



X36LOS – 3. cvičení

Bezdrátové sítě



WiFi

- Wireless Fidelity ('logo'  pro 802.11a,b zařízení)
- WLAN – wireless LAN
- standardy IEEE 802.11a,b,g(,n)
- přenos v pásmu 2,4GHz (b,g,n) a 5GHz (a,n)



802.11 standardy

Protocol	Release Date	Op. Frequency	Throughput (Typ)	Data Rate (Max)	Modulation Technique	Range (Indoor)	Range (Outdoor)
Legacy	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s		~20 Meters	~100 Meters
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	OFDM	~35 Meters	~120 Meters
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	DSSS	~38 Meters	~140 Meters
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	OFDM	~38 Meters	~140 Meters
802.11n	June 2009 (est.)	2.4 Ghz 5 GHz	74 Mbit/s	248 Mbit/s		~70 Meters	~250 Meters
802.11y	June 2008 (est.)	3.7 GHz	23 Mbit/s	54 Mbit/s		~50 Meters	~5000 Meters



Architektura sítě

- Ad Hoc
 - IBSS (Independent Basic Service Set)
- AP (Access Point)
 - propojení AP
 - pevnou sítí
 - WDS (Wireless Distribution System)



Zabezpečení (1)

- Autentizace a šifrování
- WEP – Wired Equivalent Privacy
 - sytem auth.: open vs. shared key
 - WEP klíč (40b-232b) + inicializační vektor IV (24b)
 - zabezpečení každý paketu zvlášť
 - Weak Keys – špatný IV (WEPplus)
 - šifrování DES
 - oprava: WEP2, WEP+, dWEP



Zabezpečení (2)

- WPA – WiFi Protected Access (2003)
 - personal (pre-shared key) vs enterprise (802.1x)
 - používá TKIP (Temporal Key Integrity Protocol)
 - lepší IV (ochrana před Weak Keys)
 - Re-keying (automatická výměna klíče)
 - Message Integrity Check
 - Per Packet Mixing (měnění pozice IV)
 - šifrování AES