無線網路概論
Intro. to Wireless Internet

Lecture 07 – Bluetooth

Lecturer: 陳彥安 Chen, Yan-Ann

YZU CSE

Lecture Material

- "Wireless Communication Networks and Systems", Corry Beard and William Stallings, 2016.
  - Ch 12. Bluetooth and IEEE 802.15
- Wireless Sensor Networks and RFID Technologies
  - NCTU Open Course
  - http://ocw.nctu.edu.tw/course_detail-v.php?bgid=9&gid=0&nid=250
- Wireless Internet
  - Prof. You-Chiun Wang
  - National Sun Yat-sen University
- Wireless Networks and Applications
  - Prof. Peter Steenkiste
  - Carnegie Mellon University

Outline

- Introduction
- Bluetooth Protocol Stack
- Piconets & Scatternets
- Bluetooth Communication States
- Bluetooth links, packet format, and security
- Bluetooth HS & Smart

What is Bluetooth?

- Bluetooth is a universal radio interface operated in 2.4 GHz unlicensed band.
- It enables electronic devices to connect and communicate wirelessly via short-range (10~100 meters), ad-hoc networks.
- Bluetooth key features:
  - Peak data rate: 1 Mbps (version 1.2)
  - Low power: Peak transmission power ≤ 20 dBm
  - Low cost: Target is $5-10 per piece.
  - Ability to simultaneously handle both voice and data
  - Line of sight is not required.

History of Bluetooth (1/2)

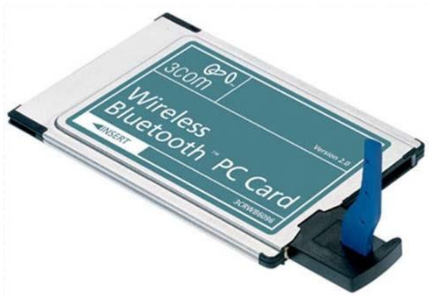
- Bluetooth was invented by L. M. Ericsson, Sweden in 1994.
- Bluetooth special interest group (SIG) was founded by Ericsson, IBM, Intel, Nokia and Toshiba in Feb 1998.
  - Today, it has more than 1,900 members.
  - Bluetooth is also defined in the IEEE 802.15.1 standard.

History of Bluetooth (2/2)

- Bluetooth is in honor of King Harald Blaatand (Bluetooth) (A.D. 940 to 985)
  - 10th century Viking king in Denmark
  - He united the country and established Christianity.
  - Viking states included Norway and Sweden, which is the connection to Ericsson (creator of Bluetooth).

Objectives of Bluetooth

- Bluetooth was originally a cable-replacement technology. Now it has the following targets:
  - Provide ubiquitous computing environment for networked devices.
  - Mobile access to LANs and Internet
  - Home networking
  - Automatic synchronization of data
  - Voice applications: Hands-free headset



Bluetooth Application Areas

- Data and voice access points
  - Real-time voice and data transmissions.
- Cable replacement
  - Eliminates need for numerous cable attachments for connection.
- Ad hoc networking
  - Device with Bluetooth radio can establish connection with another when in range.
- Top Uses
  - Mobile handsets, Voice handsets, Stereo headsets and speakers, PCs and tablets,
  - Human interface devices, such as mice and keyboards, Wireless controllers for video game consoles,
  - Cars, Machine-to-machine applications: credit-card readers, industrial automation, etc.

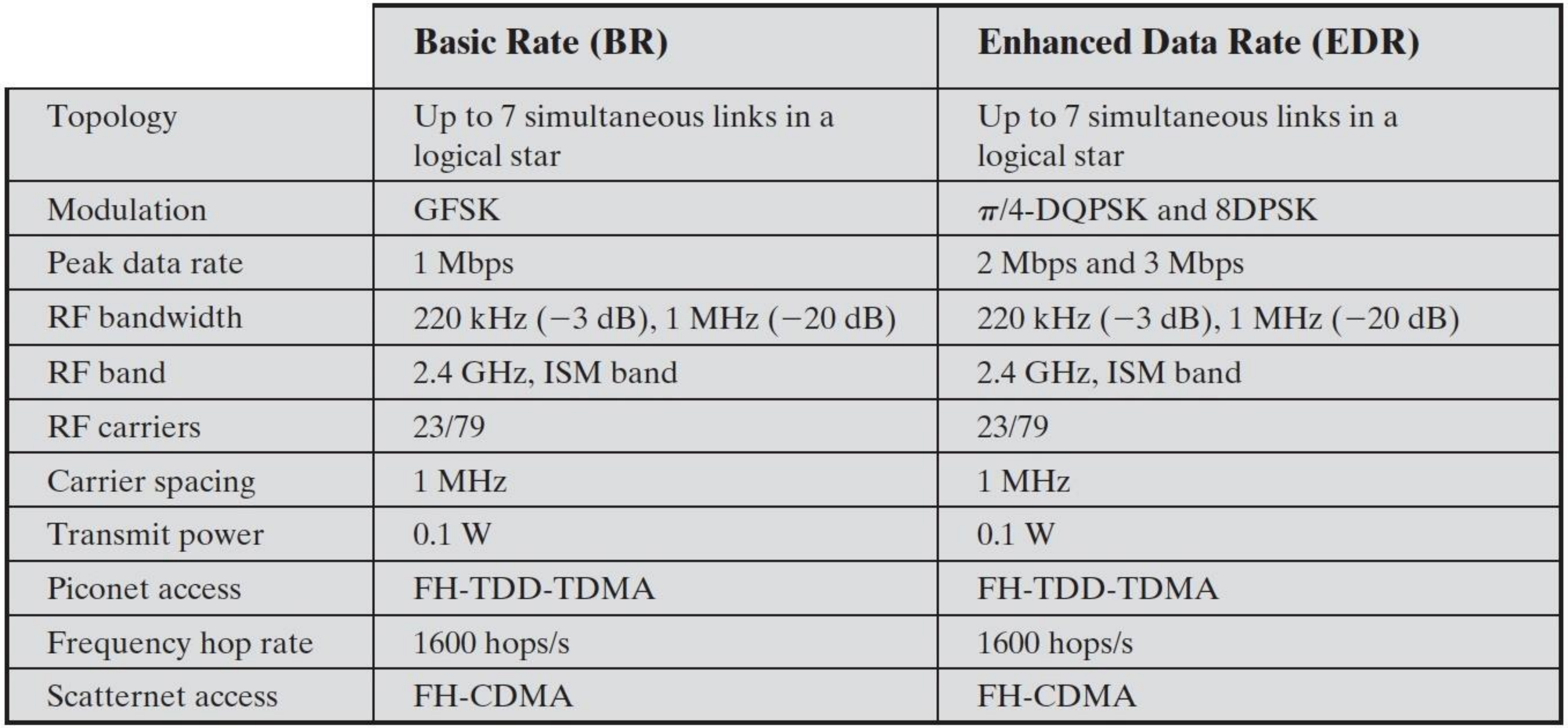
Bluetooth Pros/Cons

- Superiority
  - Wireless (no cables)
  - No setup needed
  - Low power consumption (about 1 milliwatt)
  - Industry-wide support
- Inferiority of Bluetooth
  - Short communication range (about 10 meters)
  - Very limited transmission rates (about 1 Mbps)
    - Improvement:
    - Version 2.0 -> up to 3 Mbps by using different modulation
    - Version 3.0/4.0 -> up to 24 Mbps by using Wi-Fi technology
  - Mostly for personal use (PANs)

Challenges of Bluetooth

- Bluetooth works across a diverse set of devices with varying computing power and memory.
- Dynamic environment:
  - The number, location, and variety of devices could change.
  - Connection establishment, routing, and service discovery protocols have to take this into consideration.
- Bluetooth should support unconscious connection establishment for devices.
- The size of implementation should be small.
  - The power consumption should not be more than a fraction of the host device.

Radio and Baseband Parameters



	Basic Rate (BR)	Enhanced Data Rate (EDR)
Topology	Up to 7 simultaneous links in a logical star	Up to 7 simultaneous links in a logical star
Modulation	GFSK	π/4-DQPSK and 8DPSK
Peak data rate	1 Mbps	2 Mbps and 3 Mbps
RF bandwidth	220 kHz (−3 dB), 1 MHz (−20 dB)	220 kHz (−3 dB), 1 MHz (−20 dB)
RF band	2.4 GHz, ISM band	2.4 GHz, ISM band
RF carriers	23/79	23/79
Carrier spacing	1 MHz	1 MHz
Transmit power	0.1 W	0.1 W
Piconet access	FH-TDD-TDMA	FH-TDD-TDMA
Frequency hop rate	1600 hops/s	1600 hops/s
Scatternet access	FH-CDMA	FH-CDMA

Bluetooth Standard Documents

- Bluetooth specification describes how the Bluetooth technology works.
  - That is, the Bluetooth protocol architecture.
  - Core specifications: details of various layers of Bluetooth protocol architecture
- Bluetooth profile describes how the technology is used.
  - That is, how different parts of the specification can be used to fulfill a desired function for a Bluetooth device?
  - Profile specifications: use of Bluetooth technology to support various applications

Outline

- Introduction
- Bluetooth Protocol Stack
- Piconets & Scatternets
- Bluetooth Communication States
- Bluetooth links, packet format, and security
- Bluetooth HS & Smart

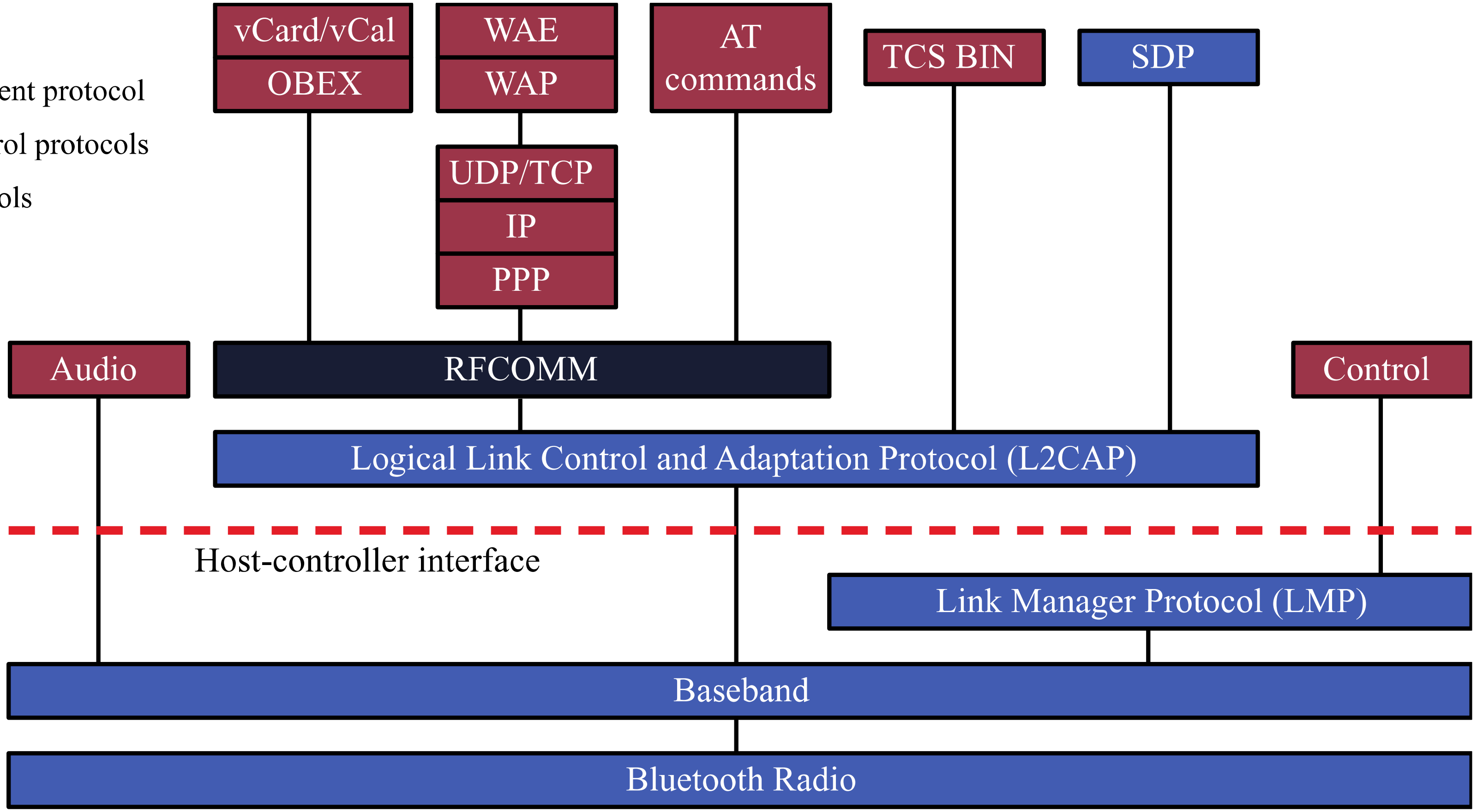
Bluetooth Protocol Stack

🟦 = Core protocols

⬛ = Cable replacement protocol

🟥 = Telephony control protocols

🟥 = Adopted protocols

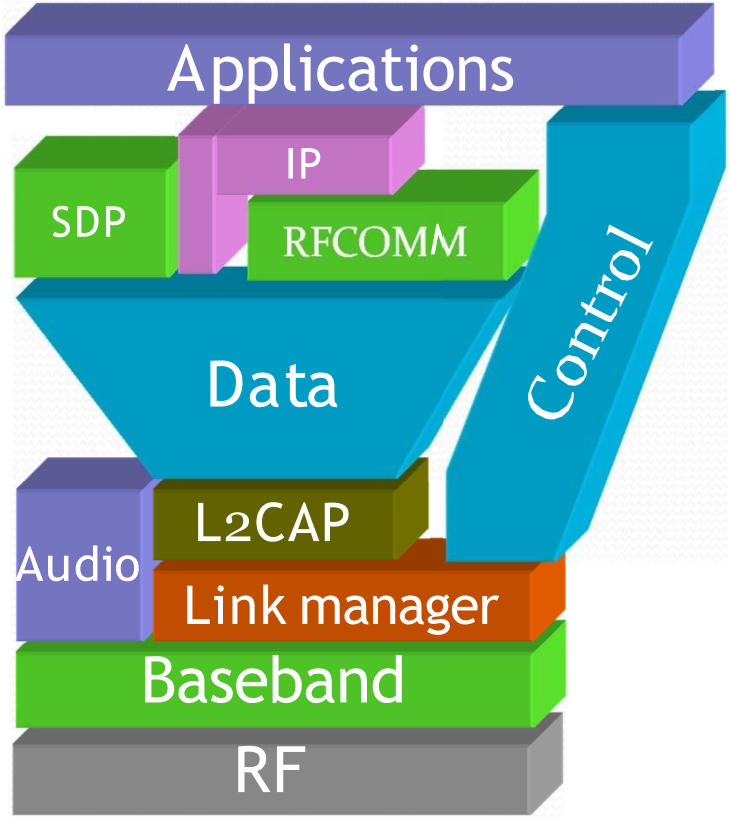


vCard/vCal
OBEX
WAE
WAP
UDP/TCP
IP
PPP
AT commands
TCS BIN
SDP
Audio
RFCOMM
Control
Logical Link Control and Adaptation Protocol (L2CAP)
Host-controller interface
Link Manager Protocol (LMP)
Baseband
Bluetooth Radio

AT	=	Attention sequence (modem prefix)	TCS BIN	=	Telephony control specification - binary
IP	=	Internet Protocol	UDP	=	User Datagram Protocol
OBEX	=	Object exchange protocol	vCal	=	Virtual calendar
PPP	=	Point-to-Point Protocol	vCard	=	Virtual card
RFCOMM	=	Radio frequency communications	WAE	=	Wireless application environment
SDP	=	Service discovery protocol	WAP	=	Wireless application protocol
TCP	=	Transmission control protocol			

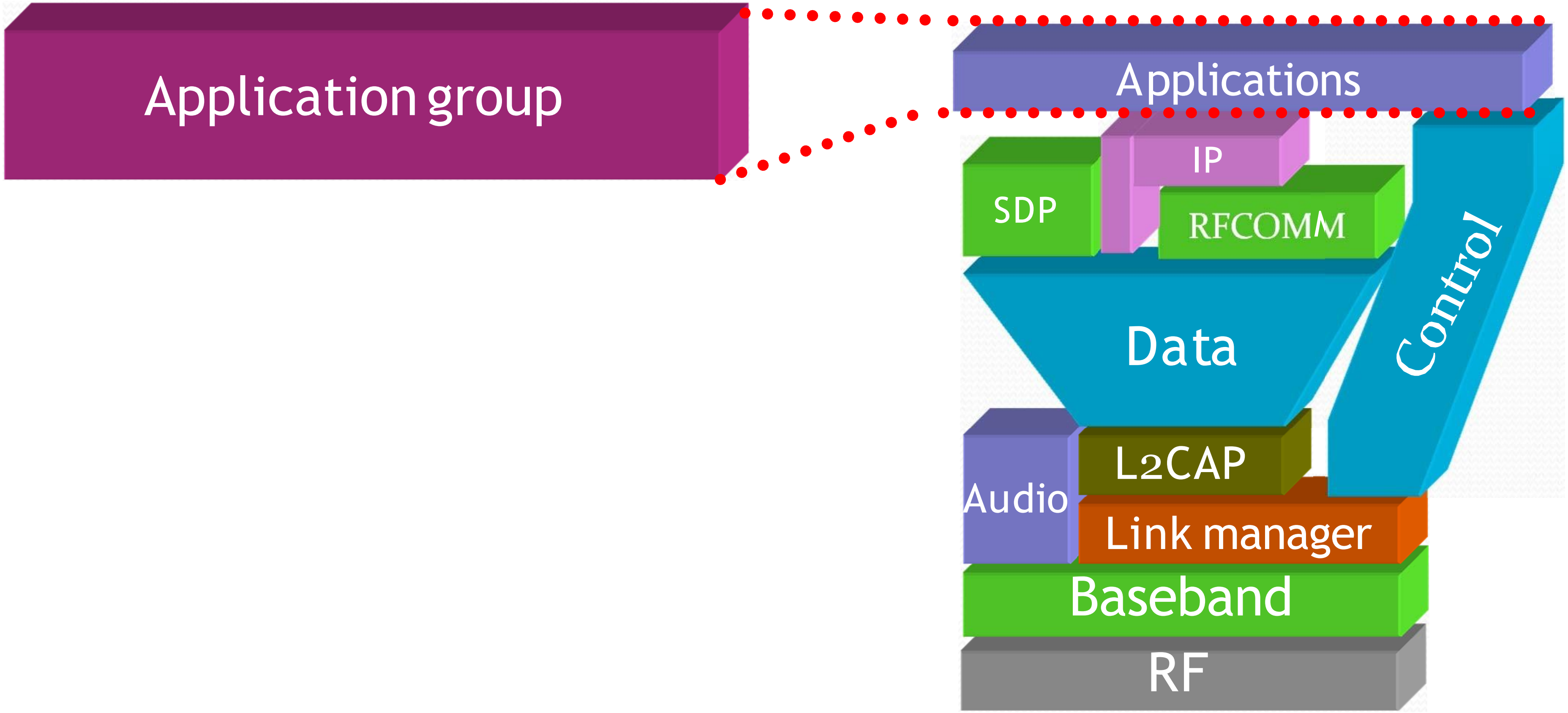
Bluetooth Protocol Group

- Bluetooth protocol stack can be divided into three major groups:
  - Application group
  - Middleware protocol group
  - Transport protocol group



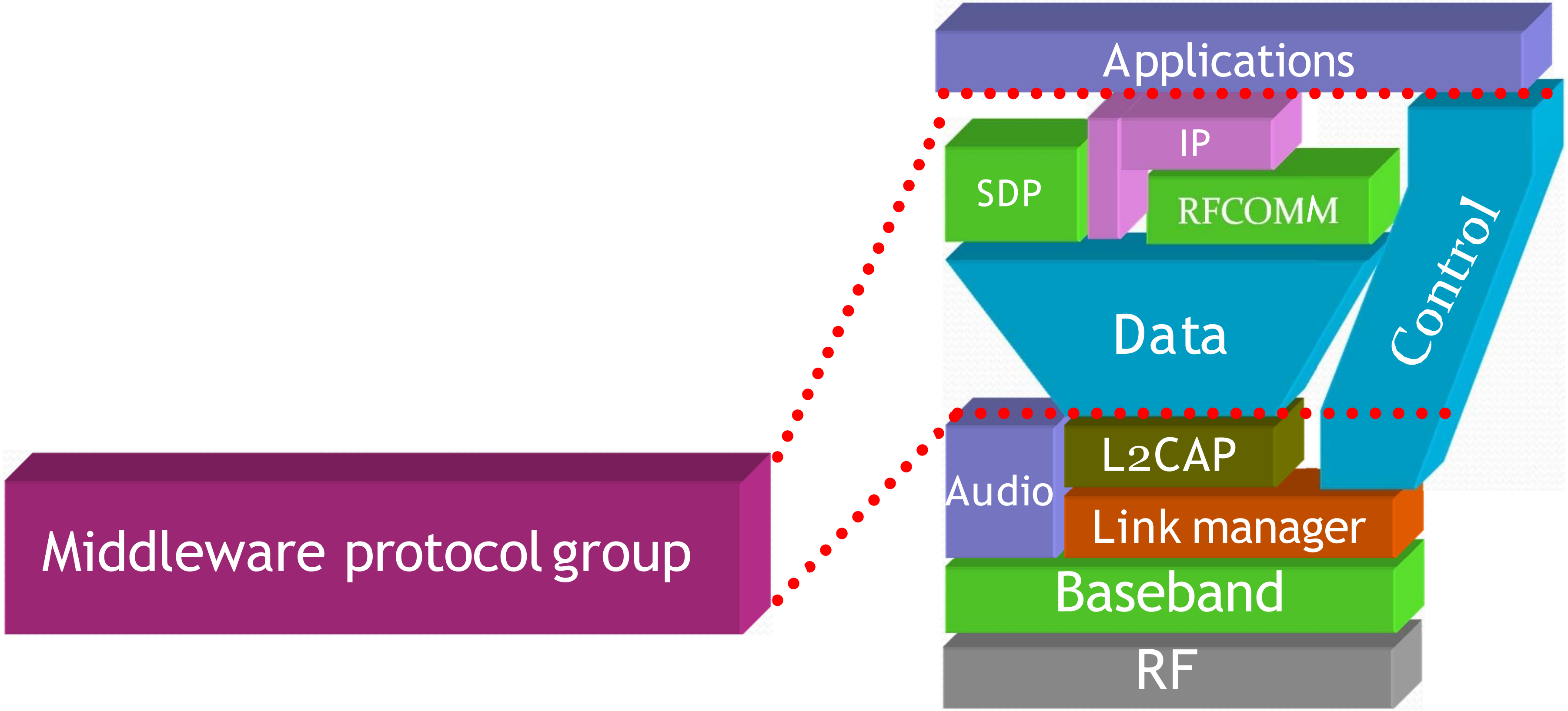
Application Group

- Application group consists of both Bluetooth-aware and Bluetooth-unaware applications.



Middleware Protocol Group (1/2)

- Middleware protocols are used to allow existing and new applications to operate over Bluetooth, which mainly including:
  - Packet-based telephony control signaling protocol
  - SDP: Service discovery protocol

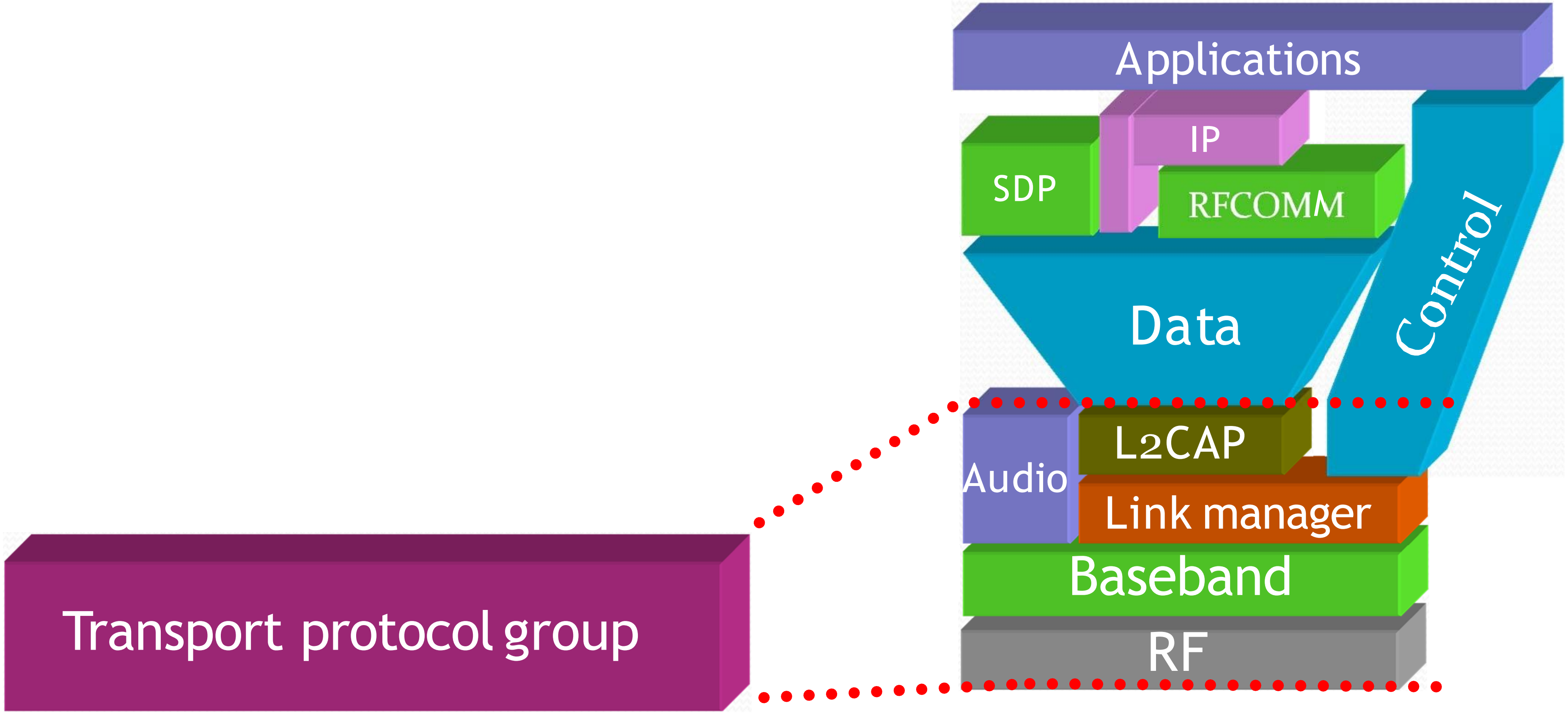


Middleware Protocol Group (2/2)

- Service discovery protocol (SDP):
  - SDP allows applications to discover device information, services, and characteristics.
  - It runs on a client-server model.
    - Each device runs only one SDP server.
    - One client may be run for each application.
- TCP/IP:
  - Network protocols for data communication and packet routing
- RFCOMM:
  - A cable-replacement protocol
  - Emulation of serial ports over wireless network

Transport Protocol Group (1/3)

- Transport protocol group allows Bluetooth devices to locate each other.
  - It creates, configures, and manages both physical and logical links, which allow higher-layer protocols and applications to pass their data.



Transport Protocol Group (2/3)

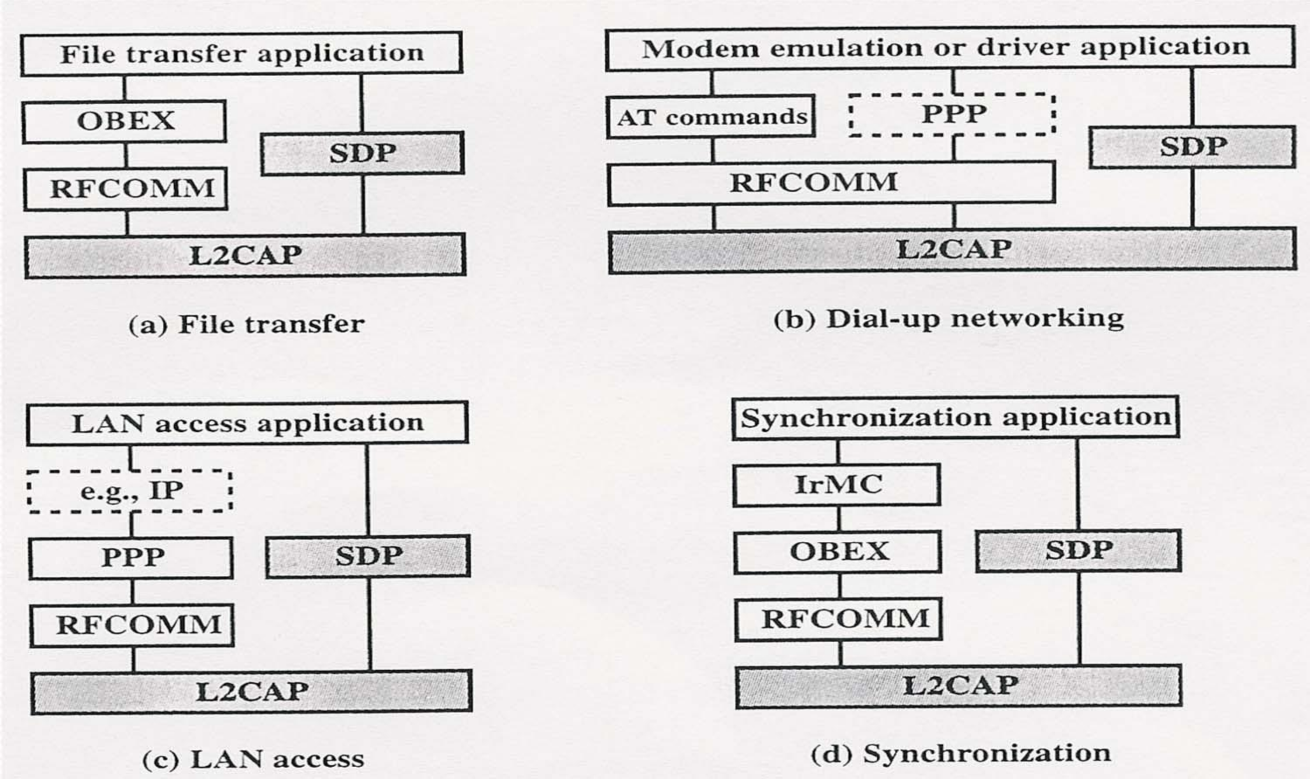
- Radio frequency (RF):
  - Send and receive modulated bit streams.
  - It deals with frequency hopping, modulation, and transmitting power.
- Baseband:
  - Define the timing and framing mechanisms.
  - Provide flow control on each link.
- Link manager:
  - Link setup between BT devices and ongoing link management.
  - Manage the connection states (e.g., authentication and encryption).
  - Enforce fairness among devices.
  - Deal with the power management mechanism.

Transport Protocol Group (3/3)

- Logical link control & adaptation protocol (L2CAP):
  - Adapts upper-layer protocols to the baseband layer.
  - Handle multiplexing of higher-level protocols.
  - Provide segmentation and reassembly of large packets.
  - Support device discovery and quality of service.
  - Provide connectionless and connection-oriented services.
- Audio:
  - Audio data are directly mapped to the baseband layer.

Bluetooth Usage Models

- Bluetooth usage models are defined in profile documents.
  - Each usage model defines a set of protocols that implement a particular Bluetooth-based application.



(a) File transfer

(b) Dial-up networking

(c) LAN access

(d) Synchronization

Profiles

- Over 40 different profiles are defined in Bluetooth documents
  - Only subsets of Bluetooth protocols are required
  - Reduces costs of specialized devices
- All Bluetooth nodes support the Generic Access Profile
- Profiles may depend on other profiles
  - Example: File Transfer Profile
    - Transfer of directories, files, documents, images, and streaming media formats
    - Depends on the Generic Object File Exchange, Serial Port, and Generic Access Profiles.
    - Interfaces with L2CAP and RFCOMM protocols
- Examples
  - SPP
    - https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=260866&vId=290097
  - A2DP
    - https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=457083

Common Usage Models

- Bluetooth defines three common usage models:
  - Voice & data access points
  - Peripheral interconnects
  - Personal area networking (PAN)

Voice & Data Access Points

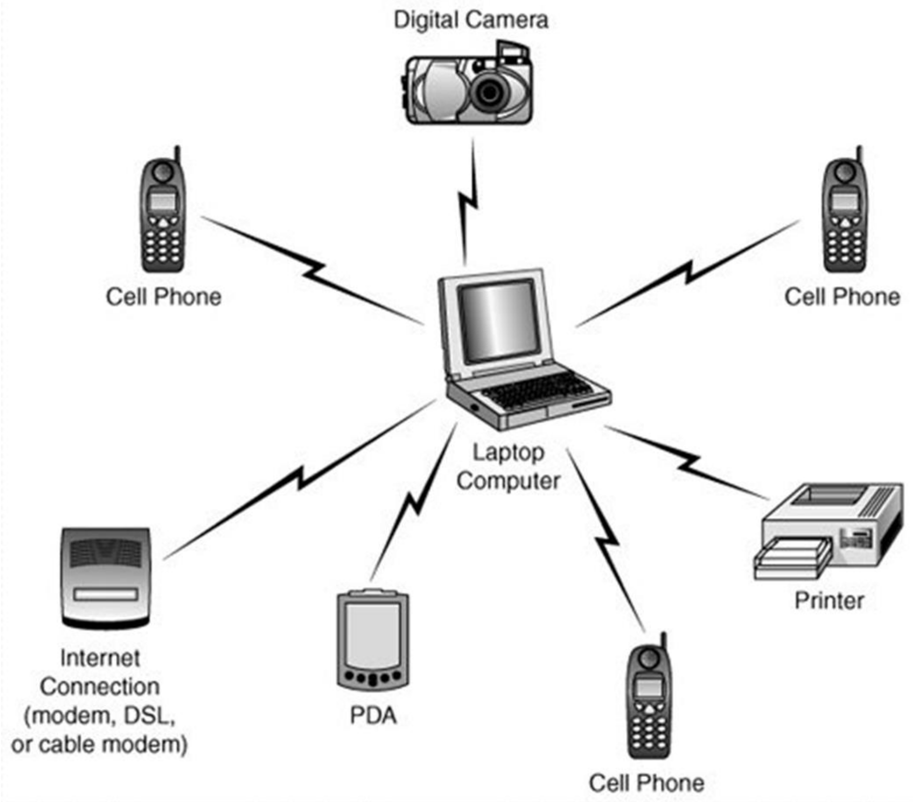
- Connect a computing device to a communicating device.
- Allow any device with a Bluetooth chip to connect to the Internet when it locates within the communication range of an access point.
  - [Example]
    A notebook can connect to the Internet by using a mobile phone to serve as an access point.
  - Envision public data access points.

Peripheral Interconnects

- Standard peripheral devices such as keyboards, mice, and headsets can work over a wireless link.
  - The same device can be used in multiple functions.
  - [Example]
    A headset can access phones while in the office, and interface with a cellular phone when mobile.

Personal Area Networking (PAN)

- PAN usage model allows the dynamic formation and breakdown of a piconet (i.e., ad-hoc personal network).

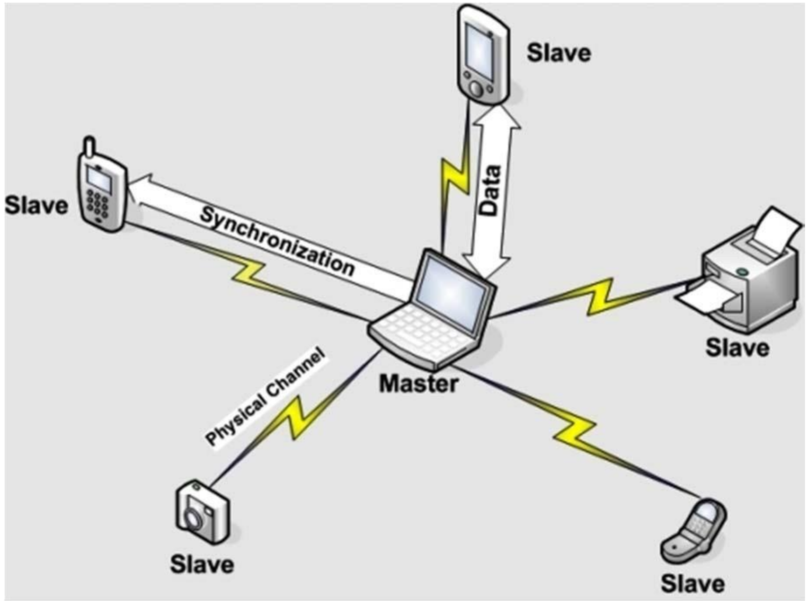


Outline

- Introduction
- Bluetooth Protocol Stack
- Piconets & Scatternets
- Bluetooth Communication States
- Bluetooth links, packet format, and security
- Bluetooth HS & Smart

Piconet (1/2)

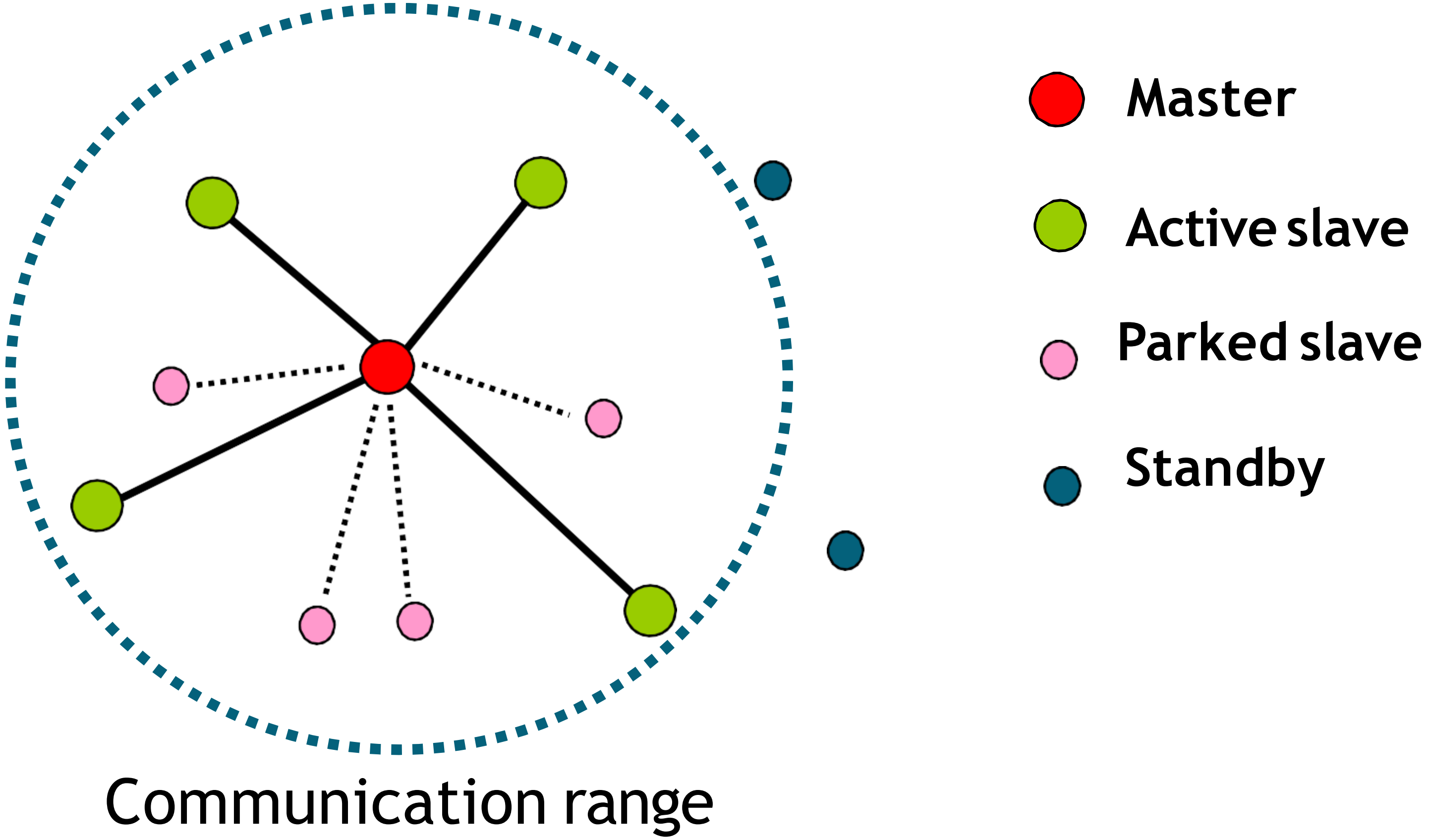
- A Bluetooth piconet is a collection of devices connected through the Bluetooth technology in an ad hoc fashion.
- A piconet starts with two connected devices, and may grow to up to eight connected devices.



Piconet (2/2)

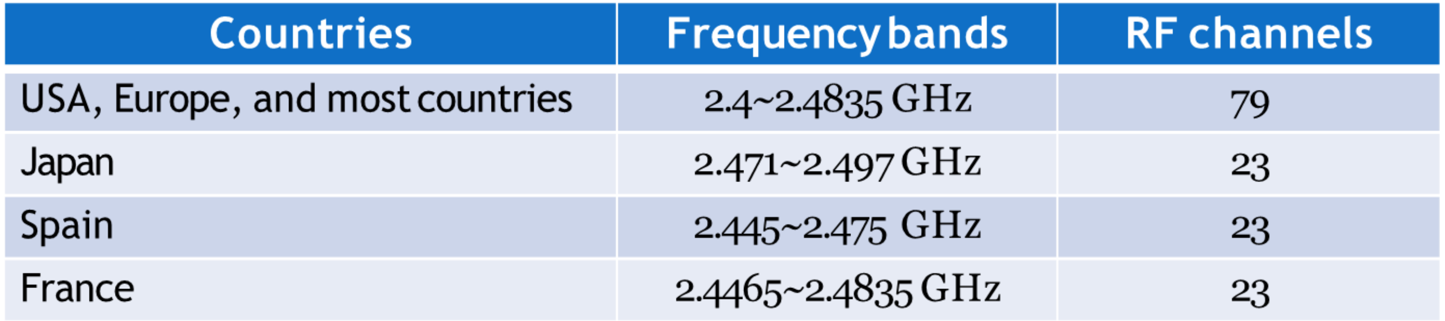
- In general, all Bluetooth devices are peer units and have identical implementations.
- However, when forming a piconet, one device will act as a master, and other devices act as slaves for the duration of piconetconnection.
  - There are up to seven (active) salves in a piconet.
  - Participants may change roles if a slave wants to take over as the master.
- Each piconet is defined by a different hopping channel to which Bluetooth devices synchronize to.
  - Each piconet has the maximum capacity of 1 Mbps (version 1.2).
- Hopping pattern is determined by the master.
  - The decision is based on its device address and clock as parameters.

Structure of a Piconet



Channels in a Piconet (1/2)

- Piconet channel is represented by a pseudo-random hopping sequence (through 79 or 23 RF frequencies).

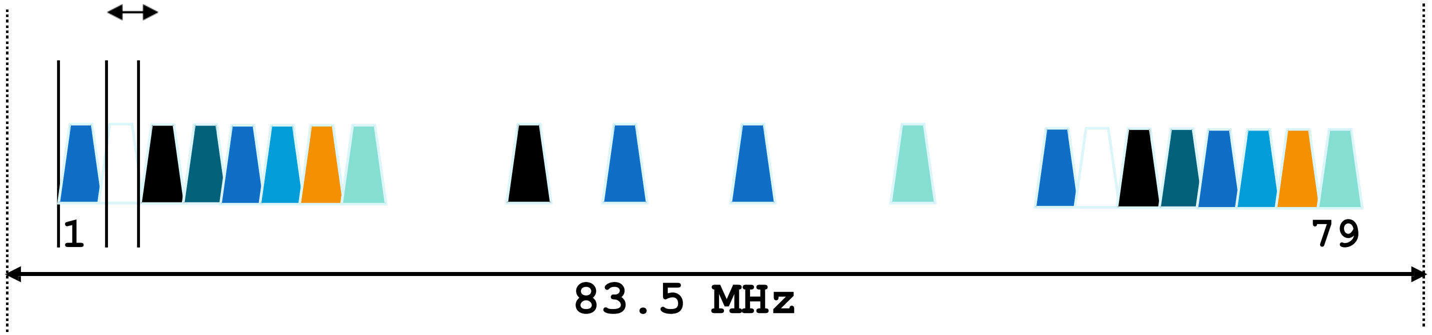


Countries	Frequency bands	RF channels
USA, Europe, and most countries	2.4~2.4835 GHz	79
Japan	2.471~2.497 GHz	23
Spain	2.445~2.475 GHz	23
France	2.4465~2.4835 GHz	23

- Hopping sequence is unique for each piconet and it is determined by the master’s address. The phase is decided by the master’s clock.
- The channel is divided into time slots.
  - Each time slot has a duration of 0.625ms. (1600 hops per second)
- Each slot corresponds to a different hop frequency.

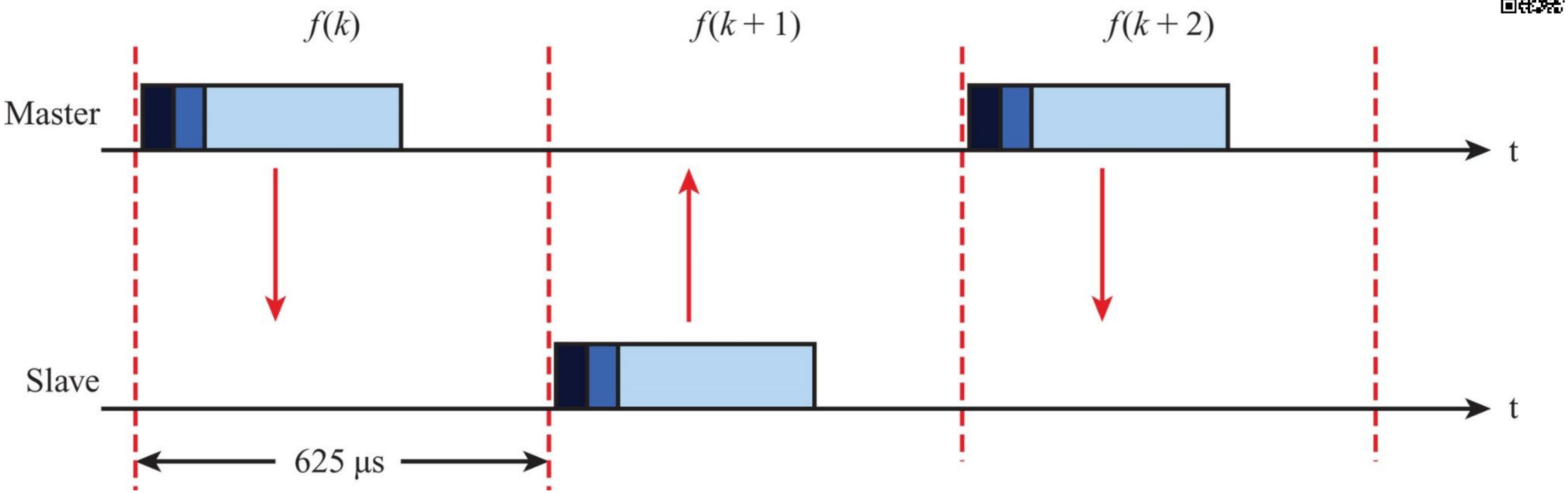
Channels in a Piconet (2/2)

- Divide the frequency band into 1 MHz-hop channels.
- Radio hops from one channel to another in a pseudo-random manner as dictated by a hop sequence.
- The instantaneous (hop) bandwidth remains small.
- Frequency hopping can help alleviate the narrow-band interference.



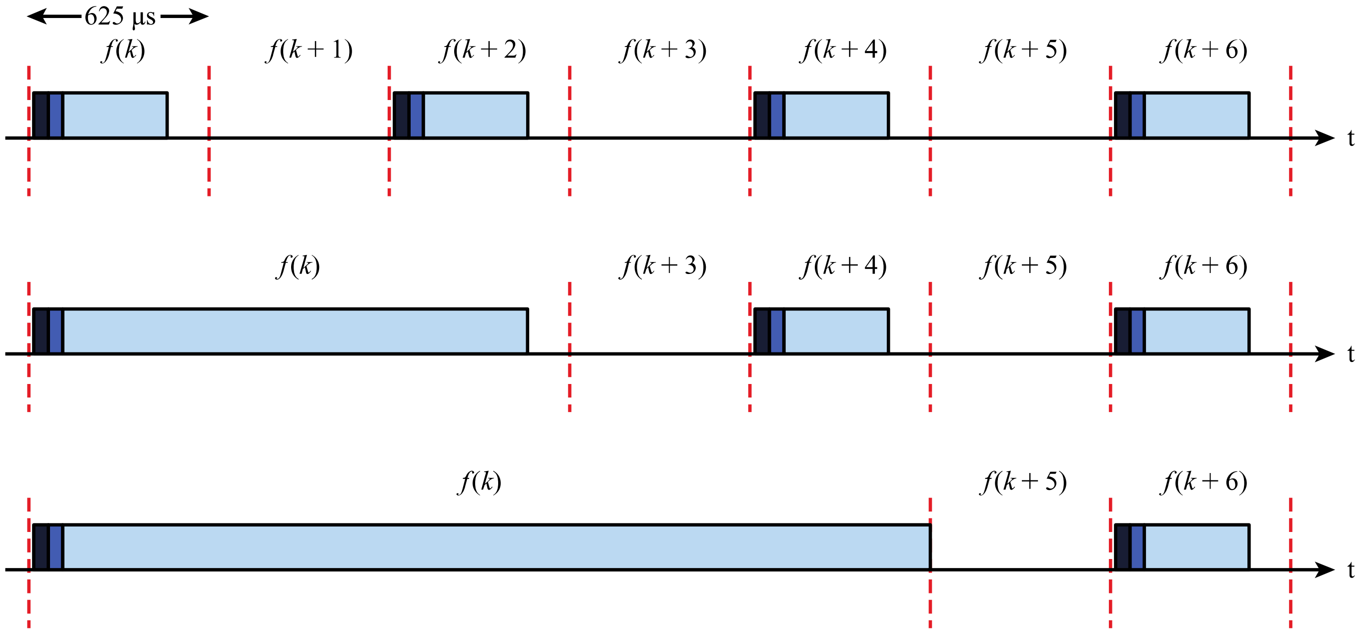
Time-division Duplex (1/2)

- Bluetooth uses a time-division duplex (TDD) method.
  - One packet can be transmitted per slot.
- Time slots are alternatively used for sending and receiving.
  - Strict alternation of slots between the master and the slaves
  - Master can send packets to a slave only in even slots.
  - Slave can send packets to the master only in odd slots.



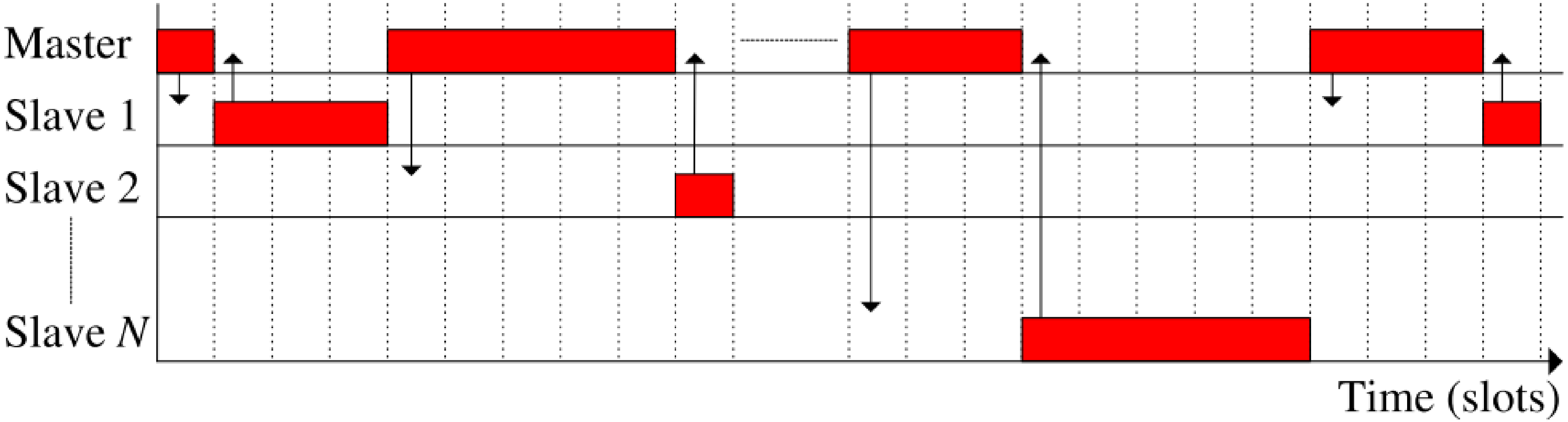
Time-division Duplex (2/2)

- Bluetooth allows a device to use 1, 3, or 5 continuous slots to transmit packets.
- While transmitting multi-slot packets, the frequency remains the same.
  - After transmitting the multi-slot packet, the device goes back to the normal frequency as that in transmitting 1-slot packets.
  - Thus, such packets may encounter higher out-band interference.



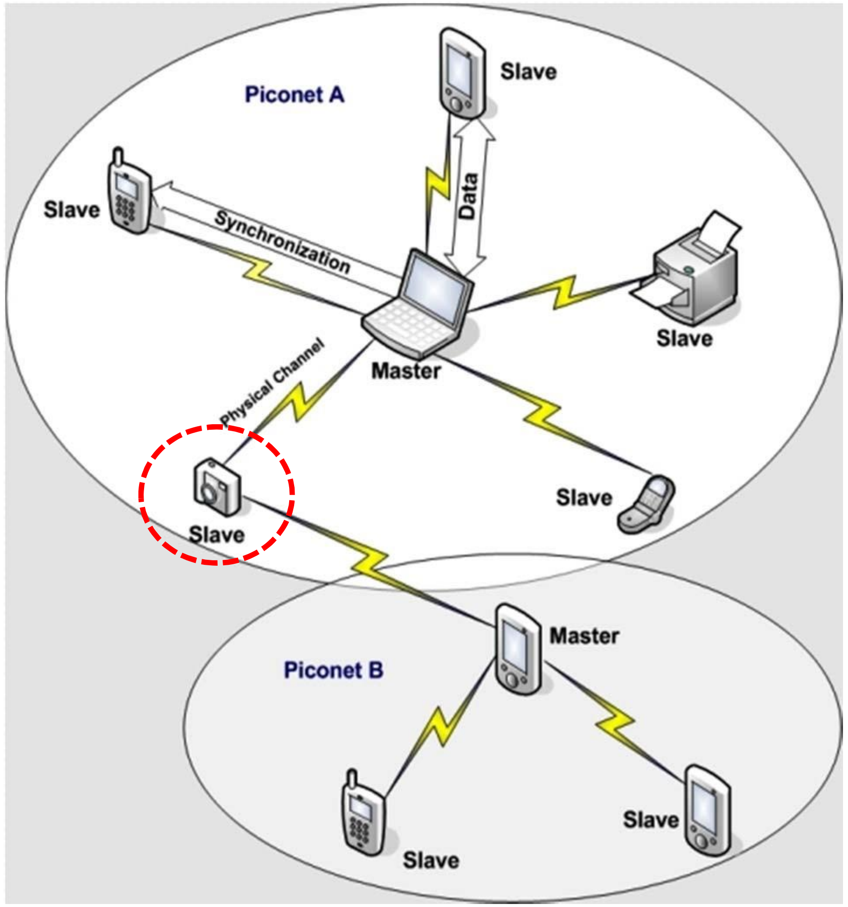
TDD in a Piconet

- The master schedules the traffic in a piconet according to an intra-piconet scheduling algorithm.



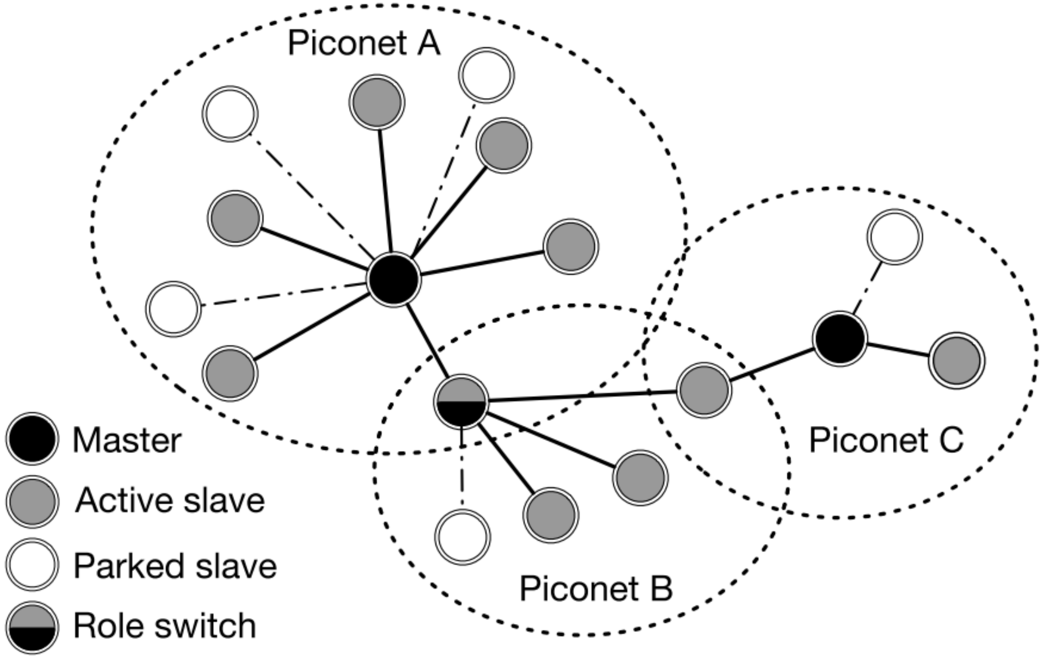
Scatternet

- A device in one piconet may also serve as one part of another piconet.
  - This device can be either a master or slave in each piconet.
  - A group of overlapping piconets is called a scatternet.
- Users in a piconet share a 1 Mbps channel. However, individual throughput decreases drastically as more devices are added.
- Collisions do occur when two piconets use the same 1 MHz hop channel simultaneously. When the number of piconets increases, the performance degrades gracefully.



Inter-piconet Communication

- A device may participate in more than one piconet on a time division multiplexing (TDM) basis.
  - To participate in a piconet, the device needs the master’s identity and the clock offset.
  - While leaving the piconet, it must inform the master.
- Master can also multiplex as a slave on another piconet.
  - However, all traffics in its piconet will suspended in its absence.

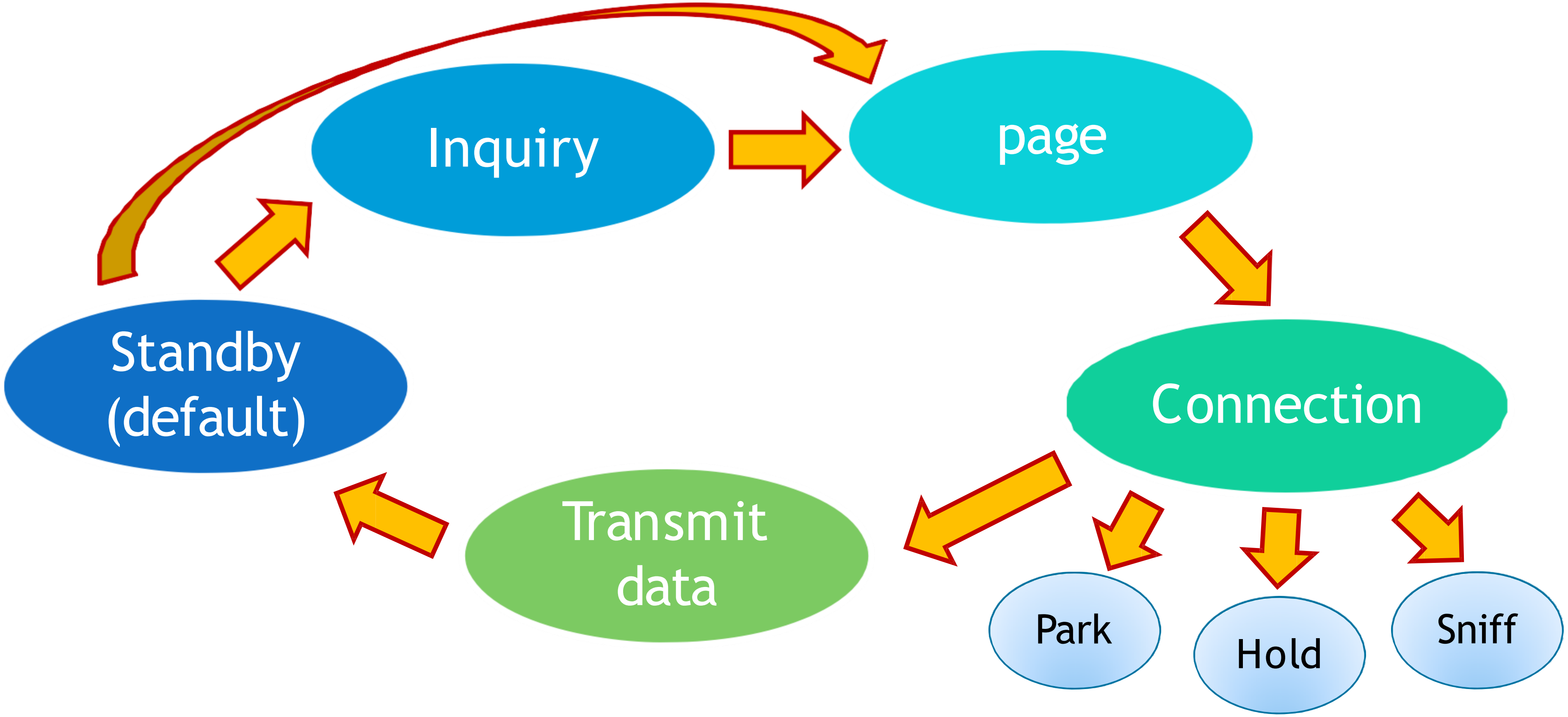


Outline

- Introduction
- Bluetooth Protocol Stack
- Piconets & Scatternets
- Bluetooth Communication States
- Bluetooth links, packet format, and security
- Bluetooth HS & Smart

Bluetooth State Machine

- To form or join a piconet, a Bluetooth device must enter the connection state.



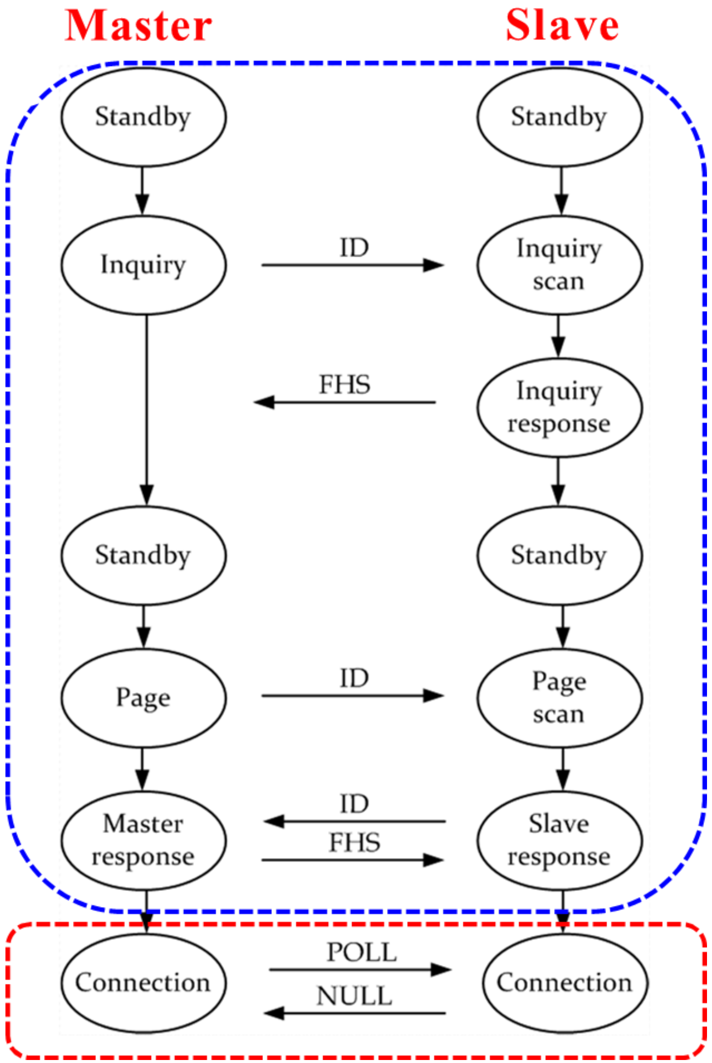
Inquiry & Page States

- Both inquiry and page states are used to help a master to invite slaves to join its piconet.
- However, both master and slave do not know the frequency hopping pattern of each other.
  - Thus, they can send frequency hopping synchronization (FHS) packets to exchange such information.
  - Before entering the connection state, all devices follow the slave's hopping pattern.
  - After entering the connection state, all devices follow the master's hopping pattern.

Detailed Flowchart

Slave’s hopping pattern

Master’s hopping pattern



Four Modes of a Slave

- After entering the connection state, the slave can switch to one of the following modes:
  - Active mode
  - Sniff mode
  - Hold mode
  - Park mode

Active Mode

- Slave actively participates in the piconet by listening, transmitting, and receiving packets.
- Master periodically transmits information to the slave to maintain synchronization.

Sniff Mode

- Slave only wakes up in specific slots, and goes to the reduced-power mode in the rest of slots.
  - This is a low-power mode, where the listening activity of a slave is reduced.
- In this mode, the slave listens the channel only at fixed intervals T_{sniff}, at the offset slot D_{sniff} for N_{sniff} times.
  - These parameters are given by LMP (Link Management Protocol) of the master when it issues the SNIFF command to the slave.

Hold Mode

- Slave goes to the reduced-power mode and temporarily does not support data links (for T_{hold} seconds).
  - However, the slave may still participate in voice exchanges.
- While in the reduced-power mode, the salve can do other things such as scanning, paging, inquiring, or attending another piconet.
- Slave still keeps its active member address (AM_ADDR).

Park Mode (1/2)

- Slave does not participate in the piconet, but it still wants to remain as a member and keep time-synchronized.
  - Thus, the slave gets a parking member address (PM_ADDR), and loses its active address (AM_ADDR).
- This is a very low power mode with very little activity.
  - The slave only stays synchronized to the channel.
- The parked slaves regularly listen for beacon signals at intervals decided by the beacon structure.

Park Mode (2/2)

- A parked slave has to be informed about a transmission in the beacon channel (supported by the master) to keep it in synchronization and send it any information.
  - Any message to be sent to a parked salve must be transmitted over the broadcast channel.
- The park mode allows a master to have more than seven slaves.

Outline

- Introduction
- Bluetooth Protocol Stack
- Piconets & Scatternets
- Bluetooth Communication States
- Bluetooth links, packet format, and security
- Bluetooth HS & Smart

Communication Links

- Bluetooth supports two types of communication links:
- Synchronous connection oriented (SCO)
  - For voice communication
- Asynchronous connection link (ACL)
  - For data communication

SCO Links (1/2)

- SCO link is a point-to-point, full-duplex link between the master and one slave.
  - It provides fixed bandwidth for the slave.
- SCO link is established once by the master, and kept alive until the master releases it.
- Master reserves slots used for SCO links on the channel to preserve time-sensitive information.
  - Slots are spaced by regular intervals.
  - Each piconet can have up to three SCO links.

SCO Links (2/2)

- SCO packets are never retransmitted.
  - Bandwidth-guaranteed, but not error-free-guaranteed.
  - Typically used for voice connections (to guarantee continuity)

ACL Links (1/2)

- ACL link is a point-to-multipoint, momentary link between the master and all slaves.
- ACL can only use slots that are not reserved for SCO links.
  - A slave is allowed to send only when it is addressed in the previous master-initiated slot.
  - However, ACL communication can include a slave that already involves in a SCO link.
- Data retransmission is applicable.
  - Packet-switching style

ACL Links (2/2)

- ACL links can have 1-, 3-, or 5-slots.
  - Data can be sent either unprotected, or protected by the forward error correction (FEC) code.

Type	Data rate(kbps)
DM1	108.8
DH1	172.8
DM3	256.0
DH3	384.0
DM5	286.7
DH5	432.6

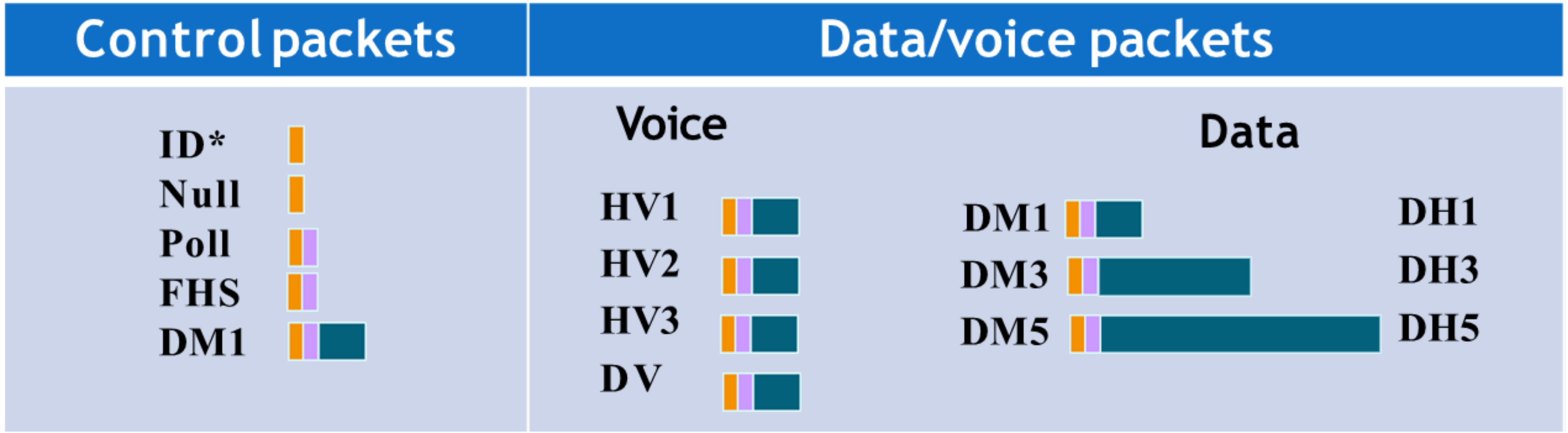
DM: data - medium rate

DH: data - high rate

DMx = x-slot FEC-encoded

DHx = x-slot unprotected

Bluetooth Packet Types



🟧 Access code

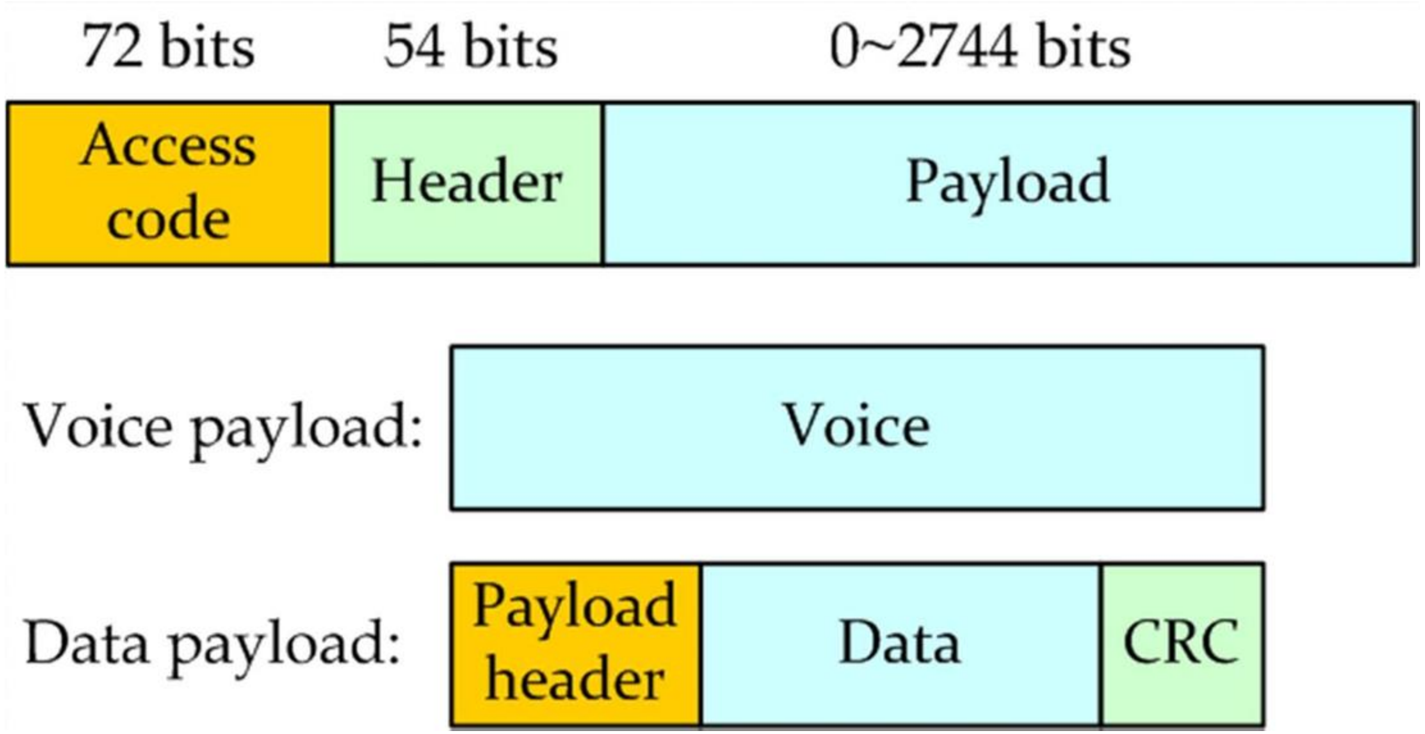
▮ Header

▬ Payload

FHS: Frequency hopping synchronization
DM: Data – medium rate
DH: Data – high rate
HV: High quality voice
DV: Data voice

Bluetooth Packet Structure

- Both voice and data payloads can include optional FEC.

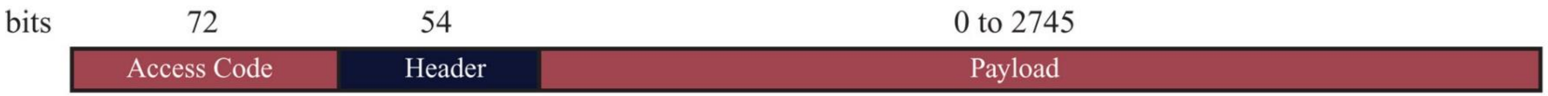


72 bits | 54 bits | 0~2744 bits

Access code | Header | Payload

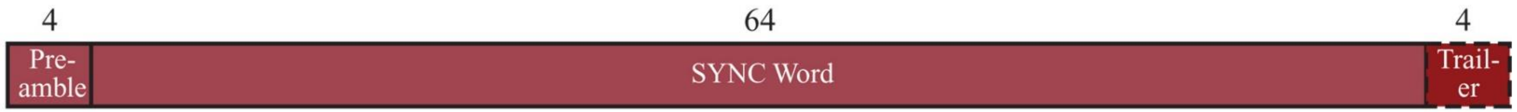
Voice payload: Voice

Data payload: Payload header | Data | CRC



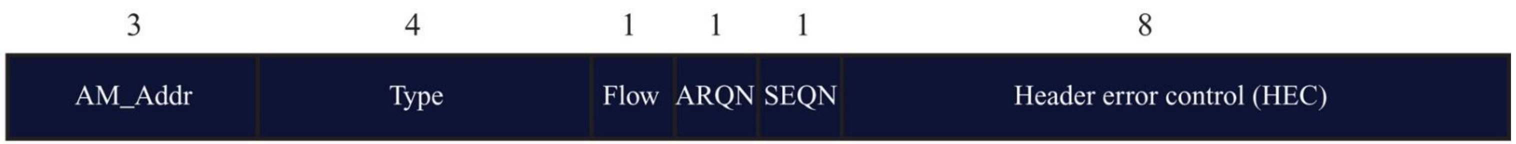
bits	72	54	0 to 2745
	Access Code	Header	Payload

(a) Packet format



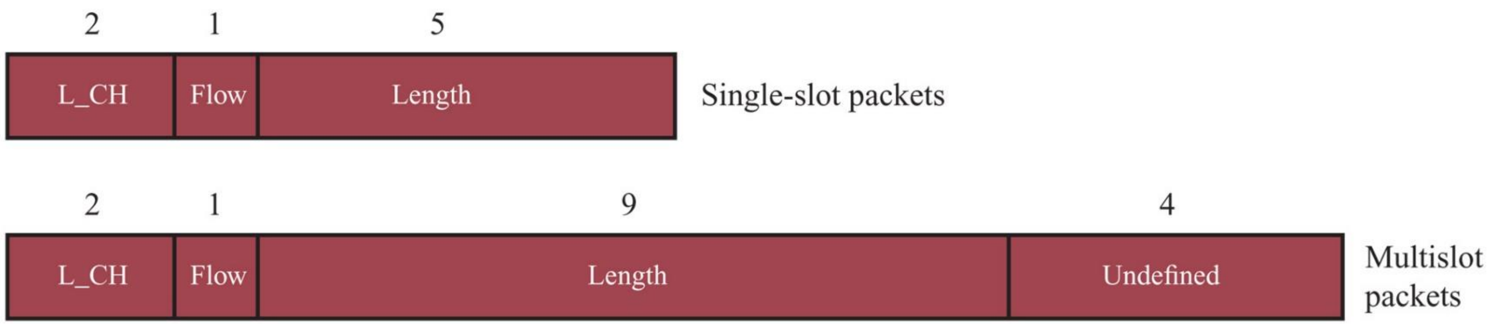
4	64	4
Pre-amble	SYNC Word	Trail-er

(b) Access code format



3	4	1	1	1	8
AM_Addr	Type	Flow	ARQN	SEQN	Header error control (HEC)

(c) Header format (prior to coding)



2	1	5	
L_CH	Flow	Length	Single-slot packets

2	1	9	4	
L_CH	Flow	Length	Undefined	Multislot packets

(d) Data payload header format

Access Code

- Access code is used for timing synchronization, inquiry, and paging.
- Bluetooth access codes:
  - Channel access code (CAC): Identify a piconet.
  - Device access code (DAC): Used for signaling procedures like paging and paging response
  - Inquiry access code (IAC):
    - General IAC is common to all devices.
    - Dedicated IAC is for a dedicated group of Bluetooth devices that share a common characteristic.

Packet Header Fields

- AM_ADDR
  - contains “active mode” address of one of the slaves.
- Type
  - identifies type of packet
- Flow
  - 1-bit flow control
- ARQN
  - 1-bit acknowledgment
- SEQN
  - 1-bit sequential numbering schemes
- Header error control (HEC)
  - 8-bit error detection code

Payload Format

- Payload header
  - L_CH field – identifies logical channel
  - Flow field – used to control flow at L2CAP level
  - Length field – number of bytes of data
- Payload body
  - contains user data
- CRC
  - 16-bit CRC code

Security in Bluetooth

- In Bluetooth, authentication and encryption are provided by the link manager.
- Personal identification number (PIN) is translated into a 128-bit link key for authentication.
- After authentication, the radios will settle on a suitable length encryption key to be used.
- Bluetooth uses PIN codes to establish trusted relationships between devices.
- FHSS also provides a certain degree of security.

Outline

- Introduction
- Bluetooth Protocol Stack
- Piconets & Scatternets
- Bluetooth Communication States
- Bluetooth links, packet format, and security
- Bluetooth HS & Smart

Bluetooth High Speed

- Bluetooth 3.0+HS
- Up to 24 Mbps
- New controller compliant with 2007 version of IEEE 802.11
- Known as Alternative MAC/PHY (AMP)
  - Optional capability
- Bluetooth radio still used for device discovery, association, setup, etc.
- Allows more power efficient Bluetooth modes to be used, except when higher data rates are needed

Bluetooth Smart

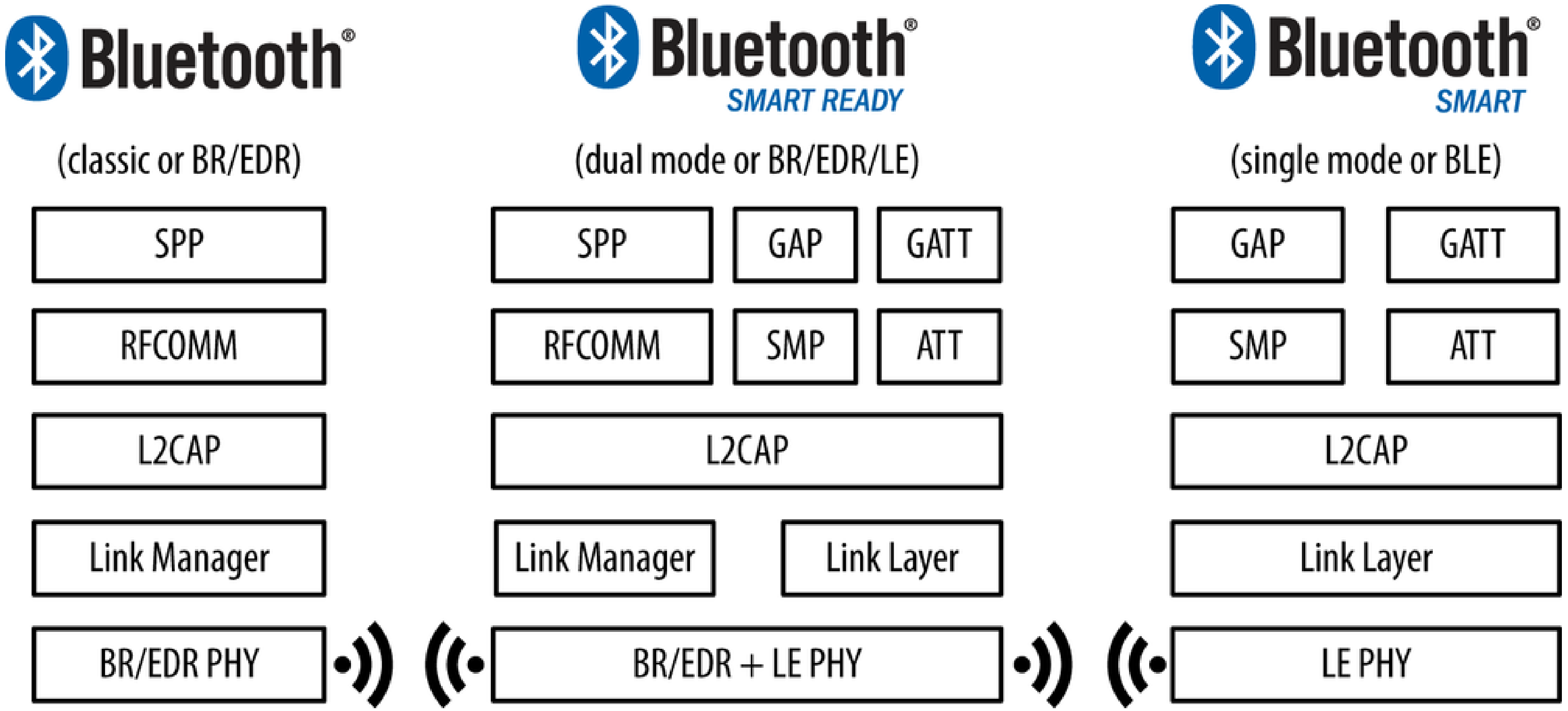
- Bluetooth 4.0
- Previously known as Bluetooth Low Energy
- An intelligent, power-friendly version of Bluetooth
- Can run long periods of time on a single battery
- Also communicates with other Bluetooth-enabled devices
  - Legacy Bluetooth devices or Bluetooth-enabled smartphones
- Possible successful technology for the Internet of Things
  - For example, health monitoring devices can easily integrate with existing smartphones

Bluetooth Smart

- Same 2.4 GHz ISM bands as Bluetooth BR/EDR
  - But uses 40 channels spaced 2 MHz apart instead of 79 channels spaced 1 MHz apart
- Devices can implement a transmitter, a receiver, or both
- Implementation
  - Single-mode Bluetooth Smart functionality
    - Reduced cost chips that can be integrated into compact devices.
  - Dual-mode functionality to also have the Bluetooth BR/EDR capability
- 10 mW output power
- 150 m range in an open field

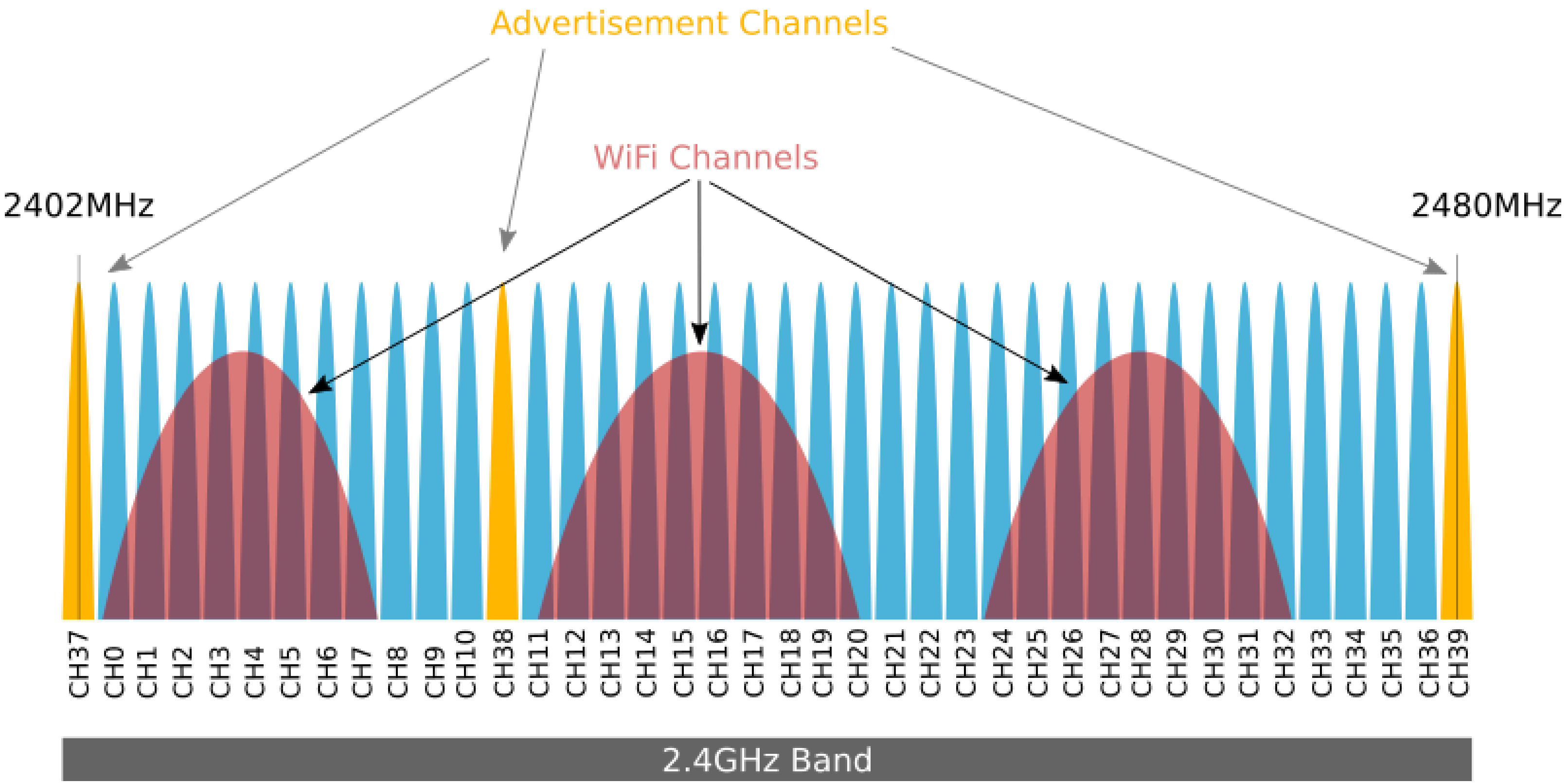
Comparison (1/4)

- Protocol stack



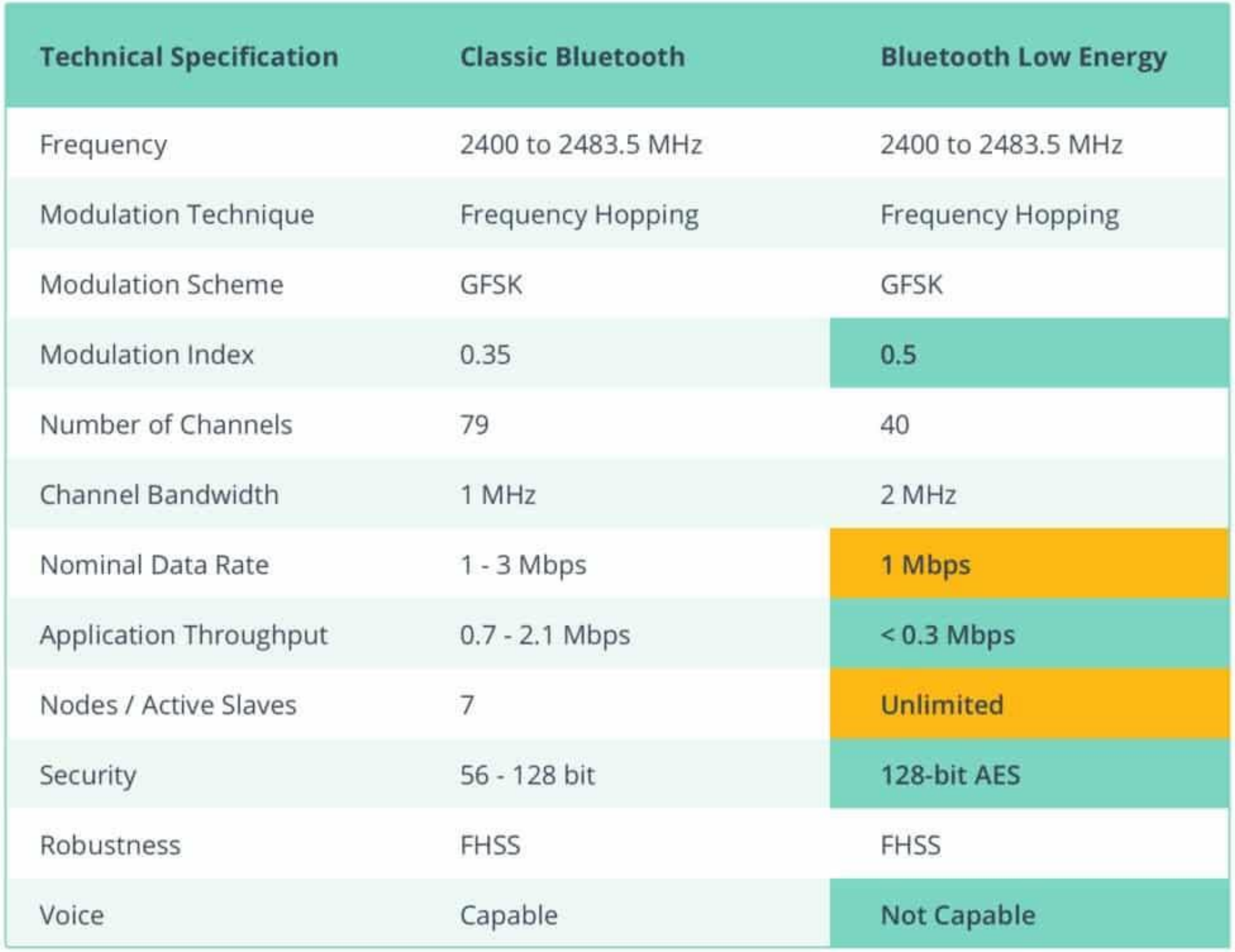
Comparison (2/4)

- BLE Spectrum



Comparison (3/4)

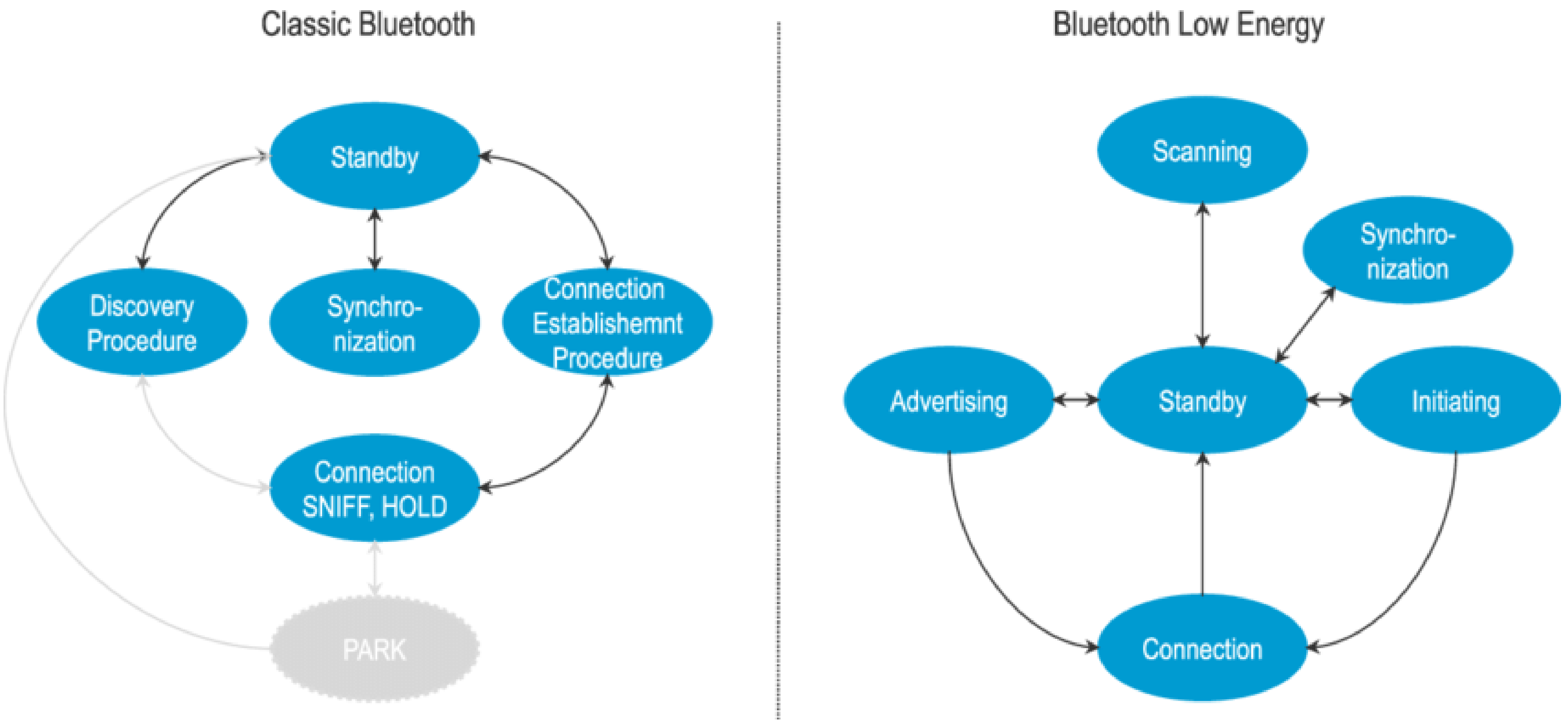
- Specification



Technical Specification	Classic Bluetooth	Bluetooth Low Energy
Frequency	2400 to 2483.5 MHz	2400 to 2483.5 MHz
Modulation Technique	Frequency Hopping	Frequency Hopping
Modulation Scheme	GFSK	GFSK
Modulation Index	0.35	**0.5**
Number of Channels	79	40
Channel Bandwidth	1 MHz	2 MHz
Nominal Data Rate	1 - 3 Mbps	**1 Mbps**
Application Throughput	0.7 - 2.1 Mbps	**< 0.3 Mbps**
Nodes / Active Slaves	7	**Unlimited**
Security	56 - 128 bit	**128-bit AES**
Robustness	FHSS	FHSS
Voice	Capable	**Not Capable**

Comparison (4/4)

- Link state diagram



Summary

- Bluetooth operates on 2.4GHz and provide short-range communication with lower data rates.
- Bluetooth supports both data and voice transmissions.
- Bluetooth stack is composed of application group, middleware protocol group, and transport protocol group.
- Piconet is a basic unit in Bluetooth networks. Multiple overlapping piconets form a scatternet.
- After entering the connection state, a slave can choose to enter active, sniff, hold, and park modes.
- Bluetooth has SCO and ACL links.
- Bluetooth security can be realized by PIN codes and FHSS.