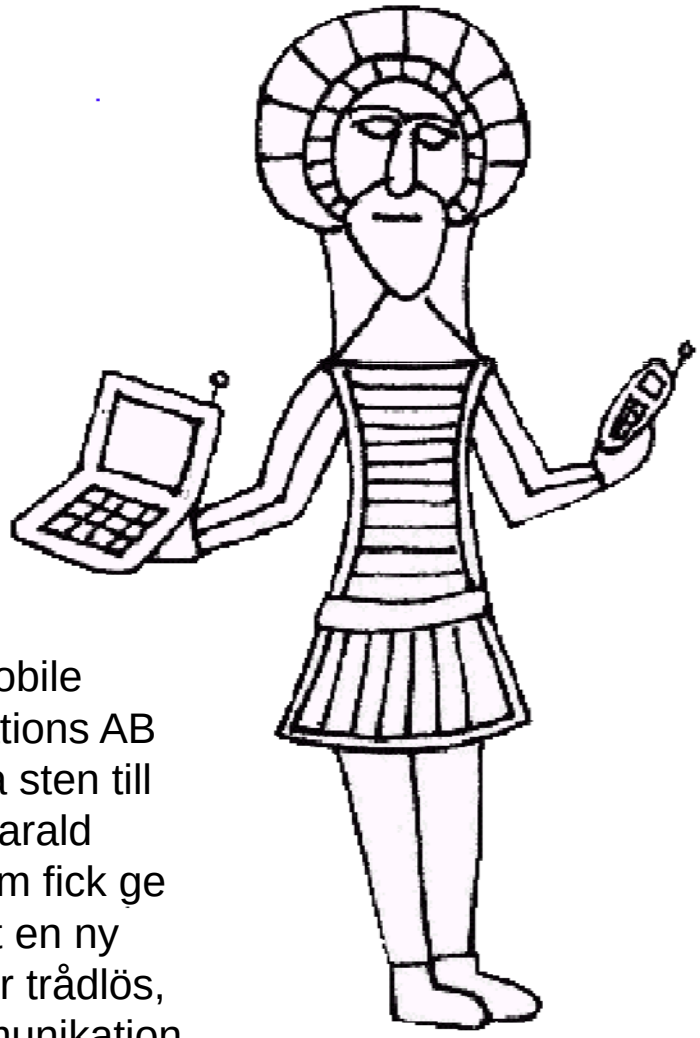
Chapter 3: Introduction to Bluetooth

Prof. Yuh-Shyan Chen
Department of CSIE
National Taipei University

一． 藍牙歷史和應用

在很久很久以前，丹麥一個叫哈拉爾德（ Harald Gormsson）的海盜，通過自己的力量統一了北歐四分五裂的國家，後來成為國王（有點像秦始皇）。這個國王喜歡吃藍梅，牙齒常常被染成藍色，由此人們都叫他“藍牙”（Bluetooth）（他的名字也可能來源於丹麥文“bla”，意思是黑色皮膚的，或“棕褐色的”，象徵著偉大的人物。）。 公元1998年，還是在北歐，一個叫愛立信的公司提出一種無線通信技術，為了使這種技術“一統天下”，取名“藍牙”。 “藍牙”技術正是取自10世紀丹麥國王哈拉爾德的別名。

History and hi-tech…



1999:
Ericsson mobile communications AB reste denna sten till minne av Harald Blåtand, som fick ge sitt namn åt en ny teknologi för trådlös, mobil kommunikation.

…and the real rune stone

Located in Jelling, Denmark,
erected by King Harald “Blåtand”
in memory of his parents.
The stone has three sides – one side showing a picture of Christ.

Inscription:
"Harald king executes these sepulchral monuments after Gorm, his father and Thyra, his mother. The Harald who won the whole of Denmark and Norway and turned the Danes to Christianity."

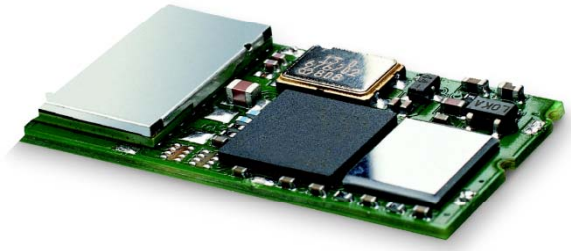
Btw: Blåtand means “of dark complexion” (not having a blue tooth…)

This could be the “original” colors of the stone.
Inscription:
“auk tani karthi kristna” (and made the Danes Christians)

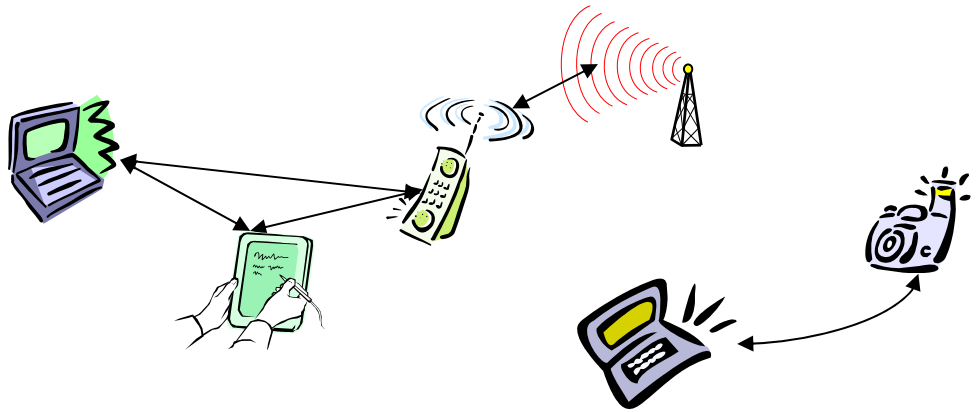
Bluetooth

Idea

- Universal radio interface for ad-hoc wireless connectivity
- Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
- Embedded in other devices, goal: 5€/device (2002: 50€/USB bluetooth)
- Short range (10 m), low power consumption, license-free 2.45 GHz ISM
- Voice and data transmission, approx. 1 Mbit/s gross data rate



One of the first modules (Ericsson).



Bluetooth

History

- 1994: Ericsson (Mattison/Haartsen), “MC-link” project
- Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
- 1998: foundation of Bluetooth SIG (Special Interest Group), (was: Bluetooth)
  www.bluetooth.org
- 1999: erection of a rune stone at Ercisson/Lund ;-)
- 2001: first consumer products for mass market, spec. version 1.1 released

Special Interest Group

- Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
- Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
- > 2500 members
- Common specification and certification of products

Bluetooth™


Bluetooth.com | The Official Bluetooth® Technology Info Site - Microsoft Internet...
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
網址(D) http://www.bluetooth.com/bluetooth/
移至 連結
Google SIG Go Bookmarks 32 blocked Check AutoLink Settings
Bluetooth SIG Shop | Bluetooth.org
Bluetooth
Experience More
Learn
Connect
Apply
About the Bluetooth SIG
Press & Analysts
Bluetooth Assembler
Select Language
search site enter keywords here search >
BLUETOOTH EXPERIENCES WITH YOUR MUSIC
Rock out wherever you go! Experience more of your Music in more places
Featured Product
Hamburg MP57
Welcome Longhorns®!
Register now for a chance to win 2007 Bowl Game Tickets wherever the Longhorns play! Submit your
SIGnature Q4 2007
SIGnature
Get the most up-to-date news in Bluetooth technology with the latest issue of SIGnature. Read now about new technologies and use
News
It's going to be a Bluetooth Christmas
26 Sept. 2007 | Mobile Choice UK
http://www.bluetooth.com/Bluetooth/Apply/Experience_Music.htm
網際網路
開始
22:53
Monday

Characteristics

2.4 GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing

- Channel 0: 2402 MHz … channel 78: 2480 MHz
- G-FSK modulation, 1-100 mW (miniwatt, a unit of power equal to one thousandth of a watt) transmit power

FHSS and TDD

- Frequency hopping with 1600 hops/s
- Hopping sequence in a pseudo random fashion, determined by a master
- Time division duplex for send/receive separation

Voice link – SCO (Synchronous Connection Oriented)

- FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched

Data link – ACL (Asynchronous ConnectionLess)

- Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched

Topology

- Overlapping piconets (stars) forming a scatternet

Piconet

Collection of devices connected in an ad hoc fashion

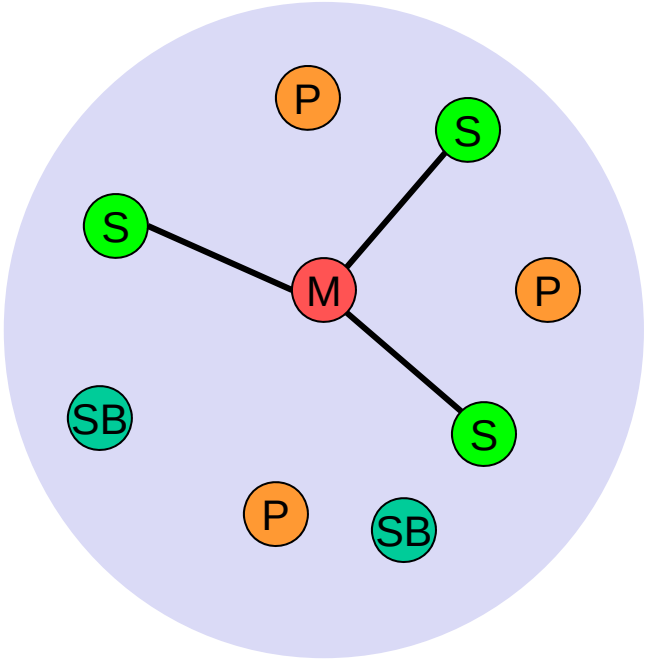
One unit acts as master and the others as slaves for the lifetime of the piconet

Master determines hopping pattern, slaves have to synchronize

Each piconet has a unique hopping pattern

Participation in a piconet = synchronization to hopping sequence

Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)



M=Master
S=Slave
P=Parked
SB=Standby

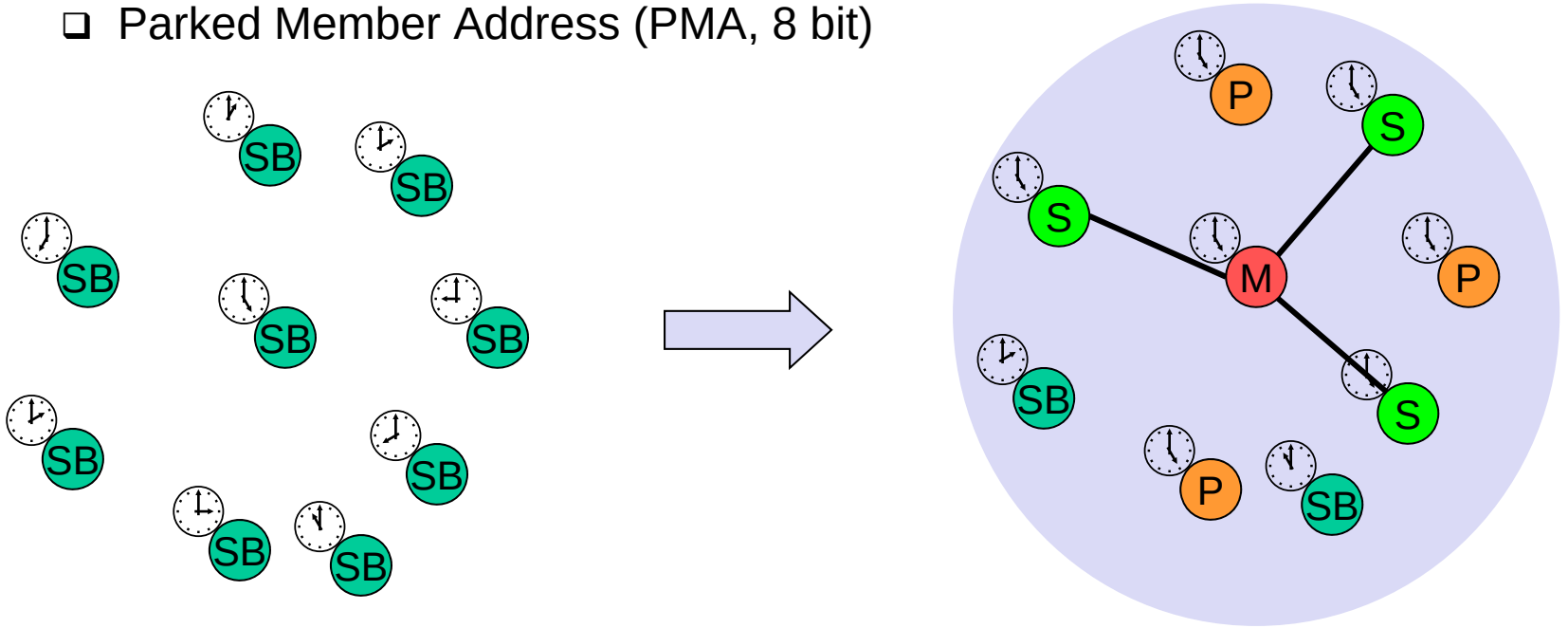
Forming a piconet

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)



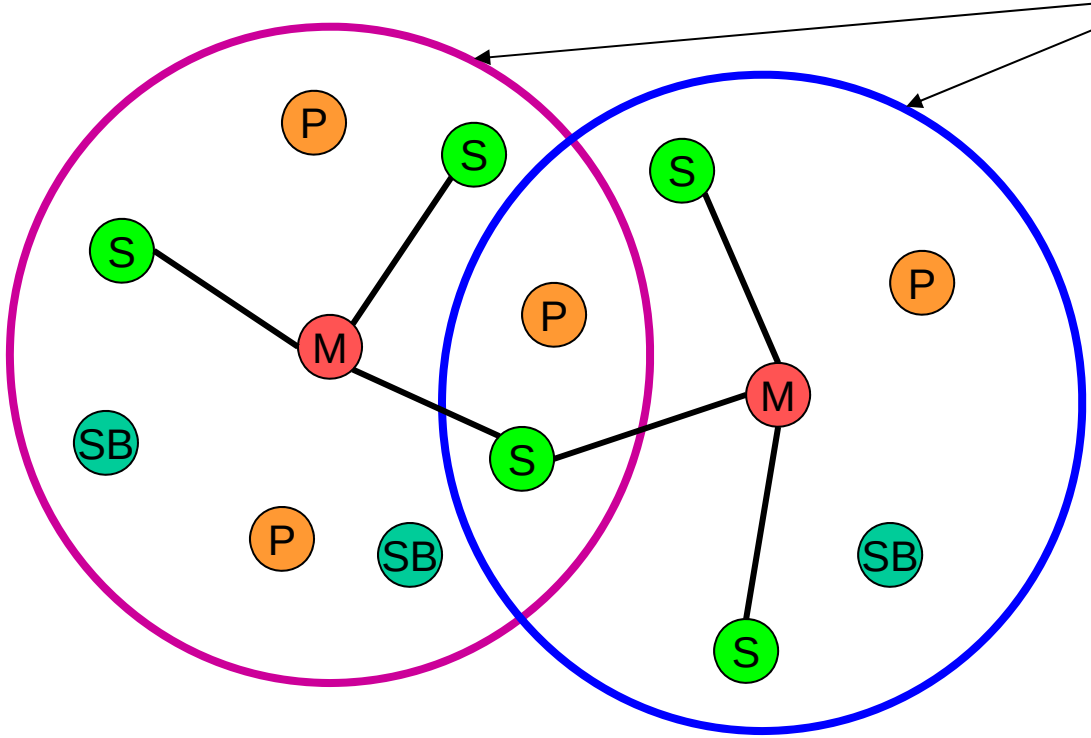
Scatternet

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

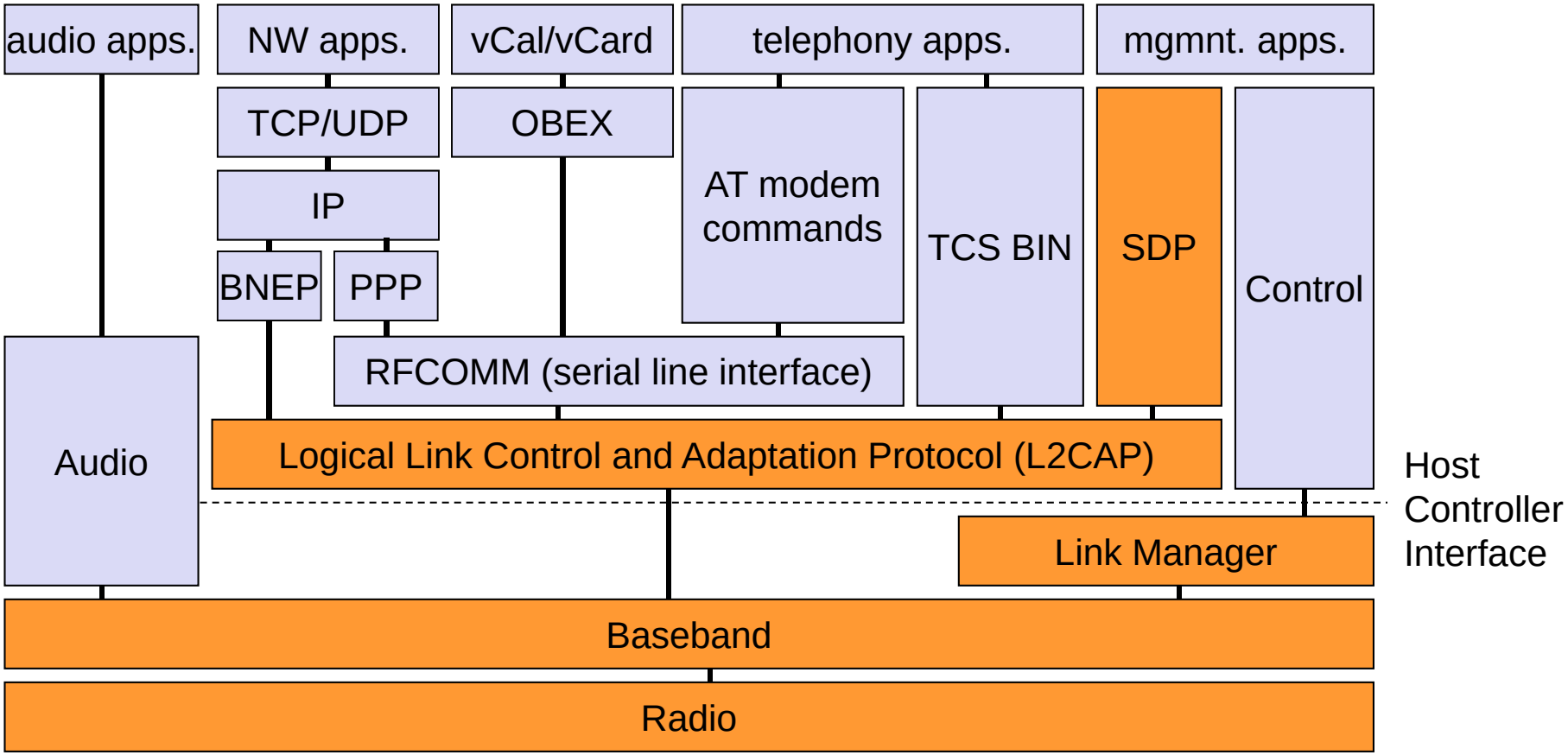
- Devices jumping back and forth between the piconets



Piconets (each with a capacity of < 1 Mbit/s)

M=Master
S=Slave
P=Parked
SB=Standby

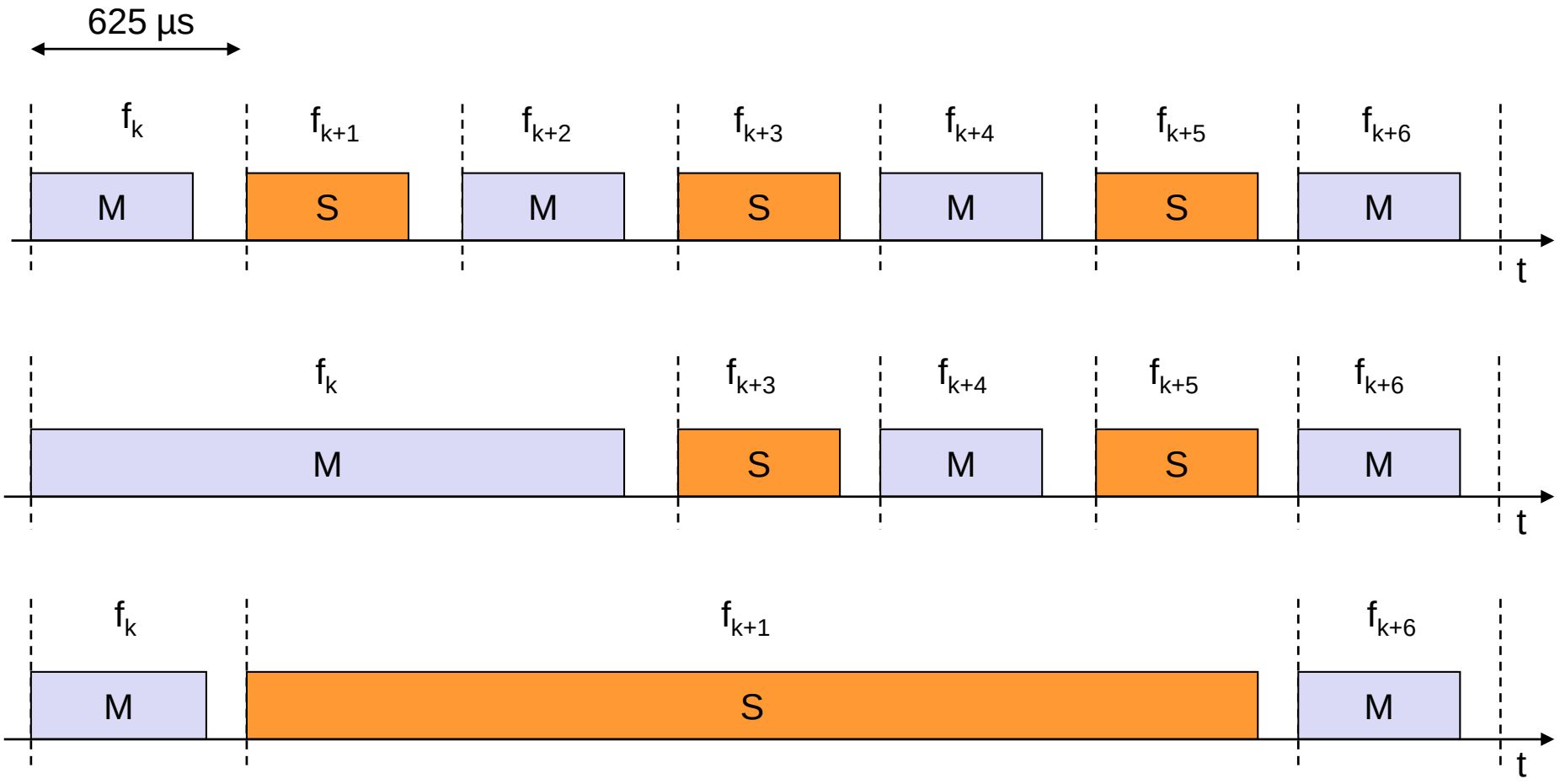
Bluetooth protocol stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

Frequency selection during data transmission



Property

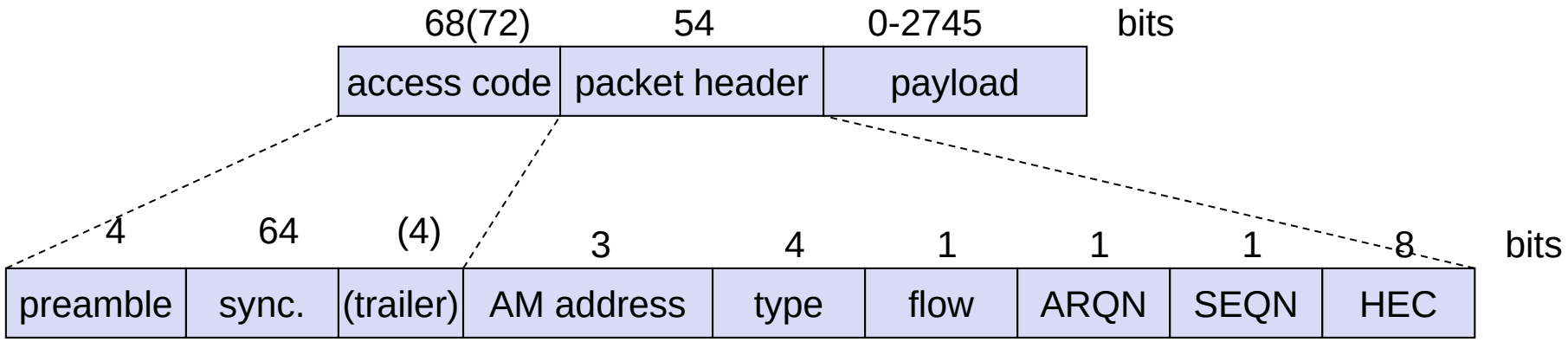
The master always uses the even frequency slots, and odd slots are for the slaves.

Baseband

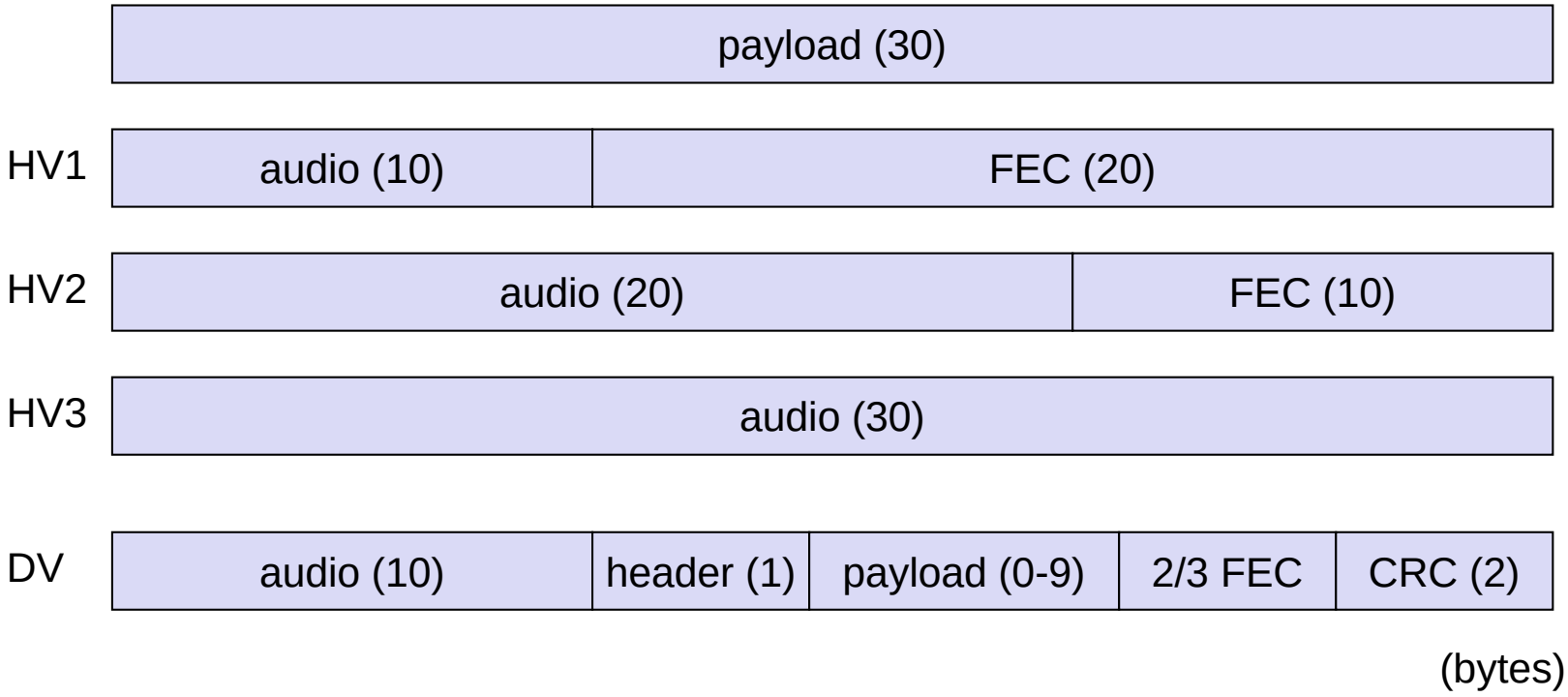
Piconet/channel definition

Low-level packet definition

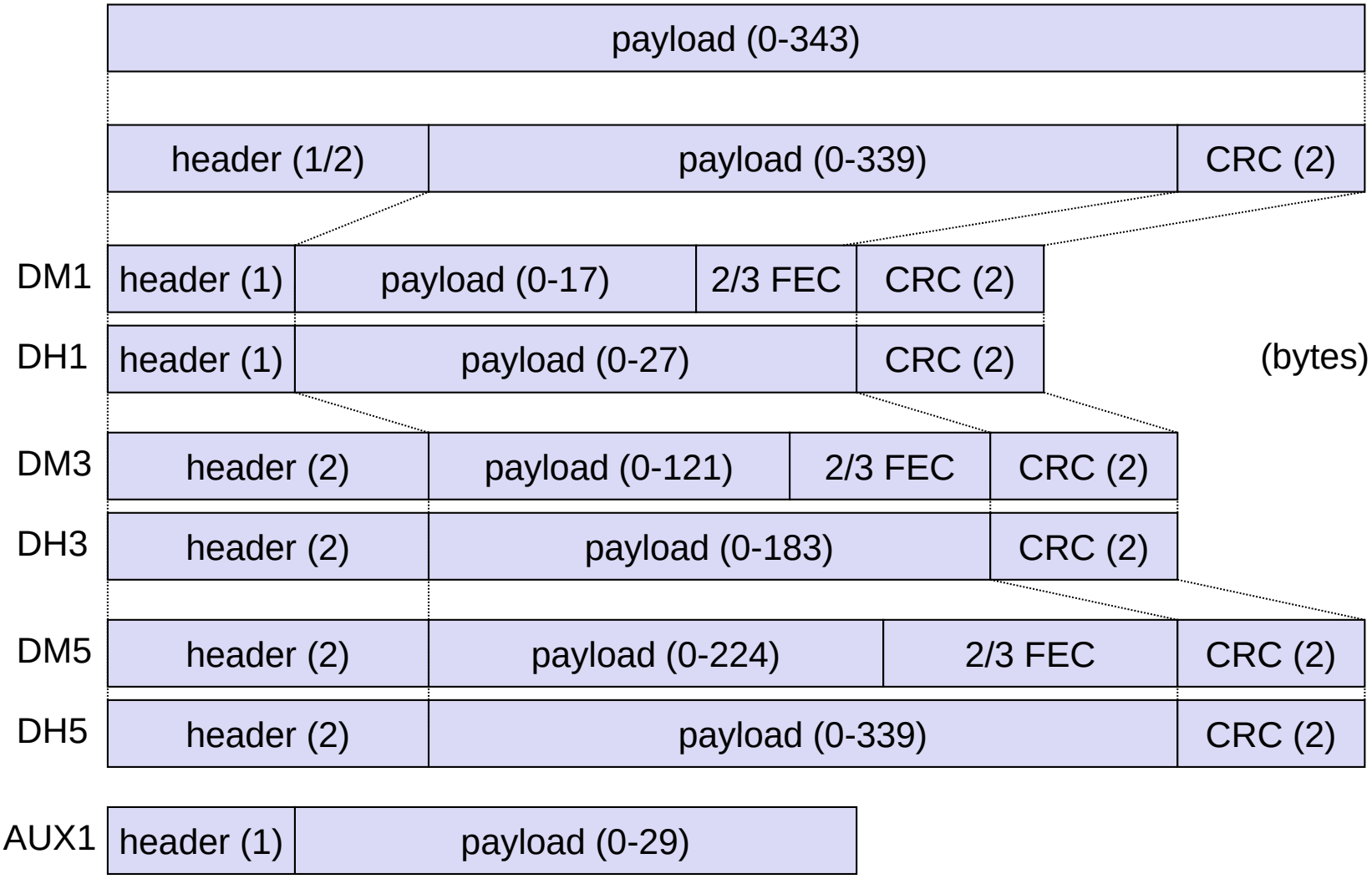
- Access code
  - Channel, device access, e.g., derived from master
- Packet header
  - 1/3-FEC, active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum



SCO payload types



ACL Payload types

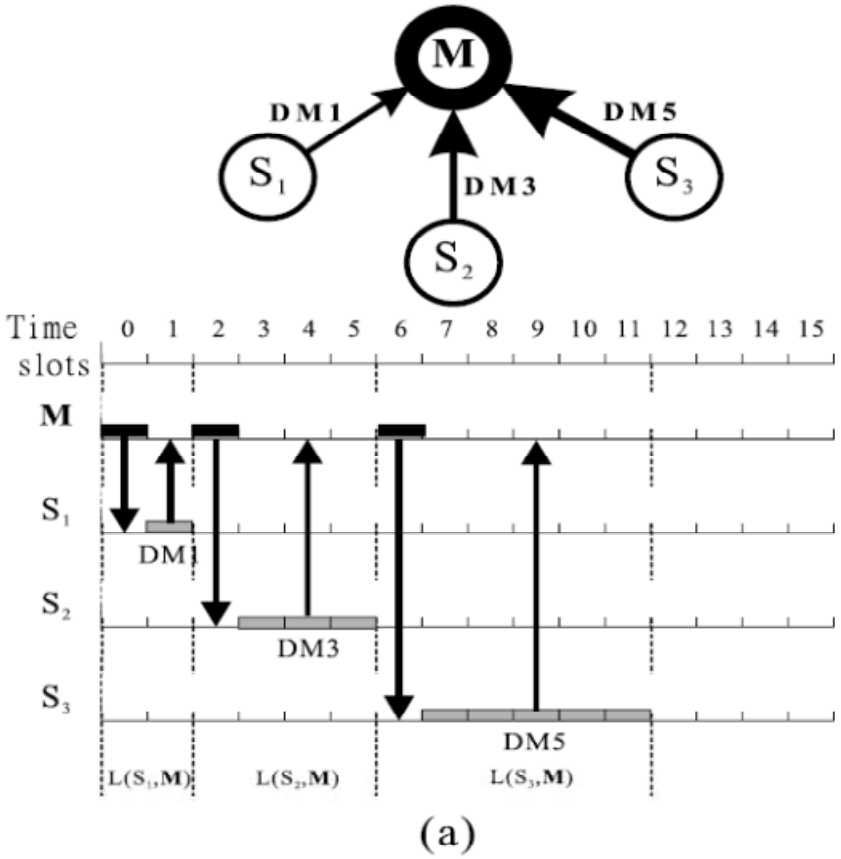


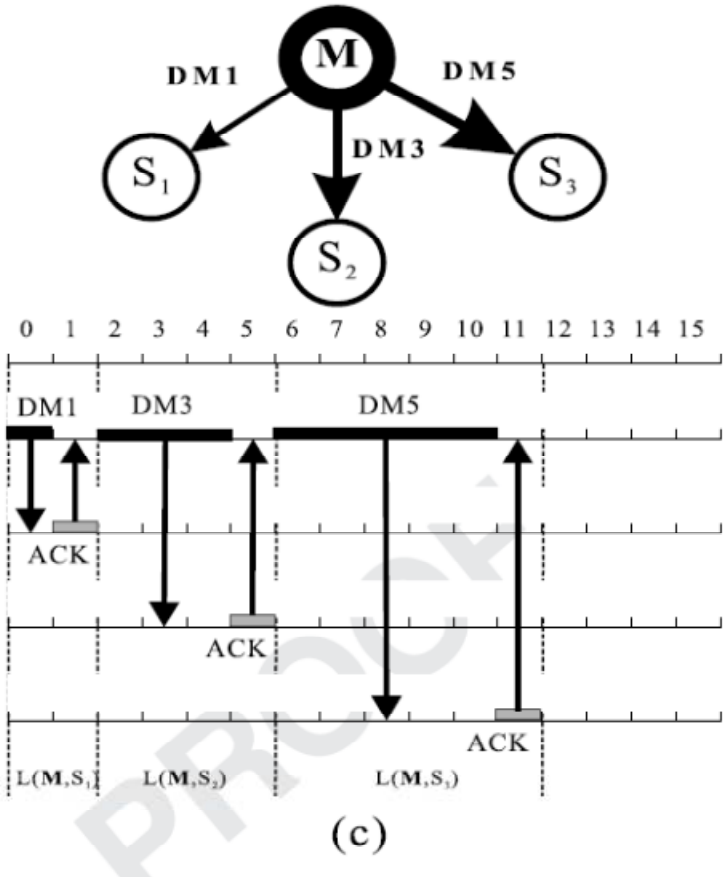
Baseband data rates

	Type	Payload Header [byte]	User Payload [byte]	FEC	CRC	Symmetric max. Rate [kbit/s]	Asymmetric max. Rate [kbit/s] Forward	Reverse
ACL 1 slot	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
3 slot	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
5 slot	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
SCO	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 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D		

*D*ata *M*edium/*H*igh rate, *H*igh-quality *V*oice, *D*ata and *V*oice

Example


M
DM1
DM5
DM3
S1
S2
S3
Time slots
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
M
S1
S2
S3
DM1
DM3
DM5
L(S1,M)
L(S2,M)
L(S3,M)
(a)


M
DM1
DM5
DM3
S1
S2
S3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
DM1
DM3
DM5
ACK
ACK
ACK
L(M,S1)
L(M,S2)
L(M,S3)
(c)

Baseband link types

Polling-based TDD packet transmission

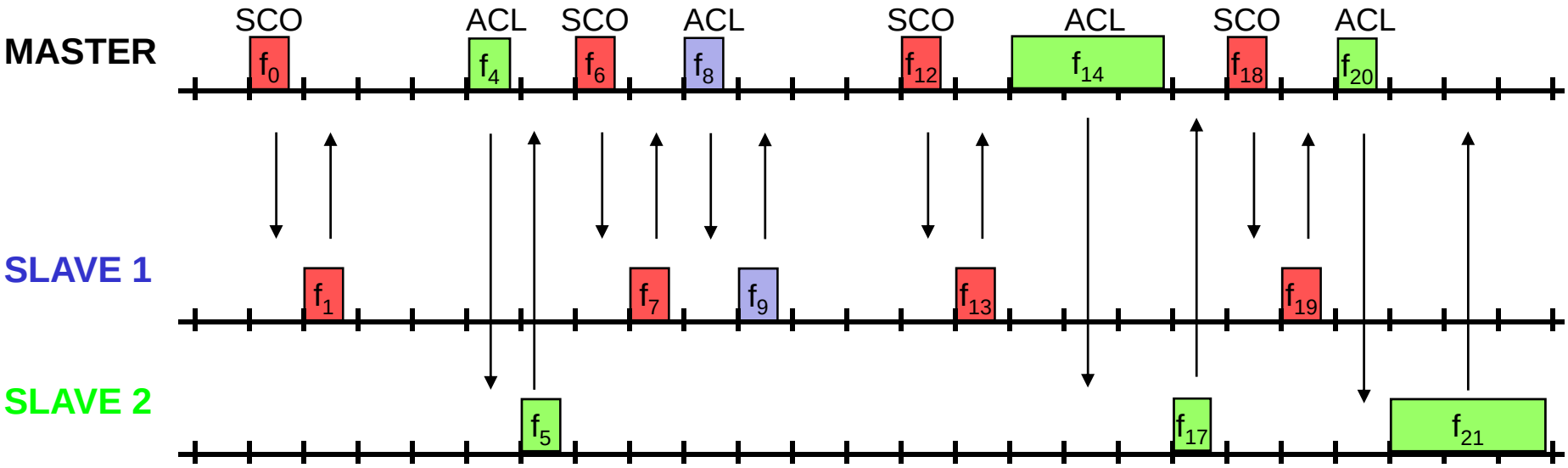
- 625μs slots, master polls slaves

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



Robustness

Slow frequency hopping with hopping patterns determined by a master

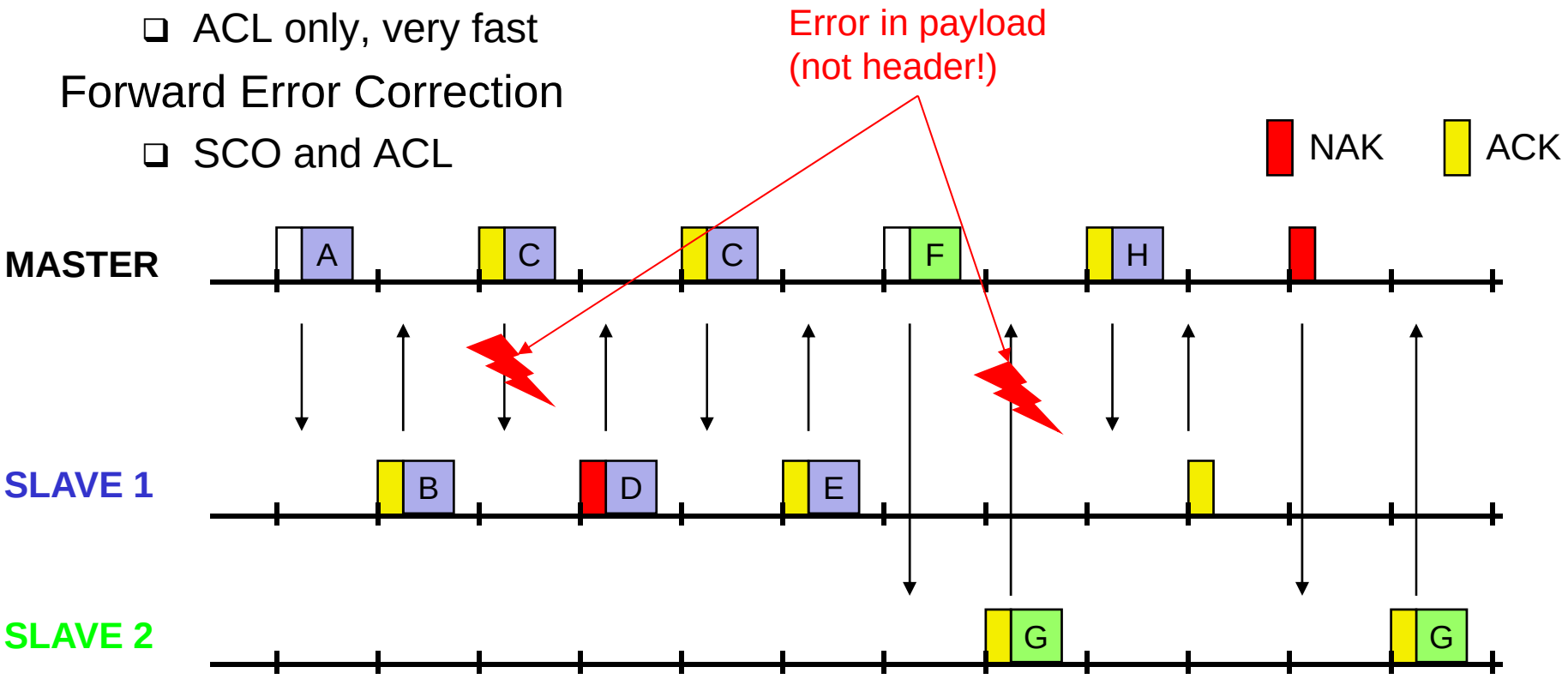
- Protection from interference on certain frequencies
- Separation from other piconets (FH-CDMA)

Retransmission

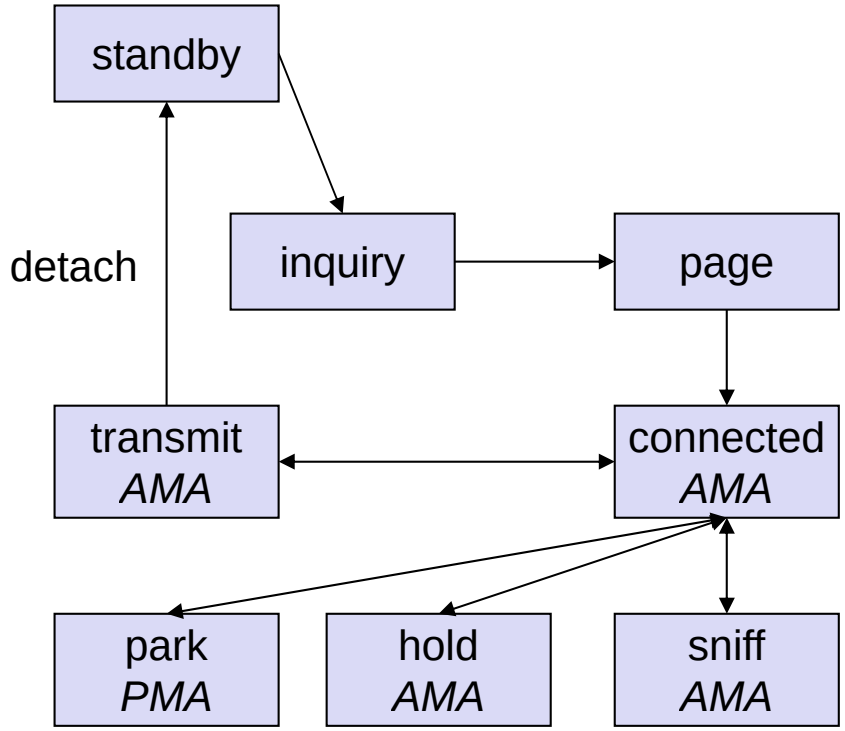
- ACL only, very fast

Forward Error Correction

- SCO and ACL



Baseband states of a Bluetooth device



AMA: 3-bit active member address

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

Example: Power consumption/CSR BlueCore2

Typical Average Current Consumption (1)

VDD=1.8V Temperature = 20°C

mini ampere = 10^{-3} ampere

Mode	
SCO connection HV3 (1s interval Sniff Mode) (Slave)	26.0 mA
SCO connection HV3 (1s interval Sniff Mode) (Master)	26.0 mA
SCO connection HV1 (Slave)	53.0 mA
SCO connection HV1 (Master)	53.0 mA
ACL data transfer 115.2kbps UART (Master)	15.5 mA
ACL data transfer 720kbps USB (Slave)	53.0 mA
ACL data transfer 720kbps USB (Master)	53.0 mA
ACL connection, Sniff Mode 40ms interval, 38.4kbps UART	4.0 mA
ACL connection, Sniff Mode 1.28s interval, 38.4kbps UART	0.5 mA
Parked Slave, 1.28s beacon interval, 38.4kbps UART	0.6 mA
Standby Mode (Connected to host, no RF activity)	47.0 µA
Deep Sleep Mode(2)	20.0 µA

Notes:

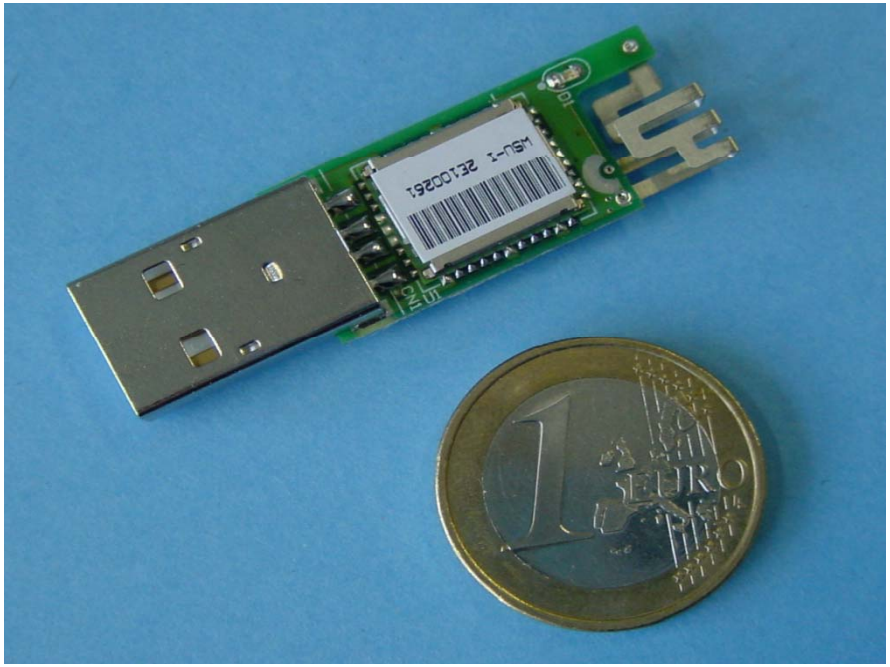
(1) Current consumption is the sum of both BC212015A and the flash.

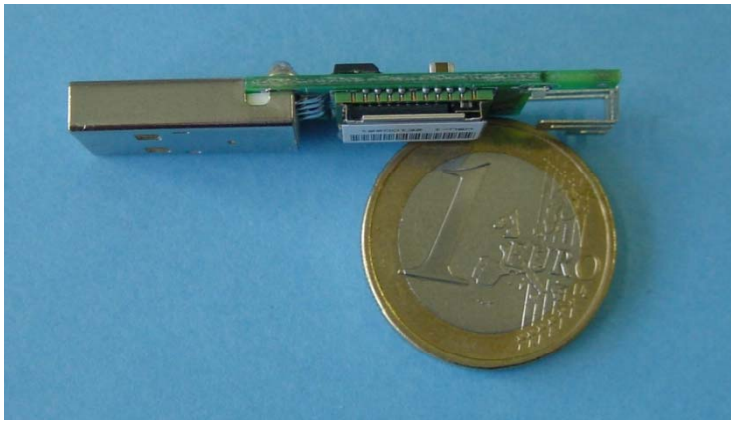
(2) Current consumption is for the BC212015A device only.

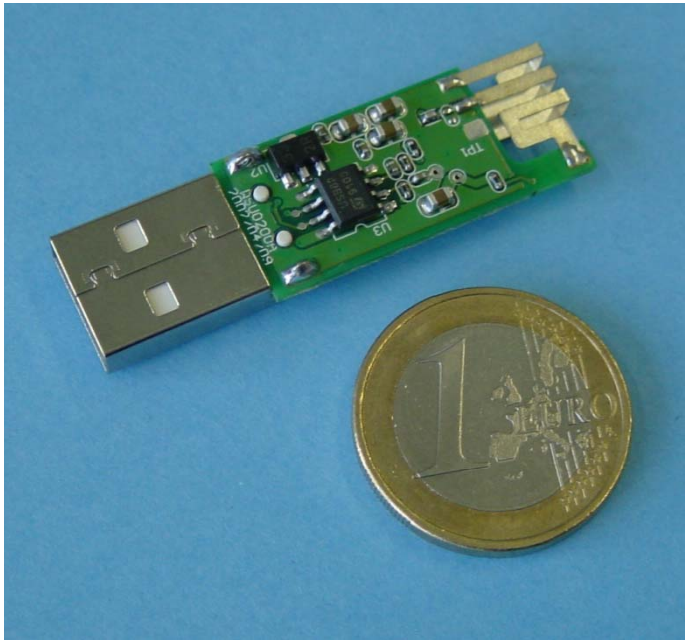
(More: www.csr.com)

micro ampere = 10^{-6} ampere

Example: Bluetooth/USB adapter (2002: 50€)







L2CAP - Logical Link Control and Adaptation Protocol

Simple data link protocol on top of baseband

Connection oriented, connectionless, and signalling channels

Protocol multiplexing

- RFCOMM, SDP, telephony control

Segmentation & reassembly

- Up to 64kbyte user data, 16 bit CRC used from baseband

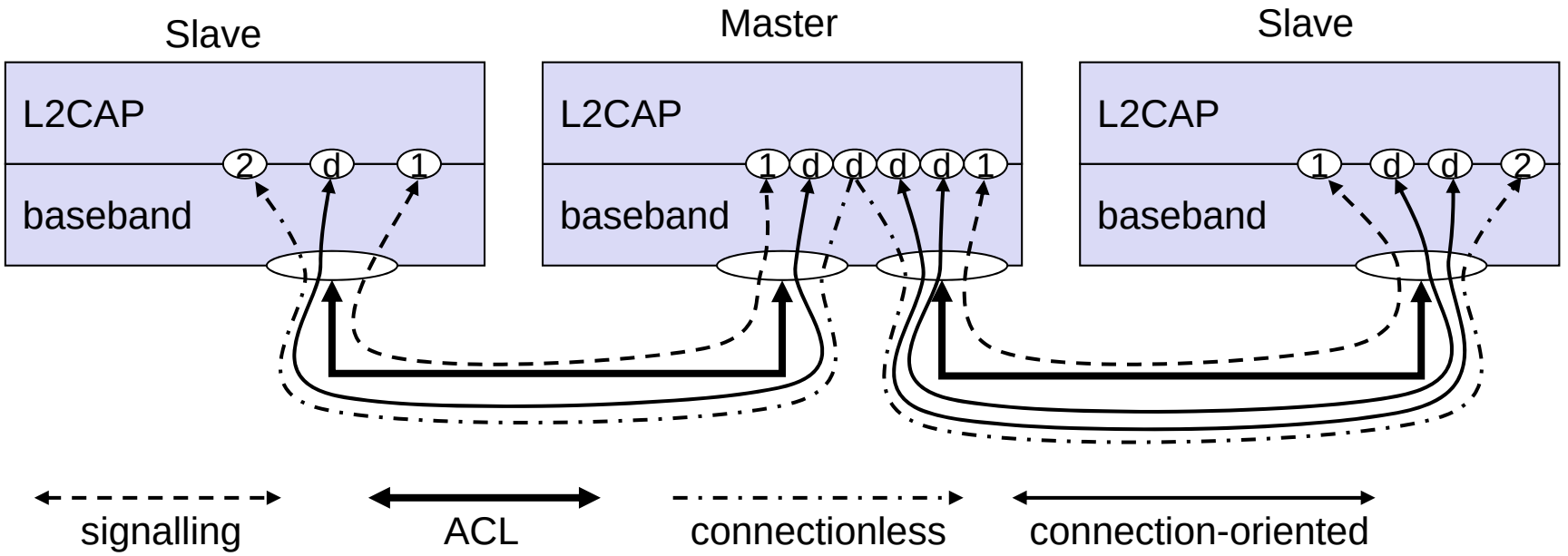
QoS flow specification per channel

- Follows RFC 1363, specifies delay, jitter, bursts, bandwidth

Group abstraction

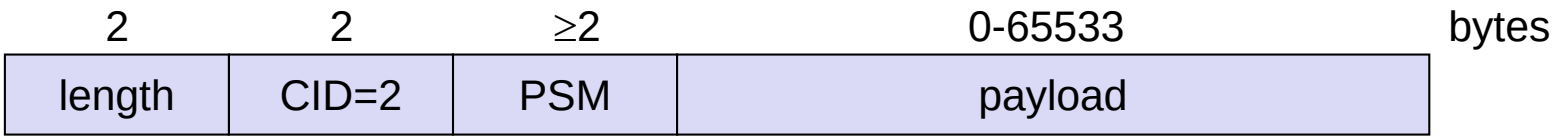
- Create/close group, add/remove member

L2CAP logical channels

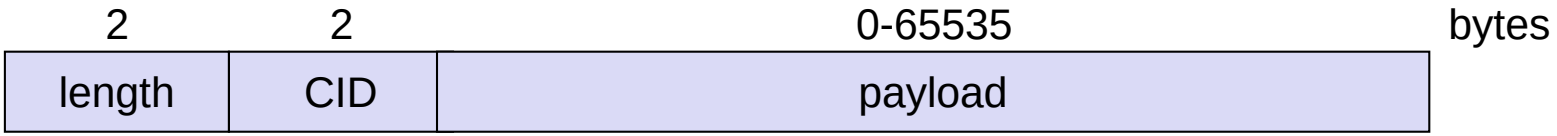


L2CAP packet formats

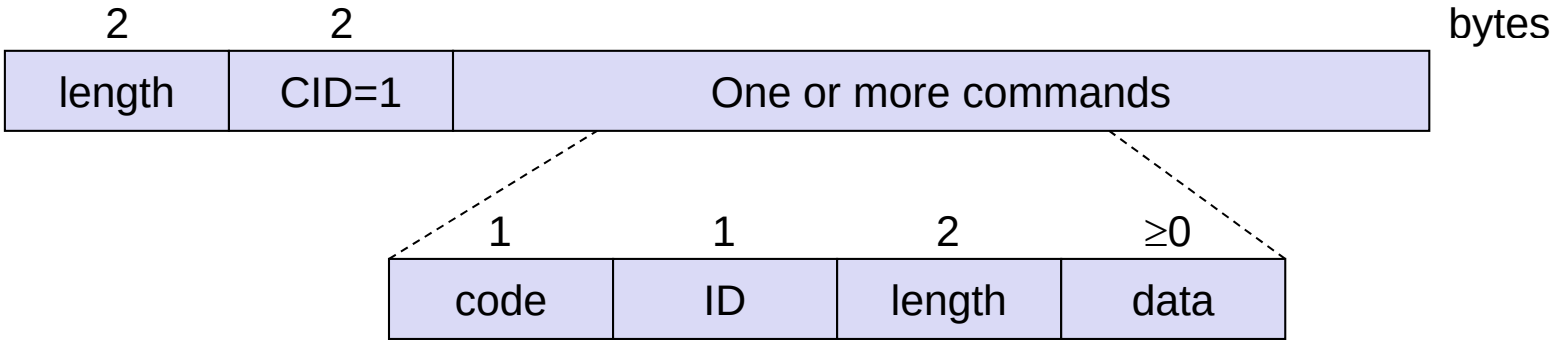
Connectionless PDU



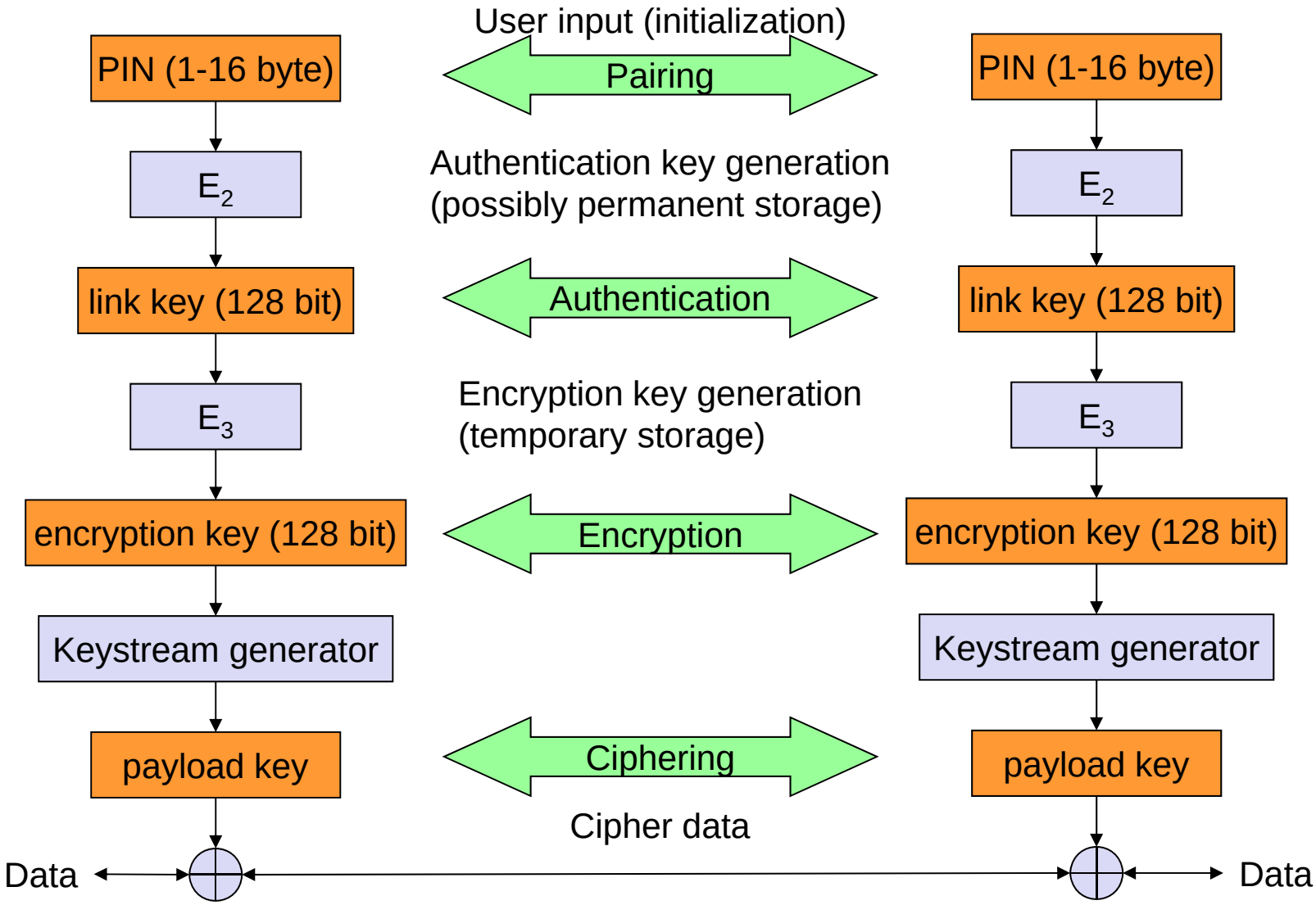
Connection-oriented PDU



Signalling command PDU



Security



SDP – Service Discovery Protocol

Inquiry/response protocol for discovering services

- Searching for and browsing services in radio proximity
- Adapted to the highly dynamic environment
- Can be complemented by others like SLP, Jini, Salutation, …
- Defines discovery only, not the usage of services
- Caching of discovered services
- Gradual discovery

Service record format

- Information about services provided by attributes
- Attributes are composed of an 16 bit ID (name) and a value
- values may be derived from 128 bit Universally Unique Identifiers (UUID)

Additional protocols to support legacy protocols/apps.

RFCOMM

- Emulation of a serial port (supports a large base of legacy applications)
- Allows multiple ports over a single physical channel

Telephony Control Protocol Specification (TCS)

- Call control (setup, release)
- Group management

OBEX

- Exchange of objects, IrDA replacement

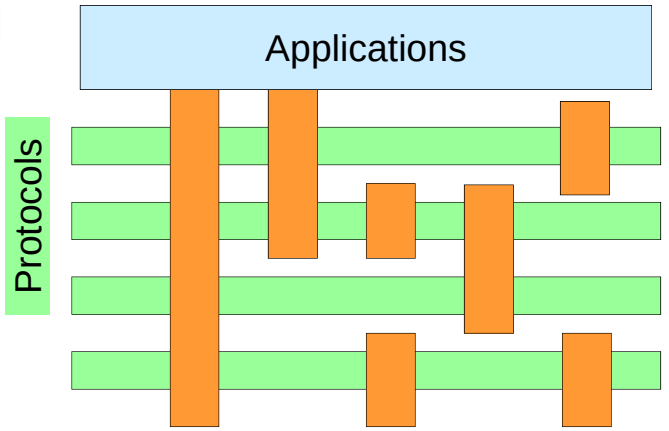
WAP

- Interacting with applications on cellular phones

Profiles

Represent default solutions for a certain usage model
- Vertical slice through the protocol stack
- Basis for interoperability

Generic Access Profile
Service Discovery Application Profile
Cordless Telephony Profile
Intercom Profile
Serial Port Profile
Headset Profile
Dial-up Networking Profile
Fax Profile
LAN Access Profile
Generic Object Exchange Profile
Object Push Profile
File Transfer Profile
Synchronization Profile



Additional Profiles
Advanced Audio Distribution
PAN
Audio Video Remote Control
Basic Printing
Basic Imaging
Extended Service Discovery
Generic Audio Video Distribution
Hands Free
Hardcopy Cable Replacement

WPAN: **IEEE 802.15.1** – Bluetooth

Data rate
- Synchronous, connection-oriented: 64 kbit/s
- Asynchronous, connectionless
  - 433.9 kbit/s symmetric
  - 723.2 / 57.6 kbit/s asymmetric

Transmission range
- POS (Personal Operating Space) up to 10 m
- with special transceivers up to 100 m

Frequency
- Free 2.4 GHz ISM-band

Security
- Challenge/response (SAFER+), hopping sequence

Cost
- 50€ adapter, drop to 5€ if integrated

Availability
- Integrated into some products, several vendors

Connection set-up time
- Depends on power-mode
- Max. 2.56s, avg. 0.64s

Quality of Service
- Guarantees, ARQ/FEC

Manageability
- Public/private keys needed, key management not specified, simple system integration

Special Advantages/Disadvantages
- Advantage: already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer to peer, scatternets
- Disadvantage: interference on ISM-band, limited range, max. 8 devices/network&master, high set-up latency

WPAN: **IEEE 802.15.2**

802.15.2: Coexistance

- Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference

WPAN: **IEEE 802.15.3**

802.15.3: High-Rate

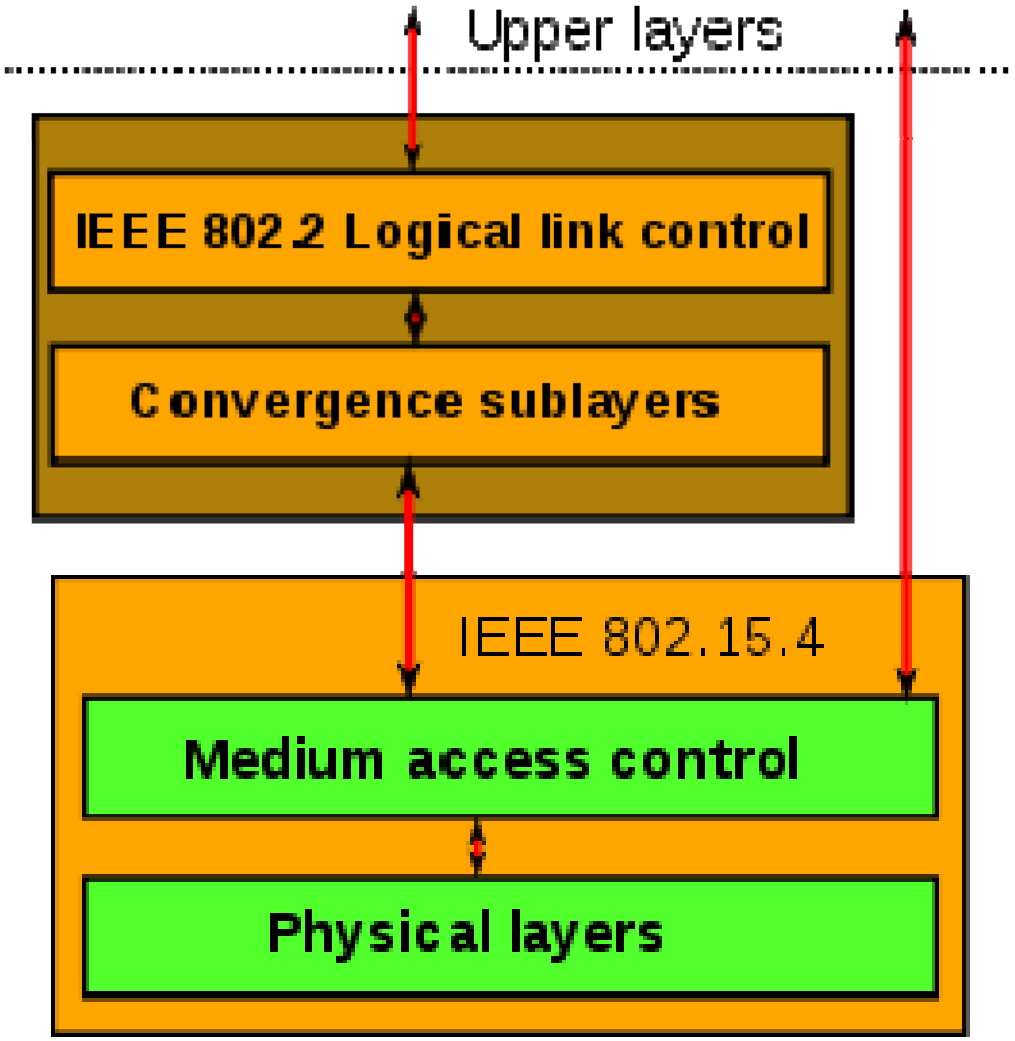
- Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
- Data Rates: 11, 22, 33, 44, 55 Mbit/s
- Quality of Service isochronous protocol
- Ad hoc peer-to-peer networking
- Security
- Low power consumption
- Low cost
- Designed to meet the demanding requirements of portable consumer imaging and multimedia applications

WPAN: **IEEE 802.15.4**

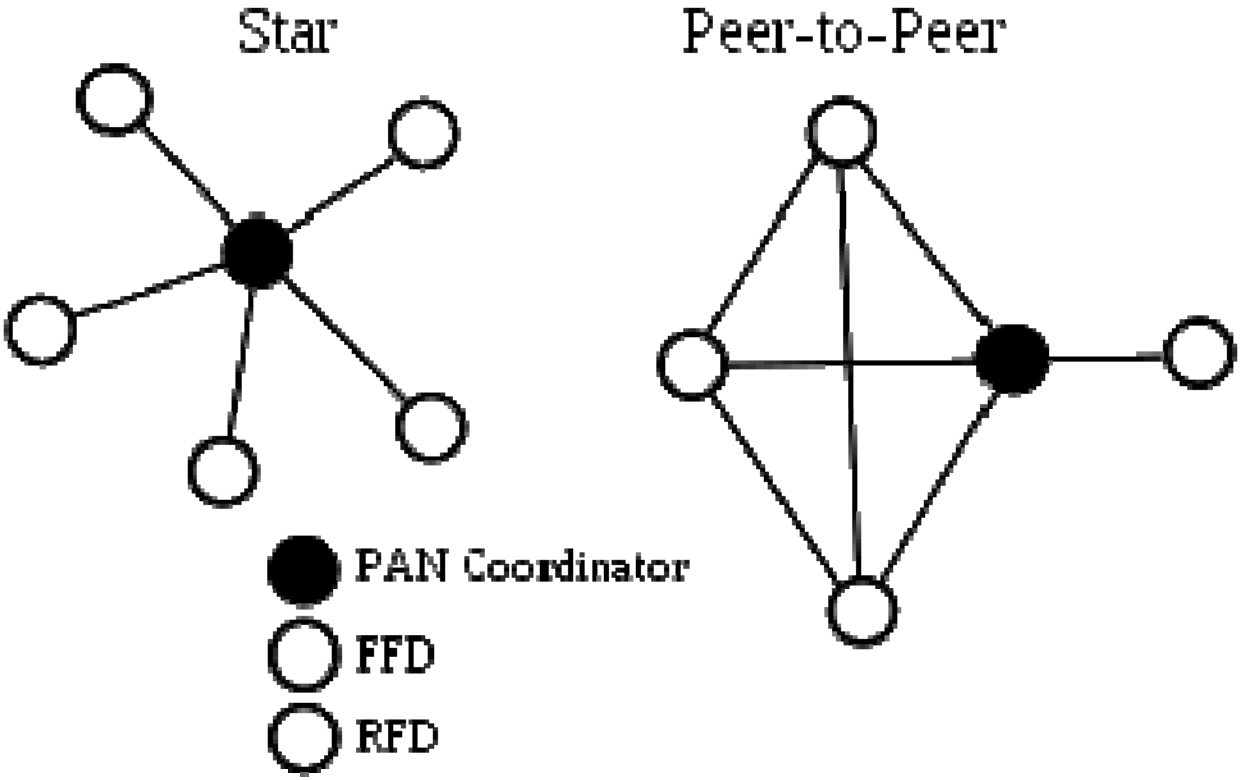
802.15.4: Low-Rate, Very Low-Power

- Low data rate solution with multi-month to multi-year battery life and very low complexity
- Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
- Data rates of 20-250 kbit/s, latency down to 15 ms
- Master-Slave or Peer-to-Peer operation
- Support for critical latency devices, such as joysticks
- CSMA/CA channel access (data centric), slotted (beacon) or unslotted
- Automatic network establishment by the PAN coordinator
- Dynamic device addressing, flexible addressing format
- Fully handshaked protocol for transfer reliability
- Power management to ensure low power consumption
- 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band

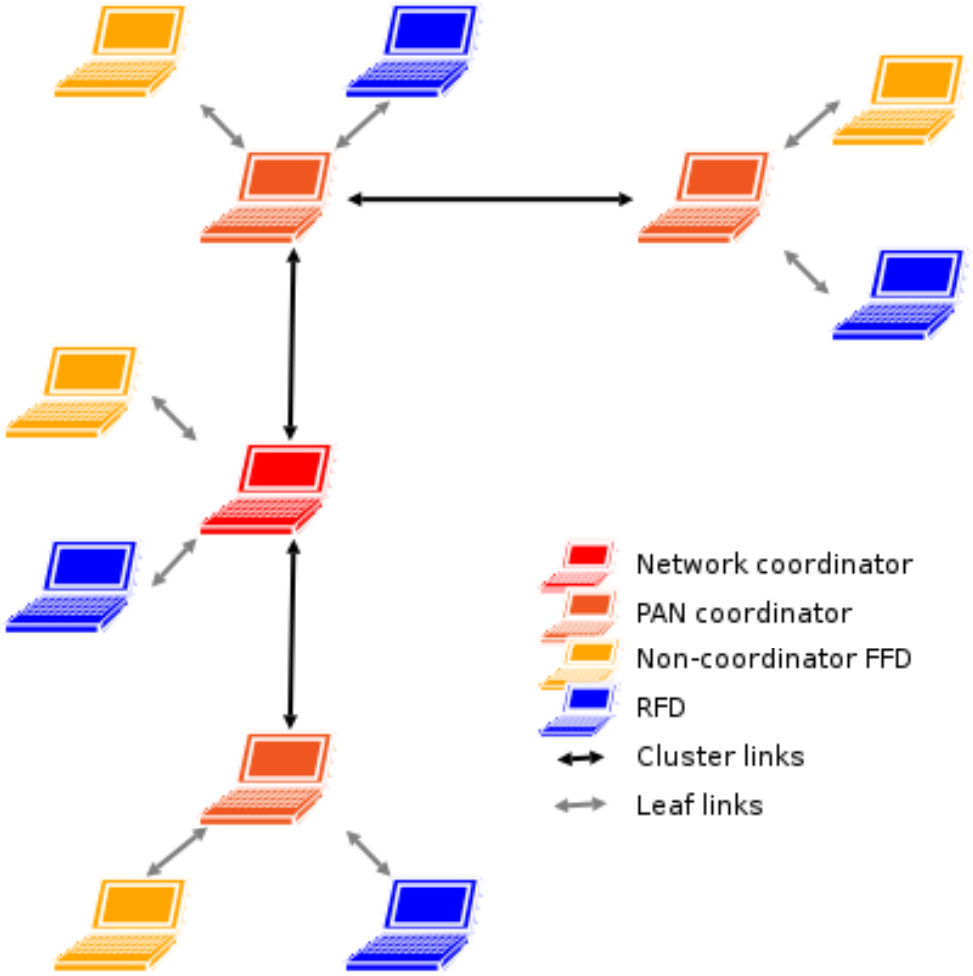
IEEE 802.15.4 Protocol Stack



Networks can be built as either peer-to-peer or star networks



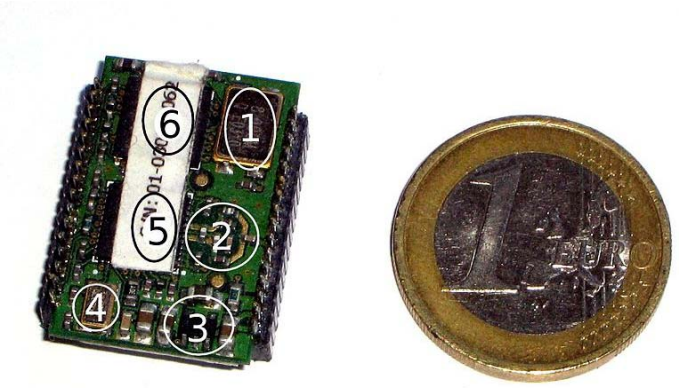
IEEE 802.15.4 Cluster Tree



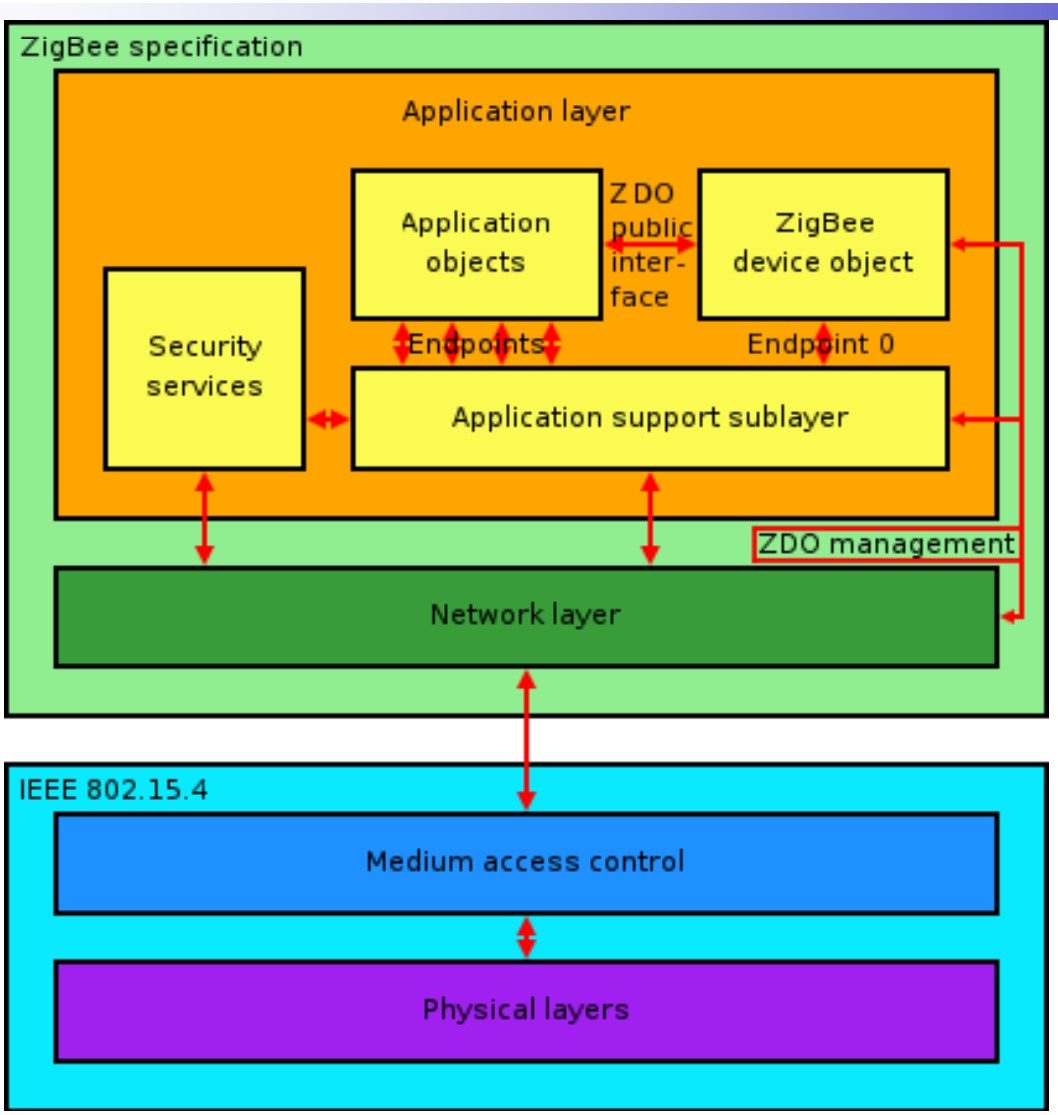
ZigBee

- **ZigBee** is a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2003 standard for wireless personal area networks (WPANs), such as wireless headphones connecting with cell phones via short-range radio.
- The technology defined by the ZigBee specification is intended to be simpler and less expensive than other WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking.

ZigBee module.



ZigBee protocol stack



6LoWPAN

- **6LoWPAN** is an acronym of *IPv6 over Low power Wireless Personal Area Networks*. 6lowpan is the name of a working group in the internet area of the IETF.
- The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices,"[2] and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things.
- The 6lowpan group has defined **encapsulation** and **header compression** mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15.4 based networks.
  - IPv4 and IPv6 are the work horses for data delivery for **local-area networks**, **metropolitan area networks**, and **wide-area networks** such as the Internet. Likewise, IEEE 802.15.4 devices provide sensing communication-ability in the wireless domain. The inherent natures of the two networks though, is different.
- The base specification developed by the 6lowpan IETF group is RFC 4944. The problem statement document is RFC 4919.

Homework #3:

1. What's piconet and scatternet in Bluetooth networks ?
2. What's ACL and SCO in Bluetooth networks ?