Mobile Communications
Chapter 7: Wireless LANs

- Characteristics
- HIPERLAN
  - Standards
    - PHY
    - MAC
  - Ad-hoc networks
    - Bluetooth

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 (1-10 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 very 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**
- WaveLAN, HIPERLAN, Bluetooth
Comparison: infrastructure vs. ad-hoc networks

**infrastructure network**
- Access Point (AP)
- Wired network

**ad-hoc network**
- Devices communicating directly

---

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 (ESS: Extended Service Set) based on several BSS
IEEE standard 802.11

- **Mobile terminal**
- **Fixed terminal**
- **Server**
- **Infrastructure network**
- **Access point**
- **Application**
- **TCP**
- **IP**
- **LLC**
- **802.11 MAC**
- **802.11 PHY**

- **IEEE 802.11**
  - **PHY**
  - **MAC**
  - **LLC**
  - **IP**
  - **TCP**

- **IEEE 802.3**
  - **PHY**
  - **MAC**
  - **LLC**
  - **IP**
  - **TCP**
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 (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, synchronization
### 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 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)
- 111001110100000

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

Service Length
- future use, 00: 802.11 compliant
- 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
- no guaranteed, hard priorities
- 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

<table>
<thead>
<tr>
<th>SIFS</th>
<th>PIFS</th>
<th>DIFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>medium busy</td>
<td>contention</td>
<td>next frame</td>
</tr>
</tbody>
</table>

Mobile Communications: Wireless LANs 7.12.1

Jochen H. Schiller
1999 7.7
Mobile Communications: Wireless LANs

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

- Station 1
- Station 2
- Station 3
- Station 4
- Station 5

Busy medium not idle (frame, ack etc.)
Packet arrival at MAC
Elapsed backoff time
Residual backoff time
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

Mobile Communications: Wireless LANs

DFWMAC-PCF I

Mobile Communications: Wireless LANs
DFWMAC-PCF II

- point coordinator
- wireless stations
- stations’ NAV
- NAV contention free period
- contention period

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

<table>
<thead>
<tr>
<th>bytes</th>
<th>Frame Control</th>
<th>Duration</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Sequence Control</th>
<th>Address 4</th>
<th>Data</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>0-2312</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

version, type, fragmentation, security, ...
MAC address format

<table>
<thead>
<tr>
<th>scenario</th>
<th>to DS</th>
<th>from DS</th>
<th>address 1</th>
<th>address 2</th>
<th>address 3</th>
<th>address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad-hoc network</td>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, from AP</td>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, to AP</td>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>DA</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>infrastructure network, within DS</td>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

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)**

![Diagram showing TIM and DTIM intervals with various states of the medium and station.](image-url)
### Power saving with wake-up patterns (ad-hoc)

![Diagram showing the power saving with wake-up patterns (ad-hoc)]

**Diagram Explanation:**
- **ATIM window**: Period during which a station can transmit an ATIM frame.
- **beacon interval**: Time between beacons.
- **Station 1**: Shows events such as beacon frame, random delay, transmit ATIM, transmit data, and acknowledge ATIM.
- **Station 2**: Shows similar events with slight variations.

### 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 up to 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 10 Mbit/s

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

ETSI - HIPERLAN

ETSI standard
- European standard, cf. GSM, DECT, ...
- Enhancement of local Networks and interworking with fixed networks
- integration of time-sensitive services from the early beginning

HIPERLAN family
- one standard cannot satisfy all requirements
  - range, bandwidth, QoS support
  - commercial constraints
- HIPERLAN 1 standardized since 1996
Overview: original HIPERLAN protocol family

<table>
<thead>
<tr>
<th>HIPERLAN 1</th>
<th>HIPERLAN 2</th>
<th>HIPERLAN 3</th>
<th>HIPERLAN 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>wireless LAN</td>
<td>access to ATM fixed networks</td>
<td>wireless local loop</td>
</tr>
<tr>
<td>Frequency</td>
<td>5.1-5.3GHz</td>
<td>17.2-17.3GHz</td>
<td></td>
</tr>
<tr>
<td>Topology</td>
<td>decentralized ad-hoc/infrastructure</td>
<td>cellular, centralized</td>
<td>point-to-multipoint</td>
</tr>
<tr>
<td>Antenna</td>
<td>omni-directional</td>
<td>directional</td>
<td></td>
</tr>
<tr>
<td>Range</td>
<td>50 m</td>
<td>50-100 m</td>
<td>5000 m</td>
</tr>
<tr>
<td>QoS</td>
<td>statistical</td>
<td>ATM traffic classes (VBR, CBR, ABR, UBR)</td>
<td></td>
</tr>
<tr>
<td>Mobility</td>
<td>&lt;10m/s</td>
<td>stationary</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>conventional LAN</td>
<td>ATM networks</td>
<td></td>
</tr>
<tr>
<td>Data rate</td>
<td>23.5 Mbit/s</td>
<td>&gt;20 Mbit/s</td>
<td>155 Mbit/s</td>
</tr>
<tr>
<td>Power conservation</td>
<td>yes</td>
<td>not necessary</td>
<td></td>
</tr>
</tbody>
</table>

Check out Wireless ATM for new names!

HIPERLAN 1 - Characteristics

Data transmission
- point-to-point, point-to-multipoint, connectionless
- 23.5 Mbit/s, 1 W power, 2383 byte max. packet size

Services
- asynchronous and time-bounded services with hierarchical priorities
- compatible with ISO MAC

Topology
- infrastructure or ad-hoc networks
- transmission range can be larger than coverage of a single node ("forwarding" integrated in mobile terminals)

Further mechanisms
- power saving, encryption, checksums
HIPERLAN 1 - Services and protocols

CAC service
- definition of communication services over a shared medium
- specification of access priorities
- abstraction of media characteristics

MAC protocol
- MAC service, compatible with ISO MAC and ISO MAC bridges
- uses HIPERLAN CAC

CAC protocol
- provides a CAC service, uses the PHY layer, specifies hierarchical access mechanisms for one or several channels

Physical protocol
- send and receive mechanisms, synchronization, FEC, modulation, signal strength

HIPERLAN layers, services, and protocols
**HIPERLAN 1 - Physical layer**

**Scope**
- modulation, demodulation, bit and frame synchronization
- forward error correction mechanisms
- measurements of signal strength
- channel sensing

**Channels**
- 3 mandatory and 2 optional channels (with their carrier frequencies)
- mandatory
  - channel 0: 5.1764680 GHz
  - channel 1: 5.1999974 GHz
  - channel 2: 5.2235268 GHz
- optional (not allowed in all countries)
  - channel 3: 5.2470562 GHz
  - channel 4: 5.2705856 GHz

**HIPERLAN 1 - Physical layer frames**

Maintaining a high data-rate (23.5 Mbit/s) is power consuming - problematic for mobile terminals
- packet header with low bit-rate comprising receiver information
- only receiver(s) address by a packet continue receiving

**Frame structure**
- LBR (Low Bit-Rate) header with 1.4 Mbit/s
- 450 bit synchronization
- minimum 1, maximum 47 frames with 496 bit each
- for higher velocities of the mobile terminal (> 1.4 m/s) the maximum number of frames has to be reduced

**Modulation**
- GMSK for high bit-rate, FSK for LBR header
**HIPERLAN 1 - CAC sublayer**

Channel Access Control (CAC)
- assure that terminal does not access forbidden channels
- priority scheme, access with EY-NPMA

Priorities
- 5 priority levels for QoS support
- QoS is mapped onto a priority level with the help of the packet lifetime (set by an application)
  - if packet lifetime = 0 it makes no sense to forward the packet to the receiver any longer
  - standard start value 500ms, maximum 16000ms
  - if a terminal cannot send the packet due to its current priority, waiting time is permanently subtracted from lifetime
  - based on packet lifetime, waiting time in a sender and number of hops to the receiver, the packet is assigned to one out of five priorities
  - the priority of waiting packets, therefore, rises automatically

**HIPERLAN 1 - EY-NPMA I**

EY-NPMA (Elimination Yield Non-preemptive Priority Multiple Access)
- 3 phases: priority resolution, contention resolution, transmission
- finding the highest priority
  - every priority corresponds to a time-slot to send in the first phase, the higher the priority the earlier the time-slot to send
  - higher priorities can not be preempted
  - if an earlier time-slot for a higher priority remains empty, stations with the next lower priority might send
  - after this first phase the highest current priority has been determined
HIPERLAN 1 - EY-NPMA II

Several terminals can now have the same priority and wish to send

- contention phase
  - Elimination Burst: all remaining terminals send a burst to eliminate contenders (1111010100010011100001100010110, high bit-rate)
  - Elimination Survival Verification: contenders now sense the channel, if the channel is free they can continue, otherwise they have been eliminated
  - Yield Listening: contenders again listen in slots with a nonzero probability, if the terminal senses its slot idle it is free to transmit at the end of the contention phase
  - the important part is now to set the parameters for burst duration and channel sensing (slot-based, exponentially distributed)

- data transmission
  - the winner can now send its data (however, a small chance of collision remains)
  - if the channel was idle for a longer time (min. for a duration of 1700 bit) a terminal can send at once without using EY-NPMA

- synchronization using the last data transmission

HIPERLAN 1 - DT-HCPDU/AK-HCPDU

<table>
<thead>
<tr>
<th>LBR</th>
<th>0 1 2 3 4 5 6 7</th>
<th>bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>HBR</td>
<td>0 1 2 3 4 5 6 7</td>
<td>byte</td>
</tr>
</tbody>
</table>

LBR:
- LBR: HBR-part Indicator
- HDAC: HDA CheckSum
- BLIR: Block Length Indicator
- TDIR: Type Indicator
- SC: Source Address
- UD: User Data (1-2422 byte)
- PAD: Padding
- CS: CheckSum
- AIDS: AID CheckSum

HBR:
- TI: Type Indicator
- SA: Destination Address
- UD: User Data (1-2422 byte)
- PAD: Padding
- CS: CheckSum
- AIDS: AID CheckSum

Acknowledgement HCPDU:
- HI: HBR-part Indicator
- HDA: Hashed Destination HCSAP Address
- HDAC: HDA CheckSum
- BLIR: Block Length Indicator
- TDIR: Type Indicator
- SA: Source Address
- UD: User Data (1-2422 byte)
- PAD: Padding
- CS: CheckSum
- AIDS: AID CheckSum
HIPERLAN 1 - MAC layer

Compatible to ISO MAC
Supports time-bounded services via a priority scheme
Packet forwarding
- support of directed (point-to-point) forwarding and broadcast
  forwarding (if no path information is available)
- support of QoS while forwarding
Encryption mechanisms
- mechanisms integrated, but without key management
Power conservation mechanisms
- mobile terminals can agree upon awake patterns (e.g., periodic
  wake-ups to receive data)
- additionally, some nodes in the networks must be able to buffer
  data for sleeping terminals and to forward them at the right time (so
called stores)

HIPERLAN 1 - DT-HMPDU

<table>
<thead>
<tr>
<th>Bit</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>LI: Length Indicator</td>
<td>1–2</td>
</tr>
<tr>
<td>1</td>
<td>TI: Type Indicator</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>RL: Residual Lifetime</td>
<td>4–5</td>
</tr>
<tr>
<td>3–5</td>
<td>PSN: Sequence Number</td>
<td>6–7</td>
</tr>
<tr>
<td>6–7</td>
<td>DA: Destination Address</td>
<td>8–13</td>
</tr>
<tr>
<td>8–13</td>
<td>SA: Source Address</td>
<td>14–19</td>
</tr>
<tr>
<td>14–19</td>
<td>ADA: Alias Destination Address</td>
<td>20–25</td>
</tr>
<tr>
<td>20–25</td>
<td>ASA: Alias Source Address</td>
<td>26–31</td>
</tr>
<tr>
<td>26–31</td>
<td>UP: User Priority</td>
<td>32</td>
</tr>
<tr>
<td>32</td>
<td>ML: MSDU Lifetime</td>
<td>33</td>
</tr>
<tr>
<td>33</td>
<td>KID: Key Identifier</td>
<td>34</td>
</tr>
<tr>
<td>34</td>
<td>IV: Initialization Vector</td>
<td>35–37</td>
</tr>
<tr>
<td>35–37</td>
<td>UD: User Data, 1–2383 byte</td>
<td>38–(n-2)</td>
</tr>
<tr>
<td>38–(n-2)</td>
<td>SC: Sanity Check (for the</td>
<td>(n-1)–n</td>
</tr>
</tbody>
</table>

Data HMPDU \(n = 40–2422\)
Information bases

Route Information Base (RIB) - how to reach a destination
- [destination, next hop, distance]

Neighbor Information Base (NIB) - status of direct neighbors
- [neighbor, status]

Hello Information Base (HIB) - status of destination (via next hop)
- [destination, status, next hop]

Alias Information Base (AIB) - address of nodes outside the net
- [original MSAP address, alias MSAP address]

Source Multipoint Relay Information Base (SMRIB) - current MP status
- [local multipoint forwarder, multipoint relay set]

Topology Information Base (TIB) - current HIPERLAN topology
- [destination, forwarder, sequence]

Duplicate Detection Information Base (DDIB) - remove duplicates
- [source, sequence]

Ad-hoc networks using HIPERLAN 1

Information Bases (IB):
- RIB: Route
- NIB: Neighbor
- HIB: Hello
- AIB: Alias
- SMRIB: Source Multipoint Relay
- TIB: Topology
- DDIB: Duplicate Detection

Forwarder

1. Forwarder
2. Forwarder
3. Forwarder
4. Forwarder
5. Forwarder
6. Forwarder

neighborhood
(i.e., within radio range)
Bluetooth

Consortium: Ericsson, Intel, IBM, Nokia, Toshiba - many 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 ofIrDA, low range, lower data rates
- 2.4 GHz, FHSS, TDD, CDMA

States of a Bluetooth device (PHY layer)

- STANDBY
- inquiry
- page
- transmit
- connected
- PARK
- HOLD
- SNIFF
- unconnected
- connecting
- active
- low power
Bluetooth MAC layer

- Synchronous Connection-Oriented link (SCO)
  - symmetrical, circuit switched, point-to-point
- Asynchronous Connectionless Link (ACL)
  - packet switched, point-to-multipoint, master polls

Access code
- synchronization, derived from master, unique per channel

Packet header
- 1/3-FEC, MAC address (1 master, 7 slaves), link type, alternating bit ARQ/SEQ, checksum

<table>
<thead>
<tr>
<th>access code</th>
<th>packet header</th>
<th>payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>72</td>
<td>54</td>
<td>0-2745</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC address</th>
<th>type</th>
<th>flow</th>
<th>ARQN</th>
<th>SEQN</th>
<th>HEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>8</td>
</tr>
</tbody>
</table>

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