**Universitatea Politehnica Bucureşti**

Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei

Temă de casă

MAC (Media Access Control)

**Studenți: Matei Ioan-Tiberiu**

**Petre Mihai-Cătălin**

**Grupa: 443A**

**Prof. coordonator:**

**Conf. Dr. Ing. Ștefan Stăncescu**

2016

CUPRINS

[*1.* MAC - Petre Catalin 3](#_Toc441190584)

[1.1 Introducere 3](#_Toc441190585)

[1.2 Funcții efectuate în subnivelul MAC 4](#_Toc441190586)

[1.3 Mecanismul de adresare 6](#_Toc441190587)

[1.3.1 Tipuri de adrese MAC 6](#_Toc441190588)

[1.4 Mecanismul de control al accesării canalelor 7](#_Toc441190589)

[*2.* MAC - măsurători de performanță 8](#_Toc441190590)

[2.1 Performanțele protocoalelor MAC în cadrul standardului IEEE 802.11 8](#_Toc441190591)

Matei Tiberiu

[2.2 Performanțele protocoalelor MAC în comunicațiile prin satelit 10](#_Toc441190592)

Petre Catalin

[*3.* MAC - probleme apărute la conexiunea wireless Matei Tiberiu 13](#_Toc441190593)

[*4.* Bibliografie 16](#_Toc441190594)

# MAC

## Introducere

În modelul de referință IEEE 802 din domeniul rețelelor de calculatoare, **Controlul Accesului la Mediu** (MAC) este primul subnivel din nivelul *Legătură de date (Data Link)* al modelului OSI (Open Systems Interconnection). Subnivelul MAC oferă mecanisme de **adresare** și de **control** al accesului la canale făcând posibilă comunicarea între mai multe dispozitive conectate în aceeași rețea. Componenta hardware care implementează MAC-ul este numită *media access controller*.

Subnivelul MAC acționează ca o interfață între subnivelul LLC și nivelul Fizic (Physical) al rețelei. Nivelul MAC emulează un canal de conexiune logică full-duplex într-o rețea multi-point. Aces canal poate asigura serviciu de comunicații unicast, multicast sau broadcast.

Scopul acestei lucrări este înțelegerea modului de funcționare al nivelul MAC și prezentarea problemelor care apar în utilizarea acestuia.

Nivelul **Data Link** este al doilea nivel din modelul OSI care se ocupă cu transferul datelor între dispozitivele aflate în rețea. Nivelul Data Link este format din subnivelele LLC și MAC.

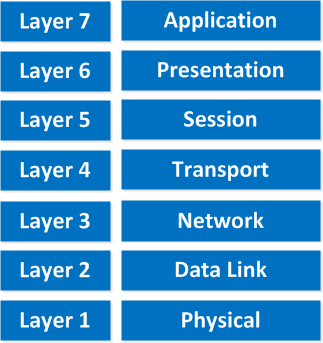


Figura 1 - Modelul OSI

*LLC (Logical Link Control*- controlul legăturii logice), administrează comunicația legăturii de date și definește folosirea punctelor interfeței logice, numite puncte de acces la servicii.

*MAC (Media Access Control*– controlul accesului la mediu), controlează accesul și delimitează cadrele, detectează erorile și recunoaște adresele, fiind inferior subnivelului LLC. Acesta comunică direct cu placa de rețea și este responsabil pentru transportul fără erori al datelor între două calculatoare din rețea (protocoalele 802.3, 802.4, 802.5 si 802.12).

Caracteristici ale MAC: Media Access Control este unul dintre cele două subnivele ale nivelului Legătură de Date (Data Link) ce se ocupă cu distribuirea conexiunii fizice în rețea. Fiecare sistem are propria adresă MAC unică. Ethernet este un exemplu de protocol ce lucrează la nivelul Media Access Control. MAC controlează modul în care mai multe echipamente folosesc același canal de comunicație.

## Funcții efectuate în subnivelul MAC

Subnivelul MAC în cazul familiei de protocoale 802.3 este responsabil pentru *verificarea canalului* pe care urmează să se transmită pachetul de date pentru a constata dacă acesta este "ocupat" (dacă există o transmisie în desfăşurare) şi *intrarea în transmisie* în caz contrar, pentru *constatarea apariţiei unei coliziuni* şi implementarea măsurilor ce trebuiesc luate într-o astfel de situaţie. Acest nivel se constituie într-o interfaţă între datele utilizatorului (nivelul aplicaţie) şi nivelul fizic în ambele sensuri. Astfel, datele de nivel aplicaţie sunt transmise conform regulilor impuse de nivelul MAC (partajarea accesului la mediu, mecanisme de retransmisie) sub forma impusă de nivelul fizic (nivele de tensiune, reguli de codare etc). În sens opus, datele recepţionate la nivelul fizic sunt procesate de către placa de reţea şi transmise nivelului aplicaţie.

Potrivit standardului IEEE 802, principalele funcții ale nivelului MAC sunt:

* Delimitarea și recunoașterea frame-urilor
* Adresarea stațiilor destinație (atât ca stații individuale cât și ca grupuri de stații)
* Transportul informației de adresare trimisă de stația sursă
* Transferul transparent de date al pachetelor LLC, sau al informației echivalente din subnivelul Ethernet
* Protecție împotriva erorilor, în general prin intermediul generării și verificării FCS (frame check sequence)
* Controlul accesului la mediul fizic de transmisiune [1]

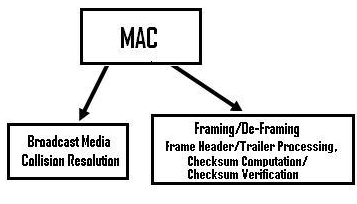


Fig. 2 - Funcții MAC

Subnivelul MAC interacționează cu nivelul Fizic (Physical) și este în principal responsabil pentru *framing* și *deframing* și pentru soluționarea coliziunilor.

**Framing / deframing**: Pe partea de transmitere, subnivelul MAC este responsabil pentru crearea frame-urilor din pachetele din nivelul de rețea, adăugând un frame header și frame trailer. Frame header-ul este alcătuit din adrese layer 2 (adrese MAC) și alte câteva câmpuri pentru control; frame trailer-ul este alcătuit din CRC/checksum. După crearea unui frame, nivelul MAC este responsabil pentru interacțiunea cu procesorul nivelului fizic pentru a transmite frame-ul.

Pe partea de recepție, subnivelul MAC primește frame-urile de la nivelul fizic și este responsabil pentru acceptarea fiecărui frame după examinarea fiecărui header în parte.

**Soluționarea coliziunilor**: În legăturile broadcast, unde mai multe noduri sunt asociate aceleiași legături, trebuie să existe un protocol de soluționare a coliziunilor pentru fiecare nod. Subnivelul MAC este responsabil pentru această sarcină, prin implementarea protocoalelor standard de soluționare CSMA/CD, CSMA. Pentru legăturile half-duplex, MAC-ul se asigură că un pachet este trimis pe o legătură doar în timpul acordat acesteia. [2]

## Mecanismul de adresare

Adresele de rețea locală folosite în rețelele IEEE 802 și FDDI sunt numite adrese MAC; aceste adrese se bazează pe schema de adresare folosită în implementările Ethernet. O adresă MAC este un număr serial unic. Odată ce o adresă MAC a fost asociată unei interfețe de rețea (de obicei la data fabricației), dispozitivul caruia acea interfață aparține este identificat în mod unic între toate celelate dispozitive de rețea existente în lume. Acest fapt garantează că fiecare dispozitiv dintr-o rețea va avea o adresă MAC diferită și face posibil ca pachetele de date să fie transmise către o destinație dintr-o subrețea, de exemplu host-urile interconectate printr-o combinație de switch-uri, hub-uri și bridge-uri. Astfel, de exemplu, când un pachet IP ajunge în rețeaua/subrețeaua destinație, adresa IP destinație este asociată de protocolul ARP (pentru IPv4) sau NDP (pentru IPv6) adresei MAC al hostului destinație.

Două exemple de rețele fizice care folosesc adrese MAC IEEE 802 pe 48 de biți sunt rețelele Ethernet și Wi-Fi.

Fiecare staţie conectată la un mediu de transmisie poate fi identificată cu ajutorul unei adrese unice pe 48 de biţi, cunoscută sub numele de adresă MAC şi care este atribuită plăcii de reţea a calculatorului de către fabricantul acesteia.

Folosirea adreselor MAC este unul dintre cele mai importante aspecte ale tehnologiei Ethernet LAN. Adresele MAC folosesc numere în sistem hexazecimal și asigură schimbul de informație în rețeaua locală prin identificarea sursei și a destinației unui mesaj.

Adresa MAC identifică în mod unic o placă de rețea.

### Tipuri de adrese MAC

O adresă MAC ***unicast*** este adresa unică folosită atunci când un pachet este trimis de la un singur dispozitiv către un singur dispozitiv destinație.

Un pachet ***broadcast*** conține adresa IP destinație care are toți biții de host egali cu valoarea 1. Acest lucru semnifică faptul că toate host-urile din rețeaua locală vor primi și procesa pachetul. Multe protocoale de rețea, precum DHCP și ARP, folosesc broadcast-uri.

Adresele ***multicast*** permit unui dispozitiv sursă să trimită un pachet către un grup de mai multe dispozitive. Dispozitivelor care aparțin unui grup multicast li se asociază o adresă IP de grup multicast. Deoarece adresele multicast reprezintă un grup de adrese, ele pot fi folosite doar ca și destinație a unui pachet; sursa va avea întotdeauna adresă unicast. Adresa MAC multicast este formată din secvența hexazecimală 01-00-5E și din cei mai mici 23 de biți din adresa IP multicast transformați în 6 caractere hexazecimale.

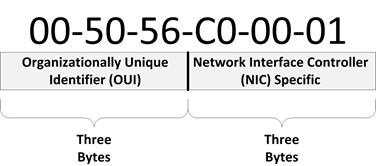


Figure 3 - Alcătuirea adresei MAC

## Mecanismul de control al accesării canalelor

Mecanismul de control al accesării canalului oferit de nivelul MAC mai este cunoscut sub numele de protocol de acces multiplu. Prin acesta este posibil ca anumite stații să partajeze mediul fizic la care sunt conectate. Câteva exemple de medii fizice partajate sunt rețelele de tip bus, ring, hub și wireless. Protocolul cu acces multiplu poate detecta sau evita coliziunile între pachetele de date dacă este folosită o metodă de acces al canalului, sau poate rezerva resurse pentru a stabili un canal logic o astfel de metodă este folosită.

Cel mai folosit protocol cu acces multiplu este CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Așa cum îi spune și numele, acest protocol este bazat pe sesizarea purtătoarei și detecția coliziunilor.

# MAC - măsurători de performanță

## Performanțele protocoalelor MAC în cadrul standardului IEEE 802.11

Ne propunem analiza performanței protocolului Medium Access Control (Media Access Control) în cadrul standardului IEEE 802.11. Pentru a proiecta o rețea eficientă în cadrul mediului wireless s-a ales protocolul CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) ca protocol standard pentru rețele wireless locale (LAN). Protocolul CSMA/CA este predispus coliziunilor, iar orice dispozitiv va fi nevoit să execute algoritmul BEB (Binary Exponential Backoff) de retransmitere pentru rezolvarea coliziunilor și pentru menținerea stabilității canalului CSMA/CA. De notat faptul că evaluarea performanțelor protocolului MAC în cadrul 802.11 prin cuprinderea detaliilor, sub condiții reale ale traficului, s-a dovedit dificilă. De aceea, s-a recurs la condiții simpliste cum ar fi surse Poisson ce au dimensiuni fixe ale frame-urilor de date și la simplificarea algoritmului de retransmitere folosit în standardul 802.11. Astfel, ne așteptăm la rezultate ale analizei de performanță oarecum limitate. În concordanță cu IEEE 802.11, echipamentele accesează canalul folosind o metodă de bază de acces (*basic access method*) sau o metodă opțională de tipul *four-way handshaking access method* cu un mesaj adițional de schimb de tipul *Request-To-Send/Clear-To-Send* (RTS/CTS) (Fig. 4).[4]

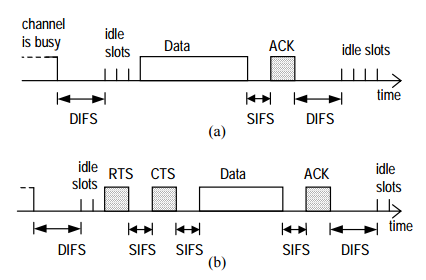
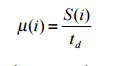


Fig. 4. Tipuri de accesare în cadrul 802.11 : (a) Accesare de tipul Basic accesss method. (b) Accesarea de tipul Four-way handshaking access method

*(*[*http://www.ee.cityu.edu.hk/~zukerman/IC\_80.pdf*](http://www.ee.cityu.edu.hk/~zukerman/IC_80.pdf)*)*

Pentru analiza de performanță, vom folosi saturația throughput-ului a IEEE 802.11 dezvoltată în cadrul unor funcții de coordonare distribuite. Saturația throughput-ului, *S(i)*, se regăsește în cadrul ratei de funcționare a protocolului, µ(i), ce se poate calcula cu ajutorul formulei:



, unde µ(i) este media ratei de funcționare, i este numărul stațiilor active, td este durata medie a transmisiunii de tip payload și S(i) este saturația throughput-ului. Vom considera un număr finit de echipamente, *k*, ce se află în convergența ariei de acoperire radio în cadrul rețelei de tipul IEEE 802.11. Fiecare echipament poate avea două stări: idle și activ. Echipamentul va rămâne în stare activă până la completarea transmisiunii, după care se va întoarce la starea idle. Va deveni activ dupa un timp distribuit exponențial (Fig. 5) [3]

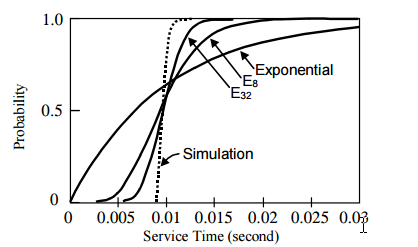


Fig. 5. Funcția de distribuție cumulativă pentru variabile distribuite și rata de funcționare pentru un protocol MAC al IEEE 802.11 pentru un număr de echipamente k=20 și un payload = 8184 biți

*(*[*http://www.ee.cityu.edu.hk/~zukerman/IC\_80.pdf*](http://www.ee.cityu.edu.hk/~zukerman/IC_80.pdf)*)*

În tabelul de mai jos vom specifica parametrii folosiți în analiza și simularea protocolului MAC în cadrul standardului 802.11:

|  |  |
| --- | --- |
| Descrierea parametrului | Valoare |
| Parametrii nivelului fizic | Standardul FHSS |
| Rata de bit a canalului | 1 Mb/s |
| Metode de acces | Basic, Four-way handshaking |
| Fereastră minimă de backoff | 8 |
| Fereastră maximă de backoff | 256 |
| Payload-ul maxim într-un frame de date | 8184 biți |
| Payload | 8184, 4348, 2430, 512 biți |

Conform rezultatelor, putem observa eficiența protocolului MAC în cadrul standardului IEEE 802.11 mai ales în cadrul metodei de acces four-way

handshaking. Chiar dacă această metodă de acces necesită operații de schimb ale frame-urilor suplimentare, beneficiile unei astfel de metode sunt net superioare.

## Performanțele protocoalelor MAC în comunicațiile prin satelit

Protocoalele de control al accesului la mediu permit stațiilor de comunicații din diverse locații să reglementeze transmiterea pachetelor și să administreze lățimea de bandă a rețelei cu scopul de a utiliza cât mai eficient resursele rețelei. În anii recenți, multe protocoale MAC au fost propuse sau deja dezvoltate pentru diferite medii de lucru cu diferite cerințe de utilizator. O explicație pentru faptul că există mai multe protocoale MAC este că protocoalele potrivite pentru o anumită aplicație nu sunt de obicei potrivite pentru alte aplicații. Cele mai utilizate protocoale de nivel înalt precum FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), TCP/IP (Transmission Control Protocol/Internet Protocol) folosesc unul sau mai multe protocoale MAC de nivel scăzut.

În continuare se va face o analiză a protocoalelor MAC potrivite pentru comunicațiile prin satelit.

Mediul de comunicații din spațiu posedă câteva constângeri majore ce elimină din start câteva protocoale MAC. În primul rând, întârzierea mare a propagării pe canale cu acces multiplu limitează aplicabilitatea unor clase de protocoale MAC, precum o clasă largă pentru rețele LAN și WAN. În al doilea rând, datorită diferenței de întarziere a propagării între legăturile terestre-sateliți, impactul asupra oricărei performanțe a unui protocol MAC calculate poate fi semnificativ. Nu în ultimul rând, schimbările fizice asupra controlerelor din spațiu sunt limitate, dacă nu chiar imposibile, iar acest lucru necesită un mecanism de control simplu pentru protocoalele luate în considerare.

În rețelele prin satelit, întârzierile de propagare sunt factori de limitare majori asupra protocoalelor MAC.

Protocoalele MAC au fost studiate și clasificate pentru diferite medii și aplicații. Pot fi clasificate în protocoale de latență mică (LAN și WAN) și protocoale de latență mare (comunicațiile prin satelit) și după funcționalitate, clasificare bazată pe natura statică sau dinamică a canalului, mecanismul de control centralizat sau distribuit sarcinile canalului, comportamentul adaptiv al algoritmului de control:

* Protocoale cu sarcină fixă
* Protocoale cu sarcină bazată pe cerere
* Protocoale cu acces aleator
* Protocoale hibride între cele cu acces aleator și cele restrictive
* Protocoale adaptive

La *protocoalele de acces multiplu cu sarcină fixă (FAMA)*, alocarea benzii canalului la o stație este o sarcină statică și este independentă de activitățile stației. Acest lucru se realizează împărțind banda în mai multe slot-uri, fiecare fiind asociat unei stații. Protocoalele FAMA se pot împărți în două categorii: Time-division multiple access(TDMA) sauFrequency-division multiple access(FDMA).

*Protocoalele cu sarcină bazată pe cerere*: în situațiile în care traficul este aleator și imprevizibil, protocoalele cu sarcină fixă sunt ineficiente. De aceea, este de dorit ca sarcinile să se aloce dinamic în funcție de cerințele de performanță. O suită de protocoale dinamice este Mini-Slotted Alternating Priorities (MSAP). Aceste protocoale sunt potrivite pentru un număr mic de stații.

*Protocoale cu acces aleator:* aceste protocoale sunt simplu de implementat și sunt adaptabile în funcție de cereri, dar în anumite situații pot fi risipitoare de capacitate datorită coliziunilor. Un exemplu de protocol cu acces aleator este Pure Aloha.

* Pure Aloha: la acest protocol, stațiile nu sunt sincronizate și transmit pachete doar atunci când sunt gata. În cazul în care unul sau mai multe pachete intră în coliziune, fiecare utilizator realizează producerea coliziunii și retransmite pachetul după o întârziere aleatoare.
* Selective-Reject Aloha
* Slotted Aloha
* Carrier Sense Multiple Access (CSMA)

*Protocoale restrictive:*

* Reservation Aloha
* PODA (Priority-Oriented Demand Assignemt)

*Protocoale hibride:*

* Round-Robin Reservation
* Aloha Reservation

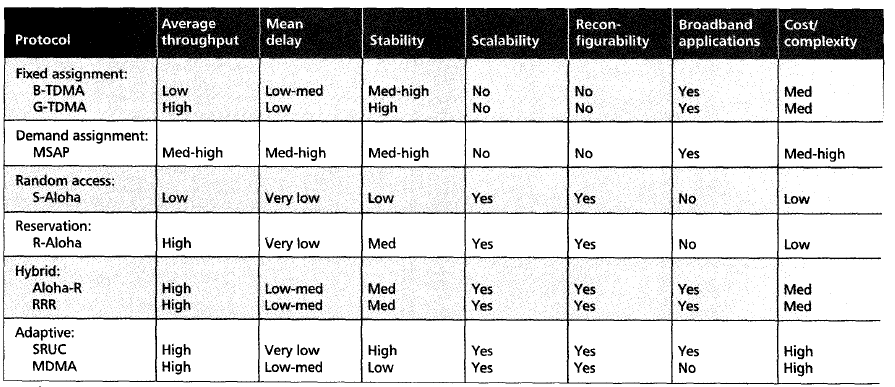


Fig. 6 - Comparație de performanțe

În ciuda faptului că nu există niciun protocol care să lucreze mai bine decât celelalte în anumite aplicații și scenarii, unele protocoale au anumite caracteristici ce le fac mai potrivite pentru comunicațiile prin satelit. În general, protocoalele hibride care folosesc atât protocoale cu acces aleator cât și protocoale restrictive au caracteristici mai bune ale transferului. De asemenea, se pot adapta la rețele dinamice prin scalabilitate și reconfigurabilitate. *[4]*

# MAC - probleme apărute la conexiunea wireless

Optiunea de filtrare a adreselor MAC ofera posibilitatea de a defini o lista a dispozitivelor ce pot avea acces in cadrul retelei Wi-Fi in mod exclusiv. In teorie, aceasta optiune ofera un control suplimentar asupra retelei stabilite. Din pacate, in practica, aceasta protectie este dificil si laborios de configurat si prezinta probleme cu securitatea in ideea ca este deetul de usor de spart.

Multi oameni considera filtrarea prin adrese MAC parte extra a securitatii retelei insa nu este chiar asa. In cele mai multe cazuri, encriptia WPA, sau mai ales encriptia WPA2 (ambele Wi-Fi Protected Access, in legatura directa cu standardul IEEE 802.11, sunt protocoale de securitate si programe de securitate dezvoltate de Wi-Fi Alliance pentru protectia retelelor wireless de calculatoare). *[5]*

*Cum funcționează filtrarea pe baza adreselor MAC?*

Fiecare dispozitiv vine cu o adresa unica media access control (pe scurt, adresa MAC) ce reuseste identificarea echipamentului in retea. De obicei, un router nu tine cont si permite conectarea oricarui dispozitiv (cat timp utilizatorul cunoaste asa-numitul 'passphrase'). Prin aplicarea filtrarii pe baza adreselor MAC, router-ul va defini o lista a adreselor MAC acceptate in retea si va permite conectarea echipamentelor daca, in urma controlului si comparatiei pe baza listei, aproparea se va face in mod specific. Cel mai probabil, router-ul va permite configurarea acestei liste a adreselor MAC chiar prin intermediul interfetei web de configurare. Prin folosirea acestei interfete putem filtra anumite device-uri pe baza MAC-ului aferent (Fig. 7). In cadrul retelei si in cadrul circulatiei pachetelor in cadrul retelei, adresa MAC este folosita pentru a se asigura faptul ca fiecare pachet ajunge la destinatia corecta. Orice utilizator poate monitoriza traficul in cadrul retelei Wi-Fi, poate examina pachetele pentru a afla o adresa MAC acceptata in cadrul listei de filtrare. Afland astfel adresa MAC se poate conecta in cadrul retelei Wi-Fi cu un alt dispozitiv, cu o adresa MAC modificata pentru a face parte din lista de filtrare. Putem spune ca acest lucru este imposibil din moment ce dispozitivul initial cu adresa MAC era deja conectat si memorat in lista. Din pacate, folosind anumite atacuri (precum "deauth" sau chiar "deassoc" - atacuri de tipuri 'denial of service') putem deconecta in mod fortat dispozitivul initial din cadrul retelei. Astfel, un nou utilizator se poate reconecta folosind adresa MAC aflata prin interogarea traficului in reteaua Wi-Fi. Aceasta metoda manuala poate dura mai putin de cateva zeci de secunde (folosind anumite unelte cum ar fi Kali Linux cu programul Wireshark asociat pentru aflarea adresei MAC si folosind comenzi precum *aireplay-ng* pentru deconectarea echipamentului initial), fara a lua in calcul si anumite scripturi shell sau metode sau programe automate (Fig. 8).

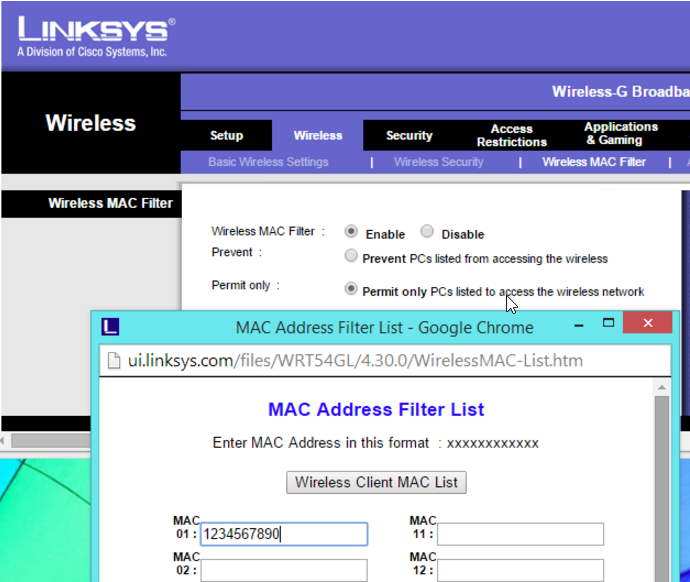


Fig. 7. Configurarea listei de filtrare a adreselor MAC in cadrul interfetei web

*(*[*http://www.howtogeek.com/wp-content/uploads/2014/12/ximg\_547f9334781f4.png.pagespeed.gp+jp+jw+pj+js+rj+rp+rw+ri+cp+md.ic.u-gbLemS3m.png*](http://www.howtogeek.com/wp-content/uploads/2014/12/ximg_547f9334781f4.png.pagespeed.gp+jp+jw+pj+js+rj+rp+rw+ri+cp+md.ic.u-gbLemS3m.png)*)*

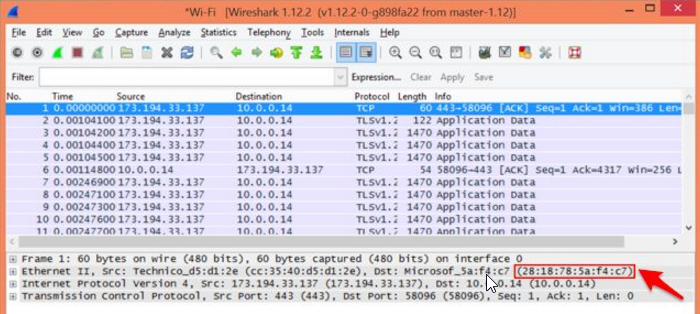


Fig. 8. Aflarea adresei MAC folosind programul Wireshark

*(*[*http://www.howtogeek.com/wp-content/uploads/2014/12/ximg\_547f98047b7d2.jpg.pagespeed.gp+jp+jw+pj+js+rj+rp+rw+ri+cp+md.ic.\_U7TmjKUjD.jpg*](http://www.howtogeek.com/wp-content/uploads/2014/12/ximg_547f98047b7d2.jpg.pagespeed.gp+jp+jw+pj+js+rj+rp+rw+ri+cp+md.ic._U7TmjKUjD.jpg)*)*

Folosirea acestei metode este foarte ineficienta, consuma foarte mult timp deorece utilizatorul va fi nevoit sa obtina adresa MAC a tuturor echipamentelor pe care doreste sa le conecteze si va fi nevoit sa introduca fiecare adresa in cadrul interfetei web de configurare a router-ului pentru a alcatui lista de filtrare. Timpul consumat creste astfel direct proportional cu numarul device-urilor pe care dorim sa le conectam.

Desi ne dorim configurarea unui router o singura data, va trebui sa luam in calcul faptul ca la introducerea unui device in retea va trebui accesarea interfetei web a router-ului pentru introducerea noii adrese MAC a echipamentului pe care dorim sa-l adaugam in lista de filtrare.

Astfel, putem considera faptul ca filtrarea pe baza adreselor MAC este mai mult o unealta de management sub forma unui feature specific administrarii de retea decat o optiune suplimentara de securitate. Singura capabilitate ce priveste intr-o oarecare masura securitatea filtrarii este posibilitatea de a alege device-urile ce pot fi online in reteaua creata. *[6]*

O alta problema o constituie identitatea device-ului prin adresa MAC ce poate fi foarte usor atribuita identitatii unei persoane. Aceasta adresa poate fi considerata un identificator unic ce poate conduce la persoana ce poseda dispozitivul respectiv. Chiar infrastructura unei retele memoreaza, de cele mai multe ori, date despre dispozitivele ce sunt conectate in cadrul retelei.

Log-urile router-elor wireless includ adresa MAC a device-urilor conectate (contin informatii de la asocieri, autentificari, deconectari) iar orice eveniment la nivel de retea are asociat o adresa MAC cu un timestamp (secventa de caractere sau de informatie codificata ce identifica momentul in care un eveniment a avut loc).

In cadrul conexiunii wireless, folosind anumite unelte software precum *aircrack-ng*,impreuna cu protocolul de retea ce poate efectua analiza *tshark* (versiunea programului Wireshark ce actioneaza in linia de comanda) si dupa aplicarea anumitor filtre putem dezvolta unelte ce pot asocia adresa MAC device-ului conectat in cadrul retelei wireless (Fig. 9). *[7]*

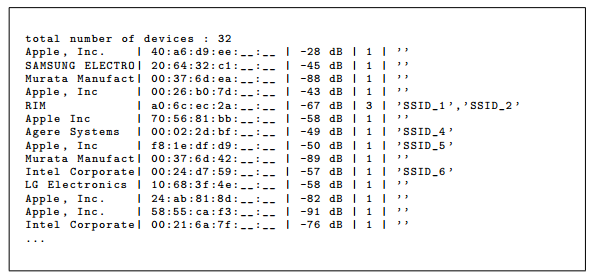


Fig. 9. Model ce afiseaza device-urile conectate si adresa MAC asociata

*(https://hal.archives-ouvertes.fr/file/index/docid/858324/filename/Wi-Fi\_Stalking.pdf)*

# Bibliografie

Andrew Tanenbaum – "Retele de calculatoare" editia IV, Ed. Byblos 2003

[1] "IEEE 802-2001 (R2007) IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture"

[2] http://computernetworkingsimplified.com/data-link-layer/components-data-link-layer-llc-mac/

[3] Performance Analysis of the IEEE 802.11 MAC Protocol Chuan Heng Foh and Moshe Zukerman ARC Special Research Center for Ultra–Broadband Information Networks EEE Department, The University of Melbourne Parkville, Vic. 3010, Australia

[4] Hassan Peyravi – Medium Access Control Protocols Performance in Satellite Communications – IEEE Communications Magazine, March 1999

[5]  "Understanding WEP Weaknesses". [Wiley Publishing](https://en.wikipedia.org/wiki/Wiley_Publishing). Retrieved 2010-01-10.

[6] http://www.howtogeek.com/204458/why-you-shouldn%E2%80%99t-use-mac-address-filtering-on-your-wi-fi-router/

[7] Mathieu Cunche. I know your MAC Address: Targeted tracking of individual using Wi-Fi. International Symposium on Research in Grey-Hat Hacking - GreHack, Nov 2013, Grenoble, France. 2013.