



*Josef Hrubý*

Moderní technologie Internetu

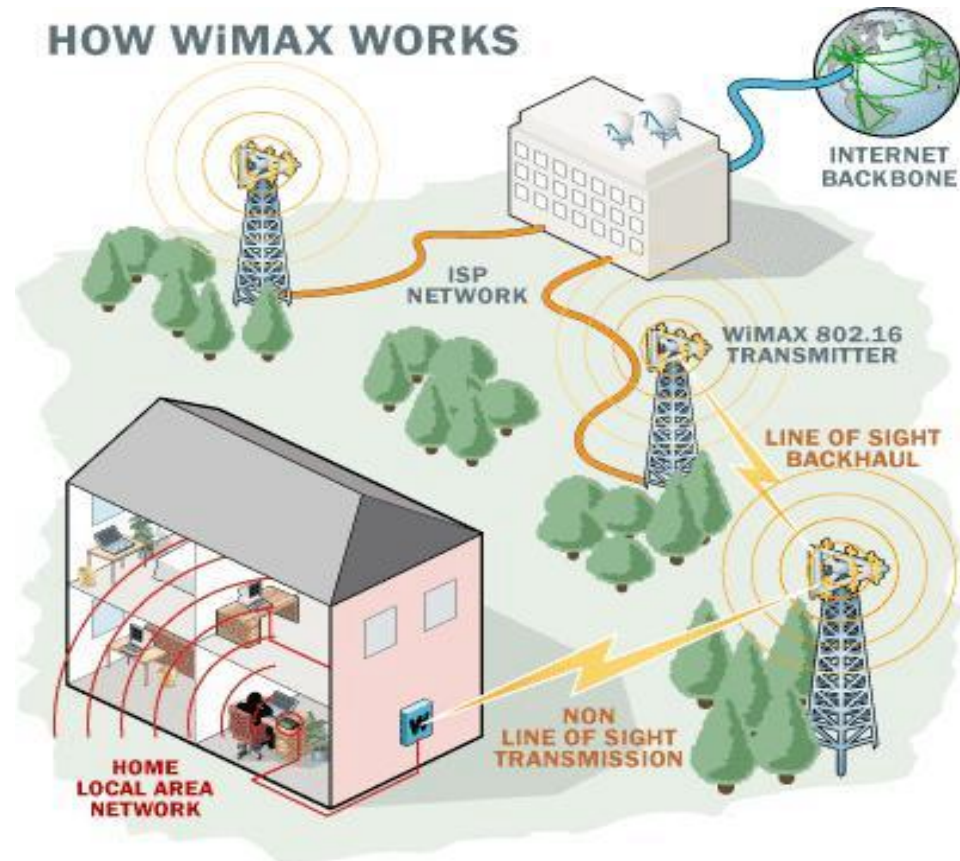
26.10.2007



# WiMAX

- | *Worldwide Interoperability for Microwave Access*
- | Stále se vyvíjející bezdrátovou technologií
- | Definován v IEEE 802.16
- | WiMAX ~ WiFi
- | WiMAX != WiFi

# Jak to funguje



## Vývoj norem

- | 802.16 (2001)
- | 802.16a (2003)
- | 802.16b (2003)
- | 802.16c (2003)
- | 802.16d (2004)
- | 802.16e (2005)
- | 802.16f (2005)
- | 802.16g (2007)

## 802.16

- | 2001
- | 10 – 66 GHz
- | Kapacita 134 Mbit/s
- | Požadavek přímé viditelnosti (LOS)
- | Topologie point-to-multipoint
- | Neprosadil se

## 802.16a

- | 2003
- | 2-11 GHz
- | Kapacita 75 Mbit/s
- | Bez požadavku na přímou viditelnost (NLOS)
- | Dosah 3-5 km, 50 km
- | Samoorganizující se mesh topologie

## 802.16b, 802.16c

### 802.16b

- | QoS přímo na linkové vrstvě
- | Upřednostňování provozu citlivého na zpoždění a jeho kolísání

### 802.16c/d

- | Profily systému 802.16
- | Vlastnosti pro interoperabilitu zařízení

## 802.16e

- | 2005
- | Mobilní WiMAX
- | do 6 GHz
- | mobilní host až do rychlosti 150 km/h
- | nižší přenosová kapacita (cca 15 Mbit/s)



## Přehled norem

Standard	802.16	802.16a	802.16e
Standardizace	2001	2003	2005
Spektrum	10-66 GHz	2-11 GHz	< 6 GHz
Podmínky kanálu	LOS	NLOS	NLOS
Bitová rychlost	32 – 134 Mbit/s	Až 75 Mbit/s	Až 15 Mbit/s
Modulace	QPSK, 16QAM, 64QAM	BPSK, 64QAM (256QAM)	BPSK, 64QAM (256QAM)
Mobilita	fixní	Fixní, přenosný	Nomadic, plně mobilní
Dosah	2 – 5 km	7 – 10 km (max. 50 km)	2 – 5 km

# Fyzická vrstva

- I Definuje použití kmitočtů 2-11 GHz
- I Využívá OFDM (*Orthogonal Frequency Division Multiplexing*)

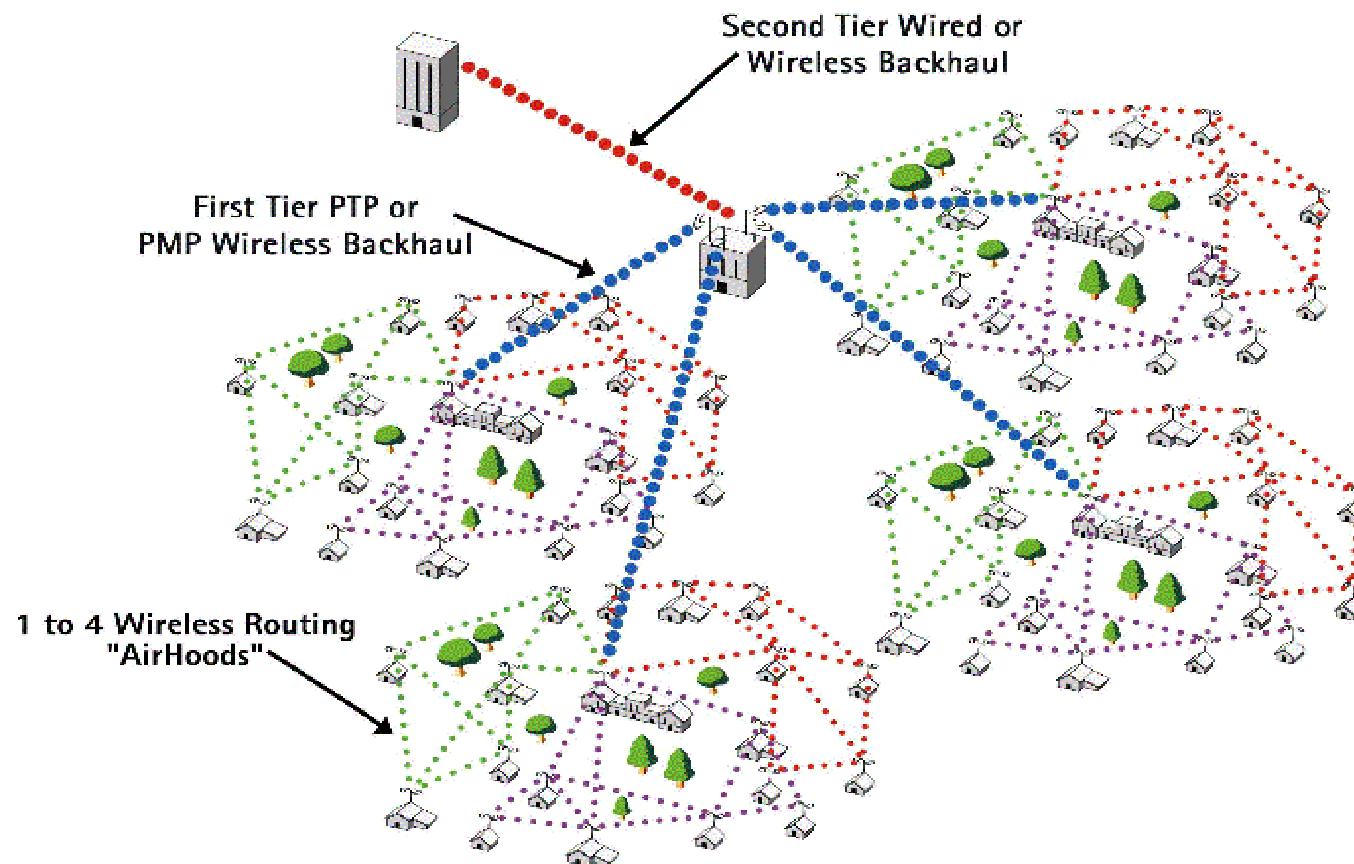
## Varianty fyzické vrstvy:

- I OFDM + OFDMA
- I TDD (*Time-Division Multiplexing*)
- I FDD (*Frequency-Division Duplex*)
- I Šířka pásma 1.5 – 20 MHz

# Topologie

- | WMAN – typicky *point-to-multipoint*
- | topologie *mesh* – efektivní
- | Replikace signálu na cestě od základové stanice
- | „*hop by hop*“
- | Využití moderních antén (*beam-forming*)

# Mesh topology



## MAC vrstva

- | TDM pro dopředný směr
- | TDMA pro zpětný směr
- | Centralizovaný plánovač
- | Garance maximálního zpoždění
- | Jednodušší podpora pro skupinové vysílání

## MAC vrstva

- | Podpora pružného přidělování šířky pásma
- | Specifikace řízení vysílacího výkonu
- | Měření kvality kanálu
- | DFS – bezlicenční pásma
- | Dělení buněk do sektorů
- | Řízení rádiového spoje RLC
- | Certifikát X.509 pro autentizaci a autorizaci
- | PKM – ochrana dat
- | DES – šifrování + 3DES s klíčem

## Adresace a spojení

- I Každá účastnická stanice má 48 bitovou MAC adresu, používána při registraci pro ustanovení odpovídajícího spojení
- I Spojení jsou identifikována 16 bitovým CID, což dovoluje až 64K spojení v rámci každého downlink/uplink kanálu
- I Požadavky na kanál vždy vycházejí z CID

## Adresace a spojení

- I Při inicializaci účastnické stanice by měla být mezi základovou a účastnickou stanicí založena tři spojení v každém směru
- I Základní spojení je určeno pro zasílání krátkých urgentních zpráv řízení MAC
- I Primární spojení slouží k zasílání delších, an zpoždění méně kritických zpráv řízení MAC
- I Sekundární spojení slouží pro zasílání zpráv řízení standardních protokolů vyšších vrstev (DHCP, TFTP, SNMP atd. ) – tyto zprávy přenášeny v IP paketech



## Spojovaný charakter

- I Komunikace mezi základnovou stanicí a koncovou stanicí na úrovni MAC vrstvy  
navázání spojení => přenos => ukončení spojení
- I Po registraci účastnické stanice se vytvoří jedno spojení pro každý tok služby
- I Základnová a koncová stanice si mohou dohodnout požadovanou třídu QoS v rámci toku služby
- I Základnová stanice sestavuje na základě známých údajů o hostech a jejich požadavcích přenosový plán

## Třídy QoS

- **Unsolicited Grant Service**
- **Real-Time Polling Service**
- **Non Real-Time Polling Service**
- **Best Effort Service**

# Zabezpečení

- | Velký důraz na zabezpečení sítě a uživatelů
- | Protokol PKM
  - podvrstva *privacy*
  - PKM = „*protokol pro management klíčů*“
  - zajišťuje distribuci klíčů klientům
  - synchronizace klíčů
  - klienti – autorizace + periodická reautorizace
  - autentizace klienta na základě certifikátů
  - model klient/server
  - **PKMv1**: X.509, RSA, symetrické šifrovací algoritmy
  - **PKMv2**: nová hierarchie klíčů, AES-CMAC, MBS

# Šifrování

- | Šifrování veřejným klíčem
- | Zabezpečení výměny klíčů pro šifrování provozu (TEK)
- | 2-úrovňový mechanismus pro odlehčení zatížení síťových prostředků
- | Provoz šifrován pomocí 168b 3DES (VPN)
- | Volitelné 802.11i
- | Šifrování pouze datových rámců
- | Rámce pro management dovolují získat informace o uživateli sítě (*záplavové útoky*)

## Autentizace a autorizace

- | Na základě digitálního certifikátu X.509
- | Certifikát = veřejný klíč + MAC klient. Stanice
- | Autorizační klíč zašifrovaný veřejným klíčem
- | Pravidelná reautorizace zákl. stanice
- | Zpráva „*authentication information*“
- | „*authorization request*“ = AK + SAID + CID
- | „*authorization reply*“
- | Jednostranná autorizace => *Man-in-the-Middle*
- | 802.16e - EAP

## Bezpečnostní hrozby

- | Falešné základnové stanice
- | Útoky typu DoS
- | Útoky typu *Man-In-The-Middle*
- | Falšování zpráv pomocí managementu sítě



## WiMAX Forum

- | Podpůrná organizace WiMAXu (2003)
- | Spolupráce s IEEE a ETSI
- | Ve vedení Samsung Electronics
- | Propaguje technologii
- | Certifikuje produkty podle příslušných norem
- | Příprava profilů
- | Zahrnuje 240 firem včetně Microsoftu, Intelu, dalších.



WiMAX  
FORUM

# Výhody a uplatnění

## VÝHODY:

- I Nízké investiční náklady
- I Práce za nepřímé viditelnosti
- I Podpora ze strany WiMAX Fora
- I Podpora výrobce čipů (Intel)

## POUŽITÍ

- I Páteřní mikrovlnné propojení
- I Pevný bezdrátový přístup
- I Mobilní přístup
- I Konkurence xDSL

## PROBLÉMY:

- I Frekvenční pásmo pro Evropu

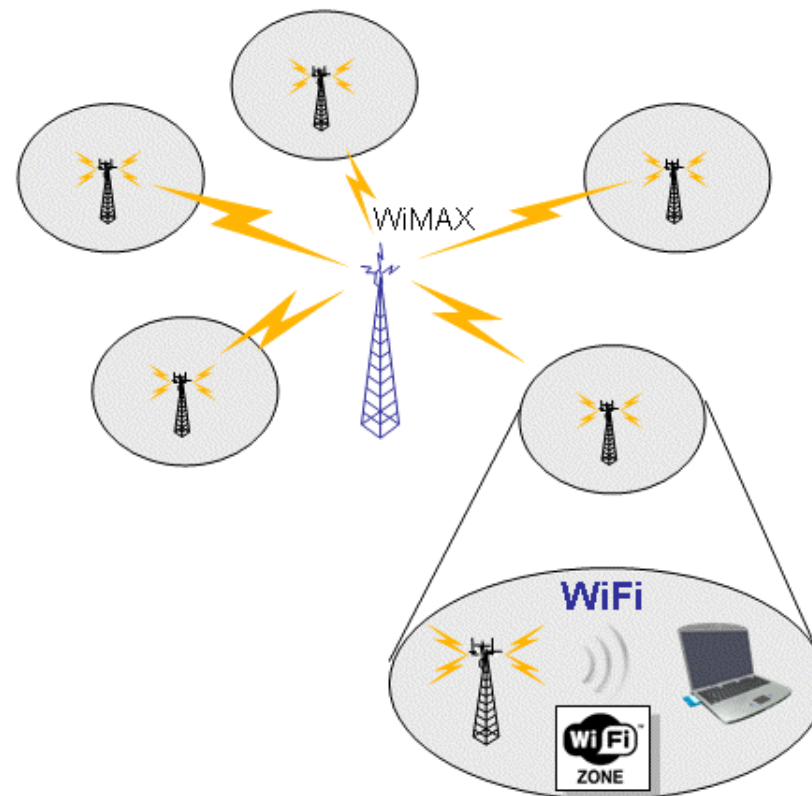


## WiMAX vs. xDSL

charakteristika	xDSL	WiMAX
médium	Vyhrazené	Sdílené
Max. pokrytí	5 km, 7 km	12 ~ 15, 1 ~ 2 [km]
Architektura	DSLAM, xDSL NT	BS, SS
Max. rychlost	8 Mb/s, 800 kb/s	70 Mb/s, 4Mb/s
Roaming	Ne	Ano
QoS	Jako u ATM	Diferenciace služeb
Škálovatelnost	Závislé na DSLAM, přeslechy	Závislé na provozu, minimální rušení
Napájení u zákaz.	Ze sítě	Ze sítě nebo baterií

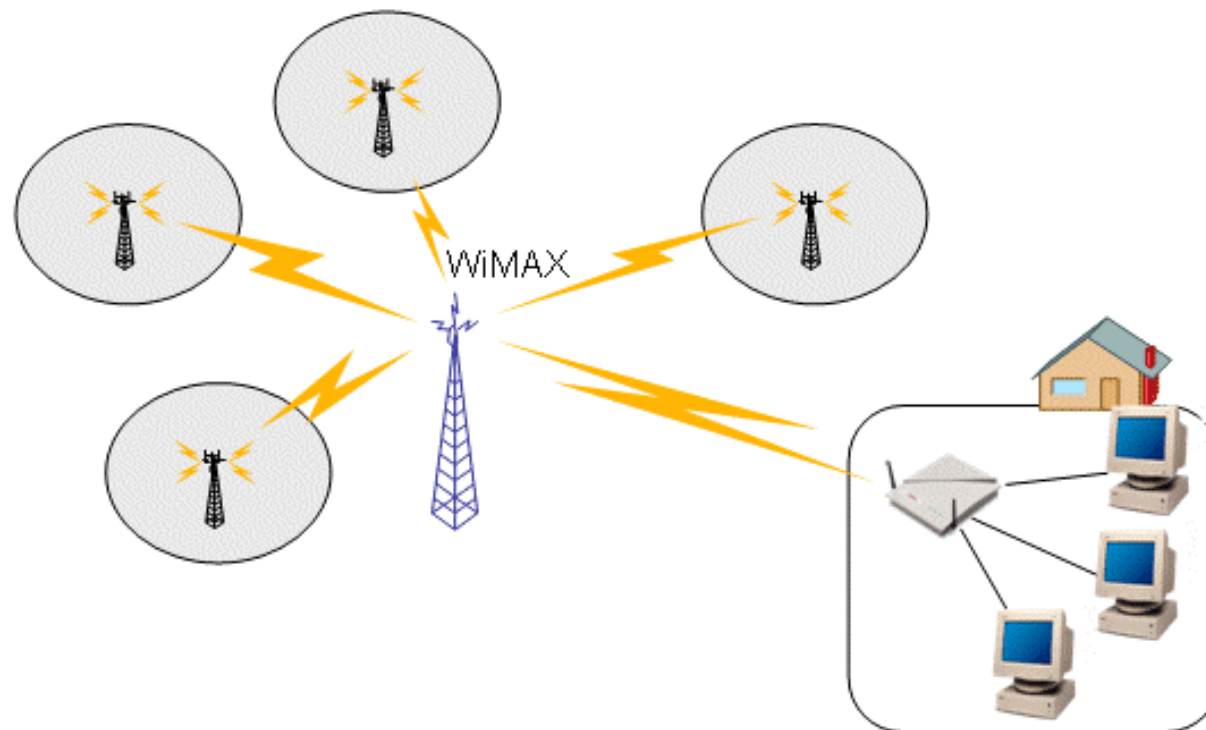
# Použití I

Připojení jednotlivých WiFi hotspotů:



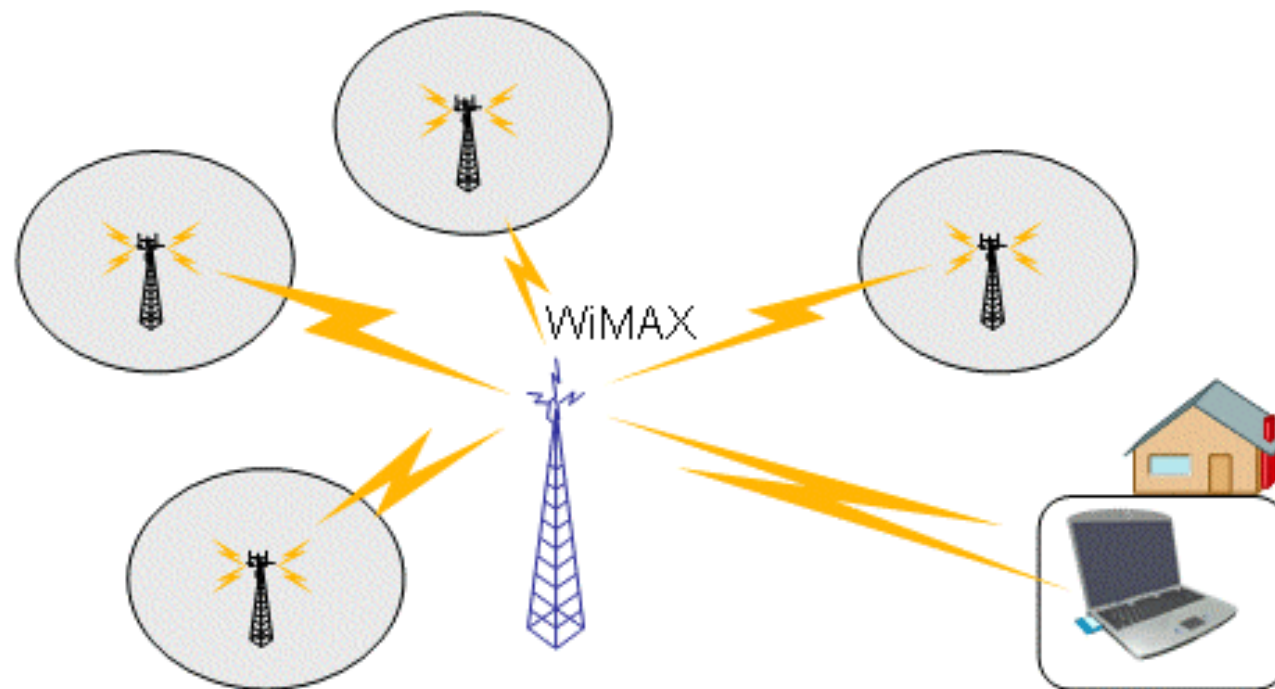
## Použití II

Konektivita pro jednotlivé LAN



## Použití III

Konektivita pro jednotlivé hosty (i mobilní 802.16e)



# Komponenty



# Strategie Intelu

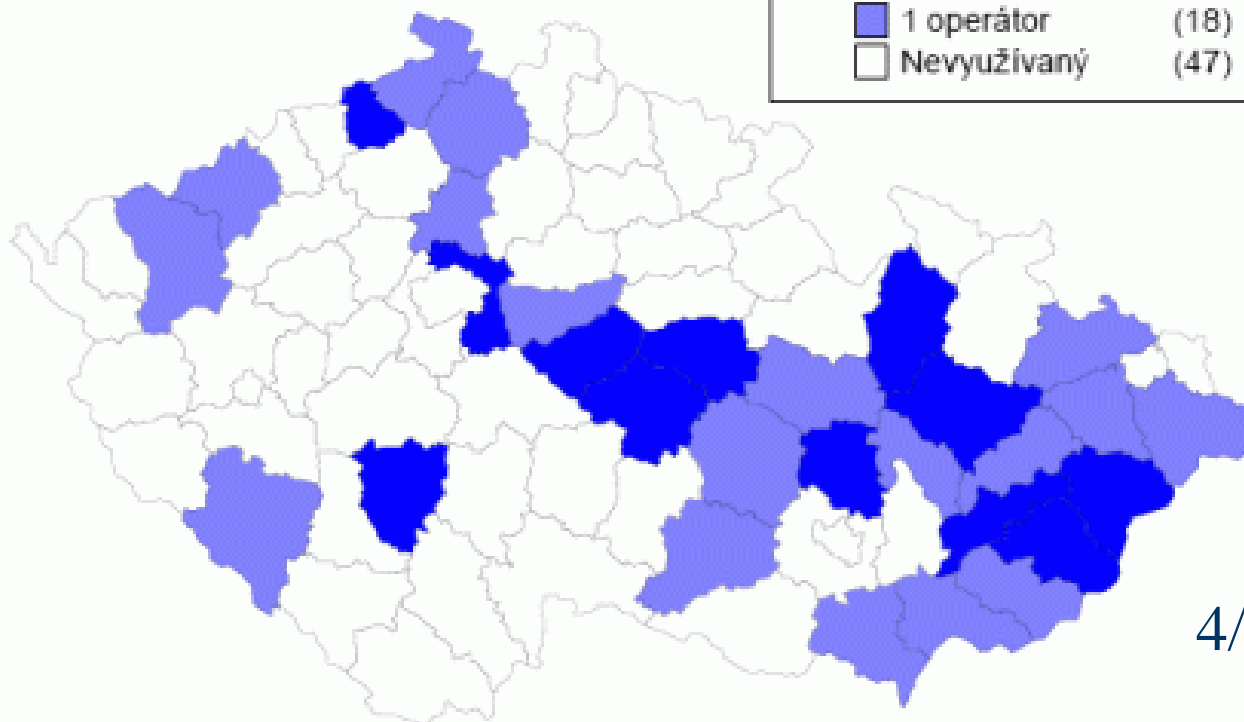


# WiMAX v ČR

## WiMAX Broadband

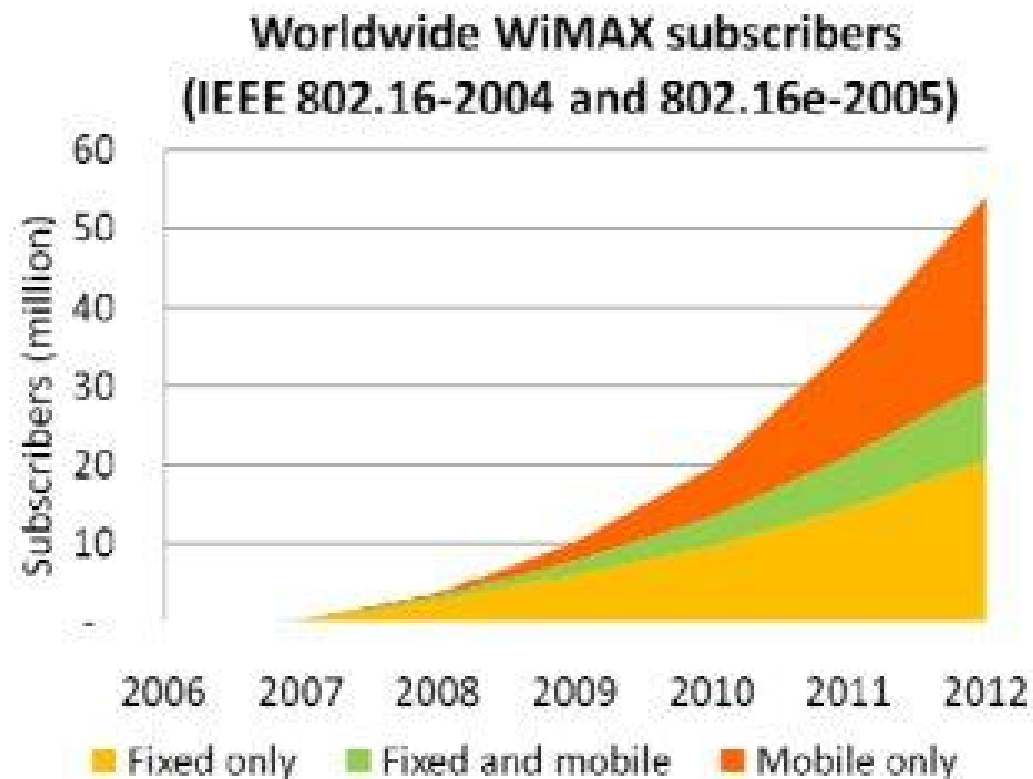
Dostupnost WiMAX 3,5 GHz

- 2 a více operátorů (12)
- 1 operátor (18)
- Nevyužívaný (47)



4/2006

# Budoucnost





## Odkazy

- | [WiMAX Forum](#)
- | [WiMAX.cz](#)
- | [Mobilmania.cz](#)
- | [ISDN.cz](#)
- | [utfg](#)