

**Universitatea Politehnica Bucuresti**  
**Facultatea de Electronica, Telecomunicatii si Tehnologia informatiei**

**Tema: Mac- Wireless LANs**

**Priiu Ana-Maria, 441A**  
**Zanfir Catalin, 441A**  
**Manole Laurentiu, 442A**

## **Cuprins:**

### **Pruiu Ana-Maria**

Introducere.....	3
Arhitectura unui WLAN.....	4
Arhitecturi de retele WLAN.....	6

### **Zanfir Catalin**

OFDM.....	9
802.11.....	12
DSSS.....	15

### **Manole Laurentiu**

Introducere roaming.....	18
Nivele de roaming.....	19
Roamingul telefoniei wireless.....	21

## Wireless LAN

### 1.1 Introducere

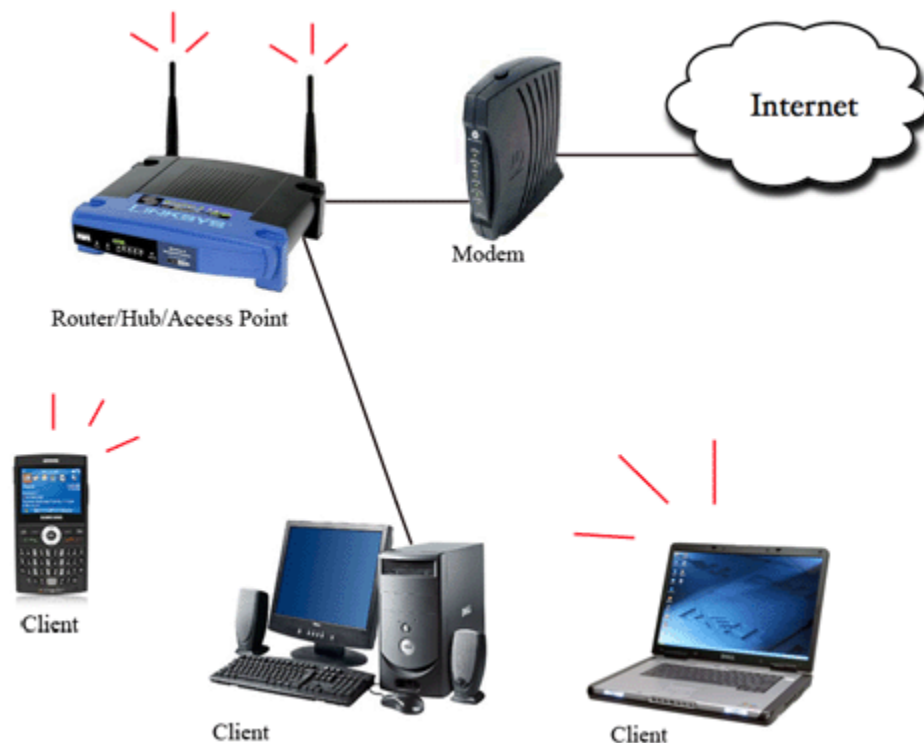
Wireless Local Area Network este o denumirea generica a tehnologiei si a retelelor de dispozitive bazate pe transmisii de date fara fir. Telefoanele mobile dotate cu tehnologia Wlan se pot conecta la o retea locala sau pot accesa internetul prin intermediul unei retele locale atata timp cat se afla in aria de acoperire a retelei.

Tehnologia Wireless a contribuit la simplificarea procesului de creare a unei retele prin faptul ca permite mai multor calculatoare sa se conecteze simultan la aceleasi resurse in incinta casei sau chiar intr-o firma fara a fi nevoie de cabluri suplimentare. Aceste resurse pot fi o conexiune broadband la internet, imprimante in retea, fisiere si chiar partajarea unor fisiere audio sau video. [2]

Un WLAN, ca si un LAN clasic necesita un mediu fizic prin care sa se realizeze transmiterea unei purtatoare de semnal. Se pot utiliza unde infrarosii sau frecvente radio. Pentru undele radio, banda de frecventă este cuprinsa intre 2.4 GHz si 5GHz. În majoritatea tarilor, aceste valori nu sunt rezervate pentru dispozitive licentiate, de aceea nu necesita licente guvernamentale speciale pentru a functiona. Exista posibilitatea ca o retea wireless sa se conecteze la o retea care foloseste fire.

WLAN –urile au viteze mari de transfer pornind de la 1 Mbps si ajungand pana la 54 Mbps, unii furnizori oferind solutii si pentru viteze de 108 MBPS. Standardul 802.11n poate ajunge de la 300 pana la 600 Mbps.

Deoarece semnalul wireless poate fi captat de toti cei care se afla in aria de acoperire trebuiesc luate masuri de securitate pentru a ne asigura ca doar utilizatorii autorizati pot accesa WLAN-ul propriu.[2]



## **Avantajele WLAN-urilor:[3]**

Principalele avantaje ale WLAN-urilor sunt:

- Comoditate: pot fi utilizate rețele WLAN publice.
- Mobilitate: se poate utiliza fără a întrerupe conexiuni.
- Instalare: este foarte simplă deoarece nu sunt necesare cabluri, nu sunt necesare elemente fixe în rețea, folosindu-se în principal sisteme distribuite.
- Scalabilitate: posibilitatea de a adăuga sau de a scoate dispozitive foarte repede.
- Costuri: este necesară o investiție inițială, dar banii investiți se recuperează rapid.

## **Dezavantajele WLAN-urilor:[3]**

Cele mai importante dezavantaje ale WLAN-urilor sunt următoarele:

- Securitate: din cauza faptului că antenele folosite nu sunt direcționate, semnalul poate fi recepționat de oricine. Se pot folosi metode de criptare, dar acestea au dezavantajul că prin codificare este împiedicată interceptarea, dar nu este împiedicată perturbarea.
- Distanță: în mod obișnuit distanța este de 10 metri.
- Siguranță: răspandirea undelor radio poate fi influențată de mai mulți factori, reducându-se puterea semnalului. Fenomenele de interferență care apar pot afecta eficiența demodulației.
- Viteza: având în vedere cele spuse mai sus se poate observa faptul că pe măsură ce distanța crește scade viteza de transfer, dar viteza maximă poate fi mai mică decât viteza curentă printr-o rețea cu cablu. În același timp în multe situații viteza unui link wireless este mai mare decât viteza de conectare.
- Rata emisiilor: se generează impulsuri electrice care pot afecta sănătatea umană.

## **1.2 Arhitectura unui WLAN:**

### **Statii:**

Toate componentele care se conectează la un mediu wireless într-o rețea poartă numele de stații. Toate stațiile sunt echipate cu controlere de interfață de rețea wireless (WNIC-wireless network interface controller). Aceste stații pot face parte din una din cele două categorii: puncte de acces (access points) sau clienți.

Punctele de acces (AP), de obicei rutere, sunt stații de bază pentru rețeaua fără fir. Ele transmit și recepționează frecvențele radio pentru a permite comunicarea între dispozitivele wireless.

Clienții wireless pot fi dispozitive mobile precum laptop-uri, telefoane mobile, smartphone-uri sau dispozitive fixe precum desktop-uri și stații de lucru care sunt echipate cu interfețe pentru rețele wireless. [5]

### **BSS( Basic service set):**

BSS-ul este totalitatea statiilor care pot comunica una cu cealalta. BSS-ul (setul serviciului de baza) reprezinta blocul de baza din care sunt alcatuite retelele wireless care trebuie sa acopere distante mari. Fiecare BSS are un ID de identificare numit BSSID, care este adresa MAC a punctului de acces care deservește BSS-ul. Exista dooua tipuri de BSS: BSS independent care mai este notat si IBSS si BSS de infrastructura.

Un BSS independent este o retea ad-hoc care nu contine puncte de acces, ceea ce inseamna ca nu se poate conecta la un alt BSS. Aceste BSS-uri sunt de fapt elementele principale care alcatuiesc o retea WLAN.

In figura de mai jos sunt reprezentate doua BSS-uri, fiecare dintre ele avand cate doua statii si totodata este reprezentata si aria de acoperire a fiecarui BSS printr-un cerc. Daca una din statatiile BSS-ului iese din aria de acoperire a BSS-ului respectiv atunci ea nu mai poate comunica cu celelalte statii membre ale aceluiasi BSS. [5]



### **ESS (Extended service set):**

Un ESS (setul serviciului extins) reuneste mai multe BSS-uri. Punctele de acces in ESS-uri sunt conectate prin sisteme distribuite. La fel ca si BSS-urile si ESS-urile au un identificator (ID) numit SSID care este un sir de caractere pe maxim de 32 de biti. Atunci cand vrea sa se conecteze la un WLAN un client scaneaza mai intai toate retelele si abia apoi selecteaza SSID-ul pentru a se conecta la o anumita retea wireless. [5]

### **DS (Distibution system):**

Un sistem de distributie (DS) conecteaza punctele de acces intr-un ESS. Un sistem de distributie este folosit pentru a transporta cadrele la destinatie. Este elementul de retea care asigura transmiterea cadrelor intre punctele de acces. Conceptul de sistem de distributie poate fi utilizat pentru a creste acoperirea retelei prin roaming intre celule. Sistemul de distributie poate fi cablat sau poate fi wireless. Majoritatea sistemelor de distributie actuale se bazeaza pe protocoalele MESH sau WDS, desi alte sisteme sunt in folosinta. [5]

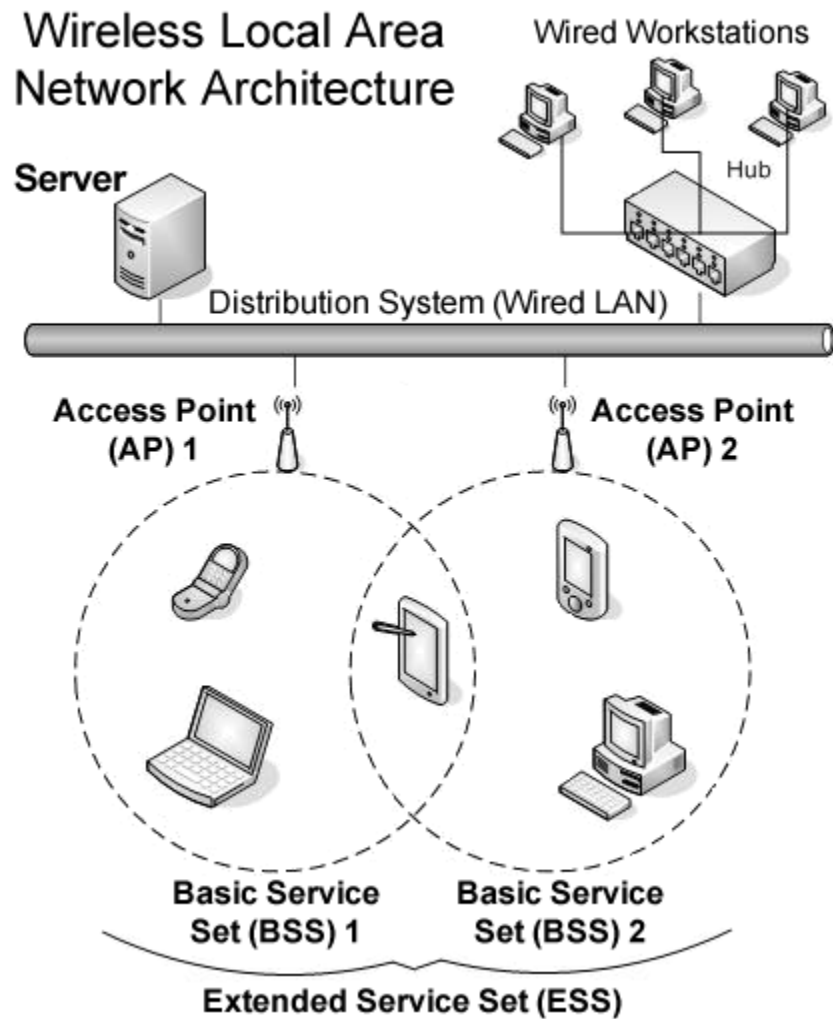


Fig. Arhitectura unui WLAN [4]

### 1.3 Arhitecturi de rețele WLAN:

Cele mai utilizate tipuri de arhitecturi WLAN sunt următoarele:

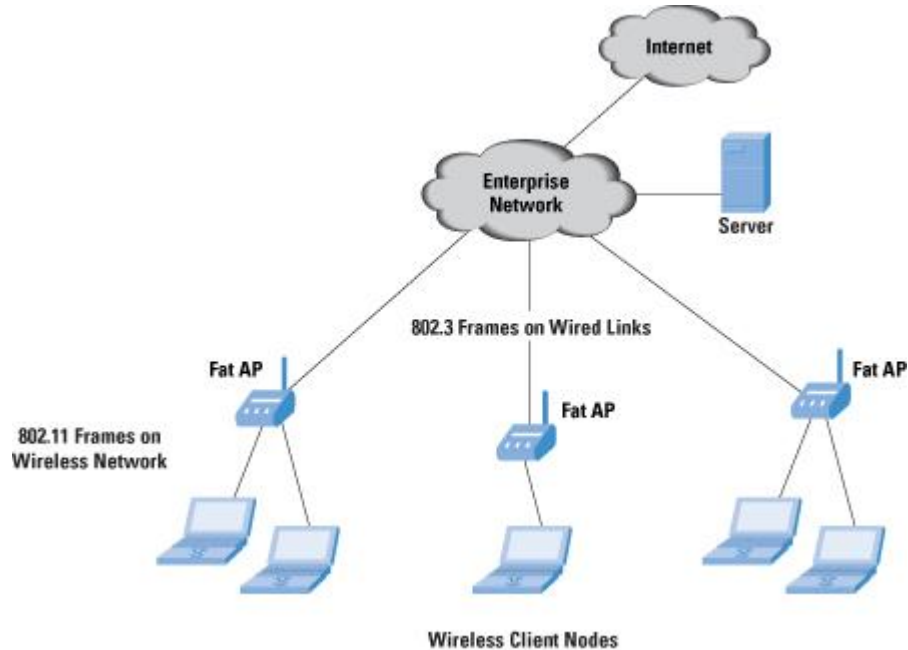
- Arhitectura autonoma (Autonomous Architecture)
- Arhitectura centralizata (Centralized Architecture)
- Arhitectura distribuita (Distributed Architecture)

#### Arhitectura autonoma:

Intr-o retea autonoma punctele de acces implementeaza in intregime functia 802.11, asa ca intr-o retea cu cabluri LAN cadrele sunt cadre 802.3. Fiecare punct de acces poate fi accesat in mod independent ca un element separat de retea. Punctele de acces in cele mai multe rețele se numesc "Fat AP".

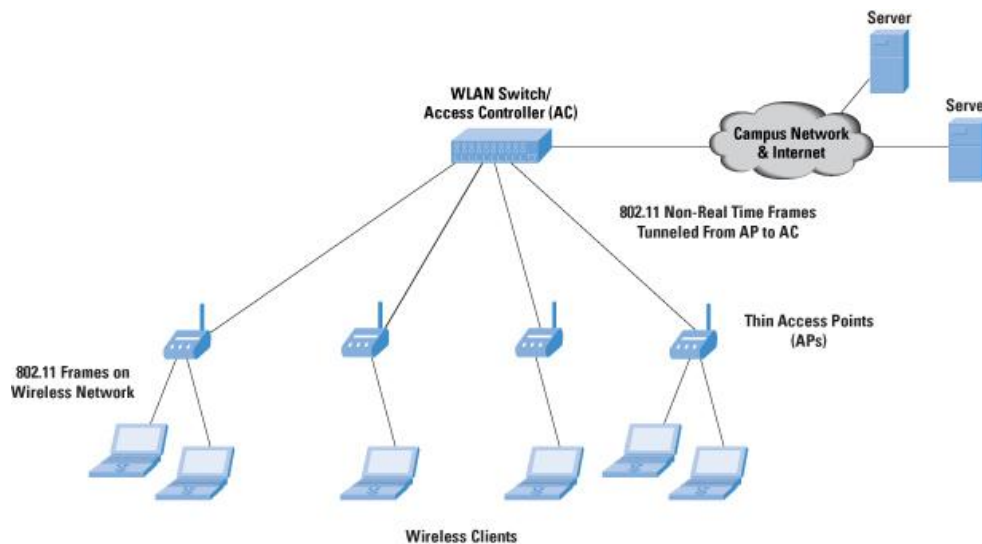
In fazele initiale ale implementarii WLAN, cele mai multe puncte de acces sunt automatizate si pot fi gestionate ca elemente independente de retea.

In decursul ultimilor ani arhitecturile centralizate cu controlere de acces (AC) si puncte de acces (AP) au castigat popularitate. Principalul avantaj al arhitecturii centralizate este ca ofera administratorilor de retea un mod structurat si ierarhic de control al multipleror puncte de acces. [6]



### Arhitectura centralizata:

Arhitectura centralizata este o arhitectura ierarhica care implica un controler WLAN care este responsabil pentru configurarea, controlul si managementul mai multor puncte de acces. Controlerul WLAN este de asemenea cunoscut si sub numele de AC (Acces Controller). Functia 802.11 este impartita intre AP si AC. Deoarece punctele de acces din acest model au o functie redusa in comparatie cu arhitectura autonoma, ele sunt de asemenea cunoscute ca "Thin AP". [6]



### **Arhitectura distribuita:**

In arhitectura distribuita diferite puncte de acces pot forma retele distribuite cu alte puncte de acces prin fire sau conexiuni wireless. O retea plasa de puncte de acces este un exemplu de o astfel de arhitectura. Punctele de acces intr-o retea plasa pot fi legate prin legaturi 802.11 sau legaturi pe cablu 802.11. Aceasta arhitectura este adesea utilizata in retele municipale si alte instalari unde sunt implicate componente "in aer liber". [6]

### **Bibliografie:**

1. <http://www.ijunkey.com/how-to-improve-your-wireless-network/wlan/>
2. <http://insecure.home.ro/wlan.pdf>
3. [http://alpha.tmit.bme.hu/meresek/wlan\\_eng.htm#wlannet](http://alpha.tmit.bme.hu/meresek/wlan_eng.htm#wlannet)
4. [http://en.wikipedia.org/wiki/File:Wlan\\_arch.png](http://en.wikipedia.org/wiki/File:Wlan_arch.png)
5. [http://www.h3c.com/portal/Technical\\_Support\\_Documents/Technical\\_Documents/Routers/H3C\\_MSR\\_50\\_Series\\_Routers/Configuration/Operation\\_Manual/13-WLAN\\_Volume\(V1.05\)/13-WLAN\\_Volume\(V1.05\)/200909/648837\\_1285\\_0.htm](http://www.h3c.com/portal/Technical_Support_Documents/Technical_Documents/Routers/H3C_MSR_50_Series_Routers/Configuration/Operation_Manual/13-WLAN_Volume(V1.05)/13-WLAN_Volume(V1.05)/200909/648837_1285_0.htm)
6. [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_9-3/wireless\\_lan\\_switches.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-3/wireless_lan_switches.html)



## Zanfir Catalin, grupa 441 A

### Fundamentele OFDM (Orthogonal Frequency Division Multiplexing)

Natura aplicatiilor wlan necesita viteze de transfer mari. In mod evident natura constant schimbatoare a canalele wireless ce necesita viteze mari de transfer nu este un lucru usor. Ideea unei transmisii multi-carrier a iesit la suprafata recent, pentru a usura canalele wireless de comunicatii cu transfer mare de date. OFDM este o forma speciala de transmisie multicarrier unde toti suboperatorii sunt ortogonali unul fata de altul. OFDM promite o transmisie capabila de o rata de date mai mare, avand o complexitate si precizie rezonabila.

La un nivel mare de rate de date, distorsiunea canalului asupra datelor este foarte semnificanta si este aproape imposibila de recupera datele transmise initial cu un simplu receptor. Un receptor cu o structura complexa este necesar pentru a face egalizare computationale extensive si algoritmi de estimare asupra pentru a recupera semnalul transmis original. OFDM poate simplifica drastic aceasta problema a egalizarii prin schimbarea frecventei selective a canalului catre un canal constant. O simpla egalizare este necesara pentru a estima canalul si pentru a recupera datele.

Este imperativ ca sistemele de telecomunicatii din viitor sa fie eficiente din punct de vedere spectral pentru a suporta un numar mare de utilizatori. OFDM foloseste spectrul disponibil intr-un mod foarte eficient, ceea ce este folositor pentru comunicatii multimedia. Astfel, OFDM are o sansa foarte buna de a deveni tehnologia de baza pentru 4G. sistemele pure OFDM sau cele hibride vor fi alegerea cea mai buna pentru nivele fizice pentru tehnicile cu acces multiplu in generatia viitoare de sisteme de telecomunicatii.

“Modulatia cu diviziune ortogonala de frecvente este o metoda ce permite transferul cu rate mari in canale extrem de ostile la o complexitate redusa.” [\[sursa\]](#)

#### *Codarea si intercalarea canalului*

Pentru ca purtatorii OFDM sunt impartiti intr-o gama de frecventa, vor mai fi inasa si niste atenuari ale unor frecvente selective la un moment variabil de timp. O atenuare mare pe o frecventa particulara poate avea ca efect o pierdere de date pe acea frecventa pentru un moment de timp dat, astfel, o parte din subpurtatorii pot fi puternic atenuati si vor cauza erori. In aceste situatii, sistem FEC ( forward error control/correction) al COFDM-ului ( Coded OFDM) poate repara aceste eori.

Experientele arata ca sistemele de baza OFDM nu sunt capabile sa obtina un BER de  $10^{-5}$  sau  $10^{-6}$  fara o codare de canal, astfel toate sistemele OFDM de la ora actuala sunt convertite in COFDM. Beneficiile COFDM sunt de de doua ori mai bune in termeni de imbunatire a performantei. Primul beneficiu este cel adus de codarea canalului si consta in micșorarea erorilor brute, iar al doilea este ca intercalarea aduce diversitatea frecventelor. intercalarea asigura ca iesirile adiacente dintrun codor de canal sunt plasate departe una de alta in domeniul frecventelor. Este putin probabil ca amandoi

biti vor avea o atenuare mare, rezultand astfel ca macar unul din biti sa fie receptionat intact la receptor, imbunatindu-se astfel performanta BEF.

*Sistemele OFDM depind de urmatoarele considerente:*

- Latime de banda: marimea latimii de banda va juca un rol semnificativ in determinarea numarului de subpurtatori , deoarece cu o banda mai larga, putem pune un numar mare de subpurtatori avand un spatiu de garda rezonabil.
- Rata de biti : sistemul trebuie sa fie capabil sa intretina rata de date necesara utilizatorilor. De exemplu, pentru a mentine o comunicatie multimedia wireless, sistemul trebuie sa opereze la cel putin 10 Mbps.
- Latenta tolerabila. Experientele dintr-un mediu interior arata o latenta impartita pe maxim cateva sute de nanosecunde cel mult, pe cand experientele dintrun mediu exterior se pot ridica pana la 10 microsecunde.
- Valori Doppler. Utilizatorii pe un vehicul aflat in miscare cu o viteza mare vor experimenta o deplasare Doppler mai mare fata de pietoni, ei experimentand un efect Doppler mai mic.

Eficienta spectrala:

In figura alatura se ilustreaza diferentele dintre sistemele FDM si OFDM.

In cazul OFDM, o mai buna eficienta spectrala se obtine prin mentinerea ortogonalitatii intre sub-purtatori . Cand ortogonalitatea este mentinuta intre subcanale diferite in timpul transmisiunii, atunci este posibil sa separem semnalele in partea receptorului. Benzile de garda pastreaza subcanalele departe unele fata de altele astfel incat separatia canalelor diferite este posibila. Inserarea benzilor de garda rezulta in folosirea ineficienta a resurselor spectrale.

Ortogonalitatea face posibila in OFDM aranjarea subpurtatorilor in astfel incat benzile laterala ale purtatorilor individuali se suprapun si ,totusi, semnalele sunt receptionate de receptor fara a fi afectate de ICI. Receptorul actioneaza ca un OFDM comparata cu FDM [\[sursa\]](#) demodulator , translatand fiecare subpurtator pana la DC, avand semnalul rezultat integrat peste un o perioada pentru recuperarea cruda a datelor. Daca celelalte subpurtatoare sunt toate convertite la frecventele care in domeniul timp ,au un numar intreg de cicli intr-un perioada de simbol  $T_{sym}$  , atunci

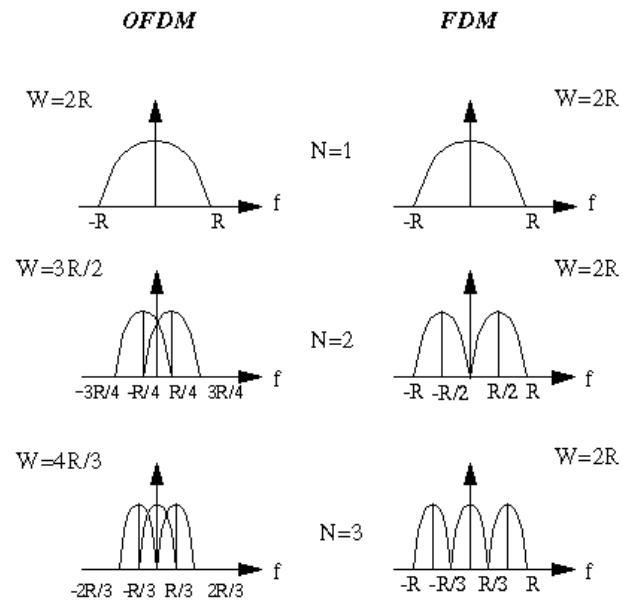


fig1 .Eficienta spectrala

integrarea procesului rezulta contributie nula din partea celorlalti purtatori. Astfel, subpurtatorii sunt liniar independenti, adica ortogonali, daca spatierea dintre purtatori este un multiplu de  $1/T_{sym}$ .

#### *Avantaje OFDM*

1. Frumusetea OFDM-ului consta in simplitate. Un truc ce face ca transmitatoarele OFDM sa aiba un cost mic este abilitatea de a implementa maparea bitilor catre purtatori unici prin folosirea IFFT-ului.
2. Spre deosebire de CDMA, receptoarele OFDM preia energia semnalelor in domeniul frecventelor, astfel ca este abila de a capabila de a proteja pierderile de energie in domeniul frecventelor.
3. Intrun canal cu variatii relativ mici de timp este posibila o imbunatatirea semnificanta a capacitatii prin adaptarea ratei de date pe sub-purtator in corelatie cu raportul semnal-zgomot al acelu sub-purtator particular.
4. Transmitatorul OFDM simplifica efectul de canal, astfel, o structura mai simpla de receptor este de ajuns pentru a recupera semnalul transmis. Daca folosim scheme de modulatie coerent e, atunci estimari simple de canal sunt necesare, iar pe de alta parte, nu mai avem nevoie de estimatoare de canala daca sunt folosite scheme de modulatie diferentia.
5. Procedurile de preservare a ortogonalitatii in OFDM sunt mult mai simple decat cele ale tehnicilor CDMA si TDMA, chiar si in conditii de cai multiple.
6. OFDM poate fi folosita pentru aplicatii multimedia de viteza mare avand un cost scazut.
7. OFDM poate suporta pachete cu acces dinamic.
8. Retelele cu o singura frecventa sunt posibile in OFDM, ceea ce este atractiv pentru aplicatii de broadcast.

#### *Dezavantaje OFDM:*

1. Necesitatea unei sincronizari stricte. OFDM este foarte sensibil la erori de sincronizare in domeniul timp si frecventa, in special pentru erorile de sincronizare in frecventa, unde orice se poate strica. Demodularea unui semnal OFDM cu un offset in frecventa poate duce la o rata de erori foarte mare. Exista doua surse ale erorii de sincronizare: prima fiind diferenta dintre frecventa oscilatorului local din transmitator si din receptor, iar a doua miscarea relativa dintre transmitator si receptor ce da un efect Doppler.
2. Raportul puterii de varf si medie(PAPR). PAPR este proportional cu numarul de subpurtatori folositi pentru sistemele OFDM. Un sistem cu un numar mare de subpurtatori va avea un raport PAPR mare. Un raport PAPR mare face dificila implementarea convertor Digital-Analog si convertor Analog-Digital. Exista 3 metode a micsora PAPR: tehnici de distorsiune ale semnalului, tehnici de codare si tehnica scrambling.

3. Interferente de canal (CCI) . In sistemele de comunicatii celulare, CCI este combatut prin tehnici de combinare de antene adaptive, cum ar fi sectorizarea, antene directe, vectori de antene.

### *Parametrii OFDM*

1. Numarul de subpurtatori : marind numarul de subpurtatori se va reduce rata de date catre fiecare subpurtator.
2. Timpul de garda si duratia simbolului.
3. Spatierea subpurtatorilor.
4. Tipul modulatiei pe subpurtatori.
5. Codarea FEC

### **Retelele Wireless 802.11**

802.11 este un membru al familiei IEEE802 , ce sunt o serie de specificatii pentru tehnologii de retele locale . Specificatiile IEEE 802 sunt concentrate pe cele mai joase nivele din modelul OSI deoarece incorporeaza atat componentele fizice cat si cele de date. Toate retelele 802 au o adresa MAC si o componenta fizica. Macul este un set de reguli folosit pentru a se determina cum se va accesa mediul si pentru a trimite date, dar detaliile de transmisie si receptie sunt lasate pentru componenta fizica.

Specificatiile individuale din seria 802 sunt identificate printr-un numar secund. De exemplu, 802.3 este specificatia pentru o retea Carrier Sense Multiple Access cu detectie de coliziune, si este asociata de obicei , in mod gresit, cu Ethernet-ul. 802.5 reprezinta specificatia pentru Token Ring. 802.2 reprezinta LLC-ul Logical Link Control, iar managementul trasaturilor este descris in 802.1 .

Specificatia 802.11 de baza include MAC-ul si cele 2 niveluri fizice :nivelul cu spectrul cu salt in frecventa (FHSS) si nivelul cu modulatia cu spectru imprastiat prin secventa directa (DSSS). Versiuni ulterioare ale 802.11 adauga mai multe niveluri fizice. 802.11b specifica un nivel cu secventa directa avand o rata mare de transmisie (HR/DSSS); 802.11a descrie un nivel fizic bazat pe acces multiplu cu diviziune ortogonala in frecventa(OFDM).

Retelele 802.11 au 4 mari componente fizice :

*Sistemul de distributie* : cand cateva puncte de acces sunt conectate pentru a forma o mai mare zona de acoperire ele trebuie sa comunice una cu cealalta pentru a detecta miscarile statiilor mobile. Sistemul de distributie este componenta logica din 802.11 si este folosita pentru a inainta cadre catre destinatar. 802.11 nu specifica nici o tehnologie particulara folosita pentru sistemul de distributie.

*Punctele de acces.* Cadrele unei retea 802.11 trebuie convertite in alt timp de cadru pentru livrare. Dispozitivele numite puncte de acces fac functia de punte wireless-catre- cablu. Asta fiind principala lor functie.

*Mediul wireless.* Pentru a muta/transfera cadre de la o statie la alta , se foloseste un mediu wireless. Sunt definite cateva nivele fizice diferite, iar arhitectura permite ca multiple nivele fizice sa fie dezvoltate pentru a suporta MAC-ul 802.11. initial, doua nivele fizice de frecvente radio RF si un nivel fizic infrarosu au fost standardizate.

*Statiile.* Retelele sunt construite pentru a transfera date intre doua statii. Statiile sunt dispozitive computationale cu interfata pentru retea wireless. in mod obisnuit, statiile sunt fie laptopuri, fie calculatoare tip desktop.

Administratorii de retea familiari cu Ethernet-ul vor fi imediat confortabili cu 802.11 . Cele doua sunt atat de asemanatoare, prin mostenire, incat 802.11 este de obicei referita ca fiind "Ethernet wireless".Elementele esentiale prezente in Ethernet sunt prezente si in 802.11. Statiile sunt identificate prin adrese MAC de 48 bytes IEEE 802. In mod conceptual, cadrele sunt livrate bazandu-se pe adresa MAC. Livrarea de cadre nu este fiabila, desi 802.11 incorporeaza mecanisme de fiabilitate de baza pentru a depasi calitatile slabe mostenita ale canalelor radio folosite.

Un mod de a defini o tehnologie de retea este de a defini serviciile pe care le ofera si pentru a permite proiectatilor sa implementeze acele servicii dupa bunul lor plac. 802.11 ofera 9 servicii. Doar 3 dintre acestea sunt folosite pentru a transfera date, restul sunt folosite pentru managementul operatiilor ce permit retelei pentru a tine evidenta nodurilor mobile si pentru a livra cadre in mod corespunzator.

#### *Servicii 802.11:*

*Distributia* : acest serviciu este folosit de statiile mobile in infrastructura retelei ori de cate ori se transmit date. Cand un cadru a fost acceptat de un punct de acces, foloseste serviciul de distributie pentru a livra cadrul catre destinatar. Orice comunicatie care foloseste un punct de acces trece prin serviciul de distributie, incluzand comunicatiile intre 2 statii mobile asociate cu acelasi punct de acces.

*Integrarea.* Este un serviciu oferit de sistemul de distributie, el permite conexiunea unui sistem de distributie la un o retea non- 802.11 IEEE. Functia de integrare este specifica sistemului de distributie folosit si nu este specificat de 802.11 , exceptand termenii de servicii pe care trebuie sa il ofere.

*Asocierea* : Livrarea cadrelor catre statiile mobile este posibila deoarece statiile mobile se inregistreaza sau se asociaza cu punctele de acces. Sistemul de distributie poate folosi informatia din inregistrare pentru a determina care punct de acces poate fi folosit pentru fiecare statie mobila. Statiile neasociate nu sunt in retea, la fel cum statiile de lucru cu cablurile ethernet scoase nu sunt nici ele in retea. 802.11 specifica functiile pe care trebuie sa le ofere sistemul de distribuire folosind datele de asociere.

*Reasocierea.* Cand o statie mobila se muta intre arii de servicii dintr-o zona cu un singur serviciul extins, trebuie sa evalueze puterea semnalului si, in functie de asta, sa aleaga alt punct de acces. Reasocierea sunt initiate de statiile mobile cand conditiile de

semnal indica faptul ca o alta asociere ar fi mai potrivita. Reasocierile nu sunt initiate de punctele de acces.

*Disasocierea.* Pentru a se incheia o asociere existenta, statiile pot folosi serviciul de disasociere. Cand statiile invoca acest serviciu, orice date mobila stocata in sistemul de distributie este stearsa. Odata ce disasocierea este completa statia mobila nu mai este conectata la retea. Mac-ul este proiectat astfel incat sa se acomodeze cu statiile care apeleaza acest proces pentru o deconectare 'politicoasa' cat si pentru statiile ce intrerup brusc conexiunea.

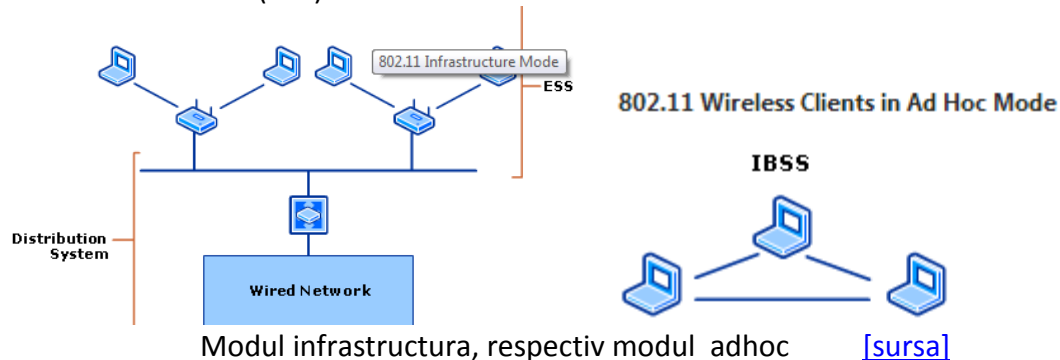
*Autentificarea.* Este folosita pentru a oferi securitatea la accesul retelei. Numai statiile autentificate pot folosi reteaua.

*Deautentificarea.* Acest proces inchide o statie autentificata inainte.

*Intimitatea :* retelele wireless ofera un serviciu de intimitate numit Wired Equivalent Privacy, si , desi nu este foarte bun, scopul sau este de a oferi o izolare a retelei prin incriptarea cadrelor cand se face transferul prin aer prin interfata 802.11.

*Livrarea MSDU:* Retelele nu sunt folositoare fara abilitatea de a transmite datele catre destinatar. Statiile ofera un serviciu de livrare MAC Service Data Unit ce este responsabil pentru a ajunge la punctul final.

Aceste retele opereaza in doua moduri : ad-hoc si infrastructura. Standardul IEEE defineste modul ad-hoc ca Independent Basic Service Set (IBSS), si modul infrastructura ca Basic Service Set (BSS).



In modul ad-hoc fiecare client comunica direct cu ceilalti clienti din raza de transmisie . Acest mod este proiect astfel incat clientii din aceiasi raza de transmisie pot comunica direct unul cu celalalt, iar daca un client din afara retele doreste sa comunice cu unul din afara, un membru trebuie sa actioneze ca poarta si sa performeze rutare.

In modul infrastructura fiecare client trimite datele de comunicat unui statii centrale sau punct de acces. Punctul de acces se comporta ca un bridge ethernet si inainteaza toate comunicatiile unei retele potrivite, fie retelei wireless fie retelei cablate.

Inaintea transmisiei datelor, intre clientii wireless si punctele de acces trebuie stabilita o relatie, o asociere. Numai dupa ce aceasta asociere este stabilita cele doua statii wireless pot schimba date. Procesul de asociere consta intr-un proces cu doi pasi incluzand 3 stari : neautentificat si neasociat, autentificat si neasociat, autentificat si

asociat. Pentru a tranzitiona intre cele 3 stari, partile ce doresc sa comunice schimba mesaje , denumite management frames.

Procesul de asociere al unui client wireless si un punct de acces. Toate punctele de acces transmit un management frame la un interval de timp. Pentru a se asocia cu un punct de acces si a se alatura BSS, un client cauta ce puncte de acces sunt in jurul sau. Clientul selecteaza BSS-ul dorit intr-o maniera independenta. Un client poate sa transmita un management frame de testare , pentru a gasi un punct de acces cu SSID dorit. Dupa ce punctul de acces a fost identificat, clientul si punctul de acces fac o autentificare mutuala prin schimbarea de management frames . dupa ce autentificare a fost efectuata cu succes , clientul se muta in a doua stare : autentificat si neasociat. Din acesta stare, pentru a ajunge in starea finala , cele doua parti trimit mesaje de autentificare catre punctul de acces, iar acesta raspunde triminand mesaje de asociere. Dupa acest ultim pas, clientul face parte din retea wireless si poate trimite date pe retea.

*Mecanisme de securitate ale 802.11:*

*Protocol Wired Equivalent Privacy.* A fost proiectat pentru a asigura confidentialitate pentru traficul retelelor ce folosesc protocolul wireless.

*Open System Authentication.* Este protocolul de autentificare standard al 802.11. Dupa cum e si numele sau, acest sistem autentifica orice utilizator ce doreste sa se autentifice.

*Shared Key Authentication.* Aceasta tehnica foloseste o provocare standard si un raspuns impreuna cu o cheie comuna secreta pentru a asigura autentificarea. Sistemul ce doreste autentificarea trimite un mesaj ce indica dorinta de a folosi autentificarea de tip 'cheie secreta' . celalalt sistem raspunde la acest mesaj, triminand o 128 de octeti pentru initiator. Acest text este generat de WEP si este mesajul secret. Cand initiatorul primeste acest mesaj, el copiaza acest mesaj, si scrie un nou mesaj constand in cheia secreta criptata cu ajutorul WEP si il trimite inapoi. Sistemul celalalt decripteaza acest mesaj primit si verifica daca este la fel cu cel trimis. Daca sunt egale, autentificare este facuta cu succes.

*Closed network acces control.* Cu acest mecanism, un manager de retea poate face o retea deschisa sau inchisa. In retea deschisa, oricine poate folosi retea, iar in retea inchisa numai acei clienti ce au numele retelei sau SSID o pot folosi.

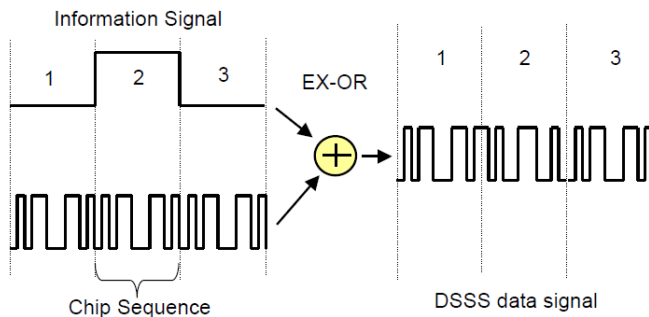
*Acces Control Lists.* Fiecare punct de acces poate limita accesul la retea folosind o lista cu adrese MAC. Daca MAC-ul unui client este in lista, atunci el poate folosi retea, daca nu, accesul este restrictionat.

## **DSSS. Direct Sequence Spread Spectrum**

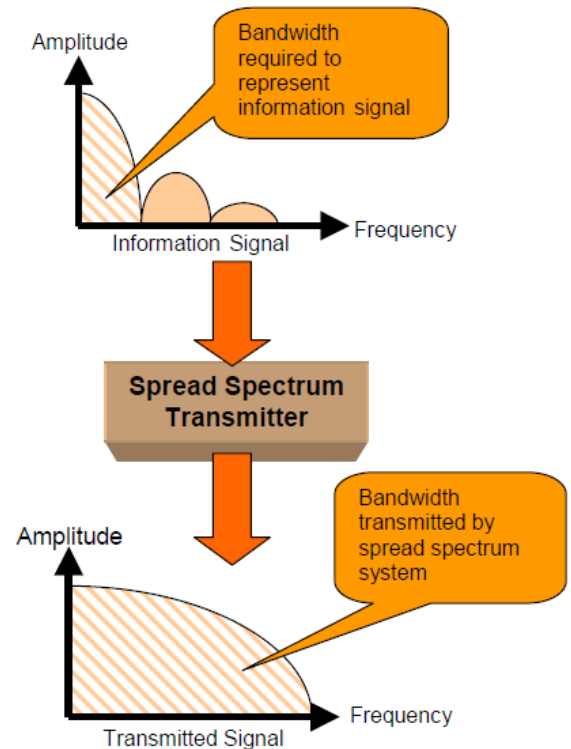
DSSS combina un semnal de date la statia emitatoare cu o secventa avand o rata de biti mare, cunoscuta sub numele de chipping code sau castig de procesare. Un castig de procesare mare , imbunatateste rezistenta semnalului la interferente. Castigul de

procesare minim pe care FCC il aproba este 10, iar multe produse comerciale sunt sub 20, IEEE 802.11 il are de 11. In comparatie cu tehnica de salt in frecventa, secventa directa poate atinge valori mai mari de 2Mbps.

DSSS-ul poate fi folosit pentru a mari securitatea transmisiei si de a preveni blocarea, problemele de cale multipla si probleme cand semnalul este atenuat. Poate fi folosite si ca o tehnica de acces multiplu cum ar fi CDMA, unde fiecare fiecare utilizator foloseste o secventa pseudo aleatoare diferita. [1]



Imagini preluata din : [\[sursa\]](#)



### Caracteristici DSSS

- Potential mare al ratelor de date din straturi fizice individuale
- Cel mai numar de celule radio separate geografic din cauza limitarii numarului de canale
- Este cea mai buna tehnica pentru aplicatii intense de banda.

Un transmitator DSSS actioneaza asupra unui sir de date avand o anumita rata de biti. Acest sir de date este de obicei convertit intr-un sir de simboluri unde fiecare simbol este reprezentat printr-un grup de 1,2 sau mai multi biti. Tehnici de modulatie similare ca cele folosite in modemuri voice-band data sunt folosite pentru a actiona asupra sirului de simboluri si genereaza semnalul pentru transmis. Transmitatorul DSSS moduleaza sau multiplica fiecare bit de date sau simbol cu un secventa aleatoare de pseudo semnale de zgomot, numita si secventa 'chip'. Aceasta multiplicare ofera fenomenul imprastierii de spectru.

Pentru a realiza imprastierea de spectru, modulatorul DSSS multiplica fiecare simbol cu secventa de chip. Secventa de chip este defapt o serie de valori de 1 si -1 .



considerand un semnal reprezentat de I,Q coordonate (1,1) coordonate polare sau fazoriale de 45 de grade. Acel simbol este multiplicat cu fiecare membru din secventa chop. In cazul unei valori de +1 , simbolul este neschimbat. In cazul unei valori de -1, simbolul este deplasat cu 180 in faza, sau in coordonate de (-1,-1).

Modulatia DSSS combina eficient un sir de biti de ce are o rata relativ mica cu o secventa chip de rata mare de n chip-uri pe interval de simbol. Parametrul n se numeste factor de imprastiere. In cazul semnalului modulat DSSS, rata de simboluri si latimea benzii pentru transmisie sunt inmultite cu un factor de n.

Receptorul DSSS foloseste aceiasi secventa chip ca si transmitatorul pentru a extrage datele din semnalul imprastiat. Semnalul primit este mai intai procesat printru filtru trece banda pentru a elimina zgomotul si interferentele ce nu sunt in domeniul de banda. Aceasta operatie izoleaza intreaga banda de interes. O functie decorelatoare elimina secventa chip si recupereaza semnalul original.

Bibliografie :

Ofdm: [http://en.wikipedia.org/wiki/Orthogonal\\_frequency-division\\_multiplexing](http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing)  
[http://www.encyclopediapro.com/mw/Orthogonal\\_Frequency\\_Division\\_Multiplexing](http://www.encyclopediapro.com/mw/Orthogonal_Frequency_Division_Multiplexing)

802.11

[http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11)  
[http://technet.microsoft.com/en-us/library/cc757419\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx)

Dsss:

[http://web.diegm.uniud.it/pierluca/public\\_html/teaching/reti\\_di\\_calcolatori/documentazione\\_tecnica/DSSS.pdf](http://web.diegm.uniud.it/pierluca/public_html/teaching/reti_di_calcolatori/documentazione_tecnica/DSSS.pdf)  
[http://en.wikipedia.org/wiki/Direct-sequence\\_spread\\_spectrum](http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum)

## WIRELESS LAN – ROAMING

### INTRODUCERE

Roamingul este, in contextul unei retele wireless 802.11, un proces in care un client care are stabilita o conexiune WI-FI se muta dintr-un acces point in alt acces point care au acelasi ESS (Extendet Service Set) fara a pierde conexiunea. Ca o baza pentru proiectarea unei retele wireless care asigura un roaming efectiv, este important sa intelegem in primul rand conceptele de baza ale roamingului. Pentru retelele wireless, roamingul are loc la cateva nivele. Dupa cum se poate vedea in figura 1<sup>i</sup>, roamingul poate avea loc atat la Layer 2 cat si la Layer 3. Cand un utilizator se muta in raza de acoperire, clientul radio trece automat de la un AP (acces point) la altul pentru a reusi sa mentina conexiunea. Acesta este un roaming de Layer 2, uneori denumit ca roamingul AP-ului. In plus, terminalul poate avea nevoie sa treaca de la o subretea la alta, acesta fiind Roamingul de Layer 3. Ideea generala a roamingului este aceea de a avea mobilitate, de a putea pastra o conexiune permanenta si in cazul in care, de exemplu , migrezi de dintr-un birou in altul si treci de la un AP la altul. Utilizatorii asteapta se asteapta sa aiba aceeasi acealeasi servicii transparente ca acelea pe care le au in cazul telefoanelor mobile cand se muta dintr-o celula in alta, dar in cazul 802.11 lucrurile nu stau chiar atat de usor<sup>ii</sup>.

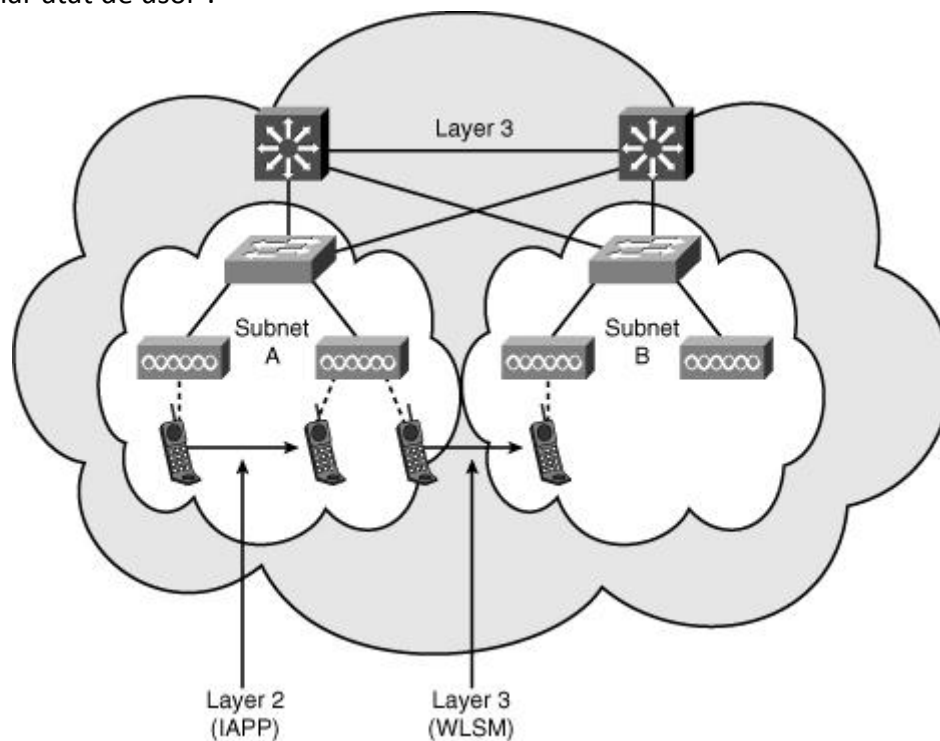


Figura 1

Exista foarte multa publicitate in ziua de azi despre roamingul in WI-FI, de exemplu un nou grup de la IEEE care se ocupa cu testerea WI-FI au descoperit ca este

posibil sa compari timpii de roaming fara o definire a roamingului. In timp ce multi producatori de switch-uri wireless folosesc un roaming de Layer 3, cativa producatori (cum ar fi Bluesocket si Vernier) rezolva aceasta problema prin pastrearea tuturor AP-urilor intr-o singura subretea, deci doamingul are loc la Layerul 2 iar dispozitivul cu care se migreaza pastreaza acealasi IP. Dar nici problema roamingului in aceeasi subretea nu este una deloc simpla.

Cand un client WLAN se iese din raza de actiune a AP-ului si intra in raza de actiune a altui AP din aceeasi subretea, este nevoie sa se gaseasca cel mai bun AP,sa se decida cand se face trecerea la acesta, sa se faca asocierea cu acesta si sa se faca orice autentificare este necesara, dupa cum sunt setate regulile de securitate. Scanarea si decizia fac parte din procesul de roaming care ii permit clientului de a gasi un nou AP pe canalul cel mai potrivit in timp ce utilizatorul este in miscare. Cand acest lucru se intampla clientul trebuie sa se asocieze cu noul AP, dupa care trebuie sa se reautentifice cu serverul principal. Aceste lucruri sunt transparente utilizatorului, dar intarzierea in realizarea acestor etape nu trebuie sa existe, asocierea si autentificarea realizandu-se in mai putin de o secunda. Urmatoarea parte a procesului este pentru restul retelei care trebuie sa ia cunostiinta despre faptul ca dispozitivul (clientul) a trecut intru-un alt AP. Aceasta comunicatie intre AP-uri nu a fost posibila in specificatiile genererale ale 802.11, dar un nou protocol 802.11f a fost publicat de catre IEEE, initial ca un standard pentru incercari si a ramas in aceasta stare de incercare timp de doi ani, dupa care a devenit un standard general pentru a facilita interoperabilitatea intre AP-uri de la diferiti producatori<sup>iii</sup>.

## **NIVELE DE ROAMING**

### **Roamingu Acces Pointurilor**

Prin colaborarea producatorilor de WLAN-uri, specificatiile IAPP (Inter-Access Point Protocol) ofera un protocol comun de roaming care mermit utilizatorului sa se migreze in interiorul unei cladiri si in acelasi timp sa pastreze o conexiune la retea prin intermediul MAP (Multivendor Access Point). Testele interoperabilitatii arata ca IAPP functioneaza cu oa mare varietate de AP-uri. WI-FI Alliance include interoperabilitatea roamingului ca un lucru necesar pentru emiterea unei certificari WI-FI.

Specificarile IAPP sunt create pe baza capabilitatii standardului IEEE 802.11, care foloseste intefretele sistemului de distributie al AP-ului pe care 802.11 il ofera. IAPP lucreaza opereaza intre AP-uri folosind UDP (User Data Diagram) si IP (Internet Protocol) ca o baza a comunicatiilor. IAPP defineste doua Protocele de baza: protocolul de anuntare (Announce Protocol) si protocolul de predare (Handover Protocol). Protocololul de anutare setat cu adresa clientului (standardul spune ca acesta trebuie sa fie un adresa de broadcast, dar unele implementari inca folosesc adresa de unicast a AP-ului anterior sau cea o adresa de multicast) si este folosit pentru a preveni updatarea tabelii cu adrese MAC de catre switchuri. Protocolul de predare este unul de notificare din noul AP catre adresa de multicast IAPP (Inter-Access Point Protocol), si contina adresa MAC a statiei cu care a tocmai a fost asociata. Toate AP-urile vor primi acest pachet, iar cel cu care a fost asociat statia va folosi secventa de numere inclusa pentru a determina ca avem informatie noua si va sterge vechile asocieri din tabla interna. IAPP

este folosit pentru schimbul de informatie dintre AP-uri. Formatul acestei informatii este specificat ca si „context” dar actualul continut nu este definit, deci nu este inca atat de folositor cat timp interoperabilitatea intre producatori este ceea ce ne preocupa.

Finalizarea si proliferarea amendamentelor IEEE 802.11r si 802.11k standardului 802.11 au un impact pozitiv asupra roamingului AP-urilor. 802.11r ofera un roaming lin intre AP-uri. Principala utilizare a 802.11r este pentru oferirea efectiva a roamingului pentru VoIP si mecanisme de securitate. 802.11r ofera functii pentru determinarea calitatii serviciului (QoS) si de realizarea de protocoale de securitate inainte de predare pentru evitarea intarzierii dupa preluare. 802.11k lucreaza in combinatie cu 802.11r prin oferirea de informatii pentru gasirea celui mai bun AP disponibil si pentru propunerea de preluare<sup>iv</sup>.

### **Roamingul De Subretea**

In timp ce un dispozitiv client migreaza dintr-o subretea in alta subretea, acesta ar putea avea nevoie sa obtina o adresa IP valida pentru noua subretea. Dispozitivul se poate folosi de catre DHCP pentru a obtine o adresa IP, dar aceasta nu e eficienta mereu cand este vorba de mobilitate. DHCP nu este proiectata sa reinvoiasca adresele cand sunt depasite limitele subretelei. In consecinta, ar putea fi necesar sa configuram un WLAN care sa opereze intr-o singura subretea.

Acest lucru ar putea sa functioneze in cazul unei retele private, dar problemele roamingului apar atunci cand dispozitivul trebuie sa migreze catre alta retea.

Unele companii, totusi, ar putea vrea sa implementeze mai multe subretele in cadrul unei aceluasi WLAN din anumite motive, cum ar fi un management mai usor, facilitarea serviciilor bazate pe locatii, scaderea imbrasierii pachetelor de broadcast in interiorul retelei. De exemplu, o companie doreste sa livreze o informatie specifica utilizatorilor pe baza locatie lor intr-o cladire anume. Prin proiectarea diferitelor subretele in interiorul aceluasi WLAN, locatia unui utilizator poate fi determinata si continutul sa fie livrat pe baza locatiei lui. Locatia unui utilizator in interiorul unui aeroport de exemplu, poate sa ii ofere o harta a terminalelor, sa ii indice informatii despre zboruri si unde se afla cafenelele.

Cu ajutorul mai multor subretele utilizatorii moboilii trebuie sa fie capabili sa migreze cu usurina dintr-o subretea in alta cand traverseaza o cladire. In timp ce utilizatorii migreaza prin subretele trebuie sa existe un mecanism la Layerul 3 care sa se asigure ca dispozitivul configurat cu o adresa IP specifica poate sa continue comunicarea cu aplicatiile.

### **ROAMINGUL ISP – wireless**

Cu hotspoturile WI-FI, exista un o migrare foarte limitata intre provideri de servicii de internet wireless. WI-FI Alliance a incercat sa dezvolte un standart acum cativa ani pentru a face usoara migrarea intre ISP-uri, dar au renuntat datorita incompatibilitatii semnificative intre controlere de acces diferite. In general, standardele pentru migrarea de la un ISP la altul sunt inexistente. Ca rezultat, trebuie negociati termenii de agreere intre ISP la crearea unei WI-FI hotspot de arie larga si

trebuie creat un sistem de control al accesului care este agreatii de catre tot IPS participantii.

## **ROAMINGUL TELEFONIEI IP WIRELESS**

O aplicatie in care roamingul are un impact foarte puternic este telefonie wireless. Daca se doreste folosirea unor telefoane IP wireless in cadrul unui WLAN, trebuie ca proiectantul sa se asigure ca WLAN-ul suporta roamingul efectiv. Utilizatorul care foloseste telefonul trebuie sa fie capabil sa se mute in cadrul cladirii in timp ce sistemul permite roamingul atat la Layerul 2 cat si la Layerul 3. Fara o trecere lina utilizatorulmca intamplina intreruperi de apeluri.

Roamingul la Layerul 2 are loc atunci cand un telefon IP wireless iese din raza de actiune a unui AP si se reasociaza cu un alt AP. Deoarece acest tip de migrare va aparea foarte frecvent datorita faptului ca utilizatorul se muta in interiorul cladiri, cum ar fi de exemplu un spital sau un depozit, cu siguranta ca roamingul la Layerul 2 este cel mai rapid (in mod ideal este mai mic de 100 de milisecunde). Timpul de tranzitie este acela intre cel dintre ultimul pachet RTS din AP curent si primul pachet RTS din noul AP cu care a fost asociat.

Un factor important in buna functionare a acestui tip de telefonie o reprezinta alegerea telefoanelor, fiind necesara folosirea unor telefoane care suporta o migrare rapida. De exemplu telefoanele IP wireless CISCO 7920 sunt proiectate special pentru a permite un roaming la Layerul 2 foarte rapid astfel incat sa nu se evite intreruperea apelurilor. Telefonul CISCO 7925, de exemplu, initiaza un proces de reasociere cu un AP diferit daca telefonul nu primeste 3 pachete consecutive de la AP curent si frame-ul de unicast catre AP nu este cunoscut.

Roamingul la Layerul 3 poate cauza intarzieri substantiale care pot duce la pierderea apelurilor de voce. Acest lucru depinde de de solutie wireless care este implementata, mai ales daca nu sunt implementate proprietatile roamingului de voce. Ca un rezultat, este bine de evitat telefoanele IP wireless care folosesc roamingul de Layer 3. In cazul de fata este de preferat, daca este posibil, sa se defineasca o singura subretea in intregul WLAN. Acest lucru va evita roamingul la Layerul 3. Daca nu este posibila folosirea unei singure subretele, este bine sa se minimizeze posibilitatea folosirii roamingului la Layer 3.

---

<sup>i</sup> [http://ptgmedia.pearsoncmg.com/images/chap11\\_9781587058899/elementLinks/dd831114.jpg](http://ptgmedia.pearsoncmg.com/images/chap11_9781587058899/elementLinks/dd831114.jpg)

<sup>ii</sup> Andrew Tanenbaum – Computer Networks

<sup>iii</sup> <http://features.techworld.com/mobile-wireless/435/wlan-roaming--the-basics/>

<sup>iv</sup> Jim Geier - Designing and Deploying 802.11n Wireless Networks