# Securitate rețele

## 3.3. Securitatea reţelelor wireless

# 3.3.1. Recunoaşterea importanţei solicitării unei parole pentru protejarea accesului la o reţea wireless.

- Dacă aveţi o conexiune la o reţea wireless, care este neprotejată, ar trebui să vă gândiţi să o protejaţi prin parolă. Într-adevar, este mai uşor să lăsaţi o conexiune la internet fără parolă, deoarece vă puteţi conecta cu uşurinţă dacă aveţi un nou calculator sau dacă aveţi musafiri (are doresc să se conecteze).
- Este important să ne amintim că există pericole pentru fişiere și computer, dacă nu vă securizaţi conexiunea la reţea.
- Dacă permiteţi unei persoane necunoscute să se conecteze la reţeaua dvs. wireless nesecurizată, există o posibilitate ca cineva neautorizat să acceseze, să modifice sau chiar să copieze informaţii de pe computer.
- Pe de altă parte, dacă sunt mai multe dispozitive (neautorizate) conectate la echipamentul de reţea, care utilizează servicii de download şi upload, atunci lăţimea de bandă alocată fiecărui computer legitim va fi mult micşorată, ceea ce se traduce printr-o viteză scăzută a conexiunii.
- Un alt punct important constă în faptul că o conexiune la o reţea wireless ce este protejată printr-o parolă poate fi criptată cu un standard de securitate, pentru asigurarea confidenţialităţii datelor transmise.
- Setarea unei parole, cât şi a unui tip de criptare pentru o reţea wireless se realizează în interfaţa router-ului, pe baza utilizatorului şi a parolei furnizate de producătorul echipamentului.

# 3.3.2. Recunoaşterea diferitelor tipuri de securitate wireless, precum: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC)

- **Wired Equivalent Privacy (WEP)** este un protocol de securitate pentru reţele locale fără fir (WLAN). WEP este conceput pentru a oferi acelaşi nivel de securitate ca cea a unei reţele locale cu fir (LAN).
- LAN-urile sunt în mod inerent mai sigure decât WLAN-urile pentru că reţelele locale sunt oarecum protejate de părţile de structură, unele sau toate făcând parte din reţeaua din interiorul unei clădiri, unde accesul poate fi restricţionat.
- WLAN-urile, care transmit datele prin unde radio, nu au aceeaşi structură fizică şi, prin urmare, sunt mai vulnerabile la manipulare. WEP îşi propune să ofere securitate prin criptarea datelor astfel încât acestea să fie protejate când sunt transmise de la un punct la altul. Cu toate acestea, s-a constatat că WEP nu este la fel de sigur cum se credea.

- WEP este folosit la cele mai mici două straturi ale modelului OSI - stratul fizic şi stratul legături de date. Prin urmare, nu oferă securitate end-to-end (de la primul la ultimul strat).
- Modelul OSI (Open Systems Interconnection) este un grup de protocoale de comunicaţie aşezate ierarhic, folosit pentru a realiza o reţea de calculatoare şi un model pentru schimbul datelor între acestea.
- În ordine crescătoare, aceste straturi
  - 1 fizic,
  - 2 Legătura de date,
  - 3 reţea,
  - 4 transport,
  - 5 sesiune,
  - 6 nivel prezentare,
  - 7 aplicație

- **WI-FI Protected Access (WPA)** este o tehnologie de securitate pentru rețele de calculatoare WI-FI, WPA îmbunătăţeşte caracteristicile de autentificare şi criptare WEP (Wired Equivalent Privacy). De fapt, WPA a fost dezvoltat de Industria de networking ca răspuns la punctele slabe ale WEP.
- WPA oferă o criptare mai puternică decât WEP, prin utilizarea uneia dintre cele două tehnologii standard: Temporal Key Integrity Protocol (TKIP) şi Advanced Encryption Standard (AES).
- Tehnologia **Media Access Control** (MAC) furnizează instrumente de identificare unică şi de acces a sistemelor de calcul la o reţea de calculatoare, ce utilizează protocolul Internet (IP). Într-o reţea wireless, MAC reprezintă protocolul de control radio al calculatorului, integrat în stratul 2 - legături de date, al modelului de referinţă OSI.
- MAC stabileşte un număr unic de identificare fiecărui adaptor de reţea, numit adresă MAC, în funcţie de care administratorul de reţea poate permite conectarea la reţea a dispozitivului respectiv.

# 3.3.3. Conectarea la o reţea wireless protejată / neprotejată

- Pentru a vă conecta la o reţea wireless utilizând sistemul de operare Microsoft Windows 7, parcurgeţi următorii paşi:
  1. Executaţi click pe butonul **Start**
  2. Din meniul Start selectaţi **Control Panel**.
  3. În fereastra panoului de control executați click pe **NetWork and Sharing Center**

4. Selectaţi opţiunea **Connect to a network**.

5. în fereastra din partea dreaptă-jos a ecranului executaţi click pe reţeaua dorită. Debitaţi opţiunea **Connect automatically** dacă nu doriţi conectarea automată la reţea, iar apoi apăsaţi butonul **Connect.**