

Otázka: Bezdrátové sítě

Předmět: Informatika

Přidal(a): Puřas

Typy bezdrátových sítí

1. Wifi (IEEE 802.11 x)

x nahrazují písmena, která specifikují druh standardu

- a – 5 GHz, 54 Mb/s pro profesionální spoje
- b – 2,4GHz, 11 Mb/s překonané, pro koncového zákazníka (BFU)
- g – 2,4GHz, 54 Mb/s standard pro BFU (starší AP, překonané)
- n – 2,4 / 5 GHz, přenosová rychlost AP – podle rádií (současný standard) koncová stanice max kolem 150 Mb/s
- ac – 5 GHz, 433 Mbps, šířka kanálu 80 Hz (nový)

Antény (směr signálu- polarizace- zisk (citlivost))

- směr signálu
 - všesměrové (kratší vzdálenost, ale širší pokrytí)
 - sektorové
 - směrové (musí se zaměřit, dlouhá vzdálenost)
- polarizace (musí být stejná na přijmači i vysílači)
 - kruhová

- lineární
 - horizontální
 - vertikální
- Zisk (dB)
 - Výkon síťové karty + zisk antény - ztráta vedení k anténě < povolená norma ČTU

Zabezpečení

1. Skrytí SSID
2. Filtrování podle MAC
3. Šifrování
 1. WEP (staré = nebezpečné)
 2. WPA (slabé šifrování)

- WPA2 (Silná šifra AES)

Osobní heslo - 1 heslo pro všechny

Podnikové certifikáty

2. BlueTooth (IEEE 802.15.1)

v1.2 - 2.0 3 MB/s, 2,4 GHz

v3.0 24 MB/s, 2,4 GHz

Třídy (podle dosahu v terénu)

1. 1m

2. 10m
3. 100m

Využití

- Připojení telefonů, notebooků, tiskáren, headset...
- Max 11 zařízení

3. **WiMax** (IEEE 802.16)

- Dosah 60 km s rychlostí 70 Mb/s a odolnost proti rušení (může být vedle Wifi)
- Last mile technologie
- Využití zatím v nepřístupném terénu

Dva standardy

1. Mobilní WiMax (2,4 - 5 GHz)
2. Stacionární Wimax (2,4 - 11 GHz)

Rozdíl Wifi a Wimax

- Zatímco Wifi slouží spíše koncovým uživatelům, WiMax slouží spíše poskytovatelům díky mnohem delšímu dosahu a mohl by se stát i konkurencí 3G

4. **Irda**

- Infračervený
- 2 Mb/s
- Dosah 20 cm

- Používán u telefonů a notebooků a PSP

5. Laserové spoje

- Dosah 10 km
- Rychlost 100 Mb/s
- Vyžaduje přímou viditelnost

Technologie

1. CDA
 - Vytáčení přes mobily
2. GSM (digitální)
 - GPRS
 - Edge
 - 3G
 - 4G

Zabezpečení

Způsoby zneužití

- Krádež části přenosového pásma
- Maskování podvodné aktivity přes naši síť (odpovědnost padá na vlastníka sítě)
- Odposlech naší komunikace

Způsoby zabezpečení

- Filtrovat zařízení (téměř překonáno)
- Heslo a šifrování (některé metody překonány (WEP))
- Účty na proxy serveru (školy)

Metody určené hlavně pro Wifi

1. Filtrování MAC adres
 - Prolomeno
 - MAC adresy se dají odposlechnout
2. WEP (Wired Equivalent Privacy)
 - Slabá šifra
 - Stejně šifrování pro všechna spojení
 - Nedostatečné
3. WPA (Wifi Protected Access)
 - Šifruje všechny komunikace zvlášť
 - WPA1 - TKIP (Slabá proudová šifra)
 - Není doporučováno
 - WPA2 - AES (asymetrické blokové šifrování)
 - Doporučováno
4. Využití proxyserveru jako brány, ke které se musí nejprve uživatel přihlásit a až poté uvidí síť a bude mít přístup k internetu

Bluetooth

1. PIN
 2. Uživatel musí akceptovat
 3. Možnost definice zařízení, která se mohou připojit pomocí HW adresy
- Význam převážně pro mobilní telefony