Capitolul 7:
Rețele Wireless

De ce wireless?

- Mobilitate
  - creșterea în popularitate a dispozitivelor mobile: laptop-uri, PDA-uri
  - roaming
- Ușurință în instalare
  - hoteluri și săli de conferință
  - clădiri vechi
- Cost redus

Rețelele business din ziua de azi evoluează pentru a oferi suport persoanelor ce se află în mișcare. Dacă folosești un telefon mobil pentru aplicații de instant messaging acest lucru este datorat mobilității oferite de rețelele actuale.

Sunt multe infrastructuri ce permit mobilitate, dar cele mai actuale sunt tehnologiile Wireless.

Angajații oricărei firme beneficiază actualmente de tehnologii wireless ce le permit să își verifice email-ul, voice mail-ul de oriunde folosind un PDA sau un telefon mobil.

În afară de mobilitate, Wireless-ul oferă o mai mare ușurință în instalare față de orice soluție cablată cât și un cost mai redus.

Folosind tehnologii wireless, costurile necesare unei soluții cablate sunt aproape eliminate.

Mediul de transmisie

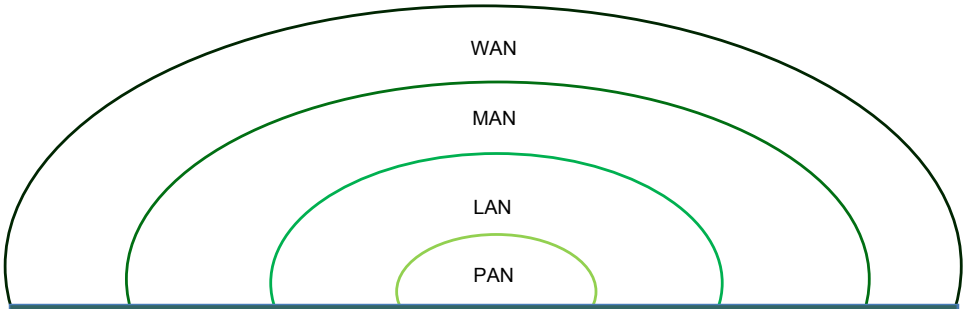
- Unde electromagnetice
  - unde radio
  - microunde
- Probleme de transmisie
  - atenuarea semnalului
  - interferențe
- Probleme de securitate
  - limitarea ariei de acoperire
  - mediu cu acces multiplu → bandă partajată

Rețelele Wireless folosesc ca mediu de transmisie undele electromagnetice, în principal undele radio. Din această cauză, în comparație cu rețelele cablate, tehnologiile Wireless sunt mai predispuse la interferențe datorită celorlalte echipamente de folosință zilnică ce folosesc unde radio.

Tehnologiile Wireless întâlnesc aceleași provocări ca și cele cablate când este vorba de distanța de transmisie. Astfel, odată ce un echipament Wireless se îndepărtează de sursa semnalului se observă o atenuare semnificativă pană la punctul în care semnalul nu se mai recepționează deloc.

Undele radio nu pot fi mărginite astfel încât pachetele ce circulă pe acest mediu au un risc mai ridicat în ceea ce privește atacurile de securitate. Pachetele pot fi interceptate de oricine are access la mediu.

Tehnologii Wireless



	PAN	LAN	MAN	WAN
Standard	Bluetooth	IEEE 802.11a/b/g	802.16 MMDS,LMDS	GSM,GPRS, CDMA, 2.5-3G
Viteză	<1 Mbps	Peste 100Mbps	22+ Mbps	10 – 384 Kbps
Rază	Mică	Medie	Medie-Mare	Mare
Aplicații	Peer-to-Peer Device-to-Device	Retele Enterprise	Last-mile Access	PDA, Telefoane Mobile

Wireless LAN-urile au aceeași origine ca și LAN-urile Ethernet. Ambele au fost ratificate de IEEE în portofoliul 802 LAN/MAN de standarde ale arhitecturilor de rețele de calculatoare. Cele mai importante standarde existente în portofoliu au fost 802.3 (Ethernet) și 802.11 (wireless LAN).

Comunicațiile portabile au devenit o necesitate zilnică în lumea actuală. Astfel portabilitatea și mobilitatea sunt prezente în echipamente precum tastaturi fără fir, căști, telefoane prin satelit sau GPS-uri (Global Positioning System). Pentru a satisface nevoile fiecărui echipament Wireless avem actualmente următoarele standarde cu facilități specifice fiecărei nevoi.

Tehnologii Wireless

- PAN (Personal Area Network)
  - Bluetooth, IEEE 802.15
- **LAN (Local Area Network)**
  - **IEEE 802.11**
- MAN (Metropolitan Area Network)
  - IEEE 802.11, IEEE 802.16, IEEE 802.20
- WAN (Wide Area Network)
  - GSM, CDMA, Satelite

Standardele PAN Bluetooth și 802.15 permit viteze de transmisie de sub 1 Mbps pentru distanțe scurte folosite în principal pentru aplicații peer-to-peer sau device-to-device.

Standardul LAN 802.11 permite viteze de transmisie de 11 pana la 54 Mbps pentru distanțe medii folosit în rețelele Enterprise.

Standardele MAN 802.11, 802.16 și 802.20 permit viteze de transmisie de 10 până la 100 Mbps pentru distanțe medii și lungi și sunt folosite în principal pentru Last Mile Access.

Standardele WAN GSM, CDMA permit viteze de transmisie de 10 Kbps până la 2 Mbps pentru distanțe lungi și sunt folosite în principal pentru dispozitivele mobile de date.

Benzi ISM

- Industrial, Scientific and Medical
- Benzi publice
  - nu necesită licențiere
- Frecvențe înalte
  - 6MHz – 245GHz (nu întreg spectrul)
  - ușor absorbite în atmosferă
- Dezavantaj: sunt aglomerate
  - mouse, tastatură wireless
  - telecomenzi
  - stații emisie-recepție

802.11 Wireless LAN este un standard IEEE ce definește cum benzile de frecvențe radio din ISM (Industrial, Scientific and Medical) sunt folosite la nivelul mediului fizic și al subnivelului MAC.

Benzile ISM sunt benzi publice ce nu necesită licențiere ce se află în intervalul 6MHz – 245 GHz frecvențe înalte ce se atenuează ușor în atmosferă.

Faptul că aceste benzi nu necesită licențiere constituie și un dezavantaj deoarece din această cauză ele sunt foarte aglomerate. Majoritatea vendor-ilor de dispozitive fără fir aleg să folosească aceste benzi.

Tehnologii Wireless LAN

- **802.11** (1997)
  - primul standard wireless, acum “legacy”
  - 900 MHz / 2.4 GHz
  - 1-2 Mbps
- **802.11b** (1999)
  - 11 Mbps
  - 2.4 GHz

Tehnologiile Wireless au evoluat odată cu creșterea nevoilor de viteză și performanțe sporite. Astfel 802.11 la apariție avea viteze de 1 – 2 Mbps și folosea banda de 2.4 Ghz. La acea vreme LAN-urile pe tehnologii cablate operau la viteze de 10 Mb/s așa că tehnologia Wireless nu a fost primită cu prea mult entuziasm.

De atunci, tehnologiile Wireless au evoluat continuu trecând prin 5 standarde : 802.11a, 802.11b, 802.11g și 802.11n, 802.11ac.

802.11b este un standard ce atinge viteze de pană la 11 Mbps folosind modularea de tip DSSS (Direct Sequence Spread Spectrum) în banda de 2.4 GHz. Deși nu este unul din punctele importante de reținut este bine de știut că modularea OFDM determină viteze mai rapide de transmisie în timp ce modularea DSSS este mai simplă și mai ieftin de implementat.

Tehnologii Wireless LAN

- **802.11a** (1999)
  - 54 Mbps
  - 5GHz
- 802.11a și 802.11b nu sunt compatibile

802.11a este unul din primele standarde apărute cu o viteză de până la 54 Mbps ce adoptă modularea de tip OFDM (Orthogonal Frequency Division Multiplexing) și banda de 5GHz. Dispozitivele ce operează în banda de 5 GHz intâmpină mai puține interferențe decât cele care operează pe banda de 2.4 GHz deoarece sunt mai putine dispozitive ce rulează pe această frecvență. Un dezavantaj important al benzii de 5 GHz este faptul că frecvența mai înaltă o face să fie mai puțin penetrantă astfel fiind mult mai puțin performantă datorită obstacolelor. Un al doilea dezavantaj este faptul că frecvența mai înaltă scade distanța de propagare a semnalului față de banda de 2.4 GHz. Din această cauză 802.11a a fost mai puțin folosit decât 802.11b sau 802.11g.

Tehnologii Wireless LAN

- **802.11g** (2003)
  - 54 Mbps
  - 2.4 Ghz
  - compatibil cu 802.11b, dar incompatibil cu 802.11a
- **802.11n** (2009)
  - până la 600Mbps
  - 2.4 GHz și 5 GHz
  - compatibil cu 802.11a/b/g
- WiFi Alliance
  - reglementarea standardelor

Tehnologiile Wireless care au cea mai mare cota de piață în momentul actual sunt 802.11g (retificat în 2003) și 802.11n (retificat în 2009).

802.11g este un standard ce folosește modularea OFDM în banda de 2.4 GHz atingând astfel viteze de până la 54Mbps. 802.11g suportă însă de asemenea și modulare DSSS pentru a oferi compatibilitate cu standardul 802.11b. Banda de 2.4 GHz oferă o propagare la o distanță mai bună decât banda de 5GHz. 802.11g cumulează astfel avantajele standardelor 802.11a (viteza) și 802.11b (distanța). 802.11b a fost multă vreme standardul dominant pe piața Wireless.

802.11n este un standard inovator ce folosește mai multe antene de transmisie. El poate funcționa atât pe banda de 2.4 GHz cât și pe cea de 5 GHz și poate atinge viteze de până la 600 Mbps. 802.11n folosește modulare de tip OFDM o noutate specifica acestui standard fiind tehnologia MIMO (Multiple Input/ Multiple Output) ce permite transmiterea unui pachet în bucăți pe canale diferite simultan.

Comparație tehnologii WLAN

Standard	802.11a	802.11b	802.11g	802.11n
Publicare	1999	1999	2003	2009
Frecvență	5GHz	2.4GHz	2.4GHz	2.4GHz / 5GHz
Viteză	54Mbps	11Mbps	54Mbps	160-600 Mbps
Modulare	DSSS	OFDM	OFDM	MIMO
Acoperie Interior Exterior	35m 120m	38m 140m	38m 140m	70m 250m
Avantaje	Semnal puternic pe rază mică	Preț scăzut	Viteza mai mare ca b Compatibil cu b	Acoperire mare Vizteză mare
Dezavantaje	Incompatibil cu b și g (mai răspândite)	Interferențe	Interferențe	Standard nou și încă scump

Actualmente standardul 802.11g este în continuare cel mai folosit dar odată cu dezvoltarea echipamentelor mai performante pentru transmiterea datelor pe standardul 802.11n se previzioneaza că acesta va avea monopolul în tehnologiile Wireless.

Putem clasifica tehnologiile WLAN în funcție de tipul de modulație pe care acestea le folosesc: OFDM, DSSS și MIMO.

DSSS (Direct-sequence spread spectrum) este folosit de 802.1a.

OFDM (Orthogonal frequency-division multiplexing) este o metodă de encodare a datelor digitale pe mai multe frecvențe și este folosit în implementările 802.1b și 802.1g.

MIMO (Multiple-input and multiple-output) este tehnologia ce permite folosirea unor antene multiple atât la emoțător cât și la receptor pentru a imbunătăți performanța comunicării. Tehnologia WLAN ce beneficiază la ora actuală de această modulare este 802.1n.

Dispozitive Wireless

- Wireless NIC
- Wireless Bridge

Asemenea Ethernet NIC-ului, Wireless NIC-ul foloseşte tehnica de modulare setată de tehnologia WLAN folosită şi encodează un stream de date în semnale radio. NIC-urile wireless sunt adesea asociate cu echipamentele mobile precum un laptop sau PDA. Aceste NIC-uri se găsesc în mai multe forme în funcţie de metoda de conectare la echipamente precum: NIC-uri PCI, NIC-uri PCMCIA, şi NIC-uri USB.

În ultimul timp marea majoritate a echipamentelor mobile vin din fabrica cu NIC-uri Wireless încorporate, datorită dezvoltării infrastructurilor de acces mobil la nivelul corporaţiilor si spaţiilor publice.

Dispozitive Wireless

- Access point
- Router Wireless

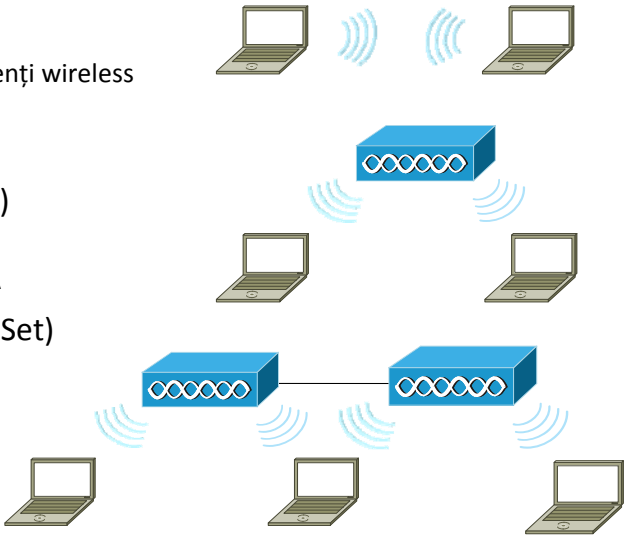
Un Access Point (AP) conectează clienții wireless la rețeaua wired. De regulă clienții wireless nu comunică între ei direct ci prin intermediul unui AP. Access Point-ul convertește datele TCP/IP din încapsularea frame-ului 802.11 a rețelei wireless în încapsulare 802.3 pentru transmisia pe rețeaua Ethernet.

Datorită modului de transmisie și recepție a datelor în mediul Wireless, echipamentele nu detectează coliziunile ci sunt proiectate pentru a le evita (nu se pot detecta coliziuni in aer).

Ruter-ul Wireless acționează ca un Access Point, Switch Ethernet și Ruter. În primul rând este un AP ce interconectează clienții wireless, în al doilea rând oferă posibilitatea interconectării de echipamente Ethernet cu ajutorul unui switch 10/100/1000 full-duplex fiind și un router ce oferă funcția de gateway permițând conectarea la alte infrastructuri.

Tipuri de rețele WLAN

- Ad hoc
  - conexiune între doi clienți wireless
  - nu necesită un AP
- BSS (Basic Service Sets)
  - necesită un AP
  - zona de acoperire: BSA
- ESS (Extended Service Set)
  - rețea de AP-uri



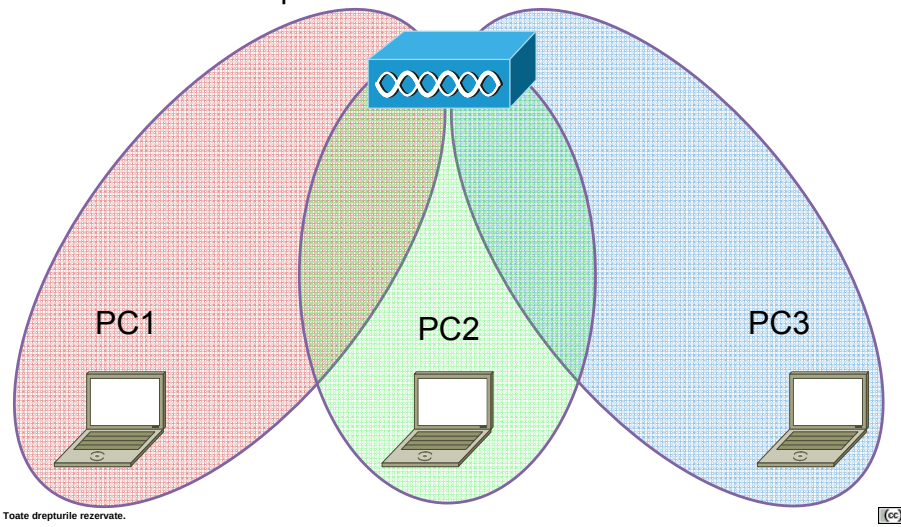
Rețele ad-hoc sunt rețele wireless care funcționează fără un Access Point. Clienții care sunt configurați să funcționeze în acest mod își configurează parametrii wireless între ei. Standardul 802.11 clasifică rețelele ad hoc drept independent BSS (IBSS).

Topologiile de tip Basic Service Set folosesc un AP ce oferă infrastructurii posibilitatea de a adăuga servicii și o rază de acțiune sporită pentru clienți. Toți parametrii wireless sunt configurați de către AP. Aria de acțiune în topologia BSS se numește BSA (Basic service area).

Un alt tip de topologie este ESS (Extended Service Set) ce folosește un număr mai mare de topologii BSS interconectate pentru a spori raza de acoperire a infrastructurii numită ESA. În cadrul acestei topologii fiecare BSS este identificat unic prin BSSID, acesta reprezentând adresa MAC a Access Point-ului.

CSMA/CA

- Carier Sense Multiple Access with Collision Avoidance



Una din problemele majore ale comunicației wireless este faptul că nu putem asculta și recepționa în același timp. O consecință a acestei limitări este faptul că nu putem implementa collision detection.

O altă problemă ar fi cea a terminalului ascuns în care PC1, în raza de acțiune a AP-ului și în afara razei de acțiune a transmițătorului PC3, nu poate ști dacă PC3 trimite sau nu informații.

Soluția acestor probleme este implementarea CSMA/CD ce funcționează în felul următor:

Un nod/client ce dorește să transmită date trebuie să asculte pe canal un timp predefinit pentru a determina dacă un alt nod transmite pe același canal. În cazul în care canalul este liber, nodul va putea transmite datele iar în caz contrar va amâna transmisia pentru un timp aleatoriu.

Pași în conectarea la un WLAN

- Probing
  - descoperirea rețelelor WLAN din raza de acoperire
  - trimitere cerere de asociere
- Autentificare
  - autorizare în rețea
- Asociere
  - MAC-ul stației este asociat cu AP-ul

Înainte ca un client 802.11 să poată trimite date pe WLAN, el trebuie să parcurgă următorii pași:

Prin **802.11 Probing** clienții descopera sau caută o rețea specifică trimițând o cerere de asociere numită Probe. Această cerere specifică SSID și bit rate-ul când se dorește asocierea cu un AP. În situațiile în care clientul dorește să descopere WLAN-urile disponibile va trimite o cerere fără să anunțe SSID-ul.

Autentificarea se realizează folosind diferite mecanisme precum WEP, WPA sau WPA2, ultimul pas fiind asocierea cu un AP.

În acest stadiu al conectării, clientul invață BSSID AP-ului (MAC-ul AP-ului) iar access point-ul va mapa un port logic numit AID (Association ID) clientului.

După asocierea clientului cu un access point , acesta va putea trimite și primi date.

Probleme de securitate

- Semnalul wireless
  - nu poate fi delimitat într-o zonă dorită
  - interferențe din partea altor dispozitive
- Accesul la rețeaua wireless
  - War drivers
- Denial of Service
- Man în the Middle

Tehnologiile wireless folosesc undele radio și acest lucru implica un set de riscuri aparte. O problema persistenta în design-ul de infrastructuri wireless este limitarea zonei de acoperire.

Lipsa unui circuit închis duce la amplificarea riscurilor unor atacuri de retea precum **denial-of-service** și **Man în the Middle.**

Un atac de tip **denial-of-service** (dos) sau distributed denial-of-service (ddos) este o incercare de a bloca resursele unui calculator. Indiferent de metodologie, scopul unui asemenea atac este în general de a bloca un serviciu care ruleaza în retea .

Într-un atac **Man în the Middle** atacatorul se pozitioneaza între client și echipamentul de retea putând intercepta tot traficul acestuia destinat clientului.

Protocoale de securitate WLAN

- Open
  - nu necesită cunoașterea unei parole
  - securitate asigurată prin filtrare de adrese MAC
- WEP
  - Wireless Equivalent Privacy
  - intrdus odată cu standardul 802.11 revizuit (1999)
  - chei statice => ușor de spart
- WPA
  - WiFi Protected Access
  - rezolvă probleme de securitate ale WEP
  - algoritm TKIP

Toate produsele wireless sunt configurate standard în modul Open Access. Acest mod este preferat pentru locuri publice precum cafenele și campus-urile facultăților, oferind un mod facil de conectare – nu este necesară nicio parolă pentru access la rețea. Cu toate acestea, natura deschisă a rețelei înseamnă ca pachetele trimise pe conexiuni HTTP nesecurizate pot fi ușor interceptate.

WEP este prima modalitate de securizare a unei retele wireless, fiind disponibil începând cu 802.11b. Deși necesită o parolă la conectare, aceasta poate fi ușor aflată de persoane malițioase dacă se reușește capturarea unui număr suficient de pachete.

Securitatea WPA este cea mai modernă și mai sigură metoda de securizare a unei rețele wireless – utilizează algoritmul TKIP pentru a genera chei unice pentru fiecare dispozitiv în parte, ceea ce face foarte grea “ghicirea” parolei prin forță brută.

Rezumat

- CSMA/CA
- Unde electromagnetice
- WPA, WEP, Open Access

1. Care este distanța maximă pentru 802.11g ?
2. Câte canale nu se suprapun pentru 802.11b?
3. Ce fel de modulare are 802.11?
4. Descrieți pașii de conectare la WLAN.
5. Descrieți funcționalitatea CSMA/CA.