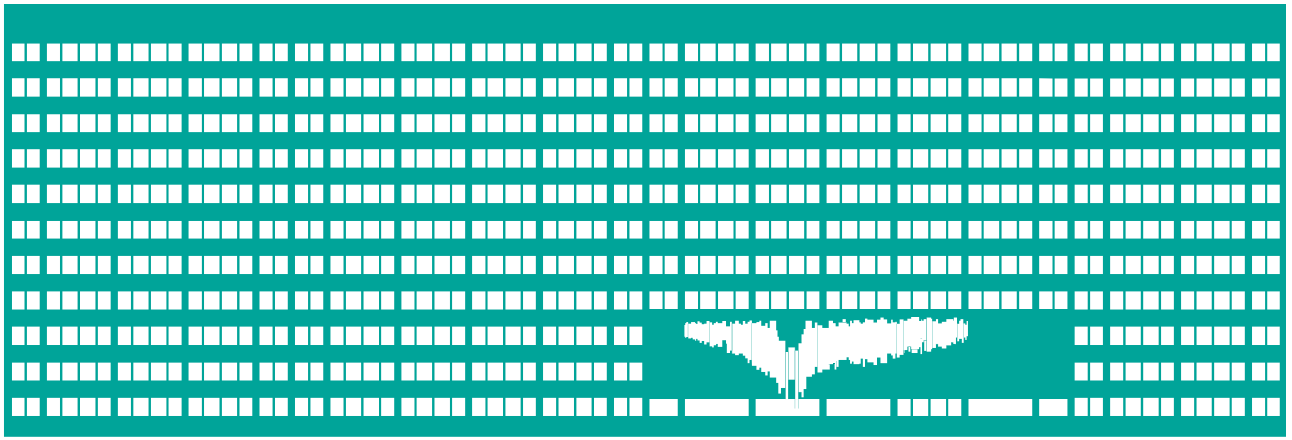
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Overview of RF Wireless Network Technologies



MS (Mobile Computing)
Lecture 9

Wireless systems

- Radio frequency systems
  - Radio waves
    - Usually amplitude or frequency modulation
  - Microwaves
    - Easily passes through the earth or walls.
    - Less Interference, more bandwidth
- Infrared
  - IR remotes, PtP links, …
  - Require direct visibility, line-of-sight

Cellular networks

Radio networks consisting of a number of radio cells.

- Advantages:
  - increased capacity
  - reduced power usage
  - better coverage
- Types:
  - FDMA (+TDMA)
  - CDMA

Cellular network generations (1)

- 0G – Private mobile networks, Push-to-talk
- 1G – Analog signal, f > 150 MHz, listen-to-handset. Usually no encryption, noise in signal, interference.
- 2G – Digital signal, increased capacity, decreased output power, error detection & correction, higher capacity, encrypted, IMEI+IMSI identification → no handset cloning. Dropouts. Can be used for data transfers
  - Dial-up (CSD → HSCSD → 2.5G)
  - Signaling channel – SMS
  - Packet data
    - GPRS & MMS→ 2.5G, up to 115 kbit/s
    - EGPRS/EDGE → 2.75G, up to 236.8 kbit/s (4 timeslots)

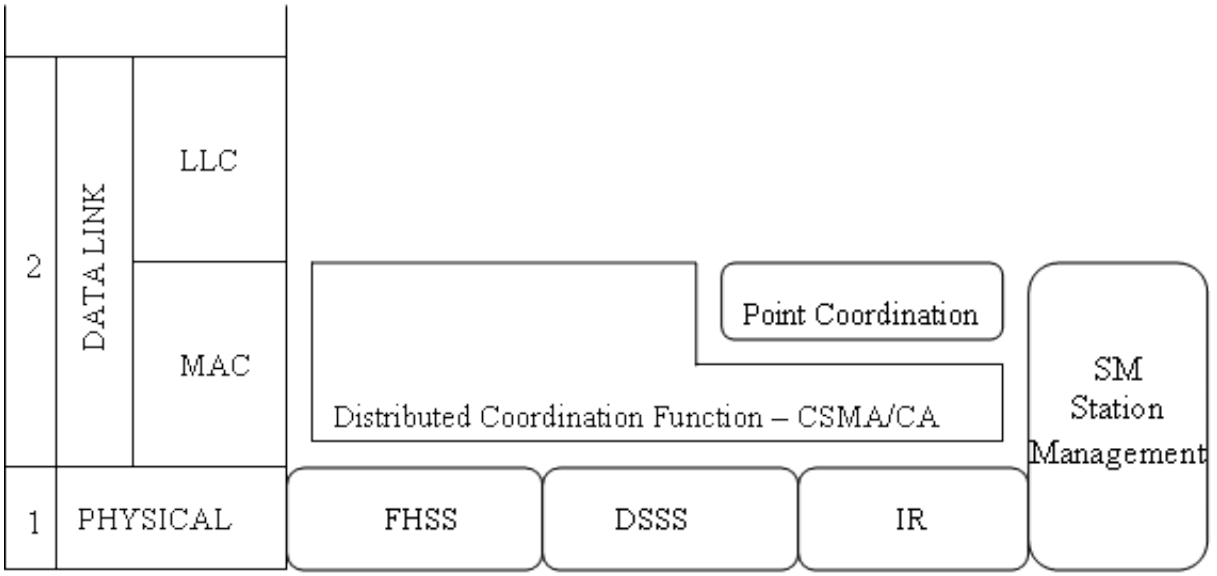
Cellular network generations (2)

- 3G – simultaneous voice & data transfer. Peak data rates of at least 200 kbit/s. Universal Mobile Telecommunicat. System (UMTS) & Wideband CDMA in Europe.
  - High Speed Packet Access (HSPA) – 3.5G
    - downlink (HSDPA) – up to 7.2 Mbit/s, uplink (HSUPA) – up to 5.76 Mbit/s
  - Evolved HSPA (HSPA+) – 3.75G
    - up to 56 Mbit/s downlink & 22 Mbit/s uplink
  - 3.9G – other, getting close to bandwidth requirements for 4G. MIMO technology.
    - 3GPP Long-term Evolution (LTE) - peak rates of at least 100 Mbit/s downlink & 50 Mbit/s uplink, currently
  - Mobile WiMAX
- 4G (at least 1Gbit/s stationary & 100 Mbit/s mobile)

Current IEEE 802 Networks

- 802.11 – Wireless Local Area Networks (WLAN)
  - 802.11 a/b/g/n – WiFi networks
  - 802.11s – Mesh networks with WiFi certification
- 802.15 – Wireless Personal Area Networks (WPAN)
  - 802.15.1 – Bluetooth
  - 802.15.2 – 802.11 & 802.15 networks coexistence
  - 802.15.4 – Low Rate WPAN → ZigBee (-2003, -2006)
- 802.16 – Broadband Wireless Access
  - 802.16m - WiMAX

IEEE 802.11 Recommendation Structure



- FHSS – Frequency Hopping Spread Spectrum (802.11)
- DSSS – Direct-sequence spread spectrum (802.11, 11b)
- OFDM – Orthogonal frequency-division multiplexing (802.11g, 802.11n)

Selected IEEE 802.11 Recommendations – Protocols

- 802.11-1997 (the original standard) - 1 & 2 Mbps
  - Current revision – 802.11-2016 – includes 802.11 a, b, d, e, g, h, I, j, k, n, p, r, s, u, v, w, y & z (-2016) aa-af. We will use original "well known" letters in following slides.
- 802.11a (802.11-2016 clause 17) - 5 GHz (USA)
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 802.11b (802.11-2016 clause 16) - 2.4 GHz (USA, Europe, Japan)
  - Extends 802.11 by DSSS 1, 2, 5.5 and 11 Mbps
- 802.11g (802.11-2016 clause 18) - 2.4 GHz (USA, EU)
  - Speeds like 802.11a (but at 2.4 GHz band)
- 802.11n (802.11-2016 clause 19) – 2.4 & 5 GHz
  - MIMO, wider bandwidth (20/40 MHz), speeds up to 144.4 Mbit/s for 20 MHz & 300 Mbit/s for 40 MHz.

Selected IEEE 802.11-2012 Recommendations (original letters)

- ~~802.11f – fast roaming between APs~~, withdrawn 2006
  - Avoids the need of reoccurring authentication during handover between APs, useful for latency-critical mobile application (IP telephony, multimedia transfers, …). Superseded by:
    - 802.11k – Radio Resource Management – best available AP
    - 802.11r – Fast Roaming - fast & secure handoffs
- 802.11u – standard for devices such as laptop computers or cellular phones to join a wireless LAN
- 802.11p – Wireless Access in Vehicular Environments (WAVE), enhancements to 802.11 required to support Intelligent Transportation Systems (ITS) applications.

Selected IEEE 802.11-2012 Recommendations (original letters)

- 802.11h - 5 GHz (Europe) - Power management, solving radar & satellite interference
  - Dynamic Frequency Selection (DFS)
  - Transmit Power Control (TPC)
- 802.11i – security + QoS
  - 802.11e defines QoS frame & headers
- 802.11s – mesh networking, defining how wireless devices can interconnect to create a WLAN mesh network, which may be used for static topologies and ad-hoc networks

New 802.11 Recommendations

- 802.11ac (802.11-2016 clause 22) – 5 GHz
  - Multi-station WLAN throughput >= 1 Gb/s, single station 500 Mb/s, 80/160 MHz range, up to 8 streams, up to QAM-256.
- 802.11ad (802.11-2016 clause 21) – 60 GHz, WiGig
  - theoretical maximum throughput up to 7 Gbit/s.
  - will be used in a new wireless USB specification.

WiFi networks

„Wireless Fidelity“

- Components of network:
  - Access Point
  - Wireless clients (stations)
  - Distribution System
  - Wireless medium (frequency band)
- Usage Alternatives:
  - Ad-hoc – manual, peer-to-peer, 2 or more nearby nodes
  - Infrastructure – access point provides access to permanent infrastructure, usually bridge to wired network
    - May provide other functions (NAT, DHCP, other PnP, …)

WiFi network architectures

- Independent Service Set (IBSS)
  - A group of directly communicating stations
  - No frame relaying
  - Not interconnected with a wired network
- Basic Service Set (BSS)
  - Utilizes access point, stations communicate using AP
- Extended Service Set (ESS)
  - Interconnects multiple BSS using distribution system, which is out of scope of the IEEE 802.11 standard
  - Ethernet × various solutions of Wireless Distribution Systems (WDS)

WiFi remarks

- Terminology
  - Service Set = logical group of stations
  - BSS = Basic Service Set
  - SSID = Service Set Identifier
  - BSSID = BSS Identifier = AP MAC address
    - Classic 48-bit MAC addresses apply.
  - ESSID = Enhanced Service Set Identifier
- 802.11 can be used over infrared as well

Wireless Media Access Methods

- Distributed Coordination Function (DCF)
  - CSMA/CA – collision avoidance, res. timeslot for ACK
- Point Coordination Function (PCF)
  - for real-time applications (QoS may be implemented)
  - AP assigns the bandwidth to individual stations (polling)
  - Commonly combined together with DCF
    - Contention-Free Period and Contention Period (superframe)
  - Not implemented and utilized very often today
- IEEE 802.11e (802.11i)
  - 8 priorities, IFS (inter-frame spacing) has to be proportional to the priority value. Admission control (distributed/centralized). Timeslot reservation.

WiFi security

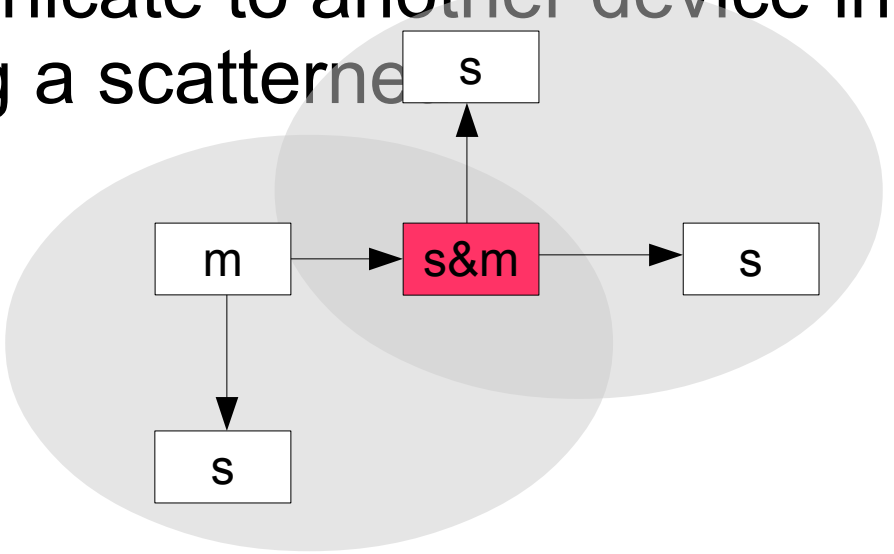
- Authentication
  - One-way
    - Station authenticates to the AP
  - Open and Shared Key Mode
    - Open = no authentication
    - Shared Key = authentication using the shared WEP key
      - challenge-response protocol
  - Authentication frame - used for both request and response
- Encryption
  - WEP – Wired-Equivalent Privacy - shared key (64/128B), used for encryption and authentication. Cracked ~ min
  - WPA, WPA2 (AES) – WiFi Protected Access
  - 802.1x mechanisms – EAP, PEAP, EAP-TLS, …

Bluetooth

- Called after Harald I, originally envisioned by Erikson in 1994 with 10m distance limitation
- Bluetooth SIG of majority Telco companies (since 1998)
- Uses FHSS, 79 frequency bands (1 MHz) at 2.4 GHz
  - Originally Gaussian frequency-shift keying (GFSK) – 1 Mbps in Bluetooth 1.x – basic rate (BR)
  - Differential QPSK & 8PSK (D-QPSK, D-8PSK) in 2.x – 2 Mbps & 3 Mbps – enhanced data rate (EDR), coexists
- Packet-based, master-slave architecture, master generates clock signal.

Bluetooth network topology

- Bluetooth-enabled devices are organized in groups called piconets: master and up to seven active slaves.
  - Master + single slave use point-to-point communication
  - multiple slaves → point-to-multipoint communication.
  - Master unit initiates the communication. A device in one piconet can communicate to another device in another piconet, forming a scatternet



Bluetooth classification

- Low power consumption, short range, low-cost chips
- Classes (higher-class devices support lower classes):
  - Class 1 – up to ~ 100m, 100 mW
  - *Class 2* – up to ~ 10m, 2.5 mW
  - Class 3 – up to ~ 1m, 1 mW
- Bluetooth main versions:
  - 1.2 – 1 Mbps, Basic rate
  - 2.0 & 2.1 - optional 2/3 Mbps EDR + small improvements, secure simple pairing in 2.1
  - 3.0 + HS – BT link used for establishment of co-located 802.11 link with speeds up to ~24 Mbps. AMP
  - 4.0 – adds Bluetooth low energy to 3.0

Bluetooth protocol stack

- Mandatory protocols:
  - ***LMP*** (*Link Management Protocol*) – control of radio link between two devices. Implemented on controller.
  - ***L2CAP*** (*Logical Link Control & Adaptation Protocol*) – packet service multiplexing multiple connections of higher-level protocols, segmentation, 48 B → 64 kB per packet, default MTU 672 B. Additional Streaming & Enhanced ReTransmission Modes
  - ***SDP*** (*Service Discovery Protocol*) – services & their parameters – detection of supported profiles
- *HCI* (*Host/Controller Interface*) – communication with host stack (e.g. USB, UART). Optional for single-chip solutions.
- *RFCOMM* (*Serial Port Emulation*) – virtual serial stream

Other Bluetooth protocols

All of following profiles are optional:

- BNEP (Bluetooth Network Encapsulation Protocol) - transferring another protocol stack's data via L2CAP channel. Main purpose is the transmission of IP packets in the Personal Area Networking Profile.
- AVCTP (Audio/Video Control Transport Protocol) - used by the remote control profile to transfer AV/C commands over an L2CAP channel, e.g. music control buttons on a stereo headset use it to control the player.
- AVDTP (Audio/Video Distribution Transport Protocol) - used by advanced audio distribution profile (A2DP) to stream music to stereo headsets over an L2CAP channel. In future should be used by video distribution profile.
- PPP, IP stack, OBEX, Wireless Application Protocol

Bluetooth parameters

- Baseband Error Correction – 1/3 & 2/3 FEC, automatic repeat-request
- Modes:
  - Globally discoverable – answers name-based inquiries at any time (provides device name, class, list of services & technical information). Limited discoverability – only limited time interval for answering inquiries
  - In invisible mode, clients can still connect known 48-bit MAC address
- Pairing – (user) request to bind two devices together, shared secret selection – fixed, numeric, alphanumeric
  - Secure Simple Pairing since 2.1 – even without user interaction.

Bluetooth profiles

- Bluetooth profiles are intended to ensure interoperability among different devices and applications. A profile defines the roles and capabilities for specific types of applications.
  - Generic Access Profile - connection procedures, device discovery, and link management. At a minimum all Bluetooth devices must support this profile.
  - Service Discovery Application and Profile – features and procedures for an application to discover services registered in other devices.
  - Serial Port Profile - requirements for Bluetooth devices that need to set up connections emulating serial cables.
  - …

Offering Bluetooth services

- The steps involved in registering a service are defined in the Service Discovery Protocol (SDP), which is part of the Bluetooth Specification, and are as follows:
  - create a service record,
  - add the service record to the Service Discovery Database,
  - set security measures associated with connections to clients,
  - accept connections from clients
- Each Bluetooth service offered by a host is represented by a Service Record in the Service Discovery Database (SDDB). To connect to a service a client obtains a Service Record from the server and uses the information therein to connect to the service.

IEEE 802.15.4

- Low-rate wireless personal area networks (LR-WPANs)
  - basis for the ZigBee, WirelessHART, and MiWi
  - low-speed ubiquitous communication between devices
  - very low-cost communication of nearby devices with little to no underlying infrastructure, low power consumption
- Transfer rates (typically DSSS is used)
  - basic framework - 10-meter communications range with a transfer rate of 250 kbit/s
  - 20 & 40 kbit/s originally, 100 kbit/s in current standard
- Timeslot reservation for real-time comm, CSMA/CA
- Bands: 868.0-868.6 MHz (1 CH, EU), 902-928 MHz (10 CH, US), 2.4 GHz (up to 14 CH, worldwide)
- 6LoWPAN – low power mesh network using IPv6 for node addresses

IEEE 802.15.4 – parameters

- Network model (64 or 16 bit unique device IDs)
  - *Full function device* (FFD) – may work as area coordinator, message relaying × *reduced function device* (RFD) – very simple, low resource devices, can communicate with FFDs only.
  - At least one FFD as a coordinator, topology:
    - peer-to-peer – only limited by the distance between each pair of nodes, meant to serve as the basis for ad-hoc networks
    - star – FFD is the hub of this star topology
- Data transport architecture
  - Data, ACK, beacon & control (MAC command) frames
  - Superframe with 16 equal-length timeslots, contention inside superframe

ZigBee

- Specification for a suite of high level communication protocols using low-power, small digital radios for monitoring & control
- Expected to be main building block of ubiquitous networks. Currently: wireless light switches, electrical meters + in-home-displays, consumer electronics via short-range radio.
- Maintained by the ZigBee Alliance – specifications, certification. Publishes application profiles for OEMs
- Devices must activate from sleep in 15 ms – low latency
- Ad-hoc on-demand routing protocol (AODV)

ZigBee basics

- Specifications
  - ZigBee Home Automation, ZigBee Smart Energy, ZigBee Telecommunication Services, ZigBee Health Care, ZigBee Remote Control
  - ZigBee Building Automation, ZigBee Retail Services, …
- Device types
  - ZigBee coordinator (ZC) – FFD, exactly one ZigBee coordinator in each network – the device that started the network originally, can store security keys
  - ZigBee Router (ZR) – besides running an application, it can pass on data between other devices.
  - ZigBee End Device (ZED) – RFD, sleeps most of the time, less expensive to manufacture than a ZR or ZC.

ZigBee non-IEEE functions

- Application may consist of communicating objects which cooperate to carry out the desired tasks
- Work may be distributed among different devices
- Within a single device, up to 240 application objects can exist (+broadcast +special object for ZDO)
- Two services available for application objects to use:
  - key-value pair service (KVP) – for configuration purposes, compressed XML
  - message service – designed to offer a general approach to information treatment
- Security – basic security relies on initial installation of the keys, 128-bit keys for security mechanism in SA

ZigBee application areas

- Home Entertainment and Control – smart lighting, advanced temperature control, safety and security, movies and music
- Home Awareness – water sensors, power sensors, energy monitoring, smoke and fire detectors, smart appliances and access sensors
- Mobile Services – m-payment, m-monitoring and control, m-security & access control, m-healthcare & tele-assist
- Commercial Building – energy monitoring, HVAC, lighting, access control
- Industrial – process control, asset management, environmental management, energy management, industrial device control, machine-to-machine (M2M) communication

Low-Power Wide-Area Networks

- ISM bands are often utilized to reduce costs
  - Limited time for node to transmit (single node 1% at 868MHz)
- Many different (often patented) technologies
  - Sigfox – global coverage, node → base station mainly, annual fees, (ultra-)narrowband technology, BPSK, 12 bytes per message, up to 140 messages per day, infrastructure owned by Sigfox, range up to 30-50 km rural, 3-10 km urban areas
  - LoRa/LoRaWAN – patented by Semtech, currently developed by LoRa alliance, bi-directional, MSK radios communication, node and base station may use same HW, spread-spectrum (~125 kHz), frequency hopping, 300 b/s – 38.4 (100) kb/s, max. packet length 256 bytes
  - NarrowBand IoT (NB-IOT) – 3GPP initiative for LPWANS in cellular networks
  - LTE Advanced for Machine Type Communications (LTE-MTC) – 3GPP LTE evolution for connected things
  - Weightless – 1kb/s – 10 Mb/s, EnOcean (energy harwesting), Ultra Narrow Band (UNB) – 250 kb/s-10MB/s,

IEEE 802.16 WiMAX (obsoleted)

- Worldwide Interoperability for Microwave Access (WiMAX) – common name associated to the IEEE 802.16a/REVd/e standards.
- Standards are issued by the IEEE 802.16 subgroup that originally covered the Wireless Local Loop technologies with radio spectrum from 10 to 66 GHz.
- IEEE 802.16 (2001) – Air Interface for Fixed Broadband Wireless Access System MAC & PHY specs 10-66 GHz
  - One PHY: Single Carrier
  - Connection-oriented, TDM/TDMA MAC, QoS, Privacy

IEEE 802.16 WiMAX standards

- IEEE 802.16a (2003)
  - Amendment to 802.16, MAC Modifications and Additional PHY Specifications for 2 – 11 GHz (NLoS)
  - Three PHYs: OFDM, OFDMA, Single Carrier
  - Additional MAC functions: OFDM and OFDMA PHY support, Mesh topology support, ARQ
- IEEE 802.16d (2004) – combines 802.16 & 802.16a
- IEEE 802.16e (2005)
  - MAC Modifications for limited mobility
  - Scaling of the Fast Fourier transform (FFT) to channel bandwidth, Adaptive Antenna Systems + MIMO, QoS for VOIP, Turbo codes, Antenna diversity schemes, hybrid ARQ, …

WiMAX parameters

- Range up to 50 km, speeds up to 70Mbps (shared). Mobile speeds up to ~37 Mbps (maximal vehicle speed for working WiMAX – 150 km/h).
- Frequency bands:
  - licensed: 2.3 GHz, 2.5 GHz & 3.5 GHz (2/3 of licensed users worldwide, 20 channels) × unlicensed: 2.4 GHz, 5.4 GHz, 5.8 Ghz
- Bandwidth: 3.5/7/14/20 MHz
- OFDM: 256/512/1024 carriers
- FEC: 1/2, 2/3, 3/4
- Modulation – based on C/N ratio: BPSK, QPSK, 8PSK, QAM-16, QAM-64

WiMAX uses

The bandwidth and range of WiMAX make it suitable for the following potential applications:

- Portable mobile broadband connectivity across cities and countries through a variety of devices.
- Wireless alternative to cable and DSL "last mile" broadband access.
- Data, telecommunications (VoIP) and IPTV services (triple play).
- Source of Internet connectivity independent on business location

Duplex Scheme Support

- The duplex scheme is Usually specified by regulatory bodies, e.g., FCC
- Time-Division Duplex (TDD)
  - Downlink & Uplink time share the same RF channel
  - Dynamic asymmetry
  - Does not transmit & receive simultaneously (low cost)
- Frequency-Division Duplex (FDD)
  - Downlink & Uplink on separate RF channels
  - Full Duplexing (FDX): can Tx and Rx simultaneously;
  - Half-duplexing (HDX) SSs supported (low cost)

MAC addressing, IDs & use

- Subscriber station (SS) has 48-bit IEEE MAC address
- (Fixed) WiMAX Base station (BS) has a 48-bit base station ID – it is not a MAC address (BSID contains 24-bit operator indicator)
- 16-bit connection ID (CID)
- 32-bit service flow ID (SFID)
- 16-bit security association ID (SAID)
- Connection-oriented service
  - Point-to-Point
  - Point-to-Multipoint

QoS Classes in WiMAX

- UGS (Unsolicited Granted Services) – allocated capacity, e.g. for VoIP
- RTPS (Real-Time Polling Services) – BS asks periodically SS, e.g. multimedia, audio, …
- NRTPS (Non-Real-Time Polling Services) – longer delay OK – FTP downloads
- BE (Best Effort) – e.g. HTTP
- ERT-VR (Extended Real-Time Variable Rate Services) – latency guaranteed, not speed. Defined in IEEE 802.16e

Security in WiMAX

- Authentication
  - x.509 SS to BS (not the other way)
- Encryption
  - DES for encryption
  - 168bit 3DES for key exchange
  - Data frames only