Wireless personal area networks

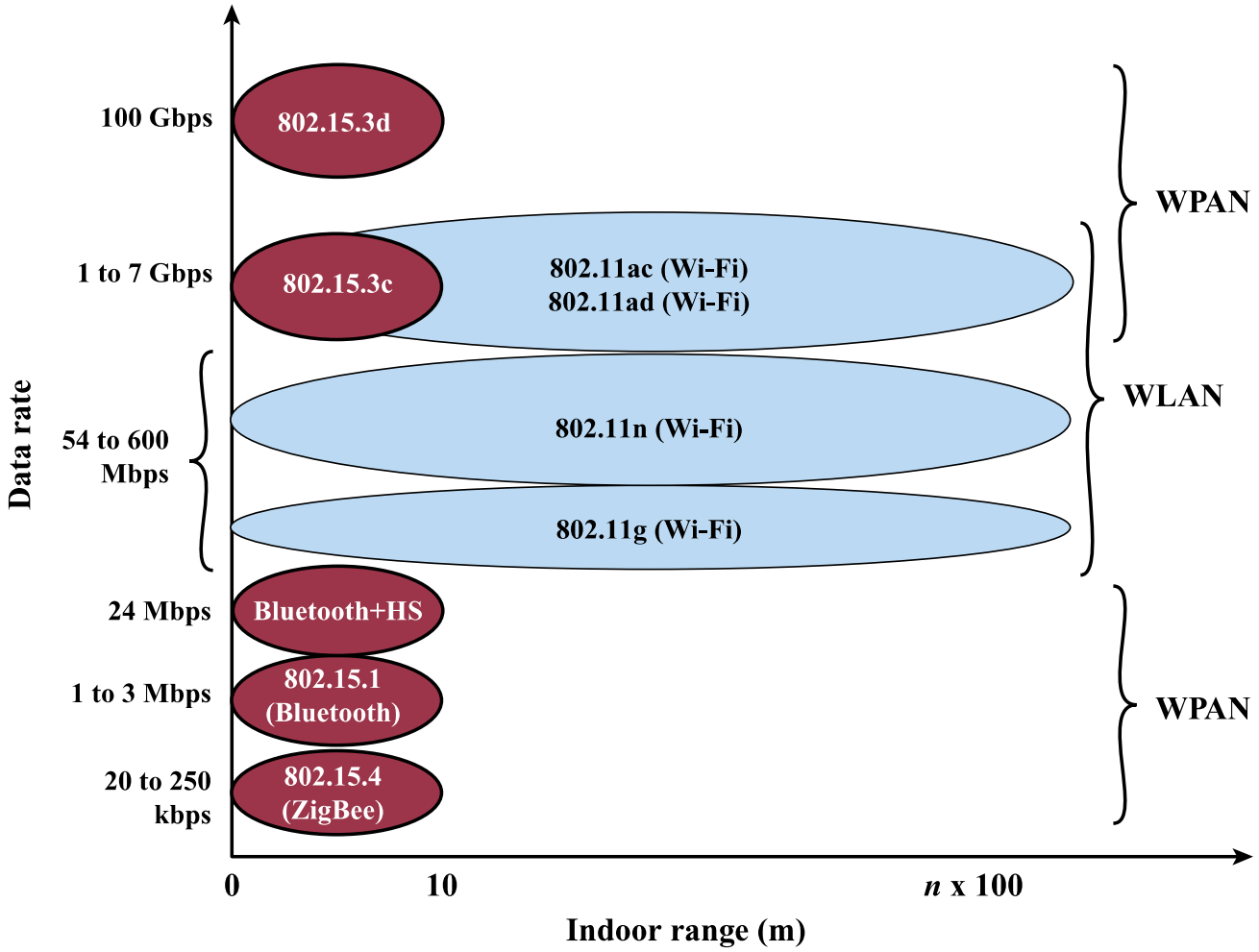
EP2950

KTH Technology
and Health

Outline

- ✓ Internet of things and short-range radio
- ✓ Bluetooth
- ✓ IEEE 802.15.4 and ZigBee

Wireless local networks

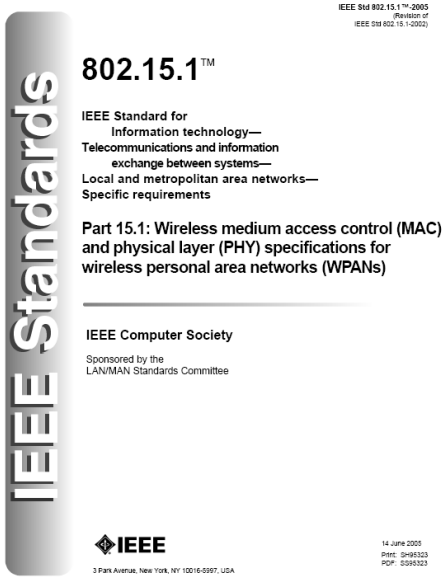


Internet of things and short-range radio

- 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
  - 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

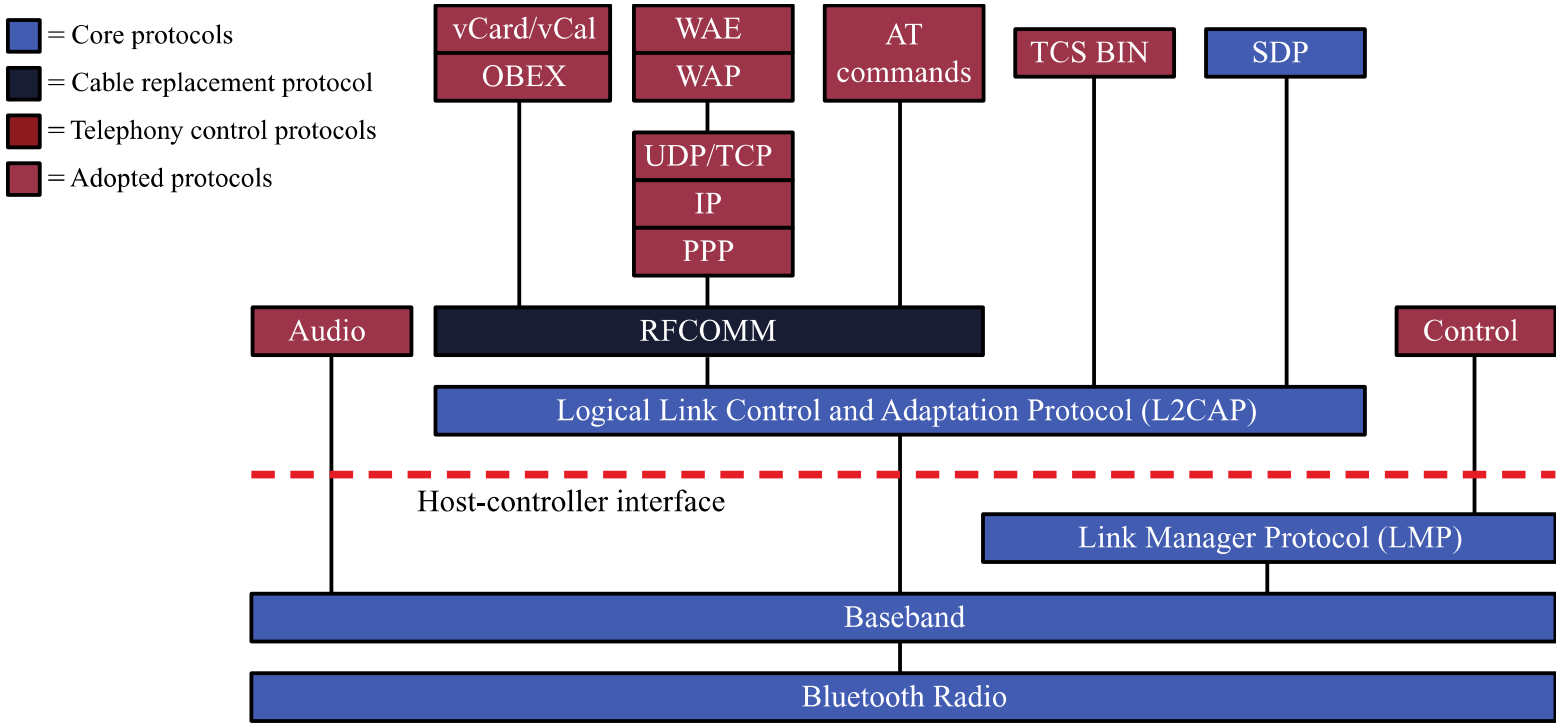
- ✓ IEEE 802.15.1 Standard (2005)
- ✓ Bluetooth special interest group (SIG)



Bluetooth started as the code name for the association when it was first formed and the name stuck. The name "*Bluetooth*" is from the 10th century Danish King Harald Blatand - or Harold *Bluetooth* in English. King Blatand was instrumental in uniting warring factions in parts of what are now Norway, Sweden, and Denmark

- General application areas
  - Data and voice access points
  - Cable replacement
  - Ad hoc networking
- Short-range
  - Normally around 10m – can be extended
  - Piconet with maximum 8 devices
- Low power
- Core specifications
  - Radio and link layer
- Profile specifications
  - Interoperability
  - Define which parts of core specifications are used

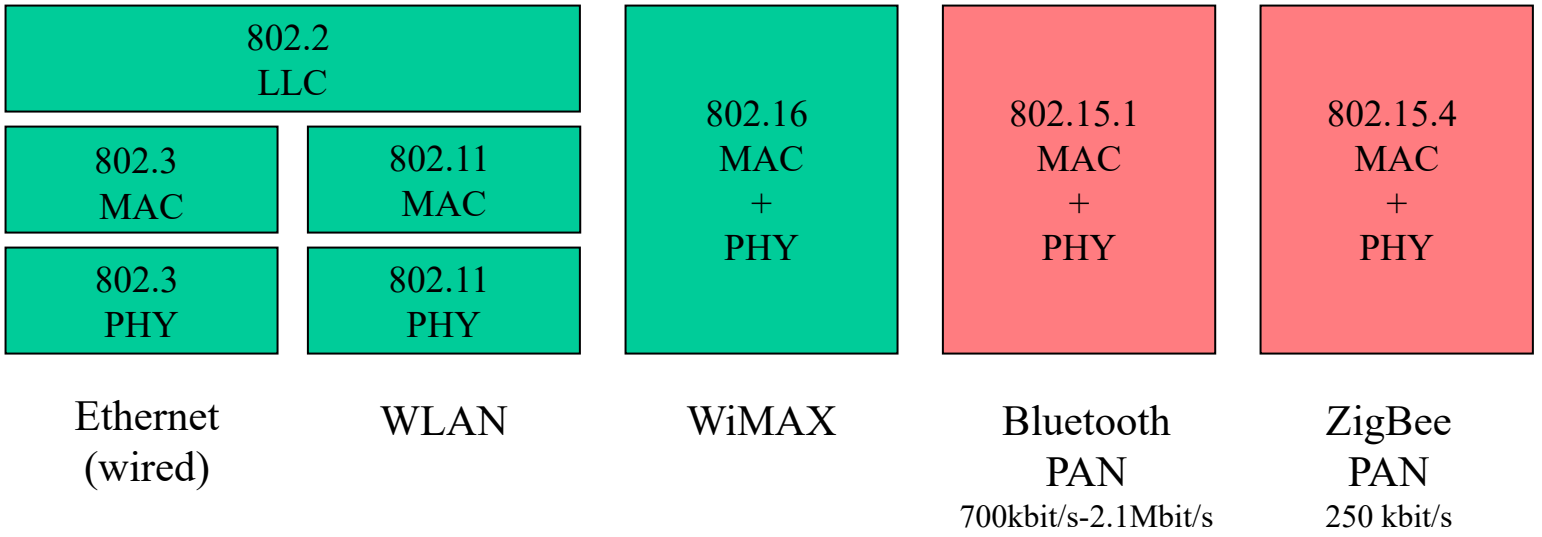
Bluetooth protocol stack



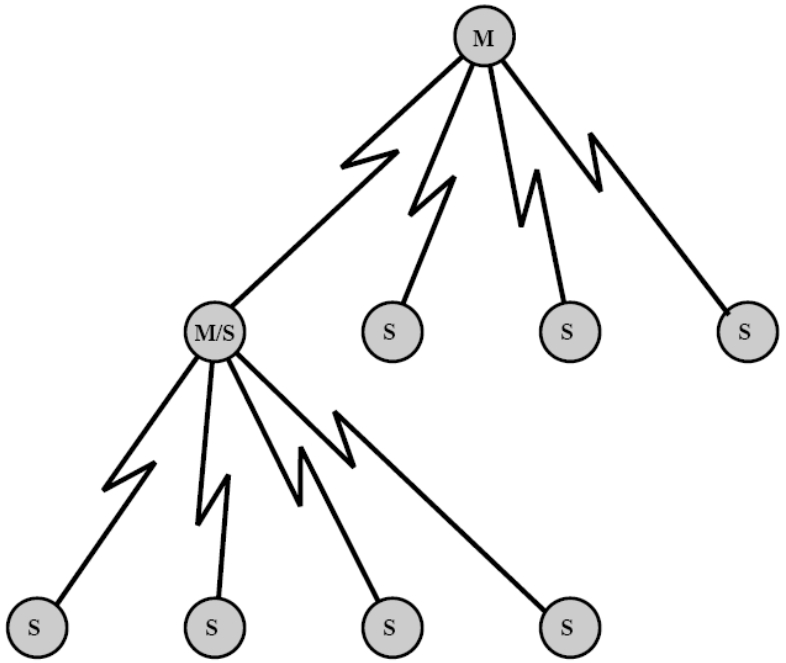
AT	=	Attention sequence (modem prefix)	TCS BIN	=	Telephony control specification - binary
IP	=	Internet Protocol	UDP	=	User Datagram Protocol
OBEX	=	Object exchange protocol	vCal	=	Virtual calendar
PPP	=	Point-to-Point Protocol	vCard	=	Virtual card
RFCOMM	=	Radio frequency communications	WAE	=	Wireless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

- Core protocols
  - Radio – physical layer
  - Baseband – addressing, packet format, timing, transmit power
  - Link manager protocol (LMP) – link setup and management
  - Logical link control and adaptation protocol (L2CAP) – adapt upper layer protocols
  - Service discovery protocol (SDP)
- RFCOMM – cable replacement
- Telephony control protocol (TCS BIN)
- Adopted protocol
  - PPP – point-to-point protocol
  - TCP/UDP/IP
  - OBEX – object exchange protocol, similar to HTTP
  - WAE/WAP – wireless application protocol

- ✓ IEEE 802 standards
- ✓ Personal area networks
  - ✓ Bluetooth 802.15.1
  - ✓ Zigbee 802.15.4



- Bluetooth operation
- Piconet
  - Bluetooth nodes discover each other within radio proximity
  - Master-slave
  - One master and up to 7 slaves
  - 10m range (up to around 100m)
- Scatternet
  - Connecting piconets
  - One device in one or more piconet



- Piconets
  - Master defines the physical channel to be used in the piconet
    - Frequency-hopping (FH) and timing offset
    - Based on the “device address” to randomize FH
  - Slaves tune to the same channel
  - Master polls the slaves in a round robin manner
- Parallel piconets or scatternet
  - Collision happens if the same frequency used in the FH
  - Collision probability increases with the number piconets

✓ Bluetooth radio specification

- ✓ Piconet
  - Frequency hopping - time division duplex - time division multiple access
- ✓ Scatternet
  - FH code division (frequency hopping sequence used in each piconet is determined by the master's Bluetooth address)

Topology	Logical star
Modulation	GFSK, 8PSK
Peak rate	1Mbit/s, 3Mbit/s
RF band	2.4GHz (ISM)
RF sub-carriers	23/79
Transmit power	0.1W, 2.4mW, 1mW
Piconet access	FH-TDD-TDMA
Scatternet access	FH-CDMA

- Red: version 2.1, higher bitrate
- Effective rate: 0.7, 2.1Mbps
- RF band ISM band (industrial, scientific, medical)

Transmission power

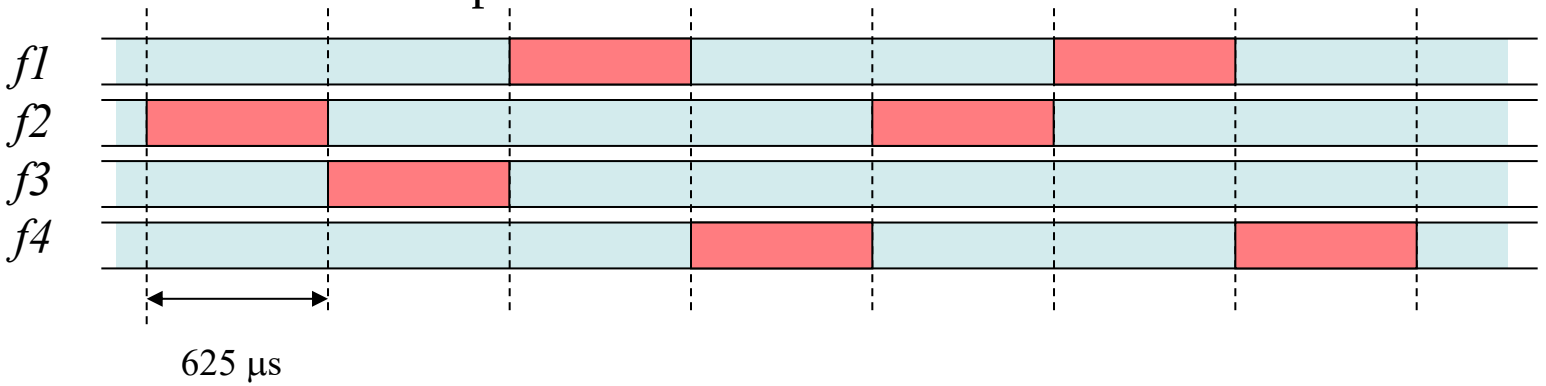
class 1	0.1W, power control	100m
class 2	2.4mW, power control optional	10m
class3	1mW, no power control	10cm

✓ Bluetooth radio frequency allocation

Area	Regulatory Range	RF Channels
U.S., most of Europe, and most other countries	2.4 to 2.4835 GHz	$f = 2.402 + n$ MHz, $n = 0,\ldots, 78$
Japan	2.471 to 2.497 GHz	$f = 2.473 + n$ MHz, $n = 0,\ldots, 22$
Spain	2.445 to 2.475 GHz	$f = 2.449 + n$ MHz, $n = 0,\ldots, 22$
France	2.4465 to 2.4835 GHz	$f = 2.454 + n$ MHz, $n = 0,\ldots, 22$

✓ Physical channel (FH channel in Stallings)

- ✓ 79 RF channels, each of 1MHz bandwidth
  - ✓ Jump from channel to channel according to a pseudo-random sequence *f(k)*
    - Sequence determined by the master's Bluetooth address
    - Bad quality frequencies skipped
  - ✓ One jump per 625μs timeslots
    - Timeslot length from telephony to provide very low delay / delay variance
  - ✓ FH scheme determines which RF channel to use
  - ✓ Channel access control determines which device can transmit within the piconet

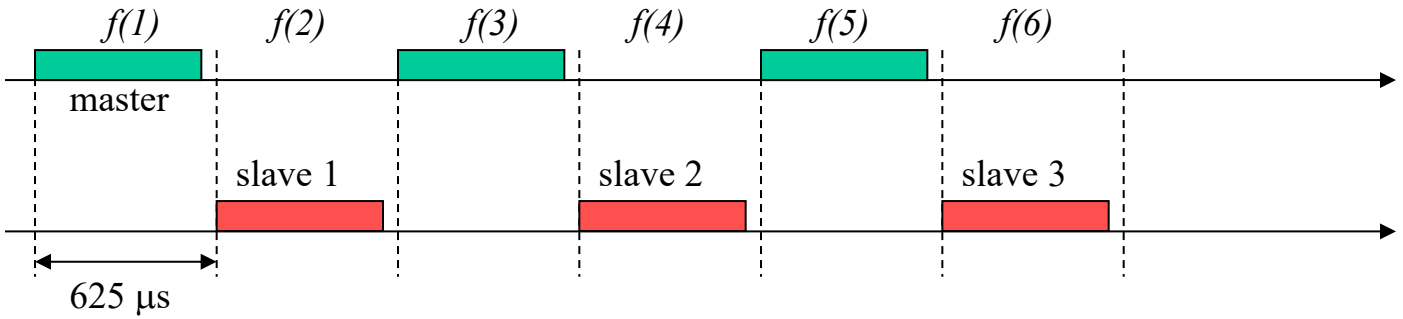


“Piconet physical channel:

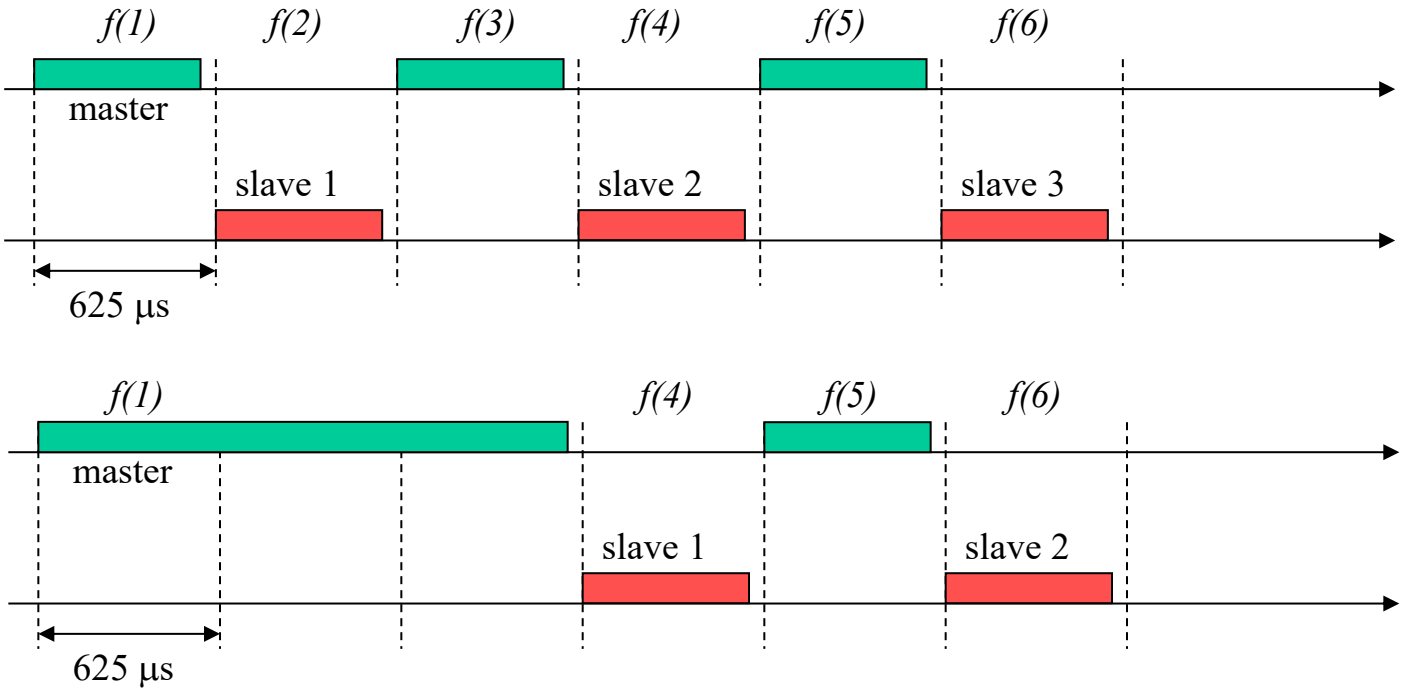
A channel that is divided into time slots in which each slot is related to a radio frequency (RF) hop frequency. Consecutive hops normally correspond to different RF hop frequencies and occur at a standard hop rate of 1600 hop/s. These consecutive hops follow a pseudo-random hopping sequence, hopping through a 79-RF channel set, or optionally fewer channels when adaptive frequency hopping(AFH) is in used.”

Baseband – FH-TDD-TDMA

- TDD: time division duplex
  - Time is divided for master–slave and slave-master communication
- TDMA: time division multiple access
  - Time is divided among the slaves
  - Channel access through polling – the master contacts all slaves in a round-robin manner
  - Or with reservation



- ✓ Packets for 1, 3, 5 slot length
- ✓ Round-robin sequence kept
- ✓ Frequencies skipped if longer packets are used



- Links between master and slaves
  - Physical links
  - Logical transport links
- Asynchronous connectionless links (ACL)
  - Used for data transmission
  - Point-to-point and point-to-multipoint
  - 1, 3 or 5 slot packets
  - Slave answers in next timeslot
  - Error control
    - ARQ: one bit sequence number
    - 16 bit CRC
    - 2/3 forward error correction code (15,10) Hamming code

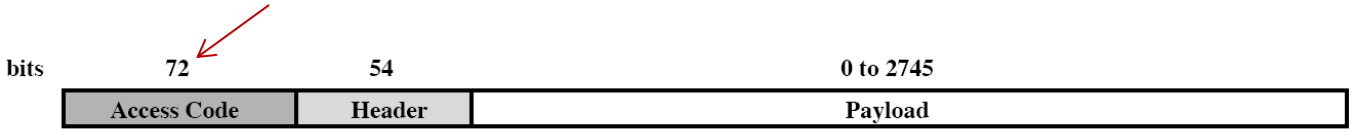
- ✓ Synchronous connection-oriented links (SCO)
  - ✓ Voice communication (or combined data and voice)
  - ✓ Circuit-switched connection between master and a slave
  - ✓ Error control
    - No retransmission
    - 2/3 forward error correction code (15,10) Hamming code
    - 1/3 forward error correction: three copies of each bit

Table 15.4 Achievable Data Rates on the ACL Link

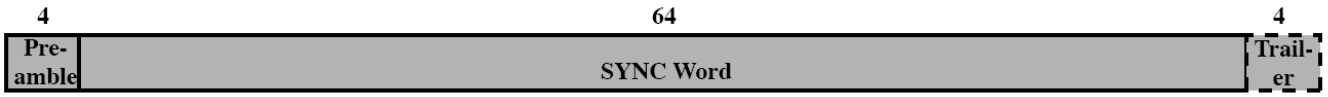
Type	Symmetric (kbps)	Asymmetric (kbps)	
DM1	108.8	108.8	108.8
DH1	172.8	172.8	172.8
DM3	256.0	384.0	54.4
DH3	384.0	576.0	86.4
DM5	286.7	477.8	36.3
DH5	432.6	721.0	57.6

DMx = x-slot FEC-encoded
DHx = x-slot unprotected

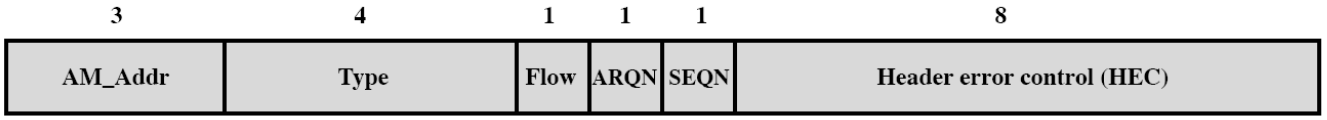
✓ Baseband packet format



(a) Packet format

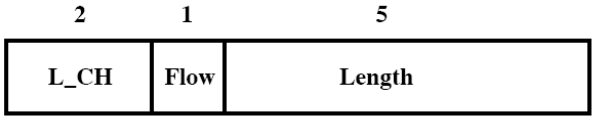


(b) Access code format

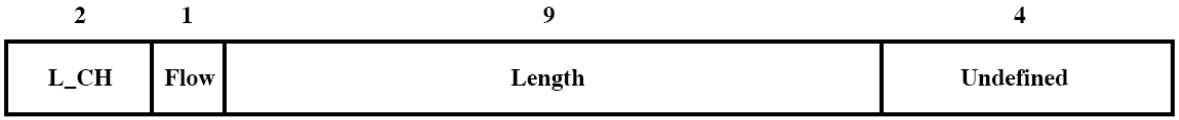


= 18 bits

(c) Header format (prior to coding)



Single-slot packets



Multislot packets

(d) Data payload header format

- Access code
  - Channel Access Code (CAC) - identifies a piconet
    - Derived from master's BD_ADDR
  - Device Access Code (DAC) - for paging and responses
    - Derived from slave's device address
  - Inquiry Access Code (IAC) - for inquiry
    - General and dedicated codes shared by all Bluetooth devices
- Addresses
  - BD_ADDR – Bluetooth device address (48 bits)
  - LT_ADDR – Logical transport address (3 bits)
    - Formerly AM_ADDR – active member address
  - AR_ADDR – Access request address
  - PM_ADDR – Parked member address

- ✓ Access code SYNC word derivation
  - ✓ High auto-correlation and low cross-correlation

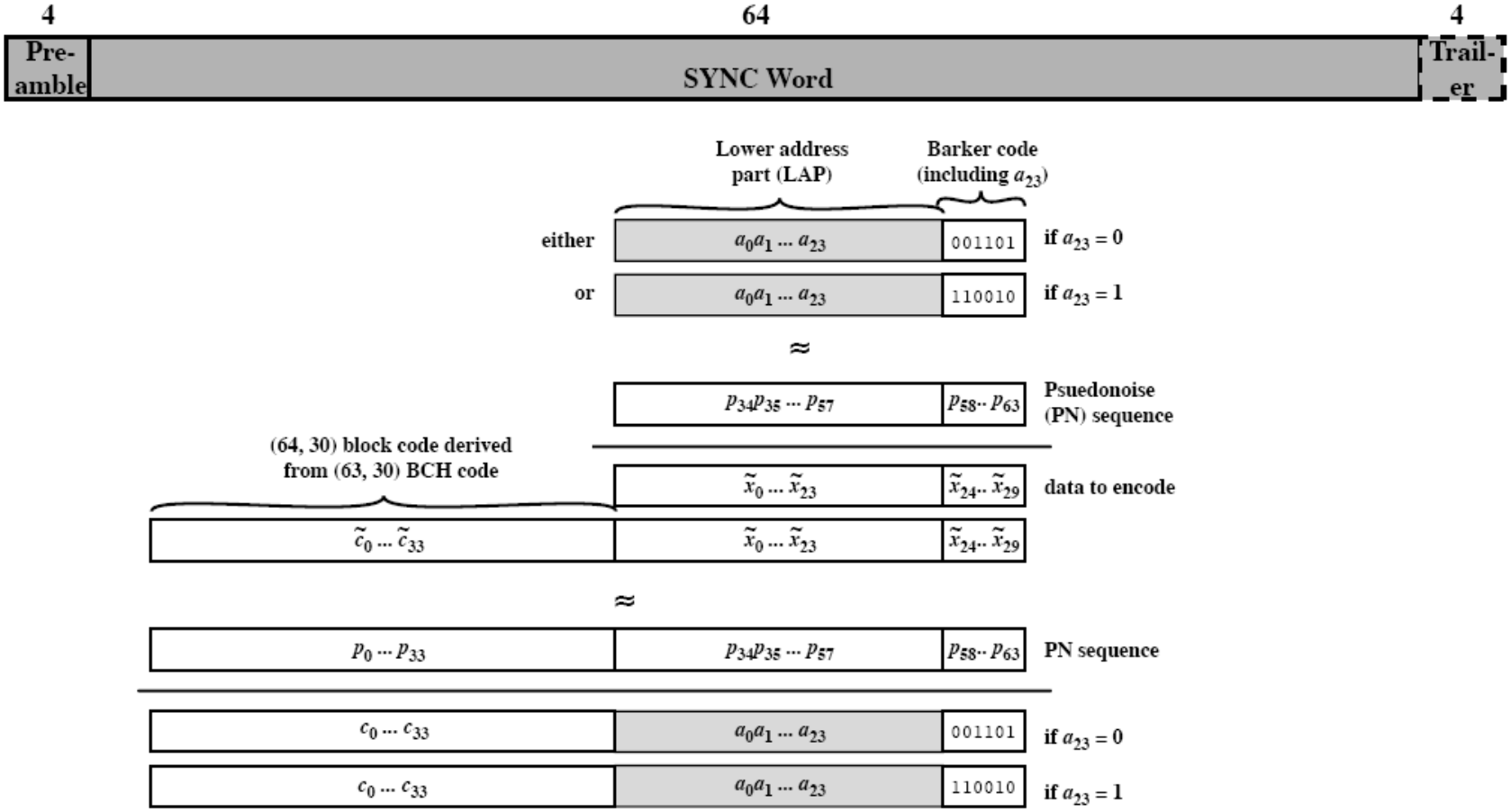
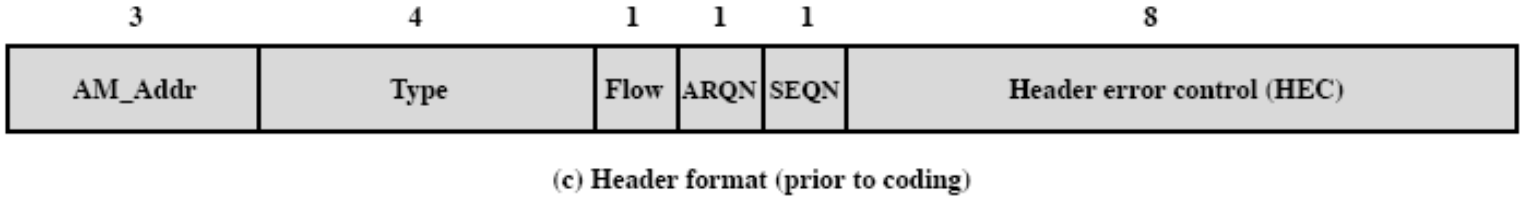


Figure 15.8 Construction of Sync Word

Packet header functions



(c) Header format (prior to coding)

- AM_ADDR – contains "active mode" address of one of the slaves – called LT_ADDR in current standard
- 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
- 10 bits before and 54 bits after encoding – Explain!

- ✓ Bluetooth packet types
- ✓ SCO packets
  - ✓ HV1, HV2, HV3 – high quality voice
    - 64kb/s, different FEC encoding
  - ✓ DV – data-voice combined
- ✓ ACL packets
  - ✓ DH1, DH3, DH5 – data high rate
    - 1, 3 or 5 timeslots, different error coding
- ✓ POLL packets
  - ✓ Master to slave. Must be acknowledged. No payload.
- ✓ NULL packets
  - ✓ Return information to source. Need not be acknowledged.

Type Code	Physical Link	Name	Number of Slots	Description
0000	Common	NULL	1	Has no payload. Used to return link information to the source regarding the success of the previous transmission (ARQN), or the status of the RX buffer (FLOW). Not acknowledged.
0001	Common	POLL	1	Has no payload. Used by master to poll a slave. Acknowledged.
0010	Common	FHS	1	Special control packet for revealing device address and the clock of the sender. Used in page master response, inquiry response, and frequency hop synchronization. 2/3 FEC encoded.
0011	Common	DM1	1	Supports control messages and can also carry user data. 16-bit CRC. 2/3 FEC encoded.
0101	SCO	HV1	1	Carries 10 information bytes; typically used for 64-kbps voice. 1/3 FEC encoded.
0110	SCO	HV2	1	Carries 20 information bytes; typically used for 64-kbps voice. 2/3 FEC encoded.
0111	SCO	HV3	1	Carries 30 information bytes; typically used for 64-kbps voice. Not FEC encoded.
1000	SCO	DV	1	Combined data (150 bits) and voice (50 bits) packet. Data field 2/3 FEC encoded.
0100	ACL	DH1	1	Carries 28 information bytes plus 16-bit CRC. Not FEC encoded. Typically used for high-speed data.
1001	ACL	AUX1	1	Carries 30 information bytes with no CRC or FEC. Typically used for high-speed data.
1010	ACL	DM3	3	Carries 123 information bytes plus 16-bit CRC. 2/3 FEC encoded.
1011	ACL	DH3	3	Carries 185 information bytes plus 16-bit CRC. Not FEC encoded.
1110	ACL	DM5	5	Carries 226 information bytes plus 16-bit CRC. 2/3 FEC encoded.
1111	ACL	DH5	5	Carries 341 information bytes plus 16-bit CRC. Not FEC encoded.

Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)	Asymmetric Max. Rate (kb/s)	
						Forward	Reverse
DM1	1	0-17	2/3	yes	108.8	108.8	108.8
DH1	1	0-27	no	yes	172.8	172.8	172.8
DM3	2	0-121	2/3	yes	258.1	387.2	54.4
DH3	2	0-183	no	yes	390.4	585.6	86.4
DM5	2	0-224	2/3	yes	286.7	477.8	36.3
DH5	2	0-339	no	yes	433.9	723.2	57.6
AUX1	1	0-29	no	no	185.6	185.6	185.6
2-DH1	2	0-54	no	yes	345.6	345.6	345.6
2-DH3	2	0-367	no	yes	782.9	1174.4	172.8
2-DH5	2	0-679	no	yes	869.1	1448.5	115.2
3-DH1	2	0-83	no	yes	531.2	531.2	531.2
3-DH3	2	0-552	no	yes	1177.6	1766.4	235.6
3-DH5	2	0-1021	no	yes	1306.9	2178.1	177.1

Table 6.9: ACL packets

Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)
HV1	na	10	1/3	no	64.0
HV2	na	20	2/3	no	64.0
HV3	na	30	no	no	64.0
DV[1]	1 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D
EV3	na	1-30	No	Yes	96
EV4	na	1-120	2/3	Yes	192
EV5	na	1-180	No	Yes	288
2-EV3	na	1-60	No	Yes	192
2-EV5	na	1-360	No	Yes	576
3-EV3	na	1-90	No	Yes	288
3-EV5	na	1-540	No	Yes	864

Table 6.10: Synchronous packets

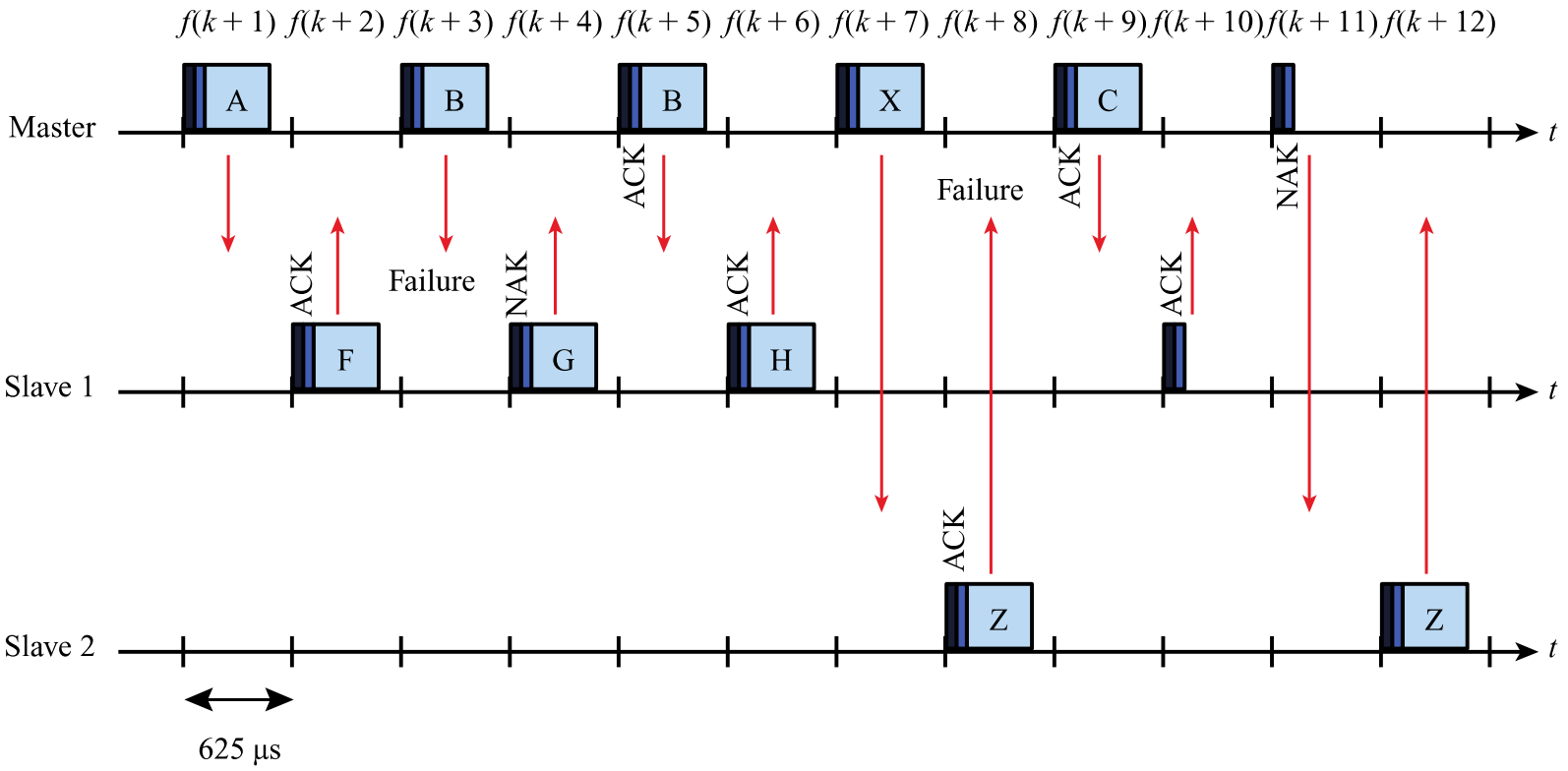
- ✓ Logical links
  - ✓ Link control (LC)
    - Low-level link control such as ARQ and flow control
  - ✓ ACL control (ACL-C)
    - Link manager
  - ✓ Asynchronous/isochronous user (ACL-U)
    - ACL asynchronous and almost synchronous data traffic
  - ✓ Stream
    - SCO synchronous voice data
- ✓ Logical transports
  - ✓ Carry different logical links
  - ✓ ACL, SCO, eSCO etc.

- ✓ Abstract from Bluetooth Core spec. v3.0+HS (high speed)

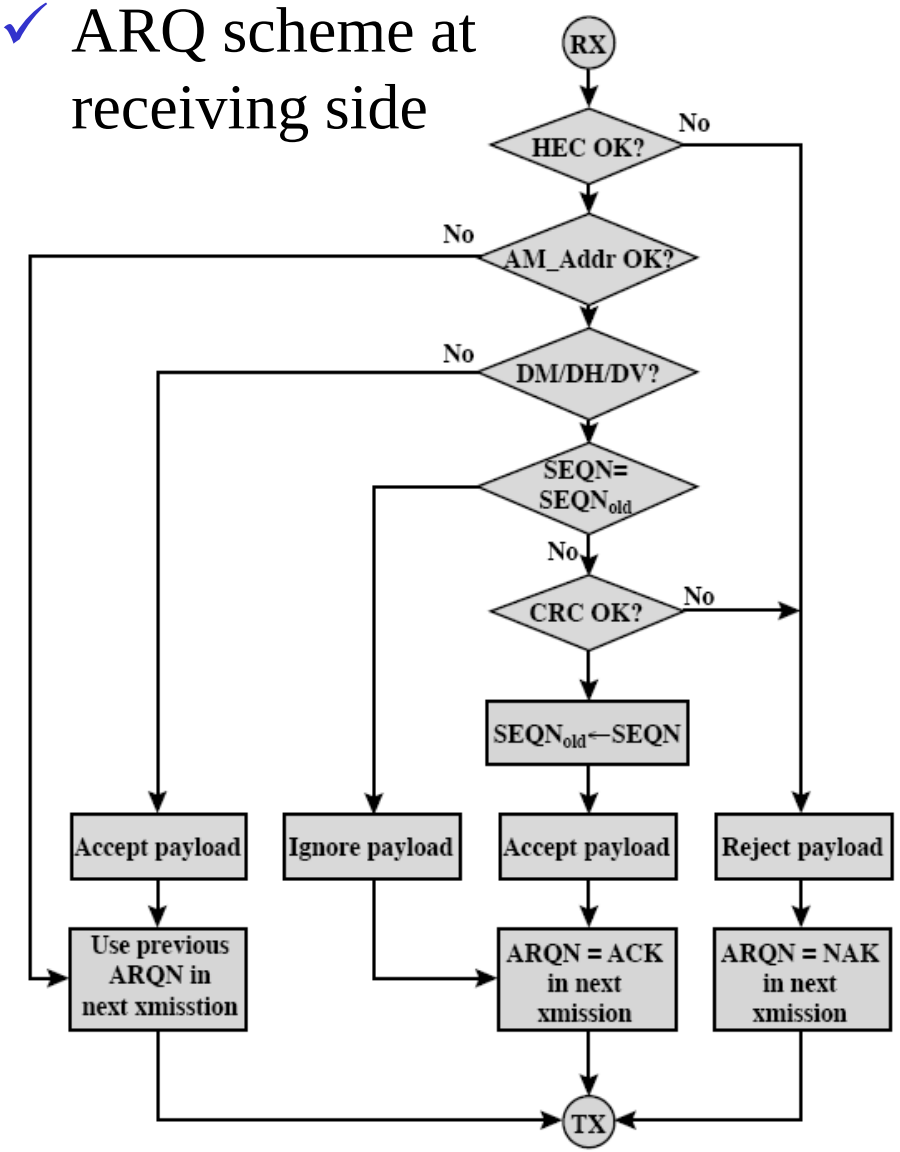
Logical transport	Links supported	Supported by	Bearer	Overview
Asynchronous Connection-Oriented (ACL)	Control (LMP) ACL-C or (PAL) AMP-C User (L2CAP) ACL-U or AMP-U	Active physical link, basic or adapted physical channel, AMP physical channel.	BR/EDR, AMP	Reliable or time-bounded, bi-directional, point-to-point.
Synchronous Connection-Oriented (SCO)	Stream (unframed) SCO-S	Active physical link, basic or adapted physical channel	BR/EDR	Bi-directional, symmetric, point-to-point, AV channels. Used for 64Kb/s constant rate data.

AMP (alternate MAC/PHY) - high speed supports 802.11a,b,g
BR/EDR – basic rate (1Mb/s) and enhanced data rate (2-3Mb/s)

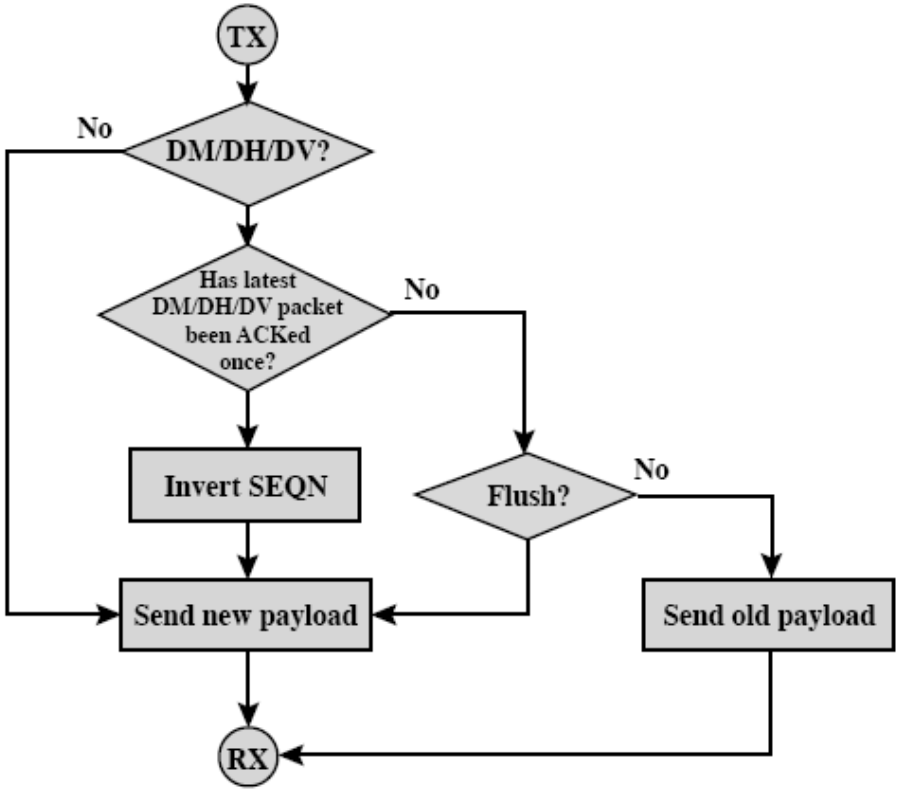
✓ Retransmissions



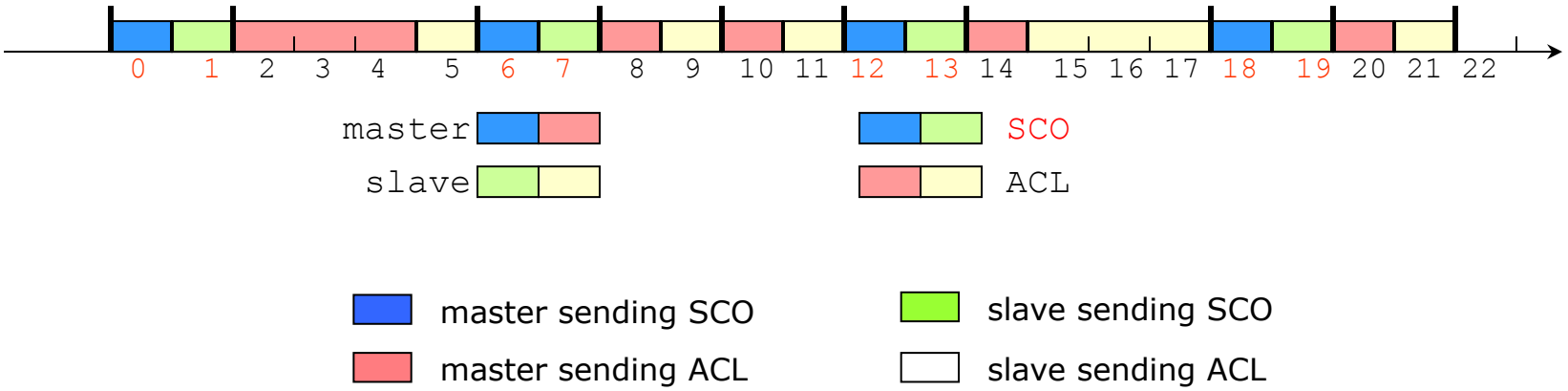
- ARQ scheme at receiving side



- ARQ scheme at transmitting side



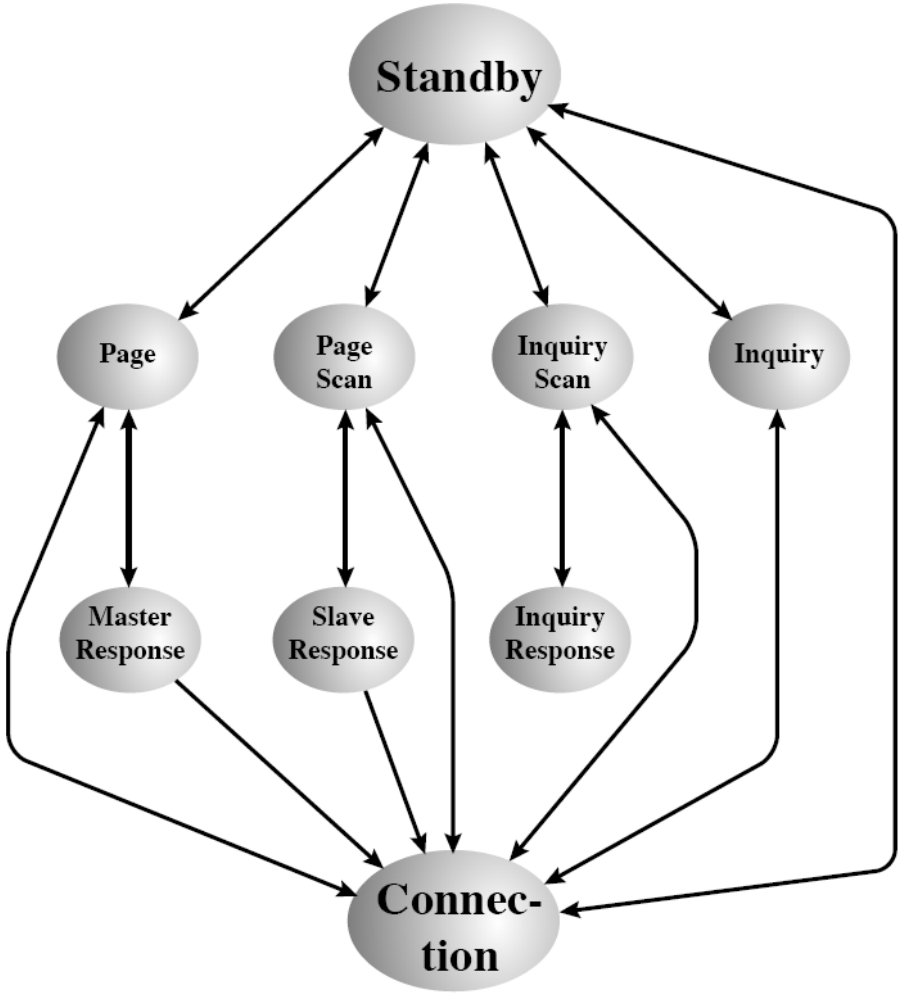
✓ SCO and ACL communication



- ✓ Summary of error control for Bluetooth
  - ✓ Scrambling
  - ✓ Header error control – 8-bit CRC
  - ✓ Payload error control – 16-bit CRC
  - ✓ 1/3 FEC – every bit repeated three times
  - ✓ 2/3 FEC, Hamming (15,10)
  - ✓ Automatic repeat request (ARQ)
    - Error detection
    - Positive acknowledgement
    - Retransmission after timeout
    - Negative acknowledgement and retransmissions

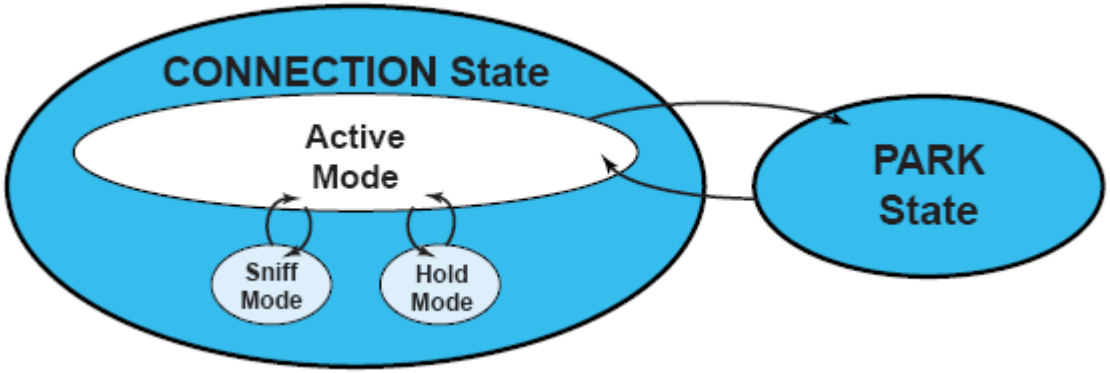
- ✓ Link controller states
  - ✓ Main states
    - Standby
    - Connection
    - Park
  - ✓ Sub states to set up connections and device discovery
    - Page, page scan, inquiry, inquiry scan, master response, slave response, inquiry response

✓ Link controller states

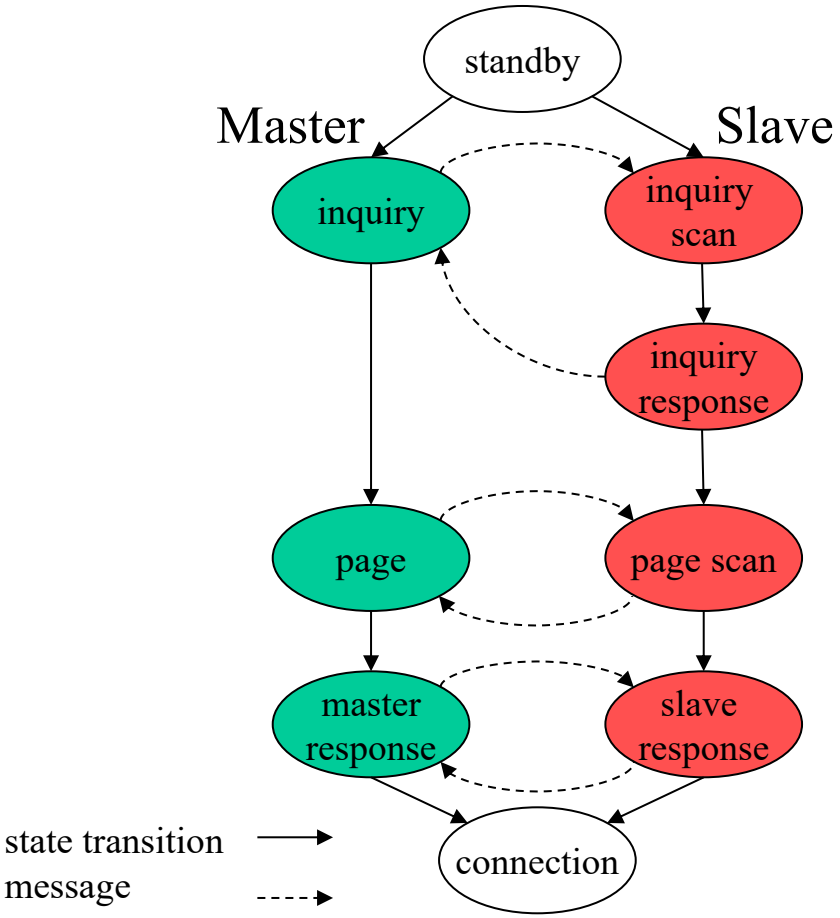


- ✓ Standby
  - Default state
- ✓ Inquiry
  - Find and identify devices within range
  - Master activate and connect to slaves
- ✓ Connection
  - Connection between master and slave
- ✓ Park
  - Low-power mode, enables more than 7 slaves, gets PM_ADDR instead of LT_ADDR

- Connection state modes
  - Active
    - The slave listens, transmits and receives packets
  - Hold
    - Reduced power status. Only SCO packets
  - Sniff
    - Reduced power status. Listens to specified timeslots

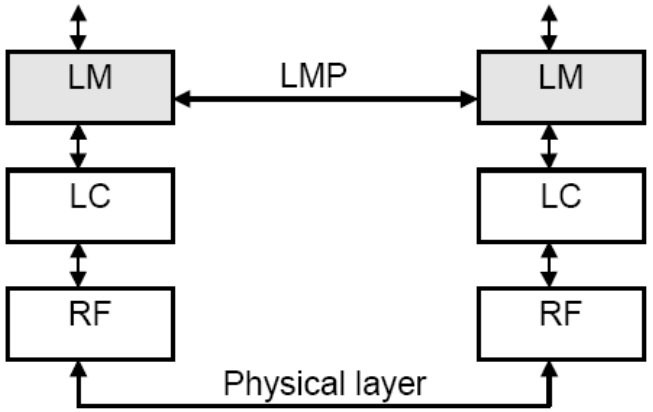


✓ Connection setup



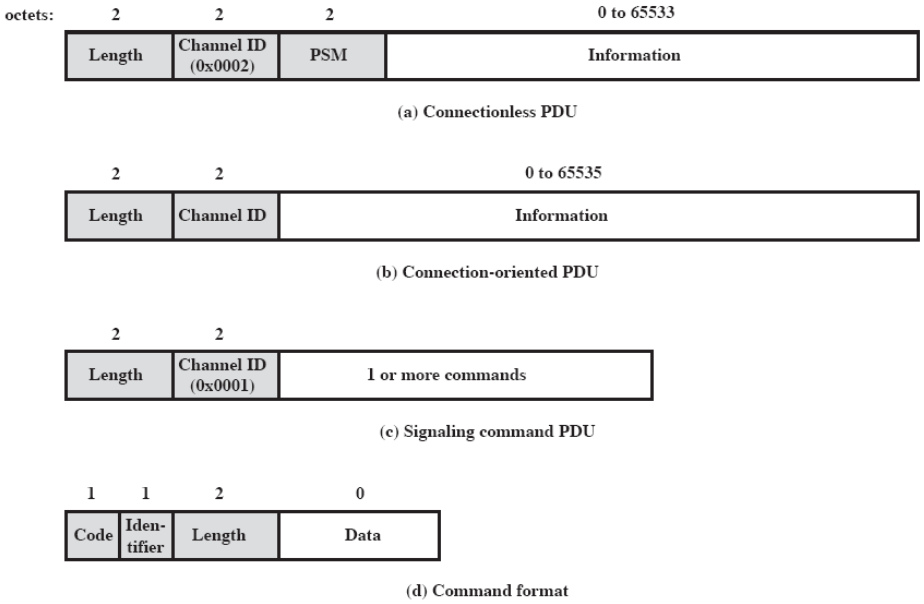
- Predefined wake-up channels and starting FH sequence
- Master broadcast on 32 wake-up channels, slave scan channels periodically
- If inquiry detected, slave responds with its address
- Master pages all found devices in turn
- Slaves confirm
- Master transmits address and clock
- Slaves confirm
- Both of them in connection state, start to use the FH defined by the master address

- Link manager protocol (LMP)
  - Setup of logical transports and logical links
  - Synchronization and clock offset
  - Authentication
  - Pairing
  - Feature list for connections
  - Uses ACL logical transport



3-slot packets
5-slot packets
encryption
slot offset
timing accuracy
switch
hold mode
sniff mode
park mode
RSSI
channel quality-driven data rate
SCO link
HV2 packets
HV3 packets
μ-law log
A-law log
CVSD
paging scheme
power control

- ✓ Logical link control and adaptation protocol (L2CAP)
  - ✓ Services for higher layers protocols
    - Connection-mode service
    - Connectionless service
    - Signaling
    - Identify higher layer recipients (multiplexing)



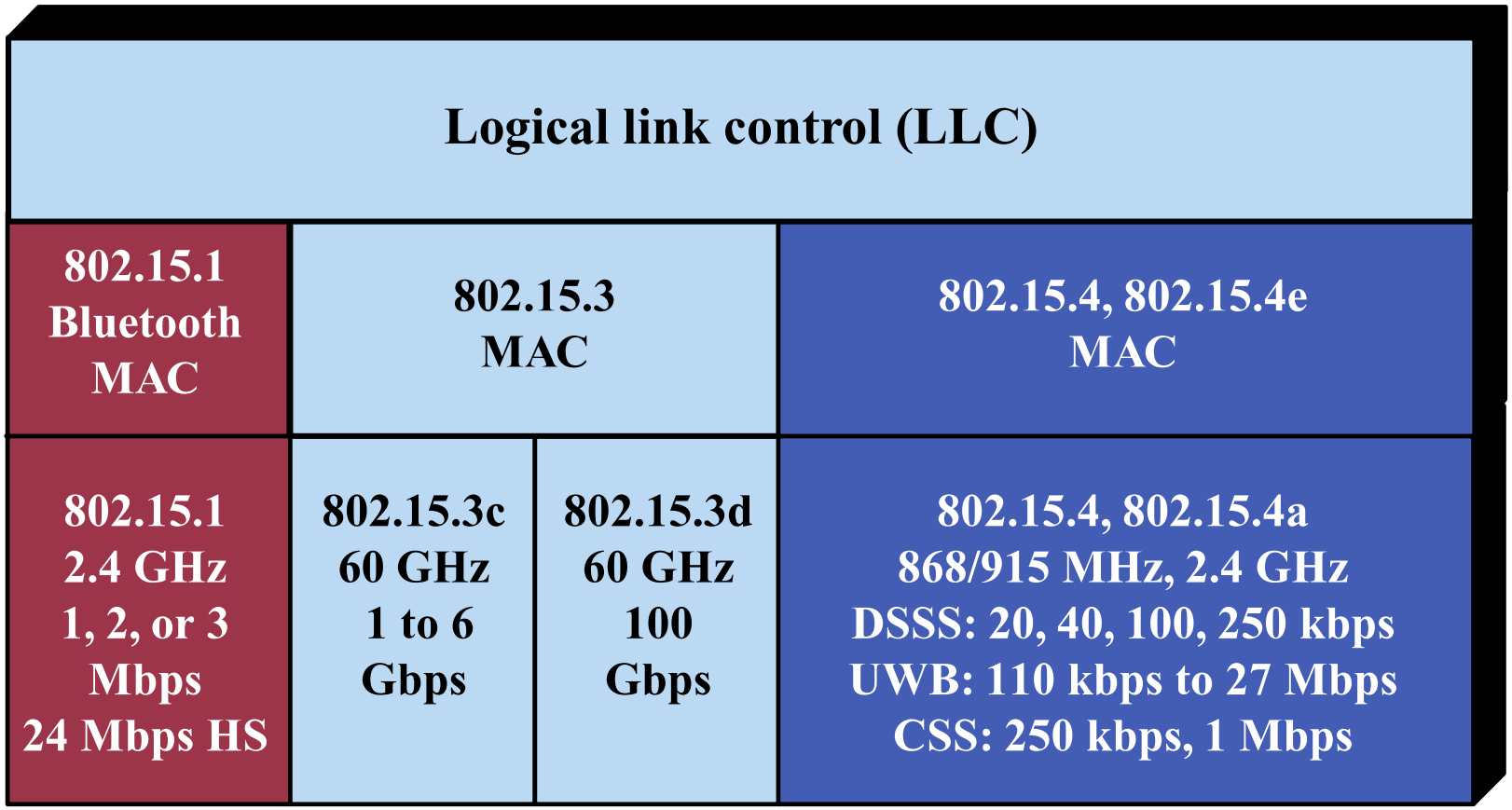
- ✓ Bluetooth specifications
  - ✓ v2.0+EDR (enhanced data rate)
    - Nominal data rate 3Mb/s
  - ✓ v2.1+EDR (+ simple secure pairing)
  - ✓ v3.0+HS (up to 24Mb/s)
  - ✓ v4.0, v4.1, v4.2 LE (low energy)

Bluetooth®

- 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)
  - 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 low energy
  - ✓ Bluetooth 4.0, 4.1, 4.2
  - ✓ 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

IEEE 802.15 architecture



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
- ✓ EEE 802.15.4k – Low Energy Critical Infrastructure Networks (LECIM)
  - 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

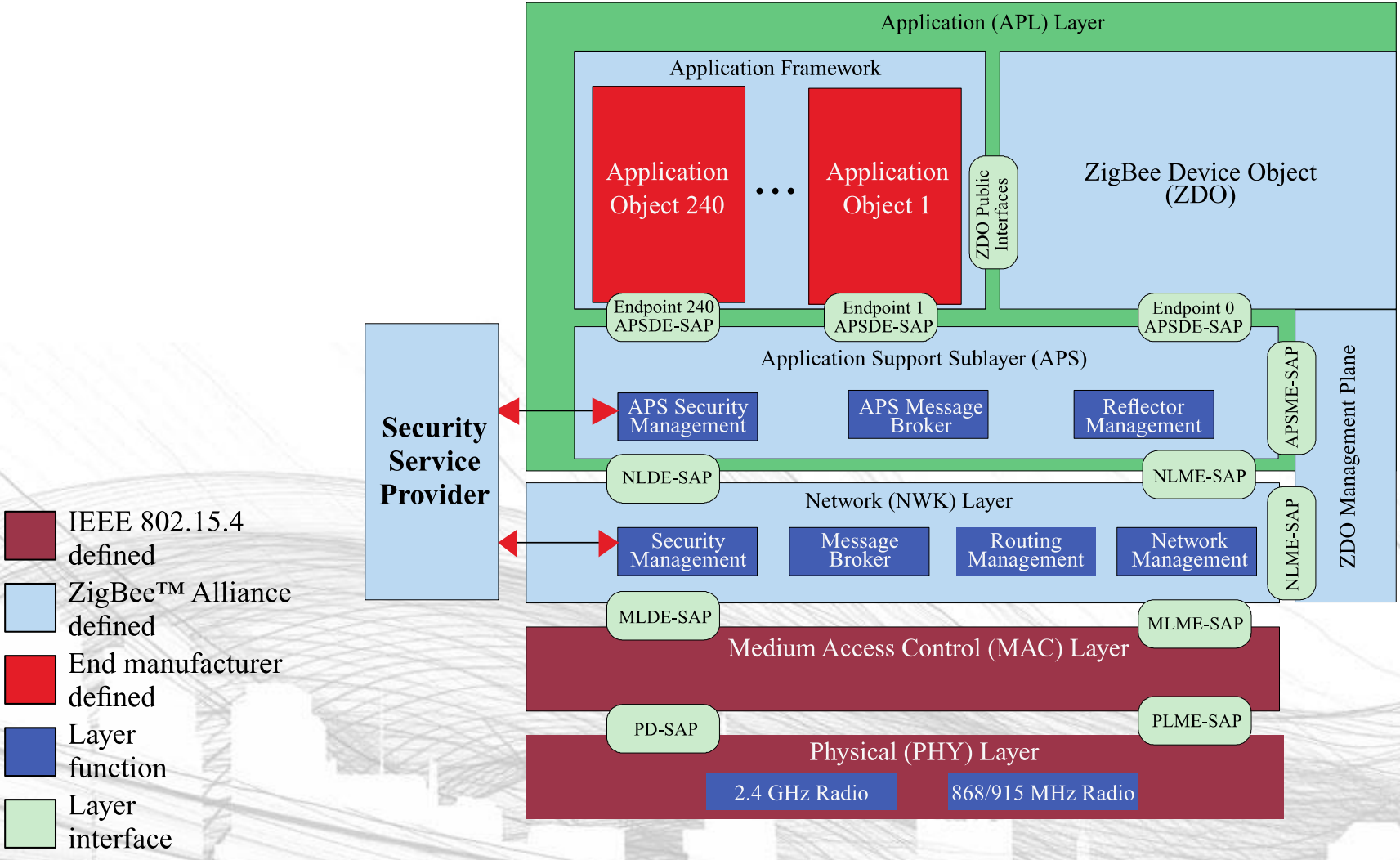
ZIGBEE

- ✓ 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.

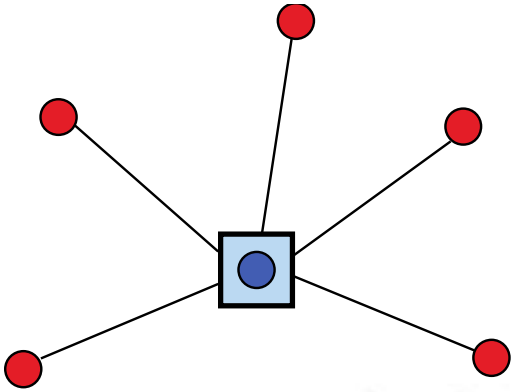
ZIGBEE ARCHITECTURE



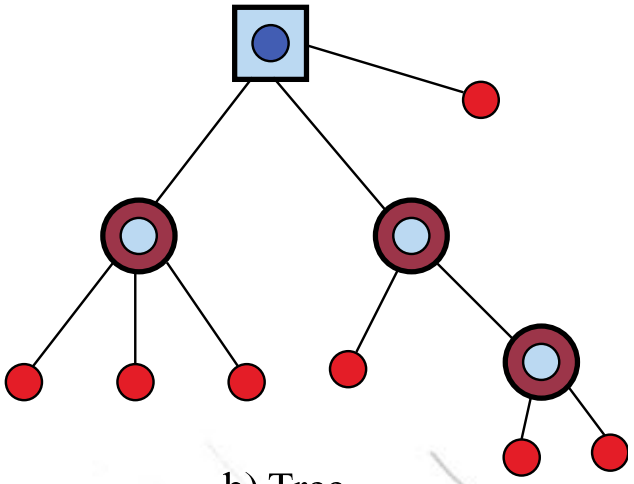
ZIGBEE

- ✓ 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

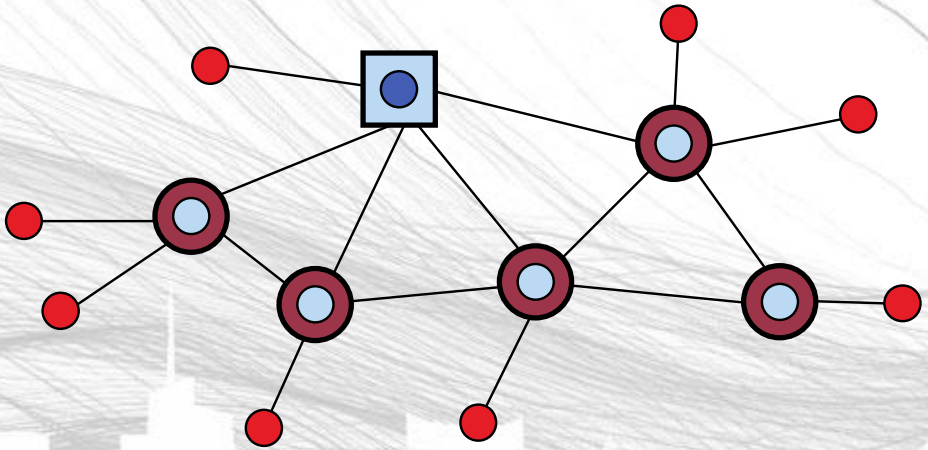
ZIGBEE NETWORK



a) Star



b) Tree



c) Mesh

ZigBee Coordinator

ZigBee Router

ZigBee End Device

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)