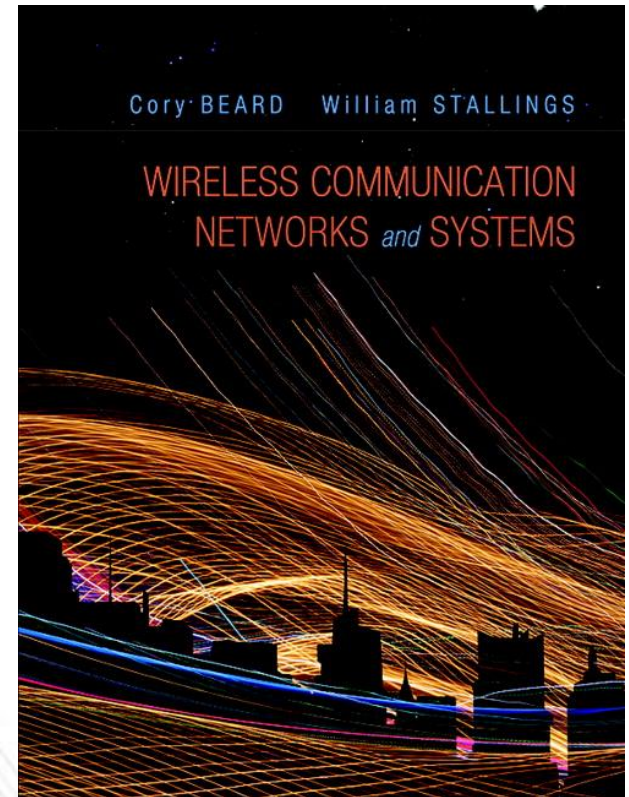


# CHAPTER 12

# BLUETOOTH AND

# IEEE 802.15



## Wireless Communication Networks and Systems

1<sup>st</sup> edition

**Cory Beard, William Stallings**

© 2016 Pearson Higher

Education, Inc.

These slides are made available to faculty in PowerPoint form. Slides can be freely added, modified, and deleted to suit student needs. They represent substantial work on the part of the authors; therefore, we request the following.

If these slides are used in a class setting or posted on an internal or external www site, please mention the source textbook and note our copyright of this material.

All material copyright 2016

Cory Beard and William Stallings, All Rights Reserved

# IEEE 802.15

- **Wireless Personal Area Networks**
  - Short-range communication
  - Low-cost, low-energy to provide long battery life
- **Several standards have been provided**
- **We focus on 802.15 technologies**
  - Other viable WPAN alternatives exist

# INTERNET OF THINGS

- Key application area for short-range communications
- Future Internet
  - Large numbers of wirelessly connected objects
  - Interactions between the physical world and computing, digital content, analysis, and services.
  - Called the Internet of Things
    - And many other “Internet of ...” titles
  - Useful for health and fitness, healthcare, home monitoring and automation, energy savings, farming, environmental monitoring, security, surveillance, education, and many others.
- Machine-to-machine communications (MTM, M2M, D2D, etc.), also machine-type communications (MTC)
  - Devices working together for data analysis and automated control

# BLUETOOTH

- Universal short-range wireless capability
- Uses 2.4-GHz band
- Available globally for unlicensed users
- Devices within 10 m can share up to 2.1 Mbps or 24 Mbps of capacity
- Supports open-ended list of applications
  - Data, audio, graphics, video
- Started as IEEE 802.15.1
  - New standards come from the Bluetooth Special Interest Group (Bluetooth SIG)
    - Industry consortium
  - Bluetooth 2.0, 2.1, 3.0, and 4.0

# 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

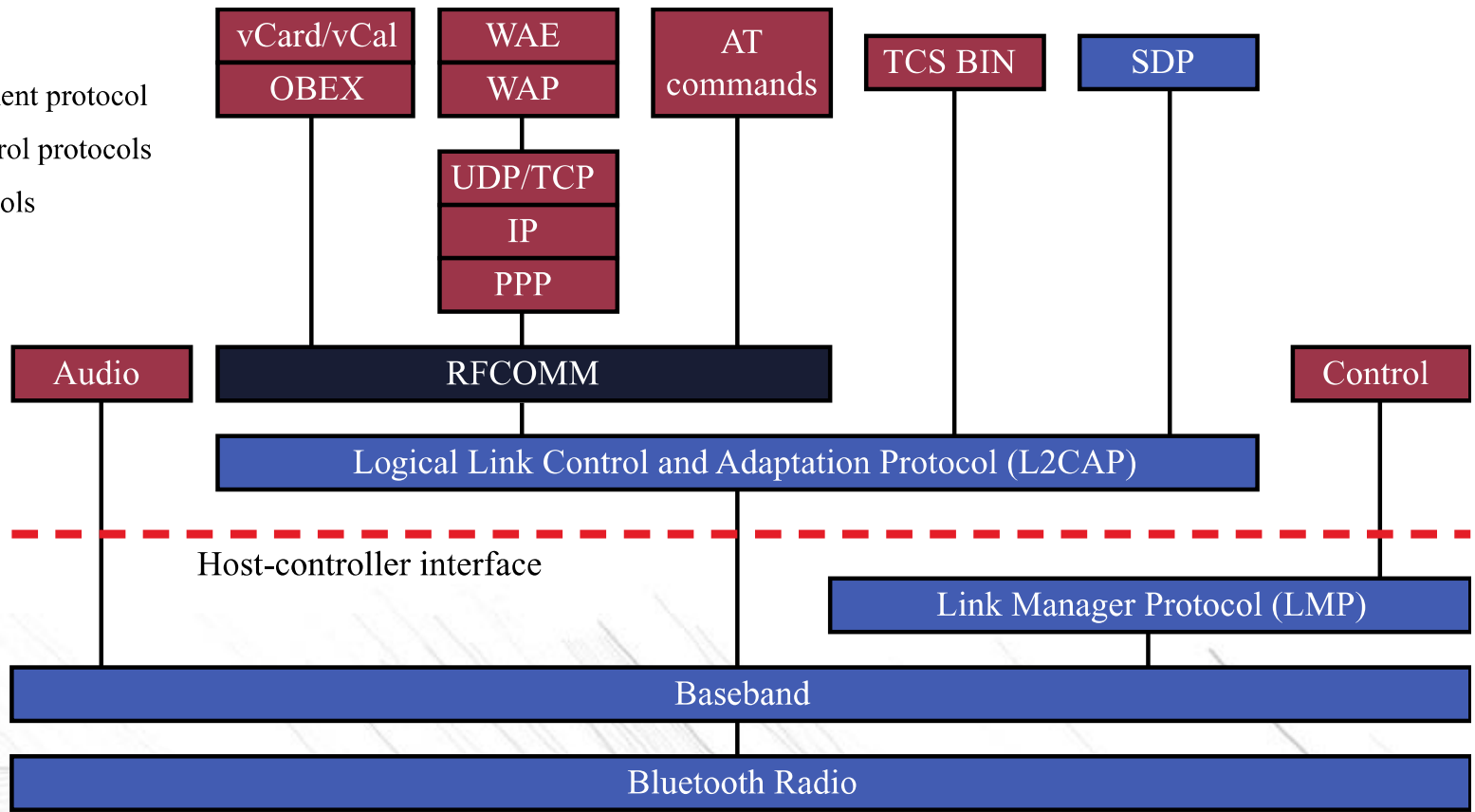
# TOP USES OF BLUETOOTH

- 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 STANDARDS DOCUMENTS

- Core specifications
  - Details of various layers of Bluetooth protocol architecture
- Profile specifications
  - Use of Bluetooth technology to support various applications
- We first focus on
  - 2.1 Basic/Enhanced Data Rate (BR/EDR)
- Later standards
  - 3.0 Alternative MAC/PHY (AMP)
  - 4.0 Bluetooth Smart (Bluetooth Low Energy)

- = Core protocols
- = Cable replacement protocol
- = Telephony control protocols
- = Adopted protocols



- |        |                                     |         |  |
|--------|-------------------------------------|---------|--|
| 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     |         |  |

## 12.1 BLUETOOTH PROTOCOL STACK





# PROTOCOL ARCHITECTURE

- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
  - Baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)

# PROTOCOL ARCHITECTURE

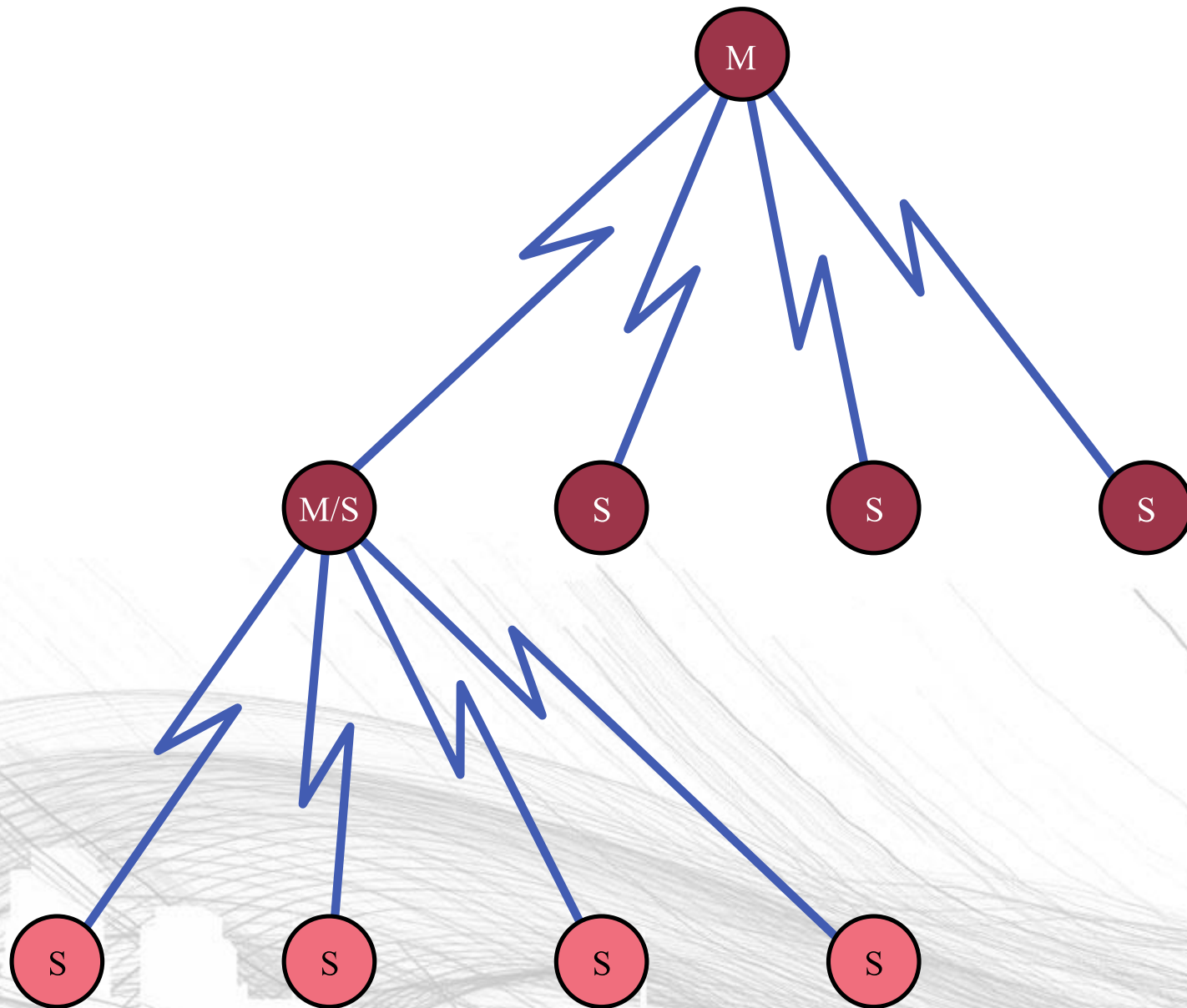
- Cable replacement protocol
  - RFCOMM
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols
  - PPP
  - TCP/UDP/IP
  - OBEX
  - WAE/WAP

# 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

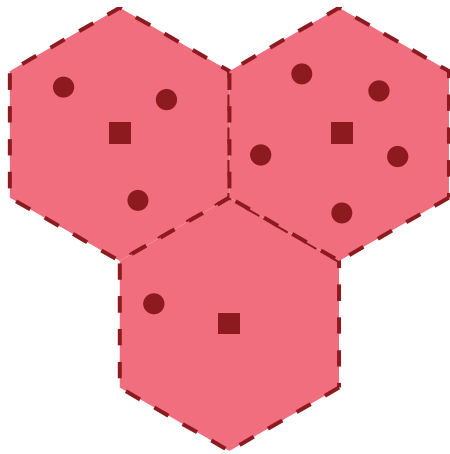
# PICONETS AND SCATTERNETS

- Piconet
  - Basic unit of Bluetooth networking
  - Master and one to seven slave devices
  - Master determines channel and phase
- Scatternet
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth

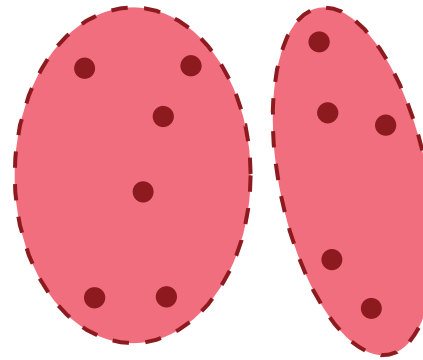


## 12.2 MASTER/SLAVE RELATIONSHIPS

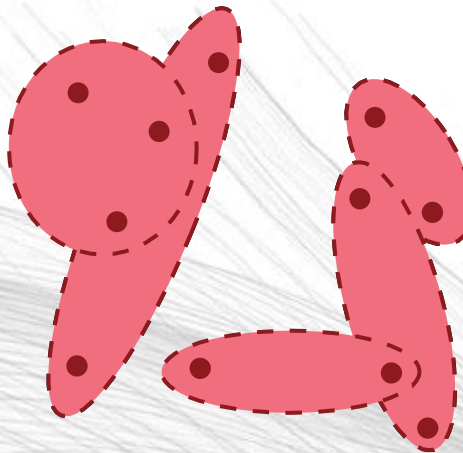




**(a) Cellular system (squares represent stationary base stations)**



**(b) Conventional ad hoc systems**



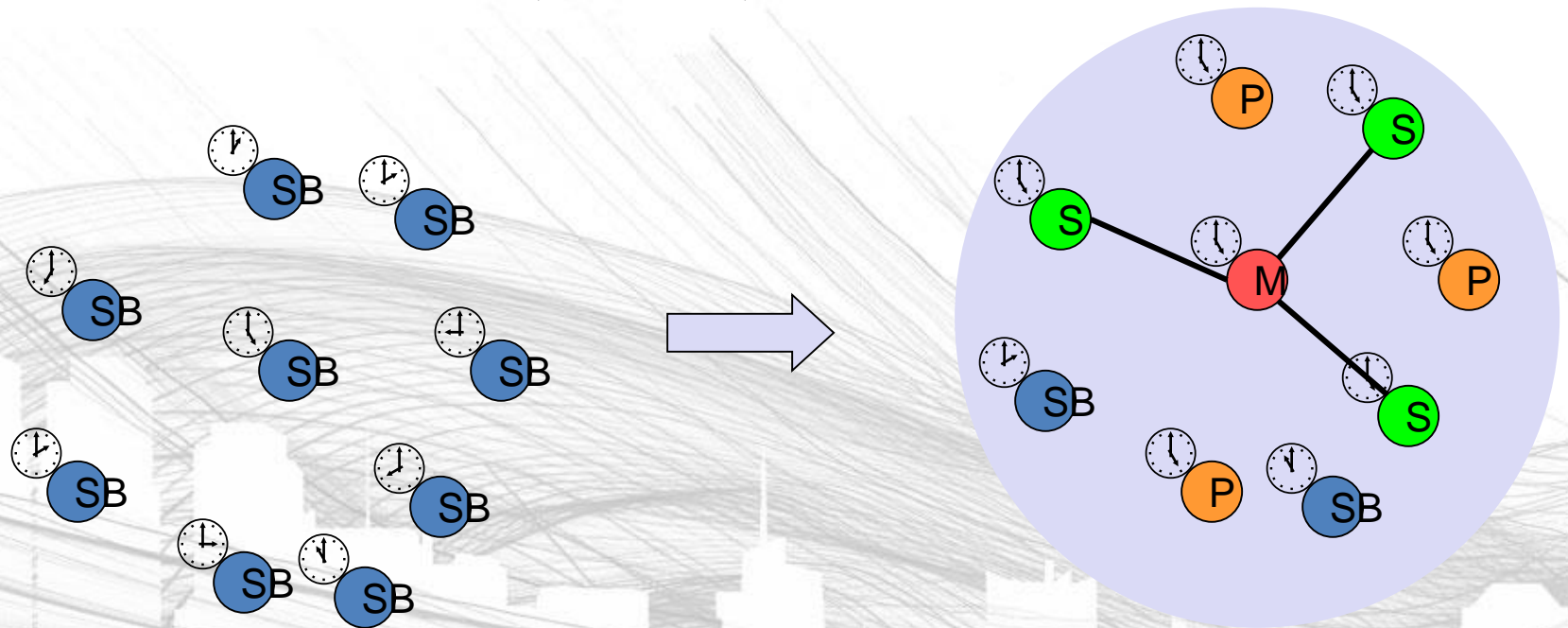
**(c) Scatternets**

## **12.3 WIRELESS NETWORK CONFIGURATIONS**



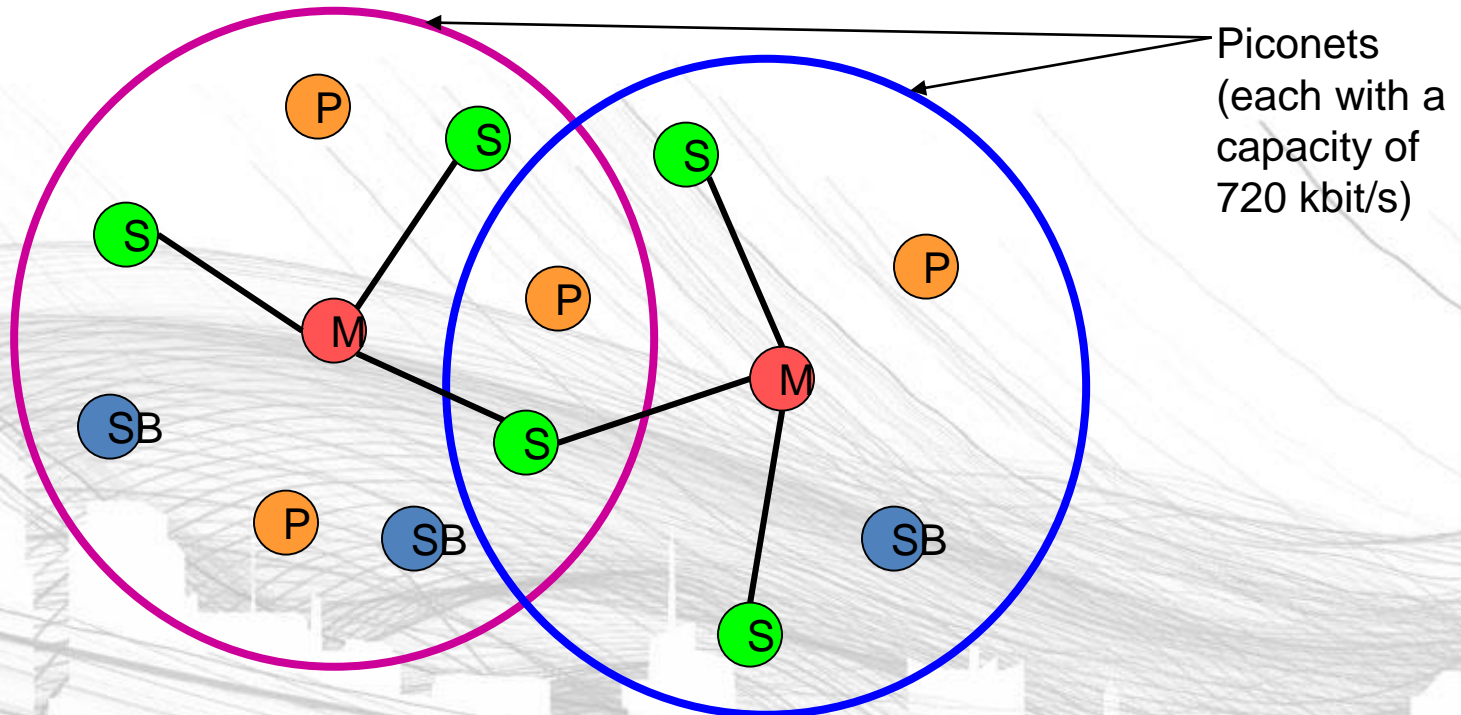
# FORMING A PICONET

- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)



# SCATTERNET

- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jumping back and forth between the piconets





# RADIO SPECIFICATION

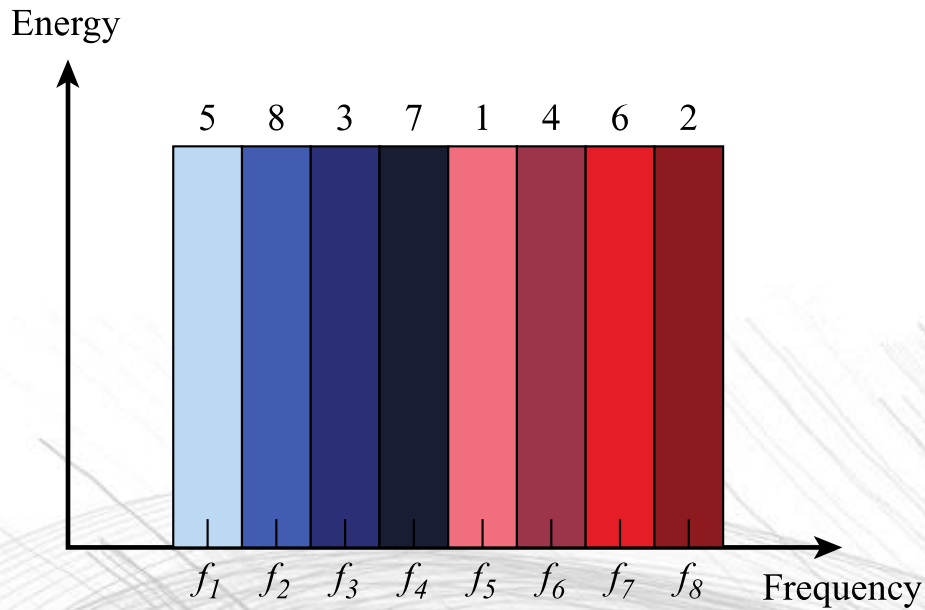
- Classes of transmitters
  - Class 1: Outputs 100 mW for maximum range
    - Power control mandatory
    - Provides greatest distance
  - Class 2: Outputs 2.4 mW at maximum
    - Power control optional
  - Class 3: Nominal output is 1 mW
    - Lowest power

# FREQUENCY HOPPING IN BLUETOOTH

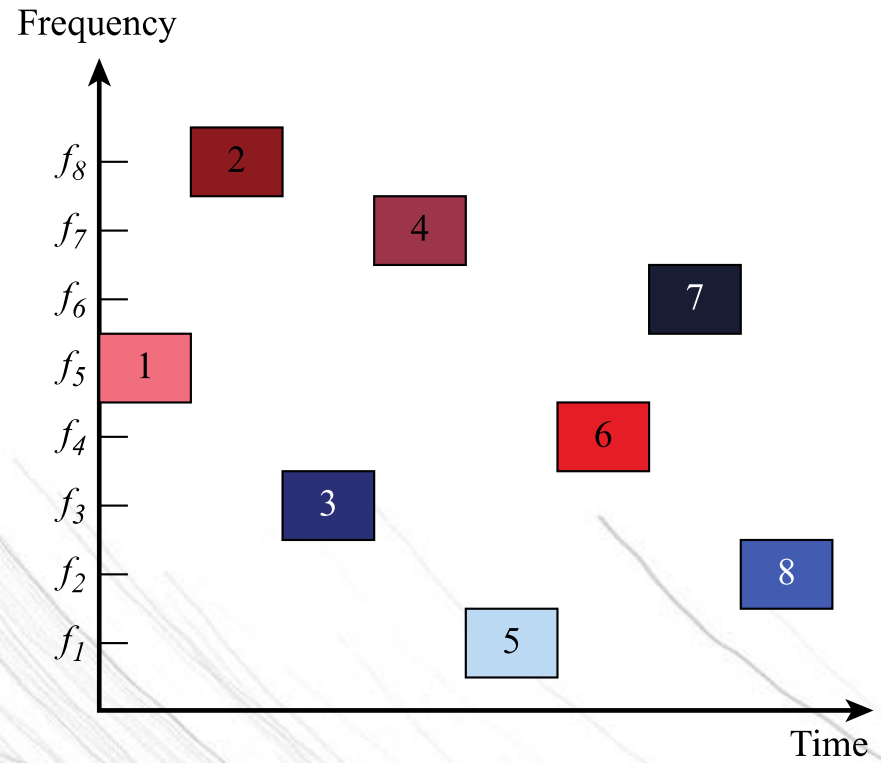
- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets

# FREQUENCY HOPPING

- Total bandwidth divided into 1MHz physical channels
- FH occurs by jumping from one channel to another in pseudorandom sequence
- Hopping sequence shared with all devices on piconet
- Piconet access:
  - Bluetooth devices use time division duplex (TDD)
  - Access technique is TDMA
  - FH-TDD-TDMA



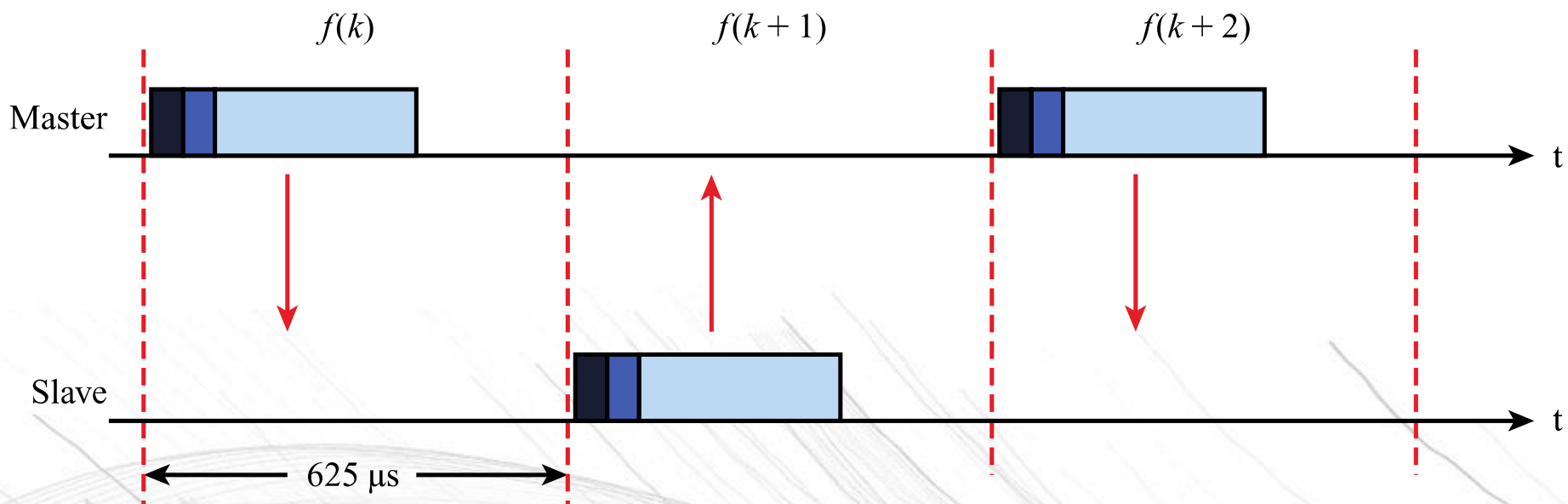
(a) Channel assignment



(b) Channel use

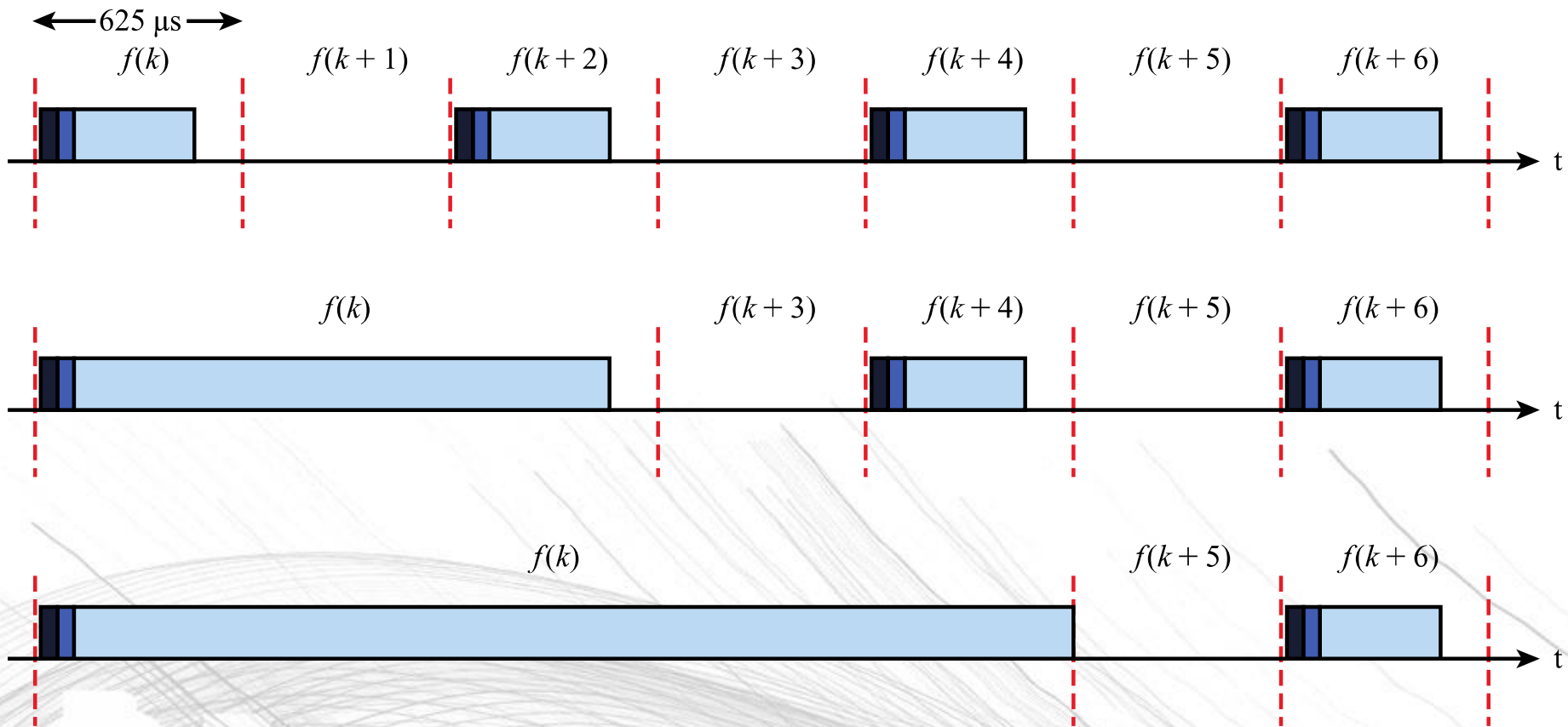
## 9.2 FREQUENCY HOPPING EXAMPLE





## 12.4 FREQUENCY-HOP TIME-DIVISION DUPLEX





## 12.5 EXAMPLES OF MULTISLOT PACKETS

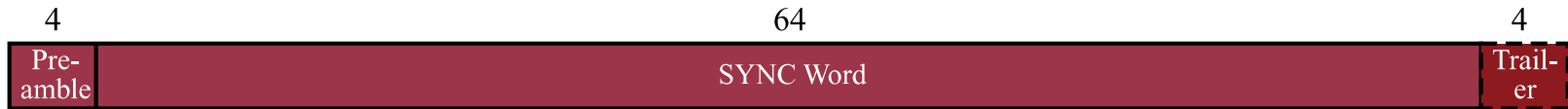


# PHYSICAL LINKS BETWEEN MASTER AND SLAVE

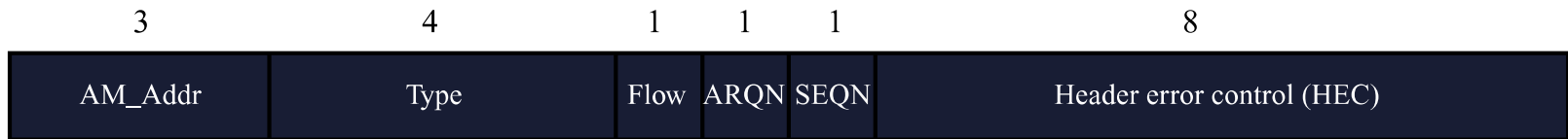
- Synchronous connection oriented (SCO)
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
- Asynchronous connectionless (ACL)
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist
- Extended Synchronous connection oriented (eSCO)
  - Reserves slots just like SCO
  - But these can be asymmetric
  - Retransmissions are supported



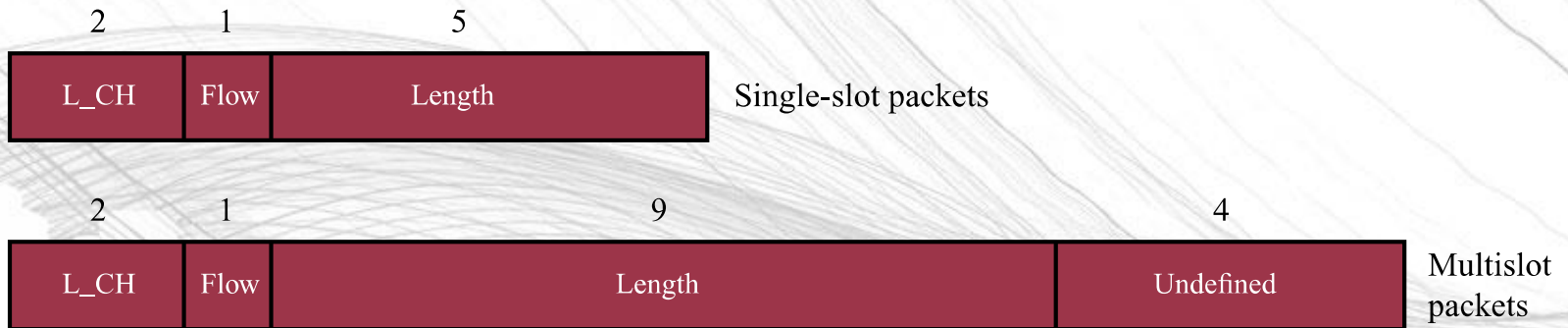
**(a) Packet format**



**(b) Access code format**



**(c) Header format (prior to coding)**



**(d) Data payload header format**

## 12.6 BLUETOOTH BASEBAND FORMATS



# BLUETOOTH PACKET FIELDS

- Access code – used for timing synchronization, offset compensation, paging, and inquiry
- Header – used to identify packet type and carry protocol control information
- Payload – contains user voice or data and payload header, if present

# TYPES OF ACCESS CODES

- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – used for paging and subsequent responses
- Inquiry access code (IAC) – used for inquiry purposes

# 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

# ERROR CORRECTION SCHEMES

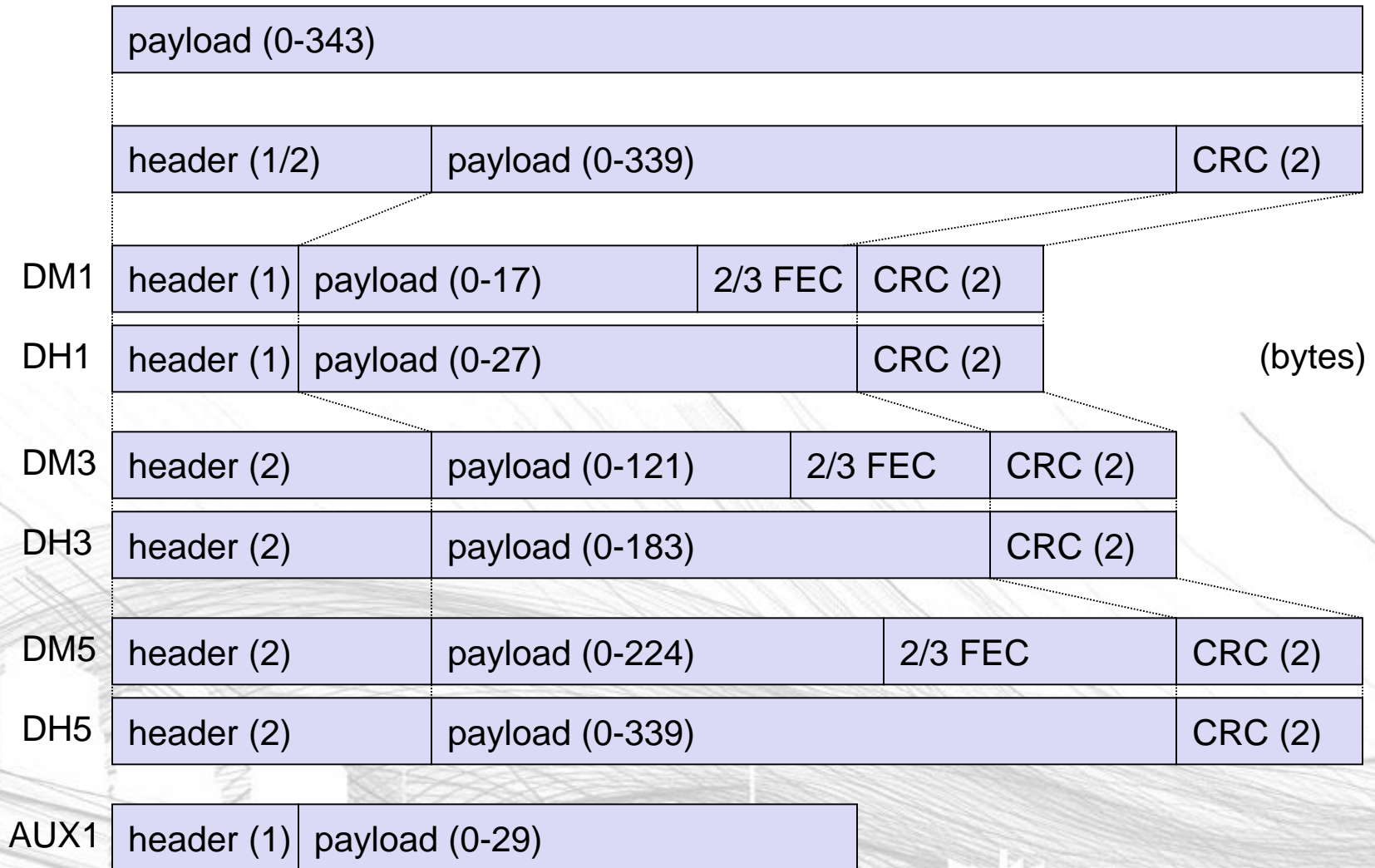
- 1/3 rate FEC (forward error correction)
  - Used on 18-bit packet header, voice field in HV1 packet
- 2/3 rate FEC
  - Used in DM packets, data fields of DV packet, FHS packet and HV2 packet
- ARQ
  - Used with DM and DH packets

# SCO PAYLOAD TYPES

	payload (30)				
HV1	audio (10)	FEC (20)			
HV2	audio (20)		FEC (10)		
HV3	audio (30)				
DV	audio (10)	header (1)	payload (0-9)	2/3 FEC	CRC (2)

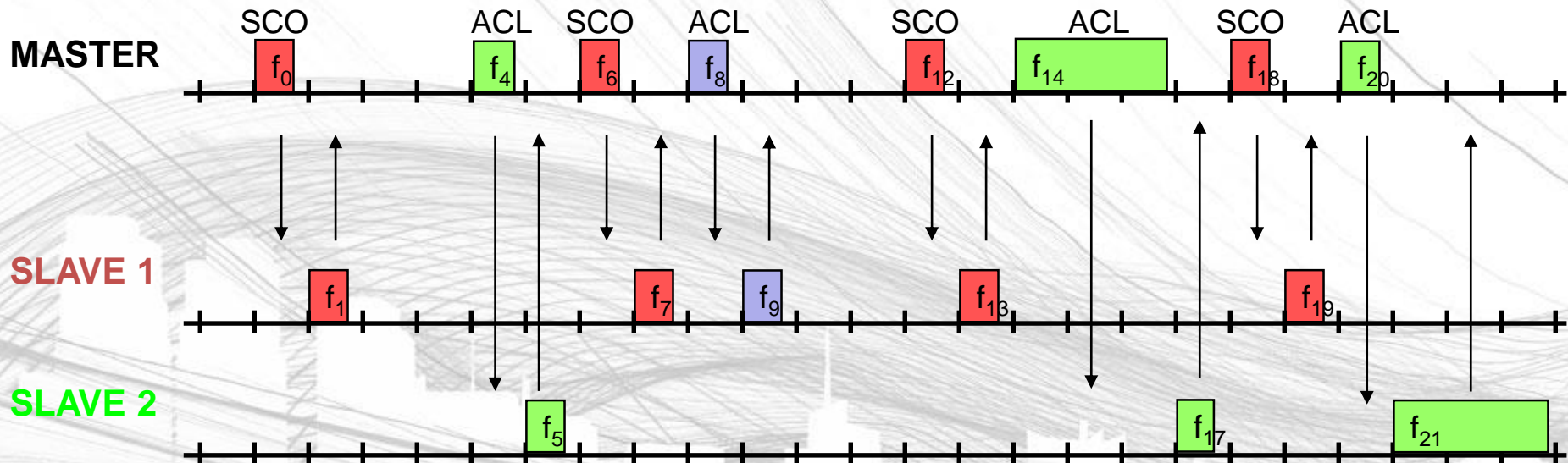
(bytes)

# ACL PAYLOAD TYPES



# BASEBAND LINK TYPES

- Polling-based TDD packet transmission
  - 625 $\mu$ s slots, master polls slaves
- SCO (Synchronous Connection Oriented) – Voice
  - Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point
- ACL (Asynchronous ConnectionLess) – Data
  - Variable packet size (1, 3, 5 slots), asymmetric bandwidth, point-to-multipoint

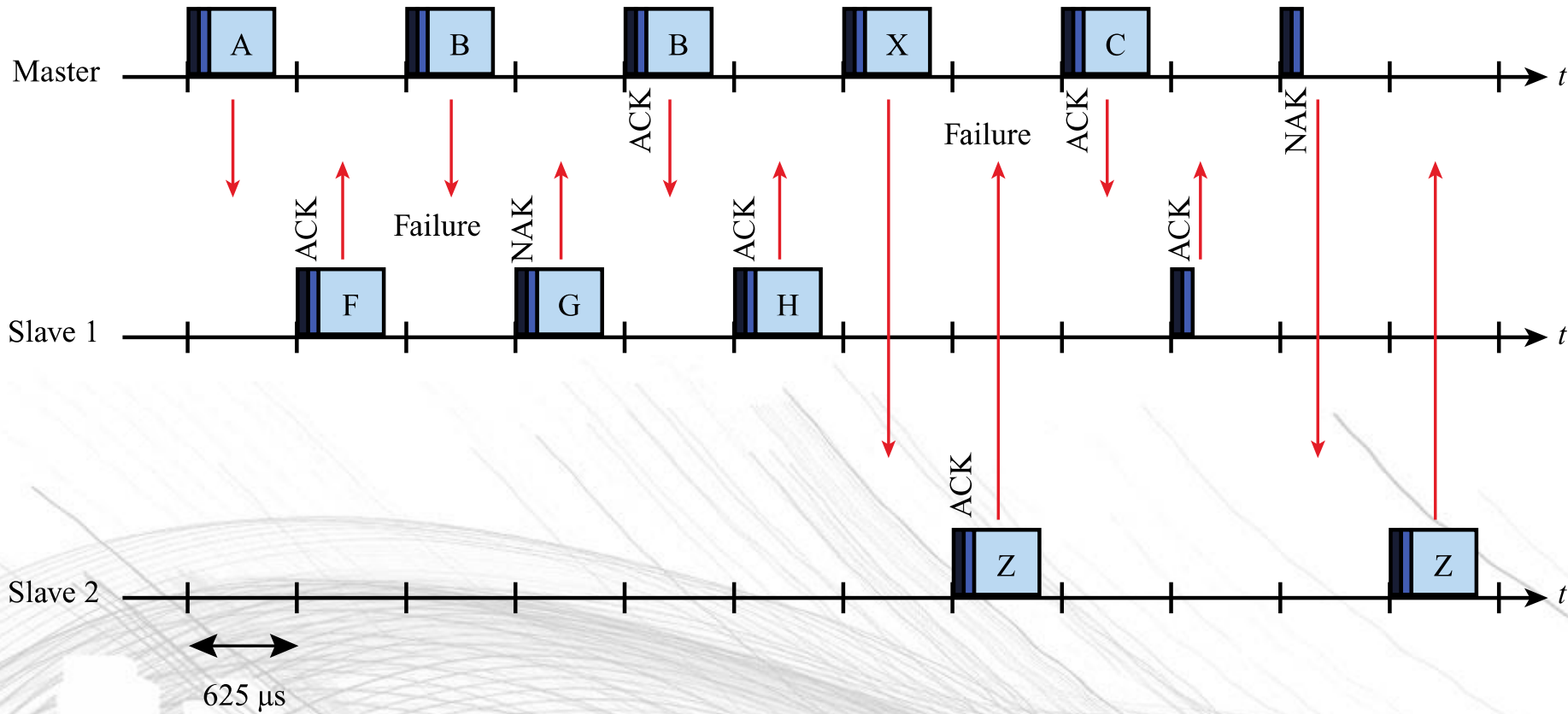




# ARQ SCHEME ELEMENTS

- Error detection – destination detects errors, discards packets
- Positive acknowledgment – destination returns positive acknowledgment
- Retransmission after timeout – source retransmits if packet unacknowledged
- Negative acknowledgment and retransmission – destination returns negative acknowledgement for packets with errors, source retransmits

$f(k+1)$   $f(k+2)$   $f(k+3)$   $f(k+4)$   $f(k+5)$   $f(k+6)$   $f(k+7)$   $f(k+8)$   $f(k+9)$   $f(k+10)$   $f(k+11)$   $f(k+12)$



## 12.7 AN EXAMPLE OF RETRANSMISSION OPERATION



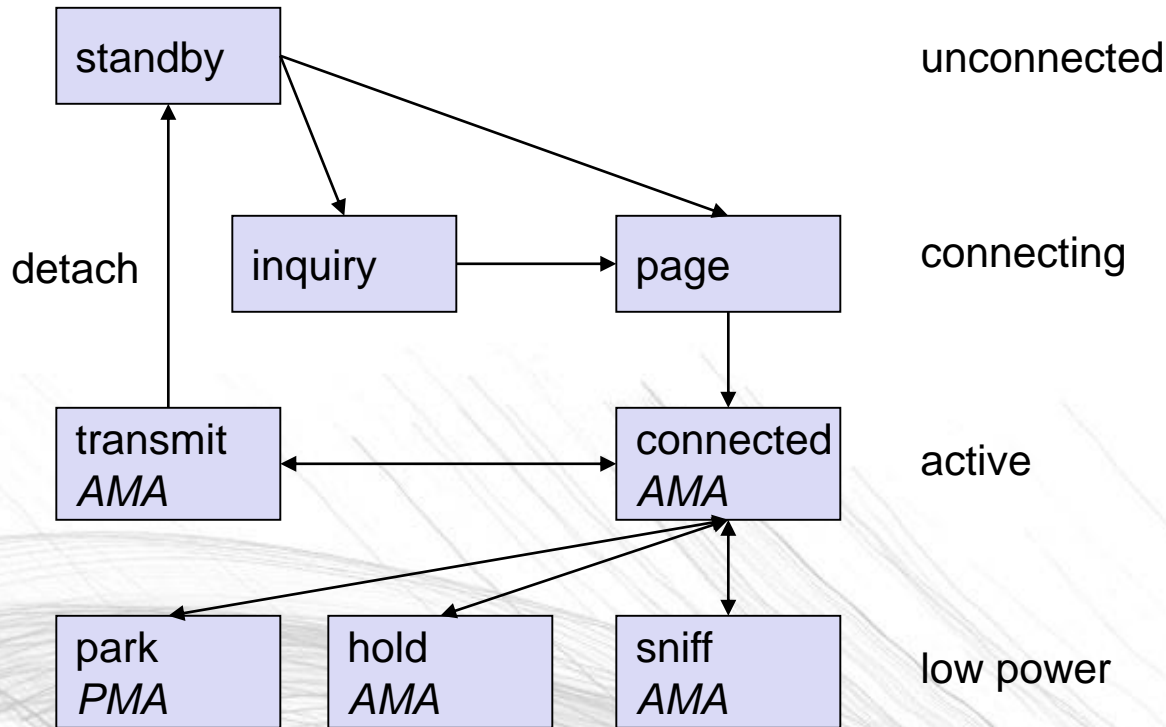
# LOGICAL CHANNELS

- Link control (LC)
- Link manager (LM)
- User asynchronous (UA)
- User isochronous (UI)
- User synchronous (US)
- User extended synchronous (UeS)

# LINK MANAGER

- Manages various aspects of the radio link between a master and a slave
- Involves the exchange LMP PDUs (protocol data units)
- Procedures defined for LMP are grouped into 24 functional areas, which include
  - Authentication
  - Pairing
  - Encryption
  - Clock offset request
  - Switch master/slave
  - Name request
  - Hold or park or sniff mode

# BASEBAND STATES OF A BLUETOOTH DEVICE



Standby: do nothing

Inquire: search for other devices

Page: connect to a specific device

Connected: participate in a piconet

Park: release AMA, get PMA

Sniff: listen periodically, not each slot

Hold: stop ACL, SCO still possible, possibly participate in another piconet

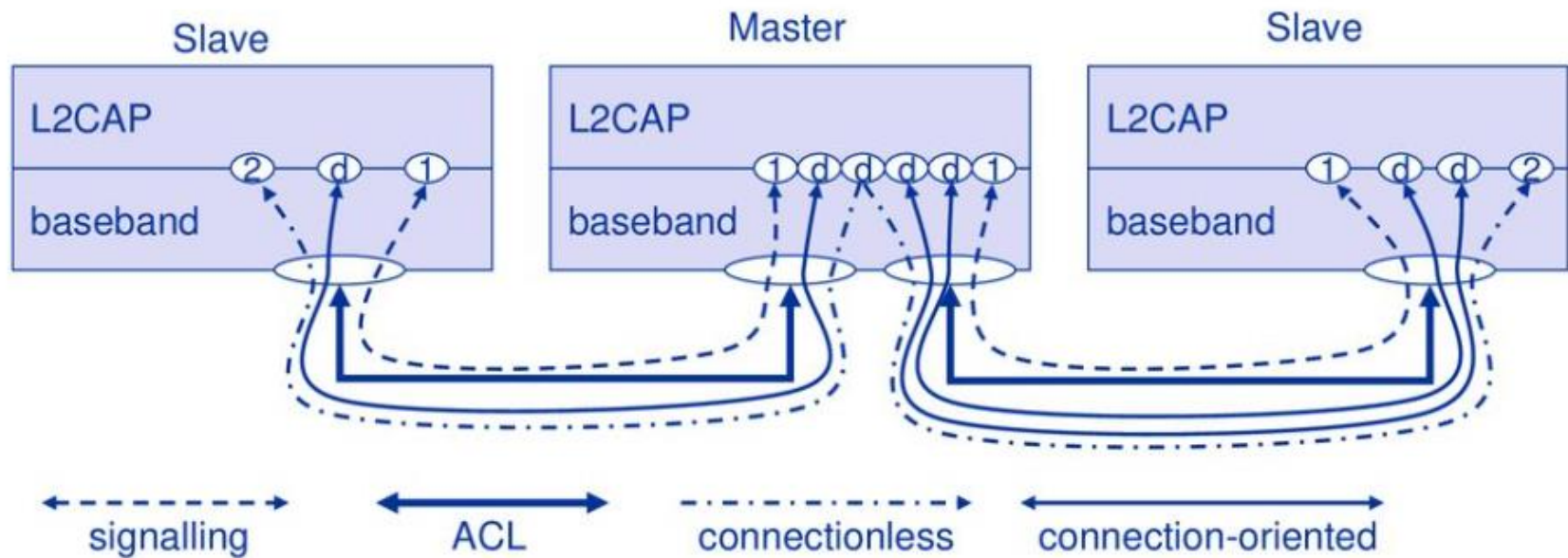
# LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL (L2CAP)

- Provides a link-layer protocol between entities with a number of services
- Relies on lower layer for flow and error control
- Makes use of ACL links, does not support SCO links
- Provides two alternative services to upper-layer protocols
  - Connectionless service
  - Connection-mode service

# L2CAP LOGICAL CHANNELS

- Connectionless
  - Supports connectionless service
  - Each channel is unidirectional
  - Used from master to multiple slaves
- Connection-oriented
  - Supports connection-oriented service
  - Each channel is bidirectional
- Signaling
  - Provides for exchange of signaling messages between L2CAP entities

# L2CAP LOGICAL CHANNELS



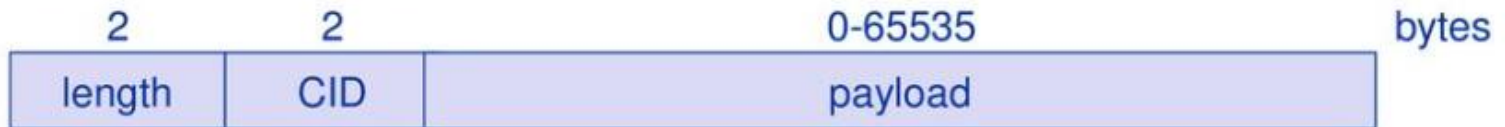


# L2CAP PACKET FORMATS

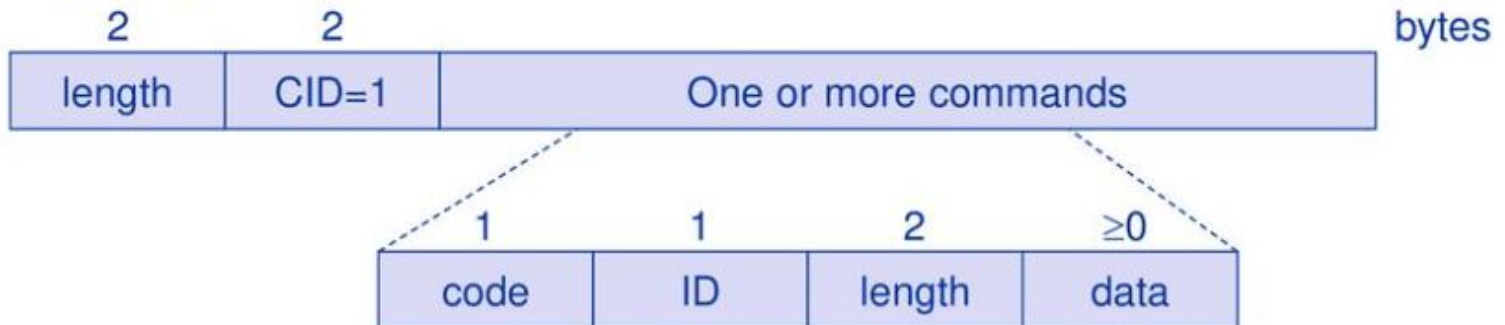
## Connectionless PDU



## Connection-oriented PDU



## Signaling command PDU



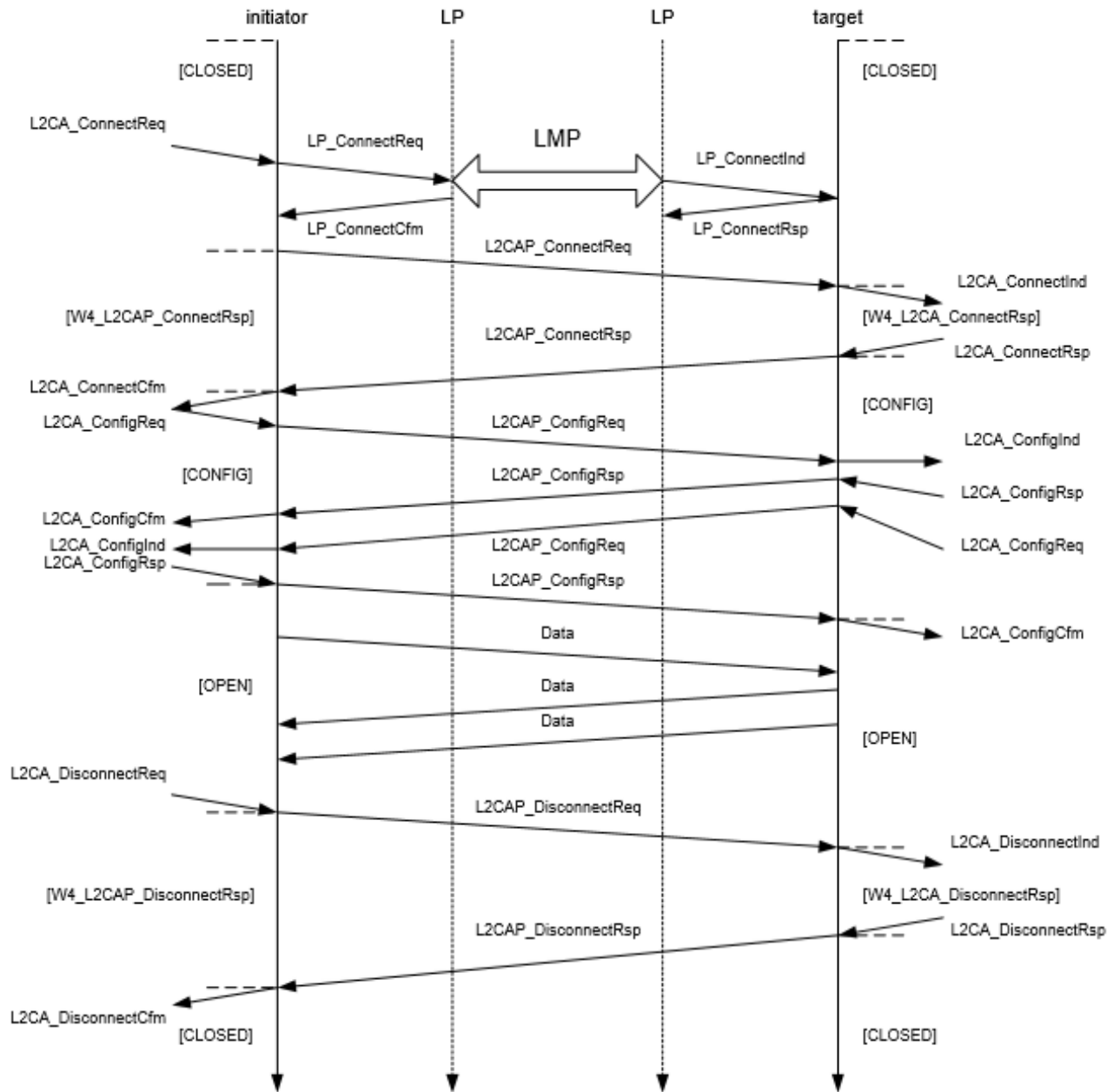
CID = Channel Identifier

PSM = Protocol/Service Multiplexer

# L2CAP SIGNALLING COMMAND CODES

<b>Code</b>	<b>Description</b>	<b>Parameters</b>
0x01	Command reject	Reason
0x02	Connection request	PSM, Source CID
0x03	Connection response	Destination CID, Source CID, Result, Status
0x04	Configure request	Destination CID, Flags, Options
0x05	Configure response	Source CID, Flags, Result, Options
0x06	Disconnection request	Destination CID, Source CID
0x07	Disconnection response	Destination CID, Source CID
0x08	Echo request	Data (optional)
0x09	Echo response	Data (optional)
0x0A	Information request	InfoType
0x0B	Information response	InfoType, Result, Data (optional)

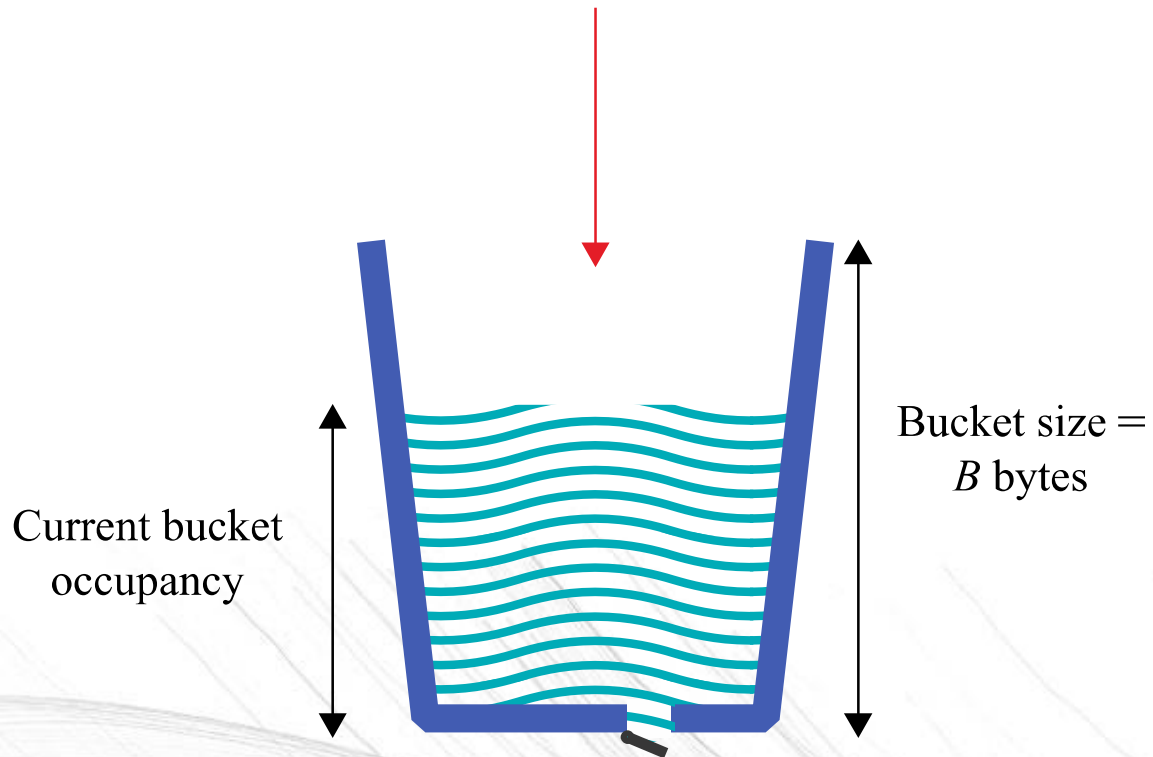
# L2CAP SIGNALLING



# FLOW SPECIFICATION PARAMETERS

- Service type
- Token rate (bytes/second)
- Token bucket size (bytes)
- Peak bandwidth (bytes/second)
- Latency (microseconds)
- Delay variation (microseconds)

Token rate =  
 $R$  bytes per second



Arriving  
data



Departing  
data



## 12.8 TOKEN BUCKET SCHEME



# 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

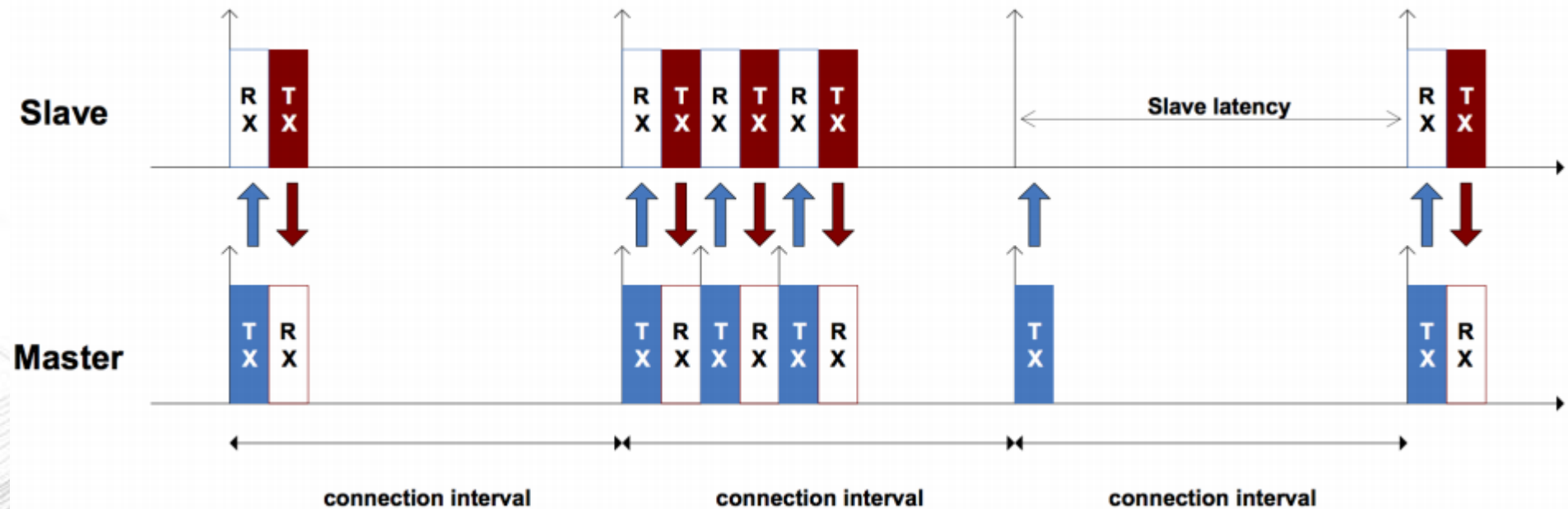
- Bluetooth 4.0
- Previously known as Bluetooth Low Energy
- An intelligent, power-friendly version of Bluetooth
- Can run long periods of time on a single battery
  - Or scavenge for energy
- Also communicates with other Bluetooth-enabled devices
  - Legacy Bluetooth devices or Bluetooth-enabled smartphones
  - Great feature
- 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



# BLUETOOTH SMART: MASTER/SLAVE CONNECTIONS



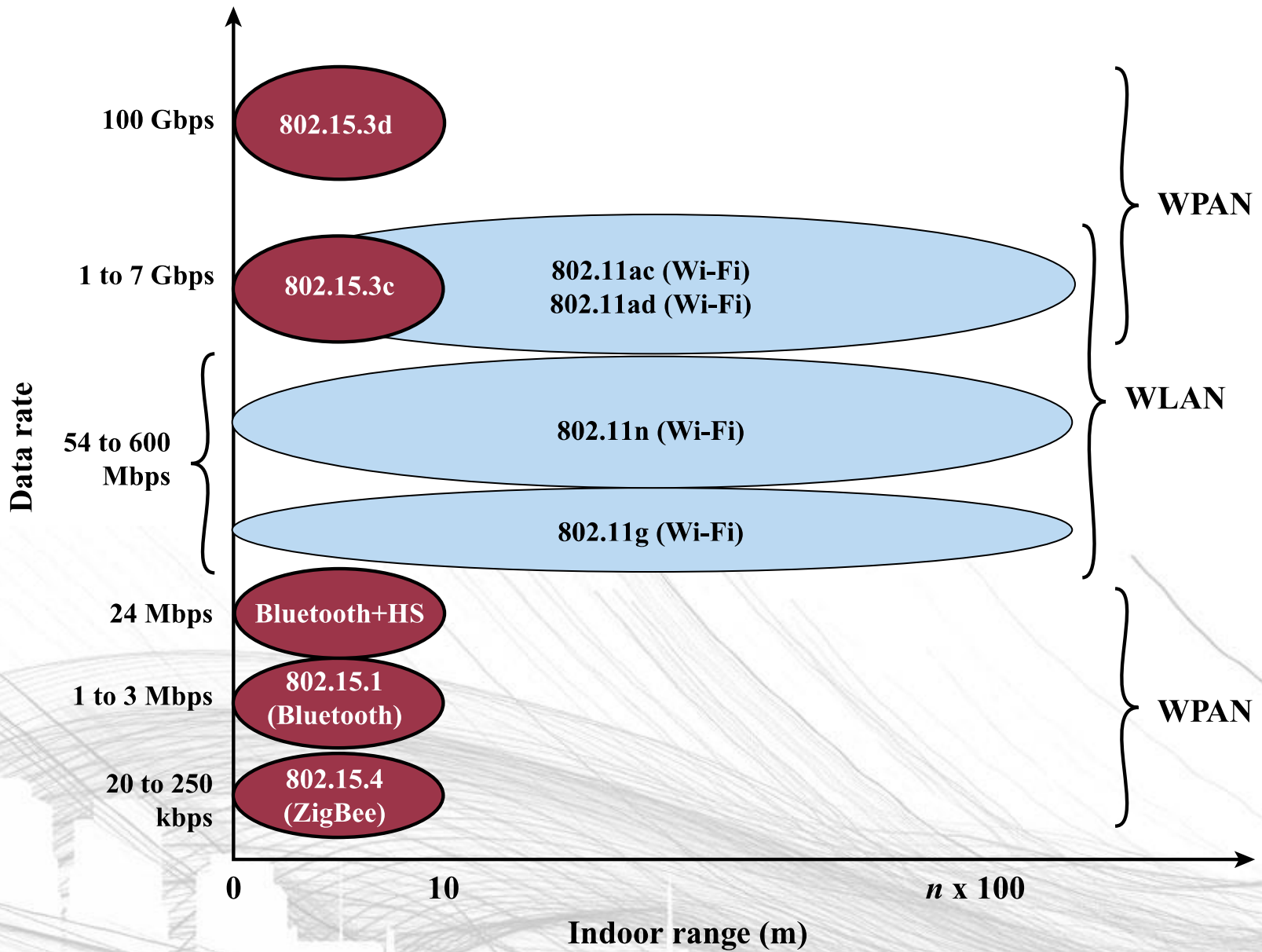
# IEEE 802.15

- After 802.15.1, work went two directions
- 802.15.3
  - Higher data rates than 802.15.1
  - But still low cost, low power compared to 802.11
- 802.15.4
  - Very low cost, very low power compared to 802.15.1
- Figure 12.9 shows different options
- Figure 12.10 shows relative distances and rates

## Logical link control (LLC)

<p><b>802.15.1 Bluetooth MAC</b></p>	<p><b>802.15.3 MAC</b></p>		<p><b>802.15.4, 802.15.4e MAC</b></p>
<p><b>802.15.1 2.4 GHz 1, 2, or 3 Mbps 24 Mbps HS</b></p>	<p><b>802.15.3c 60 GHz 1 to 6 Gbps</b></p>	<p><b>802.15.3d 60 GHz 100 Gbps</b></p>	<p><b>802.15.4, 802.15.4a 868/915 MHz, 2.4 GHz DSSS: 20, 40, 100, 250 kbps UWB: 110 kbps to 27 Mbps CSS: 250 kbps, 1 Mbps</b></p>

## 12.9 IEEE 802.15 PROTOCOL ARCHITECTURE



## 12.10 WIRELESS LOCAL NETWORKS

# IEEE 802.15.3

- High data rate WPANs
  - Digital cameras, speakers, video, music
- Piconet coordinator (PNC)
  - Sends beacons to devices to connect to the network
  - Uses superframes like 802.11
  - QoS based on TDMA
  - Controls time resources but does not exchange data
- 802.15.3c
  - Latest standard
  - Uses 60 GHz band, with same benefits as 802.11ad
  - Single-carrier and OFDM PHY modes

# IEEE 802.15.4

- Low data rate, low complexity
  - Competitor to Bluetooth Smart
- PHY options in 802.15.4 and 802.15.4a
  - 868/915 MHz for 20, 40, 100, and 250 kbps
  - 2.4 GHz for 250 kbps
  - Ultrawideband (UWB)
    - Uses very short pulses with wide bandwidth
      - Low energy density for low interference with others
    - 851 kbps and optionally 110 kbps, 6.81 Mbps, or 27.234 Mbps
  - 2.4 GHz chirp spread spectrum for 1 Mbps and optionally 250 kbps
    - Sinusoidal signals that change frequency with time

# IEEE 802.15.4

- Many other creative and practical activities
- IEEE 802.15.4f – Active Radio Frequency Identification Tags (RFIDs)
  - Attached to an asset or person with a unique identification
  - An Active RFID tag must employ some source of power
- IEEE 802.15.4g – Smart Utility Networks (SUN)
  - Facilitates very large scale process control applications such as the utility smart-grid network
- IEEE 802.15.4j – Medical Body Area Networks
- IEEE 802.15.4k – Low Energy Critical Infrastructure Networks (LECI)
  - To facilitate point to multi-thousands of points communications for critical infrastructure monitoring devices with multi-year battery life.
- IEEE 802.15.4p – Positive Train Control
  - Sensor, control and information transfer applications for rail transit

# OTHER IEEE 802.15 STANDARDS

- 802.15.2 – Coexistence between 802.11 and 802.15
- 802.15.5 – Mesh networks
  - Multihop networking
- 802.15.6 – Body area networks
- 802.15.7 – Visible light communication

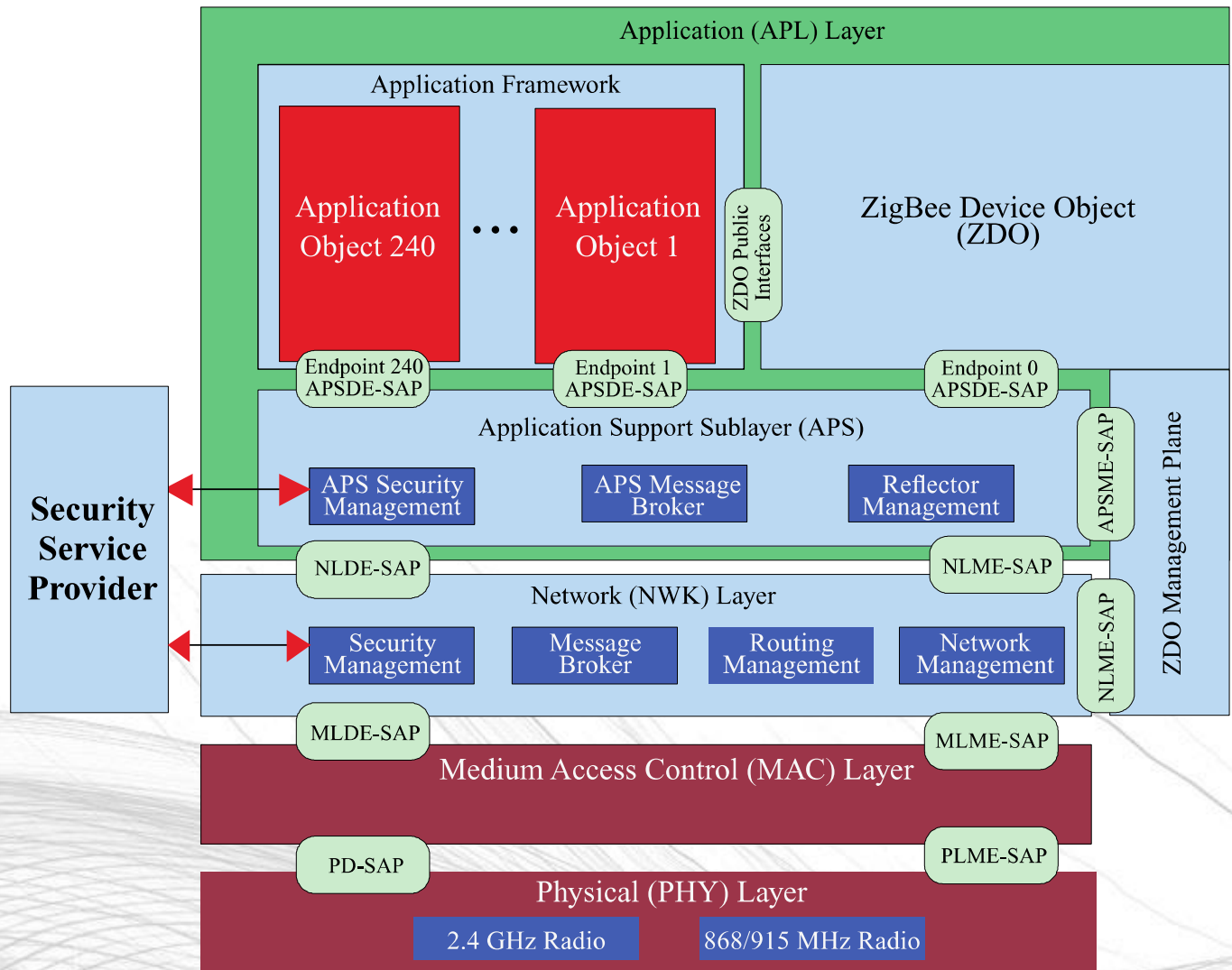


# ZIGBEE

- Extends IEEE 802.15.4 standards
- Low data rate, long battery life, secure networking
- Data rates 20 to 250 kbps
- Operates in ISM bands
  - 868 MHz (Europe), 915 MHz (USA and Australia), 2.4 GHz (worldwide)
- Quick wake from sleep
  - 30 ms or less compared to Bluetooth which can be up to 3 sec.
  - ZigBee nodes can sleep most of the time

# ZIGBEE

- ZigBee complements the IEEE 802.15.4 standard by adding four main components
  - Network layer provides routing
  - Application support sublayer supports specialized services.
  - ZigBee device objects (ZDOs) are the most significant improvement
    - Keep device roles, manage requests to join the network, discover devices, and manage security.
  - Manufacturer-defined application objects allow customization.

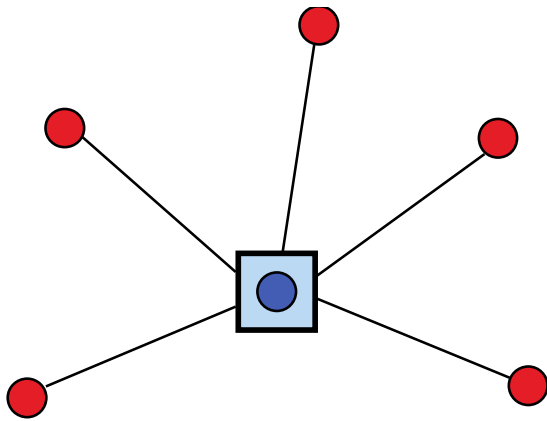


- IEEE 802.15.4 defined
- ZigBee™ Alliance defined
- End manufacturer defined
- Layer function
- Layer interface

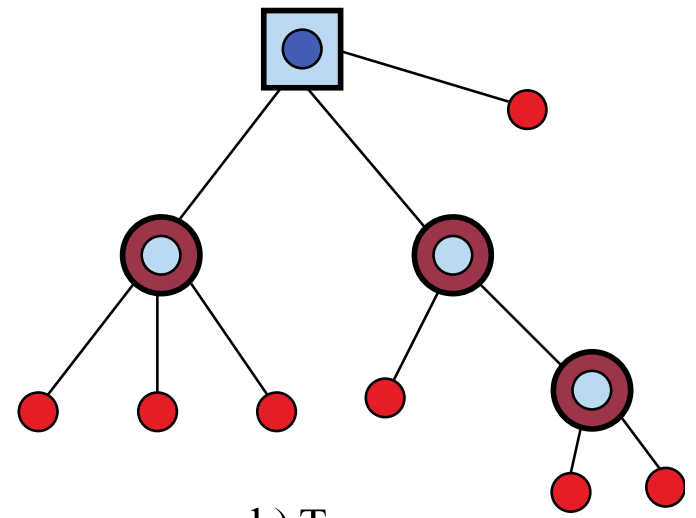
## 12.11 ZIGBEE ARCHITECTURE

# ZIGBEE

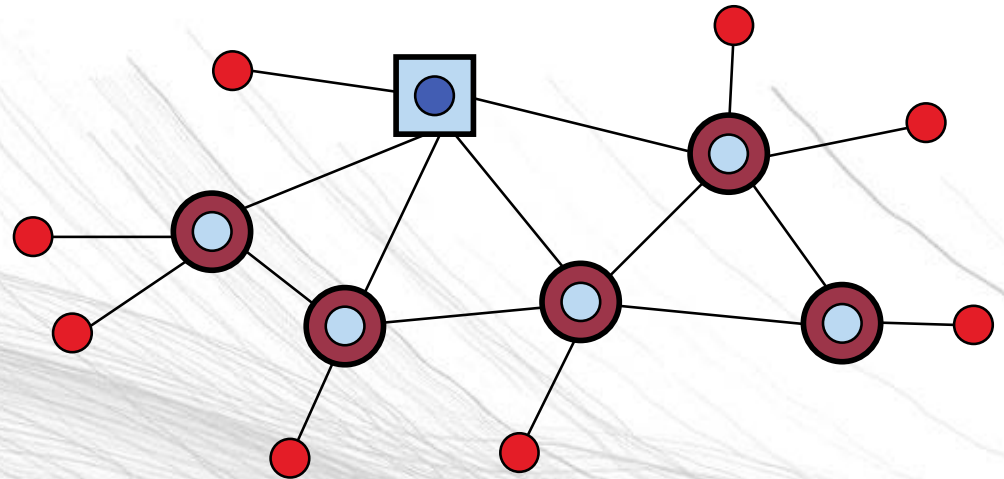
- Star, tree, or general mesh network structures
- ZigBee Coordinator
  - Creates, controls, and maintains the network
  - Only one coordinator in the network
  - Maintains network information, such as security keys
- ZigBee Router
  - Can pass data to other ZigBee devices
- ZigBee End Device
  - Only enough functionality to talk to a router or coordinator
  - Cannot relay information
  - Sleeps most of the time
  - Less expensive to manufacture






a) Star



b) Tree



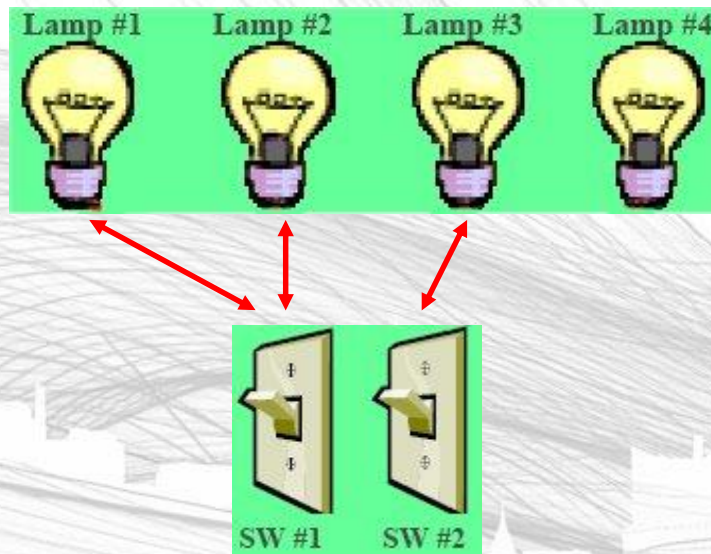
c) Mesh

-  ZigBee Coordinator
-  ZigBee Router
-  ZigBee End Device

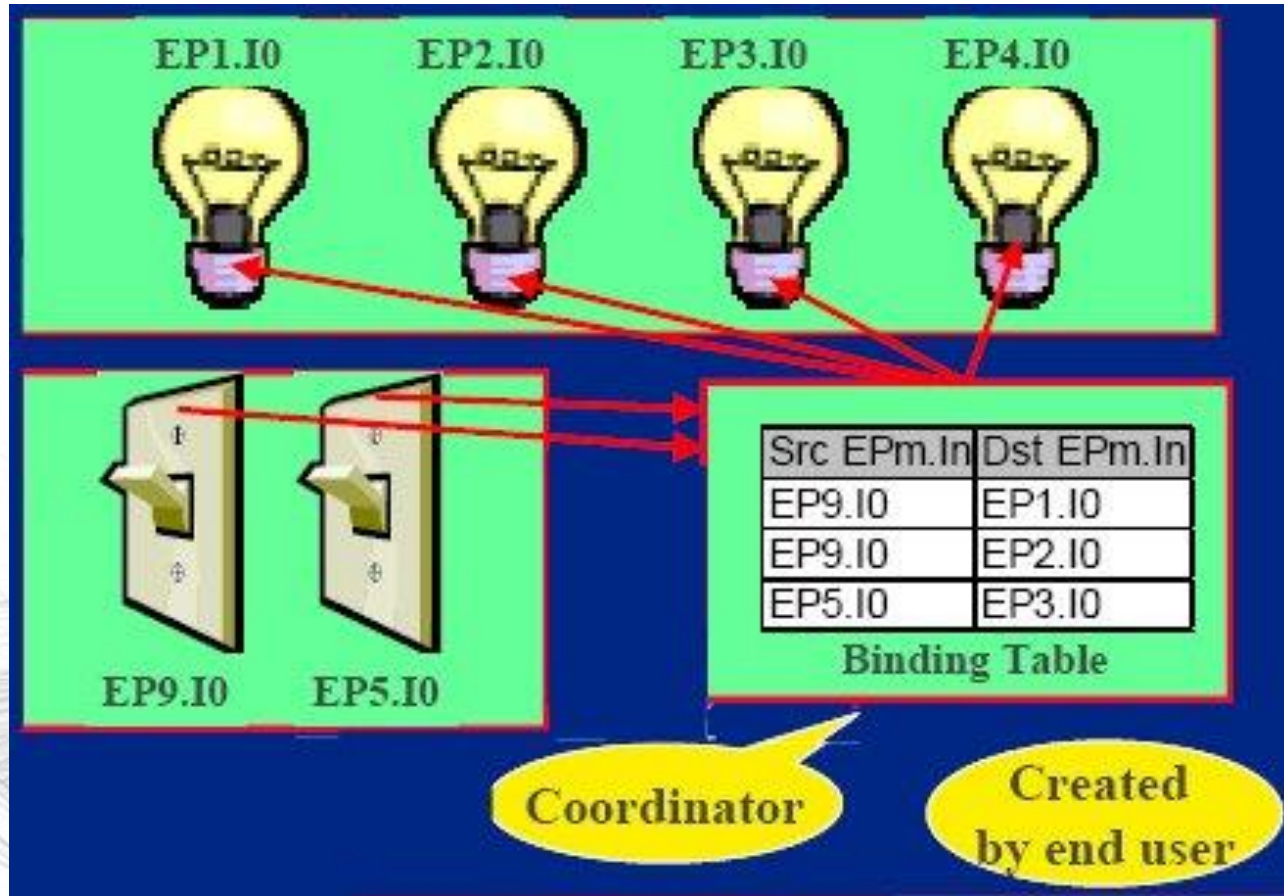
## 12.12 ZIGBEE NETWORK

# APPLICATION SUPPORT LAYER FUNCTIONS

- Zigbee Device Object (ZDO) maintains what the device is capable of doing and makes binding requests based on these capabilities
- Discovery – Ability to determine which other devices are operating in the operating space of this device
- Binding – Ability to match two or more devices together based on their services and their needs and allow them to communicate



# BINDING



EP – Endpoint (subunit of a node)

# ZIGBEE ALLIANCE

- Industry consortium
- Maintains and publishes the ZigBee standard
  - ZigBee specifications in 2004
  - ZigBee PRO completed in 2007
    - Enhanced ZigBee
    - Profile 1 – home and light commercial use
    - Profile 2 – more features such as multicasting and higher security
- Application profiles
  - Allow vendors to create interoperable products if they implement the same profile



# ZIGBEE APPLICATION PROFILES

- ZigBee Building Automation (Efficient commercial spaces)
- ZigBee Health Care (Health and fitness monitoring)
- ZigBee Home Automation (Smart homes)
- ZigBee Input Device (Easy-to-use touchpads, mice, keyboards, wands)
- ZigBee Light Link (LED lighting control)
- ZigBee Network Devices (Assist and expand ZigBee networks)
- ZigBee Retail Services (Smarter shopping)
- ZigBee Remote Control (Advanced remote controls)
- ZigBee Smart Energy 1.1 (Home energy savings)
- ZigBee Smart Energy Profile 2 (IP-based home energy management)
- ZigBee Telecom Services (Value-added services)