APPLICATION PROGRAMMING: MOBILE COMPUTING [INEA00112W]

Marek Piasecki PhD

Wireless Networks (W7/2013)

Choose yourself and new technologies

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!

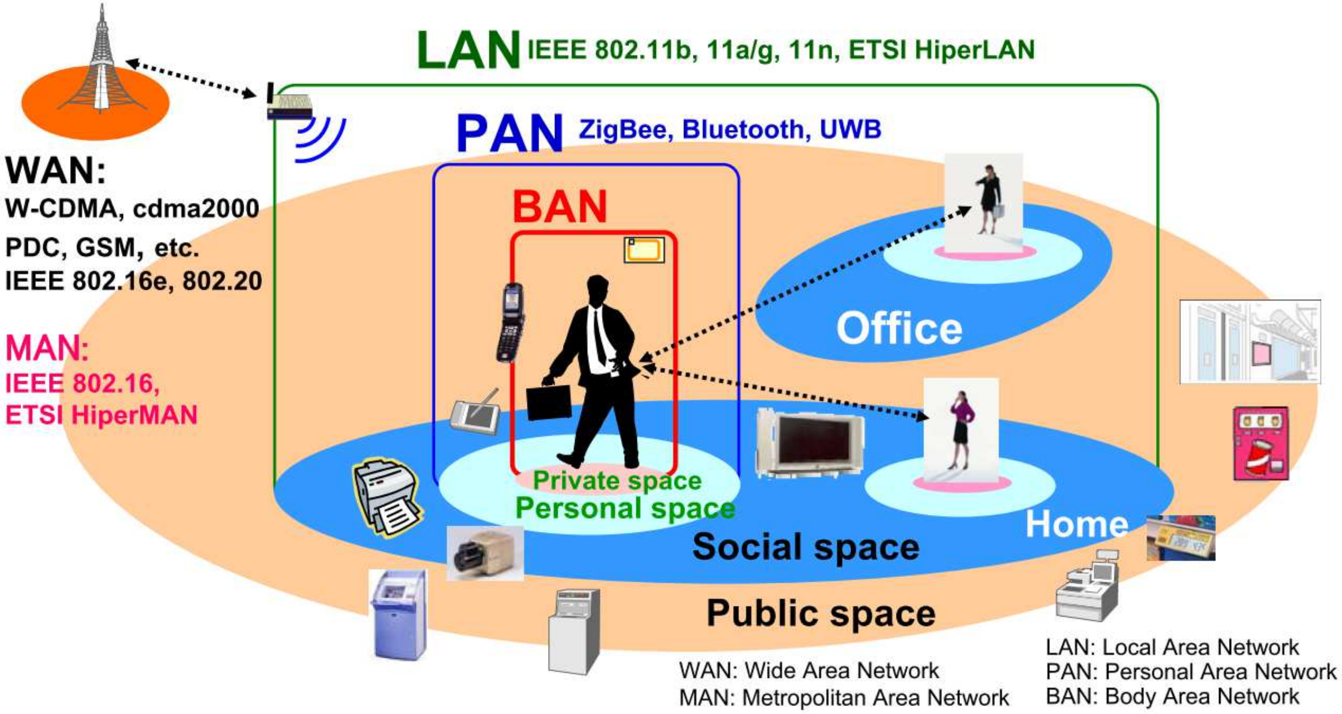
Wrocław University of Technology

EUROPEAN SOCIAL FUND

Project co-financed from the EU European Social Fund

Wireless Vision

Systems/networks should be constructed around the user



WAN: Wide Area Network
MAN: Metropolitan Area Network

LAN: Local Area Network
PAN: Personal Area Network
BAN: Body Area Network

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!
Wrocław University of Technology
EUROPEAN SOCIAL FUND
Project co-financed from the EU European Social Fund

Wireless Networks - Advantages

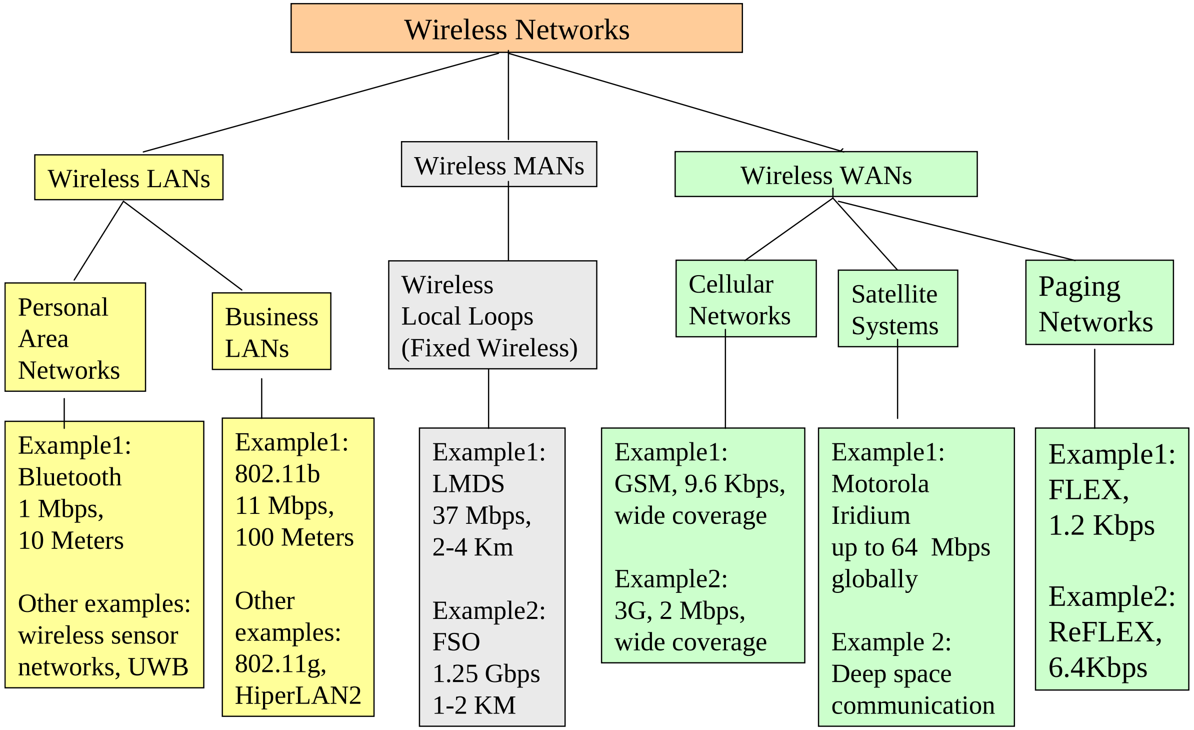
- Very flexible within the reception area
- Possible Ad-hoc networks without previous planning
- Low power for battery use
- No problems with cables / wiring difficulties (faster to build, no intrusion in historic buildings, etc.)
- Easy to use for everyone, simple management
- More robust against disasters like: earthquakes, flood, fire or users „pulling a plug”

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!
Wrocław University of Technology
EUROPEAN SOCIAL FUND
Project co-financed from the EU European Social Fund

Wireless Networks - Disadvantages

- Typically very low bandwidth compared to wired networks (1-10 Mbit/s)
- Interferences,
  higher error rate on the transmission link in comparison to Standard-LANs
  (radio emissions of electric devices, engines, lightning, …)
- No international standards at used frequency bands → Industrial Scientific Medical (ISM) band
- Restrictive regulations of frequencies → frequencies have to be coordinated, useful frequencies are almost all occupied
- Products have to follow many national restrictions if working wireless,
  it takes a very long time to establish global solutions
- Shared medium → lower security, simpler active attacking,
  need of secure access mechanisms

Different Wireless Networks



Wireless Networks

Wireless LANs

Wireless MANs

Wireless WANs

Personal Area Networks

Business LANs

Wireless Local Loops (Fixed Wireless)

Cellular Networks

Satellite Systems

Paging Networks

Example1:
Bluetooth
1 Mbps,
10 Meters

Other examples:
wireless sensor
networks, UWB

Example1:
802.11b
11 Mbps,
100 Meters

Other
examples:
802.11g,
HiperLAN2

Example1:
LMDS
37 Mbps,
2-4 Km

Example2:
FSO
1.25 Gbps
1-2 KM

Example1:
GSM, 9.6 Kbps,
wide coverage

Example2:
3G, 2 Mbps,
wide coverage

Example1:
Motorola
Iridium
up to 64 Mbps
globally

Example 2:
Deep space
communication

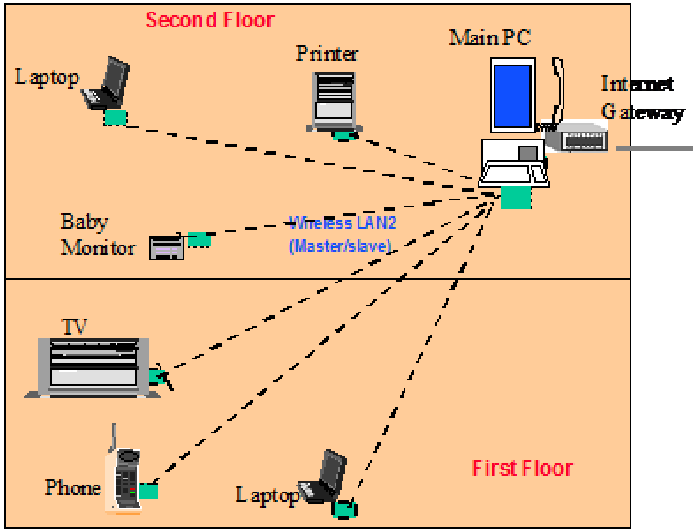
Example1:
FLEX,
1.2 Kbps

Example2:
ReFLEX,
6.4Kbps

WPAN

(Wireless Personal Area Networks)

- **Technologies:**
  - IrDA, Bluetooth, Zigbee,
  - Wireless Sensors
- **Applications:**
  - connection to peripherals
  - remote control
  - payment without physical contact
  - home networking



Infrared vs Radio

(for Personal Area Networks)

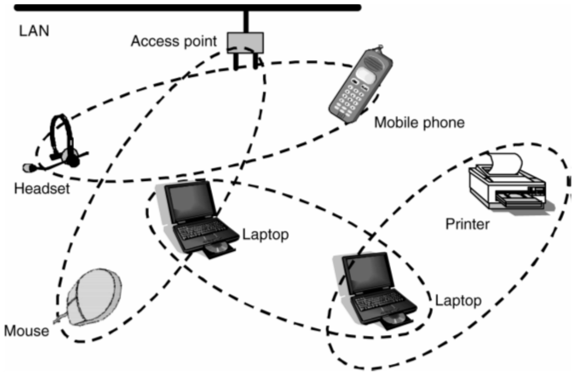
INFRARED uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.) direct light in case of LOS, one to one	**RADIO** typically using the license free ISM band at 2.4 GHz
Advantages • simple, cheap, available in many mobile devices • no licenses needed • simple shielding possible	**Advantages** • experience from wireless WAN and mobile phones can be used • coverage of larger areas possible (radio can penetrate walls, furniture etc.)
Disadvantages • interference by sunlight, heat sources etc. • many things shield or absorb IR light • low bandwidth	**Disadvantages** • very limited license-free frequency bands • shielding more difficult, • interference with other electrical devices
Example IrDA (Infrared Data Association) 115 Kbps , 1.152 & 4 Mbps, IEEE 802.11	**Example** IEEE802.11, HIPERLAN, Bluetooth

Bluetooth®

(Harald Bluetooth was the King of Denmark in the 10th century)

- Simple, cheap (less then $5 a piece), replacement of IrDA, low range, unlicensed frequency 2.4 GHz, FHSS, TDD, CDMA
- Initiated by Ericsson, Intel, IBM, Nokia, Toshiba;
  Open Standard: IEEE 802.15.1
- Generally for wireless Ad-hoc-piconets (range < 10m);
- Data rates:
  - 433,9 kBit/s asynchronous-symmetrical
  - 723,2 kBit/s / 57,6 kbit/s asynchronous-asymmetrical
  - 64 kBit/s synchronous, voice service
  - Extensions up to 20 Mbit/s → IEEE 802.15.3a – UWB (Ultra Wide Band)
- Integrated security (128 bit encryption)

Bluetooth (cont.)



Example applications:

- 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)
- „Intelligent Shop“ → shop informs the buyer about special offers via mobile phone or handles interactive inquiries for offers
- Bluetooth-capable ticket machine → Payment over mobile telephone is carried out without physical contact
- Control of home appliances by mobile telephone
  as remote control of heating or security

„Bluecasting”

Service provided by a **Bluetooth kiosk** →

e.g. BrightTouch kiosks delivering free videos from Universal Music Group to customers witin HMV stores

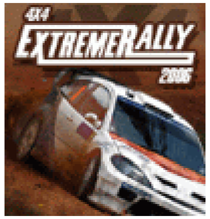
or Bluetooth enabled **news/hoarding** ↓

Examples from www.bluecasting.com:

- MTV's The Bedrooom Diaries MTV show
- Pepsi + Yahoo! Music → 80 bus shelters across New York deliver bi-weekly updates on the newest bands
- PorscheOpen - International Tournament ATP

Bluetooth Gaming

- Bluetooth multiplayer games
- Users have to be within a limited distance
  to get connected.
- In standard type of connection, the game mode
  can only be one to one.
  Utilising pico/scatternet, more players could
  participate in the same game.
- Could be played on different mobile phones
  and PDA's: e.g. Nokia, Ericsson and Motorola



Frequency & Baseband

- Bluetooth uses the unlicensed ISM frequency band around 2.4GHz
- Modulation technique used is Gaussian Frequency Shift Keying (GFSK).
- Bluetooth uses Frequency Hopping Spread Spectrum.
  - 79 different frequencies used in most countries.
  - 1600 hops/sec (or 1 hop every 625 µs).
  - Hop sequence based on master's 48bit hardware address.

Power Level Classes / Security

Three different transmission power levels:

- **Class 3** (1mW) approx. 10 meter range (most popular!)
- **Class 2** (2.5mW) approx. 20 meter range
- **Class 1** (100mW) approx. 100 meter range

Security is provided in three ways:

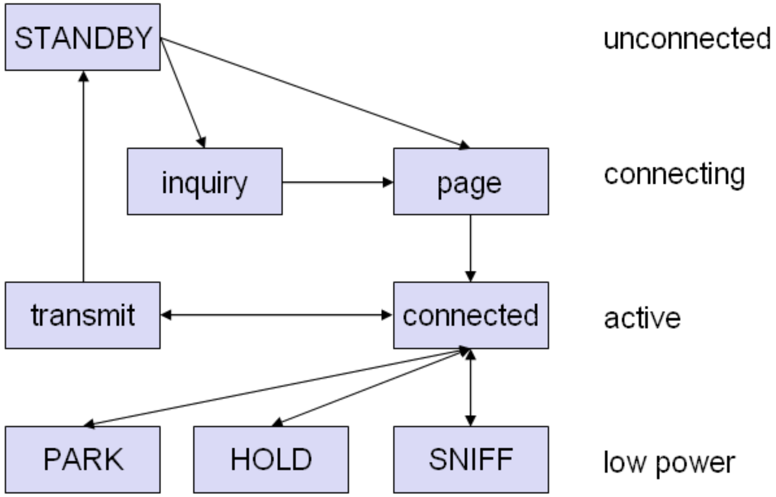
- Pseudo-random frequency hopping
- Authentication
- Encryption

Bluetooth Profile Types

1. **GAP** - **generic access profile**, which enables other profiles and defines how to do other services
2. **SPP** - **serial port profile** (over RFCOMM), such as printers use
3. **PAN** - **personal area network**, such as headset and phone, or laptop and phone
4. **SP** - **synchronisation profile**, such as syncing contacts from phone to laptop
5. **SDAP** - **service discovery application profile**,
   eg. when you look for BT enabled devices (inquiry)
   and their offered services (discovery)

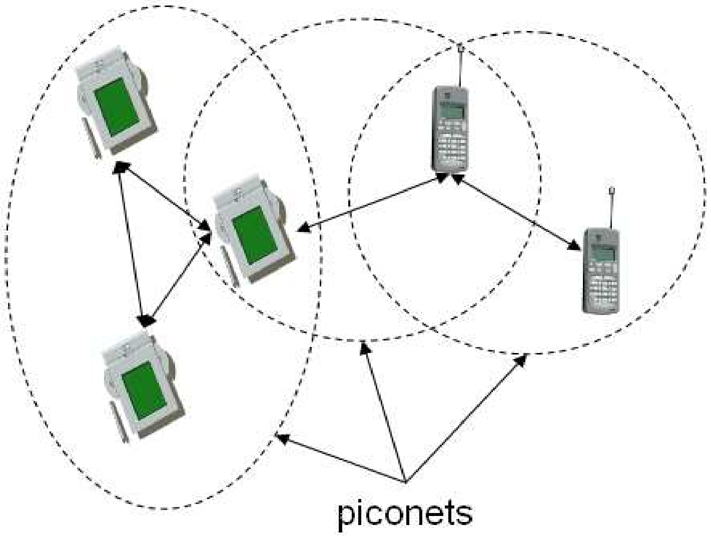
States of a Bluetooth Device

- Sniff mode allows a slave to listen to polling packets from the master at a slower rate (to reduce the power)
- In Hold mode, the slave and master agree on the duration of time that the slave can be suspended.
- Sniff mode uses a fixed time period while in Hold mode (the time period is dynamically agreed).
- In parked mode, a slave disassociates itself from the Piconet (to save power)
- A maximum of 255 slaves can be in parked mode



Bluetooth Scatternets

- **Piconet:** has one master and up to active 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
- **Scatternet:** consists of 2 or more masters and several slaves
- Up to 10 piconets can coexist in same area



Project co-financed from the EU European Social Fund

Bluetooth Problems

- Complicated Protocol
- Device discovery takes time.
  - Inquiry operation approx. 10/20 seconds
  - Page operation approx. up to 3 seconds
- Limitation of 7 active slaves in a piconet.
  No support for scatternets in the specification

WLAN

(Wireless LOCAL Area Networks)

Temptative Applications:

- Free / low cost mobile Internet access
- Networks in exhibition halls
- Spontaneous cooperation at meetings
- Information in airports / restaurants / hospitals
- Structure of networks in historic buildings
- Warehouses
- Extension of existing wired local area networks in offices, universities, etc.

IEEE 802.11 Standard

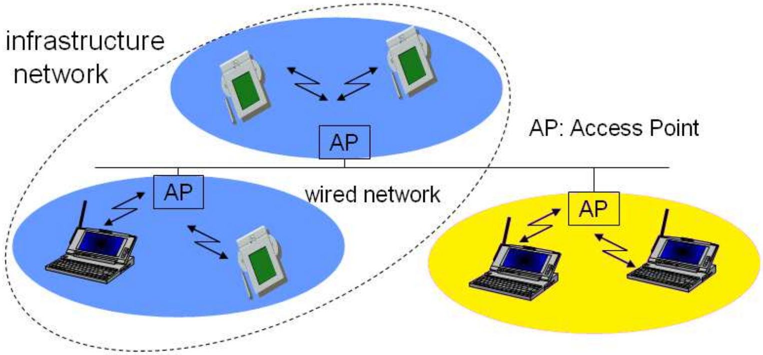
- Wi-Fi → „Wireless Fidelity”
- IEEE 802.11 → the most widely used WLAN technology
- Wireless LAN standard developed (ratified in 1997) by the IEEE (Institute of Electrical and Electronics Engineers)
- Since 1999 standardization by non-profit organisation „Wi-Fi Alliance” (consisted of more than 300 companies from around the world)
- "Wi-Fi" designates a globally operative set of standards → unlike mobile phones, any standard Wi-Fi device will work anywhere in the world.
- Designed for Local Area Networks:
  - Approx. 100m range indoors
  - Approx. 300m range outdoors (no obstacles)

802.11 Frequency Bands

- **2,4 GHz Band**
  - 2,4 to 2,4835 GHz
  - ISM-Band
  - public domain
  - 14 overlapping channels
  - 3 channels without overlapping
  - transmitted power max. 100 mW

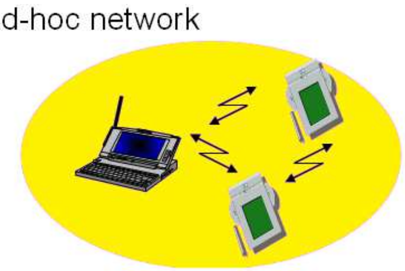
- **5 GHz Band**
  - 5,15 - 5,725 GHz in Europe
  - public domain
  - 19 channels without overlapping
  - transmitted power max. 1000 mW with TPC and DFS (Transmission Power Control) (Dynamic Frequency Selection)

802.11 Network Topologies



Infrastructure mode:

- like a star-network
- Access-Point (AP) is a central point
- AP coordinates the network nodes and communicates with other networks



Ad-hoc Mode:

- Like Peer-to-Peer Network
- All network nodes are equal
- No central Station or higher-level infrastructure available

802.11 Data Security

1. **WEP** (Wired Equivalent Privacy)
   - symmetrical cryptography, e.g. using RC4
   - but small key lengths → low security!
2. **WPA / WPA2** (WiFi Protected Access)

   subset of 802.11i, resolves the WEP problems

   - Authentication:
     - Pre-Shared-Key (PSK), 8-64 characters password, used for generation of the session key
     - Extensible Authentication Protocol based on 802.1x
       (e.g. RADIUS-Server – Remote Access Dial-in User Service)
   - Encryption:
     - Integrity Check, e.g. “Michael”
     - TKIP generates dynamic key per packet (WPA)
     - RC4 (WPA) or AES (WPA2) for encryption
   - Remaining security problems → simple PSK allows “brute force” or dictionary attack

802.11 Security – Summary

Features	WEP	WPA	WPA2/ IEEE802.11i
Encryption	RC4	RC4	AES
Key length [Bit]	40, 104	128 or more	128 or more
Data integrity	CRC-32	Michael	CCM
Header integrity	non	Michael	CCM
Key management	non	EAP-based	EAP-based

RC4 – R.Rivest Encryption symmetrical method (1987)

AES – Advanced Encryption Standard (Rijndael, 2000),
a symmetrical cryptosystem, modern DES, RC4 successor

CCM – Counter Mode with Cipher Block Chaining
Message Authentication Code Protocol

EAP – Extensible Authentication Protocol,
used on data link layer, frequently with PPP and SSL/TLS

4G Networks

(integration of advanced celular and WLAN)

Features of 4G:

- high mobility → Handover, Roaming, velocity up to 300 km/h
- switching technique → pure packet switching
- integrated multi-media-services → VoIP, TVoIP, VoD, Streaming
- high data rate → even at high mobility should be like DSL
- Size of cell → variable and scalable
- QoS → prioritization of specific data packages
- scalability → available and reliable with many users
- air interface → OFDM (better spectrum efficiency)
- security → up to date standards (AES)
- Extension / integration of:
  - UMTS: better mobility and coverage
  - WLAN: higher data rates, cheaper

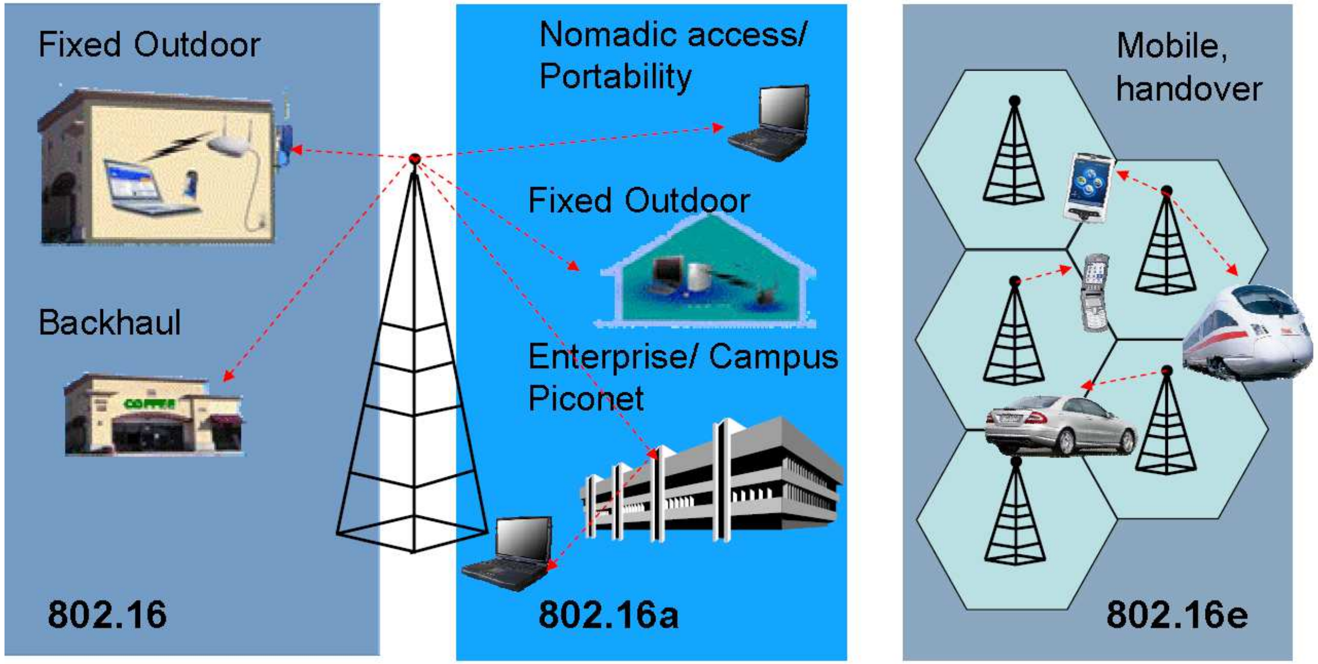
WiMAX / IEEE 802.16

(Fixed Broadband Wireless Access)

- WiMAX: Worldwide Interoperability for Microwave Access, standardized by IEEE 802.16 and WiMAX-Forum (more than 230 members, including AOL, Deutsche Telekom, Intel, Microsoft, Nokia)
- IEEE **802.16** FBWA (Fixed Broadband Wireless Access) an alternative for broadband cable services like DSL; frequency range: 10-66 GHz, in assumption of LOS (line of sight)
- Enhancement IEEE **802.16a**; frequency band: 2-11 GHz, NLOS (non line of sight)
- Enhancement IEEE **802.16e** for MBWA (Mobile Broadband Wireless Access); frequency band: 2-6 GHz, NLOS

Standard	802.16	802.16a	802.16e (rival to 802.20)
Spectrum, GHz	10-66	2-11	2-6
LOS-condition	LOS	NLOS	NLOS
Bit rate, MBit/s	32-134	<75	15
Range, km	2-5	7-10 max. 50 (cellular)	2-5
Channel bandwith, MHz	20, 25 and 28	Variable: 1,5–20	1,5 -20
Modulation	QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM
approved	2001	2004	2006

WiMAX usage scenarios



MBWA - IEEE802.20

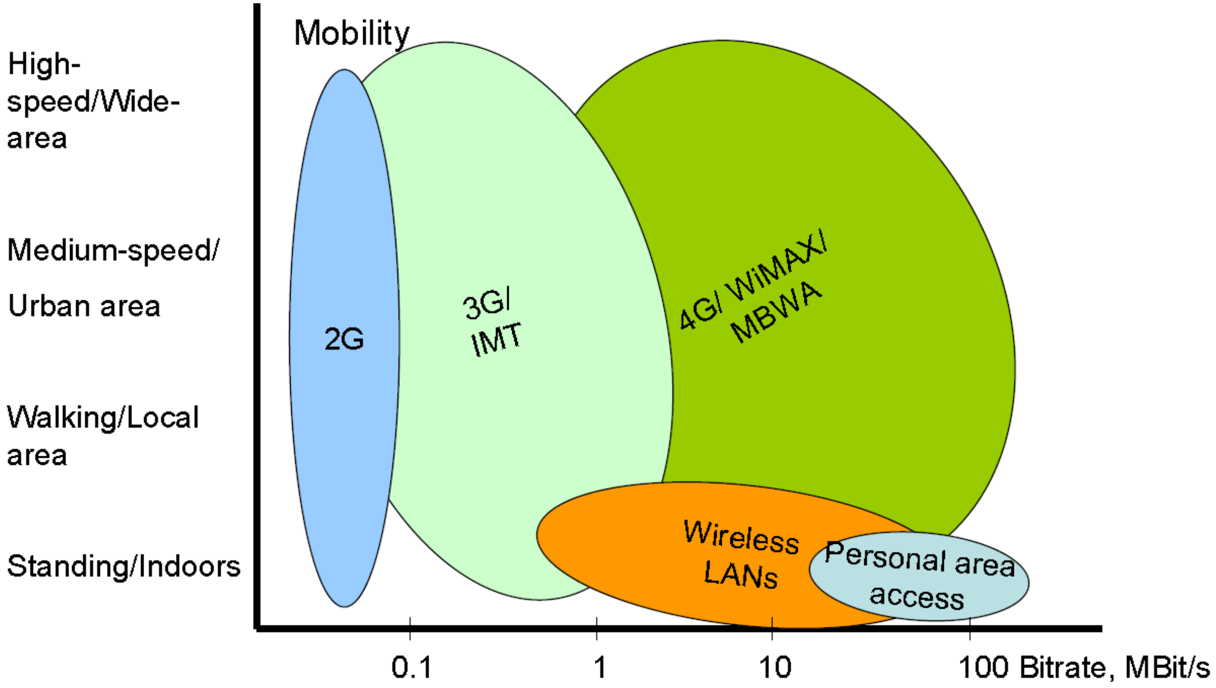
(Mobile Broadband Wireless Access)

- variable cell size
- Handover- and Roaming-mechanism
- Velocity up to 300 km/h
- Transport of IP-data traffic
- QoS on transport layer
- Licensed bands below 3,5 GHz, variable bandwidth
- NLOS, for in- and outdoor
- TDD, FDD, Half-Duplex FDD
- More than 100 simultaneous sessions per cell
- End to End Security, AES

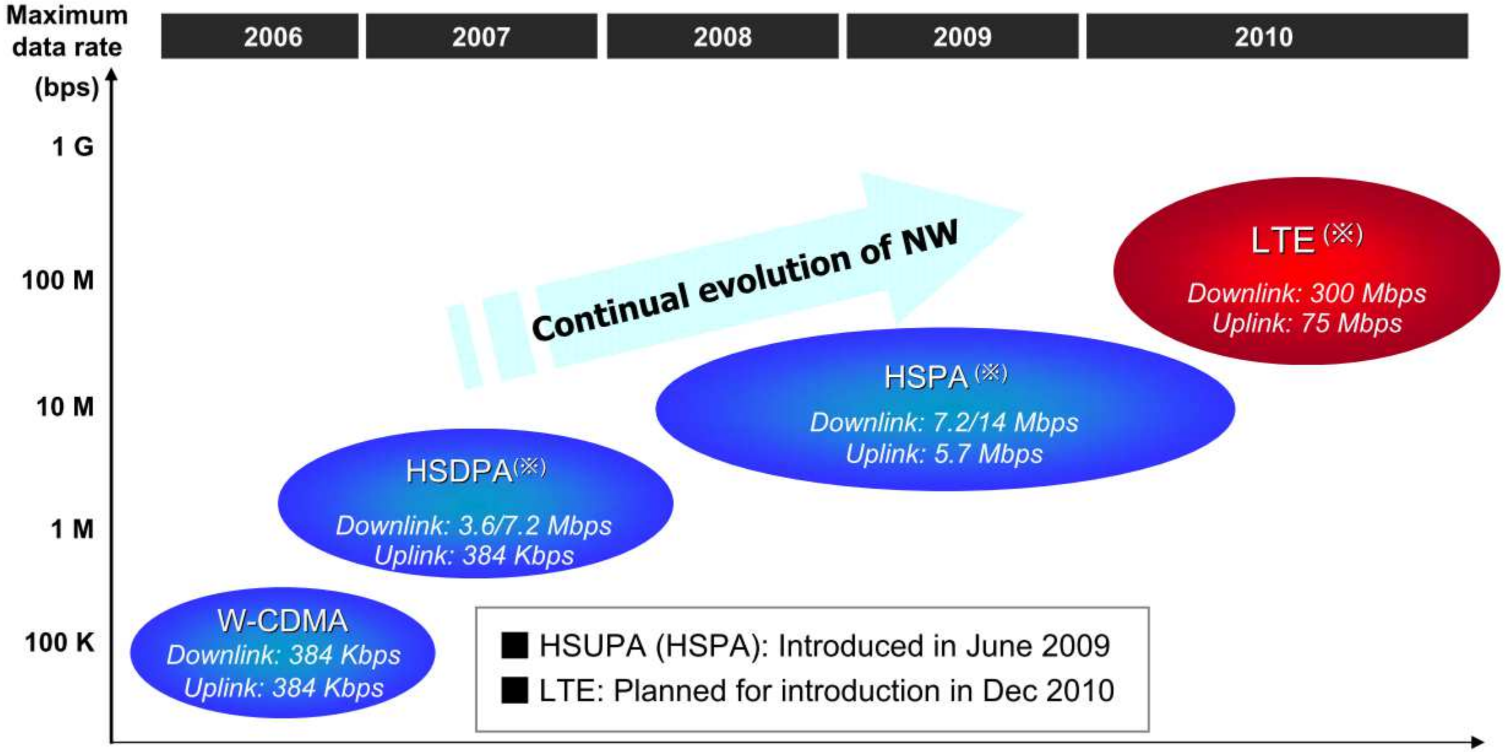
Comparison of technologies

802.11	802.16	802.16e	802.20
WLAN	WMAN	mobile WMAN	mobile WMAN
Range max. 300 m	Up to 50 km, typically 4-9 km	Up to 5 km	Several km
Less users per cell	Multiple users per cell (> 100)	Multiple users per cell (> 100)	Multiple users per cell (> 100)
max. data rate 54 Mbit/s or 100 MBit/s	Up to 134 MBit/s (dependent on bandwidth and PHY)	60 MBit/s (20 MHz channel)	72 MBit/s (20 MHz channel)
QoS only via 802.16e	QoS integrated in MAC-layer	QoS integrated in MAC-layer	QoS available
License-free bands	License-free and licensed bands	licensed bands	licensed bands
Fixed bandwidth of 20 MHz	variable bandwidth 1,25-28 MHz	variable bandwidth 1,25-20 MHz	variable bandwidth
2,4 and 5 GHz Band	10-66 and 2-11 GHz	2-6 GHz	under 3,5 GHz
limited mobility	limited mobility	good mobility	very good mobility
transmission power Up to 100 mW in the 2,4GHz-Band Up to 1 W in the 5GHz-Band	transmission power for BS max. 30 W Client (SS) max. 3 W	transmission power for BS max. 30 W Client (SS) max. 3 W	No specifications

Sumary: data rate and mobility



Emerging Technology: LTE



W-CDMA
Downlink: 384 Kbps
Uplink: 384 Kbps

HSDPA(※)

Downlink: 3.6/7.2 Mbps
Uplink: 384 Kbps

HSPA (※)

Downlink: 7.2/14 Mbps
Uplink: 5.7 Mbps

LTE (※)

Downlink: 300 Mbps
Uplink: 75 Mbps

■ HSUPA (HSPA): Introduced in June 2009
■ LTE: Planned for introduction in Dec 2010

※HSPA: High Speed Packet Access HSDPA: High Speed Downlink Packet Access LTE: Long Term Evolution

LTE

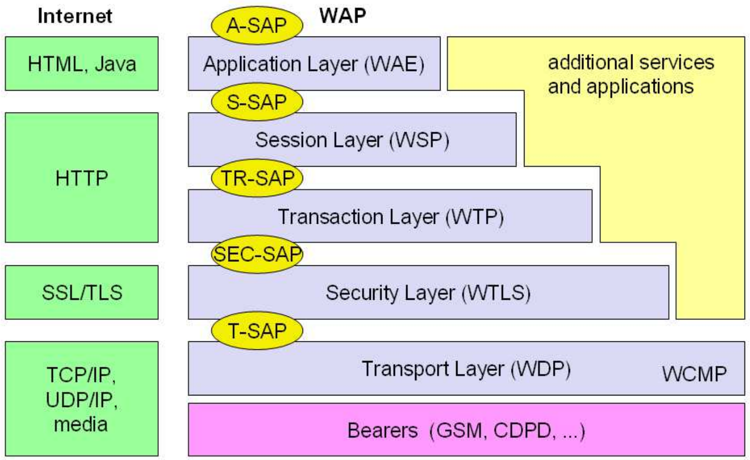
(Long Term Evolution)

- Broad standard for 4G encompassing technology standards
- More than 100MBits/sec downloads, 50Mbps uploads
- 1000MBits/sec download in hot spots
- Will be 3-5 times more powerful than anything today
- Handling up to 200 simultaneous users per 5MHz slice of spectrum
- 2008 - the first set of LTE trials completed.
- LSTI, the European LTE testing group, will continue trials through 2009 with deployments beginning in 2010.
- Expected LTE announcements by Vodafone, Verizon, Mobile China.

WAP

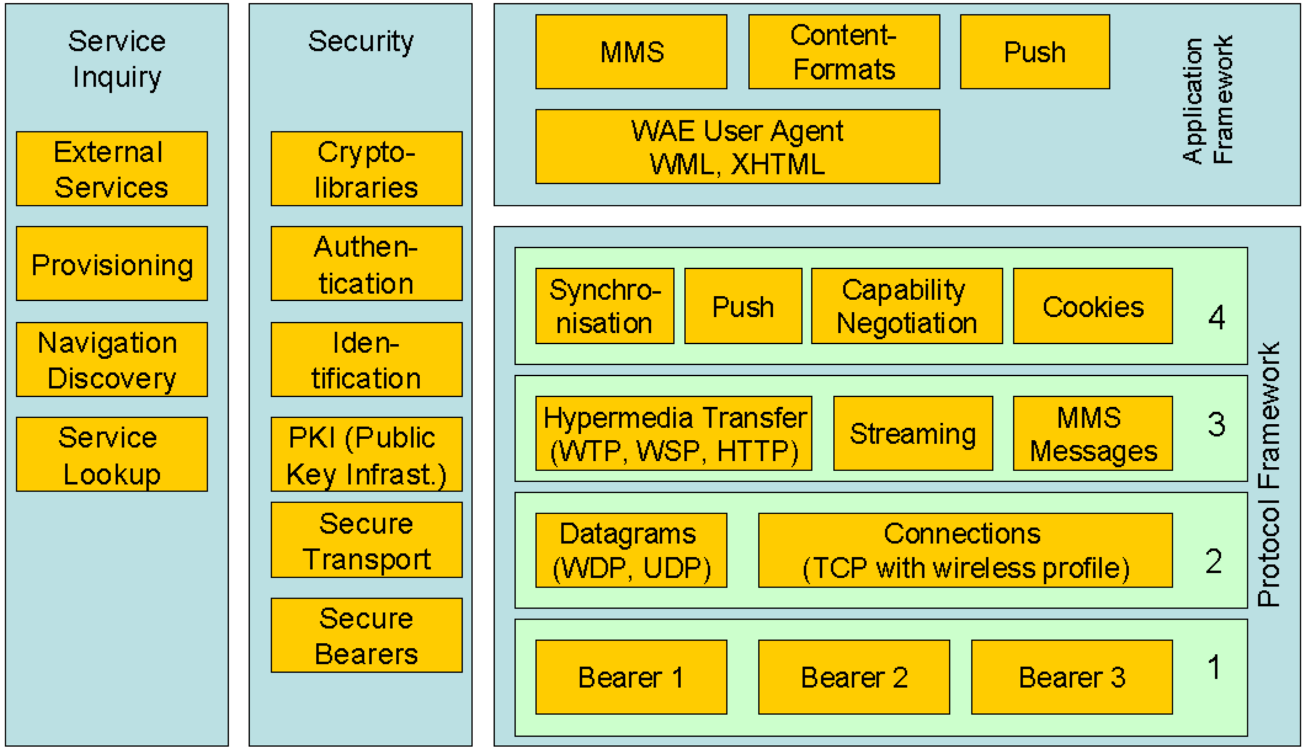
(Wireless Application Protocol)

- Standardized by Open Mobile Alliance (formerly WAP Forum, co-founded by Ericsson, Motorola, Nokia, Unwired Planet)
- Wireless Application Environment (WAE)
  - WML (Wireless Markup Language) micro-browser
  - WMLScript virtual machine and standard library
  - Wireless Telephony Application (WTA)
  - WAP Content Types
- WAP Protocol layer architecture
  - Wireless Session Protocol (WSP)
  - Wireless Transaction Protocol (WTP)
  - Wireless Datagram Protocol (WDP)
  - Interface definitions for mobile networks (e.g. UMTS, GPRS)



WAE comprises WML (Wireless Markup Language), WML Script, WTAI etc.

WAP 2.x Extended Architecture



Service Inquiry

- External Services
- Provisioning
- Navigation Discovery
- Service Lookup

Security

- Crypto-libraries
- Authentication
- Identification
- PKI (Public Key Infrast.)
- Secure Transport
- Secure Bearers

Application Framework

- MMS
- Content-Formats
- Push
- WAE User Agent WML, XHTML

Protocol Framework

4: Synchronisation, Push, Capability Negotiation, Cookies

3: Hypermedia Transfer (WTP, WSP, HTTP), Streaming, MMS Messages

2: Datagrams (WDP, UDP), Connections (TCP with wireless profile)

1: Bearer 1, Bearer 2, Bearer 3

WML

(Wireless Markup Language)

- HTML-like markup language, based on XML
  - different font styles are available,
  - tables and color graphics,
  - variables and longer-term sessions
- Deck/Card-metaphor
  - selection possibilities are separated in Cards
  - navigation takes place between Cards (hyperlinks, history, user events)
  - deck-stack corresponds to a WML-file and is a unit of download
- Alternative: Direct use of XHTML
  with adaptation to display-specific layout

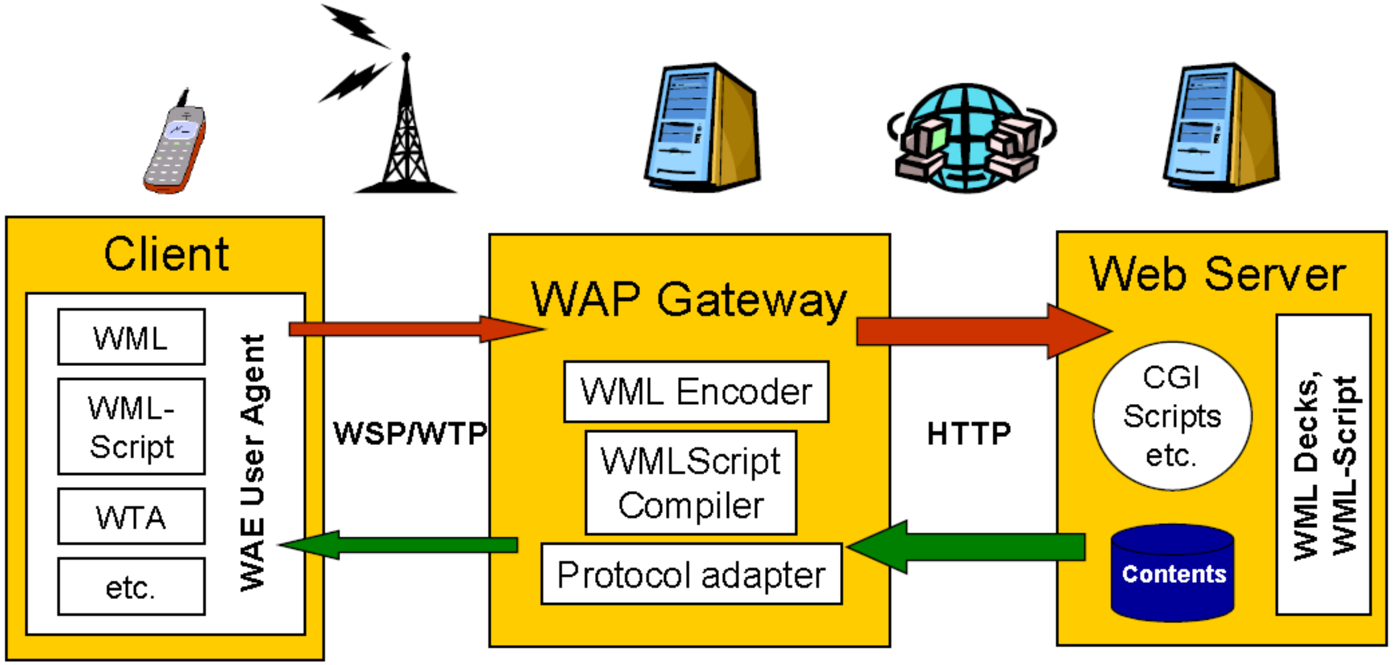
WML– text styles – example

```
<wml>
        <card id=“Card1” title=“Text Styles”>
                <p align="left">
                        <i>italic</i>,
                        <b>bold</b>,<br>
                        <big>big</big>,
                        <small>small</small>,
                        <u>underlined</u>
                </p>
        </card>
</wml>
```

WMLScript

- Scripting language, similar to JavaScript
  - procedures, loops, conditions, ...
  - optimized for devices with lower storage capacity and performance
- Integrated with WML, enables:
  - reduction of network workload; local validation of inputs
  - access to vendor-specific APIs
  - programming of conditional logic
- Bytecode-based language and virtual machine
  - Compiled language - better utilization of network capacity and device storage
  - designed with regard to simple implementation, e.g. on ROM
  - Standard library for processing of strings, URLs, ...

Web Integration - WAP Gateway


Client
WML
WML-Script
WTA
etc.
WAE User Agent
WSP/WTP
WAP Gateway
WML Encoder
WMLScript Compiler
Protocol adapter
HTTP
Web Server
CGI Scripts etc.
Contents
WML Decks, WML-Script