Wireless Networking: IEEE802.11

Slides partially adapted from "Mobile Communications" by J. Schiller
Read Chapter 7.

Characteristics of wireless LANs

Advantages

- very flexible within the reception area
- Ad-hoc networks without previous planning possible
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

Disadvantages

- typically very low bandwidth compared to wired networks (1-11 Mbit/s)
- many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
- products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000

Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary

Comparison: infrared vs. radio transmission

Infrared
- uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)

Advantages
- simple, cheap, available in many mobile devices
- no licenses needed
- simple shielding possible

Disadvantages
- interference by sunlight, heat sources etc.
- many things shield or absorb IR light
- low bandwidth

Example
- IrDA (Infrared Data Association) interface available everywhere

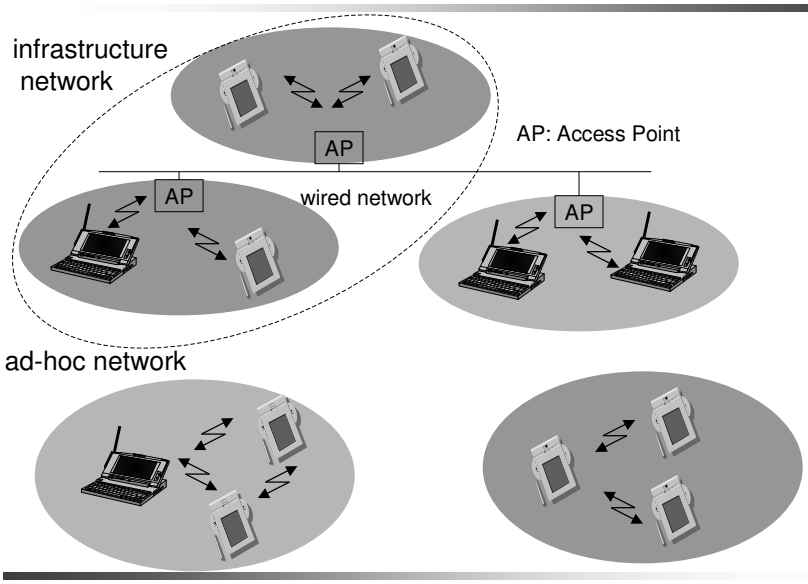
Radio
- typically using the license free ISM band at 2.4 GHz

Advantages
- experience from wireless WAN and mobile phones can be used
- coverage of larger areas possible (radio can penetrate walls, furniture etc.)

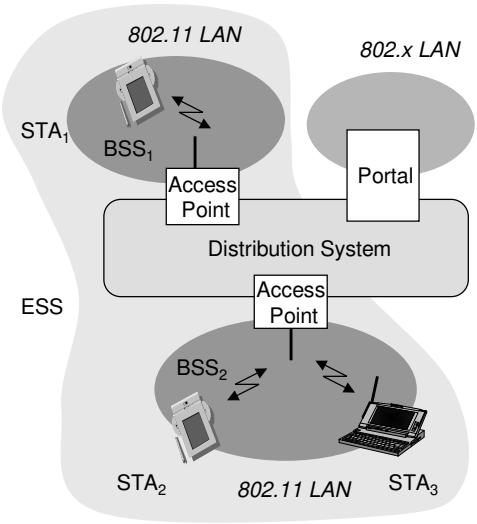
Disadvantages
- very limited license free frequency bands
- shielding more difficult, interference with other electrical devices

Example
- IEEE802.11, Bluetooth, Hiperlan

Comparison: infrastructure vs. ad-hoc networks



802.11 - Architecture of an infrastructure network



Station (STA)
- terminal with access mechanisms to the wireless medium and radio contact to the access point

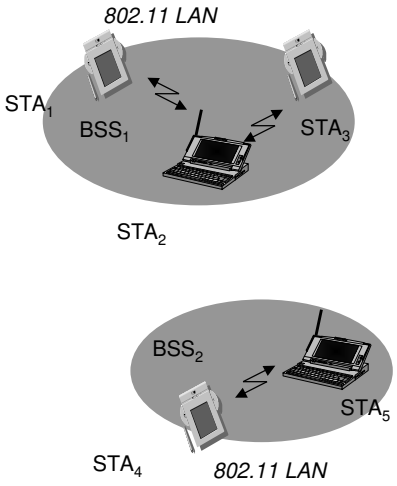
Basic Service Set (BSS)
- group of stations using the same radio frequency

Access Point
- station integrated into the wireless LAN and the distribution system

Portal
- bridge to other (wired) networks

Distribution System
- interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

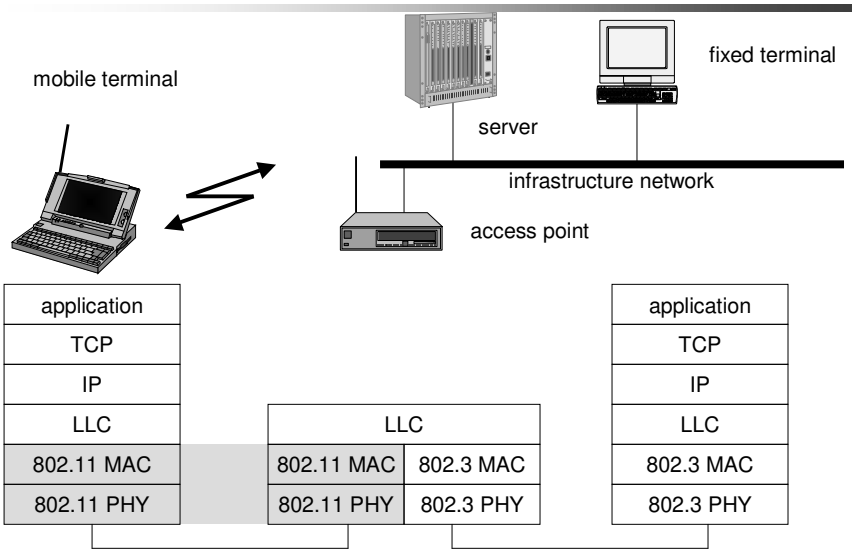
802.11 - Architecture of an ad-hoc network



Direct communication within a limited range

- Station (STA): terminal with access mechanisms to the wireless medium
- Basic Service Set (BSS): group of stations using the same radio frequency

IEEE standard 802.11



802.11 - Layers and functions

MAC
- access mechanisms, fragmentation, encryption

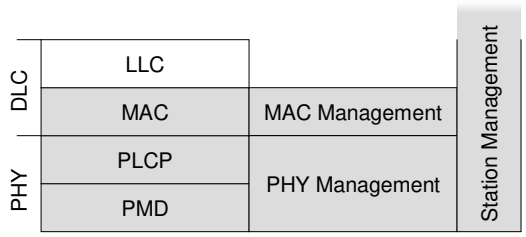
MAC Management
- synchronization, roaming, MIB, power management

PLCP Physical Layer Convergence Protocol
- clear channel assessment signal (carrier sense)

PMD Physical Medium Dependent
- modulation, coding

PHY Management
- channel selection, MIB

Station Management
- coordination of all management functions



802.11 - Physical layer

3 versions: 2 radio (typ. 2.4 GHz), 1 IR
- data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum)
- spreading, despreading, signal strength, typ. 1 Mbit/s
- min. 2.5 frequency hops/s (USA), two-level GFSK modulation

DSSS (Direct Sequence Spread Spectrum)
- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

Infrared
- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchonization

FHSS PHY packet format

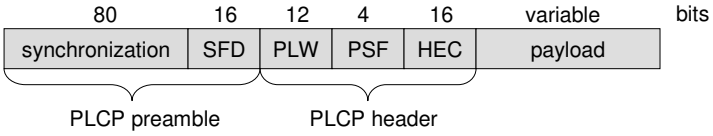
Synchronization
- synch with 010101... pattern

SFD (Start Frame Delimiter)
- 0000110010111101 start pattern

PLW (PLCP_PDU Length Word)
- length of payload incl. 32 bit CRC of payload, PLW < 4096

PSF (PLCP Signaling Field)
- data rate of payload (1 or 2 Mbit/s)

HEC (Header Error Check)
- CRC with $x^{16}+x^{12}+x^5+1$



DSSS PHY packet format

Synchronization
- synch., gain setting, energy detection, frequency offset compensation

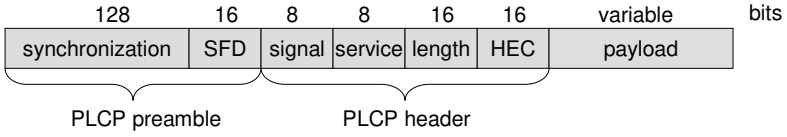
SFD (Start Frame Delimiter)
- 1111001110100000

Signal
- data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)

Service
- future use, 00: 802.11 compliant

Length
- length of the payload

HEC (Header Error Check)
- protection of signal, service and length, $x^{16}+x^{12}+x^5+1$



802.11 - MAC layer I - DFWMAC

Traffic services

- Asynchronous Data Service (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

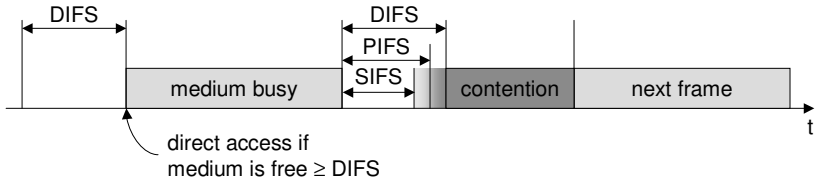
Access methods

- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- DFWMAC- PCF (optional)
  - access point polls terminals according to a list

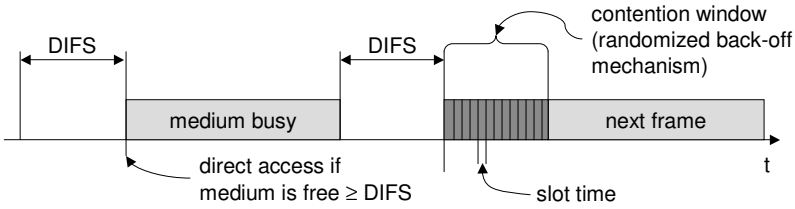
802.11 - MAC layer II

Priorities

- defined through different inter frame spaces
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service

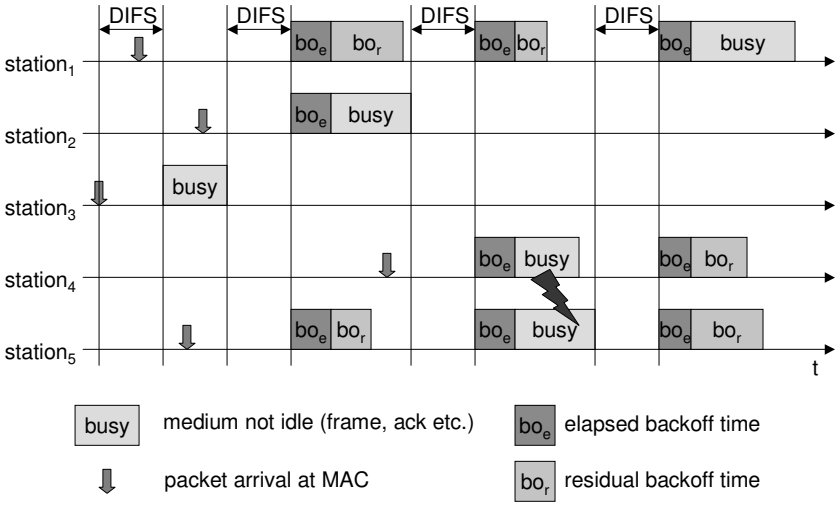


802.11 - CSMA/CA access method I



- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

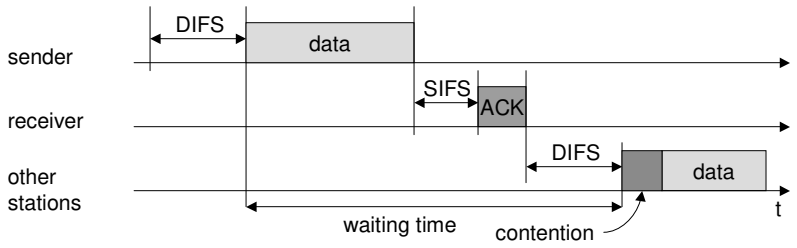
802.11 - competing stations - simple version



802.11 - CSMA/CA access method II

Sending unicast packets

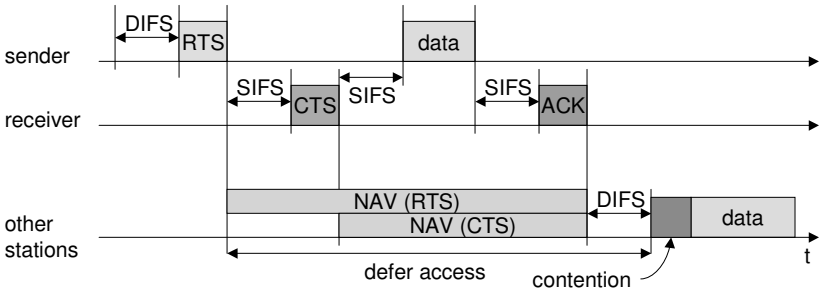
- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors



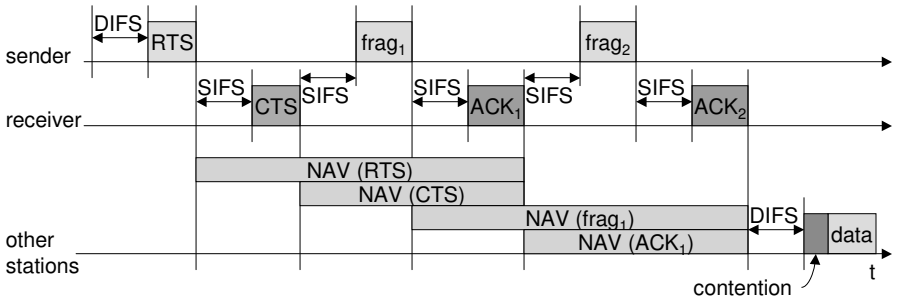
802.11 - DFWMAC

Sending unicast packets

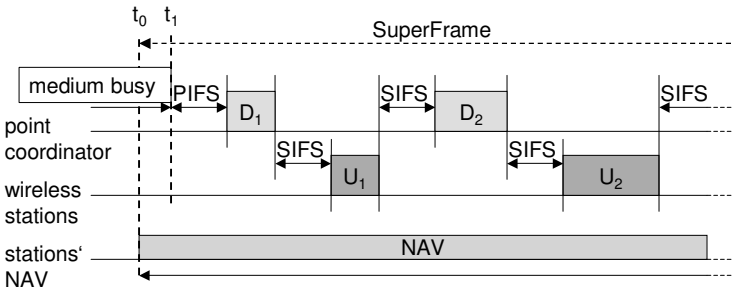
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS



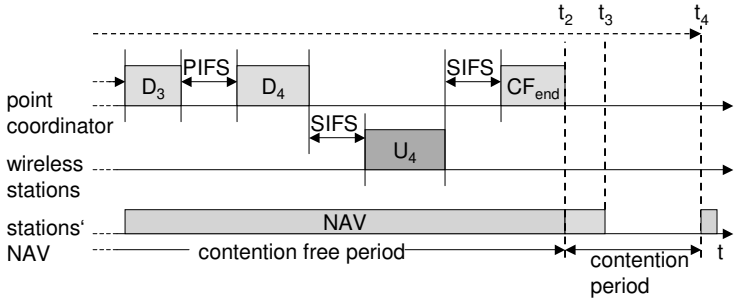
Fragmentation



DFWMAC-PCF I



DFWMAC-PCF II



802.11 - Frame format

Types
- control frames, management frames, data frames

Sequence numbers
- important against duplicated frames due to lost ACKs

Addresses
- receiver, transmitter (physical), BSS identifier, sender (logical)

Miscellaneous
- sending time, checksum, frame control, data

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

version, type, fragmentation, security, ...

MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

802.11 - MAC management

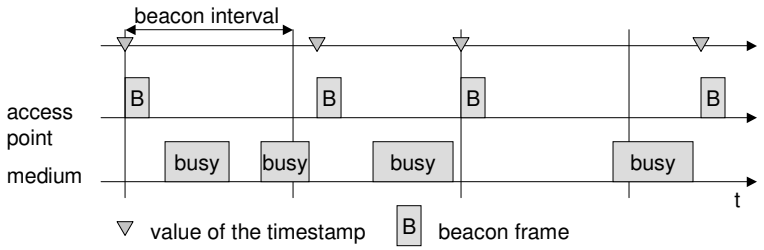
Synchronization
- try to find a LAN, try to stay within a LAN
- timer etc.

Power management
- sleep-mode without missing a message
- periodic sleep, frame buffering, traffic measurements

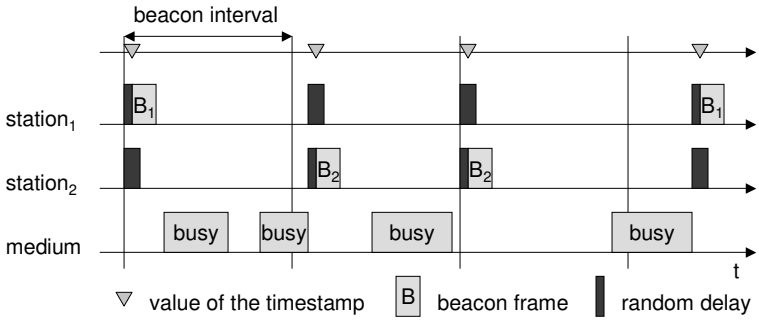
Association/Reassociation
- integration into a LAN
- roaming, i.e. change networks by changing access points
- scanning, i.e. active search for a network

MIB - Management Information Base
- managing, read, write

Synchronization using a Beacon (infrastructure)



Synchronization using a Beacon (ad-hoc)



Power management

Idea: switch the transceiver off if not needed

States of a station: sleep and awake

Timing Synchronization Function (TSF)

- stations wake up at the same time

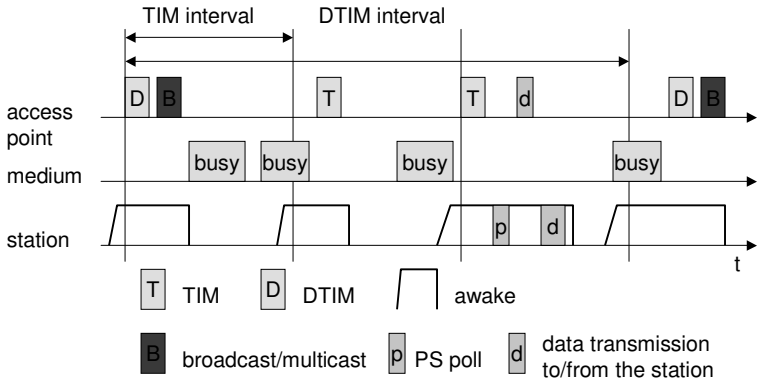
Infrastructure

- Traffic Indication Map (TIM)
  - list of unicast receivers transmitted by AP
- Delivery Traffic Indication Map (DTIM)
  - list of broadcast/multicast receivers transmitted by AP

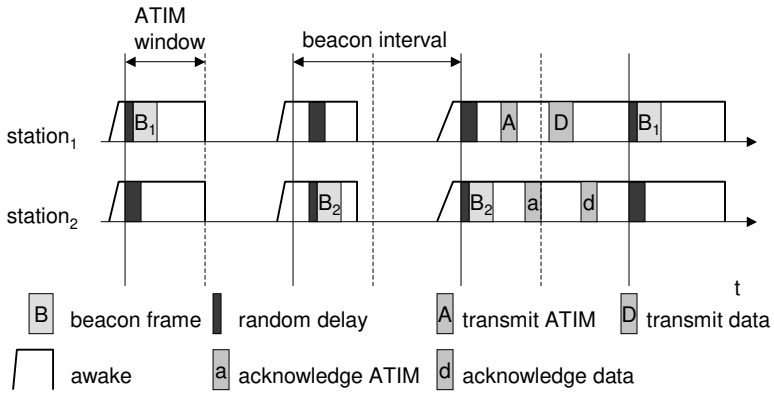
Ad-hoc

- Ad-hoc Traffic Indication Map (ATIM)
  - announcement of receivers by stations buffering frames
  - more complicated - no central AP
  - collision of ATIMs possible (scalability?)

Power saving with wake-up patterns (infrastructure)



Power saving with wake-up patterns (ad-hoc)



802.11 - Roaming

No or bad connection? Then perform:

Scanning

- scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer

Reassociation Request

- station sends a request to one or several AP(s)

Reassociation Response

- success: AP has answered, station can now participate
- failure: continue scanning

AP accepts Reassociation Request

- signal the new station to the distribution system
- the distribution system updates its data base (i.e., location information)
- typically, the distribution system now informs the old AP so it can release resources

Future developments

IEEE 802.11a
- compatible MAC, but now 5 GHz band
- transmission rates higher than 20 Mbit/s
- close cooperation with BRAN (ETSI Broadband Radio Access Network)

IEEE 802.11b
- higher data rates at 2.4 GHz
- proprietary solutions already offer 11 Mbit/s

IEEE WPAN (Wireless Personal Area Networks)
- market potential
- compatibility
- low cost/power, small form factor

Bluetooth

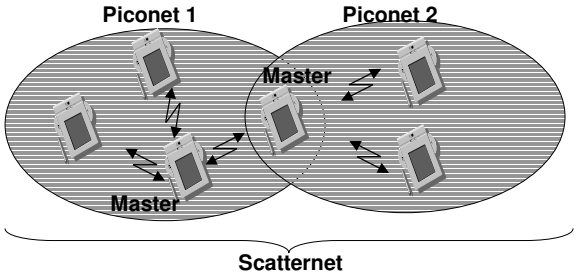
Consortium: Ericsson, Intel, IBM, Nokia, Toshiba - many other members

Scenarios:
- connection of peripheral devices
  - loudspeaker, joystick, headset
- support of ad-hoc networking
  - small devices, low-cost
- bridging of networks
  - e.g., GSM via mobile phone - Bluetooth - laptop

Simple, cheap, replacement of IrDA, low range, lower data rates, low-power
- Worldwide operation: 2.4 GHz,
- Resistance to jamming and selective frequency fading:
  - FHSS over 79 channels (of 1MHz each), 1600hops/s
- Coexistence of multiple piconets: CDMA
- Links: synchronous connections SCO (e.g., voice) and asynchronous connectionless ACL
- Interoperability: protocol stack supporting TCP/IP, OBEX, SDP
- Range: 10 meters, can be extended to 100 meters

Documentation: over 1000 pages specification:
www.ccs.neu.edu/course/com3525/ or from www.bluetooth.com

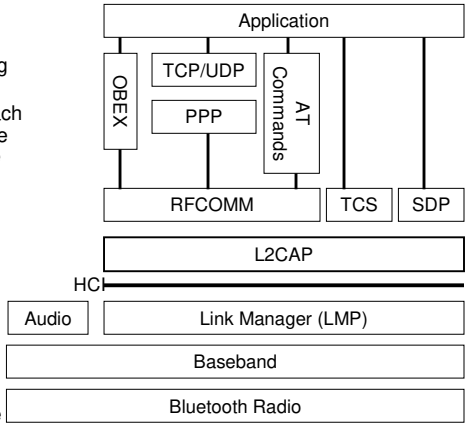
Network Topology



- Piconet = set of Bluetooth nodes synchronized to a master node
  - The piconet hopping sequence is derived from the master MAC address (BD_ADDR IEEE802 48 bits compatible address)
- Master-Slaves can switch roles
- Scatternet = set of piconets
- A node can only be master of one piconet. Why?

Protocol Architecture

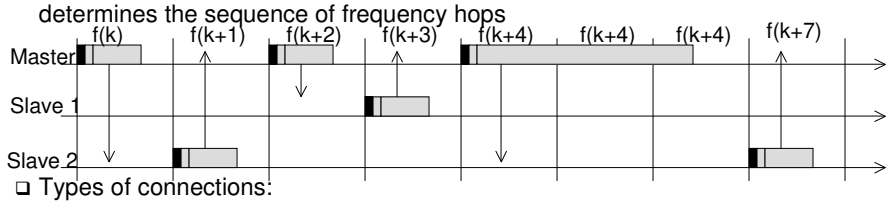
- BT **Radio** (2.4 GHZ Freq. Band): Modulation: Gaussian Frequency Shift Keying
- **Baseband**: FH-SS (79 carriers), CDMA (hopping sequence from the node MAC address)
- **Audio**: interfaces directly with the baseband. Each voice connection is over a 64Kbps SCO link. The voice coding scheme is the Continuous Variable Slope Delta (CVSD)
- Link Manager Protocol (**LMP**): link setup and control, authentication and encryption
- Host Controller Interface: provides a uniform method of access to the baseband, control registers, etc through USB, PCI, or UART
- Logical Link Control and Adaptation Layer (**L2CAP**): higher protocols multiplexing, packet segmentation/reassembly, QoS
- Service Discover Protocol (**SDP**): protocol of locating services provided by a Bluetooth device
- Telephony Control Specification (**TCS**): defines the call control signaling for the establishment of speech and data calls between Bluetooth devices
- **RFCOMM**: provides emulation of serial links (RS232). Upto 60 connections



OBEX: OBject EXchange (e.g., vCard)

Bluetooth Piconet MAC

- Each node has a Bluetooth Device Address (BD_ADDR). The master BD_ADDR determines the sequence of frequency hops

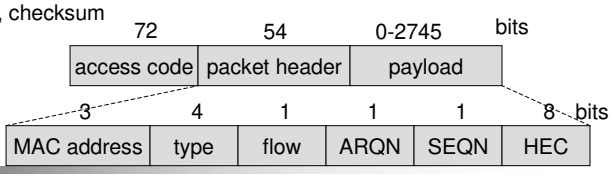


- Types of connections:

  Synchronous Connection-Oriented link (**SCO**) (symmetrical, circuit switched, point-to-point)

  Asynchronous Connectionless Link (**ACL**): (packet switched, point-2-multipoint, master-polls)

- Packet Format:
  - Access code: synchronization, when piconet active derived from master
  - Packet header (for ACL): 1/3-FEC, MAC address (1 master, 7 slaves), link type, alternating bit ARQ/SEQ, checksum



Types of packets

- SCO packets:

  Do not have a CRC (except for the data part of DV) and are never retransmitted. Intended for High-quality Voice (HV).

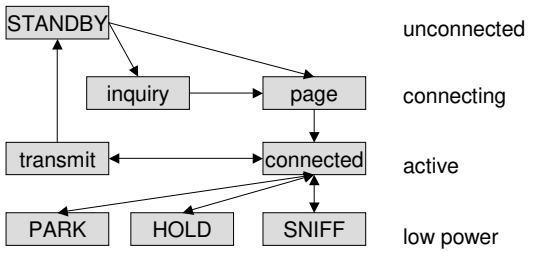
Type	Payload (bytes)	FEC	CRC	Symm. max-rate kbps
HV1	10	1/3	No	64
HV2	20	2/3	No	64
HV3	30	No	No	64
DV	10+(1-10)D	2/3D	Yes D	64+57.6D

- ACL packets: Data Medium-rate (DM) and Data High-rate (DH)

Type	Payload (bytes)	FEC	CRC	Symm. max-rate kbps	Asymm. max-rate (DL/UL)
DM1	0-17	2/3	Yes	108.8	108.8/108.9
DM3	0-121	2/3	Yes	258.1	387.2/54.4
DM5	0-224	2/3	Yes	286.7	477.8/36.3
DH1	0-27	No	Yes	172.8	172.8/172.8
DH3	0-183	No	Yes	390.4	585.6/86.4
DH5	0-339	no	Yes	433.9	723.2/185.6

States of a Bluetooth Device (PHY layer)

ACTIVE (connected/transmit): the device is uniquely identified by an AM_ADDR and is fully participating
SNIFF state: participates in the piconet only within the SNIFF interval
HOLD state: keeps only the SCO links
PARK state (low-power): release AM_ADDR but stay synchronized with master



BT device addressing:
- BD_ADDR (48 bits)
- AM_ADDR (3bits): ACTIVE, HOLD, or SNIFF
- PM_ADDR (8 bits): PARK Mode address (exchanged with the AM_ADDR when entering PARK mode)
- AR_ADDR (8 bits): not unique used to come back from PARK to ACTIVE state

Bluetooth Device Operation [Page 105 of 1084]

- Inquiry:
  - Goal: aims at discovering other neighboring devices
  - Inquiring node:
    - Sends an inquiry message (packet with only the access code: General Inquiry Access Code: GIAC or Dedicated IAC: DIAC). This message is sent over a subset of all possible frequencies.
    - The inquiry frequencies are divided into two hopping sets of 16 frequencies each.
    - In inquiry state the node will send upto $N_{INQUIRY}$ sequences on one set of 16 frequencies before switching to the other set of 16 frequencies. Upto 3 switches can be executed. Thus the inquiry may last upto 10.24 seconds.
  - To be discovered node:
    - Enters an inquiry_scan mode: listens over one frequency for $T_{w_inquiry_scal}$ time
    - When hearing the inquiry_message (and after a backoff procedure) enter and inquiry_response mode: send a Frequency Hop Sync (FHS) packet (BD_ADDR, native clock)
  - After discovering the neighbors and collecting information on their address and clock, the inquiring node can start a page routine to setup a piconet

Bluetooth Device Operation (Cont'd) [Page 102 of 1084]

- Page:
  - Goal: e.g., setup a piconet after an inquiry
  - Paging node (master):
    - Sends a page message (i.e., packet with only Device Access Code of paged node) over 32 frequency hops (from DAC and split into 2*16 freq.)
    - Repeated until a response is received
    - When a response is received send a FHS message to allow the paged node to synchronize
  - Paged node (slave):
    - Listens on its hopping sequence
    - When receiving a page message, send a page_response and wait for the FHS of the pager

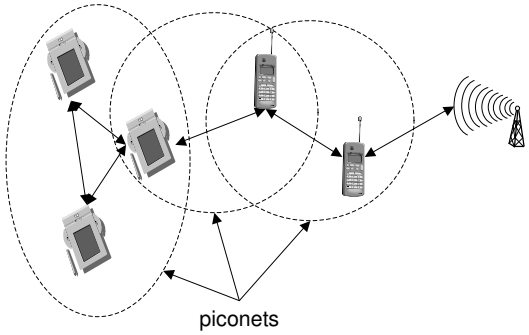
Link Manager Protocol

- Security: shared secret key
  - Authentication: challenge response
  - Weak Encryption: combination of (Linear Feedback Shift Registers) LFSR
- Connections setup/release (SCO/ACL)
- Master-slave switch
- Power-control
- Scheduling

Scatternets

Each piconet has one master and up to 7 slaves

Master determines hopping sequence, slaves have to synchronize

Participation in a piconet = synchronization to hopping sequence

Communication between piconets = devices jumping back and forth between the piconets