X36LOS – 3. cvičení

Bezdrátové sítě

WiFi

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

Architektura sítě

- STA (Station)
  - jednotlivé stanice
  - např. NIC v PC, PDA, notebook, ...
- AP (Access Point)
  - centrální komunikační prvek
  - propojení AP
    - pevnou sítí
    - WDS (Wireless Distribution System)

Připojení do sítě

- Typy autentifikace a asociace
  - neautentifikovaný a neasociovaný
    - stanice je odpojena od sítě a není asociovaná s AP
  - autentifikovaný a neasociovaný
    - stanice byla autentifikována do sítě ale ještě nebyla asociována s AP
  - Authenticated and associated
    - stanice je připojena do sítě a je schopná přijímat a vysílat data s pomocí AP

Architektura sítě

- **BSS** (Basic Service Set)
  - komunikuje jen s pomocí Access Pointu (AP)
- **IBSS** (Indipendent BSS)
  - často formovaná bez předešlého plánování – Ad Hoc síť
  - někdy nazývána jako peer-to-peer
- **DS** (Distribution systém)
  - spojuje více BSS pomocí propojení AP
- **ESS** (Extended Service Set)
  - transparentni vůči LLC

Zabezpečení (0)

- Skrývání SSID
  - SSID - Service Set Identifier - 32bit
- Autentifikace pomocí MAC

Zabezpečení (1)

- Autentizace a šifrování
- WEP – Wired Equivalent Privacy
  - MAC vrstva
  - WEP klíč (40b-232b) + inicializační vektor IV (24b)
  - zabezpečení každého paketu zvlášť
  - Weak Keys – špatný IV (WEPplus)
  - šifrování DES

Zabezpečení (2)

- WPA – WiFi Protected Access
  - používá TKIP (Temportal 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