Wireless Communications

4. Medium Access Control Sublayer

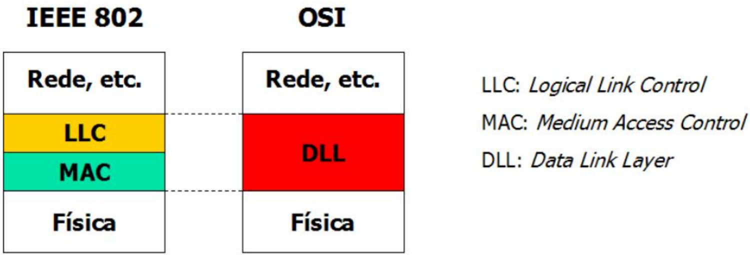
Elvio J. Leonardo

DIN/CTC/UEM

2018

Why do we need MAC for?

- Medium Access Control (MAC)
- Shared medium instead of point-to-point link
- MAC sublayer controls access to shared medium
- Examples: LANs, cellular systems, etc.
- MAC offers a unique MAC (hardware) address



MAC and LLC

- Logical Link Control (LLC)
  - Structure of the frame
  - Error control and flow control
  - Independent of the MAC used
- Medium Access Control (MAC)
  - Define how the terminal can access the network
  - Resolve disputes for access to the shared medium
- Problems MAC should handle
  - Single channel, shared by multiple terminals
  - Control should avoid and resolve access collisions
  - Static Control Mechanism
    - Examples: TDM, FDM
    - Inefficient
  - Dynamic Control Mechanism
    - Examples: ALOHA, CSMA/CD

Assumptions

- Model of the terminal
  - Independent terminals, with constant packet generation rate equal to λ (probability and a packet to be generated in Δt is $\lambda \times \Delta t$)
- Single channel
  - A single channel is available to all stations
- Collision
  - Two or more frames transmittions overlapping
  - The resulting signal is changed, perhaps lost

Assumptions

- Continuous time
  - The transmission of a frame can begin at any time
- Slotted time
  - Time is divided into discrete intervals, called **slots** (usually of constant length)
  - Each slot contains 0, 1 or more frames (unoccupied, successful transmission and collision, respectively)
- Carrier detection (carrier sense)
  - The terminal detects if the channel is being used before starting a transmission
- Collision detection
  - The station can detect if a collision has occurred

Traffic Model

- Frames have fixed length and fixed transmission time
- Number of terminals is infinite
- Terminals generate traffic following the Poisson distribution
- Traffic corresponds to the sum of new frames and retransmissions
- The probability of k transmission attempts per frame period is

$$P_k = \frac{G^k}{k!} \exp(-G)$$

  in which G is the mean value
- The channel throughput S is

$$S = G \times \text{Prob}\{\text{success}\} = G \times P_0$$

  in which the probability of success is that of the frame not colliding

Permission of Access

- Centralized
  - Central controller grants access to the medium
  - Simple and easy to manage: priorities, QoS
  - But ... central node may fail or may constitute a bottleneck
- Distributed (or decentralized)
  - All terminals collectively decide who can transmit
- Round Robin
  - Each terminal has the right to transmit periodically
  - The terminal may forfeit its turn
  - Control can be centralized (for example, polling) or distributed (for example, token ring)
  - At the end of its transmission, the terminal passes the right to transmit to the next terminal in the queue

Permission of Access

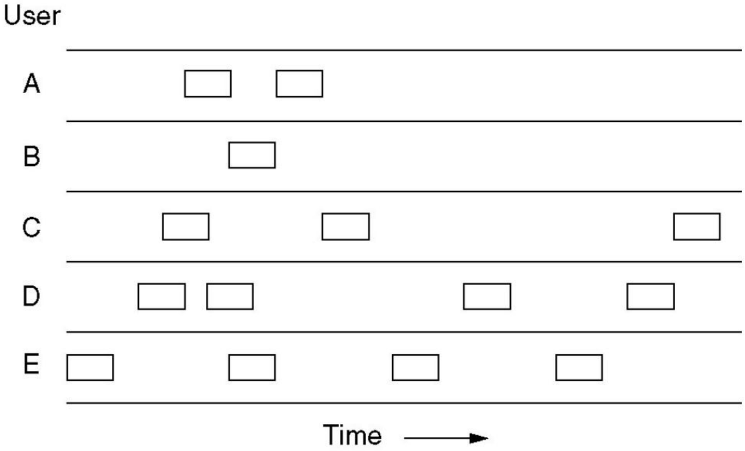
- Reservation (Scheduled Access)
  - Time is divided into slots
  - Terminal schedules the right to transmit in the near future
  - For long transmittions, multiple slots may be reserved
  - Efficient for constant stream transmissions
- Contention (Dispute)
  - Distributed control
  - Stations try to acquire medium to perform transmission
  - Good performance for bursty traffic
  - Poor performance for heavy traffic

Pure Aloha

- Introduced in the early 70s for the connection of computers scattered over the Hawaiian Islands
- Use radio transmissions
- Operation:
  - Each terminal transmits its frame regardless of the channel situation
  - In case of collision, the frames may be damaged
  - Terminals that detect collisions (either directly on the channel or because they have not receive an ACK) expect a random time before trying again
  - Low efficiency

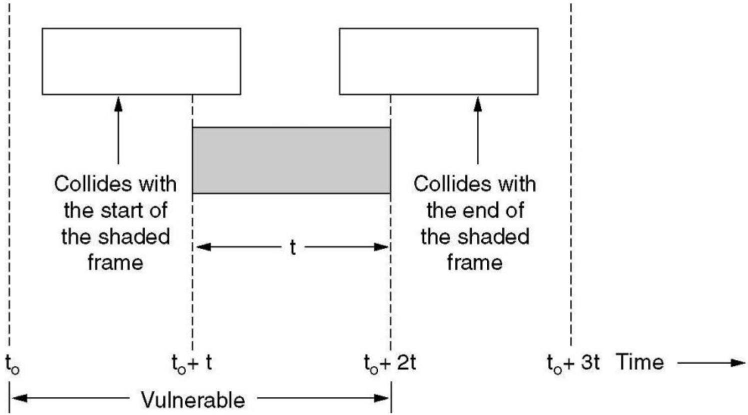
Pure Aloha

- Terminals can start transmitting at any time



Pure Aloha

- Vulnerable period for the gray frame is $2t$



Pure Aloha

- Performance
  - Successful transmission means no other packet being transmitted during 2 frame intervals, that is,

    $$\text{Prob}\{\text{success}\} = P_0 = \exp(-2G)$$

    and therefore

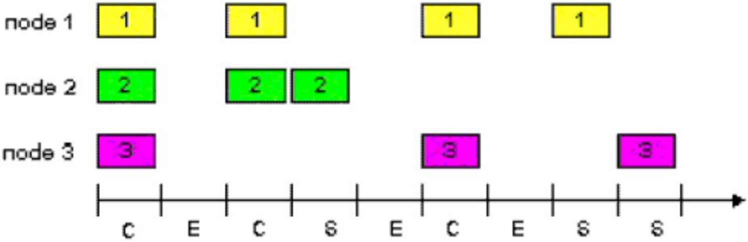
    $$S = G \times \exp(-2G)$$

  - The maximum throughput is

    $$S_{max} = 0{,}184 \text{ for } G = 0{,}5$$

Slotted Aloha

- Time is divided into slots
- Terminals can start transmission only at the beginning of the slots



Slotted Aloha

- Performance
  - With Slotted Aloha the vulnerability period is reduced to half

$$\text{Prob}\{\text{success}\} = P_0 = \exp(-G)$$

and therefore

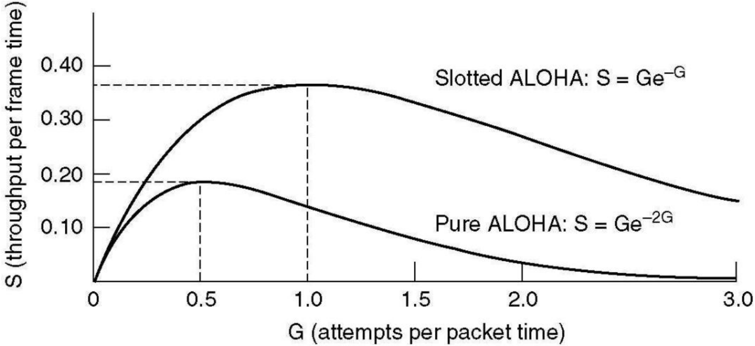
$$S = G \times \exp(-G)$$

  - The maximum throughput is

$$S_{max} = 0{,}368 \text{ for } G = 1{,}0$$

- Better performance but needs synchronization

Aloha (Comparative Performance)



Carrier Sense Multiple Acess (CSMA)

- The throughput of Aloha and Slotted Aloha are limited by the long vulnerability period
- CSMA protocols listen to the channel before transmitting
- Vulnerability period reduced to propagation time
- Proposed by Kleinrock and Tobagi (1975)
- Operation:
  - Station wishing to transmit first listen the medium to check if another transmission is in progress
  - If the medium is free, the station transmits
  - If medium is in use, station waits for a random backoff time
  - Collisions may still occur
  - Transmitter expects ACK; retransmit if ACK is not received

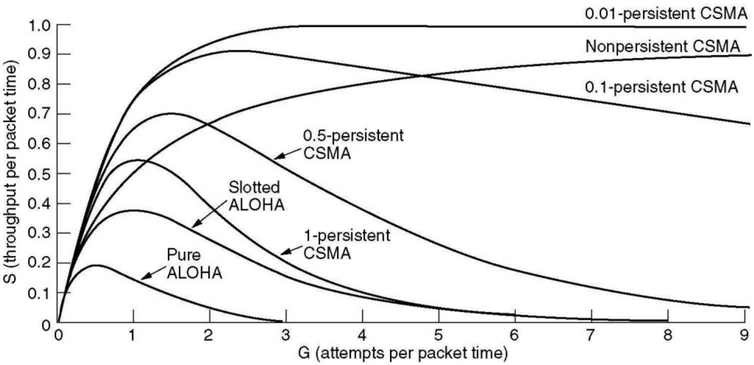
Flavors of CSMA

- Non-persistent CSMA
  - Transmits if the medium is free
  - Otherwise it waits for a random time before trying again
- 1-persistent CSMA
  - Transmits if the medium is free
  - Otherwise it waits for the medium to become free and then transmits immediately
  - In the event of a collision, it waits for a random time and restarts the transmission cycle again
- p-persistent CSMA
  - Transmits if the medium is free
  - Otherwise it waits for the medium to become free and then transmits with probability p
  - In the event of a collision, it waits for a random time and restarts the transmission cycle again

Advantages and Disadvantages

- If stations B and C want to transmit while station A is transmitting:
  - 1-persistent: B and C will collide
  - non-persistent: B and C probably will not collide
- If only station B wants to transmit while station A is transmitting:
  - 1-persistent: B transmits successfully immediately after A
  - non-persistent: B waits a random time even with the free channel

CSMA (Comparative Performance)

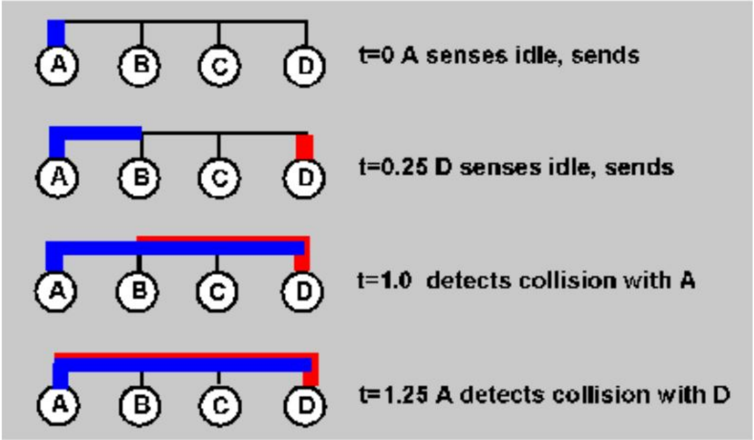


Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

- Problem: when frames collide the medium becomes unusable for the duration of both frames
- For long frames the loss is considerable
- Solution: stations listen while transmitting and thus detect collisions earlier
- Operation:
  - If the medium is free, it transmits
  - Otherwise, it waits until the medium becomes free and transmits with $p = 1$
  - In the event of a collision, it transmits a short signal of interference and then aborts the transmission
  - It waits for random time and tries again

Collision Detection

- Detection only works if stations can receive while transmitting

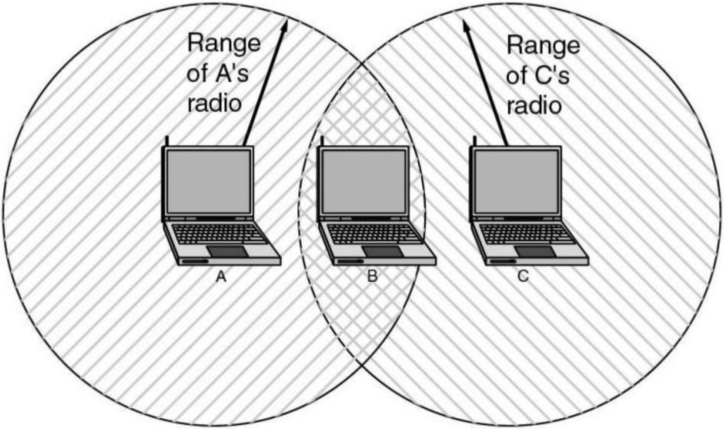


Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

- In radio transmissions, it is difficult to receive and transmit at the same time
  - How to detect collision if you can't hear while you are talking?
- Collision avoidance: better than is to avoid collisions
  - RTS/CTS Dialogue
    - RTS: Request to send
    - CTS: Clear to send
- Carrier detection (carrier sense, CS) does not always work well

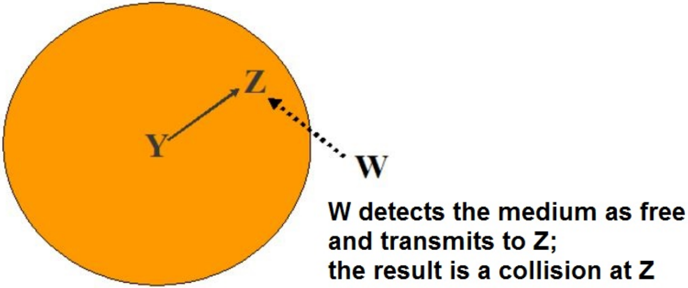
Problems with Carrier Detection

- The transmission range of one station may not cover the entire network



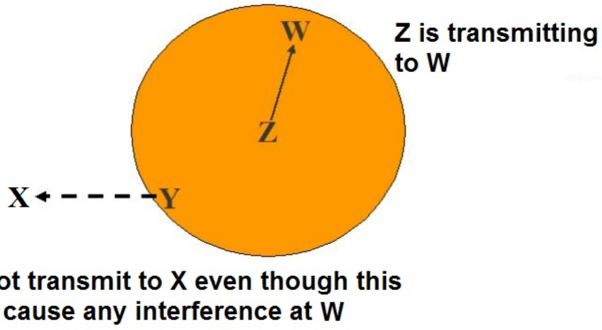
Problems with Carrier Detection

- Hidden terminal problem
  - Terminal W can't detect that Z is receiving a transmission from Y



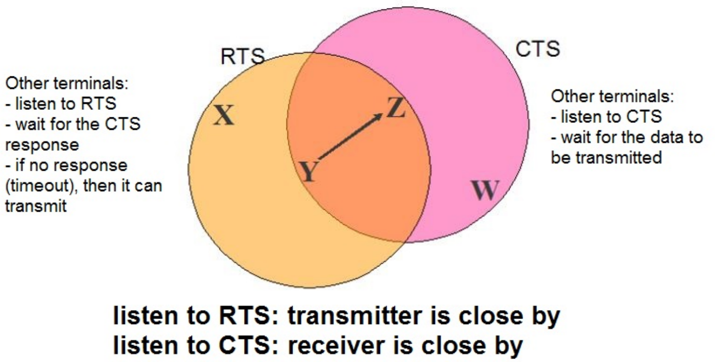
Problems with Carrier Detection

- Exposed terminal problem
  - Although possible, the transmission from Y to X does not happen



Minimizing Carrier Detection Problems

- RTS-CTS Dialogue

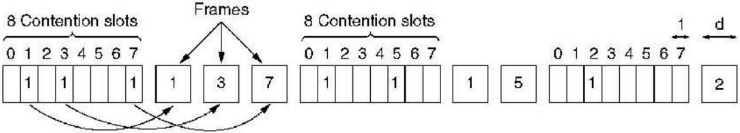


Random Access

- Advantages
  - Short delay for traffic bursts
  - Simple and with distributed control
  - Flexible to changes in number of terminals
  - Fair in the sharing of resources
- Disadvantages
  - Low channel efficiency for multi-terminal networks
  - Poor for continuous traffic (eg, voice)
  - Difficult to implement traffic priorities
  - High variance of delay times

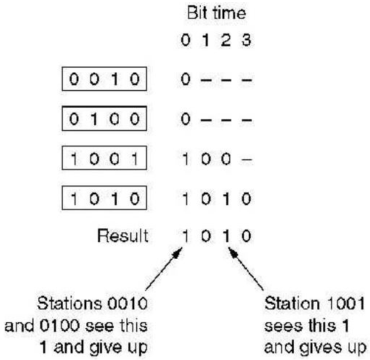
Bit-Map Reservation

- Fixed number of stations
- Station indicates intention to transmit during its slot in the contention period
- Problems in networks with large number of stations
- Lower-address stations wait longer on average than higher-address stations
- Protocol overhead is low even under low loads assuming reservation frames are shorter than data frames



Binary Decrement

- Uses the logical "or" effect by the medium
- Operation:
  - Stations transmit their address and observe the medium checking for overwrite
  - In case of overwrite they interrupt the transmission
  - Win the race to the station with the highest address

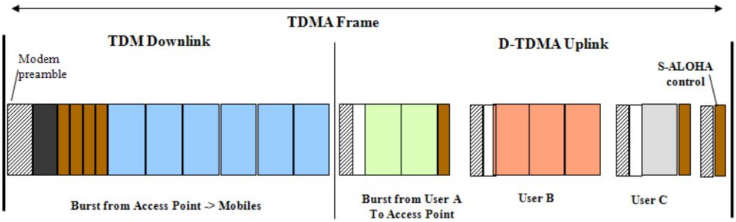


Dynamic TDMA

- Scheduling algorithm reserves a variable number of slots in each frame, depending on the demand of each user
- Previous negotiations determine how slots are allocated
- Advantages
  - Avoid contention and collisions
  - More efficient use of the channel, in particular with many users
- Disadvantages
  - Needs centralized control
  - Requires synchronization between terminals

Dynamic TDMA

- Example of a TDMA frame with uplink and downlink channels



IEEE 802.11 family

- IEEE 802.11
  - Published in 1997 for 1 or 2 Mbps
  - Infra-red link
  - Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) at 2.4 GHz
- IEEE 802.11b
  - Published in 1999 for up to 11 Mbps
  - High Rate DSSS (HR-DSSS) at 2.4 GHz
- IEEE 802.11a
  - Published in 1999 for up to 54 Mbps
  - Orthogonal Frequency Division Multiplexing (OFDM) at 5 GHz
- IEEE 802.11g
  - Published in 2003 for up to 54 Mbps
  - Orthogonal Frequency Division Multiplexing (OFDM) at 2.4 GHz
  - Compatible with 802.11b

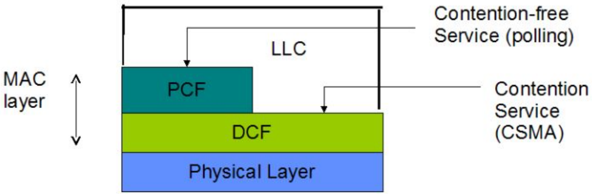
IEEE 802.11 family

- IEEE 802.11i
  - Published in 2004 as an amendment to the 802.11 standard
  - Specifies mechanisms for security
- IEEE 802.11e
  - Published in 2005 as an amendment to the 802.11 standard
  - Specifies mechanisms to provide Quality of Service (QoS)
- IEEE 802.11n
  - Published in 2009 for up to 600 Mbps
  - Up to 4 streams MIMO-OFDM at 2.4 and 5 GHz
- IEEE 802.11ac
  - Published in 2013 for up to 3466.8 Mbps with 256-QAM
  - Up to 8 streams MIMO-OFDM at 5 GHz

802.11b PCI Card

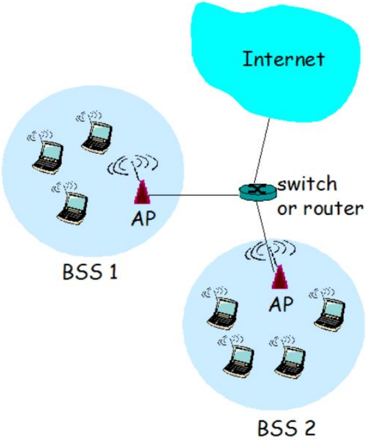
IEEE 802.11

- Distributed Coordination Function (DCF)
  - Decentralized operation using CSMA/CA
- Point Coordination Function (PCF)
  - Centralized operation, where the Access Point (AP) controls the activities of the network
    - AP polls stations
    - Service without collision because access to the environment is controlled by the AP
    - AP transmits a beacon frame with information about the system
  - Optional implementation



IEEE 802.11

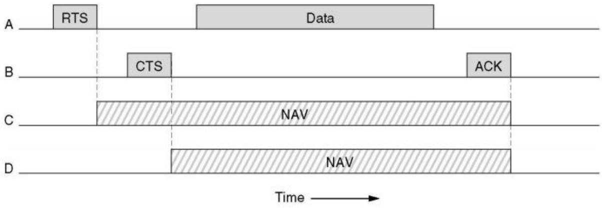
- Architecture



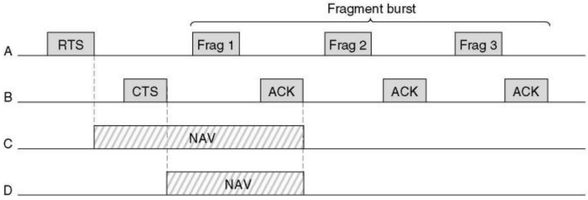
Legenda: Basic Service Set (BSS) is equivalent to a cell

IEEE 802.11

- Network Allocation Vector (NAV)

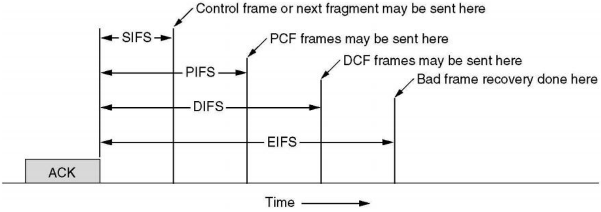


Fragment Burst:



IEEE 802.11

- Inter-Frame Spacing (IFS)



Key: Short Interframe Spacing (SIFS), PCF Interframe Spacing (PIFS),

DCF Interframe Spacing (DIFS) and Extended Interframe Spacing (EIFS)

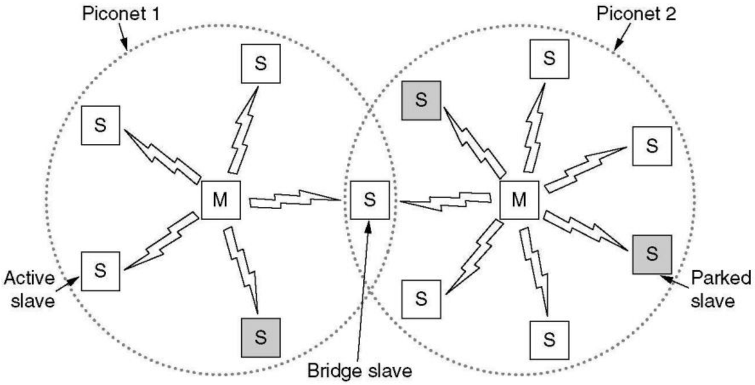
IEEE 802.11

- Services
  - Association and Disassociation
    - Mobile station attaches to and deattaches from access point
  - Reassociation
    - Equivalent to handover in base stations
  - Distribution
    - Data Routing
  - Integration
    - Interconnection with networks using other protocols
  - Authentication and Deauthentication
    - Identifies the caller to establish and release a secure connection
  - Privacy
    - Cryptography
  - Data delivery
    - Transmission and reception of data

Bluetooth

- Created by Ericsson, IBM, Intel, Nokia and Toshiba in the 90s
- Specification for Personal Area Network (PAN)
- Purpose of connecting devices, peripherals and accessories using short-range radio, low power and low cost
- Version 1.0 published in 1999; version 1.1 ratified as IEEE 802.15.1
- Piconet: network unit consisting of:
  - 1 master node
  - Up to 7 slaves nodes in the active state
  - Up to 255 nodes in the inactive (parked) or semi-inactive (sniff and hold) states
- Scatternet: set of interconnected piconets
- All communication is between master and slave

Bluetooth


Piconet 1
Piconet 2
S
S
S
S
S
M
S
M
S
S
S
S
S
S
S
Active slave
Parked slave
Bridge slave

Bluetooth

- Master
  - Provides synchronization and identification for the piconet
  - Control medium access using the round-robin scheme
  - Master (or slave) condition changes dynamically
- Active Slave
  - Active participant of the piconet
- Parked, Sniff and Hold
  - Several levels of piconet participation in energy-saving states

- Classes
  - Class 1, power 100 mW, range 100 m
  - Class 2, power 2,5 mW, range 10 m
  - Class 3, power 1 mW, range 1 m

Bluetooth

- Physical Layer
  - Uses the ISM band at 2,4 GHz
  - Band divided into 79 channels, each with 1 MHz
  - FSK modulation
  - Frequency Hopping with 1600 hops/s
  - Slots of 625 μs with 260 μs for synchronization
  - Bit period: 1 μs
- Any device must provide the following list of information when requested:
  - Device name
  - Device class
  - List of available services
  - Other information, such as manufacturer, device characteristics, version of implemented specifications, etc.

Bluetooth

- Asynchronous Connection-Less Link (ACL)
  - Used for sporadic or burst communication
  - Traffic offered on a best effort basis
  - Active slave can mantain up to one ACL connection
- Synchronous Connection Oriented (SCO)
  - Used for real-time communication
  - It has one fixed slot allocated in each direction
  - Active slave can mantain up to 3 SCO connections

- Bluetooth 2.0
  - Compatible with 1.x versions
  - Introduction of Enhanced Data Rate (EDR) that allows rates up to 2,1 Mbps
  - Better energy efficiency
  - Larger spectrum band use

Bluetooth

- Examples