REAL-TIME NETWORKS
intro to wireless, IEEE 802.11 and Bluetooth

Prof. J.-D. Decotignie

CSEM Centre Suisse d'Electronique et de Microtechnique SA

Jaquet-Droz 1, 2007 Neuchâtel

jean-dominique.decotignie@csem.ch

The Troy war

Troy –
Lemnos -
Mount Athos -
Euboea -
Euripos -
Plain of Asopos -
Mount Kithairon -
Saronic Gulf -
Argos

Chappe

More Recently

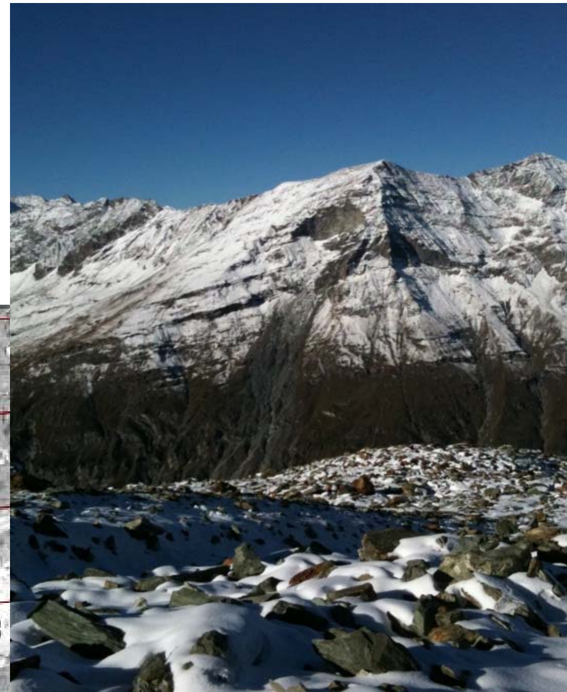
assumptions

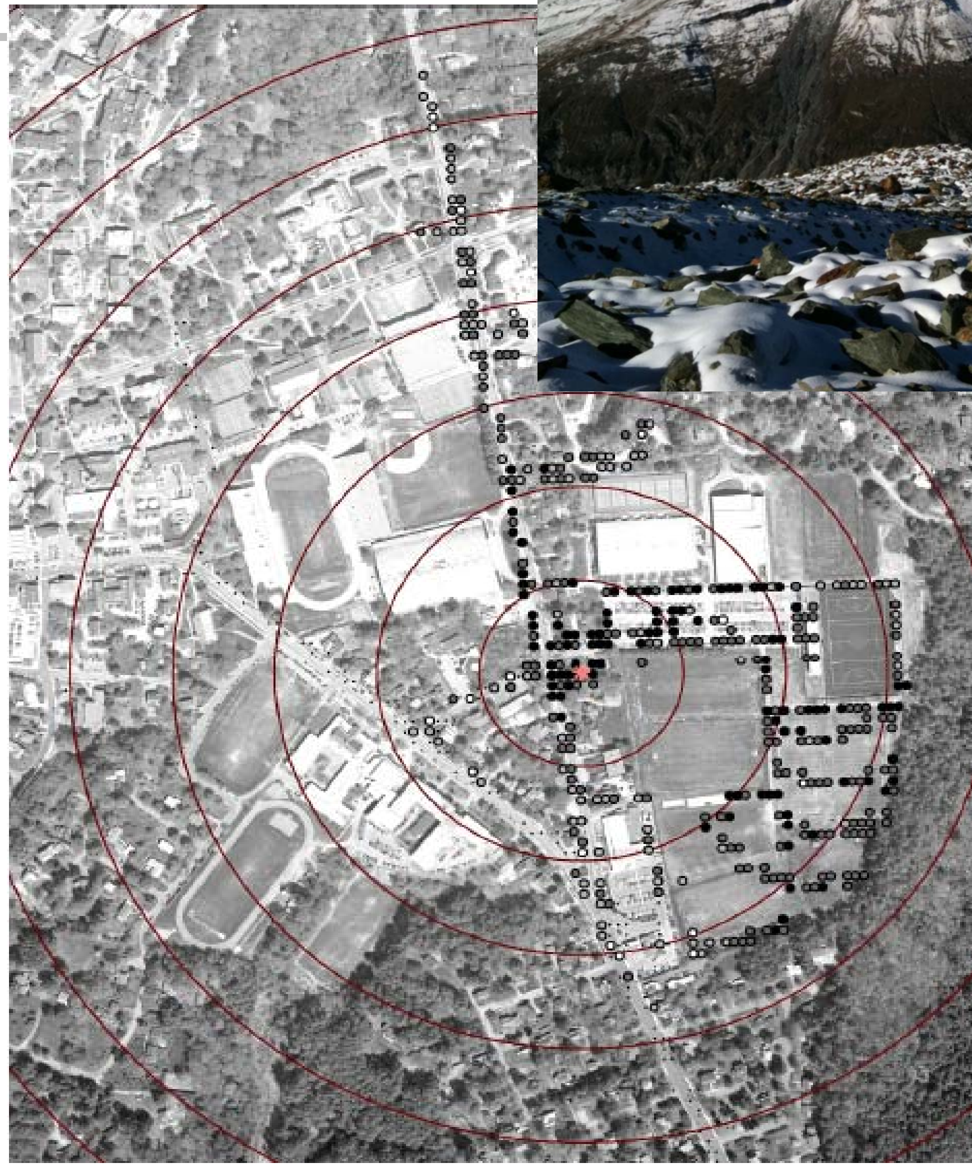
Myths about wireless transmission

- The world is flat & radio transmission area is circular
  - signal strength is a simple function of distance
- All radios have equal range
- Link quality does not change
  - if I can hear you, you can hear me & if I can hear you at all, I can hear you perfectly
- The only source of packet loss is collision
- Broadcast is for free
- Energy is proportional to the number of packets and their size
- Duty cycling is the only way to reduce energy consumption

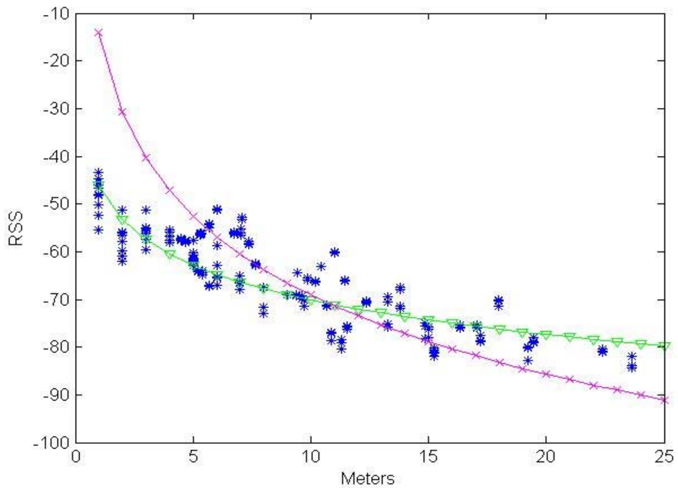
“transm. area is circular” “the world is flat”

- radio coverage is not at all circular
  - obstacles, height, fading, …
- signal strength is loosely related with distance

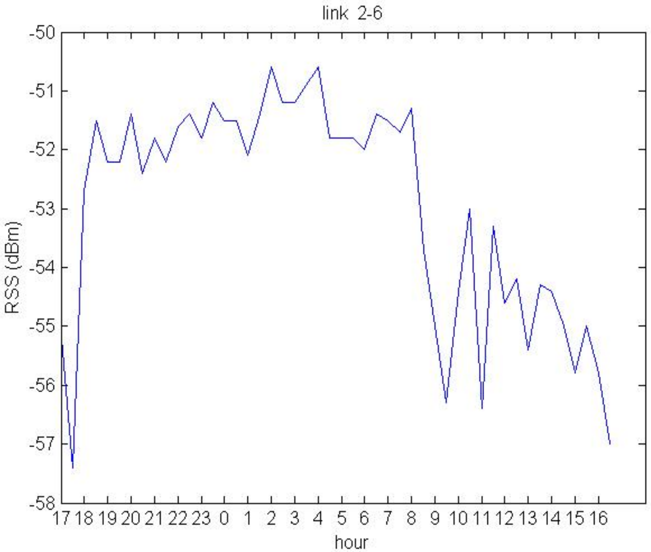


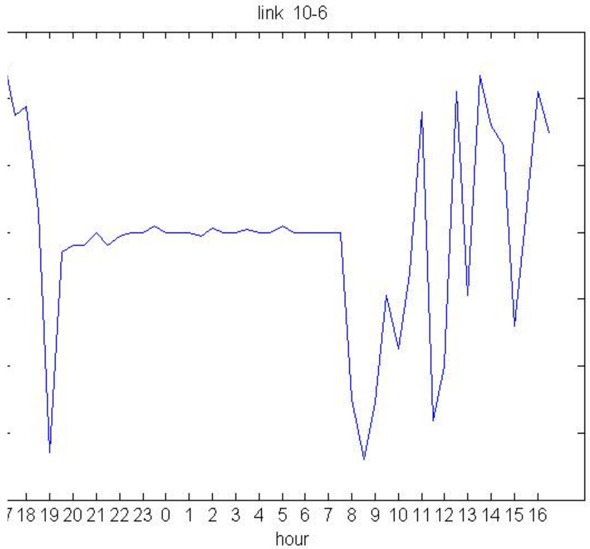


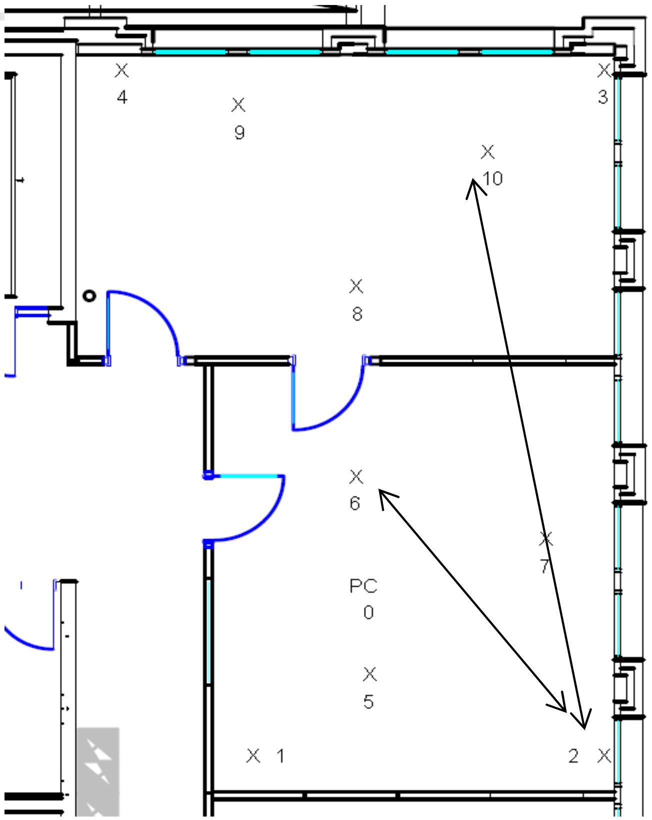
source: D. Kotz et al., 2003



“link quality does not change”



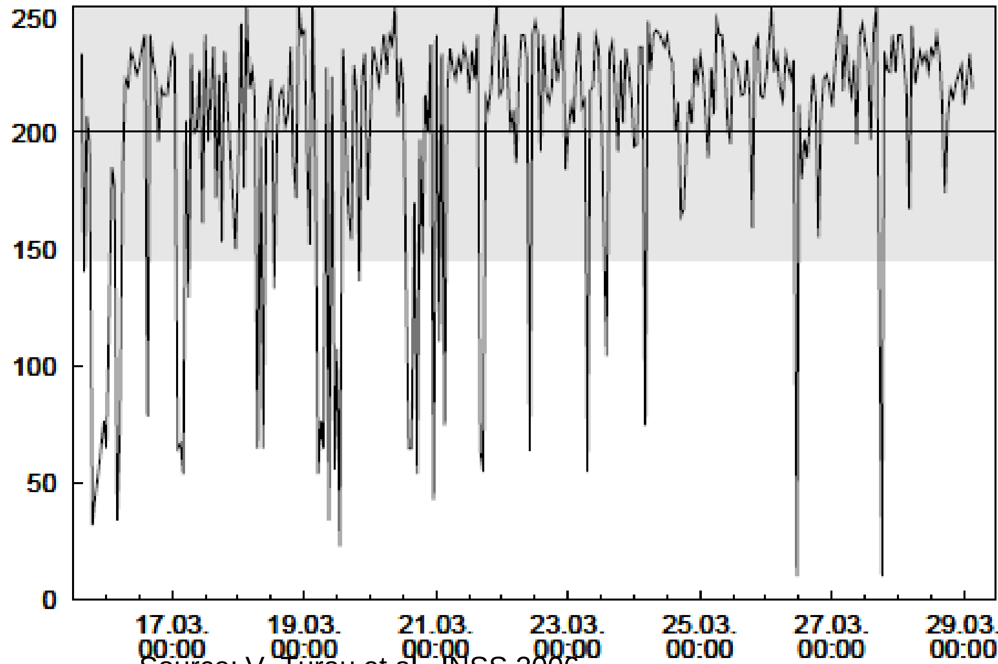




- links fall into 3 categories
  - connected, transitional, disconnected
- transitional links are often unreliable and asymmetric (even for static nodes)

“The only source of packet loss is collision”

- packet error does not mean collision
  - Coexistence: What if there are other people on the earth ????
  - Link quality change
- It is often counterproductive to retry immediately
  - At least on same channel
- There are other techniques than retry to correct errors
- Hidden / exposed terminal



Source: V. Turau et al., INSS 2006

A few words about energy

- sources of energy waste at the MAC layer:

idle listening ➔ listening when no data is available

overhearing ➔ listening to data dedicated to others

oversending ➔ emitting while there is no receiver

collisions ➔ two parties are sending at the same time

protocol overhead ➔ data that is not directly used for the application

“Broadcast is for free” / “Energy ~ to number of packets & their size”

- Broadcast means all nodes must be synchronized in time (and frequency)
  - Synchronization is not free
- Packet transmission means synchronization between sender and receiver(s)
  - There is an overhead per packet (can be large)
  - It varies with sending interval
- Turning off nodes for long periods of time
  - Introduces long latencies
  - There are other techniques (e.g. preamble sampling)

In addition

- Severe resource constraints
  - energy, bandwidth, memory size, processing
- Network dynamics
  - Nodes come and go, link go up and down

- Scalability (along number of nodes, traffic, error
- Multiple traffic requirements
  - periodic, sporadic, critical, non critical, …
  - Often unbalanced (to sink)
  - and also changing with time

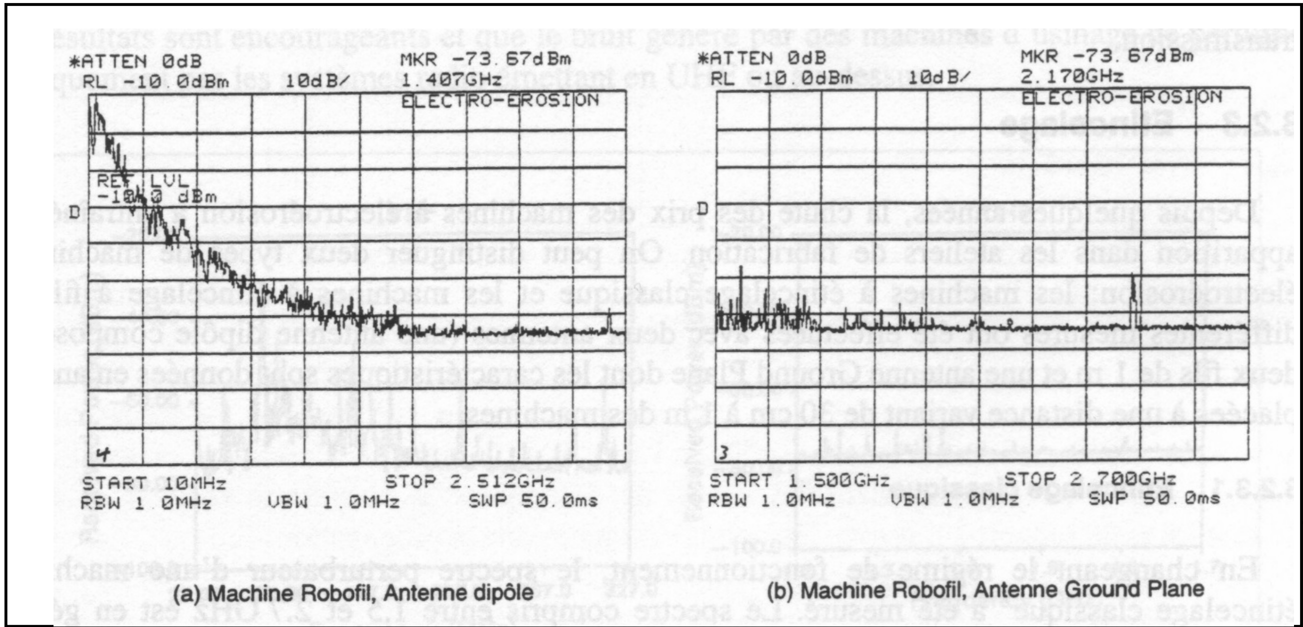
- Regulations (e.g. ETSI)
- Dependability (many sources of failure)

Context - radio transmission

- higher BER
- lower signalling rate
- limited possibility to detect collisions
- low spatial reuse
- prone to interference
- lower distances
- security concerns
- remote powering

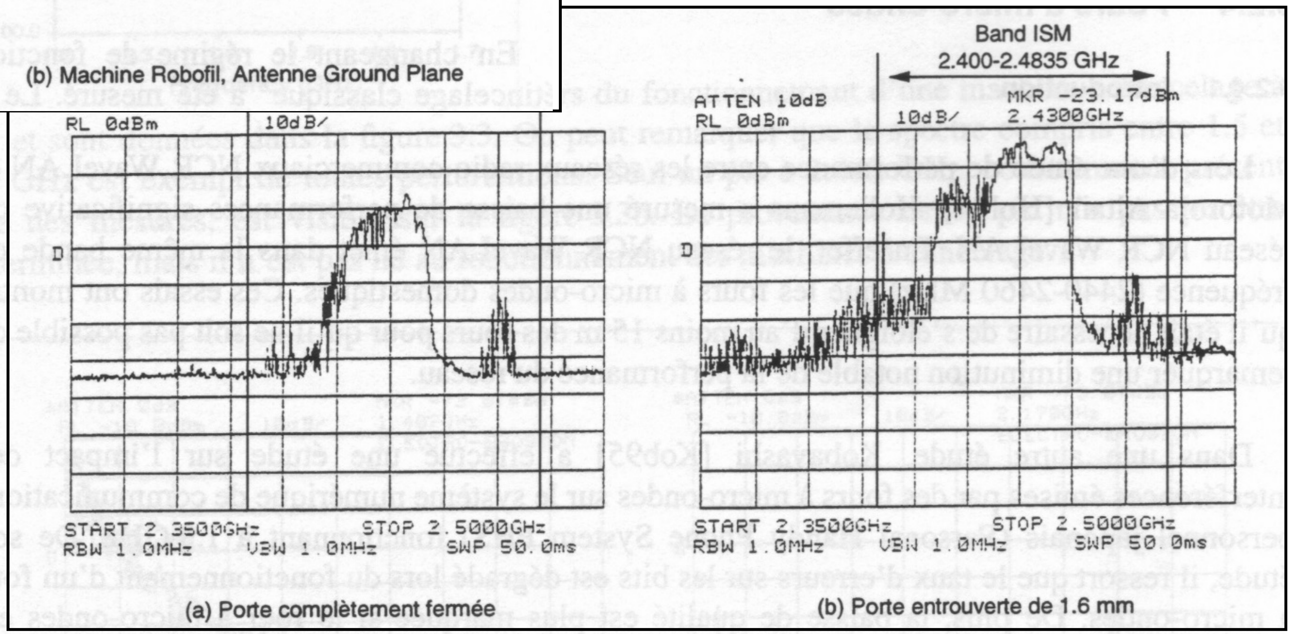
- radio transmission
  - fading
  - incompatible regulations
  - free use of ISM bands
  - higher cost
  - longer turn on and switching times
  - hidden terminal effect
- light transmission
  - line of sight
  - sensitive to heat
  - health concerns

Noise Sources



(a) Machine Robofil, Antenne dipôle (b) Machine Robofil, Antenne Ground Plane

source: Ph. Morel, 1996



(a) Porte complètement fermée (b) Porte entrouverte de 1.6 mm

Implications of wireless transmission properties

- MAC
  - master-slave (switching time ⇒ longer timeouts)
  - bus arbiter (hidden node ⇒ limitation in broadcast, reliable detection of silence ⇒ BA redundancy)
  - tokens (hidden node ⇒ token loss, switching time ⇒ longer timeouts)
  - virtual token (reliable detection of silence ⇒ token passing)
  - CSMA (no collision detection ⇒ use timeouts)
  - TDMA (switching time ⇒ longer gaps)

Implications of wireless transmission properties (2)

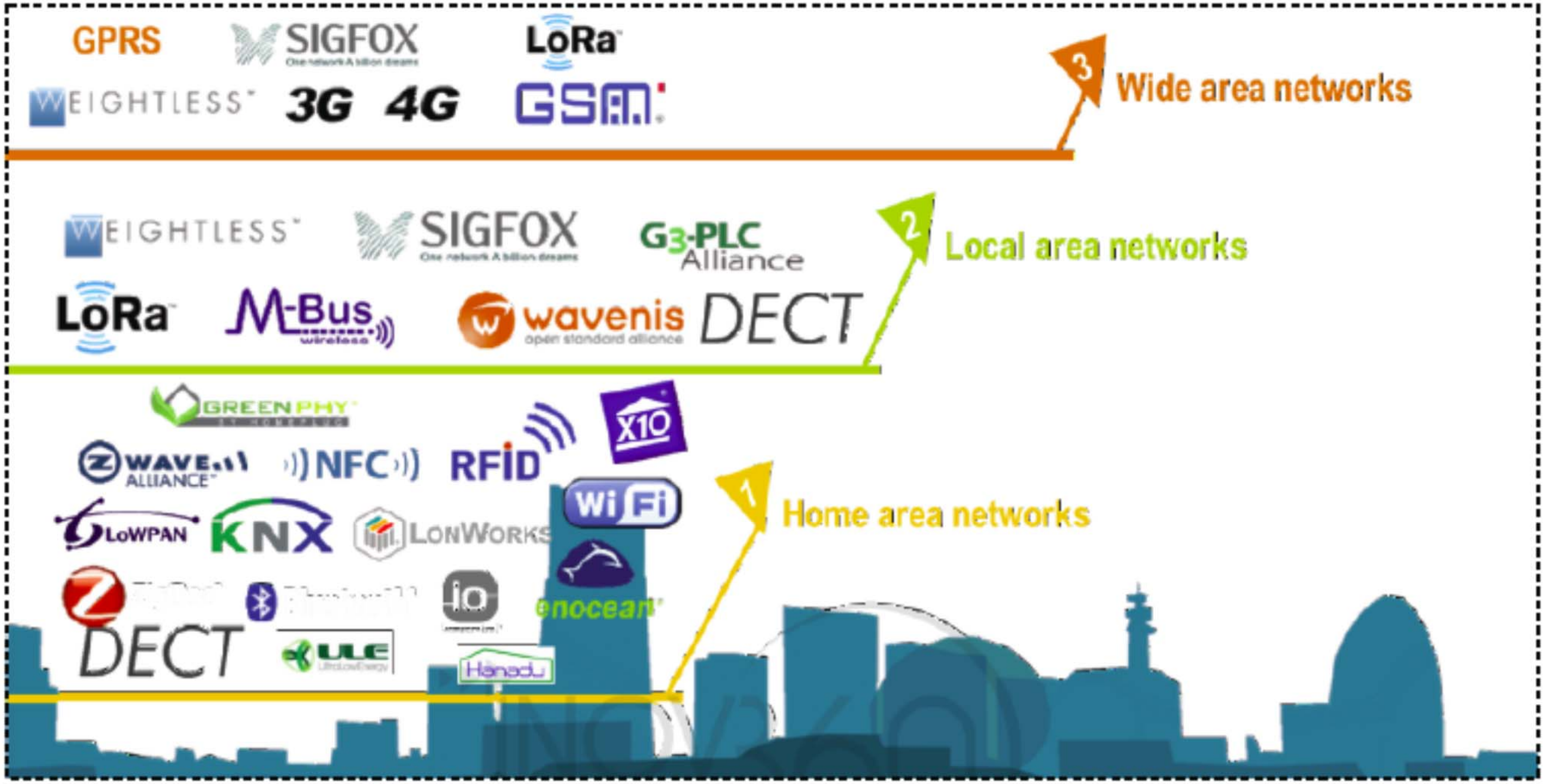
- Error recovery
  - immediate retransmission
    - lower bandwidth, impact on higher layers
  - no immediate retransmission (cyclic transmission)
    - likelihood that errors will last
  - use forward error correction codes to lower apparent FER

source: Ph. Morel, EPFL 1996

Time and Networking

- Several layers play a role in QoS
- Physical layer: robustness
- Data Link Layer: error detection/correction & guarantees at MAC and ack at LLC
- Network: classes of traffic
- Transport layer: retransmission schemes
- Application: interaction model

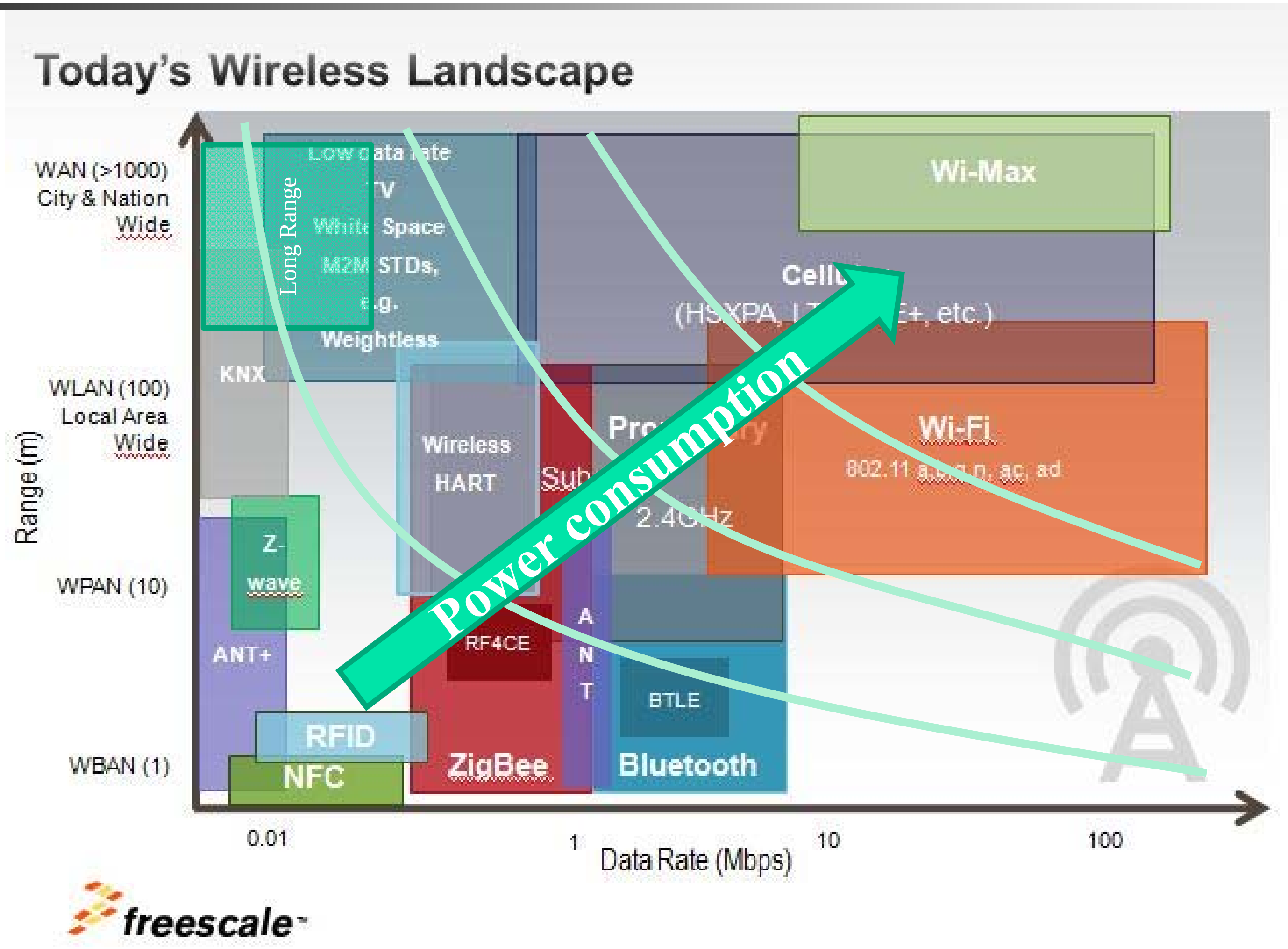
Wireless landscape



See also: http://literature.cdn.keysight.com/litweb/pdf/5992-1217EN.pdf?id=2773109

Source: Xebia, P. Antoine, S. ben Fredj

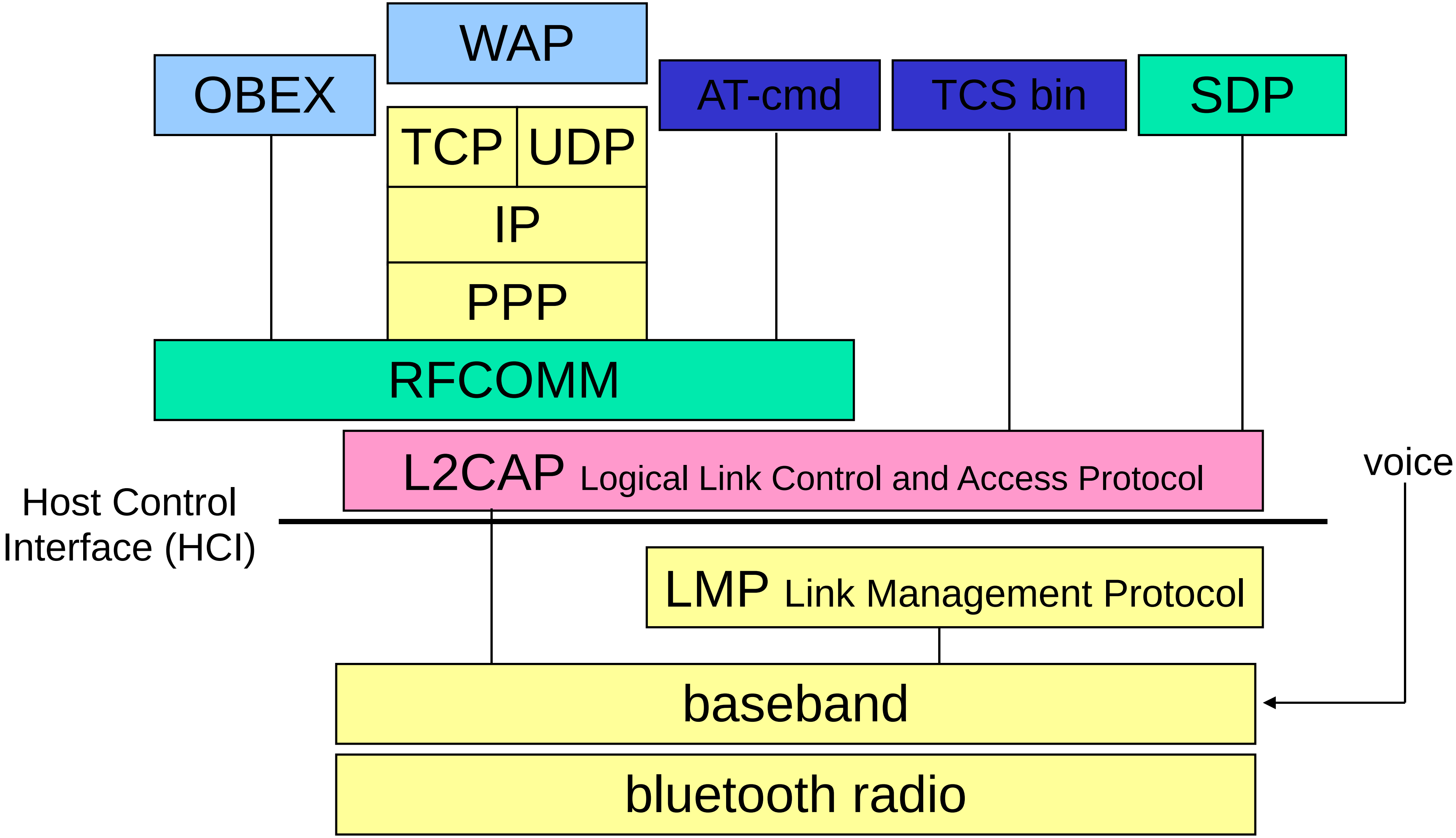
Wireless Landscape (2)



Bluetooth (IEEE 802.15.1)

- open specifications
- data and voice communication
- ISM band 2.4 GHz / FH-CDMA (1600 hops/s, 79 ch.)
- power 1mW (10m) option for 100mW
- cells with max. 8 participants (1 master - 7 slaves)
  - max. 3 voice communications (from/to master)
  - or 1 voice communication and 1 data communication
  - or 723.2+57.6 kb/s asymmetric, 433.9 kb/s symmetric
- TDD, 1 Mbit/s raw bit rate

Bluetooth Architecture

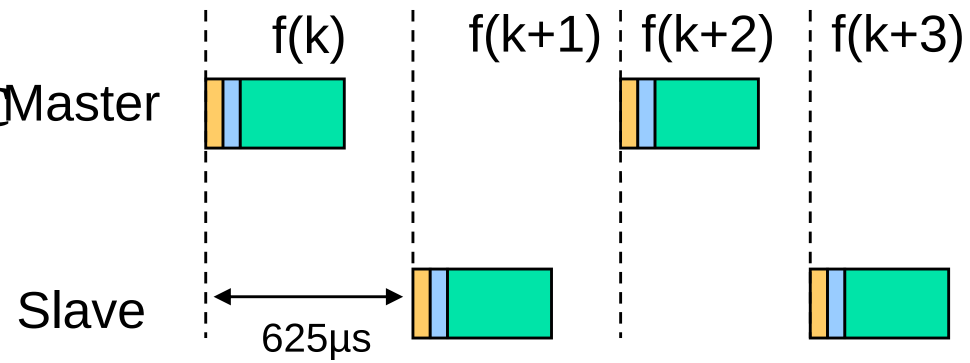


Bluetooth - MAC

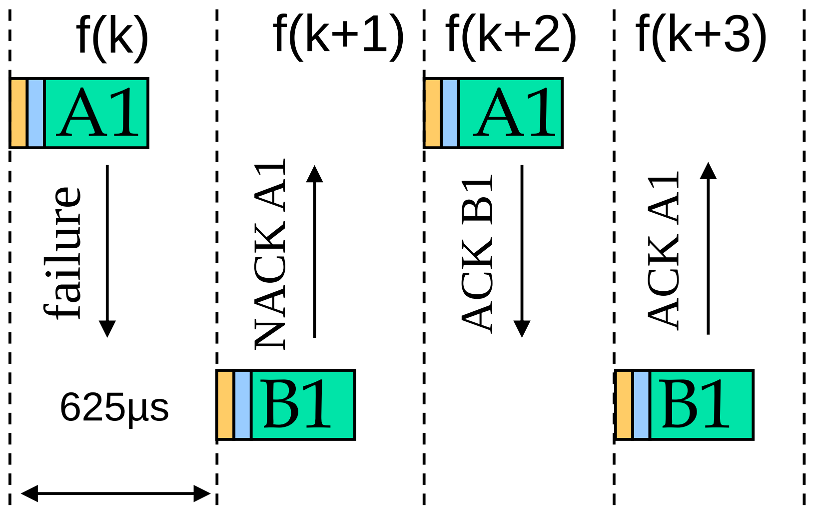
- Frequency hopping spread spectrum (1600 hops/s)
  - hopping sequence based on master identity and clock phase
  - around 23 hours duration
- TDD (Time Division Duplexing) full duplex
  - each 625µs window is used alternately by the master and a slave (frequency hop at each new slot)
  - master-slave communication (request - response)
  - Master is the one that initiated the connection

Bluetooth - TDD

- Master-slave asynchronous traffic

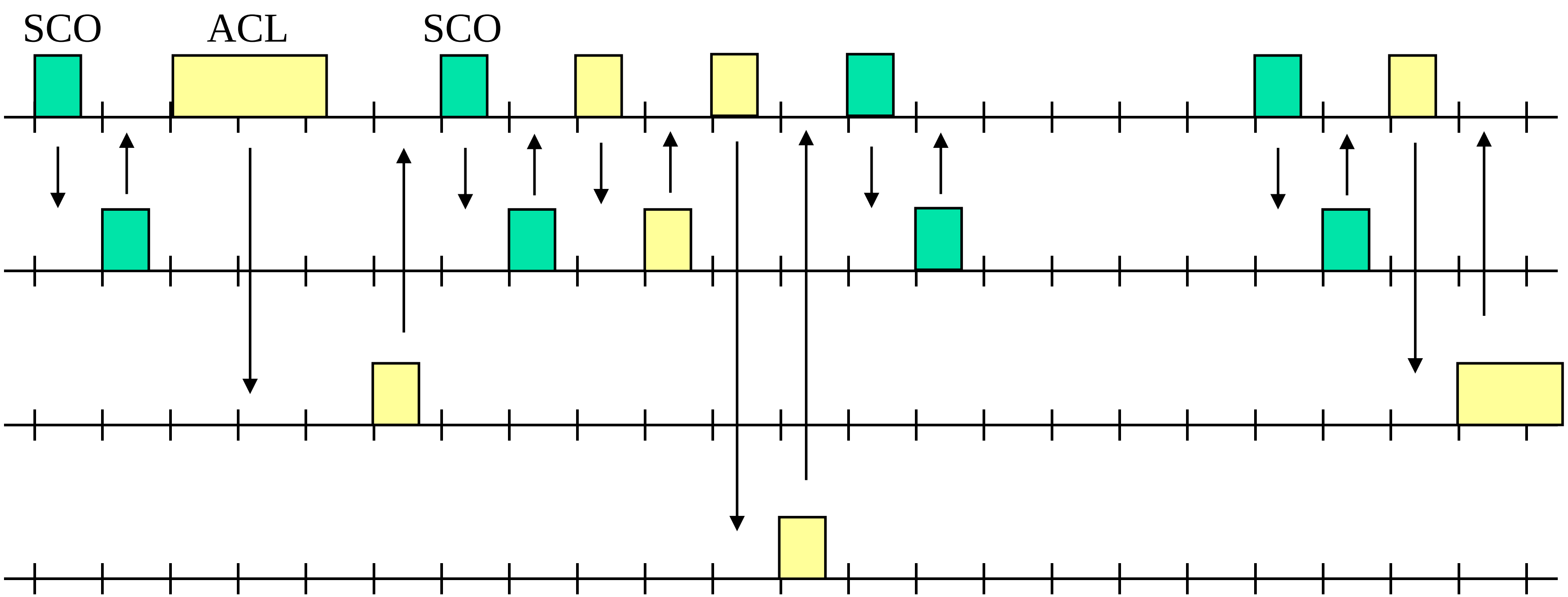


- Error recovery

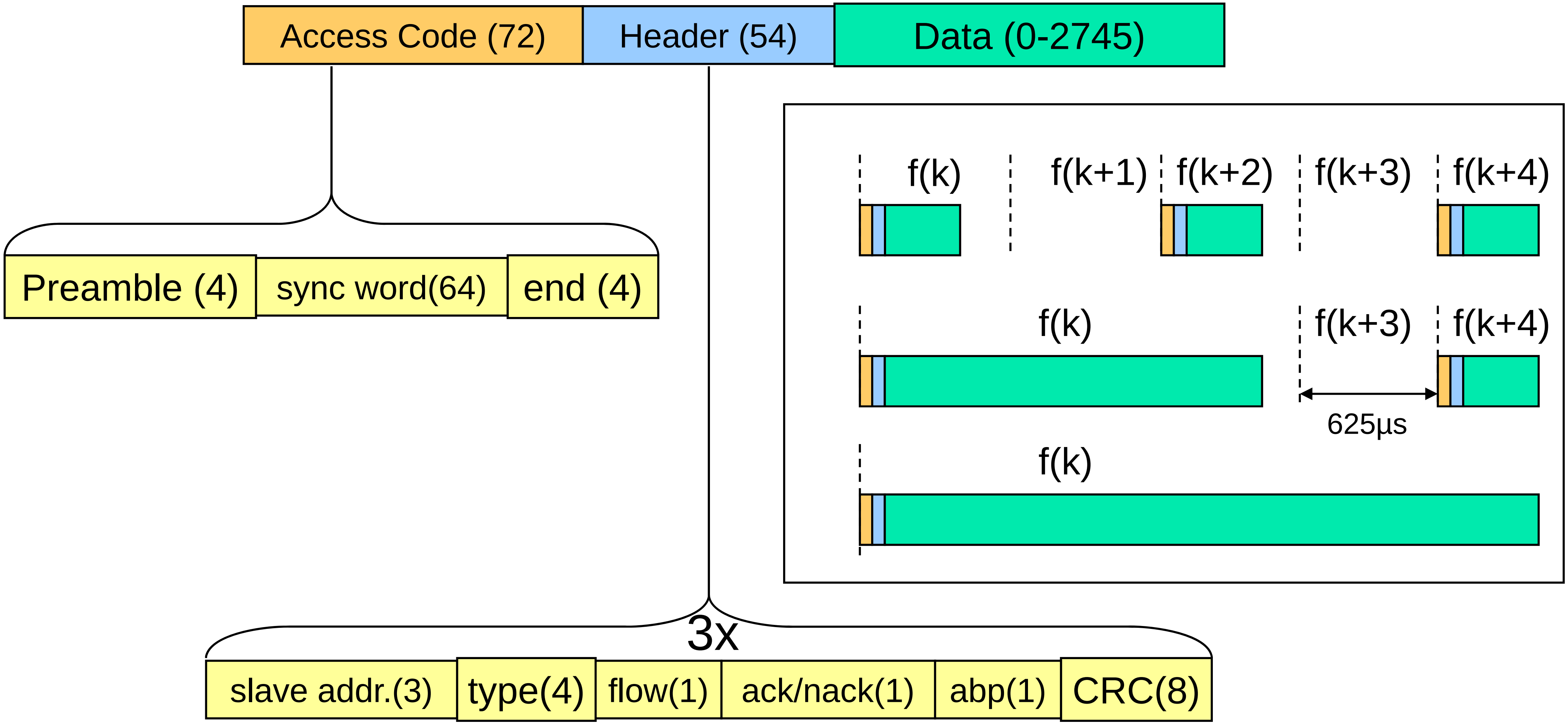


Bluetooth – Synchronous Traffic

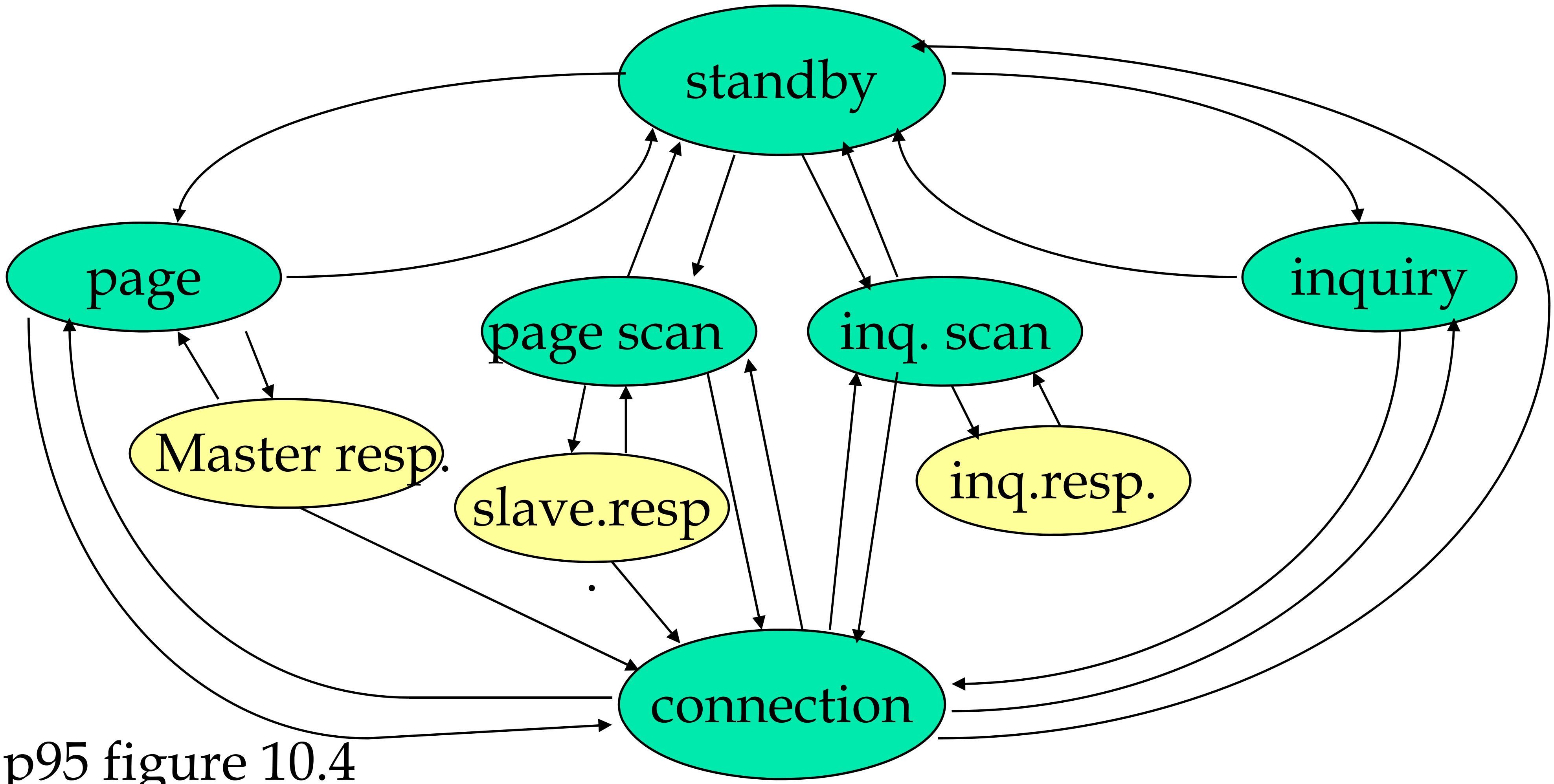
- When used synchronous (SCO) traffic is regular
- Asynchronous (ACL) traffic is interleaved



Bluetooth - packets



Bluetooth - States



p95 figure 10.4

Bluetooth –scheduling

- Local inside node
  - Seems to be FIFO
- Intra piconet
  - None specified
- Inter piconet
  - None specified

Bluetooth - Reduced Traffic Modes

- Sniff mode
  - slave needs to listen only at Tsniff interval
  - each time listens during Nsniff_attempts slots
  - each time, it receives a packet the listening time may be extended
- hold mode
  - does not handle ACL traffic for a given duration
  - SCO traffic is still supported
  - returns to normal mode after the negotiated duration
  - may be used by a station to participate to another piconet

Bluetooth - Reduced Traffic Modes (2)

- Park mode. In this mode, a slave
  - no longer participates in the piconet traffic
  - remains synchronised with the master (master broadcasts a beacon at regular intervals)
  - gives up its active member address (AM_ADDR) and receives 2 new addresses
    - Park Mode address (PM_ADDR)
    - Access Request address (AR_ADDR)
  - may be unparked by master (indicated in beacon)
  - may request to be unparked (access window after beacon)
  - virtually no limit in number of parked slaves

Bluetooth - private protocols

- LM (Link Management)
  - authentication and ciphering / parameter negotiation
  - controls power mode
- L2CAP (Logical Link Control and Adaptation Prot.)
  - adaptation to higher layer protocols
  - segmentation / re assembly (max. 64 Kbytes)
  - connection oriented / connection less services (async. Data)
  - multiplexing and group abstraction
- SDP (Service Discovery Protocol)
  - information on device capability

Bluetooth - Piconet & Scatternet

- Piconet
  - group of max. 8 participants (1 master, max. 7 slaves)
  - a station may be master in a single piconet at any given time
- Scatternet
  - set of piconets in the same geographical area
  - a station may pertain to more than a single piconet
    - must synchronize alternately of all piconets
    - HOLD allows to leave temporarily a piconet

Bluetooth - Link Manager

- Setup, control and security of links
- offers services to
  - authenticate and pair devices
  - setup encryption
  - switch role (master-slave)
  - change mode (park, sniff, hold)
  - manage paging
  - manage SCO links
  - control power
  - supervise link

Bluetooth - Link Manager (2)

- LM messages have higher priority than user data
- Max. response time 30 seconds
- Messages are always single slot packets
- First 2 bits in header indicate LM PDUs
- Flow bit = 0 (ignored)
- 1st byte of body = transaction id. (1), opcode (7)
  - Id = 0, if transaction initiated by master (=1 by slave)
- PDU sent alone (DM1) or in voice packets (HV1)

Bluetooth - Security

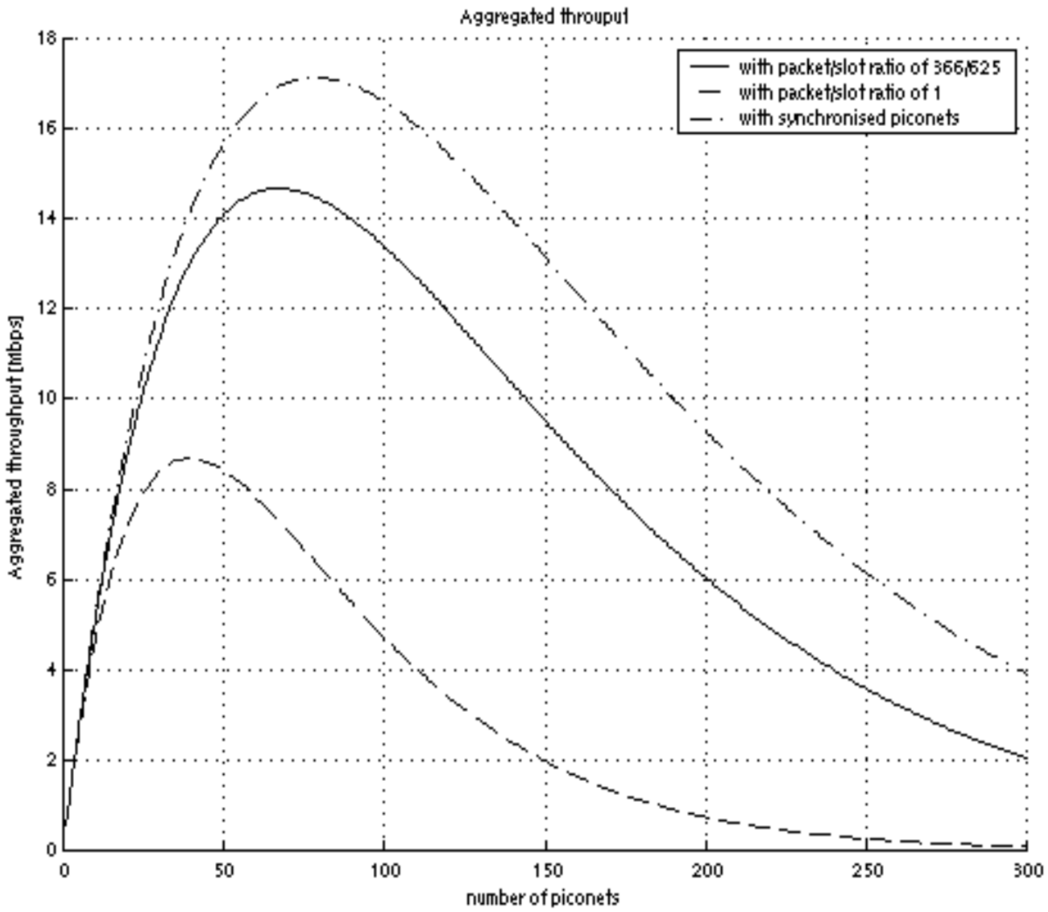
- Authentication
  - based on challenge-response scheme
  - key can be established on line or pre owned
- Encryption
  - can be used or not
  - key size can be negociated

Interference between Bluetooth piconets

- Bluetooth
  - Frequency Hopping, 79 Frequencies
  - Hop every 625 us, Packet length 366 us
- Assumptions
  - collocated piconets
  - interference => packet loss

Aggregated Throughput

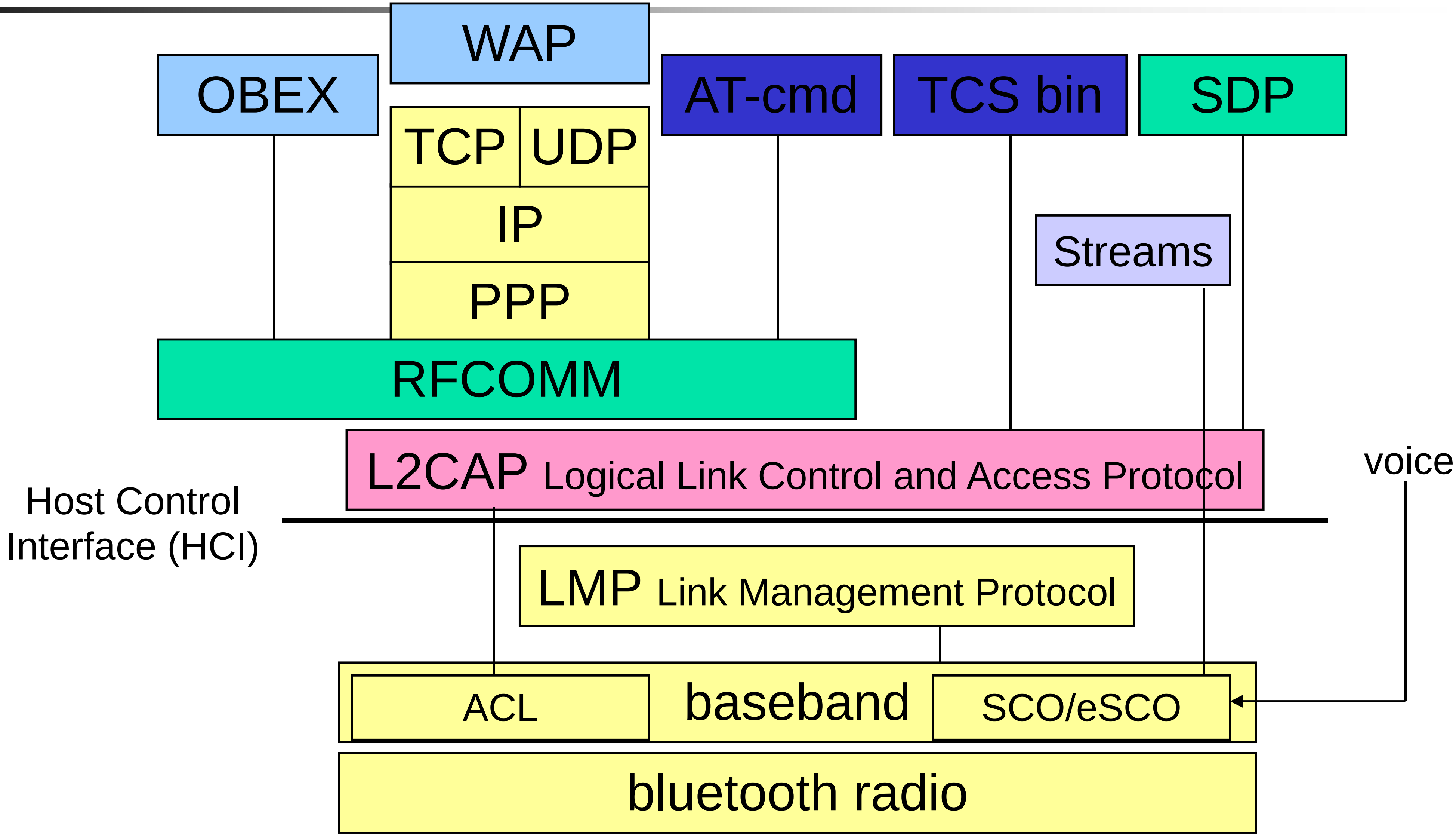
$$S_a(n) = n \cdot P_s(n)$$
$$= n \cdot a^{n-1}$$



Bluetooth - Pros and cons

- Pros
  - low interference (microwave ovens ?) and fading
  - no planning, low cost, authentication and encryption
  - power management possible
  - device discovery protocol
- Cons
  - point to multipoint, short distance
  - no real-time capability for data
  - limited capacity (# devices, throughput)
  - long connection time (up to 10.24 s)

Bluetooth - extensions



Bluetooth – Extensions (2)

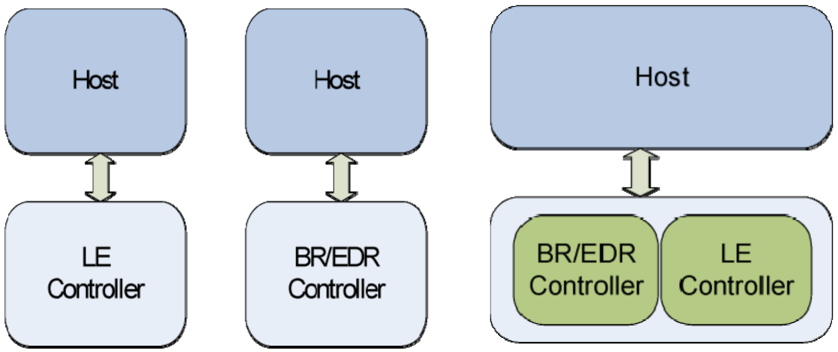
- Version 1.2 (2003)
  - Extended SCO links
  - QoS
  - Better flow management (windows)
- Version 2.0 (2004)
  - 3 Mbit/s
- Version 3.0 (2009)
  - Support for high speed alternate physical layer (802.11)
- Version 4.0 (2010)
  - Low energy version (BT Low Energy / BT Smart)
- Version 5.0 (2016)
  - Long range, 2 Mbit/s for LE, high duty cycle, BLE Mesh (2017)

Bluetooth - QoS

- On SCO and eSCO links
  - Constant bit rate / content is free (not managed by Bluetooth)
    - Management may have a higher priority
  - Error correction may be performed using retransmission
  - Only one link per slave
- On ACL links
  - Managed according to « tokens bucket » algorithm
    - Mean throughput with some peaks
  - Only lower priority than SCO and eSCO
  - May be subject to admission control

BTLE objectives

- Targets, principally low-power and low-latency, applications for wireless devices within short range (<50 m)
- To operate more than a year on a button cell battery
- lower power consumption not achieved by nature of the active radio transport, but by design of the protocol to allow low duty cycles, and the use cases envisaged.
- Designed to be lowest cost and easy to implement
- Node types

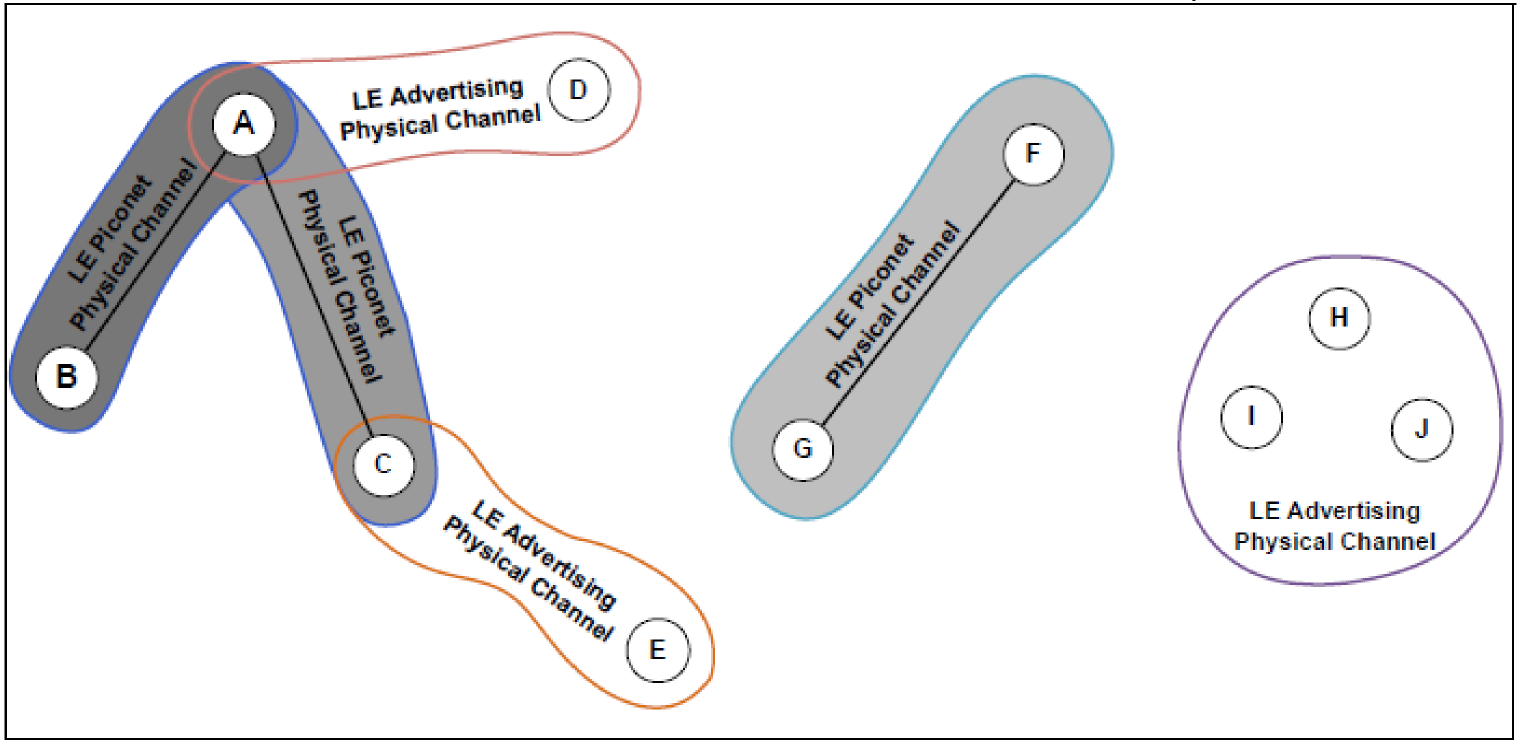


BTLE novelties

- Mostly new PHY
- New advertisement mechanism
  - => ease of discovery connection
- Asynchronous connection-less MAC: used for low latency, fast transactions (e.g. 3ms from start to finish)
  - No carrier sense before transmitting
  - Fast interactions with channel diversity and random waits
  - Connections with regular channel hopping
- New Generic Attribute Profile
  - to simplify devices and the software that uses them.

BTLE - Examples of interactions

Source: Bluetooth specification version 4, 30.6.2010.



- A master with B & C as slaves / F master with G as slave
- D advertizer with A initiator / E scanner with C advertizer
- H advertizer with I & J as scanners

BTLE advertisement

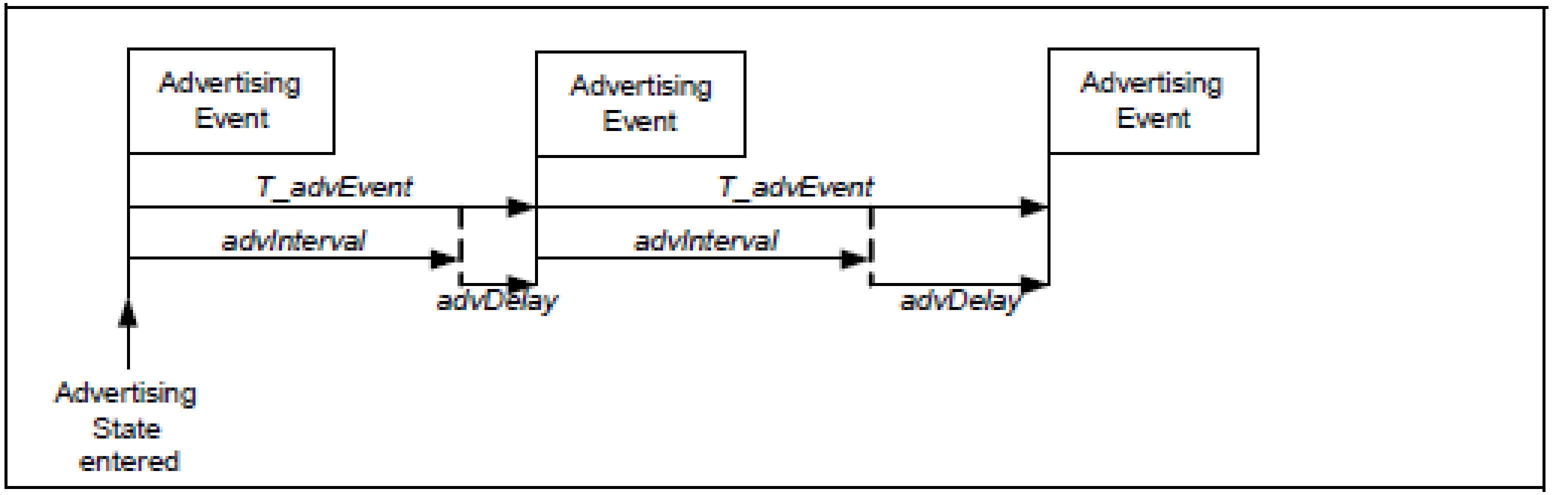


Figure 4.1: Advertising events perturbed in time using advDelay

Source: Bluetooth specification version 4, 30.6.2010.

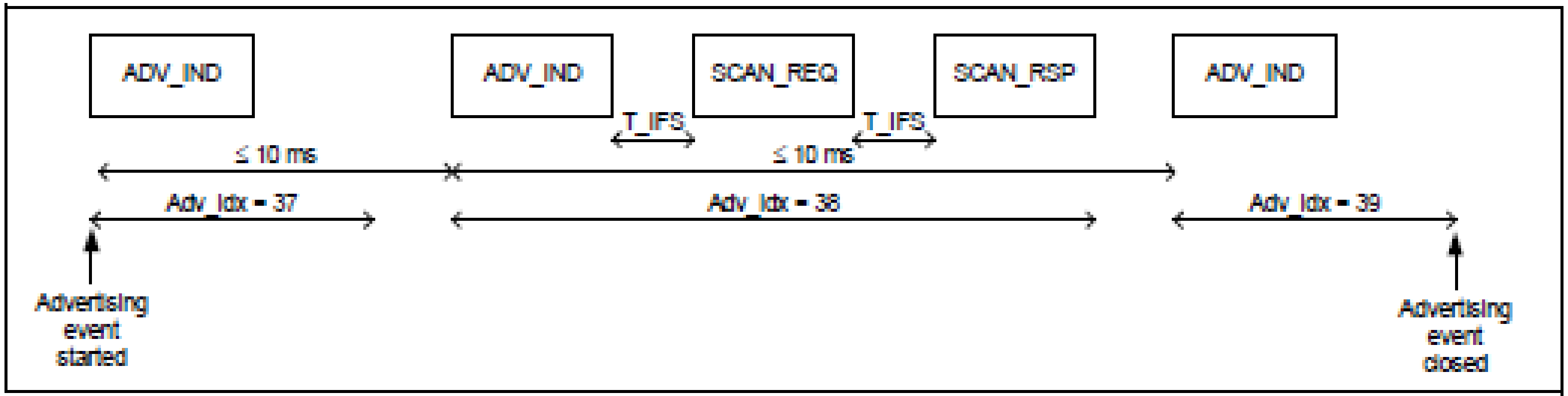


Figure 4.3: Connectable undirected advertising event with SCAN_REQ and SCAN_RSP PDUs in the middle of an advertising event

BTLE connections

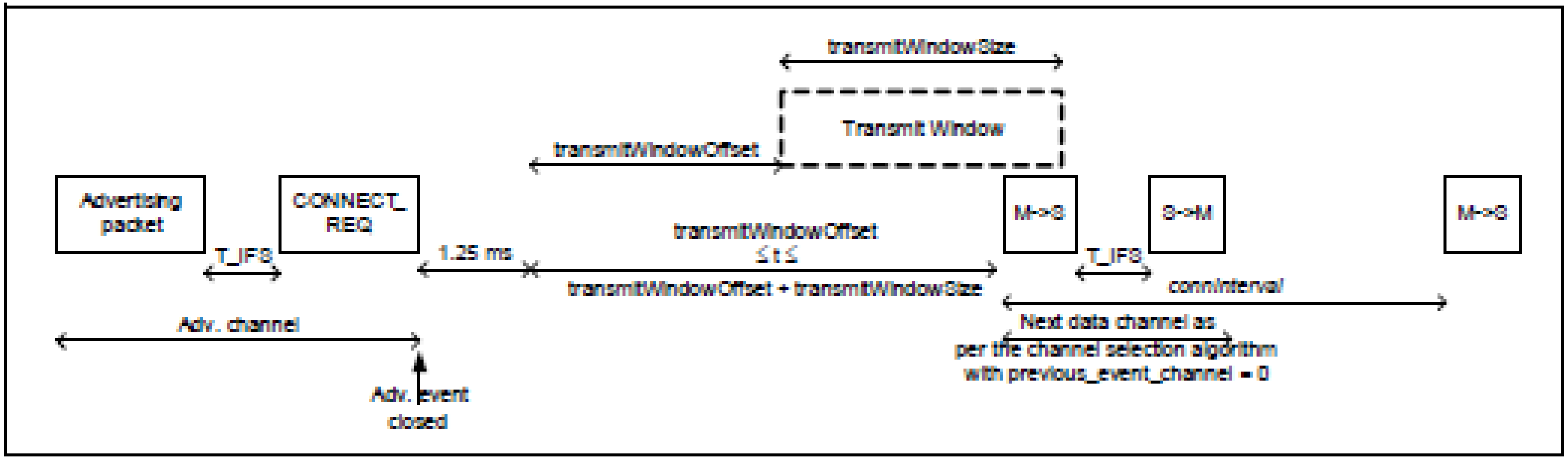


Figure 4.11: Master's view on LL connection setup with a non-zero transmitWindowOffset

Source: Bluetooth specification version 4, 30.6.2010.

BTLE 4.2 (BT Smart) - Analysis

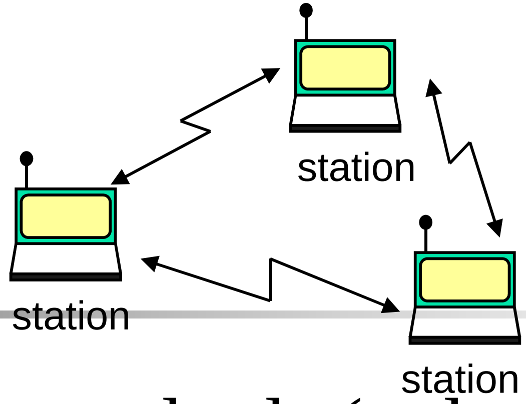
- Pros
  - Targets low energy
  - Good coexistence (channel hopping)
  - Advertisement can be fast (good for spurious interactions)
  - Security
  - Can be implemented on resource limited devices
- Cons
  - No real-time guarantee
  - Limited throughput (max. around 80-90 Kbps)

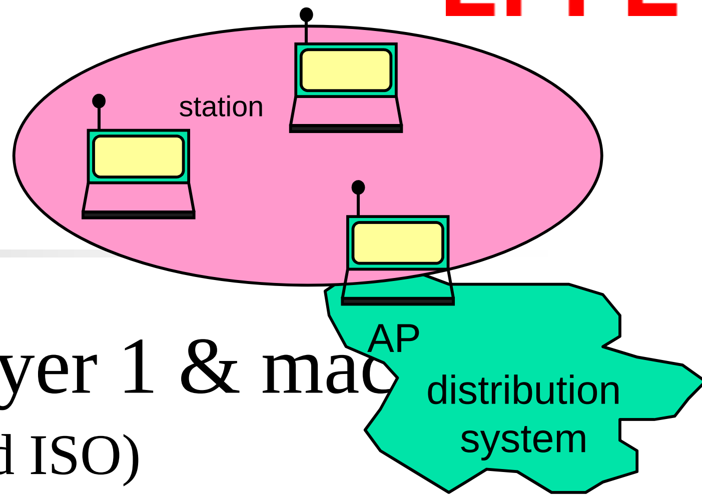
Bluetooth 5

- 2 Mbit/s for BTLE
- LE long range (300m)
- Connection-less broadcasting up to 255B
- Lower duty cycle

- Bluetooth Mesh (2017)
  - Mesh networking, based on publish-subscribe
  - M. Woolley, S. Schmidt, “Bluetooth mesh networking - An Introduction for Developers”, 2017, https://www.bluetooth.com/bluetooth-technology/topology-options/le-mesh/mesh-tech

IEEE 802.11





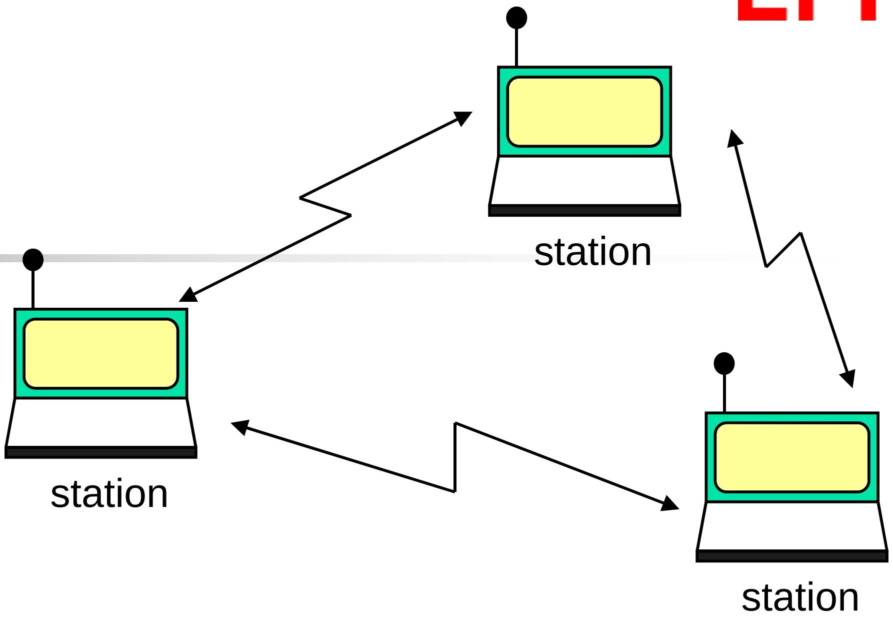
- Part of IEEE 802 standards (only layer 1 & mac
  - international standard since 1999 (IEC and ISO)
- wireless LAN with 2 operating modes
  - station to station without coordination (ad hoc network or DCF)
  - coordinated by a single base station per cell (PCF)
- 3 physical layer options (2.4 GHz radio FH & DS, IR)
  - DS SS(11 chips, 30 MHz between channels) 1, 2, 5.5 and 11 Mbit/s
  - FH SS (79 channels, 3 sets of 26 hopping sequences, > 2.5 hops/s)
    - range (30m indoor, 200m outdoor, 30km directive)
  - IR pulse position modulation, 1 & 2 Mbit/s, diffuse communication
- MAC: CSMA/CA + contention-less period (PCF)

A large family…

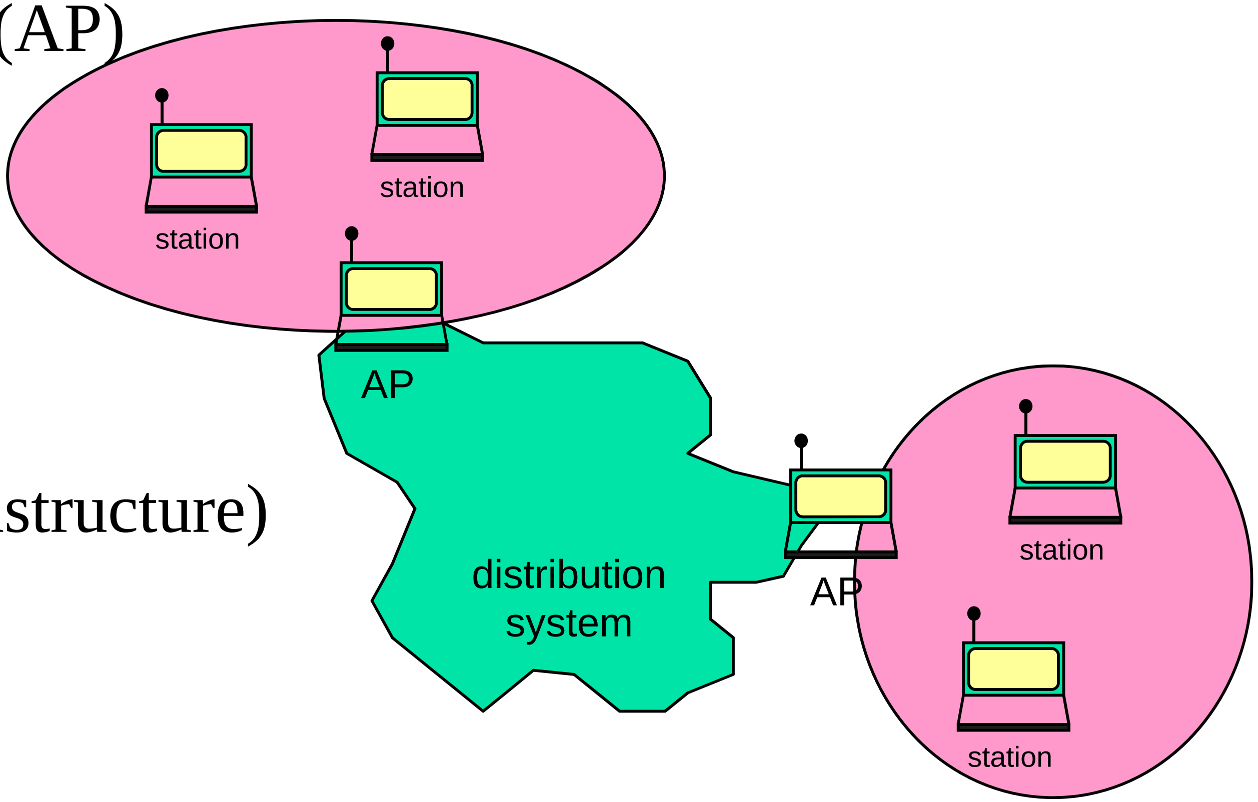
- 802.11b: 2.4GHz band, DSSS, 1,2,5.5,11 Mbit/s
- 802.11a: 5 GHz band, OFDM, up to 54 Mbit/s
- 802.11g: same but in 2.4 GHz band
- 802.11f: recommandations for inter AP protocols
- 802.11i: AES security
- 802.11h/: 5GHz band operations in Europe / Japan
- 802.11e: QoS again
- 802.11n/ac: 135 Mbit/s (2.4GHz) / 780 Mbit/s (5GHz)
- 802.11ad: 6.75Gbit/s (60 GHz) – 100 Gbit/s planned
- Projects still active (http://www.ieee802.org/11/Reports/802.11_Timelines.htm)

IEEE 802.11

- 3 modes
  - IBSS (ad hoc)



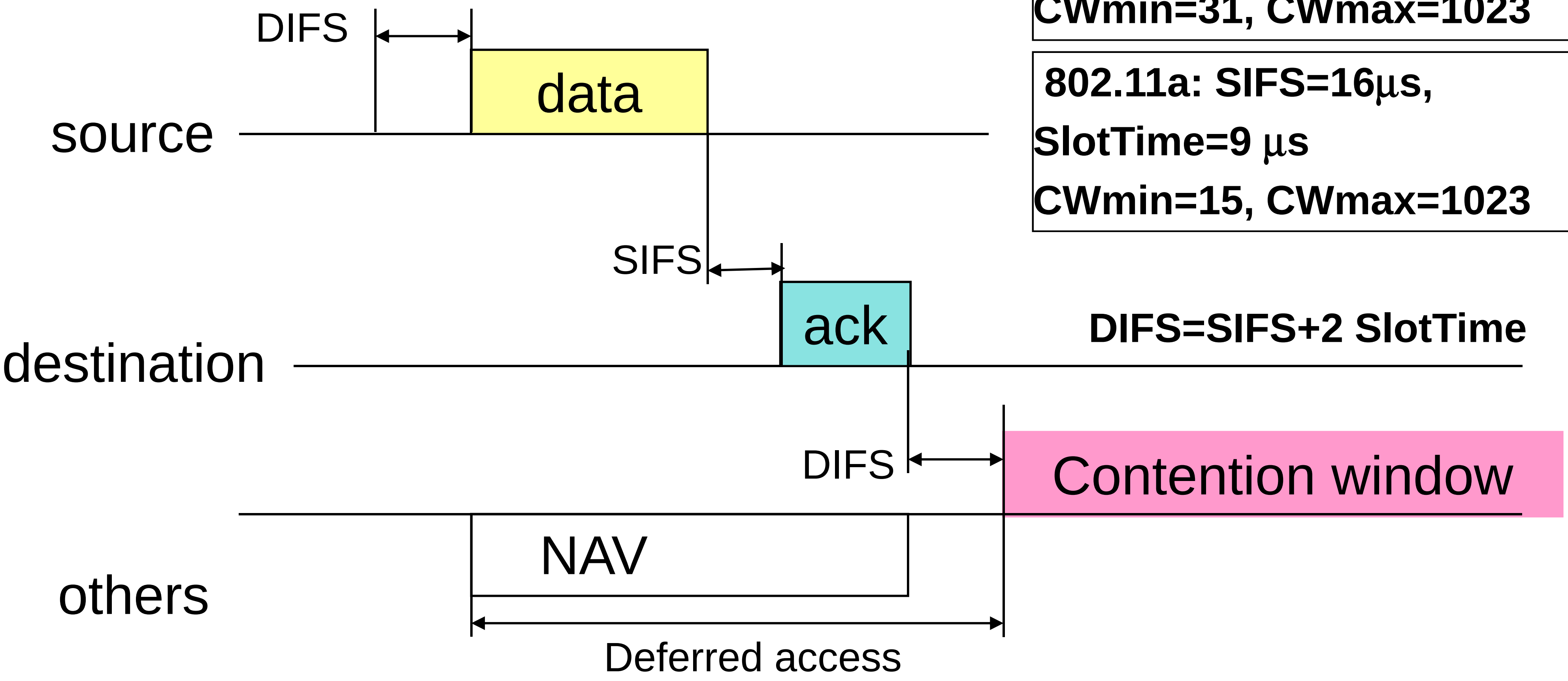
  - BSS (AP)
  - ESS (infrastructure)



IEEE 802.11 - DCF (distributed coordination function)

- Asynchronous transfer without guaranty
- CSMA / CA
  - Physical carrier detection and logical carrier detection
    - Each frame carries time required to transmit remaining traffic
    - Is used to update the Network Allocation Vector (NAV)
  - If no carrier when data arrives, immediate transmission
  - If carrier, wait until no carrier during DIFS
    - Computes backoff interval, start decrementing (freeze decrement when medium busy), and transmits when 0
  - If failure, increment backoff window (up to Cwmax)

IEEE 802.11 - DCF (2)



802.11b: SIFS=10µs,
SlotTime=20 µs
CWmin=31, CWmax=1023

802.11a: SIFS=16µs,
SlotTime=9 µs
CWmin=15, CWmax=1023

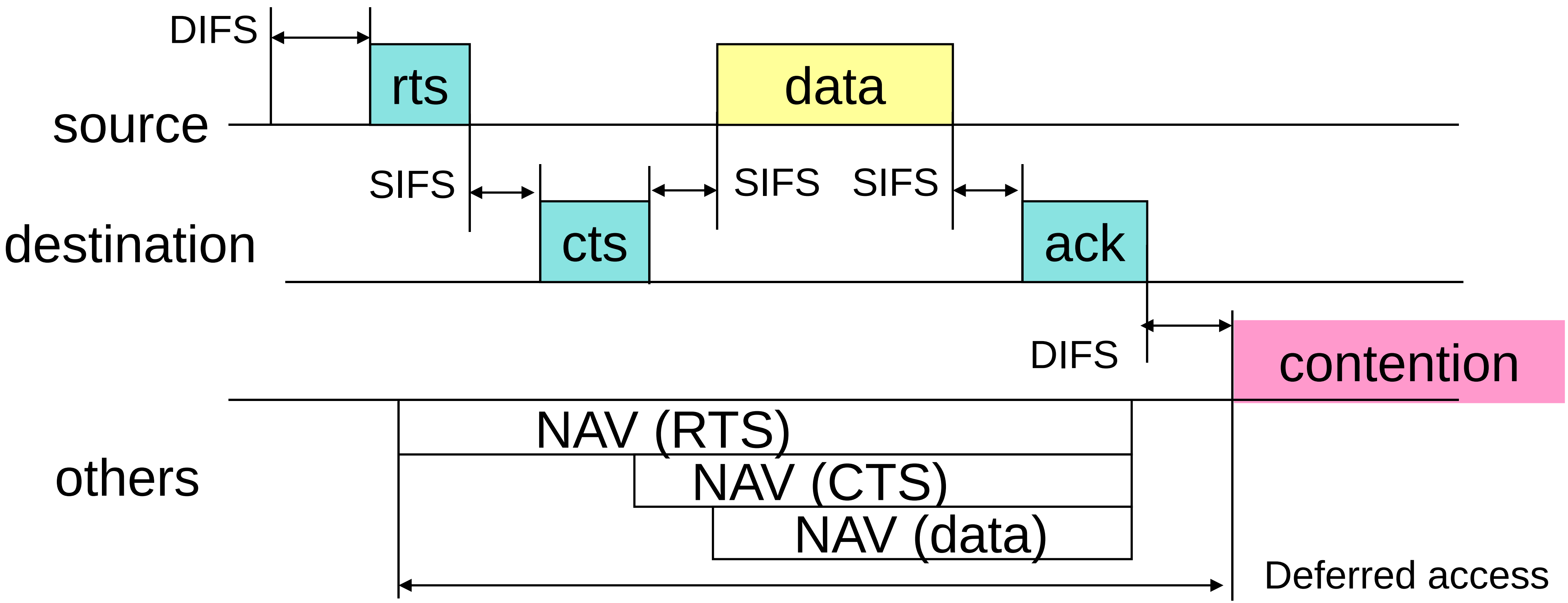
DIFS=SIFS+2 SlotTime

Transmission of long frames (MPDU)

- Maximum size 2436 bytes (20ms @1Mbit/s)
- Loss of efficiency because collision may not be detected
  - RTS/CTS mechanism
- High probability of corruption
  - Segmentation to avoid retransmission of the whole frame
  - The whole frame is transmitted without other transmissions (blocking time)

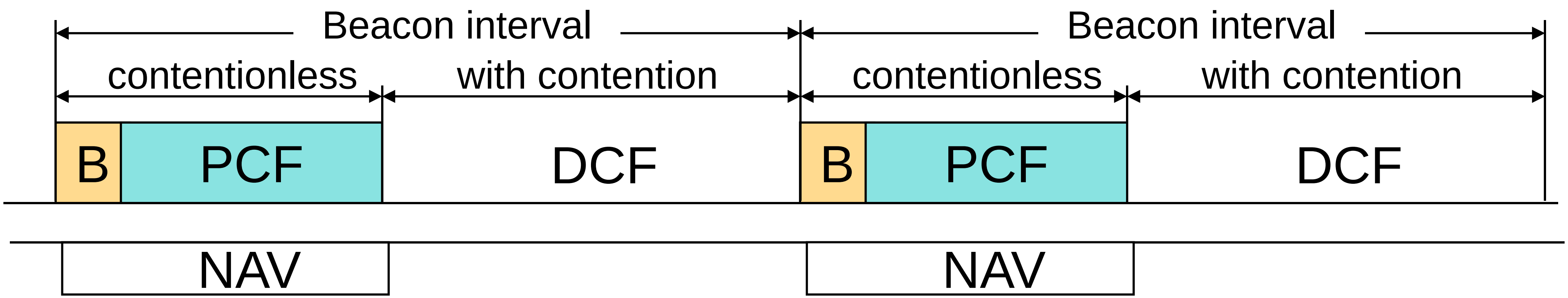
IEEE 802.11 - DCF (3)

- Collisions cannot be detected -> avoid sending long frames



IEEE 802.11 - Point Coordination Function

- Optionnal, Connection oriented
- Supports transfers without contention
- Based on a special function "point coordinator" handled by the access point AP



IEEE 802.11 - PCF

- Transfers according to a polling list
  - AP sends beacon after PIFS (SIFS+SlotTime)
  - AP sends poll to STA (optional data & ack of previous resp.)
  - STA responds with ack and optional data
- Supports station to station transfers
  - STA response is addressed to another STA (not AP)
  - Other STA must ack.
- CFP duration
  - Min: 2 times tx of the max. duration MPDU + beacon + CFP end
  - Max: beacon interval – tx time of the maximum duration MPDU
- The beacon may be delayed if a frame under transmission

IEEE 802.11 QoS limitations

- By QoS, we mean throughput, delay, jitter
- DCF
  - Best effort, no traffic differentiation
- PCF
  - Centralized traffic (even if some STA to STA possible)
  - Strong requirements on response time (SIFS ~10µs)
  - Jitter in beacon because STA may transmit across TBTT (Target Beacon Tx Time)
  - Transmission instant of polled STA variable

Possible improvements

- Station based differentiation in DCF
  - AC scheme: different backoff increase, DIFS & frame length
  - Distributed fair scheduler
  - Virtual MAC
- Station based differentiation in PCF
  - Priority based polling
  - Distributed TDMA

Possible improvements (2)

- Queue based service differentiation in DCF
  - EDCF, AEDCF
- Queue based service differentiation in PCF
  - HCF
- Error control based schemes
  - Selective repeat ARQ
  - Go back N ARQ
  - FEC
  - Hybrid FEC-ARQ

802.11e

- Included in 2007 version
  - QAP – QoS Access Point
  - QBSS – QoS Basic Service Set
  - QIBSS – QoS Independent BSS
  - QSTA – QoS Station
  - nQAP, nQBSS, nQIBSS, nQSTA – non QoS …
  - QSTA may associate to nQAP but will not provide any QoS

IEEE 802.11e (2)

- Core QoS facilities
  - EDCA (Extended DCF Access)
    - 4 access categories
  - HCCA (HCF controlled access)
    - 8 traffic streams
- Optional QoS facilities
  - Block Acknowledgement function,
  - Direct Link Set-up (DLS) and
  - Automatic Power-save Delivery (APSD)
  - Contention Free Period (CFP)

IEEE 802.11e (3)

- Introduces a Hybrid Coordination Function (HCF)
- 2 medium (channel) access mechanisms
  - Contention-based channel access (Ext. DCF access or EDCA)
    - Up to 4 backoff entities in a given station (queues)
  - Controlled channel access (HCF controlled access or HCCA)
- 2 periods, CP & CFP: EDCA in CP, HCCA in both
- 1 station coordinates a QoS supporting BSS (QBSS)
  - Hybrid coordinator (HC) (usually the QAP)
- QoS data frames carry the size of the waiting queues
- Traffic may be subjected to admission control (per class/stream)

Extended DCF Access (EDCA)

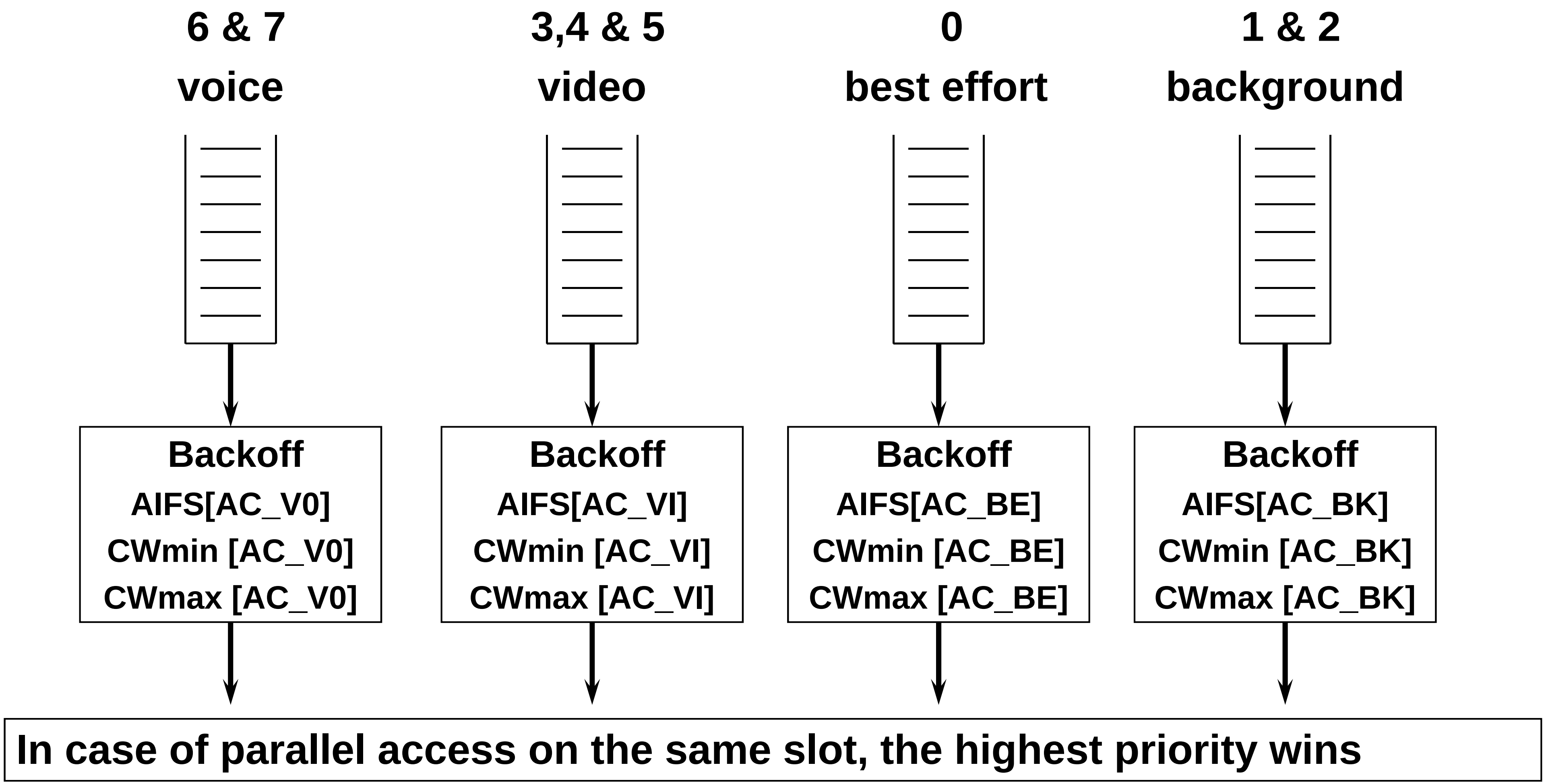
- May be used without any AP
  - Provides QoS support in ad-hoc mode (IBSS)
- Traffic differentiation based on
  - Amount of time STA senses channel idle before backoff or transmission
  - Length of contention window
  - Duration during which a station may transmit once it has acquired the channel
- May be subjected to admission control (in QBSS)

EDCA - Backoff entity rules

- Must not use radio resource more than a given limit TXOP
  - EDCA –TXOP is given by the HC (within beacons)
- Cannot transmit across TBTT (not true for HCCA)
- A frame can be sent to any other backoff entity (not only AP)
  - Requires establishment of a direct link using DL protocol
- MSDU maximum life time (dropped wo being tx)

Backoff entities in a station

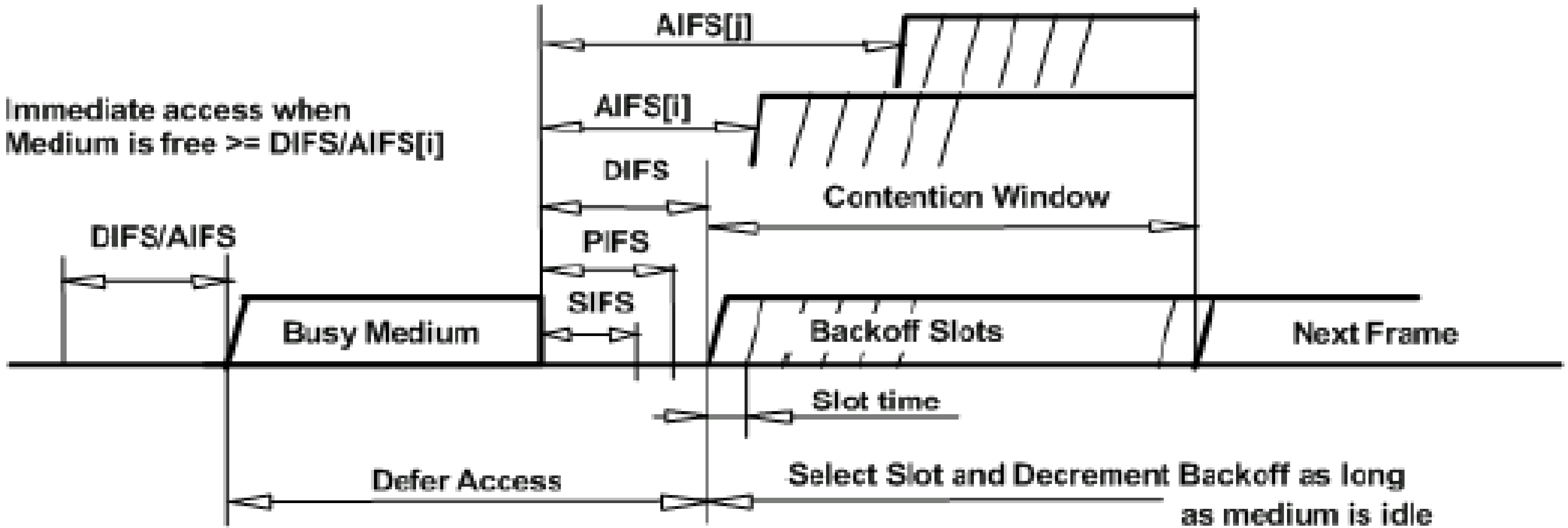
802.1D priorities



EDCA per Access Category

- Values of AIFSN, Cwmin, Cwmax and TXOPLimit are announced by the QAP in beacon/association frames
  - Fixed in QIBSS
  - QAP may use a different set of values for itself
- AIFS[AC]=AIFSN[AC]*SlotTime+SIFS
- AIFSN >=2 for non QAP
- When frame arrives at empty queue and medium has been idle for longer than AIFS[AC]+SlotTime, it is transmitted immediately
- If medium busy, wait until free and then differ for AIFS[AC]+SlotTime

Relationship between Interframe gaps



EDCA – additional rules

- Once STA has gained channel
  - If may send a sequence of consecutive MSDUs
  - As long as the elapsed time does not exceed TXOPlimit[AC]
- Admission ctrl may be mandatory for some ACs
  - Admission is based on requests (ADDTS) from QSTA to QAP

    QAP responds with average time per period

HCCA

- Allows for reservation of transmission opportunities
  - Based on request from non AP STA (up and down)
    - Must establish a traffic stream by exchanging TSPECs
  - Governed by admission control (vendor dependent)
    - Once admitted cannot be changed by QAP unless a new request is made
  - Traffic scheduled by HC collocated to QAP
    - From STA: using polls set according to QSTA requests
    - From AP: according to actual traffic

HCCA (2)

- The HC may obtain a TXOP via the controlled medium access
- It may allocate TXOP to
  - Itself by sending MSDU after medium idle for PIFS (no backoff)
  - QSTA by sending QoS CF-Poll under same rule
- New rules remove direct relationship between beacon frequency and polling frequency

HCCA traffic scheduling

- Based on TSPECs

Element ID (13)	Length (55)	TS Info	Nominal MSDU Size	Maximum MSDU Size	Minimum Service Interval	Maximum Service Interval	Inactivity Interval	Suspension Interval
Octets: 1	1	3	2	2	4	4	4	4

Service Start Time	Minimum Data Rate	Mean Data Rate	Peak Data Rate	Burst Size	Delay Bound	Minimum PHY Rate	Surplus Bandwidth Allowance	Medium Time
Octets: 4	4	4	4	4	4	4	2	2

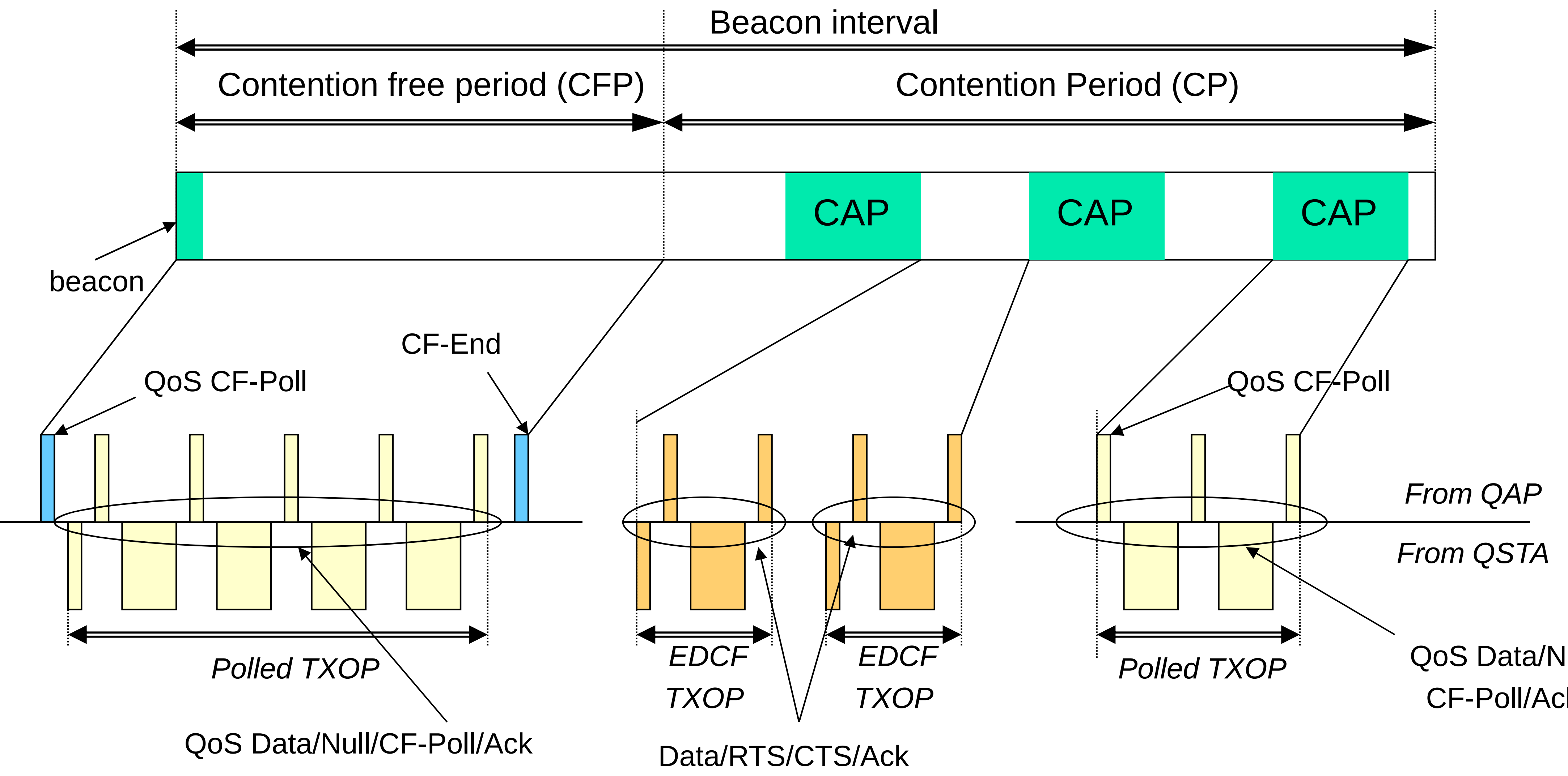
Figure 46.7—Traffic Specification element format

- QAP scheduler Computes duration of polled-TXOP in each QSTA
- Scheduler in each QSTA allocates TXOP for different TS queue according to priority order

Access rules for STA

- During CP
  - Under EDCA rules
  - In response to QoS CF-Poll
- During CFP
  - Only in response to QoS CF-Poll
    - May send multiple frames separated by SIFS as long as elapse time does not exceed TXOPLimit

HCF beacon interval and traffic



CAP: Controlled Access Phase

Other features

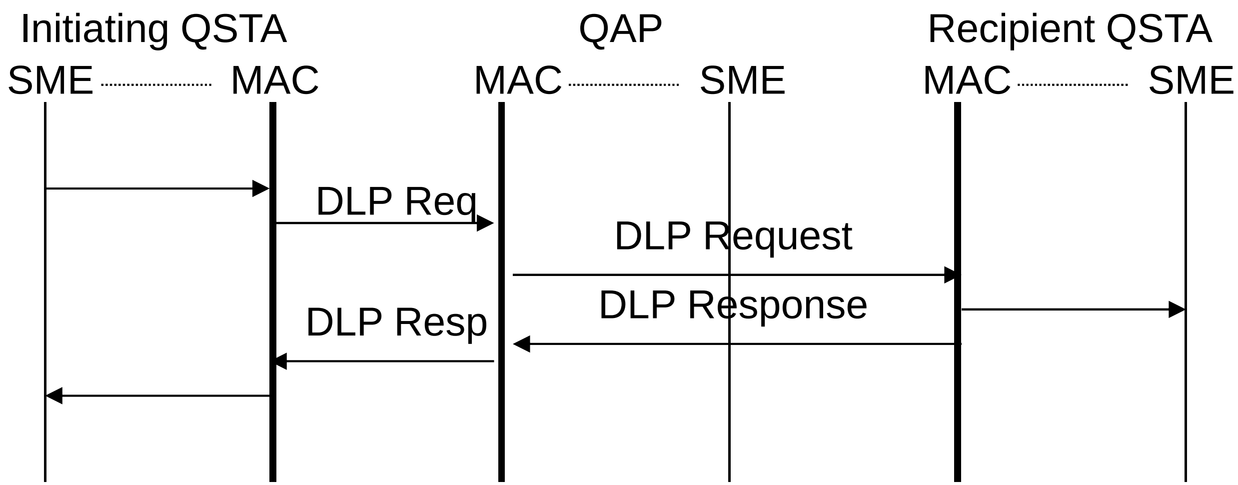
- Block acknowledgment
- Direct Link Protocol
- Power Management
  - Already in legacy standard
  - Traffic indication maps in beacon frames
- Support for time synchronisation (multicast + time since reception of a given part of the frame)
- Broadcast and multicast offered but frames must be sent once at a time
- Piggy back acknowlegments

Block acknowledgement

- Up to 64 data frames can be sent in a row (separated by SIFS) before an ack is sent back
  - Subject to TXOP duration limit
  - May be spread over several TXOPs
- Requires initial setup to check capability and reserve resources (i.e. to store blocks before reassembly)
- Ack can be immediate or delayed
- Applies both to polled TXOPs and HCCA

Direct Link Protocol

- Allows direct QSTA to QSTA transfers in QBSS
- Setup goes through QAP



- Any access mechanism may be used
  - Polled TXOP, EDCA, block ack, Traffic streams

Conclusion

- Bluetooth does not offer any QoS mechanism
  - However, there are a few possibilities starting at V2
- Bluetooth Low Energy
  - Introduced in BT V4.0
  - As name states, done for ultra-low-power devices
  - No temporal guarantees
- IEEE 802.11
  - Offers a number of possibilites for QoS
  - Much more to explore
  - Room is left open for improvements (scheduling traffic)

References

- IEEE 802.11-2012 IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
- Q. Ni et al., « A survey of QoS Enhancements for IEEE 802.11 Wireless LANs », J. of Wireless Comm. And Mobile Comp. 4 (5), pp. 547-66, 2004.
- S. Mangold et al., « Analysis of IEEE 802.11E for QoS Support in Wireless LANs », IEEE Wireless Comm. 10 (6), pp.40-50, 2003.

References (2)

- Bluetooth
  - http://www.bluetooth.org
  - J. Haartsen, "The Bluetooth Radio System", IEEE Personal Communications 7 (1), pp.28-36, 2000.
  - R. Shorey, « The Bluetooth Technology: Merits and Limitations », Proc. Int. Conf. On Personal Wireless Communications ICPWC’2000, pp.80-84.