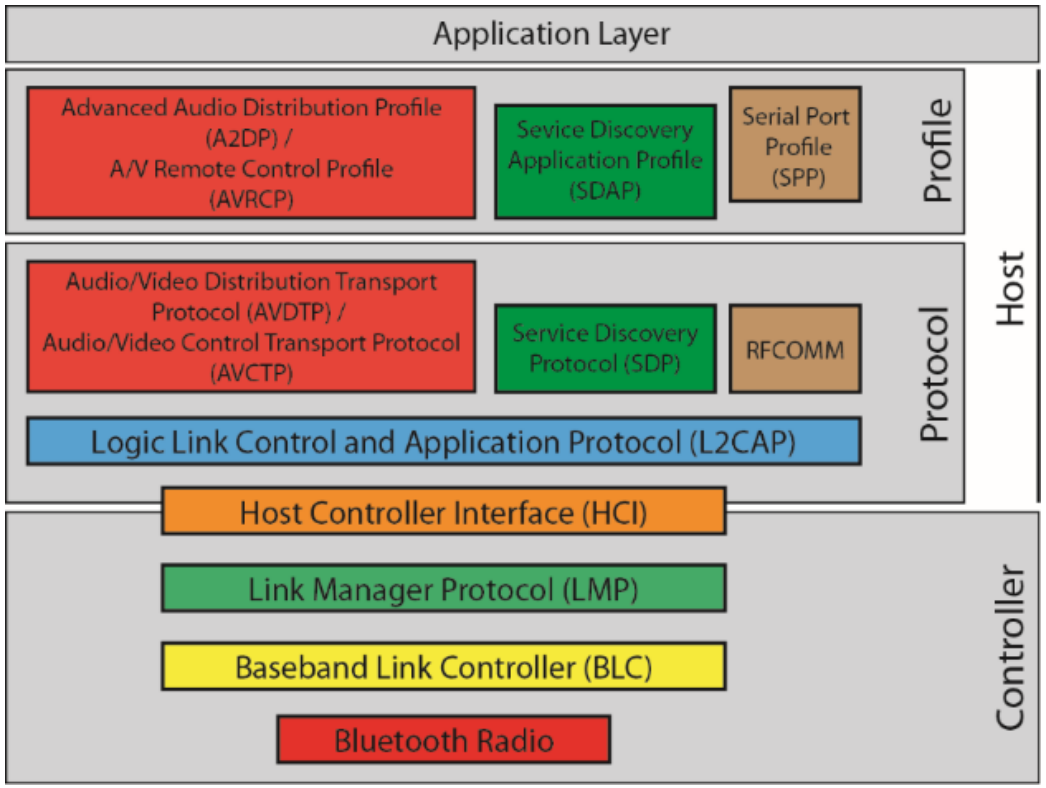
2010. 6 – 2014. 12
"Low Energy"
- Facing the IoT application
- Changed the protocol greatly, almost a new technology

- V4.0
- V4.1
- V4.2

Bluetooth: Protocol Stack

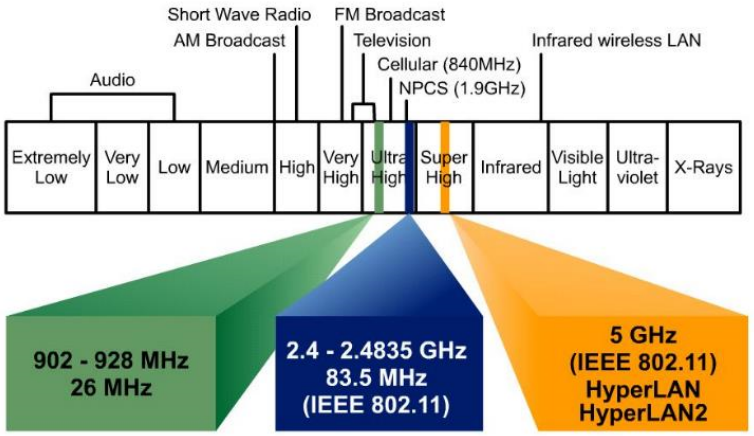
- Overview
  - Bluetooth protocol stack
    - Radio
    - Baseband
    - LMP
    - (HCI)
    - L2CAP
    - SDP

    - Optional Protocols and profiles supporting the application



Bluetooth: Radio Band

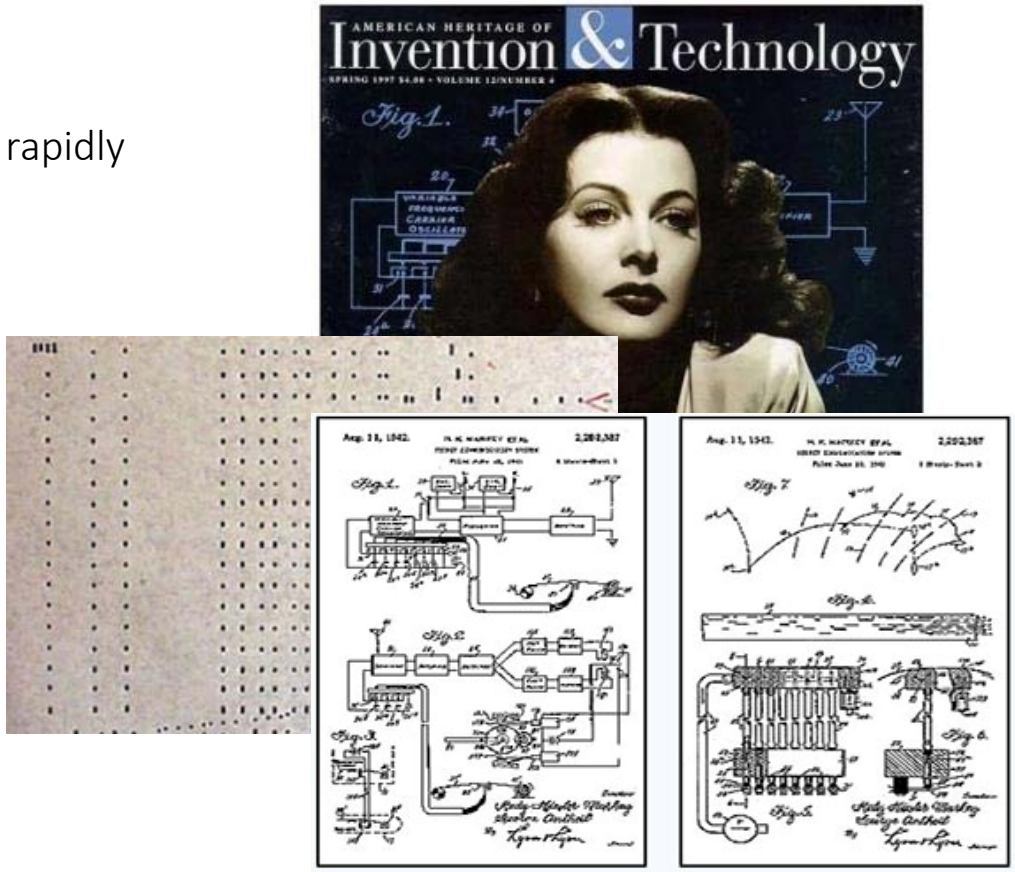
- Radio Band
  - Industrial, Science and Medical Radio Band
    Aka. ISM Band 2.45G
  - 2400MHz – 2483.5MHz
  - Worldwide
  - License Free
  - Power Constrained



  - Free to USE
  - Coexistence: WLAN(802.11), Zigbee(802.15.4), …
  - Frequency hopping

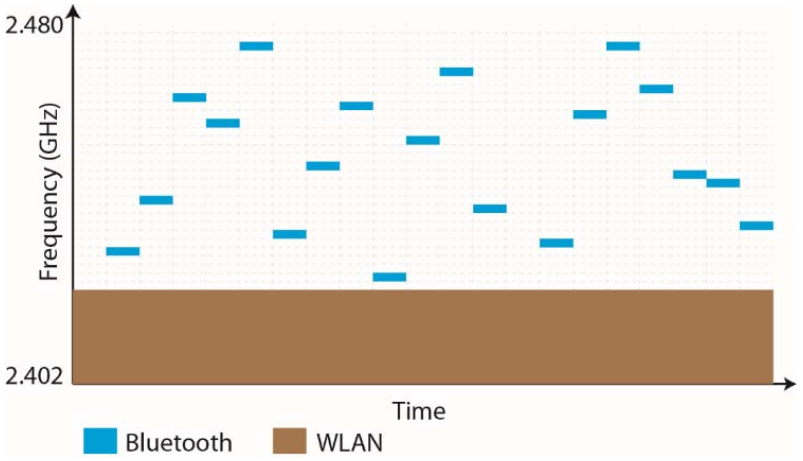
Bluetooth: FH technology

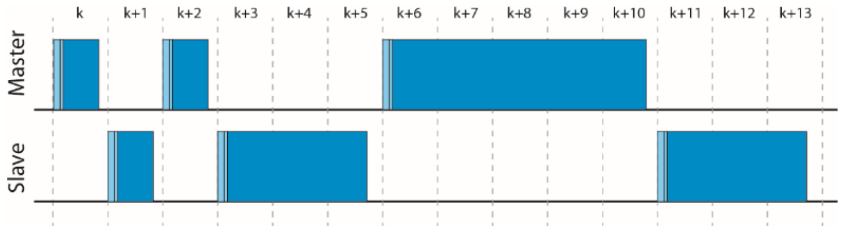
- Frequency Hopping
  - A technology that spreads its signal over rapidly changing carrier frequencies
  - Hedy Lamarr (1914 – 2000)
    Movie Star and Inventor
  - Made an auto piano wit her husband
  - Received a patent in 1942 on Frequency Hopping
  - “Secret Communication System”
    Patent No. 2,292,387
  - The patent expired in 1959
    but no one used FH until 1962



Bluetooth: FH and Time Slot

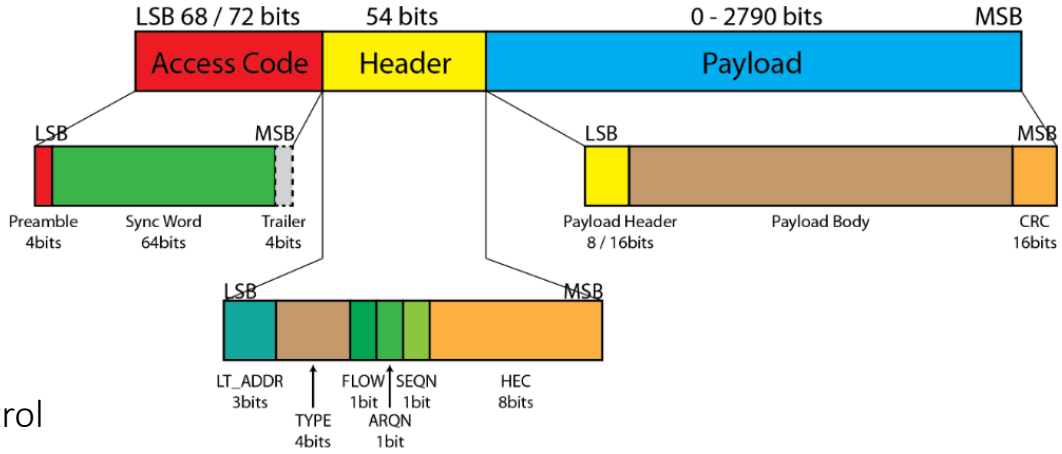
- Frequency Hopping and Time slots
  - Fast. 1600 times / sec = 625us / slot
  - FH and AFH (Adaptive Frequency Hopping)
  - “Frequency Selection Kernel” Complicated algorithm, sometimes treated as a Black Box
  - FH sequence based on the “Bluetooth CLK” and “Bluetooth Address” of the Master device
  - Single-slot Packet and multi-slot packets

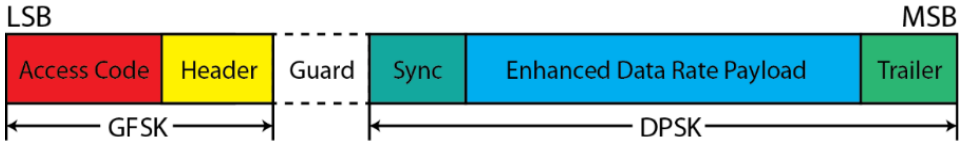




Bluetooth: Packets

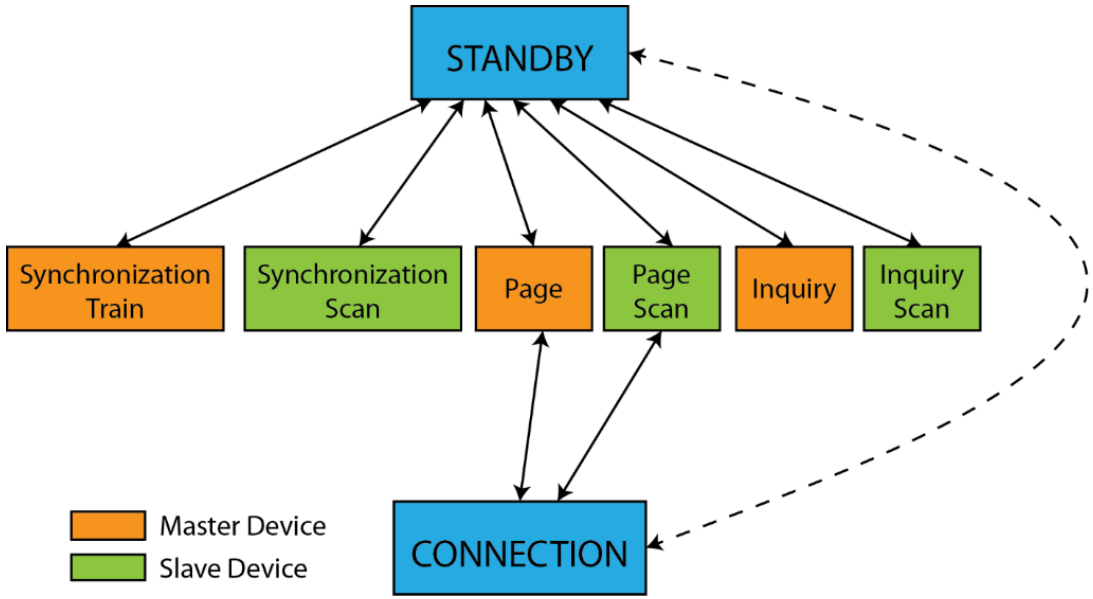
- Bluetooth Packets
  - Packets
    - Types
      - ID / FHS / DATA / Control
    - BR Packet
      - Access Code
        - Sync / Address
      - Header
        - Packet Type / Flow control
      - Payload
        - Data
    - EDR Packet
      - Guard
      - Sync
      - EDR Payload





Bluetooth: Connection

- Bluetooth Connection
  - Inquiry
  - Inquiry Scan
  - Page
  - Page Scan
  - Synchronization Train
  - Synchronization Response
  - Connection

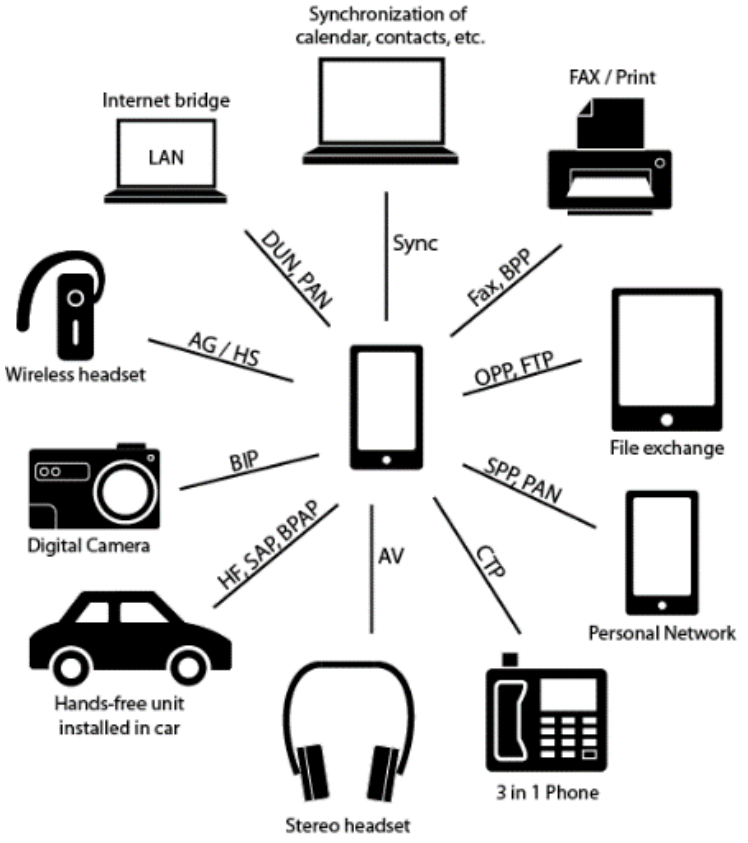


Bluetooth: Logical transmission

- Bluetooth Data Packet Types / Logical Data Links
  - Error vs Delay
    - Which one is more concerned when we transmit data / signal?
    - CS vs PS
    - TCP vs UDP
  - SCO / eSCO
    - (Extended) Synchronous Connection-Oriented
  - ACL
    - (Asynchronous Connection-Oriented Logical

Bluetooth: Profiles

- Profiles
  - Regulations on application layer
  - “Optional”
  - CTP (Cordless Telephony Profile)
  - BPP (Basic Printing Profile)
  - SPP (Serial Port Profile)
  - FTP (File Transfer Profile)
  - PAN (Personal Area Network)
  - SAP (SIM Access Profile)
  - AV (Audio Video)
  - HS (Handset Profile)
  - …



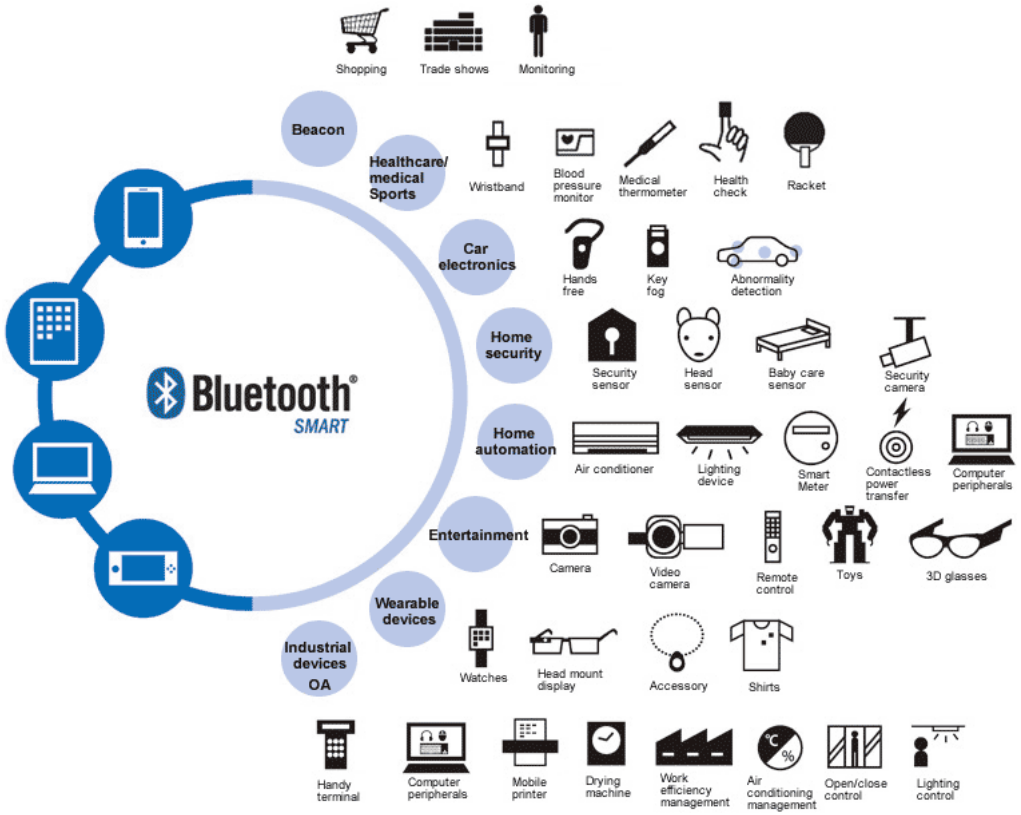
Bluetooth: Summary

- Classic Bluetooth Summary
  - Replacing the cable
    - Emphasis speed and reliability
    - Transmission based on connected link

- Advantages and disadvantages
  - Speed – relatively high, especially with EDR
    - Suitable for applications which require high data rate and stability.
    - Music / File / Voice
  - Power consumption – High
    - To perform high Duty-cycle transmission
    - To maintain the Link

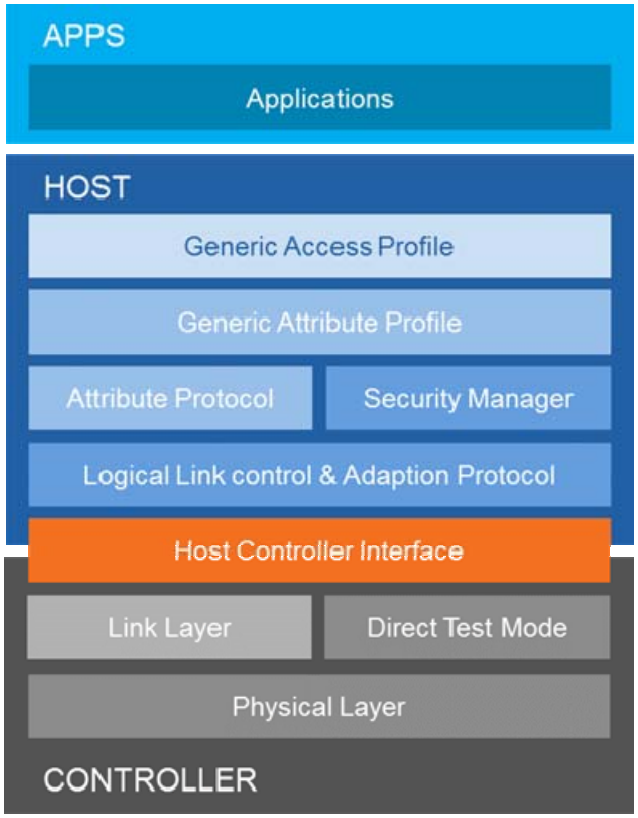
Bluetooth vs. BLE

- What does IoT need?
  - An example: A sport bracelet
    - Small data packet
    - Burst transmission
    - Power consumption sensitive
- Similarities
  - Frequency band
  - Modulation
- Difference - Simplification
  - Smaller duty cycle
  - Shorter connecting time
  - Simpler packets
  - Connectionless advertising



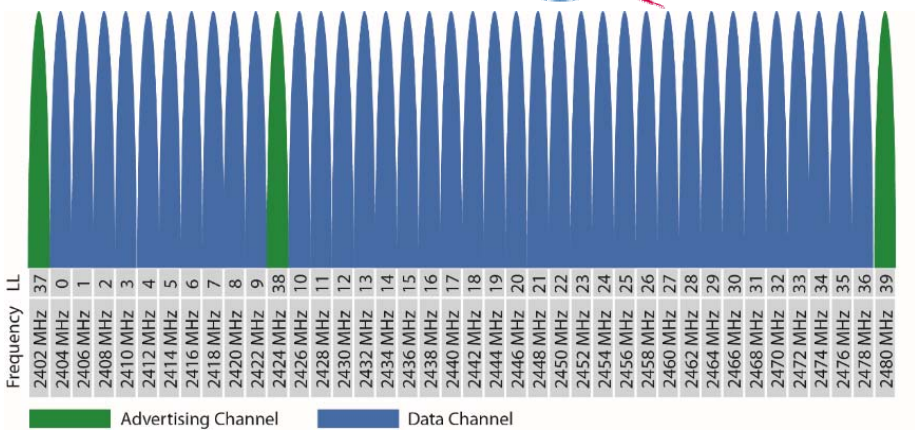
BLE Protocols

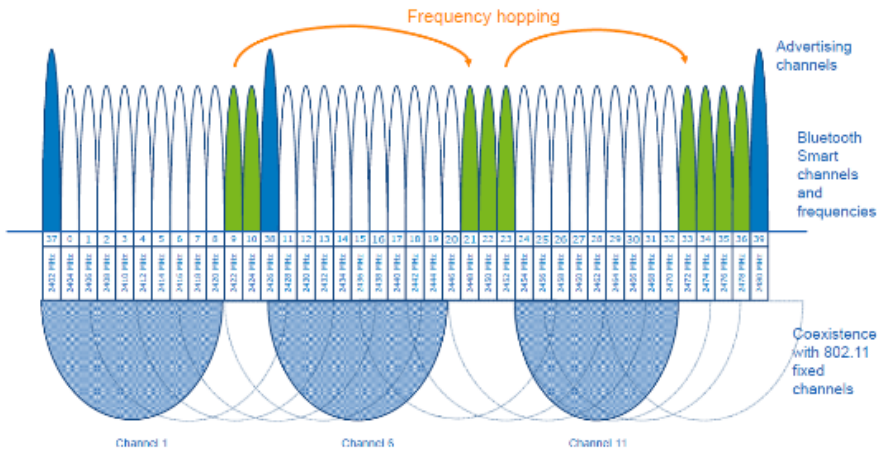
- BLE Basic Logic
  - Peripheral Device / Sensors have DATA
  - Central Device / Smartphones want to use DATA
  - Data / Readings peripheral - > central
  - Setting / Configurations central -> peripheral
- How to pass the data?
  - Advertising (Passive Scan) / Active Scan / Connection
- How to organize the data?
  - Profile / Service / Characteristic
  - Attribute / UUID



BLE – Band and Channels

- Frequency
  - Band division
    - 40 Band, 2MHz Each
    - 3 Advertising Channels and 37 Data channels
  - Frequency Hopping
    - Regular Hopping Sequence with given intervals
    - Adaptive – detect ‘used’ band to avoid interference



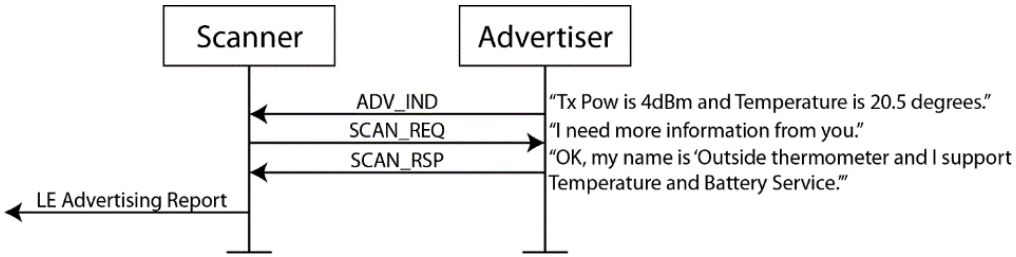


BLE – Advertising

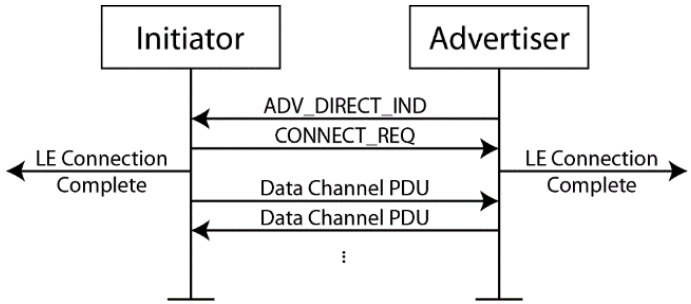
- Everything begins with advertising
  - Reporting the data / advertisement
  - Configurable channel / power / time interval
  - For broadcast or for connection
    - ADV_IND: Data and information “I can be connected, and can be scanned”
    - ADV_DIRECT_IND: Information “Only certain devices can connect to me.”
    - ADV_NON_IND: Data and information “I can be neither connected or response any scan”
    - ADV_SCAN_IND: Data and information “I will response some scan, but I can’t be connected”

BLE – Scan and connect

- Everything begins with advertising
  - Passive Scan
  - Active Scan
    - SCAN_REQ :
      “I want more information”
    - SCAN_RSP:
      “More information as you wish”

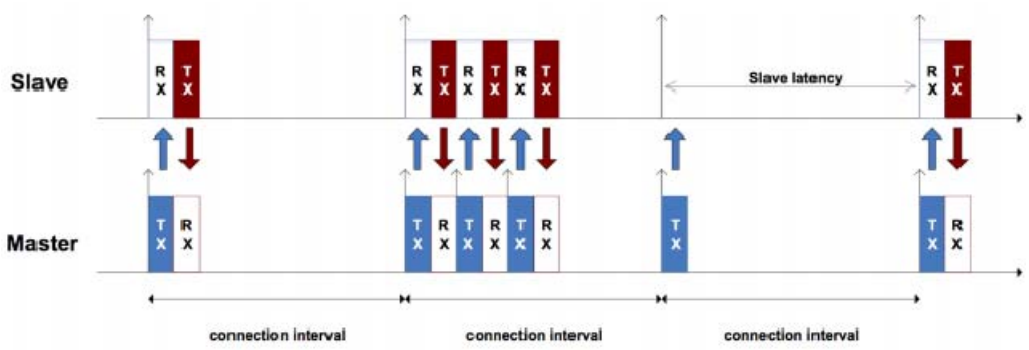


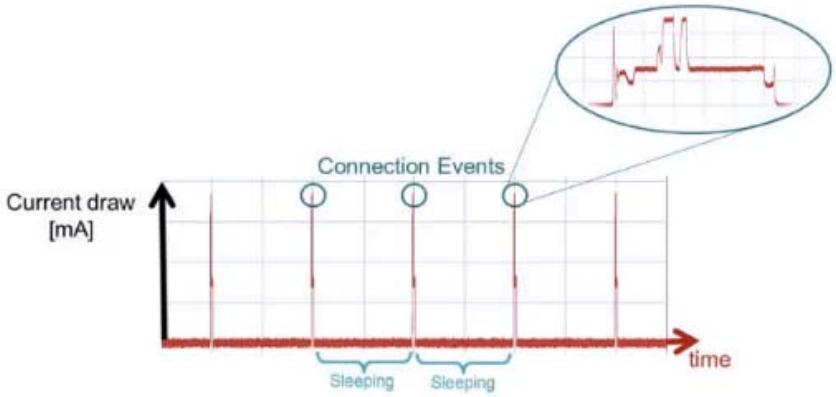
  - Connection
    - CONNECT_REQ: “OK, let’s connect”
      “Please follow these parameters: … … …”
    - NO RESPONSE NEEDED!
    - In a blink around 3ms



BLE - Connection

- BLE Connection
  - Transmit application data reliably and robustly
  - Connection Events / Connection Interval (7.5ms – 4s)
  - Slave Latency (0 – 499)
  - Connection supervision timeout (100ms – 32s)





BLE - Packets

- Packets
  - Preamble
  - Access Address
    - Fixed ‘8E89BED6’ for Advertising
  - PDU
    - Packet Data Unit
    - Follows regulations defined in GAP
    - AD structure: Length – type – data
  - CRC
    - Checks the integrity of the packet

Global Data Packet Format

Advertising Packet Format

Data Packet Format in Connection (unencrypted)

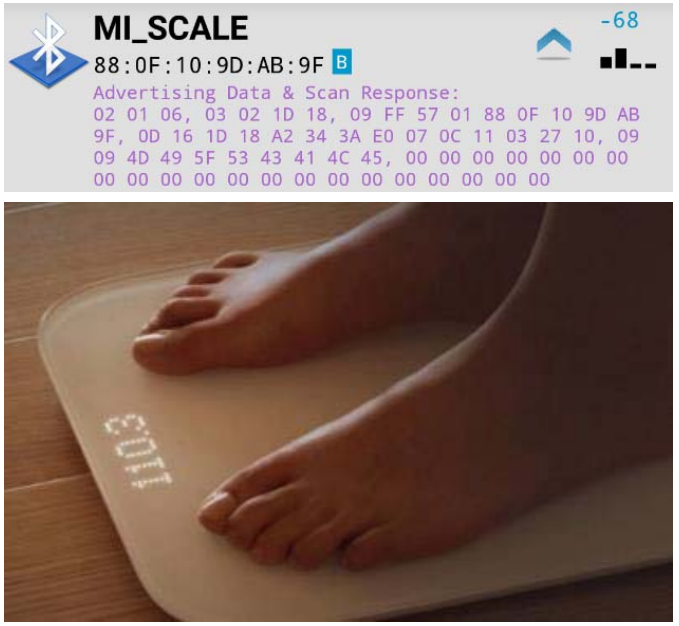
Data Packet Format in Connection (encrypted)

BLE Technologies

- An Example : Weight Scale
  - ‘Advertising Data Structure’
  - Length | Type | Data

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header				AdvA	AdvData	CRC	RSSI (dBm)	FCS
					Type	TxAdd	RxAdd	PDU-Length					
9	+1031101 =1031101	0x25	0x8E89BED6	ADV_IND	0	0	0	37	0x880F109DAB9F	02 01 06 03 02 1D 18 09 FF 57 01 88 0F 10 9D AB 9F 0D 16 1D 18 A2 34 3A E0 07 0C 11 03 27 10	0xC0391F	-54	OK

AD structure	Type	Content
02 01 06	01: FLAG	0x06: 00000110: Support only LE connection
03 02 1D 18	02: Service UID	0x181D: Weight Scale
09 FF 57 01 88 0F 10 9D AB 9F	FF: Vendor Spec.	0x0157: Huami co., Ltd. 880F109DAB9F: Device Address
0D 16 1D 18 A2 34 3A E0 07 0C 11 03 27 10	16: Service Data	0x181D: Weight Scale Service 0xA2: 10100010 SI units, Time stamp present, no user ID, no BMI 0x3A34: 14900 (x 0.005kg = 74.5kg) 0xE0070C11010203: 2016-12-17 03:39:16
09 09 4D 49 5F 53 43 41 4C 45	09: Local Name (short)	0x4D 49 5F 53 43 41 4C 45: ‘MI_SCALE’



BLE - Security

- BLE security
  - White List
    - Advertiser responds ONLY to devices with certain address
    - Valid address stored in a white list
  - Link Layer Privacy
    - Protect the address to prevent address faking
  - LE Encryption
    - AES-128 encryption
    - Protecting the content
  - (Higher level encryption)

BLE – Data exchange

- Key concepts in BLE
  - Profile
    - ‘An application’
    - Collection of services
  - Service
    - Collection of characteristics
    - Each has an unique ID (UUID)
  - Characteristic
    - A value with a known type and a known format
    - Also has an UUID
- Data exchange
  - Read / write the value of characteristics
  - May need authentication

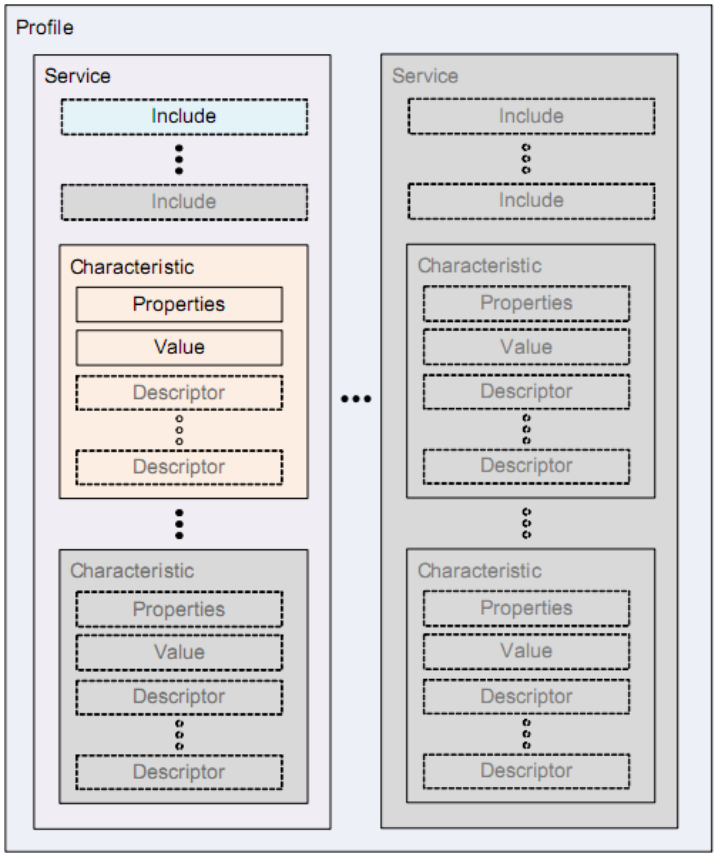


Figure 2.5: GATT Profile hierarchy

BLE Technologies

- An Example : a Heart Rate Monitor
  - Heart Rate Profile (HRP)
    - Device Information Service (0x180A)
      - … (9 Characteristics)
    - Heart Rate Service (0x180D)
      - Heart Rate Measurement (0x2A37)
      - Body Sensor Location (0x2A38)
      - Heart Rate Control Point (0x2A39)

Name: Heart Rate Measurement

Type:

Name: Heart Rate Control Point

Type:

Name: Body Sensor Location

Type:
org.bluetooth.characteristic.body_sensor_location Download / View

Assigned Number: 0x2A38

Value Fields

Names	Field Requirement	Format	Minimum Value	Maximum Value	Additional Information
Body Sensor Location	Mandatory	8bit	N/A	N/A	Enumerations

Key	Value
0	Other
1	Chest
2	Wrist
3	Finger
4	Hand
5	Ear Lobe
6	Foot
7 - 255	Reserved for future use

Review: Why Bluetooth?

- BLE vs similar technologies

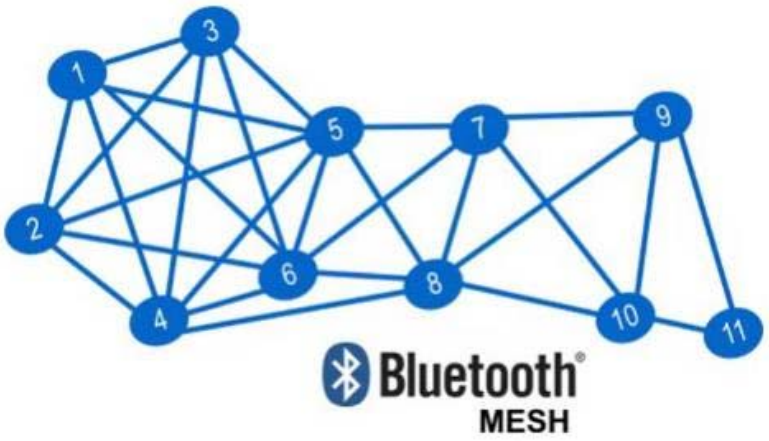
Variable	Wi-Fi	Z-Wave	Zigbee	Thread	BLE (V4.2)
Year first launched in market	1997	2003	2003	2015	2015
PHY/MAC Standard	IEEE 802.11.1	ITU-T G.9959	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.1
Frequency Band	2.4GHz	900MHz	2.4GHz	2.4GHz	2.4GHz
Nominal Range @ 0dBm	100m	30-100m	10-100m	10-100m	30m
Maximum Data Rate	54 Mbps	40-100kbpps	250kbps	250kbps	1Mbps
Topology	Star	Mesh	Mesh	Mesh	Scatternet
Power Consumption	High	Low	Low	Low	Low
Alliance	Wi-Fi Alliance	Z-Wave Alliance	Zigbee Alliance	Thread Group	Bluetooth Sig

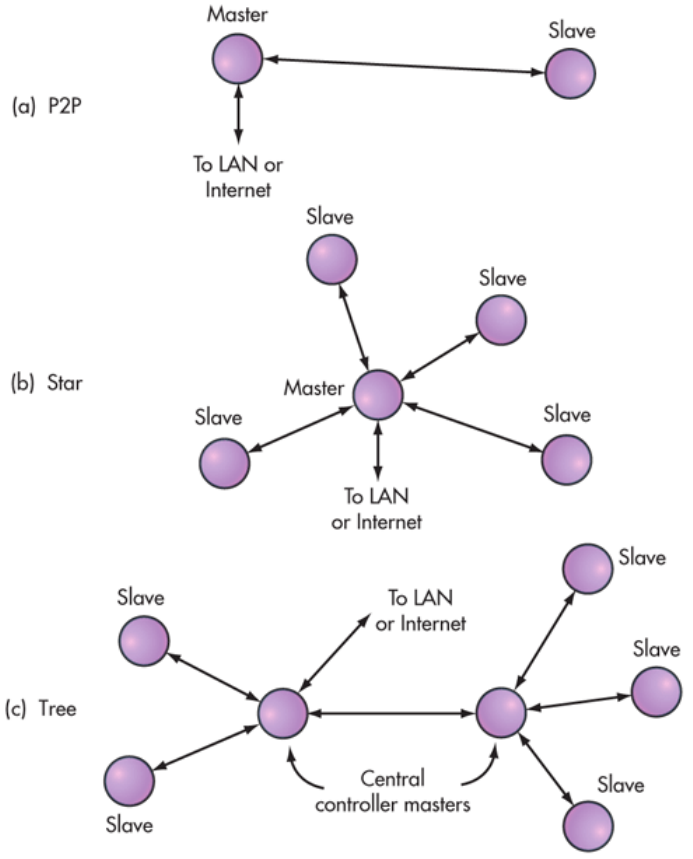
What's new?

- Bluetooth 5.0 (Released on Dec. 6, 2016)
  - "Shanghai"
  - New features
    - Longer
      - Tx power constraint relaxed
      - Channel coding applied
    - Faster
      - 2Mbps PHY Introduced
    - Greater
      - LE Advertising Extensions:
        - Logic Advertising Channel
        - Data Length 0 ~ 255 Bytes
- Bluetooth Mesh (Released in July, 2017)

BLE Technologies

- BLE Mesh
  - Mesh for IoT applications
  - Role of each node
  - Wireless Sensor Network
  - ‘Self-organizing network’





Bluetooth: Where?

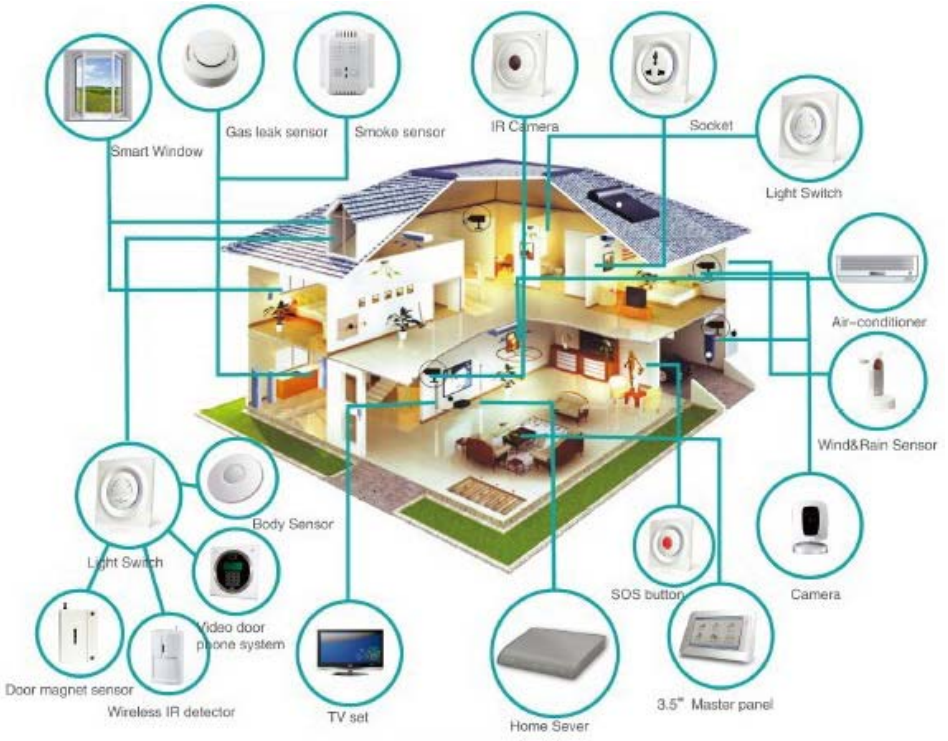
- Application scenarios
  - Audio signal transmission
    - Bluetooth earphone
    - Bluetooth speaker
    - Multimedia system in vehicles

Bluetooth: Where?

- Application scenarios
  - Industrial
    - Replacing the cable
      The original thought of Bluetooth
    - SPP (Serial Port Profile)
    - Multi UART Port
    - Makes it easy to transfer data wirelessly to smart phones / PC
    - Makes it possible to upgrade parameter / program wirelessly
    - VERY LOW COST

Bluetooth: Where?

- Application scenarios
  - Smart home
    - Remote Control for A.C, TV, …
    - Door Bell / Lock
    - Illumination
    - Music / Audio
    - Security
    - Valve for Water/Gas
    - Windows/Curtain
    - Power Socket

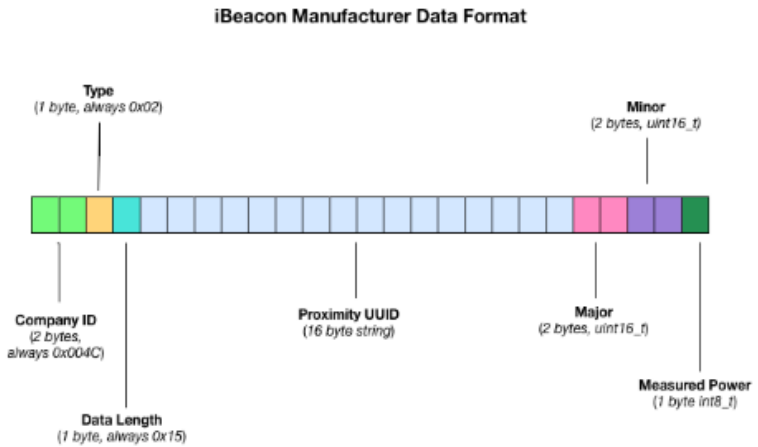


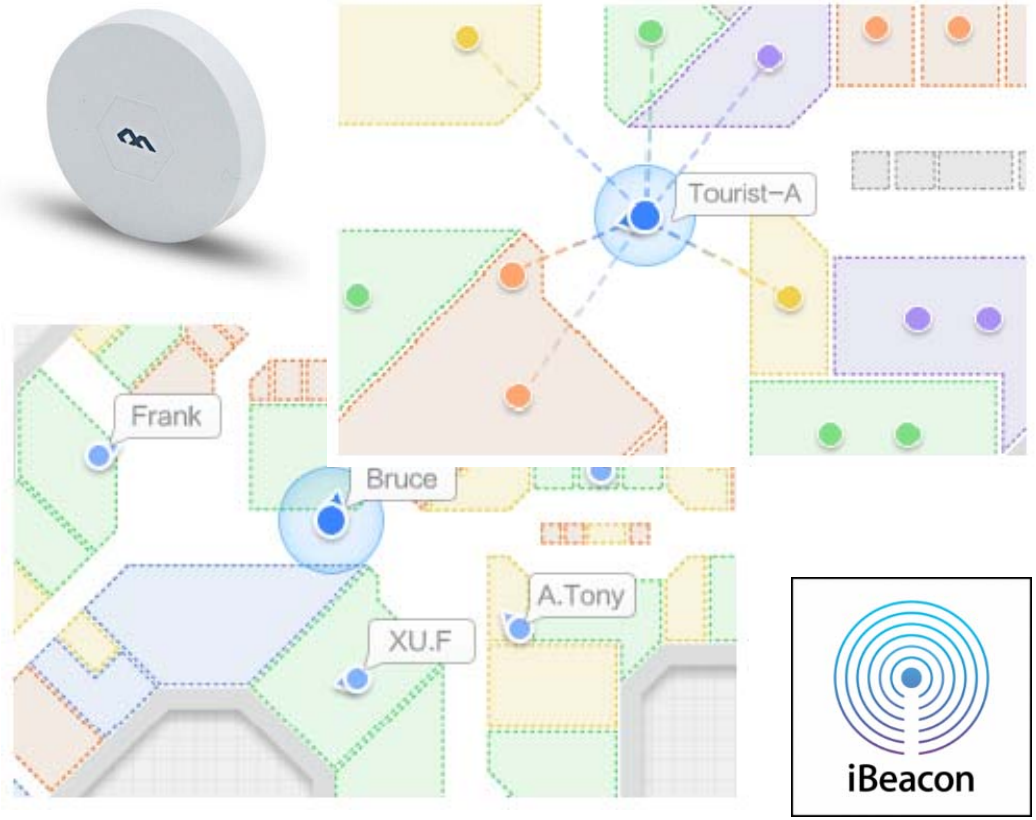
Bluetooth: Where?

- Application scenarios
  - Wearable devices
    - Smart bracelet
    - Smart watch
    - Smart shoes
    - Smart pen

Bluetooth: Where?

- Application scenarios
  - BLE broadcast
    - Advertisement
    - In-door location
    - ‘ibeacon’





Bluetooth: Where?

- Application scenarios
  - Other short range real-time communication
    - Barrier gate
    - Wireless mouse/keyboard
    - In-vehicle wireless Network
    - Shared Bicycles
    - …

Test and Authentication

- Bluetooth Qualification Tests
  - Why?
    - For SIG
      - To protect the IP, and also protect the brand
    - For Manufacturer
      - To prove the product, and to get the permission
  - What?
    - TPG – Test Plan Generator
  - How?
    - TCRL – Test Case Reference List
    - TS – Test Specifications
  - BQE
    - Bluetooth Qualification Expert
  - RF/RF-PHY Test
    - Verify the radio performance of the device
  - Protocol Conformance Test
    - Verify the protocol conformance
  - Profile Test
    - Too many types of Bluetooth devices
    - Profile defined
      - Profile Conformance Test
      - Profile Interoperability Test

Protocol Tests

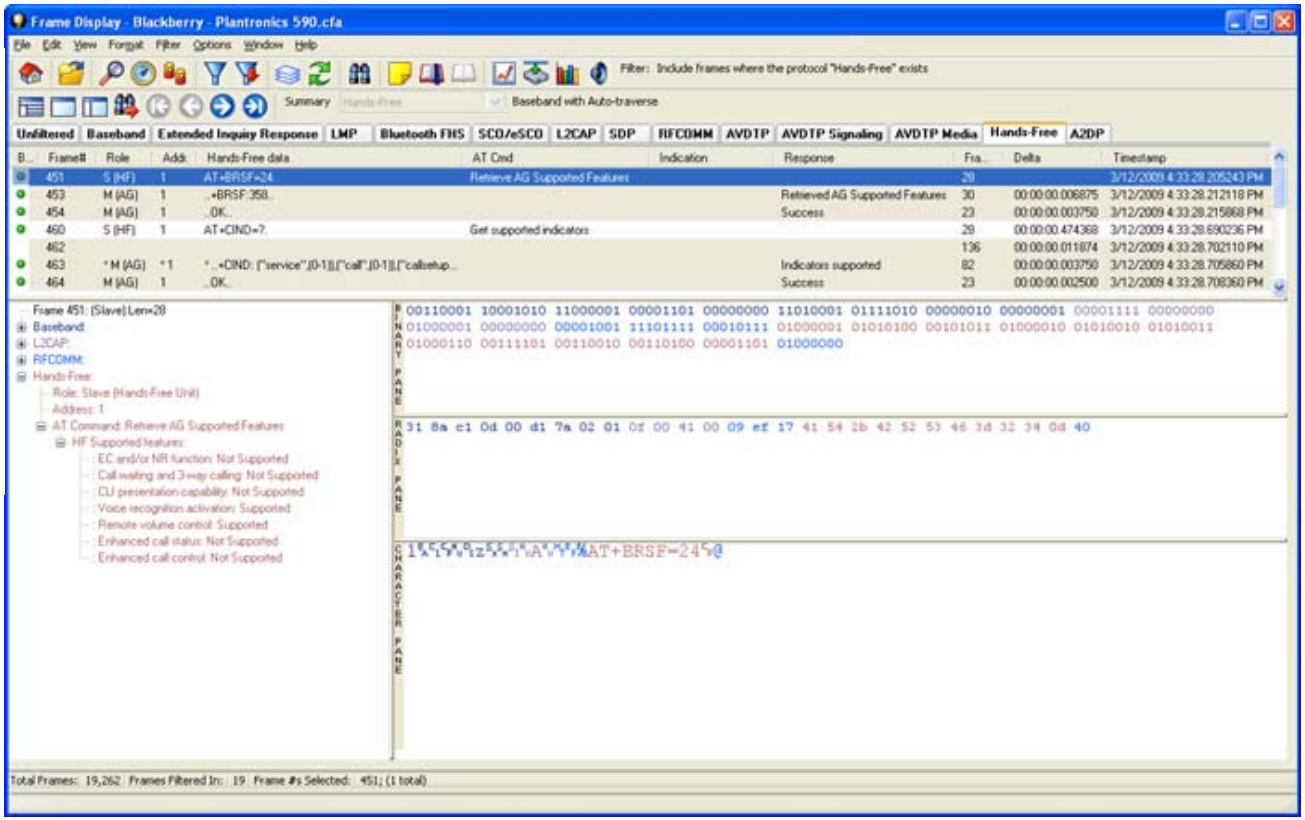
- Classic Bluetooth Mandatory tests
  - BB (Baseband)
  - LM (Link Manager)
  - L2CAP (Logical Link Control and Adaptation Protocol)
  - SDP (Service Discovery Protocol)
  - GAP (Generic Access Profile)
- BLE Mandatory tests
  - LL (Link Layer)
  - GATT (Generic Attribute profile)
  - ATT (Attribute Protocol)
  - SM (Security Manage Protocol)
  - L2CAP (Logical Link Control and Adaptation Protocol)
  - GAP (Generic Access Profile)

Core — Test Requirements for v5.0 or later

Specifications	Test Specifications	ICS (Online ICS)	IXITs/Other	TCRL (Online TCRL
802.11 MAC-PHY	802.11 MAC-PHY	ICS		TCRL
802.11 PAL	802.11 PAL	ICS		TCRL
A2MP	A2MP	ICS		TCRL
ATT	ATT	ICS	IXIT	TCRL
BB	BB	ICS	IXIT	TCRL
GAP	GAP	ICS	IXIT	TCRL
GATT	GATT	ICS	GATT Qualification Test DB IXIT	TCRL
HCI	HCI	ICS	IXIT	TCRL
L2CAP	L2CAP	ICS	IXIT	TCRL
LL	LL	ICS	IXIT	TCRL
LMP	LMP	ICS	IXIT	TCRL
RF	RF	ICS	IXIT	TCRL
RF-PHY	RF-PHY	ICS	IXIT	TCRL
SDP	SDP	ICS	IXIT	TCRL
SM	SM	ICS	IXIT	TCRL
SUM ICS - Appendix A to Declaration of Compliance: Summary of Selected Specifications in Implementation				TCRL

Protocol Tests

- Test Instrument



Profile Tests

- Test on application layer
  - Checks the accordance with profile regulations
  - Core content from SIG
  - “Optional”

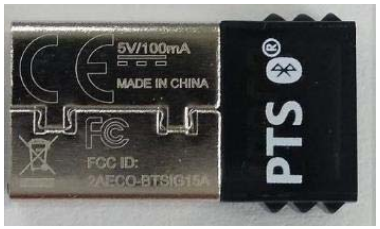
- Typical Profiles

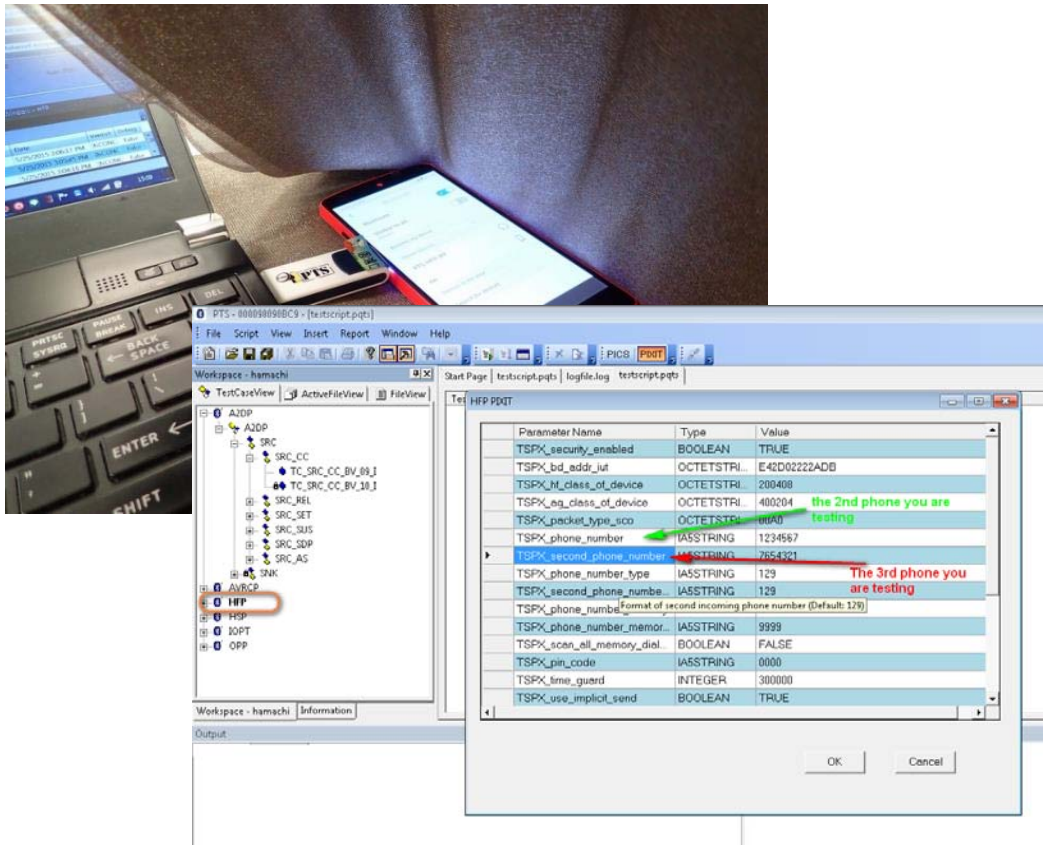
A2DP (Advanced Audio Distribution Profile)
AVRCP (Audio Video Remote Control Profile)
CTP (Cordless Telephony Profile)
FTP (File Transfer Profile)
HFP (Hands Free Profile)
HID (Human Interface Device Profile)

HSP (Handset Profile)
LAP (LAN Access Profile)
PAN (Personal Area Networking Profile)
SPP (Serial Port Profile)
SDAP (Service Discovery Application Profile)
…

Profile Tests

- Test device
  - PTS (Profile Tuning Suite)
  - Bluetooth Developer Studio Radio Module
  - Provided only by SIG





RF Tests

- Verification of Radio Performances
  - Transmitter Test
    - Output Power
      - Maximum output power
    - In-band Emission
      - Unwanted emission in ISM band
    - Modulation Characteristics
      - Frequency deviation when transmitting varieties of symbol combination
    - Carrier offset and drift
      - Initial offset of the carrier frequency
      - Long-term drift of the carrier frequency
  - Receiver Test
    - Receiving Sensitivity
      - Minimum signal level for the receiver
    - Interference Tolerance
      - Carrier / Interference
      - Receiving Intermodulation
      - Blocking performance
    - Max receiving Power
      - Maximum signal level for the receiver
    - Report integrity
      - Verifies the Package Error Rate reported

RF Tests

- Signaling test vs. non-Signaling test
  - Signaling test – classic Bluetooth
    - DUT works in the normal working status
    - General controlling command and signaling used
    - Signaling interaction as usual
    - More complicated signaling and test set
  - Non-signaling test – BLE
    - DUT works in a dedicated 'Test Mode'
    - Test commands specially designed
    - Command and respond
    - Faster and lower cost

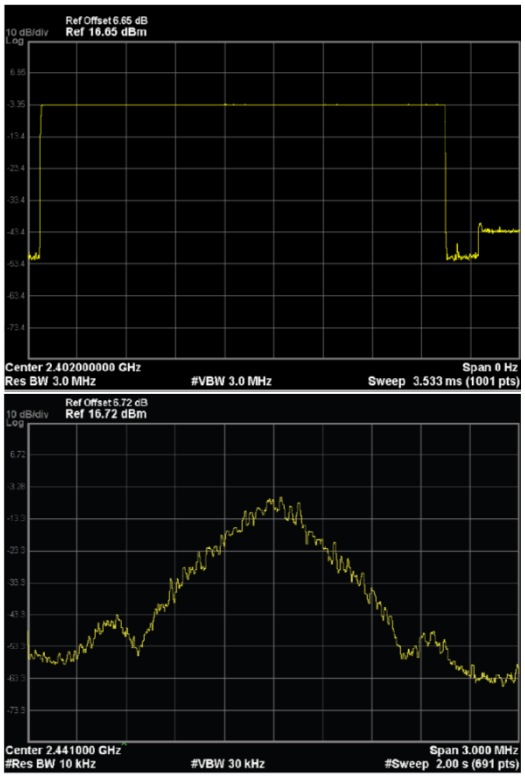
Task:
transmit '10101010' @ 2402MHz

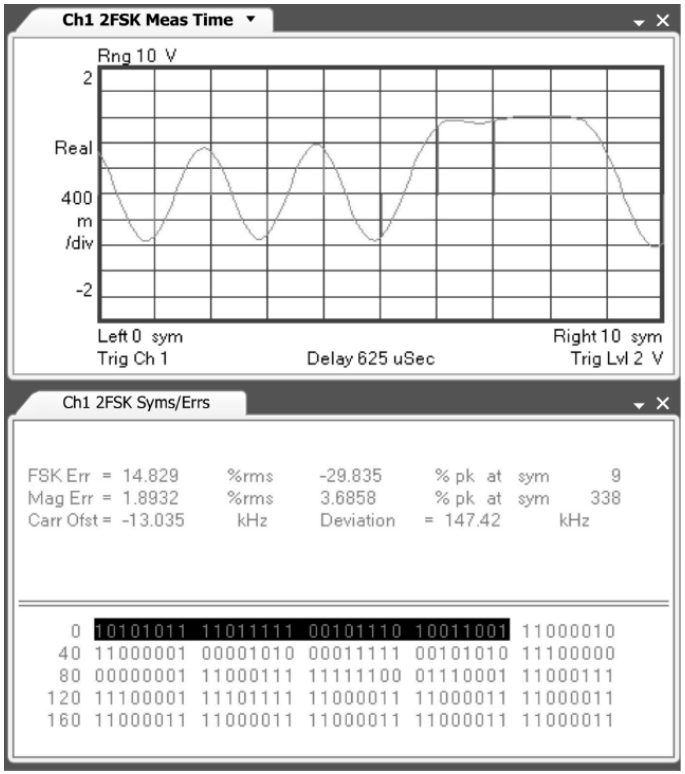
Signaling Procedures:
1. Set the DUT into engineering mode
2. Page and connect the DUT
3. Stop the frequency hopping and set the channel to 2402MHz
4. Set the DUT into loopback mode
5. Transmit signal '10101010'
6. Wait for the loopback packet

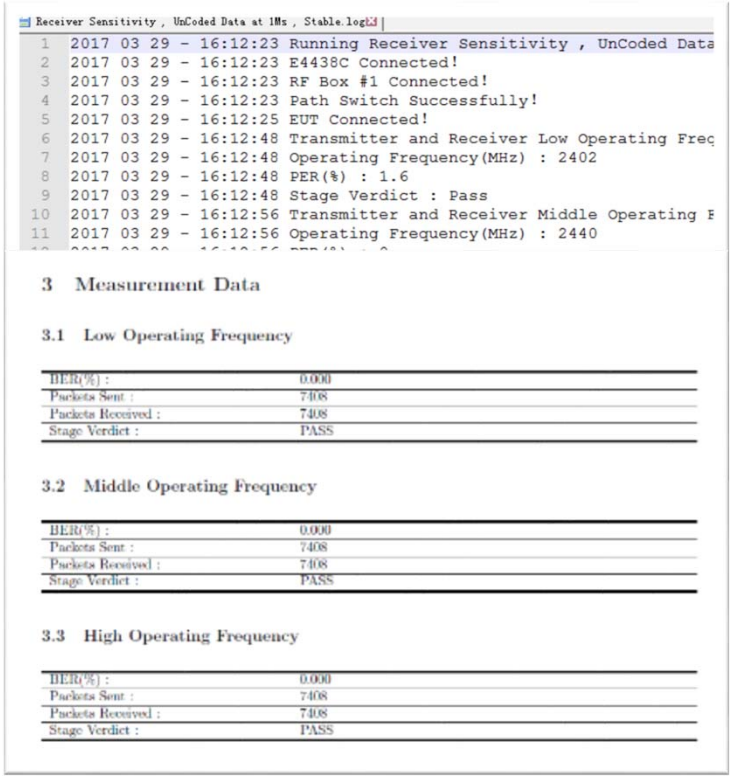
Non-signaling Procedures:
1. DUT entering Direct Test Mode
2. Tell DUT to send '10101010'@2402MHz

RF Tests

- RF tests

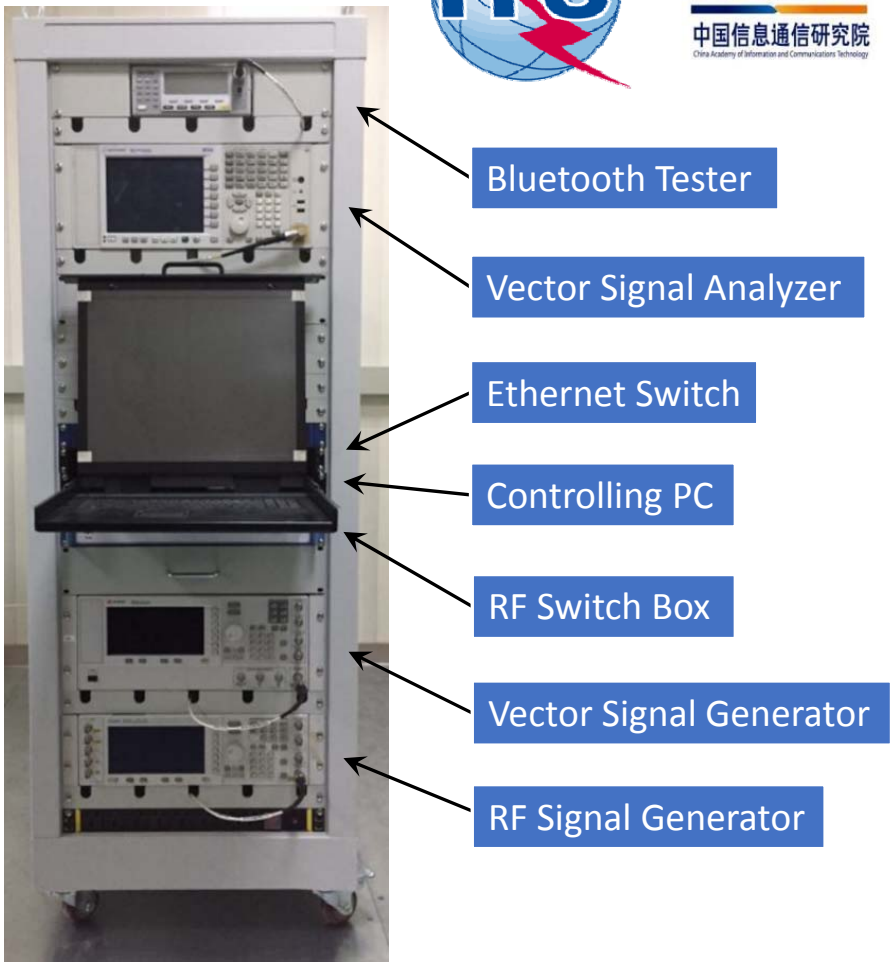






RF Tests

- RF test equipment set
  - Bluetooth tester
  - Spectrum analyzer
  - RF signal generator
  - PC controller
  - RF switch box
  - …



About CTTL - SYS

- China Telecommunication Technology Labs
  - Founded in 1981
  - Authoritative test organization
  - Supports the standards and regulation

- Main tasks
  - Information / Communication Technologies research
  - Development of ICT product standards and test methods
  - Products inspection, verification and assessment
  - Testing Instruments metrology and evaluation

- 2G/3G/4G/Microwave Equipment
- Antennas / RF Components
- WPAN (Bluetooth, NFC, RFID, Zigbee, etc…)
- Base products (Cables, Op. Fibers, accessories…)
- Signal / Service Driver test
- Power / Battery
- Anti-seismic research and test
- Metrology and calibration

About CTTL

- Our Bluetooth test solution

Bluetooth SPECIAL INTEREST GROUP

Test System Validation Decision

June 13, 2016

Test System Validation Decision

Validation is th
traceable resu
Specification.

The Bluetooth
System - V1.1
Sheet, dated 2
(hereinafter "V
System Valida

- Bluetooth
- Bluetooth
- Bluetooth

This decision i
- Bluetooth
- Bluetooth

The scope of t

The test syste
instrumentatio
compliant suc

Bluetooth SPECIAL INTEREST GROUP

Test System Validation Decision

June 26, 2017

Test System Validation Decision

Validation is the engineering process of demonstrating a test system achieves accurate, repeatable and traceable results for supported test cases and conforms to the Bluetooth Specification and Bluetooth Test Specification.

The Bluetooth Testing and Interoperability Committee (BTI) hereby acknowledges that RTSB-A Test System – V2.0.0 by CTTL-SYSTEMS is validated for the following Bluetooth Specifications (hereinafter "Validated Parts") on the basis of validation results in accordance with the Bluetooth Test System Validation Guideline Validation Guideline:

- Bluetooth Specification, Part: RF, version 5.0 and earlier
- Bluetooth Specification, Part: RF-PHY, version 5.0 and earlier

The scope of the validation decision is Test Platform and Test Case Implementation for Validated Parts.

After this decision CTTL-SYSTEMS may declare additional test cases validated within Validated Parts after the concurrence of the BTI. CTTL-SYSTEMS shall maintain validation material and make it available to Bluetooth Special Interest Group.

Bluetooth Specification Interest Group reserves the right to review validation status annually and at any time test system status has changed pertaining to validation requirements. The Bluetooth Specification

Thank You

Trainer: Yang Bo

E-mail: yangbo3@caict.ac.cn

Department: Dept. of Wireless Technology, CTTL-System, CAICT

Address: No. 11 Yuetannan Street, Xicheng Dist. Beijing, P.R.China

China Academy of Information and Communications Technology

http://www.caict.ac.cn