TWDM

Tehnologii Wireless şi Dispozitive Mobile

APLICAŢII PRACTICE

Bogdan IANCU
Adrian PECULEA
Cosmin ARDELEAN
Coordonatori:
Emil CEBUC
Vasile DĂDÂRLAT

U.T. PRESS

TWDM

Tehnologii Wireless şi Dispozitive Mobile

APLICAȚII PRACTICE

Bogdan IANCU
Adrian PECULEA
Cosmin ARDELEAN
Coordonatori:
Emil CEBUC
Vasile DĂDÂRLAT

Editura
U.T. PRESS

Prefaţă

Cartea “Tehnologii Wireless şi Dispozitive Mobile. Aplicații Practice” reprezintă o incursiune în dinamicul domeniu al tehnologiilor fără fir şi al comunicării în rețea a dispozitivelor mobile. Cele 12 capitole pun accentul asupra deprinderilor teoretice şi practice necesare proiectării, implementării şi depanării rețelelor 802.11, precum şi asupra dezvoltării aplicațiilor care permit comunicarea în rețea a dispozitivelor mobile.

Primele nouă capitole prezintă principalele aspecte teoretice referitoare la undele radio, metodele de modulare şi propagare a semnalelor RF, conceptele de bază referitoare la principalele categoriile de antene, modul de comparare al antenelor RF şi accesoriile utilizate în comunicația RF, topologiile rețelelor fără fir, standardul 802.11, fundamentele matematice necesare procesului de proiectare şi evaluare, principalele caracteristici ale dispozitivelor utilizate în comunicația 802.11, metodele de securizare a dispozitivelor si a comunicației 802.11, precum şi modalitățile de utilizare a două dintre cele mai moderne dispozitive pentru analiză spectrală RF. Aplicarea practică a conceptelor teoretice se realizează prin instalarea, configurarea şi testarea, în modul infrastructură, a principalelor dispozitive 802.11n (interfețe de rețea, puncte de acces şi rutere) utilizând sistemele de operare Windows şi Linux

Ultimele trei capitole abordează fundamentele teoretice referitoare la programarea aplicațiilor care comunică în rețea utilizând tehnologia Bluetooth, socketuri de rețea şi serviciile web (SOAP şi REST). Se prezintă procesul de dezvoltare al aplicațiilor pentru platformele Windows Phone 7 si Android, precum şi paşii necesari pentru crearea aplicațiilor de comunicare în rețea utilizând socketuri de rețea şi servicii web.

© TWDM 2012

Cuprins

I. Fundamente RF

II. Antene şi accesorii RF

III. Conectarea la rețea

IV. Analiza mediului RF: Fluke Etherscope Series II Network Assistant

V. Analiza mediului RF: Fluke Analyze-air

VI. Configurarea rețelelor wireless: configurări de bază

VII. Configurarea rețelelor wireless: configurări avansate

VIII. Configurarea rețelelor wireless: configurare VPN

IX. Securitatea în rețele wireless şi mobile

X. Programarea dispozitivelor mobile: comunicarea in retea

XI. Programarea dispozitivelor mobile: Windows Phone 7

XII. Programarea dispozitivelor mobile: Android

I. Fundamente RF

1. Obiective

Obiectivul acestui capitol este prezentarea fundamentelor referitoare la undele radio - semnale RF, a metodelor de modulare şi propagare a semnalelor RF şi descrierea unităților de măsură şi a fundamentelor matematice necesare pentru proiectarea şi evaluarea rețelelor 802.11.

2. Considerații teoretice

2.1. Semnale RF

În cadrul comunicațiilor de date în rețelele cablate, mediile de transmisie utilizate au fost, în ordinea apariției, cablurile coaxiale, cablurile torsadate şi fibra optică. Pentru transmiterea datelor (biți de informație) de-a lungul mediului de transmisie, a fost necesară o modalitate de reprezentare a cifrelor binare (0 şi 1). Pentru cablurile coaxiale şi torsadate s-a ales reprezentarea acestora utilizând niveluri de tensiune, iar în cazul fibrei optice s-a optat pentru transmiterea informației sub formă de unde de lumină.

IEEE 802.11, cunoscut ca şi Wireless Fidelity (Wi-Fi), este standardul pentru comunicații în rețelele locale de calculatoare (LAN) care utilizează frecvențele radio (radio frequencies – RF).

Un sistem wireless de bază este compus din următoarele elemente: transmițător, receptor, cablu de antenă, antene şi semnalul RF propagat (fig. 1).

Semnalul AC este transmis printr-un conductor şi emis cu ajutorul unei antene, sub formă de semnal wireless electromagnetic. Semnalele electromagnetice prezintă proprietatea de a putea circula prin diferite tipuri de medii sau prin vid.

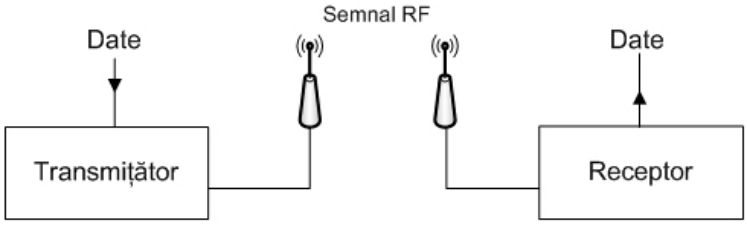


Figura 1. Comunicația wireless

Diferiți factori pot influența modul de propagare a semnalului RF prin diferite medii [1]: absorbția, reflexia, dispersia, refracția, difracția, atenuarea, amplificarea etc.

Absorbția unui semnal RF depinde mediul în care are loc propagarea, spre exemplu, un perete de beton va absoarbe mai mult din semnal decât un perete de gips-carton. Absorbția conduce la atenuarea semnalului inițial.

Un element de bază al comportamentului unui semnal RF este proprietatea de reflexie a undelor (fenomen de revenire parțială în mediul inițial după contactul cu alt mediu). Există două tipuri importante de reflexie: reflexia cerului (a ionosferei) – apare în cazul semnalelor de frecvențe de până la 1 GHz şi reflexia microundelor - apare în cazul semnalelor cu frecvențe cuprinse între 1 GHz şi 300 GHz. Reflexia este cauza majoră a performanțelor scăzute ale rețelelor fără fir.

Dispersia poate fi descrisă ca fiind o reflexie multiplă (în multiple direcții). Aceasta are loc când semnalul RF întâlnește o suprafață neuniformă.

Fenomenul de refracție se produce, în principal, datorită condițiilor atmosferice (fig. 5). Acest fenomen poate fi definit ca, curbarea unui semnal RF la trecerea printr-un mediu cu o densitate diferită, provocând modificarea direcției undei. Câteva cauze ale refracției sunt vaporii de apă, schimbările în temperatura aerului sau schimbările presiunii atmosferice. În mediul exterior, de cele mai multe ori semnalele RF sunt refractate către suprafața pământului. Însă există şi cazuri în care semnalul poate fi refractat în atmosferă. Fenomenul de refracție este foarte important în legăturile exterioare pe distanțe lungi.

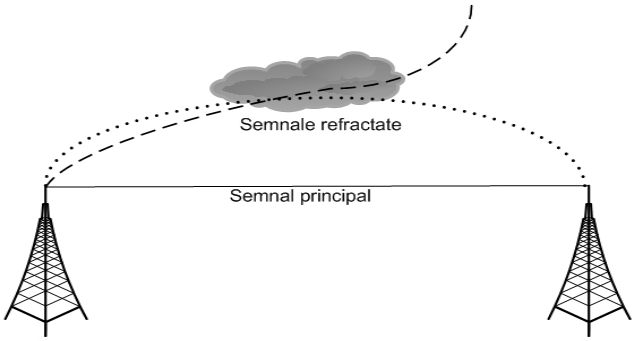


Figura 5. Fenomenul de refracție

Un alt element important, alături de refracție este fenomenul de difracție, care se definește ca mod de propagare a undelor în spatele unui obstacol, prin ocolirea marginilor lui şi prin abaterea aparentă de la traiectoria rectilinie. Zona din spatele obstacolului se numeşte *umbra RF (RF shadow)*, iar în funcție de dimensiunile şi caracteristicile obstacolului şi în funcție de caracteristicile semnalului RF, această zonă poate deveni o zonă fără acoperire sau, o zonă unde semnalul este recepționat deteriorat.

Material	**2,4 GHz**
Fundații	-15 dB
Beton, Cărămidă	-15 dB
Lift	-10 dB
Gips-carton	-3 dB
Uşă de lemn	-3 dB

Tabelul 1. Comparație material – atenuare [1]

Atenuarea este descrisă ca o descreştere a amplitudinii unui semnal. În cazul mediilor cablate (ex. cabluri torsadate), atenuarea apare datorită impedanței cablului sau datorită altor componente. În cazul mediilor fără fir, atenuarea apare datorită absorbției, distanței, etc. Tabelul 1 prezintă valorile de atenuare, în funcție de tipul de material prin care se propagă semnalele RF.

Un alt aspect important este reprezentat de atenuarea pe distanțe lungi (FSPL – free space path loss), datorită îngustării naturale a undelor când traversează distanțe mari şi se calculează astfel [1]:

$$FSLP = 32.4 + (20\log_{10}F) + (20\log_{10}D)$$

unde FSLP – măsurat în dB, D – distanța în km dintre antene şi F – frecvența în MHz. FSPL reprezintă o valoare ideală, deoarece este calculat considerând un spațiu fără obstacole.

O altă problemă este datorată fenomenului de multicale (multipath). Acesta este un fenomen de propagare care presupune apariția mai multor căi ale unui semnalului la receptor, simultan sau la intervale de câteva nanosecunde, datorită reflexiei, dispersiei sau difracției. De cele mai multe ori, acest fenomen conduce la alterarea semnalului primit (fig. 6). Un efect al fenomenului de multicale este amplificarea semnalului, cu condiția ca multiplele semnale să ajungă la receptor în acelaşi timp şi în fază.

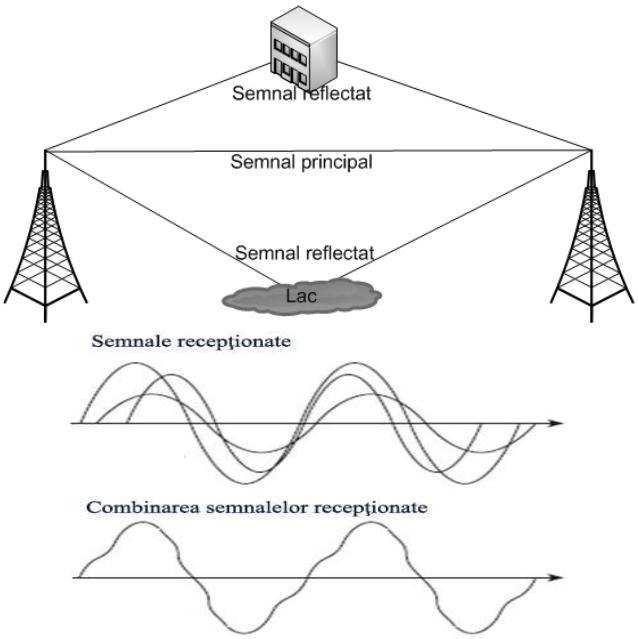


Figura 6. Fenomenul de multicale

Pentru transmisia şi recepția datelor, o tehnică de modulare a semnalelor este necesară a fi utilizată, prin alterări sau fluctuații ale semnalului RF. Trei componente ale undelor radio pot fi fluctuate sau modificate pentru a crea purtătoarea de semnal: amplitudinea, frecvența şi faza [1].

Pentru a transmite date de la un emițător la un receptor, semnalul RF trebuie manipulat astfel încât, stația receptoare să poate face diferența între 0 şi 1. Această metodă este cunoscută sub numele de *keying method.* Trei tehnici de modulare a semnalelor RF vor fi descrise: Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK), Phase Shift Keying (PSK).

Modularea în amplitudine (Amplitude Shift Keying), utilizează modificarea amplitudinii semnalului pentru reprezentarea valorilor binare (fig. 7). Această tehnică este dificil de utilizat deoarece, semnalele RF pot fi afectate de zgomot sau interferențe, ceea ce conduce la modificări ale amplitudinii semnalului inițial. Astfel, este posibil ca receptorul sa interpreteze în mod eronat semnalul primit.

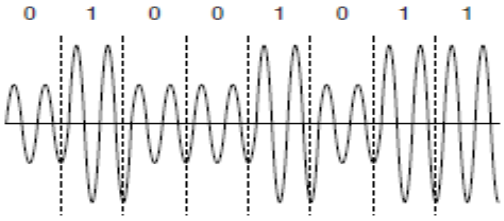


Figura 7. Tehnica ASK [1]

Modularea în frecvență (Frequency Shift Keying), variază frecvența semnalului pentru reprezentarea valorilor binare (fig. 8). Tehnica FSK a fost utilizată în primele standarde 802.11, fiind mai puțin practică, datorită resurselor de calcul necesare pentru procesarea unor semnale foarte rapide.

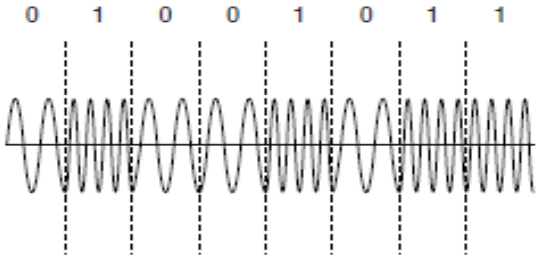
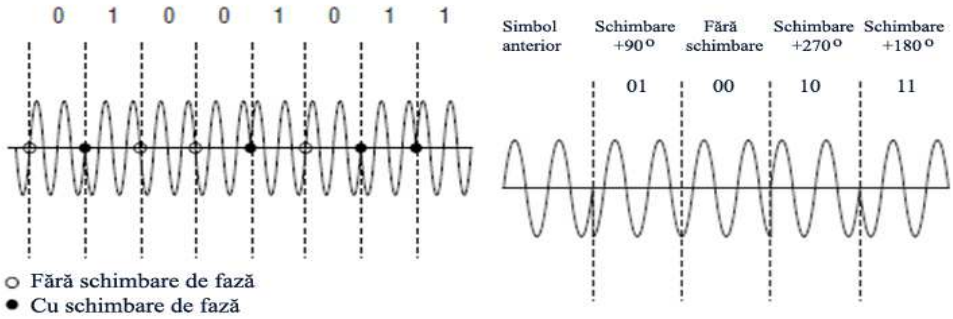


Figura 8. Tehnica FSK [1]

Modularea în fază (Phase Shift Keying), variază faza semnalului pentru reprezentarea valorilor binare (fig. 9). Tehnica PSK este larg utilizată în standarde 802.11.



a. b.

Figura 9. Tehnicile a.PSK şi b.MPSK [1]

Variante mai avansate ale acestei tehnici există, cum ar fi Multiple Phase Shift Keying (MPSK), care utilizează nu două, ci patru faze pentru reprezentarea binară, fiecare fază fiind capabilă să reprezinte două valori binare (00, 01, 10, or 11), reducându-se astfel timpul de transmisie.

2.2. Unităţi de măsură şi fundamente matematice

Tabelul 2 prezintă un sumar al unităţilor de măsură utilizate în designul unei reţele 802.11:

Unitate de măsura	**Unitate de comparaţie**
Watt (W)	Decibel(db)
Miliwatt(mW)	dbi
dBm	dBd

Tabelul 2. Unităţi de măsură

Marea majoritate a echipamentelor 802.11 transmit la puteri cuprinse între 1 şi 100 mW. Puţine echipamente punct la punct utilizează puteri mai mari de 250mW.

Decibelii (dB) nu sunt unități de măsură, ci unități de comparație, utilizate pentru a reprezenta diferența dintre două valori (ex. diferența de putere dintre două AP-uri). Un decibel (db) reprezintă a 10 parte dintr-un bel (B) şi se calculează conform formulei:

$$\text{decibels} = 10 \times \log_{10}\left({P_{out}}/{P_{in}} \right)$$

, unde P1 şi P2 sunt puterile comparate. Valorile sunt pozitive când P_{out} este mai mare decât P_{in} şi negative când P_{out} este mai mic decât P_{in}.

O altă unitate de măsură folosită este dBi (decibels isotropic) şi se defineşte ca fiind câştigul sau creşterea de putere a unei antene comparat cu un radiator izotropic (sursă teoretică de unde care prezintă aceleaşi proprietăți când sunt măsurate în toate direcțiile – radiază uniform în toate direcțiile). Această metodă este utilizată pentru compararea antenelor, deoarece antenele se măsoară în câştig, şi nu în putere.

O altă scală utilizată pentru a descrie câştigul antenelor este dBd (decibels dipole) sau câştigul în decibeli relativ la o antenă dipol. Pentru transforma dBd în dBi se poate utiliza formula:

$$\text{dBi} = \text{dBd} + 2.15$$

Pentru a compara un semnal cu 1 miliwatt de putere se utilizează dBm (decibeli relativ la 1 miliwatt). Diferența dintre dBm si celelalte unități prezentate este faptul că, dBm este o măsura de putere, nu de comparație. Un semnal de 1mW are un nivel de 0 dBm. Semnalele cu valori mai mici de 1mW vor avea valori dBm negative, iar pentru valori mai mari de 1mW vor avea valori dBm pozitive.

Reguli de conversie [1]

Regula 10-3

dB + 3 = mW × 2
dB – 3 = mW ÷ 2
dB + 10 = mW × 10
dB – 10 = mW ÷ 10

Regula dBm – mW

$$dBm = 10 \times \log_{10}(mW)$$
$$mW = 10^{(dBm \div 10)}$$

Legea pătratului invers

$$I=P/4\pi r^2$$

, unde I – puterea la distanța r, P – puterea maximă inițială, r distanța fața de sursă.

2.3. Componente RF

Figura 10 prezintă, în mod sumar, componentele RF utilizate în transmisia fără fir: transmițător-receptor, cablul de antenă, IR, EIRP, antena şi undele radio.

IR (Intentional Radiator) este definit ca un dispozitiv care generează şi emite în mod intenționat energie în frecvență prin radiație sau inducție. Acesta este alcătuit din toate componentele dintre transmițător şi antenă, excluzând antena, iar puterea IR este dată de suma componentelor sale. EIRP (Equivalent isotropically radiated power) este puterea emisă care ar fi necesară dacă semnalul ar fi radiat egal in toate directiile în loc sa fie focalizat (semnalul maxim care radiază din antenă).

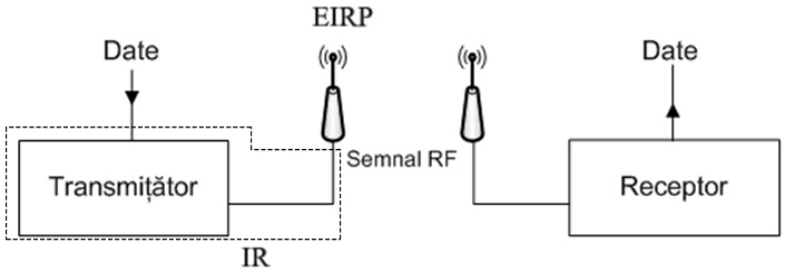


Figura 10. Componentele RF

Pentru a putea face calculele necesare pentru a determina gradul de succes al comunicației RF, parametrii RSSI (received signal strength indicator), SOM (system operating margin) şi marginea de atenuare (fade margine) trebuie luați în considerare.

RSSI este un parametru opțional 802.11 cu o valoare cuprinsă între 0 şi 255. El este conceput pentru a fi utilizat de către producătorii hardware ca o măsură relativă a puterii RF recepționată. RSSI este unul dintre indicatorii utilizați de către dispozitivele wireless pentru a determina dacă există un alt dispozitiv care transmite. Valoarea maximă este însa specifică fiecărui producător şi este denumită RSSI_max, iar datorită acestui fapt, compararea valorilor RSSI a doi sau mai mulți producători este dificilă.

SOM, cunoscut şi sub numele de link buget, este modul de calcul a cantității de semnal RF recepționat. Valoarea SOM a unui receptor depinde de senzitivitatea receptorului.

Marginea de atenuare poate fi privită ca o margine de zgomot. Problema este că semnalul primit fluctuează datorită multor influențe externe. Pentru a ține cont de această fluctuație, este o practică comună de a adăuga între 10 - 20 de dBs la valoarea senzitivității receptorului. Creşterea marginii de atenuare conduce la creşterea fiabilității legăturii.

3. Aplicații practice

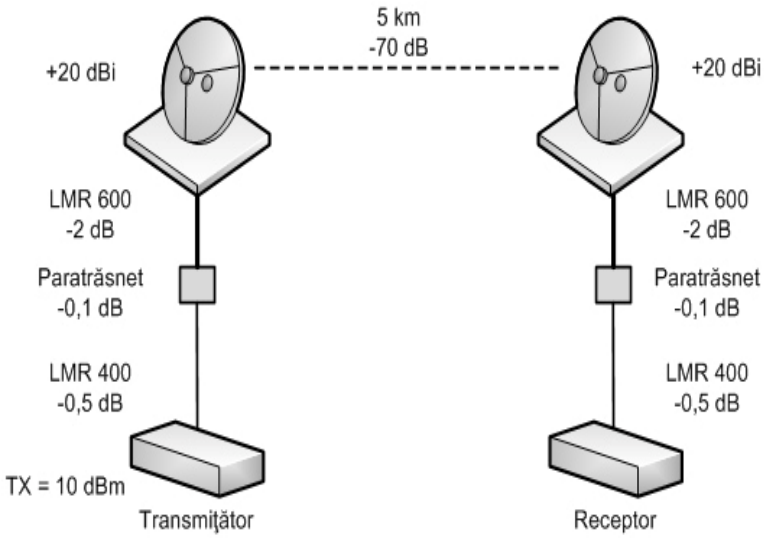
3.1. Se vor discuta caracteristicile semnalelor RF şi a principalelor componente de radio frecvență.

3.2. Se consideră un bridge wireless care generează un semnal de 100mW. Bridge-ul este conectat la antenă folosind un cablu coaxial care produce o pierdere de semnal de 3dB. Antena produce 10 dBi câştig de semnal. Calculați valorile IR şi EIRP.

3.3. Se consideră un dispozitiv wireless care generează un semnal de 40mW la o distanță de 1 metru. Calculați puterea semnalului la o distanță de 10 m, față de punctul de origine.

3.4. Se consideră un AP care generează un semnal de 20 dBm. Acesta transmite, utilizând o antenă dipol 5dBi, un semnal către un laptop aflat la o distanță de 50 m, care introduce un FSPL egal cu -73.98 dB. Senzitivitatea receptorului este de -71 dBm (la 54 Mbps). Calculați puterea semnalului recepționat şi valoarea parametrul SOM.

3.5. Se consideră o legătură punct la punct între două antene aflate la o distanță de 5 km una de cealaltă, conform desenului de mai jos.



Sensibilitatea receptorului se consideră a fi de – 15 dBm. Calculați valoarea parametrului SOM.

Bibliografie:

[1] D. Coleman, D. Westcott ,*CWNA Certified Wireless Network Administrator Study Guide*, Wiley Publishing, 2006.
[2] Cisco CCNA LAN Switching and Wireless Course.

II. Antene şi accesorii RF

1. Obiective

Obiectivul acestui capitol este prezentarea principalelor concepte de bază legate de categoriile principale de antene, modul de comparare al antenelor RF, accesoriile utilizate în comunicația RF şi înțelegerea conceptelor matematice de bază necesare instalării antenelor de comunicație.

2. Considerații teoretice

2.1. Concepte de bază

Pentru realizarea procesului de comunicare între două sau mai multe transceivere, semnalul de frecvență radio (RF) trebuie să fie emis din antena transmițătorului cu suficientă putere, astfel încât să fie recepționat şi înțeles de către receptor. Antenele reprezintă componenta critică a unui sistem RF, având scopul de a converti semnalele electrice în semnale RF şi invers. Modul de instalare al antenelor are o influență capitală în cadrul comunicării şi determină dacă aceasta s-a realizat sau nu cu succes [1].

Dimensiunea unei antene este invers proporțională cu frecvența suportată: cu cât frecvența este mai mare, antena va fi mai scurtă. În mod clasic, dimensiunea minimă a unei antene, la orice frecvență, este de ½ din lungimea de undă (ex. la frecvența de 2,45GHz, lungimea de undă λ = 12,3 cm).

Două tipuri de câştig de semnal sunt utilizate în comunicațiile RF. În cazul în care puterea este crescută utilizând anumite dispozitive electrice, cum ar fi un emițător sau un amplificator, creşterea se va numi câştig activ. În cazul în care puterea este crescută utilizând o metodă de focalizare sau de modelare a semnalului RF într-o anumită direcție, creşterea se va numi câştig pasiv. Câştigul pasiv este obținut prin focalizarea puterii existente, iar câştigul activ este obținut prin adăugare de putere.

În comerț există mai multe tipuri de antene concepute pentru diverse scopuri. Din păcate, nu este posibilă o comparare a antenelor într-un mod standard. Compararea a două sau mai multor antene, ar presupune realizarea unor numeroase măsurători în jurul antenei, utilizând un aparat de măsură RF (analizor spectral) şi apoi realizarea diferitelor calcule, ținând cont de factorii din mediul înconjurător, care ar putea denatura semnalul.

Producătorii pun însă, la dispoziția potențialilor cumpărători, şabloane de radiație, cunoscute sub numele de diagrame de azimut şi de elevație. Şabloanele de radiații sunt create în medii controlate, unde rezultatele nu pot fi denaturate de influențe externe şi reprezintă un model de semnal care este radiat de un anumit model de antenă. Graficul arată puterea semnalului în fiecare locație relativ la fiecare altă locație, şi nu în raport cu o distanță absolută de la antena sau cu un nivel absolut de putere.

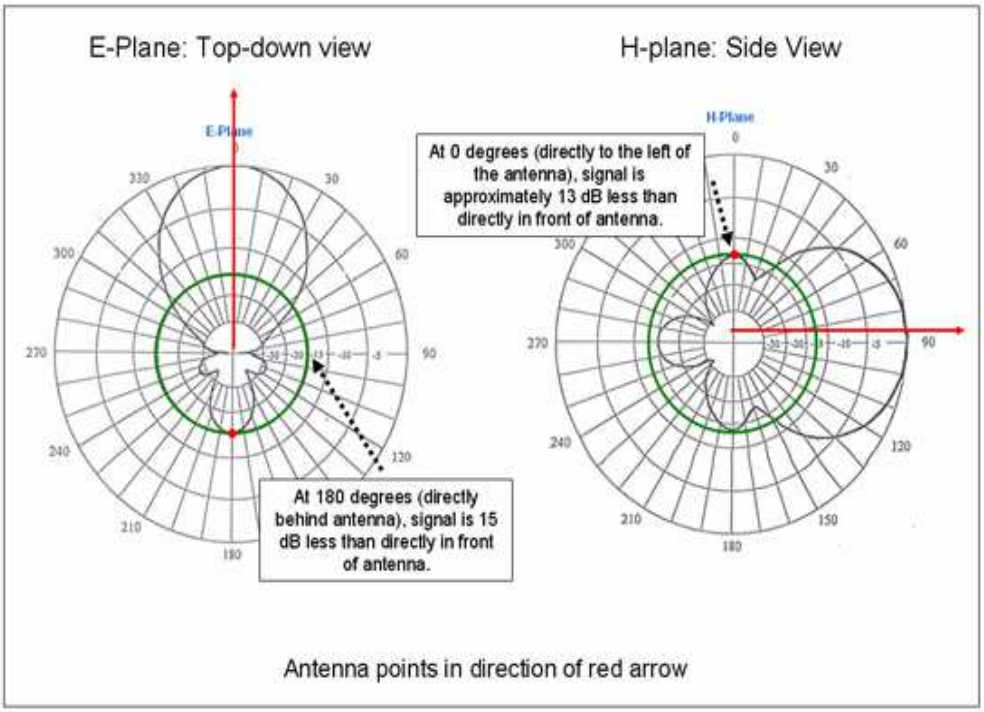


Fig. 1. Azimut şi elevație [2]

Figura 1 prezintă cele două diagrame: diagrama de azimut reprezintă o vedere top-down a şablonului de radiație, iar diagrama de elevație reprezintă

o vedere dintr-o parte a şablonului de radiaţie. O diagramă de azimut şi elevaţie vă va permite să alegeţi o antenă care maximizează aria de acoperire în punctele cheie şi care minimizează aria de acoperire în alte zone.

Modul de citire a acestor diagrame este următorul: în primul rând, se determină care a fost direcţia spre care a fost orientată antena în momentul testării. Antena este plasată în centrul diagramei şi, în mod uzual, este orientată către 0 grade pe diagrama de azimut (perfect dreaptă) şi la 90 de grade pe diagrama de elevaţie (către dreapta). Inelul exterior al graficului reprezintă nivelul semnalului maxim al antenei, fiind marcat cu 0 dB. Inelele interioare reprezintă puterea semnalului redus cu un număr de decibeli sub nivelul semnalului maxim al antenei.

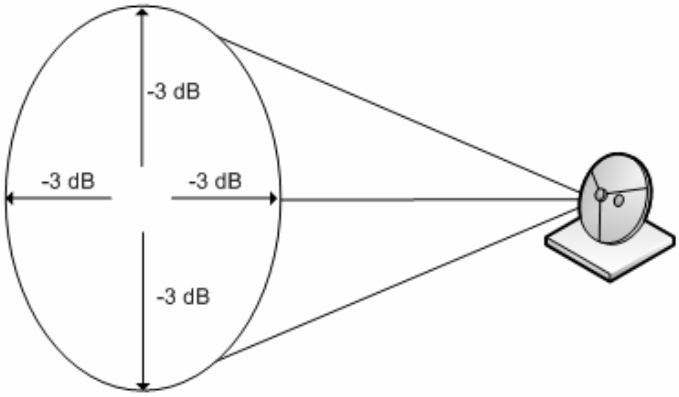


Fig. 2. Lăţimea fascicolului

Antenele RF sunt capabile să focalizeze puterea radiată, însă, datorită faptului că nu sunt reglabile, utilizatorul trebuie să decidă gradul de focalizare înainte de a achiziţiona antena [1]. Lăţimea fascicolului (fig. 2) este măsura a cât de largă sau de îngustă este focalizarea antenei, fiind măsurată atât pe orizontală, cât şi pe verticală. Este calculată din centrul antenei, sau punctul cu semnalul cel mai puternic, către fiecare punct de pe axa orizontală sau verticală, unde puterea semnalului descreşte la jumătate (-3 dB). Distanţa dintre cele două puncte de pe axa orizontală, unde puterea descreşte la jumătate este măsurată în grade şi reprezintă măsura orizontală a lăţimii fascicolului. Distanţa dintre cele două puncte de pe axa verticală, unde puterea descreşte la jumătate este măsurată în grade şi reprezintă

măsura verticală a lățimii fascicolului. Definiția lățimii fascicolului (cunoscută şi sub numele de lățimea fascicolului la jumătate de putere) este unghiul dat de şablonul antenei (fascicolul) unde puterea relativă este la sau de peste 50% din puterea maximă.

Este important de reținut că, deşi cea mai mare parte a semnalului RF generat este concentrat în zona lățimii fascicolului a antenei, există o cantitate semnificativă de semnal care radiază în afara acestei zone. Zonele exterioare sunt cunoscute sub numele de marginile antenei sau lobii posteriori.

Antenă	**Lățime fascicol Orizontal (în grade)**	**Lățime fascicol Vertical (în grade)**
Omni-direcțională	360	7 – 80
Yagi	30 – 78	14 - 64
Parabolică	4 – 25	4 - 21

Tabelul 1. Lățime fascicol – tip antenă [1]

În diagramele de azimut ale diferitelor antene se poate observa faptul ca aceste zone exterioare sunt semnificative. Tabelul 1 prezintă valorile lățimii fascicolului pentru diferite tipuri de antene.

2.2. Categorii de antene

Există trei mari categorii de antene: antene omni-direcționale – concepute pentru a furniza acoperire în toate direcțiile, antene semidirecționale – concepute pentru a furniza acoperire pe o anumită direcție, însă pe o arie mai mare de acoperire şi antene ultra-direcționale - concepute pentru a furniza acoperire pe o anumită direcție [1].

Un alt aspect important al antenelor este faptul că acestea nu amplifică semnalul doar la transmisie, ci şi la recepție.

Antene omni-direcționale

Aceste tipuri de antene radiază semnalul RF în toate direcțiile. O antenă omni-direcțională perfectă ar radia semnalul RF asemeni unui radiator

izotropic teoretic. Cel mai apropiat tip de antenă de radiatorul izotropic este antena dipol, care este antena implicită a majorității AP-urilor.

Este important de ştiu că o valoare dBi sau dBd mai mare, a unei antene, semnifică un semnal mai focalizat. La antenele omni-direcționale de mare câştig, focalizarea semnalului se realizează prin scăderea semnalului vertical şi prin creşterea puterii orizontale a semnalului. Figura 3 prezintă semnalul a trei tipuri de antene teoretice: cu cât câştigul este mai mare, cu atât semnalul este mai focalizat orizontal (alungit).Lățimea orizontală a fascicolului, pentru antenele omni-direcționale este întotdeauna de 360 de grade, iar cea verticală variază, în funcție antenă, între 7 şi 80 de grade.

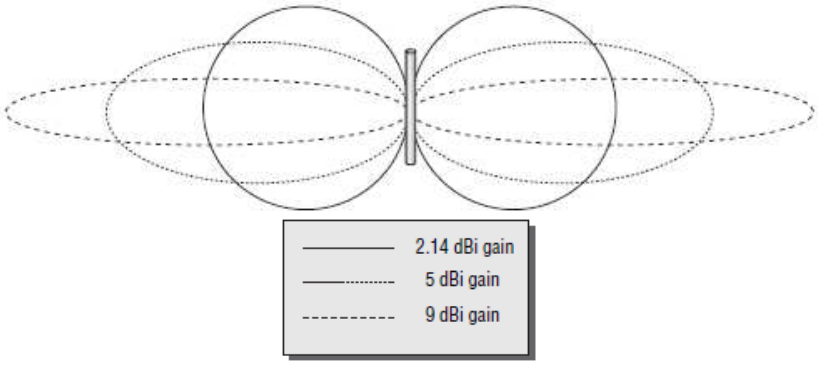


Figura 3. ablon de radiație verticală a antenelor omni-direcționale

Datorită acoperirii verticale foarte înguste, antenele omni-direcționale de mare câştig trebuie instalate doar în situațiile în care se doreşte o largă acoperire în planul orizontal. Spre exemplu, o astfel de antenă instalată la parterul unei clădiri, va asigura o acoperire optimă doar la acel nivel, iar etajele superioare vor recepționa un semnal scăzut. Pentru instalarea interioară se alege, în mod uzual, o antenă omni-direcțională de câştig scăzut, aproximativ 2.14 dBi. Antenele omni-direcționale de mare câştig se construiesc prin multiple antene dipol, suprapuse una peste alta, şi poartă numele de antene colineare.

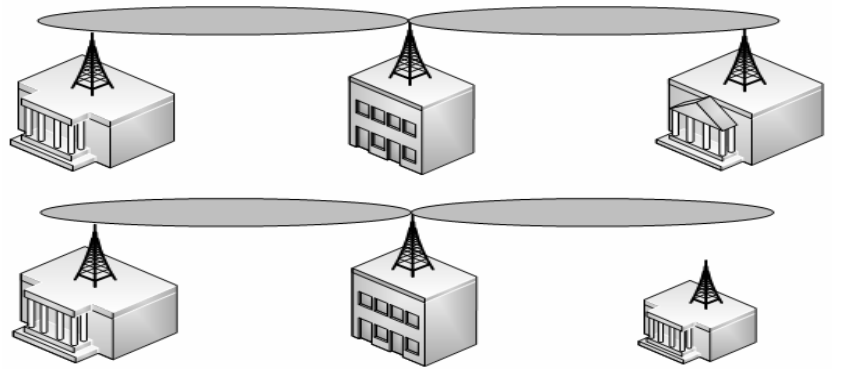


Figura 4. Cazuri de instalare în mediul exterior

Antenele omni-direcționale sunt utilizate în mod frecvent în medii punct la multipunct. Antena omni-direcțională va fi conectată la un dispozitiv (AP) plasat în centrul dispozitivelor client, pentru a oferi o acoperire cât mai largă. Antenele omni-direcționale de mare câştig pot fi utilizate şi în exterior pentru a conecta mai multe clădiri într-o configurație punct la multipunct. O astfel de antenă va fi poziționată pe o clădire centrală, iar pe celelalte clădiri se vor instala antene direcționale îndreptate către clădirea centrală (fig. 4).

Aceste configurații trebuie proiectate astfel încât câştigul să fie suficient de mare pentru a acoperi distanțele, şi suficient de redus pentru a nu omite din raza de acoperire clădirile.

Antene semi-direcționale

Antenele semi-direcționale sunt proiectate pentru a radia semnalul RF spre o anumită direcție. Sunt utilizate pentru distanțe mici şi medii, folosind ca bridge de rețea între clădirile unui campus sau aflate pe aceeaşi stradă. Trei tipuri de antene, care fac parte din această categorie, sunt: *patch, panel* şi *yagi* (Fig. 5)

a. b. c.

Figura 5. a. Antenă Patch; b. c. Antene Yagi [1]

Antenele patch şi panel sunt din categoria antenelor planare. Acestea furnizează acoperire direcțională în exterior pentru conexiuni punct la punct pe distanțe de până la 1,5 km, însă sunt utilizate în mod regulat în interior pentru conexiuni punct la multipunct. Antenele planare se utilizează frecvent, în interior, în biblioteci, depozite sau orice tip de clădire cu culoare lungi şi rafturi. Deoarece antenele planare au lățimea fascicolului orizontală de până la 180 de grade, doar o parte redusă de semnal va fi radiată în exteriorul clădirii. Utilizarea antenelor semi-direcționale în interiorul clădirilor conduce la reducerea reflexiilor, minimizând efectele negative ale fenomenului de multicale.

Din categoria antenelor yagi fac parte antenele clasice de televiziune de pe clădiri. Diferența față de o antenă de televiziune a unei antene yagi, este dată de faptul că au elementele de aceeaşi dimensiune, deoarece sunt construite pentru a putea recepționa doar o gamă îngustă de frecvențe. Antenele yagi sunt utilizate pentru comunicații punct la punct pe distanțe scurte sau medii, de până la 3 km. Un avantaj al antenelor semidirecționale este posibilitatea instalării pe clădiri, la înălțime, inclinate în jos către aria de acoperire.

Antene ultra-direcționale

Antenele ultra-direcționale sunt utilizate strict pentru comunicațiile punct la punct, de exemplu, pentru a furniza o legătură între două clădiri. Acestea pun la dispoziție cele mai înguste lățimi de fascicol dintre toate tipurile de antene. Există două tipuri de antene ultra-direcționale: antene cu

vas parabolice şi antene grid. Datorită câştigului foarte mare al acestora tipuri de antene, sunt ideale pentru comunicații pe distanțe mari, de până la 58 km. Însă datorită distanțelor lungi şi a lățimii de fascicol înguste, antenele ultra-direcționale sunt afectate de vânt, orice deviere a antenei conducând la o recepție defectuoasă sau la întreruperea comunicației. De aceea, indiferent de tipul de antenă instalat, calitatea montării va determina calitatea recepției.

Există şi alte tipuri de antene, pe lângă cele amintite anterior, cum ar fi: antenele phased array – capabile să transmită mai multe semnale simultan către mai mulți utilizatori (sunt specializate, costisitoare şi nu sunt create special pentru 802.11), sau antenele sectoriale (antene semi-direcționale, de câştig ridicat, utilizate frecvent în comunicațiile celulare).

2.3. Concepte pentru comunicația punct la punct

În general, comunicația punct-la-punct trebuie să aibă la dispoziție o linie de vedere (line of sight – LOS) neobstrucționată între două antene. În cazul comunicațiilor RF acest lucru nu este suficient, deoarece este necesar ca şi zona din jurul LOS să fie fără obstrucții. Aceasta zona din jurul LOS este cunoscută sub numele de zona Fresnel şi este adesea menționată ca linia de vedere RF (RF LOS). Zonele Fresnel sunt reprezentate în figura 6, sub formă elipsoidală, teoretic existând o infinitate de astfel de zone. Cele mai importante zone Fresnel sunt primele două, celelalte posibile având o influență neglijabilă.

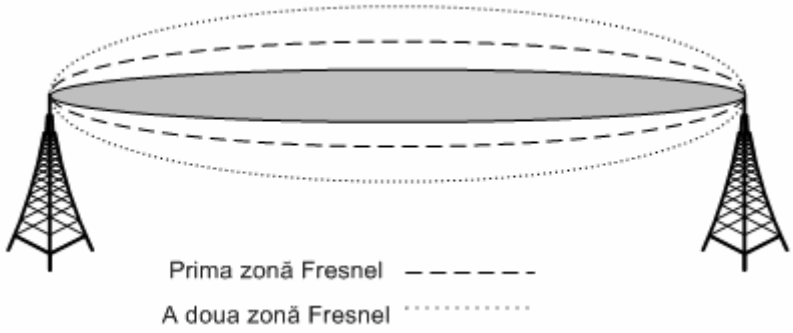


Figura 6. Zone Fresnel

Dacă prima zonă Fresnel este obstrucționată, chiar şi parțial, integritatea comunicației RF ar putea fi influențată negativ, şi ar putea conduce la scăderea puterii semnalului recepționat sau chiar la sistarea comunicației. Se recomandă ca un procent de sub 40 % din prima zonă Fresnel să poată fi afectat de obstacole, însă în practică este uzual un procent de 20 %.

Următoarele formule sunt utilizate pentru calcularea razelor zonelor Fresnel [1]:

(1) calculul razei primei zone Fresnel la mijlocul distanței:

$$r = 17.32 \times \sqrt{\frac{D}{4 \times F}}$$

, r – raza (m); D – distanța (km), F – frecvența (GHz)

(2) calculul razei unei zone Fresnel la orice distanță:

$$r = 17.32 \times \sqrt{\frac{N(d_1 \times d_2)}{(d_1 + d_2) \times F}}$$

r – raza (m); d_1 – distanța de la o antenă la obstacol (km),

d_2 – distanța de la obstacol la cealaltă antenă (km),

F – frecvența (GHz), N – zona Fresnel

Formula (1) este utilizată pentru a putea calcula la ce înălțime minimă față de sol trebuie instalate antenele, iar formula (2) este utilizată pentru a putea calcula zonele Fresnel relativ la un obstacol. Pentru a calcula zonele Fresnel trebuie ținut cont şi de curbura pământului, care acționează ca un obstacol, pe distanțe mari.

Parametrul *voltage standing wave ratio (VSWR)* este o măsură a modificărilor în impedanță pentru un semnal AC [1]. Aceste modificări există datorită nepotrivirii sau variației impedanței dintre dispozitivele unui sistem de comunicații RF. Când un transmițător generează un semnal radio AC, semnalul parcurge cablul către antenă. Însă, datorită nepotrivirii

impedanțelor dintre cablu şi antenă, o parte din energie este reflectată înapoi către transmițător. VSWR este o relație numerică între valoarea maximă măsurată a tensiunii, generată de transmițător, şi valoarea minimă măsurată a tensiunii, recepționată de antenă. VSWR este, prin urmare, un raport de nepotrivire de impedanță, cu 1:1 fiind optim (nu există nepotriviri de impedanță), însă valorile practice sunt cuprinse între 1.1:1 şi 1.5:1.

$$\text{VSWR} = \frac{V_{\max}}{V_{\min}}$$

Pentru a reduce VSWR este necesară potrivirea impedanțelor echipamentelor utilizate şi verificarea mufării şi instalării corecte a acestora. Tabelul 2 prezintă efectul VSWR pentru grade diferite de nepotrivire de impedanță.

VSWR	**Putere radiată**	**Pierdere de putere (%)**	**Pierdere de putere (dB)**
1:1	100%	0%	0 dB
1.5:1	96%	4%	~ 0 dB
2:1	89%	11%	< 1 dB
6:1	50%	50%	3 dB

Tabelul 2. Pierderi datorate VSWR [1]

2.4. Componente şi accesorii pentru antene

Cabluri RF

Următoarele aspecte trebuie luate în considerare în momentul alegerii cablurilor:

- impedanța cablului (VSWR)
- gama de frecvențe suportate
- pierderile introduse (dB)
- atenuare

Conectori RF

Următoarele aspecte trebuie luate în considerare în momentul alegerii conectorilor:

- impedanța conectorului (VSWR)
- gama de frecvențe suportate
- adaugă în medie pierderi de ½ dB

Distribuitoare (splitters) RF

Amplificatoare RF

Semnalul amplificat de către aceste tipuri de dispozitive (câştigul) este măsurat în decibeli. Tipurile de amplificatoarele pot fi cuprinse în trei mari categorii: low-noise (cu zgomot redus), high-power (de mare putere) şi altele tipuri de amplificatoare.

Amplificatoarele cu zgomot redus (LNA) sunt utilizate, în mod uzual, ca elemente de intrare ale circuitului de recepție RF. LNA-urile amplifică semnalul recepționat şi cresc puterea acestuia peste nivelul de zgomot produs de circuite ulterioare, oferind un câştig constant pe o anumită gamă de frecvențe. Datorită faptului că semnalele recepționate sunt de intensitate redusă şi includ zgomot considerabil, performanța LNA-ului afectează foarte mult sensibilitatea receptorului RF. Amplificatorul cu zgomot redus este capabil să reducă cea mai mare parte a zgomotului de intrare şi să amplifice semnalul, într-un anumit interval de frecvență, pentru a creşte SNR-ul sistemului de comunicație şi, de asemenea, pentru a îmbunătăți calitatea semnalului primit.

Amplificatoarele de mare putere (HPA) sunt utilizate pentru a amplifica semnalul RF la valoarea maximă posibilă înainte de a fi transmis (măsurată în dBm).

Următoarele aspecte trebuie luate în considerare în momentul alegerii amplificatoarelor:

- tipul amplificatorului
- amplificator unidirecțional sau bidirecțional

- instalare aproape de antenă, pentru a compensa pierderea pe cablu

Atenuatoare RF

Atenuatoare sunt folosite într-o mare varietate de aplicații pentru a produce o reducere a puterii. Atenuatoarele produc câştig subunitar şi sunt, în mod uzual, componente pasive. Atenuatoare sunt, de asemenea, utilizate pentru a echilibra liniile de transmisie, care altfel ar avea nivelurile de semnal inegale. Următoarele aspecte trebuie luate în considerare în momentul alegerii amplificatoarelor:

- cu pierdere fixă sau variabilă

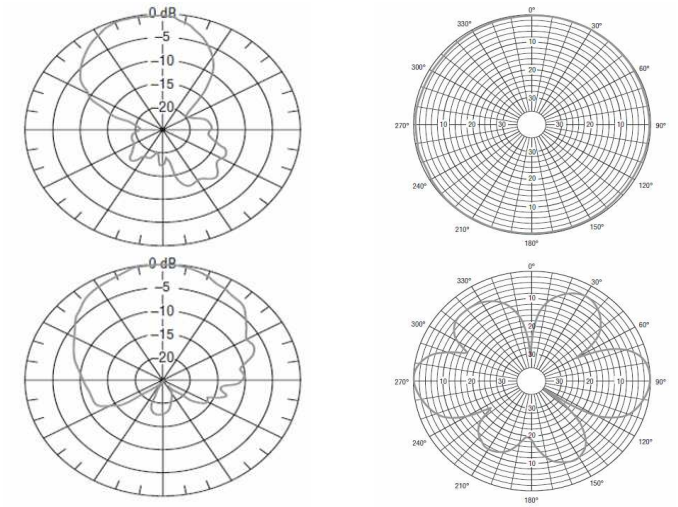
Paratrăsnet

- protejează împotriva descărcărilor electrice
- instalare aproape de antenă

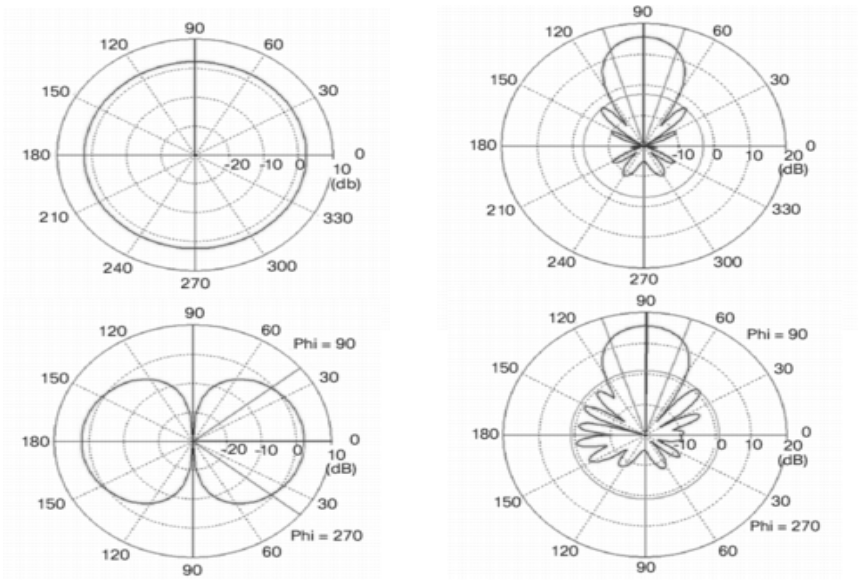
3. Aplicații practice

3.1. Se vor discuta principalele caracteristicile ale antenelor RF.

3.2. Interpretați diagramele de azimut şi elevație de mai jos. Ce tip de antenă prezintă acest tip de şablon radio?



a. b.



c. d.

3.3. Se consideră o legătură de comunicație punct la punct între două antene pe o distanță de 10 km, utilizând o frecvență de 5.7 GHz. La ce înălțime minimă față de sol trebuie instalate antenele? Care ar fi valoarea utilizată în practică?

3.4. Se consideră o legătură de comunicație punct la punct între două antene pe o distanță de 18 km, utilizând o frecvență de 2.4 GHz. La o distanță de 4 km se află un obstacol înalt de 200 m. La ce înălțime minimă față de sol trebuie instalate antenele? Care ar fi valoarea utilizată în practică? Care este influența curburii pământului?

Bibliografie:

[1] D. Coleman, D. Westcott ,*CWNA Certified Wireless Network Administrator Study Guide*, Wiley Publishing, 2006.
[2] Essential Wi-Fi, http://www.connect802.com/e_images/E/antenna_graphs.jpg
[3] Cisco CCNA LAN Switching and Wireless Course

III. Conectarea la rețea

1. Obiective

Obiectivul acestui capitol este prezentarea principalelor topologii fără fir şi 802.11, a dispozitivelor utilizate în comunicația wireless şi înțelegerea modalităților de configurare şi testare a conexiunilor wireless în sistemele de operare Windows XP, Vista şi Linux.

2. Considerații teoretice

2.1. Topologii wireless

Standardul IEEE 802.11 se referă la rețelele locale de comunicații (LAN) cu ajutorul frecvențelor radio (RF) [1]. Alături de rețelele 802.11, există alte tehnologii şi standarde de comunicații fără fir care operează pe zone de acoperire mai mici sau mai mari (Bluetooth sau ZigBee). Aceste tehnologii pot fi clasificate în patru clase de topologii majore [2]: Wireless Wide Area Network (WWAN), Wireless Metropolitan Area Network (WMAN), Wireless Personal Area Network (WPAN), Wireless Local Area Network(WLAN).

O rețea de arie largă (WAN) acoperă o vastă arie geografică. O rețea WAN ar putea parcurge o regiune sau țară, sau chiar întreaga lume. Cel mai concludent exemplu de WAN este Internetul. Multe WAN-uri publice şi private au la bază o infrastructură hardware care constă din linii E1 sau T1, fibra optica şi routere. Protocoale utilizate pentru comunicațiile cu fir WAN includ Frame Relay, ATM, MPLS, etc.

O rețea de arie largă fără fir (WWAN) acoperă, de asemenea, zone geografice întinse utilizând un mediu wireless. Rețelele WWAN utilizează, în general, tehnologiile rețelelor de telefonie celulară, cum ar fi GSM, GPRS, CDMA, TDMA, EDGE, MBWA, etc. Datele pot fi transportate la o varietate de dispozitive, cum ar fi telefoanele mobile, PDA-uri, însă ratele

de date şi lățimea de bandă ale acestor tehnologii sunt relativ mai lente, în comparație cu alte tehnologii fără fir, cum ar fi 802.11. Cu toate acestea, există noi tehnologiile celulare cu rate de transfer de date îmbunătățite. Este important de reținut însă, că infrastructura 802.11 nu poate fi utilizată ca un WWAN.

O rețea metropolitană fără fir (WMAN) oferă o acoperire unei zonei metropolitane, cum ar fi un oraş. De tehnologia comunicației fără fir WMAN este asociat un nou standard, definit de grupul 802.16 - acces fără fir în bandă largă, cunoscut sub numele de Worldwide Interoperability for Microwave Access (WiMAX). WiMAX este văzut ca un competitor al serviciilor în bandă largă DSL sau cablu.

O rețea personală fără fir (WPAN) este o rețea de calculatoare fără fir utilizată pentru comunicarea între diferite dispozitive aflate în imediata apropiere a unui utilizator. Diferite dispozitive, cum ar fi laptop-uri, PDA-uri şi telefoanele mobile pot comunica între ele folosind o varietate de tehnologii fără fir. Cele mai frecvente tehnologii fără fir în domeniul rețelelor WPAN sunt tehnologiile Bluetooth (802.15.1) şi infraroşu. Transmisia în infraroşu utilizează un mediu bazat pe unde optice, în timp ce Bluetooth este un mediu de frecvențe radio, care foloseşte tehnologia FHSS. ZigBee (802.15.1) este o altă tehnologie RF care are un potențial de cost scăzut de rețea fără fir între dispozitive, într-o arhitectură WPAN.

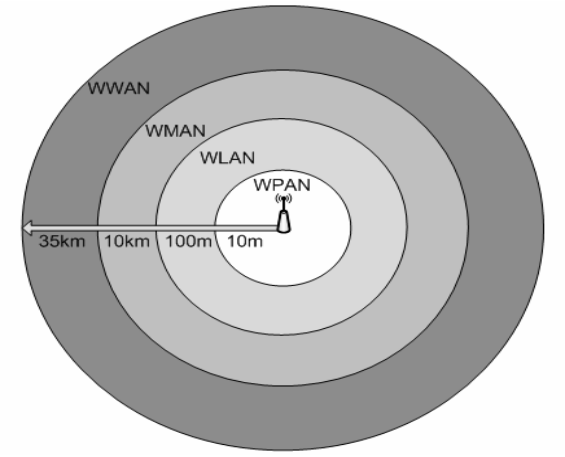


Figura 1. Topologii wireless

Standardul 802.11 este definit ca o rețea de arie locală fără fir (WLAN). Acest tip de rețea furnizează comunicații fără fir pentru clădiri private şi publice sau campusuri. 802.11 pune la dispoziție un mediu perfect adecvat pentru rețele locale, datorită gamei de viteze şi acoperirii definite de standard şi modificările sale. Utilizarea tipică a WLAN-urilor este adăugarea unor AP-uri la un backbone cablat, la care se pot conecta dispozitivele fără fir.

Figura 1 ilustrează principalele diferențe dintre aceste tehnologii, punând în evidență nivelul de acoperire şi tehnologiile utilizate:

2.1. Topologii 802.11

IEEE defineşte tehnologiile 802.11 referitoare la nivelul Fizic şi la subnivelul MAC al nivelului Legăturii de Date (reamintiți-vă modelul ISO / OSI). Trei specificații au fost definite pentru nivelul Fizic: a. Infraroşu; b. Frequency Hopping Spread Spectrum (FHSS); c. Direct sequence spread spectrum (DSSS). Plăcile 802.11 FHSS sunt adesea cunoscute sub numele de dispozitive de clauză 14, iar cele DSSS sub numele de dispozitive de clauză 15. 802.11 DSSS nu este compatibil cu 802.11 FHSS.

Principalele amendamente 802.11 sunt [2]: 802.11a – care operează în banda 5GHz *Unlicensed National Information Infrastructure (U-NII)*, 802.11b, 802.11g – care operează în banda 2.4GHz *Industrial, Scientific, and Medical (ISM)* şi recent 802.11n. Banda 2.4 GHz ISM este mult mai aglomerată decat cea de 5 GHz U-NII. Cuptoarele cu microunde, dispozitivele Bluetooth, telefoanele fără fir, şi numeroase alte dispozitive, toate operează în banda ISM 2.4 GHz şi reprezintă surse potențiale de interferență.

Standardele IEEE 802.11 au abordat întotdeauna problema lățimii de bandă. Obiectivul standardului 802.11n este de a creşte rata de transfer atât în banda de frecvență 2.4 GHz, cât şi în cea de 5 GHz. Obiectivul minim propus a fost de 100 Mbps, însă este posibilă o rată de transfer de până la 600 Mbps. 802.11n utilizează tehnologia Multiple-Input-Multiple-Output

(MIMO) la unison cu Orthogonal Frequency Division Multiplexing (OFDM). Tehnologia MIMO foloseşte antene multiple pentru recepție şi transmisie, valorificând efectul de multicale, spre deosebire de standardele precedente care încercau compensarea sau eliminarea acestuia. Principalele avantaje ale 802.11n sunt reprezentate de îmbunătățirea ratei de transfer şi a ariei de acoperire.

Tabelul 1 sumarizează caracteristicile amendamentelor 802.11 a, b, g:

	802.11 a	**802.11 b**	**802.11 g**
Frecvența	5 GHz U-NII	2.4 GHz ISM	2.4 GHz ISM
Tehnologie Spreed Spectrum	*Extended Rate Physical OFDM*	DSSS	*Extended Rate Physical OFDM* *DSSS*
Rate de Transfer	6,12,24 Mbps 9,18,36,48,54 Mbps	1,2,5.5,11 Mbps	1,2,5.5,11 Mbps 6,12,24 Mbps 9,18,36,48,54 Mbps 22,33 Mbps
Compatibilitate	-	802.11 DSSS	802.11b 802.11 DSSS
Standardizat	1999	1999	2003

Tabelul 1. Comparație 802.11 a, b, g [2]

În IEEE 802. 11 sunt definite două moduri de operare: mod infrastructură şi mod ad-hoc [3].

În *modul Infrastructură* (fig. 2), rețeaua fără fir este formată din cel puțin un punct de acces (AP) conectat la infrastructura rețelei cablate şi un set de stații wireless. Un punct de acces controlează modul de criptare în rețea şi poate înainta sau ruta traficul wireless către o rețea cablată sau în Internet. Această configurație este denumită Basic Service Set (BSS). Punctele de acces care acționează ca routere pot, de asemenea, atribui adrese IP către stații utilizând serviciul DHCP. Zona de acoperire fizică oferită de un punct de acces într-un BSS este cunoscută sub numele de Basic Service

Area (BSA). Mărimea şi forma unui BSA depind de multe variabile, inclusiv puterea de transmisie a AP-ului, câştigul antenei şi de împrejurimile fizice.

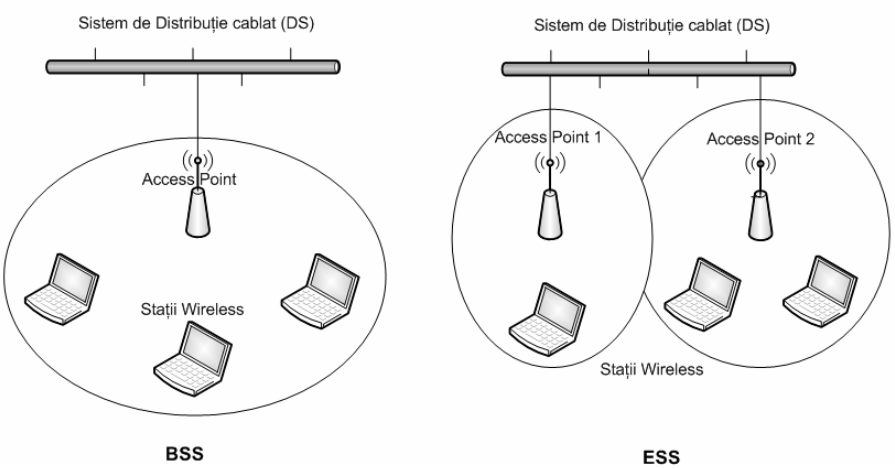


Figura 2. Mod Infrastructură

Un Extended Service Set (ESS) este alcătuit din două sau mai multe BSS-uri care formează o singură subrețea. Traficul este înaintat de la un BSS la altul, pentru a facilita circulația stațiilor wireless între BSS-uri. Aproape întotdeauna, sistemul de distribuție (DS) care conectează aceste rețele este un LAN Ethernet. Există însă şi sisteme de distribuție fără fir (WDS) care conecteză AP-urile. Deoarece marea majoritate a rețelelor fără fir necesită conectarea la rețeaua cablată (la DS), pentru a avea acces la serviciile oferite (file servers, imprimante, legătură la Internet), acestea vor utiliza o topologie de tip infrastructură.

În majoritatea ESS-urilor, AP-urile au acelaşi nume de rețea – *Service Set Identifier (SSID)* sau *Extended Service Set Identifier (ESSID)*. Există posibilitatea ca AP-urile dintr-un ESS să aibă nume de rețea diferite, şi totuşi sa aparțină de acelaşi ESS.

Modul *Ad-Hoc* (fig. 3) este un set de stații wireless 802.11 care comunică direct între ele fără a utiliza un punct de acces sau orice conexiune la o rețea cu fir. Această topologie simplă este utilă în scopul de a stabili rapid şi uşor o rețea fără fir oriunde nu există o infrastructură wireless, cum

ar fi o cameră de hotel, aeroport, etc. Modul Ad-Hoc este, de asemenea, numit peer-to-peer sau *Independent Basic Service Set (IBSS).*

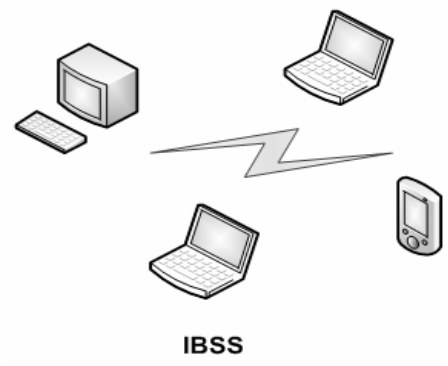


Figura 3. Mod Ad-Hoc

Pe lângă topologiile standard, descrise mai sus, există şi topologii nestandardizate, cum ar fi topologiile bridge sau mesh.

2.2. Dispozitive wireless

O *stație client* este definită ca un card radio, care nu este folosit într-un AP. Stațiile client pot fi utilizate în laptop-uri, PDA-uri, telefoane celulare sau alte dispozitive mobile.

Un *Access Point (AP)* sau Wireless Access Point (WPA) este un dispozitiv de tip half-duplex care permite dispozitivelor de comunicare fără fir conectarea la o rețea wireless. Într-o rețea cablată, echivalentul acestui dispozitiv îl reprezintă hub-ul.

Un access point poate fi privit ca un hub wireless, însă cu câteva îmbunătățiri, prezentând şi capabilități de switch. Principala funcție a unui AP este funcția de bridging, direcționând traficul, fie la backbone-ul rețelei, fie înapoi în mediul fără fir. O stație client, care are o conexiune de nivel 2 cu un AP, se defineşte ca fiind asociată cu acel AP.

Principalele adaptoare wireless, utilizate de către dispozitivele client sunt: adaptoarele PCMCIA, adaptoarele PCI, adaptoarele USB.

Un *adaptor PCMCIA* (*Personal Computer Memory Card International Association*) cunoscut, de asemenea, ca PC Card, poate fi folosit în orice ce tip de laptop sau dispozitiv handheld. Standardul actual care înlocuieşte PC card este ExpressCard. În cazul PDA-urilor, două formate de card radio, adesea folosite, sunt *Secure Digital* (SD) şi Compact Flash (CF). Aceste carduri au nevoie, de obicei, de un nivel foarte scăzut de energie.

Figura 4. Adaptoare Linksys Wireless-N

Pentru dispozitivele desktop, *adaptoarele radio PCI* (Peripheral Component Interconnect) sunt cele mai frecvent utilizate. Acestea au integrate cardurile radio şi au o mufă pentru ataşarea unei antene externe. Datorită faptului că marea majoritate a computerelor au porturi USB, *adaptorul radio USB 802.11* a devenit o alegere foarte populară. Tehnologia USB oferă simplitate în configurare, şi nu necesită o sursă externă de energie. Avantajul acestor tipuri de adaptoarele este proprietatea de a fi “hot-swappable” – pot fi conectate şi deconectate fără a necesita repornirea sistemului. Dezavantajul este dat de vitezele de transmisie mai mici.

Trebuie menționat faptul că, cardurile radio 802.11 folosite ca şi clienți, se utilizează şi în alte tipuri de dispozitive mobile, console de jocuri, telefonie VoIP wireless, senzori, etc.

2.3. Configurarea dispozitivelor 802.11 în sistemele de operare Windows/Linux

În cadrul sistemelor de operare Windows, instalarea unui dispozitiv de comunicare fără fir se efectuează în mod similar cu instalarea unui dispozitiv de comunicație cu fir. Instalarea şi configurarea stivei de protocoale TCP/IP, cât si principalele comenzi pentru testarea conectivității

unei rețele de calculatoare, sunt considerate cunoscute din cadrul laboratorului “Rețele locale de calculatoare” [4].

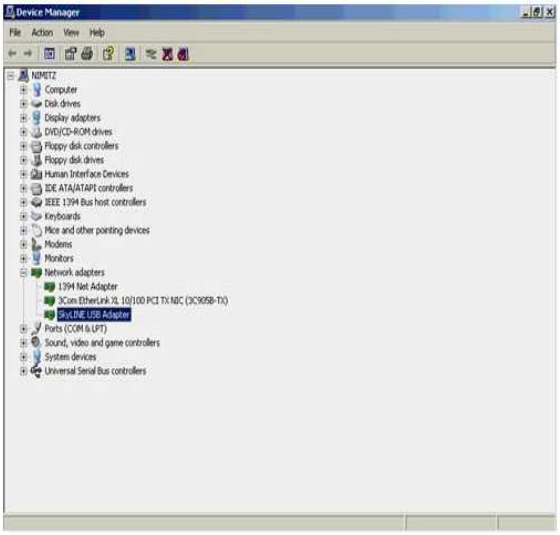
Windows XP

Pentru instalarea adaptoarele wireless se vor utiliza CD-ROM-urile de instalare (Setup Wizzard) sau, se vor descărca de pe site-ul producătorului driver-ele aferente.

Verificarea adaptoarelor instalate se realizează urmărind următorii paşi:

- click *Start* menu, right-click *My Computer*, selectați opțiunea *Manage* şi *Device Manager*
- click simbolul (+) de la linia *Network adapters*

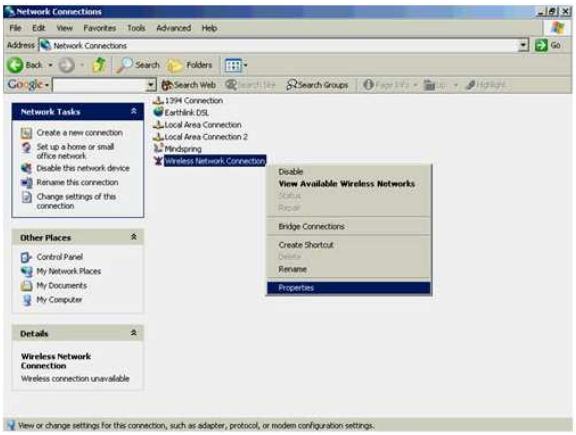
- adaptoarele wireless instalate trebuie să apară în această listă



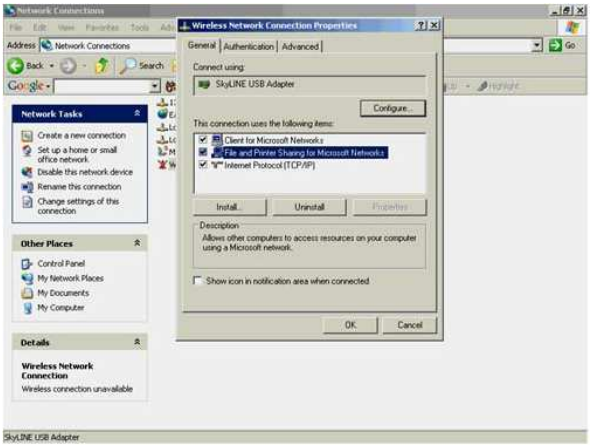
Configurarea adaptoarelor instalate se realizează urmărind următorii paşi:

- click *Start* menu, right-click *My Network Places* şi selectaţi opţiunea *Properties*

- right-click pe numele adaptorului de reţea wireless şi selectaţi opţiunea *Properties*



- verificați ca opțiunile *File and Printer Sharing for Microsoft Networks* şi *Internet Protocol (TCP/IP)* să fie selectate



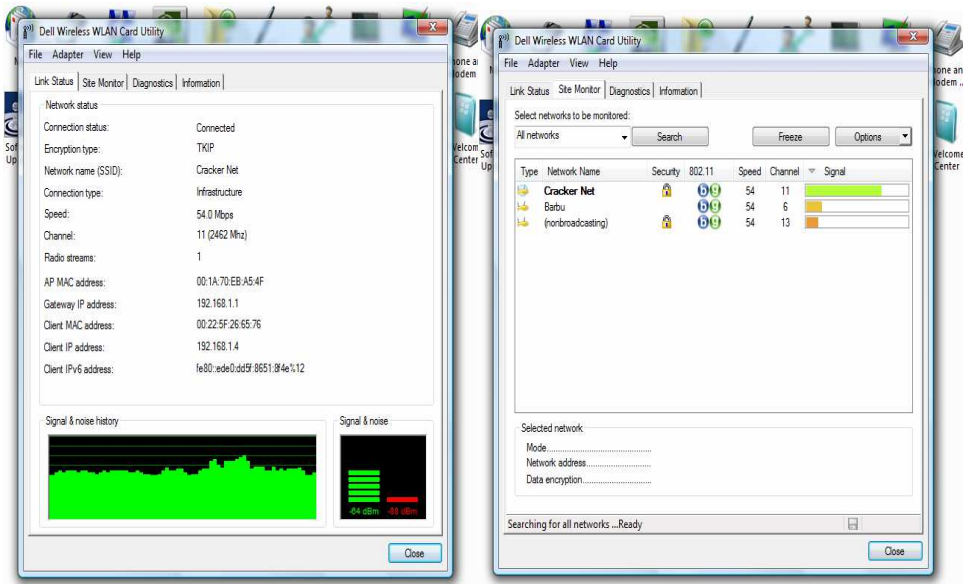
- selectați *Internet Protocol (TCP/IP)* şi apoi *Properties* pentru a configura opțiunile TCP/IP, asemenea unui dispozitiv de rețea wired.

Windows Vista

Sistemul de operare Windows Vista instalează în mod implicit stiva de protocoale TCP/IP (IPv4 şi IPv6).

Majoritatea adaptoarelor wireless sunt detectate în mod automat, iar driver-ele sunt descărcate automat utilizând o conexiune Internet. Pentru adaptoarele care nu se instalează în mod implicit, se vor utiliza CD-ROM-urile de instalare sau, se vor descărca de pe site-ul producătorului driver-ele aferente.

Marea majoritatea a producătorilor de plăci wireless, pun la dispoziția utilizatorilor diferite programe pentru monitorizarea şi diagnosticarea conexiunilor wireless (exemplu utilitar pentru Dell Wireless Card):



- Control Panel\Network and Sharing Center
  - Connect to a network
    - Proces de descoperire a rețelelor wireless disponibile (atât cele securizate, cât şi cele nesecurizate)
  - Manage wireless networks
    - Selectarea modului şi a ordinii de conectare la rețelelor wireless disponibile
  - Manage network connections (wireless şi wired)
    - Configurări avansate şi actualizări de drivere

Linux

PCMCIA

- Instalare
- Verificare si control
  - [...]#cardctl eject 0
  - [...]#cardctl insert 0
  - Vizualizare Card Information Structure (CIS):
    - [...]#cardctl info 0
    - [...]#cardctl ident 0
    - [...]#dump_cis
  - [...]#cardctl status 0
  - [...]#cardctl config 0

Wireless Network Adapters

- Vizualizare informații
    - [...]#ifconfig
    - [...]#iwconfig
- Căutare rețele
    - [...]#iwlist eth1 scan
- Căutarea unei rețele (căutare după SSID)
    - [...]#iwconfig ath0 essid “SSID Rețea”
    - [...]#ifconfig ath0 up
    - [...]#iwconfig ath0
- Vizualizare informații canale disponibile
    - [...]#iwlist ath channel
- Selectarea frecvenței/canalului (pentru plăci care nu au suport de scanare)
    - [...]#iwconfig ath0 freq 2.462G
    - [...]#iwconfig ath0 channel 11
- Setarea modului rețelei
    - [...]#iwconfig ath0 mode Ad-hoc
    - [...]#iwconfig ath0 mode Managed
- Asocierea la un AP (pe baza adresei MAC)
    - [...]#iwconfig ath0 ap 01:02:03:04:05:06
- Setarea ratei de date
    - [...]#iwconfig ath0 rate [param_rate]
    - [...]#iwconfig ath0 rate auto

3. Aplicații practice

3.1. Se vor discuta caracteristicile principalelor topologii 802.11

3.2. Se vor instala, configura şi testa, utilizând sistemul de operare Windows XP, următoarele dispozitive de comunicație wireless: PCI adapter (Linksys Wireless-N WMP300N), PCMCIA adapter (Linksys Wireless-N WPC4400N), USB adapter (Linksys Wireless-N WUSB300N).

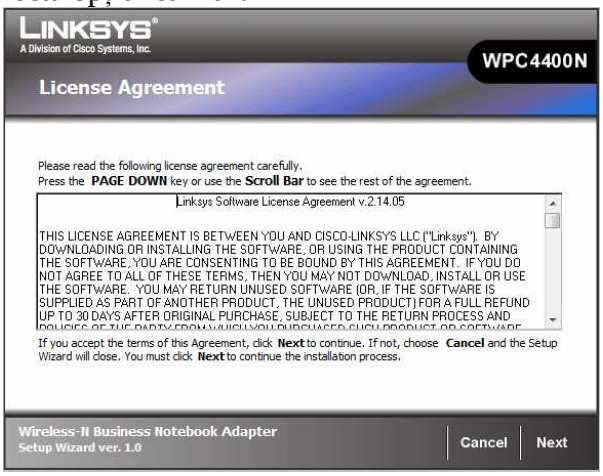
<u>Instalarea şi configurarea PCI adapter (Linksys Wireless-N WMP300N)</u>

- se va utiliza CD-ROM-ul de instalare (Setup Wizzard CD-ROM)
- se opri sistemul şi se va instala placa pe un port PCI disponibil
- se va reporni sistemul
- se va realiza conexiunea la reţeaua wireless dorită

Instalarea şi configurarea PCMCIA adapter (Linksys Wireless-N WPC4400N)

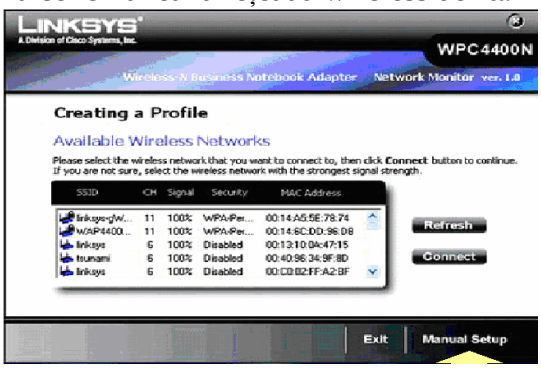
- se va utiliza CD-ROM-ul de instalare (Setup Wizzard CD-ROM)
- se va selecta opţiunea *Click Here To Start*

- se va selecta opţiunea *Next*



- se va conecta adaptorul la port CardBus al computerului şi apoi se va selecta opţiunea *Next*

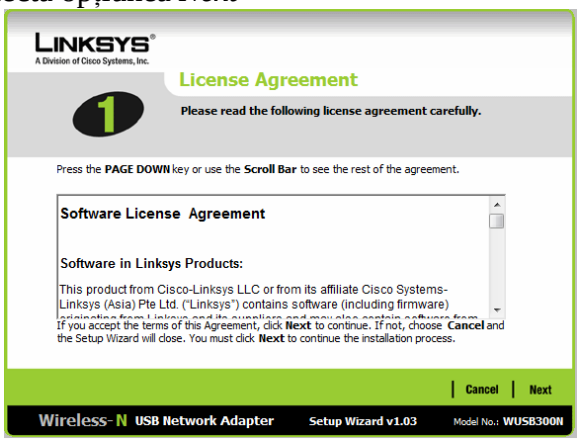
- pentru Windows XP Service Pack 2, va apărea fereastra *Found New Hardware Wizard*, unde se va selecta opțiunea *Next*, iar apoi, în următoarea fereastră *Install Software Automatically (Recommanded)*
- se va realiza conexiunea la rețeaua wireless dorită



<u>Instalarea și configurarea USB adapter (Linksys Wireless-N WUSB300N)</u>

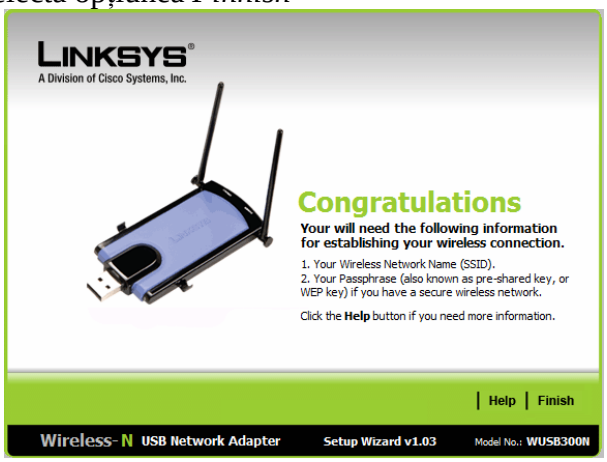
- se va utiliza CD-ROM-ul de instalare (Setup Wizzard CD-ROM)
- se va selecta opțiunea *Click Here To Start*

- se va selecta opţiunea *Next*



- se va conecta adaptorul USB la un port USB al computerului (există posibilitatea utilizării unei extensii USB sau a USB Extension Base) şi apoi se va selecta opţiunea *Next*

- se va selecta opțiunea *Finnish*



- se va realiza conexiunea la rețeaua wireless dorită, modul de conectare fiind identic cu cel al unui adaptor wireless PCI.

3.3. Se vor instala, configura şi testa, utilizând sistemul de operare Linux (Ubuntu), următoarele dispozitive de comunicație wireless: PCI adapter, PCMCIA adapter, USB adapter.

Bibliografie:

[1] M. Gast, *802.11 Wireless Networks: The Definitive Guide*, O'Reilly, 2002.
[2] D. Coleman, D. Westcott ,*CWNA Certified Wireless Network Administrator Study Guide*, Wiley Publishing, 2006.
[3] Cisco CCNA LAN Switching and Wireless Course.
[4] E. Cebuc, V.T. Dadarlat, *Rețele Locale de Calculatoare de la cablare la interconectare*, Editura Albastra 2005.

IV. Analiza mediului RF: Fluke Etherscope Series II Network Assistant

1. Obiective

Obiectivul acestui capitol este prezentarea modului de folosire a dispozitivului Fluke EtherScope Series II Network Assistant pentru analiza dispozitivelor fără fir şi a traficului în reţelele fără fir.

2. Consideraţii teoretice

2.1. Introducere

Fluke EtherScope Series II Network Assistant (fig. 1) este un dispozitiv portabil utilizat pentru instalarea, testarea, verificarea şi depanarea reţelelor LAN şi Wi-Fi.

Figura 1. Fluke EtherScope Series II Network Assistant [1]

Principalele caracteristici ale dispozitivului sunt [2]:

- depanarea reţelelor LAN Gigabit şi Wireless;
- analiza cablurilor LAN torsadate 10/100/Gigabit şi fibră optică 10/100 Mbps;
- interfaţă LAN transciever SFP pentru fibră optică Gigabit;

- analiză rețele WLAN 802.11a/b/g şi descoperire AP-uri 802.11n;
- monitorizare trafic rețea şi interfețe de switch, localizarea celui mai apropiat switch pentru a afişa detaliile şi statisticile de port;
- descoperire dispozitive de infrastructură wired şi wireless şi configurațiile acestora;
- identificare VLAN-uri pentru vizualizarea stărilor interfețelor, detaliile stațiilor conectate;
- descoperire sub-rețelele şi catalogarea elementelor din rețea după adresa de IP, domeniu de NetBIOS sau rețele IPX;
- interfata touch-screen;
- sistem de operare Linux;

2.2. Descrierea interfețelor dispozitivului

Produsul Fluke Networks EtherScope Network Assistant este un instrument mobil utilizat pentru depanarea şi întreținerea rețelelor WLAN şi LAN, care pune la dispoziția administratorilor de rețea un set de utilitare şi teste automate.

Figura 2. Fluke EtherScope Series II Network Assistant – vedere frontală [1]

Figura 2 prezintă o vedere frontală a dispozitivului, explicând principalele caracteristici şi interfețe ale dispozitivului:

- buton On/Off/Stand-by
- stilou grafic pentru interfața touch-screen
- led-uri care indică funcționarea dispozitivului
- port serial, utilizat pentru conectarea şi configurarea unor dispozitive de rețea (switch/router)
- port USB, utilizat pentru conectarea unei tastaturi sau a unui mouse
- adaptor AC

Figura 3 prezintă o vedere de sus a dispozitivului, reprezentând interfețele de rețea ale dispozitivului:

Figura 3. Fluke EtherScope Series II Network Assistant – interfețe de rețea [1]

- slot 1 - PCMCIA, utilizat pentru conectarea adaptorului wireless
- slot 2 – Compact Flash, utilizat pentru salvarea datelor de test
- port RJ45, utilizat pentru conectarea la rețele wired, bazate pe cabluri torsadate (10/100/1000 Mbps)
- interfață SFP, utilizată pentru conectarea unui transciever de fibră optică pentru conectarea directă la rețele de fibră optică (1000 Mbps)

2.3. Descrierea interfeței grafice

Figura 2, sublinează, de asemenea, modul în care display-ul touch-screen este divizat în trei zone cu caracteristici distincte.

Panoul toolbox pune la dispoziție o platformă de navigare şi informare rapidă, având următoarele butoane:

- buton pentru accesarea meniul principal
- buton pentru accesarea tastaturii
- grup de butoane pentru setări şi informări generale ale dispozitivului (luminozitate/volum,etc)
- buton pentru revenirea la ecranul anterior
- buton pentru revenirea la ecranul principal al rezultatelor testelor
- buton pentru accesarea unei liste de opțiuni de depanare şi testare a rețelei
- Details buton pentru accesarea informațiilor referitoare la un test specific
- LAN Tests buton pentru accesarea testelor pentru rețeaua wired

Panoul central reprezintă principala zonă de navigare, care oferă informații generale referitoare la testele efectuate şi la starea rețelei. Din acest panou se vor selecta diferitele teste şi se vor vizualiza la nivelul următor, în mod detaliat, prin selectare opțiunii Details.

Panoul preview oferă informații sumarizate referitoare la un anumit test selectat din panoul central, pentru a putea vizualiza, în mod succint, informațiile care vor fi accesibile la nivelul următor.

2.4. Depanarea rețelelor wireless

Dispozitivul Fluke EtherScope Series II Network Assistant pune la dispoziția administratorilor de rețea şi opțiunea de analiză şi depanare a rețelelor fără fir. Slotul 1, descris anterior, permite instalarea unui card wireless utilizând interfața PCMCIA.

Paşii care trebuie urmați pentru depanarea rețelelor fără fir sunt următorii:

- instalarea unui adaptor wireless Fluke 802.11 a/b/g
- pornirea dispozitivului şi selectarea opțiunii *WLAN Test*

- EtherScope Network Assistant execută o serie de teste pasive de scanare, iar apoi încearcă să stabilească o legătură la un AP care este configurat cu SSID-ul implicit.

Vizualizarea rezultatelor AutoTestului

După selectarea opțiunii WLAN Test, în panoul central al dispozitivul EtherScope Network Assistant vor fi afişate testele efectuate (fig. 4).

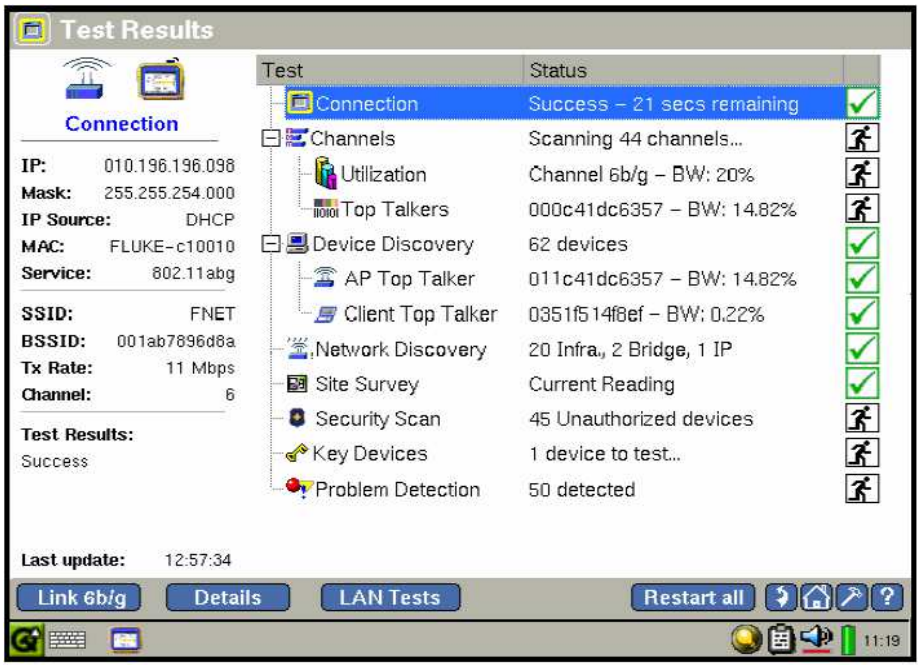


Figura 4. Vizualizare rezultate AutoTest

Icoanele din partea dreaptă a panoului central prezintă statusul fiecărui test in curs, semnificațiile fiind descrise în tabelul 1.

Se poate selecta fiecare test afişat pe panou central, iar sumarul testului va fi afişat în panoul preview. Această vizualizare sumară a testelor poate crea unui administrator de rețea o privire a ansamblu asupra configurației rețelei şi a posibilelor probleme.

Icoana	Semnificație
	Test în curs de execuție
	Test care nu se execută
	Test terminat cu succes
	Test terminat cu eșec

Tabelul 1. Status teste

Pentru a vizualiza rezultatul unui anumit test în mod detaliat, se va selecta testul, iar apoi opțiunea Details.

Autotestul conține următoarele verificări:

a. Connection – dispozitivul Fluke EtherScope va încerca conectarea la rețeaua wireless implicită. Pentru setarea unei rețele implicite se va selecta opțiunea Details, iar apoi opțiunea *Wireless Security* din panoul preview, unde se va alege SSID-ul rețelei dorite (se va selecta check-box-ul cu opțiunea *Default*) şi metoda de autentificare. Pentru salvarea setărilor se va selecta *Apply* din panoul toolbox. Opțiunea *Link* va permite asocierea dispozitivului la rețeaua selectată.

Alte opțiuni disponibile:

- TCP/IP: setarea adreselor IP, Gateway, DNS sau a modului DHCP
- Connection Log: jurnal al paşilor de conectare
- Radio: setarea caracteristicilor radio conform regulamentelor țării în care este utilizat dispozitivul
- Instrument Security: setarea securității dispozitivului
- General: setări referitoare la adresele MAC
- Authorization: setarea nivelului de încredere pentru dispozitivele detectate sau memorate (authorized/ un authorized/ neighbor)
- Group Names: creare grupuri de perechi MAC/BSSID

- Wireless Problems: setarea problemelor care vor fi urmărite
- Options
- Version

b. Channels – dispozitivul Fluke EtherScope Network Assistant va efectua o scanare a canalelor RF, în benzile de 2.4 GHz şi 5 GHz (fig. 5).

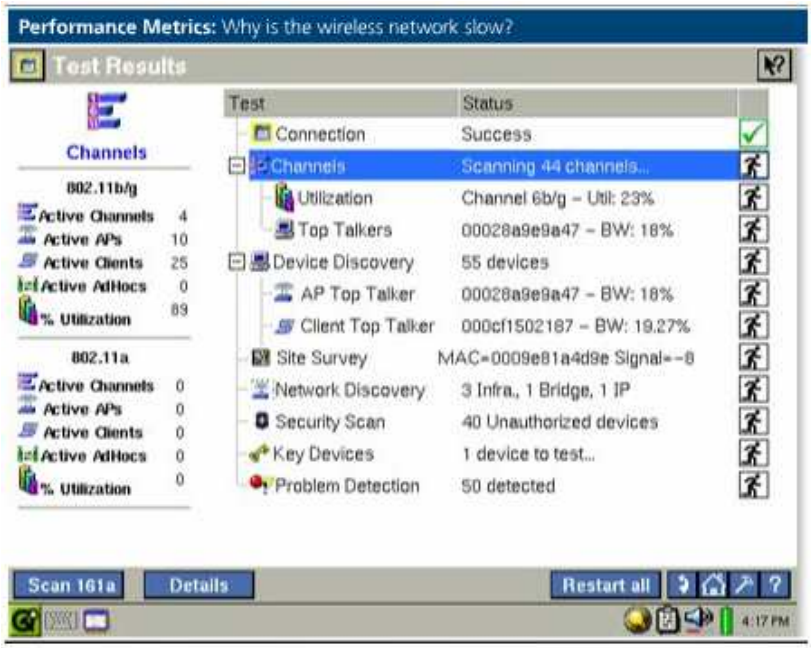


Figura 5. Test Scanare Canale RF

Panoul preview va afişa informații legate de tipul şi numarul dispozitivele disponibile, atât pentru canalele 802.11 b/g, cât şi pentru cele 802.11a. Pentru a monitoriza calitatea semnalului şi pentru a măsura diferiți parametri de calitate, pentru fiecare canal detectat, se va selecta opțiunea **Details** din cadrul panoului toolbox. Următoarele statistici sunt disponibile în cadrul acestei opțiuni:

- Signal Strength (dBm or %) - puterea semnalului
- Noise (dBm or %) - zgomot
- Signal to Noise Ratio (dBm or %) - SNR
- Total Utilization (%) – utilizare totala

- Good Packet Rate (pkts/sec) – frecvența de pachete
- Good Octet Rate (pkts/sec) – frecvența de octeți
- Error Packet Rate (pkts/sec) – frecvența de pachete cu eroare
- Error Octet Rate (pkts/sec) – frecvența de octeți cu eroare
- Retry Packet Rate (pkts/sec) – frecvența de reîncercări
- Retry Octet Rate (pkts/sec) – frecvența de reîncercări
- Retry % - reîncercări
- CrossTalk Packet Rate (pkts/sec) – frecvența de diafonie
- CrossTalk Octet Rate (pkts/sec) – frecvența de diafonie
- CrossTalk % – diafonie

Submenirile *Utilization* şi *Top Talkers* furnizează informații care sunt utile pentru verificarea şi depanarea problemelor de trafic şi de performanță în rețea. Opțiunea *Utilization* oferă statistici referitoare la cantitatea şi tipul de trafic pe canalele detectate, iar opțiunea *Top Talkers* oferă statistici referitoare la dispozitivele care utilizează rețeaua.

c. Device Discovery – dispozitivul Fluke EtherScope Network Assistant, odată asociat la un AP va efectua o scanare a rețelei wireless pentru a descoperi dispozitivele din rețea.

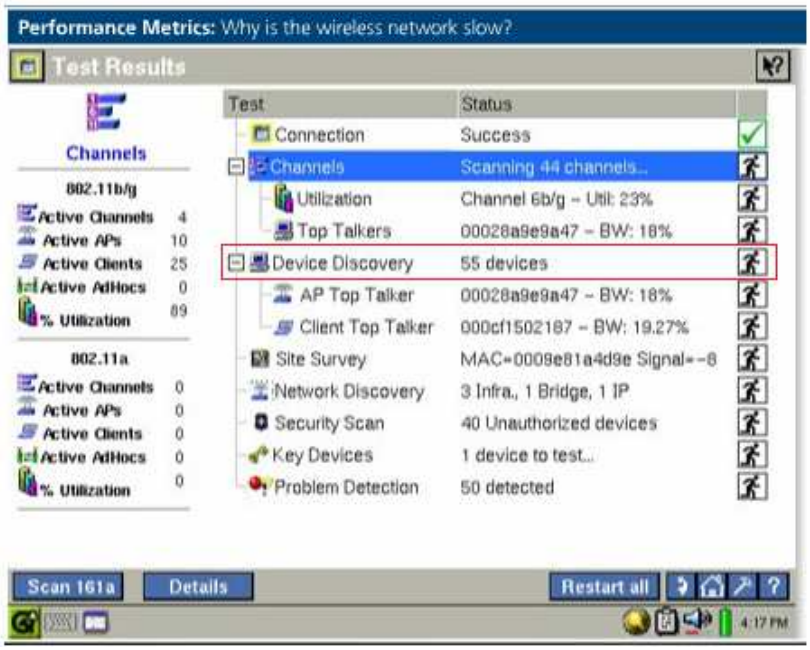


Figura 6. Test Descoperire Dispozitive

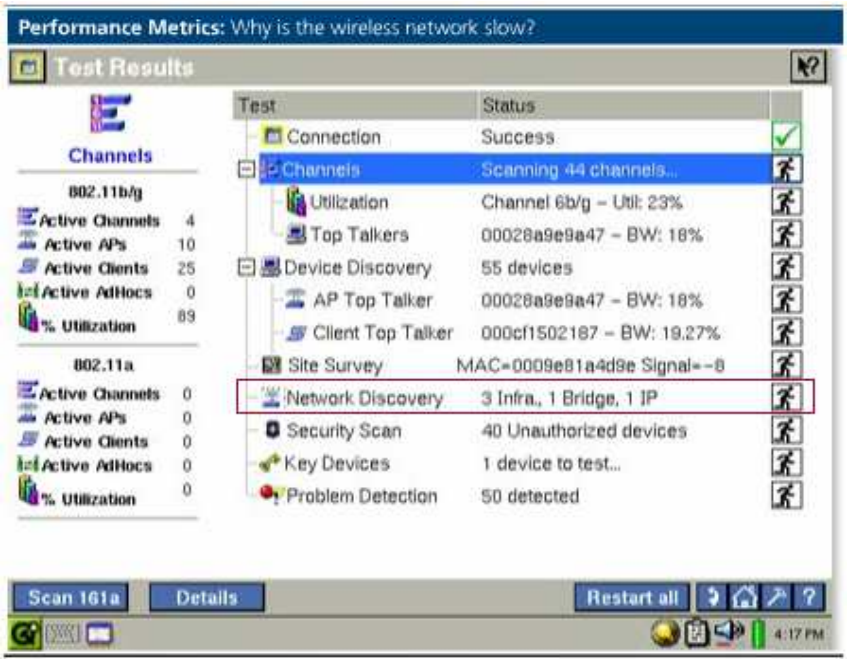
În panoul preview se va afişa o listă de categorii de dispozitive şi numărul acestora. Datorită faptului că un dispozitiv poate juca mai multe roluri, numărul total de dispozitive din fiecare categorie va putea fi mai mare decât numărul dispozitivelor existente (fig. 6).

La selectarea opțiunii Details, în panoul central se va afişa lista cu dispozitivele descoperite, identificate prin nume, adresă MAC, tipul dispozitivului (Client/AP/Bridge), SSID-ul asociat cu fiecare dispozitiv, canalul pe care comunică, puterea semnalului şi a zgomotului, informații legate de metoda de securitate utilizată. De asemenea, nivelul de autorizare al fiecărui dispozitiv este afişat (authorized/un authorized/neighbor). Un SSID prezentat sub forma *>>SSID1>>SSID2>>...>>SSIDn*, semnifică faptul că un dispozitiv este asociat mai multor SSID-uri, fiecare fiind separat de simbolul >>.

Pentru a vizualiza toate informațiile disponibile despre un anumit dispozitiv descoperit, se va selecta dispozitivul şi se va selecta opțiunea Details din cadrul panoului toolbox.

Submenirile *Client Top Talker* şi *AP Top Talker* furnizează informații legate de consumul de lățime de bandă, mai exact care este clientul şi, respectiv, access point-ul care utilizează cea mai multă lățime de bandă.

a. **Network Discovery** – acest test prezintă configurația rețelei wireless (fig. 7).
b. **Site Survey** – dispozitivul Fluke EtherScope Network Assistanat poate fi utilizat pentru a realiza examinări ale rețelei wireless, permițând salvarea datelor (fig. 8). Pentru proiectarea, verificarea şi descoperirea diferitelor rețele şi probleme, se poate utiliza acest test prin examinarea perioadică a locațiilor şi compararea datelor cu cele salvate anterior.



c. Figura 7. Test Descoperire Configurații de Rețea

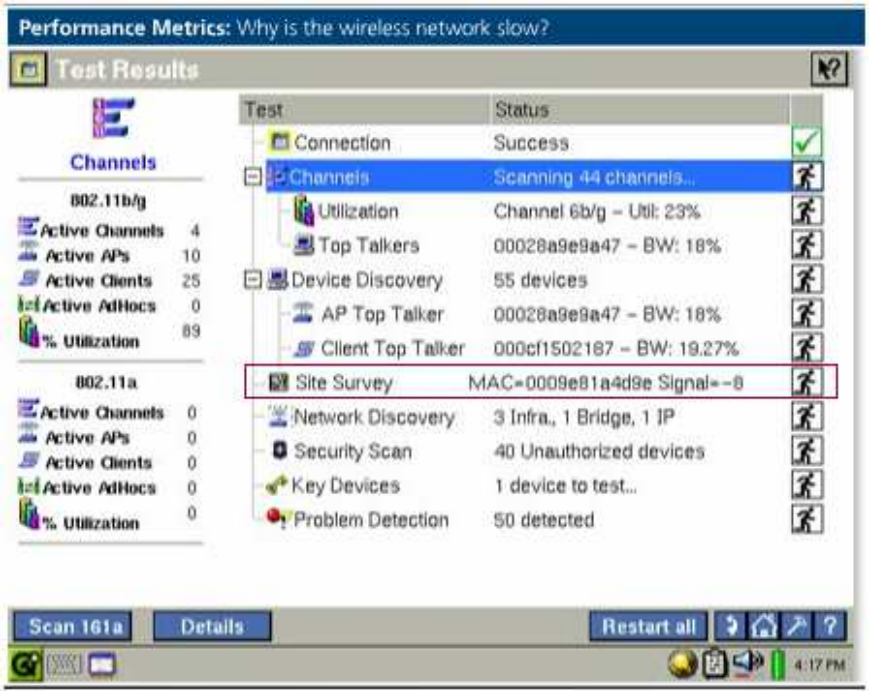


Figura 8. Test Examinare Rețea

d. **Security Scan** – acest test poate fi utilizat pentru a descoperi dispozitivele neautorizate sau neprotejate (nesecurizate).
e. **Key Devices** – acest test permite selectarea unor dispozitive pentru a putea fi testate utilizând testul de conectivitate (Ping). În mod implicit nici un dispozitiv nu este selectat, deoarece acestă opțiune va fi configurată în funcție de necesitățile administratorului de rețea.
f. **Problem detection** – acest test poate fi utilizat pentru a determina dispozitivele care prezintă probleme. Panoul preview oferă informații legate de următoarele probleme: Erori/ Avertismente/ Mesaje Info/ Probleme rezolvate. Pentru vizualizarea acestor informații se va selecta opțiunea Details din cadrul panoului toolbox. În cadrul panoului principal se prezintă problemele (Description) pentru fiecare dispozitiv (identificat prin adresă MAC/nume). Tabelul 2 sumarizează tipurile de erorile şi avertismente cunoscute de către dispozitiv.

Erori	Avertismente
Dispozitiv rogue	AP-ul propagă SSID
Dispozitiv neprotejat	AP-ul utilizează SSID-ul implicit (SSID-ul producătorului)
Canal ilegal	AP - Rate Tx scăzute
Dispozitivul nu răspunde	Client - Rate Tx scăzute
	AP - Reîncercări Tx numeroase
	Client - Reîncercări Tx numeroase
	Client - Autentificare eşuată
	Excessive Missed Beacons
	High Speed Not Supported

Tabelul 2. Erori şi Avertismente [1]

Execuția testelor de diagnostic

Dispozitivul EtherScope Network Assistant pune la dispoziție diferite informații referitoare la stații, dispozitive şi servicii de rețea şi, de asemenea, teste pentru verificarea conectivității şi a performanțelor rețelei.

Teste disponibile pot fi accesate în două moduri:

a. prin selectarea opțiunii din panoul toolbox, iar apoi alegerea testului dorit;

   Testele disponibile:

   • Ping – utilizat pentru testarea conectivității cu un alt dispozitiv

   • Trace Route – utilizat pentru a vizualiza calea parcursă până la un anumit dispozitiv

   • Web Browser – client Konqueror

   • Telnet – acces remote către un computer

   • SSH Telnet – acces remote securizat către un computer

   • Terminal

   • FTP – pornire sesiune FTP

   • TFTP – pornire sesiune TFTP (de obicei pentru actualizare firmware)

   • Wireless Throughput

b. prin alegerea unui dispozitiv şi selectarea opțiunii Details. Dacă testele de diagnostic sunt disponibile pentru dispozitivul selectat, vor fi afişate în panoul preview, de unde vor putea fi accesate.

   Testele disponibile:

   • Signal Strength – puterea semnalului (dBm)

   • WLAN Statistics – statistici

   • Tx/Rx Rate – ratele de transmisie/recepție

   • Problems – problemele detectate

   • Trace Route - utilizat pentru a vizualiza calea parcursă până la un anumit dispozitiv

   • Ping – utilizat pentru testarea conectivității cu un alt dispozitiv

• Wireless Throughput – vizualizarea throughput-ului

• Locate – localizarea dispozitivului

• Login Diagnosis – testarea procesului de logare EAP (Extensible Authentification Protocol)

• Link (doar pentru LAN wireless) – asociere la dispozitiv

3. Aplicații practice

3.1. Se vor experimenta testele WLAN ale dispozitivului Fluke EtherScope Network Assistant, utilizând configurația de test din cadrul laboratorului. Se va realiza o analiză a rețelelor WLAN 802.11a/b/g, se va monitoriza traficul şi se vor depana problemele din cadrul rețelor wireless detectate. Se vor pune în evidență diferențele dintre rețelele wired şi wireless, şi problemele specifice rețelelor 802.11. Se vor crea rapoarte pentru fiecare test rulat.

3.2. Se vor localiza dispozitivelor wireless utilizând opțiunea - Device Details – Locate, pentru fiecare dispozitiv descoperit. Se va pune în evidență utilitatea dispozitivului Fluke EtherScope Network Assistant pentru proiectarea şi instalarea rețelelor WLAN 802.11a/b/g.

Bibliografie:

[1] Fluke EtherScope Series II Network Assistant User Manual
[2] Fluke EtherScope Series II Network Assistant, http://www.analizoaredeteta.ro/old/analizoare-portabile-lan/etherscope.html

V. Analiza mediului RF: Fluke Analyze-Air

1. Obiective

Obiectivul acestui capitol este prezentarea modului de folosire a pachetului Fluke Analyze – Air pentru analiza dispozitivelor şi a traficului în reţelele fără fir.

2. Consideraţii teoretice

2.1. Introducere

Pachetul Fluke Analyze-Air (fig. 1) este destinat analizei spectrale RF, fiind acordat pentru spectrele de frecvenţă 2,4 – 2,5 Ghz şi 4,9 – 5,875 GHz. Utilitarul poate fi utilizat atât înainte de amplasarea dispozitivelor viitoarei reţele wireless – pentru detectarea, identificarea şi localizarea interferenţelor RF în WLAN 802.11, cât şi pentru depanarea reţelelor existente, datorită problemelor apărute pe parcurs.

Figura 1. Pachetul Fluke Analyze-AIR [1]

Analyze-AIR este un pachet software însoţit de un card PCMCIA şi un set de antene, menit sa transforme un notebook într-un instrument de mare acurateţe destinat analizei spectrului de frecvenţă folosit de reţelele wireless. Analyze Air are în componenţa pachetului două antene, o antenna omnidirecţională şi o antenna directională realizată special pentru depistarea dispozitivelor perturbatoare sau a dispozitivelor ilegale din reţeaua wireless.

Comportamentul în rețea al dispozitivelor, gradul lor de utilizare, cât şi utilizarea pe canale, sunt evidențiate în graficele pe care Analyze Air le pune la dispoziția administratorilor de rețea.

Principalele facilități oferite de către pachetul Fluke Analyze-AIR sunt:
- vizualizarea mediului în care se desfăşoară rețeaua wireless;
- identificarea şi listarea dispozitivelor din rețeua wireless;
- impactul dispozitivelor în rețeaua wireless;
- grafice detaliate ale rețelei wirelessş
- detectarea problemelor de securitate.

2.2. Descrierea modului de funcționare

Fluke AnalyzeAir pune la dispoziția utilizatorilor şase moduri principale de operare [2]:

a. Active Device
b. Spectrum Plots
c. Spectrum Charts
d. Devices View
e. Channel Summary
f. Device Finder

Fiecare mod de operare poate fi selectat din cele şase opțiuni subliniate în figura 2, sau din cadrul meniului *View*.

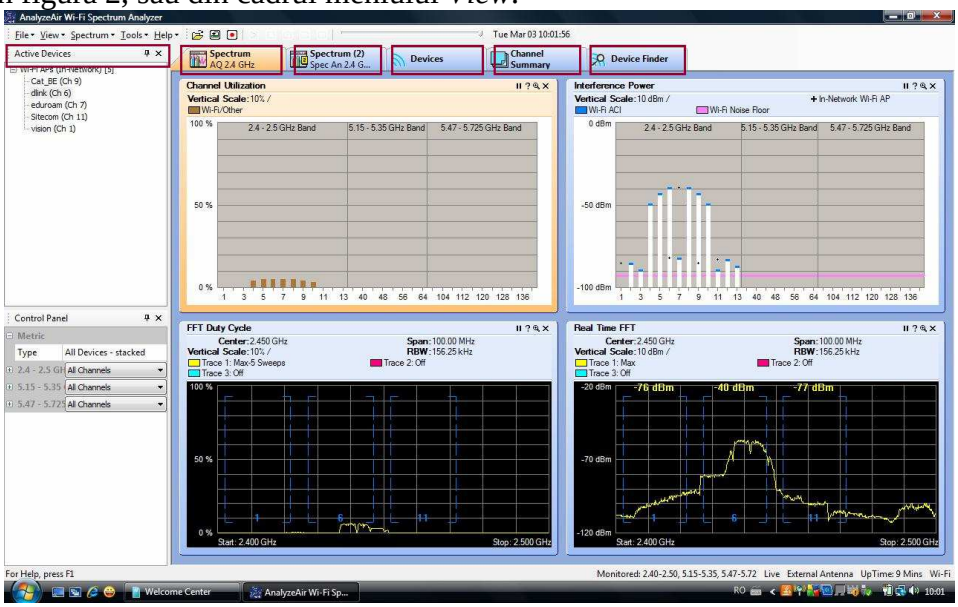


Figura 2. Moduri de operare

A. Active Devices

Acest display, localizat în partea stângă a ecranului prezintă dispozitivele active detectate de către AnalyzeAir (fig. 3).

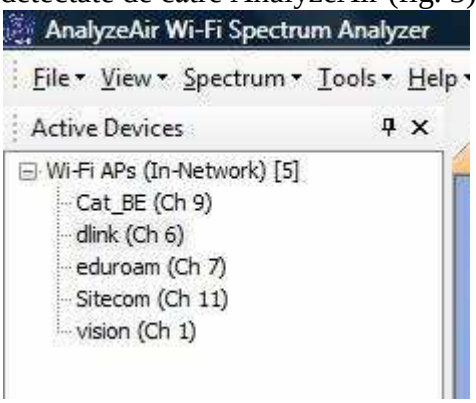


Figura 3. Modul Active Devices

Dispozitivele care pot fi detectate, utilizând pachetul Fluke Analyze-Air sunt:

- Wi-Fi APs (In-Network)
- Wi-Fi APs (Known)
- Wi-Fi APs (Unknown)
- Wi-Fi Ad Hocs
- Interferers – orice dispozitiv care nu este 802.11, dar care operează în aceeaşi bandă de frecvenţă ca şi dispozitivele 802.11. Aceste dispozitive (cuptoare cu microunde, dispozitive Bluetooth, telefoane fără fir, etc) pot produce interferenţe şi pot perturba activitatea dispozitivelor de reţea.
- Generic Interferers - dispozitiv care nu este 802.11, însă nu poate fi încadrat într-o categorie de Interferers. Totuşi diferiţi parametri ai semnalului de interferenţă vor fi detectaţi.

Pentru a localiza un anumit dispozitiv detectat, se va selecta dispozitivul, se va accesa meniul disponibil prin *right-click*, şi se va alege opţiunea *Find This Device*. În acest mod se va activa modul *Device Finder*.

Pentru a obţine informaţii suplimentare despre un anumit dispozitiv detectat, se va selecta dispozitivul, se va accesa meniul disponibil prin *right-click* şi se va alege opţiunea *What is This Device* (fig. 4).

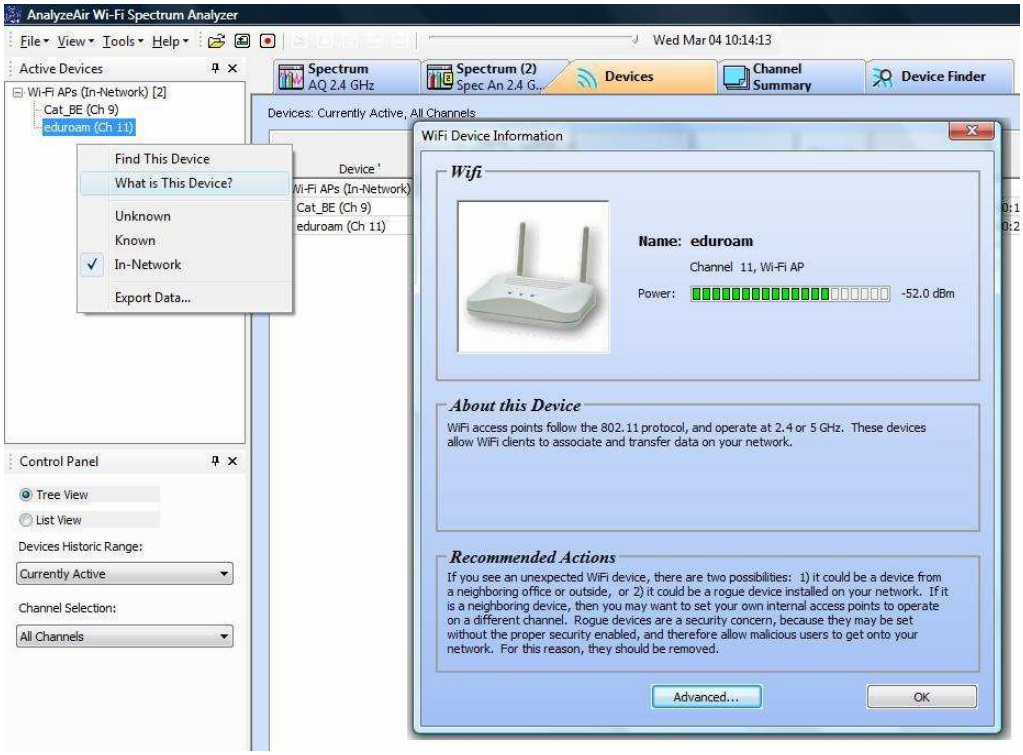


Figura 4. Descoperire dispozitiv

B. Spectrum Plots

Acestă opțiune oferă cinci tipuri de grafice care prezintă în timp real activitatea RF în funcție de frecvență şi, de asemenea, variații în activitatea RF pe intervale scurte de timp. Aceste grafice sunt unelte esențiale pentru întelegerea şi analiza mediului în care WLAN-ul funcționează. Un termen general utilizat de Fluke Anlyze-Air este ***Duty cycle*** care se referă la cât de multă energie RF este prezentă în spectru, măsurată nu ca şi energie RF brută (wați sau dBm), ci mai degrabă în termeni care indică cât de multă putere RF este prezentă în sens operațional sau funcțional. Scopul este de a avea o măsură de putere RF care să sugereaze cât de mult impact va avea puterea RF asupra performanței rețelei.

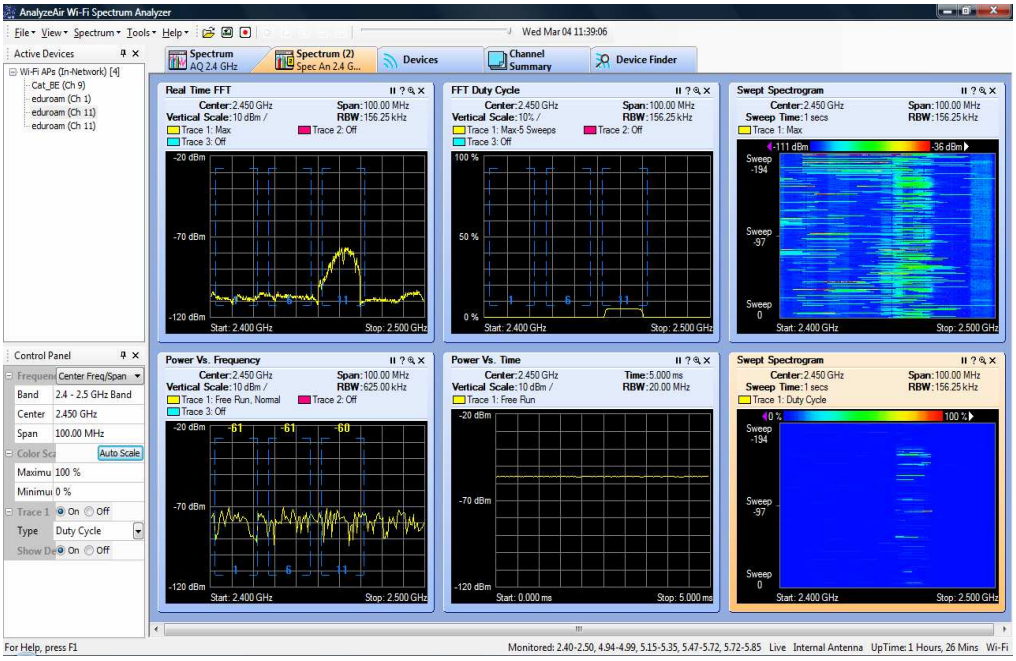


Figura 5. Spectrum plots

Pentru personalizarea analizei, prin selectarea tipurilor de grafice ce se doresc a fi vizualizate se va utiliza meniul Spectrum->Add Plot. Graficele disponibile sunt următoarele:

- *Real Time FFT* afişează puterea RF ca o funcție de frecvență. Graficul generat poate oferi trei vederi diferite: a. puterea medie (Avg) citită în timpul celui mai recent interval de măsurare; b. puterea maximă (Max); c. puterea maximă detectată (Max Hold), de la momentul începerii analizei
- *FFT Duty Cycle* afişează procentul de timp la care semnalul RF ambiant
  este mai sus de 20 dB peste pragul de zgomot.
- *Swept Spectrogram* reprezintă un mod diferit de prezentare a datelor afişate de către Real Time FFT şi FFT Duty Cycle. Codificarea utilizând culori este folosită pentru a indica, fie intensitatea puterii RF, fie RF duty cycle (selectarea se realizează utilizând Spectrum Control Panel – fereastra stânga-jos), pe un anumit interval de timp (sweep). Vederea curentă va fi întotdeauna sweep-ul cu numărul 0.

- *Power vs. Frequency* prezintă cantitatea de putere RF detectată la diferite frecvențe. Aceast grafic se bazează pe o analiză a datelor de la senzor, aceste date putând fi agregate şi combinate în diverse moduri. Real Time FFT se bazează, în schimb, pe date capturate în mod direct de la senzor.
- *Power vs. Time* afişează puterea RF ca o funcție de timp. Intervalul de timp utlizat în această analiză este foarte scurt (de ordinul milisecundelor).

De asemenea, meniul din colțul superior-drept al graficelor permite oprirea şi apoi reluarea analizei în timp real.

C. Spectrum Charts

Acest display oferă informații generalizate către inginerul de rețea, pe când Spectrum Plots oferă informații mai uşor de înțeles de către experții RF. Diagrame ca *Devices vs. Time* şi *Channel Utilization vs. Time* pot oferi informații legate de momentele când rețeaua wireless este afectată mai mult de interferențe, iar diagrame ca *Devices vs. Channel* şi *Channel Utilization* pot oferi informații generale referitoare la modul în care diferite canale pot fi afectate de activitatea RF.

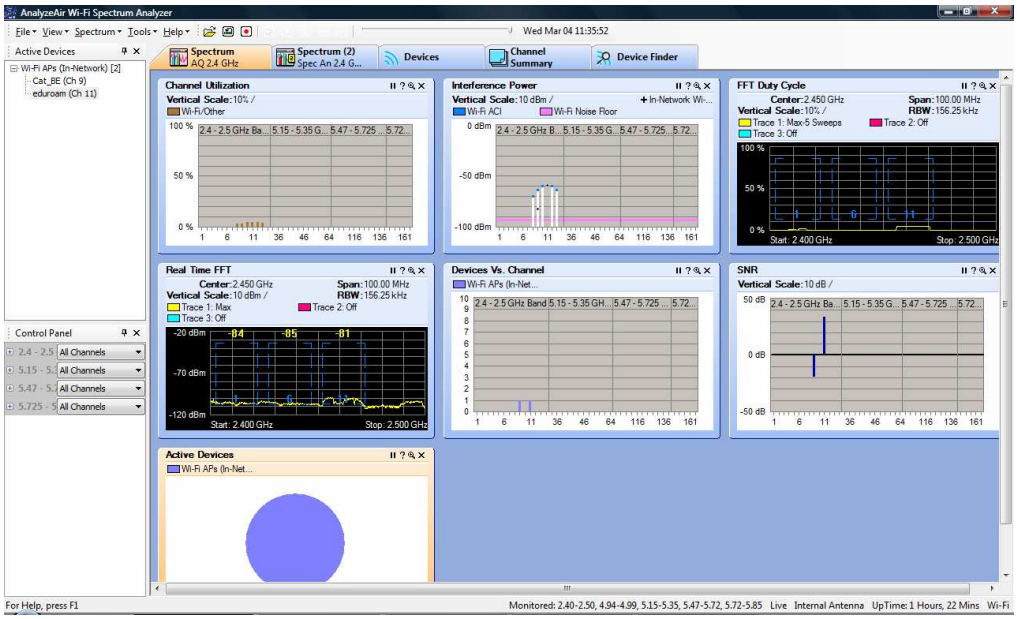


Figura 6. Spectrum charts

Pentru personalizarea acestui tip de analiză, se va utiliza meniul Spectrum->Add Chart şi se vor selecta tipurilor de diagrame ce se doresc a fi vizualizate. Analizele disponibile sunt următoarele:

- *Active Devices* reprezintă un pie chart care va indica procentul de activitate RF care aparține fiecărei surse RF. Se pot selecta canalul/banda care vor fi monitorizate.
- *Devices vs. Channel* reprezintă un bar chart care va afişa numărul de dispozitive detectate pe fiecare canal. Se pot selecta canalul/banda care vor fi monitorizate.
- *Devices vs. Time* reprezintă un line chart care va afişa numărul de dispozitive detectate la anumiți timpi. Se poate selecta intervalul de timp, canalul/banda şi tipul de dispozitive care vor fi monitorizate.
- *Channel Utilization* reprezintă un bar chart care va afişa RF duty cycle în funcție de fiecare canal. Fiecare bară va fi compusă din mai multe culori care vor reprezenta duty cycle-ul fiecărui dispozitiv de pe un anumit canal.
- *Channel Utilization vs. Time* reprezintă un line chart care va afişa RF duty cycle ca o funcție de timp.
- *Intereference Power* reprezintă un bar chart care va afişa puterea pe fiecare canal selectat. Înălțimea fiecărei bare va indica puterea tuturor semnalelor de interferență. Fiecare bară este formată din mai multe linii, fiecare linie reprezentând puterea semnalului pentru un anumit tip de dispozitiv. Cu un plus (+) este marcată puterea semnalului recepționat de către cel mai puternic In-Network Wi-Fi AP, pe un anumit canal.
- *SNR* reprezintă un bar chart care afişează nivelul SNR pe fiecare canal.

D. Devices View

Acest display oferă informații detaliate referitoare la dispozitivele de rețea şi la dispozitivele care interferează cu rețeaua wireless (fig. 7). O opțiune importantă este reprezentată de posibilitatea de a avea un istoric al dispozitivelor detectate, nu doar a celor detectate la momentul curent.

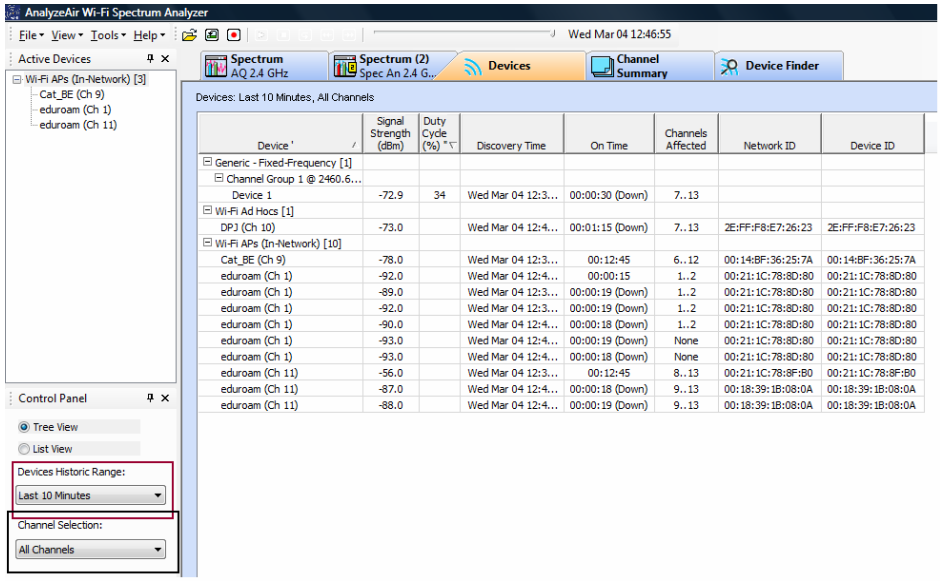


Figura 7. Devices view

E. Channel Summary

Acest display prezintă nivelurile specifice ale activității RF, pe un anumit canal, indiferent dacă sunt sau nu sunt prezente interferențe.

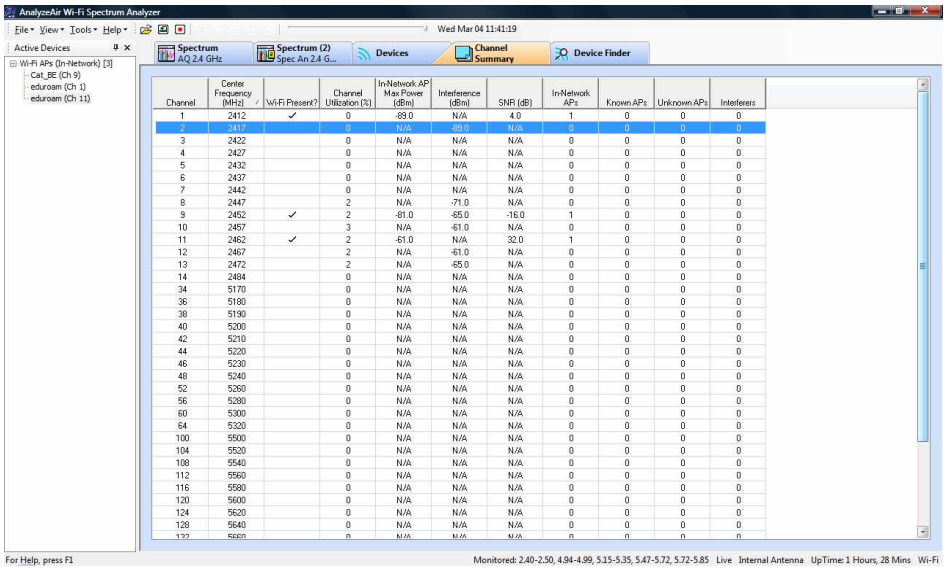


Figura 8. Channel summary

De asemenea, o analiză a dispozitivelor detectate pe fiecare canal este disponibilă, pentru a oferi informații adiționale, referitoare la canalele cele mai solicitate.

F. Device Finder

Acest display oferă posibilitatea localizării unui anumit dispozitiv selectat, transformând stația de lucru într-un dispozitiv de detecție (fig. 9).

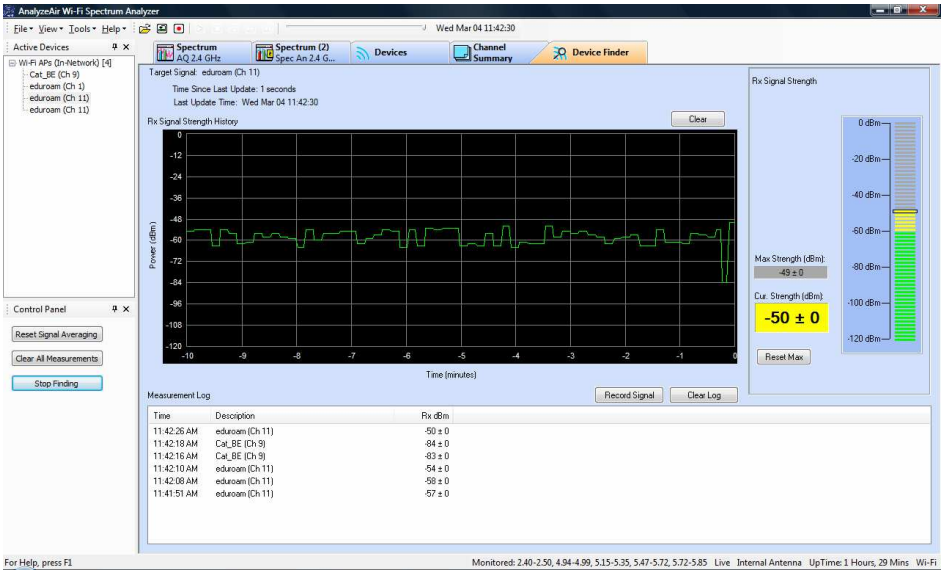


Figura 9. Device Finder

2.3. Descrierea opțiunilor de funcționare

Meniul Tools->Settings permite modificarea şi personalizarea diverselor opțiuni ale pachetului Analyze-AIR. Opțiunile disponibile sunt:

- *Sensors and Antennas*: opțiune pentru selectarea tipului de senzor utilizat pentru obținerea de date (Internal/Extenal PC Card Antenna)
- *Console Settings*: opțiune pentru modificarea modului în care Analyze-Air afişează datele.
- *Band and Channel Settings*: opțiune pentru configurarea benzilor şi a canalelor 802.11 pe care Analyze-Air le va monitoriza. Acestea pot fi selectate fie după Domeniu Reglementator (Americas/Australia, EMEA/Asia/Pacific, Japan, sau All Wi-Fi Channels), fie manual de către utilizator.

- *Alert Settings*: opțiune pentru configurarea alertelor de securitate şi a valorilor de prag pentru fiecare tip de dispozitiv. Cele două niveluri de alertă definite sunt nivelul critic şi nivelul avertizare. Valorile de prag care definesc fiecare nivel de alertă pot fi modificate pentru fiecare dispozitiv cunoscut. Tabelul 1 prezintă valorile de prag implicit definite:

	Critical	**Warning**
Active devices		
Interferer duty cycle (%)	50	25
Spectrum		
All devices channel utilization (%)	50	25
Interferer channel utilization (%)	50	25
SNR (Signal-to-Noise Ratio) (dB)	10	20
Channel Summary		
Channel utilization (%)	50	25
In-Network AP Max Power (dBm)	-88	-80
Interference (dBm)	-65	-75
SNR (Signal-to-Noise Ratio) (dB)	10	20
In-Network AP Count		2
Known AP Count		5
Unknown AP Count		1
Interferer Count		1
Ad Hoc Count		1

Tabelul 1. Alerte de securitate şi valori de prag [2]

- *SNMP Options:* opțiune pentru configurări SNMP

3. Aplicații practice

3.1. Se vor experimenta testele pachetului Fluke Analyze-Air, utilizând configurația de test din cadrul laboratorului. Se va realiza o analiză a rețelelor WLAN 802.11a/b/g, se va monitoriza traficul şi se vor depana problemele din cadrul rețelor wireless detectate. Se vor salva capturile obținute pentru analize ulterioare.

3.2. Se vor localiza dispozitivele wireless utilizând opțiunea - Device Finder, pentru fiecare dispozitiv descoperit. Se va pune în evidență utilitatea pachetului Fluke Analyze-Air, atât pentru proiectarea şi instalarea rețelelor WLAN 802.11a/b/g, cât şi pentru identificarea şi localizarea interferențelor.

3.3 Se va încărca setul de fişiere demonstrative ale pachetului Fluke Analyze-Air şi se vor analiza rezultatele salvate, pentru fiecare tip de dispozitiv detectat (Bluetooth, Cordlees Phone).

Bibliografie:

[1] Fluke Networks AnalyzeAir, Wi-Fi Spectrum Analyzer, http://www.tequipment.net/FlukeNetworksAnalyzeAir-Wi-FiSpectrumAnalyzer.html
[2] AnalyzeAir™ Wi-Fi Spectrum Analyzer 3.1 Users Manual, 2006

VI. Configurarea rețelelor wireless: Configurări de bază

1. Obiective

Obiectivul acestui capitol este prezentarea modului de instalare şi configurare a ruterului Linksys WRT350N Wireless-N Gigabit with Storage Link. Se vor descrie principalele caracteristici ale dispozitivului, modalităţile de funcţionare, precum şi avantajele/dezavantajele introduse de ruterele wireless.

2. Consideraţii teoretice

2.1. Introducere

Router-ul Linksys WRT350N Wireless-N Gigabit (fig. 1) este o componentă Wi-Fi care permite conectarea mai multor staţii fără fir la o conexiune Internet şi crearea unei rețele locale de calculatoare.

Figura 1. Router Linksys WRT350N Wireless-N Gigabit [1]

Principalele caracteristici ale dispozitivului sunt:

- Transmisie în tehnologie Wireless N (MIMO);
- Frecvență de operare: 2.4 - 2.5 GHZ;
- Internet Gigabit Router și Switch cu 4 port-uri 10/100/1000;
- Wireless Access Point cu rază mărită de acțiune;
- Securitate avansată prin Firewall SPI, criptare pe 256 de biți;
- Rată de transfer de până la 270 Mb/s;
- Standarde suportate: 802.11g, 802.3, 802.3x, Draft 802.11n, 802.11b, 802.3u, 802.3ab;
- VPN Pass Through;

i. Descrierea interfețelor dispozitivului

Figura 2 prezintă o vedere frontală a dispozitivului. Led-urile dispozitivului permit o diagnosticare rapidă a funcționării acestuia:

- *Power* – alimentarea ruterului;
- *Ethernet* 1, 2, 3, 4 – corespunzătoare porturilor Ethernet. Culoarea Verde a led-ului semnifică conectarea unui dispozitiv 10/100 Mbps, iar culoarea Portocaliu semnifică conectarea unui dispozitiv 1000 Mbps. Dacă led-ul se aprinde intermitent semnifică faptul că ruterul transmite/recepționează date;
- *Internet* – conexiune prin portul Internet;
- *USB* - conexiune cu un dispozitiv USB;
- *Wireless* – conexiune fără fir;
- *Security* – setări de securitate;

Figura 2. Vedere frontală [1]

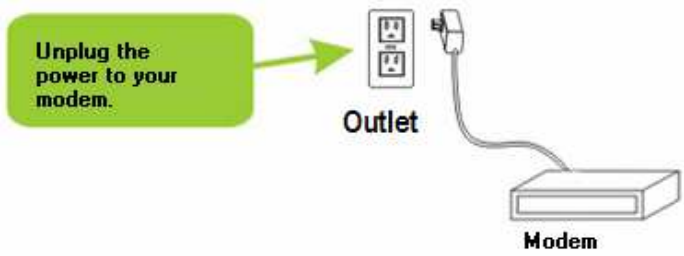
Figura 3 prezintă o vedere a interfețele de rețea/USB ale dispozitivului:

- *USB* – permite conectarea unor dispozitive USB de stocare (hard-disks, flash drives);
- *Internet* – conectarea la un broadband router;
- *Port-uri RJ45* (*ETHERNET* 1, 2, 3, 4) – utilizat pentru conectarea unor PC-uri sau a unor elemente de rețea;
- *Reset* – buton pentru resetarea la configurația implicită;

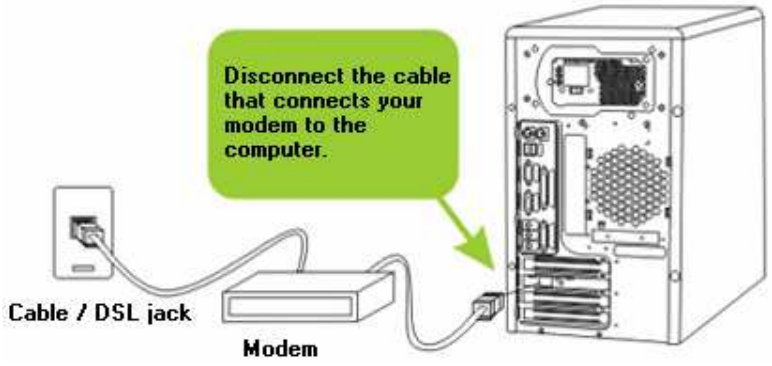
Figura 3. Interfețe de rețea/USB [1]

2.2. Conectarea şi configurarea ruterului Linksys WRT350N *Wireless-N Gigabit*

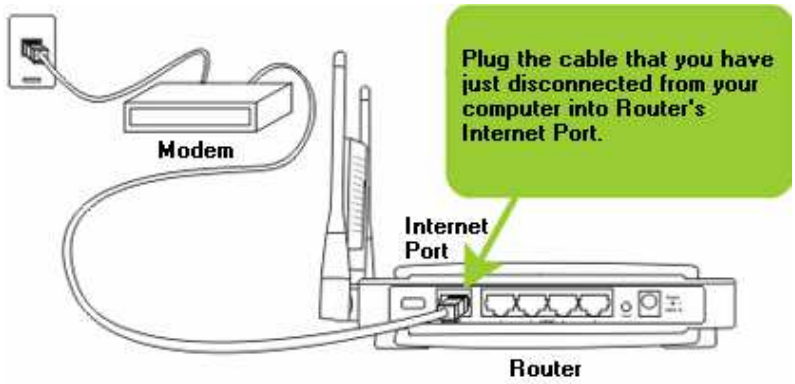
Figura 4 [1] prezintă paşii care trebuie urmați pentru conectarea ruterului la sistemul de distribuție cablat/modem. La sfârşitul pasului f, led-urile frontale vor indica activitatea ruterului.



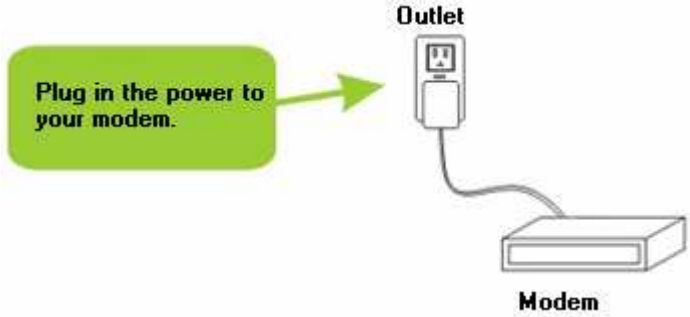
Pas a.



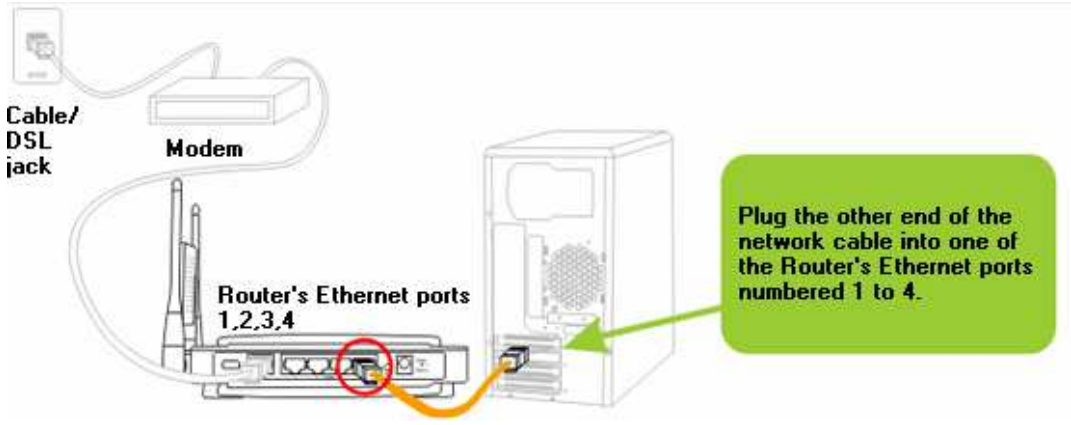
Pas b.



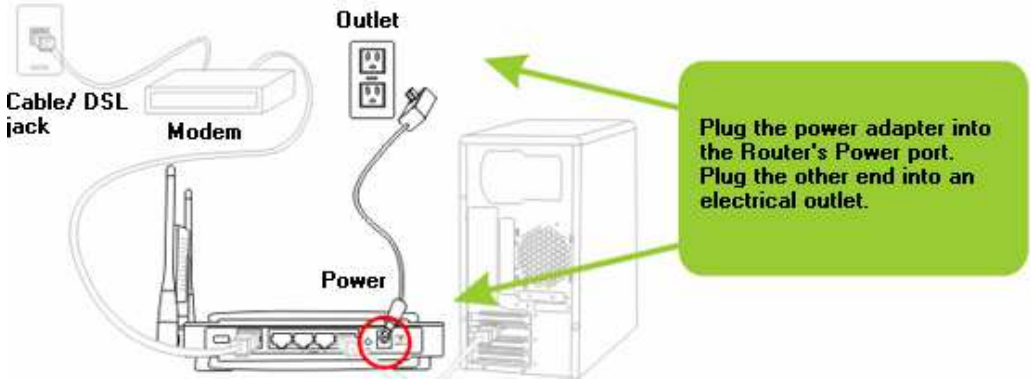
Pas c.



Pas d.



Pas e.



Pas f.

Figura 4. Conectarea ruterului wireless [1]

Configurarea ruterului Linksys WRT350N Wireless-N Gigabit se poate realiza în două moduri:

a. utilizând Setup CD-ROM-ul pe care se află un Wizzard, și care descrie modalitatea de configurare pas cu pas;

b. utilizând utilitarul web (configurare în browserul web).

Diferența principală dintre cele două modalități constă în faptul că, configurarea utilizând Setup CD-ROM-ul permite doar câteva setări de bază, pe când utilitarul web permite setarea tuturor opțiunilor disponibile. Această lucrare descrie modul de configurare bazat pe utilizarea utilitarul

web. Tabelul 1 prezintă o descriere sumară a tab-urilor principale de opțiuni:

Tab	**Funcție**
Setup	Setări conexiune Internet
Wireless	Setări conexiune wireless
Security	Setări securitate dispozitiv
Storage	Setări storage link (hard-disk, flash USB)
Access Restrictions	Setări acces Internet
Applications & Gaming	Setări acces aplicații
Administration	Setări dispozitiv
Status	Informații dispozitiv

Tabelul 1. Tab-uri de opțiuni

2.3. Configurarea utilizând Utilitarul Web

Pentru a accesa utilitarul Web (configurare utilizând browserul web), se va utiliza Internet Explorer sau Netscape Navigator, şi se va accesa http://192.168.1.1. Câmpul User nu se va completa, iar Parola implicită este *admin*.

Figura 5. Conectarea la utilitarul Web

Principalele probleme întâmpinate la accesarea ruterului sunt:

- Stația de pe care se realizează configurarea nu este setată să utilizeze serviciul DHCP (există setări de IP-uri statice);
- Nu se utilizează browserul corespunzător (IE, NN);
- Nivelul de securitate al browserului este prea ridicat, nepermițând conectarea (verificare Security Level în IE);
- Firewall-ul stației blochează accesul la serviciile http (adăugare regulă de acces sau dezactivarea temporară a firewall-ului);
- Probleme hardware (placă de rețea defectă, cablu defect, etc);

Pentru o setare de bază ruterului, se pot utiliza următoarele Tab-uri ale utilitarului:

- Setup -> Basic Setup: pentru a introduce informațiile pentru conexiunea Internet, furnizate de către ISP;
- Wireless -> Basic Wireless Settings: opțiune pentru a modifica numele rețelei şi pentru a seta un mod de securitate/parolă;
- Administration -> Management: opțiune pentru a schimba parola implicită.

În continuare se vor descrie tab-urile de opțiuni, împreună cu subopțiunile de configurare:

A. Setup

- Basic Setup: pentru a introduce informațiile pentru conexiunea Internet, furnizate de către ISP;
- DDNS: permite activarea opțiunii Dynamic Domain Name System (permite asocierea unui host fix şi a unui nume de domeniu la o adresă Internet IP dinamică);
- MAC Address Clone: opțiune pentru clonarea unei adrese MAC pe ruter;
- Advanced Routing: opțiune pentru configurații de rutare statică/dinamică;

B. Wireless

- Basic Wireless Settings: setări de bază ale rețelei wireless (nume, canal, etc);

- Wireless Security: configurarea setărilor de securitate pentru rețeaua wireless;
- Wireless MAC Filter: restricționarea accesului la rețeaua wireless prin filtrarea adreselor MAC ale stațiilor client;
- Advanced Wireless Settings: opțiune pentru configurații avansate, pentru administratorii de rețea:
    - AP Isolation: această opțiune permite izolarea clienților şi a dispozitivelor wireless din cadrul rețelei. Acestea nu vor putea comunica între ele, ci doar cu ruterul;
    - Authentication Type: opțiunea Shared Key se va selecta doar dacă receptorul şi transmițătorul utilizează cheie WEP pentru autentificare;
    - Basic Rate: ratele de date la care ruterul poate transmite;
    - Transmission Rate/N Transmission Rate: selectarea ratei de transmisie (în funcție de vitezele suportate de dispozitivele wireless);

C. Security

- Firewall: opțiune pentru configurarea firewall-ului ruterului;
- VPN Passthrough: pentru a permite/interzice unele protocoale VPN;

D. Storage

- Disk: descrie discul ataşat la ruter;
- Share: controlează accesul la partițiile discului ataşat;
- Administration: administrarea utilizatorilor/grupurilor care pot accesa partajările;
- Media Server: opțiune pentru activarea serverului media încorporat în ruter;
- FTP Server: configurarea ruterului ca server FTP local;

E. Access Restrictions

- Internet Access Policy: opțiune pentru crearea unor politici de acces Internet pentru utilizatorii locali;

F. Applications & Gaming

- Single Port Forwarding: opțiune pentru port mapping şi forwarding pentru un singur port de serviciu;
- Port Range Forwarding: pentru accesul unor servicii publice/aplicații Internet;
- Port Range Triggering: pentru urmărirea datelor ce se transmit in exterior, pentru anumite porturi;
- DMZ: zonă demilitarizată – permite unui user local acces liber către Internet.
- QoS: opțiuni de Quality of Service.

G. Administration

– opțiuni de administrare şi management ruter;

H. Status

– informații despre statusul ruterului şi a rețelei locale;

3. Aplicații practice

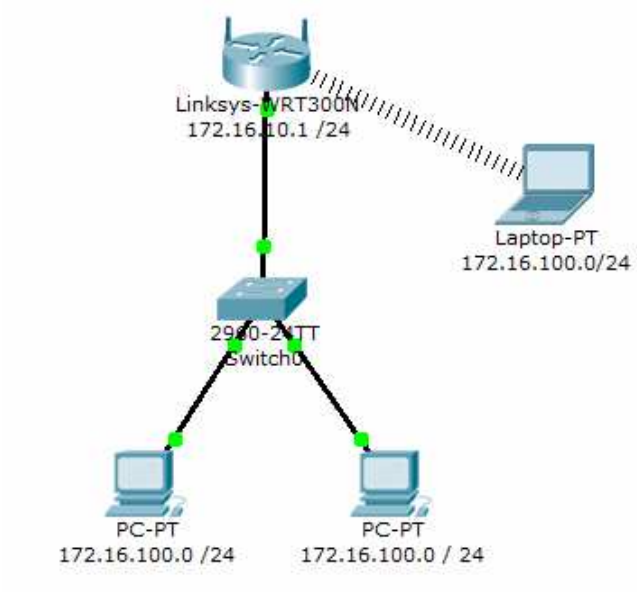
3.1. Se va conecta ruterul Linksys WRT350N Wireless-N Gigabit with Storage Link la rețeaua de test din cadrul laboratorului, conform paşilor descrişi în cadrul lucrării.

3.2 Se va configura şi se va securiza ruterul Linksys WRT350N Wireless-N Gigabit with Storage Link utilizând utilitarul Web. Se va ataşa un flash USB extern care se va partaja în rețea.

3.3 Se va testa conectivitatea la noua rețea wireless creată, prin conectarea stațiilor din cadrul laboratorului utilizând adaptoarele Linksys Wireless N USB, PCMCIA şi PCI. Pentru testare, se va utiliza utilitarul ping şi se va testa conectivitatea la Storage Link prin intermediul serviciului ftp.

3.4 Se va configura topologia fizică din figura de mai jos şi se va testa conectivitatea între dispozitive, utilizând următorii parametrii:

Dispozitiv		Adresa IP	Subnet mask	Default Gateway
Router	Internet	172.16.10.2	255.255.255.0	172.16.10.1
	Wireless	172.16.100.10	255.255.255.0	-
PCs, Laptop		172.16.100.x Dinamic (DHCP)	255.255.255.0 Dinamic (DHCP)	172.16.100.10 Dinamic (DHCP)



Dispozitiv	SSID	Canal Standard	Securizare Wireless	Parola Securizare Wireless	Parola Remote Management
Router Wireless	Wi-Fi	11	WPA2 Personal	Cisco1234	Pass1234

Bibliografie:

[1] Linksys WRT350N Wireless-N Gigabit User Manual
[2] Cisco CCNA LAN Switching and Wireless Course

VII. Configurarea rețelelor wireless: Configurări avansate

1. Obiective

Obiectivul acestui capitol este prezentarea modului de instalare şi configurare al access point-ului (AP) Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet, precum şi, configurări avansate ale router-ului Linksys WRT350N Wireless-N Gigabit. Se vor descrie principalele caracteristici ale AP-ului, modalitățile de funcționare, şi de asemenea, rolul punctelor de acces în cadrul rețelelor fără fir.

2. Considerații teoretice

2.1. Introducere

Un Access Point – punct de acces (AP) este un dispozitiv de tip half-duplex care permite dispozitivelor de comunicare fără fir conectarea la o rețea wireless. Într-o rețea cablată, echivalentul acestui dispozitiv îl reprezintă hub-ul. Un access point poate fi privit ca un hub wireless, însă cu câteva îmbunătățiri, prezentând şi capabilități de switch. Principala funcție a unui AP este funcția de bridging, direcționând traficul, fie la backbone-ul rețelei, fie înapoi în mediul fără fir. O stație client, care are o conexiune de nivel 2 cu un AP, se defineşte ca fiind asociată cu acel AP. Figura 1 prezintă o modalitate de conectare a AP-ului pentru crearea unei rețele wireless în mod infrastructură.

Un avantaj important adus rețelelor wireless, de către punctele de acces, îl reprezintă posibilitatea de Roaming pentru utilizatorii mobili. Condiția prealabilă, care trebuie îndeplinită de către AP-uri şi stațiile client, este partajarea aceluiaşi SSID şi a setărilor de securitate. Datorită faptului că AP-

ul Linksys WAP4400N suportă 802.11F (Inter-Access Point Protocol), procesul de roaming se va realiza foarte rapid.

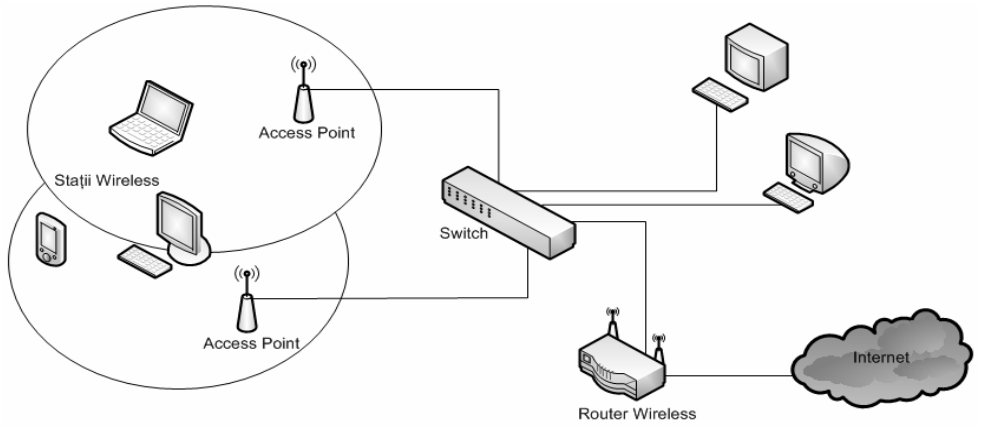


Figura 1. Exemplificarea conectării Punctelor de Acces

Punctul de acces Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet (fig. 2) este o componentă Wi-Fi care permite conectarea, în mod infrastructură, a mai multor stații fără fir la o rețea locală de calculatoare.

Figura 2. Linksys Wireless-N Access Point with Power Over Ethernet [1]

Principalele caracteristici ale dispozitivului sunt:

- Transmisie în tehnologie Wireless N (MIMO);
- Frecvență de operare: 2.4 - 2.5 GHZ;
- Suport Power over Ethernet;
- Rază mărită de acțiune;
- Rată de transfer de până la 300 Mbps;

- Standarde suportate: Draft 802.11n, 802.11g, 802.11b, 802.3, 802.3u, 802.3af (Power over Ethernet), 802.1x (Security Authentication), 802.11i - Ready (Security WPA2), 802.11e - Ready (Wireless QoS);
- DHCP Client;
- Suport Quality of Service;

2.2. Descrierea interfețelor dispozitivului

Figura 2 prezintă o vedere frontală a dispozitivului. Led-urile dispozitivului permit o diagnosticare rapidă a funcționării acestuia:

- *Power* – culoarea verde a led-ului semnifică alimentarea AP-ului prin adaptorul 12V DC;
- *PoE* – culoarea verde a led-ului semnifică alimentarea AP-ului prin cablu Ethernet;
- *Ethernet* – corespunzătoare porturilor Ethernet. Culoarea verde a led-ului semnifică conectarea la un dispozitiv 10/100 Mbps; led-ul se aprinde intermitent - semnifică faptul că AP-ul transmite/recepționează date pe acest port;
- *Wireless* – culoarea verde a led-ului semnifică conectarea la un dispozitiv wireless; led-ul se aprinde intermitent - semnifică faptul că AP-ul transmite/recepționează date;

Figura 3. Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet [1]

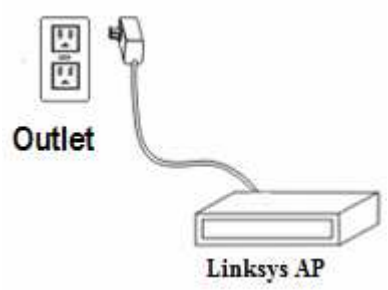
Figura 3 prezintă o vedere din spate a dispozitivului:

- *Alimentare* – alimentarea AP-ului prin adaptorul 12V DC;

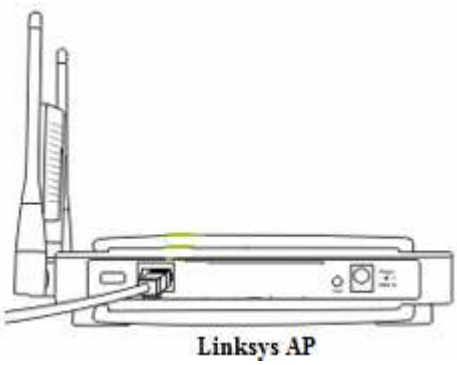
- *Port RJ45* (*ETHERNET*) – utilizat pentru conectarea unor PC-uri sau a unor elemente de rețea;
- *Reset* – buton pentru resetarea la configurația implicită;

2.3. Conectarea şi configurarea AP-ului Linksys Wireless-N Access Point with Power Over Ethernet

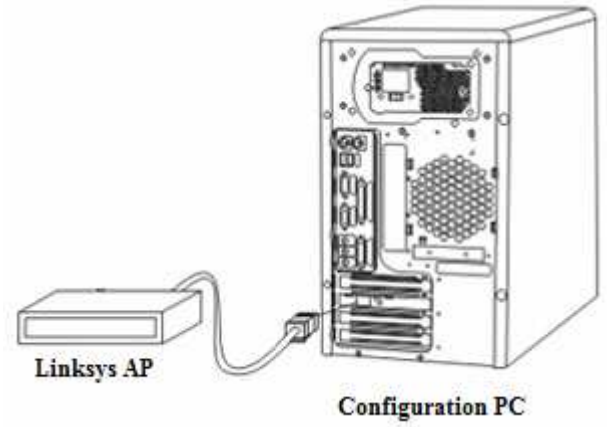
Figura 4 [1] prezintă paşii care trebuie urmați pentru conectarea AP-ului la sistemul de distribuție cablat/PC-ul pentru configurare. La sfârşitul pasului d, led-urile frontale vor indica activitatea AP.



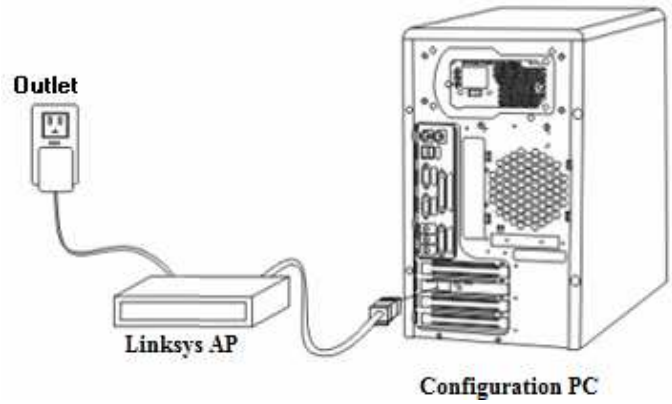
Pas a. Unplug the AP



Pas b. Conect the network cable to the AP



Pas c. Conect the network cable to the PC



Pas d. Plug the AP

Figura 4. Conectarea AP la PC [1]

Tab	Funcție
Setup	Setări generale de conexiune
Wireless	Setări conexiune wireless
Security Monitor	Setări pentru aplicația de monitorizare
Administration	Setări dispozitiv
Status	Informații dispozitiv

Tabelul 1. Tab-uri de opțiuni [1]

Punctul de acces este proiectat pentru a fi funcțional cu setările implicite, fără a fi necesară o configurare prealabilă. Însă, pentru o configurare avansată, se poate utiliza utilitarul web (configurare în browserul web), metodă ce permite setarea tuturor opțiunilor disponibile. Această lucrare descrie modul de configurare bazat pe utilizarea utilitarul web. Tabelul 1 prezintă o descriere sumară a tab-urilor principale de opțiuni:

2.4. Configurarea utilizând Utilitarul Web

Pentru a accesa utilitarul Web (configurare utilizând browserul web), se va utiliza Internet Explorer sau Netscape Navigator, şi se va accesa http://192.168.1.245. Informațiile implicite de conectare sunt:

- *User Name*: admin
- *Password*: admin.

Stația de pe care se realizează configurarea se va seta cu o adresă IP statică, din aceeaşi subrețea ca şi AP-ul (192.168.1.0/24). Dacă în rețea există un server DHCP, acesta se va configura pentru a atribui adrese IP din aceeaşi subrețea ca şi AP-ul (192.168.1.0/24).

Nu se recomandă configurarea AP-ului prin conexiune wireless, deoarece conectivitatea se poate pierde datorită modificărilor efectuate.

Figura 5. Conectarea la utilitarul Web

Principalele probleme întâmpinate la accesarea AP-ului sunt:

- Stația de pe care se realizează configurarea nu este setată să utilizeze IP-uri statice din aceeaşi subrețea cu AP-ul;
- Serverul DHCP al rețelei nu este configurat pentru a atribui adrese IP din aceeaşi subrețea ca şi AP-ul.
- Nu se utilizează browserul corespunzător (IE, NN);
- Nivelul de securitate al browserului este prea ridicat, nepermițând conectarea (verificare Security Level în IE);
- Firewall-ul stației blochează accesul la serviciile http (adăugare regulă de acces sau deactivarea temporară a firewall-ului);
- Probleme hardware (placă de rețea defectă, cablu defect, etc);

Pentru o setare de bază AP-ului, se pot utiliza următoarele Tab-uri ale utilitarului:

- Setup -> Basic Setup: pentru a introduce informațiile de rețea (adresa IP);
- Wireless -> Basic Wireless Settings: opțiune pentru a modifica numele rețelei şi pentru a seta un mod de securitate/parolă;
- Administration -> Management: opțiune pentru a schimba parola implicită.

În continuare se vor descrie tab-urile de opțiuni, împreună cu subopțiunile de configurare:

A. Setup

- Basic Setup: introducere informații legate de numele AP-ului;
    - Host Name: numele folosit pentru accesarea Utilitarului Web prin intermediul rețelei – numele cunoscut de către serverul DNS;
    - Device Name: numele folosit pentru identificarea AP-ului de către administrator în fişierele de log;
    - Network Setup: selectarea adresei IP a AP-ului, precum şi a modului de configurare (static/dinamic).
- Time: configurarea setărilor de timp. Acestea se pot realiza manual sau utilizând conexiunea cu un server NTP. Setarea corectă a acestei opțiuni va permite administratorului

determinarea cu exactitate, în cadrul fişierelor de log, a unor eventuale erori/alerte.

B. Wireless

- Basic Wireless Settings: setări de bază ale rețelei wireless (nume, canal, etc);
- Wireless Security: configurarea setărilor de securitate pentru rețeaua wireless;
- Wireless Connection Control: restricționarea accesului la rețeaua wireless prin filtrarea adreselor MAC ale stațiilor client;
- Advanced Wireless Settings: opțiune pentru configurații avansate, pentru administratorii de rețea:
    - WMM – opțiune QoS, parte a 802.11e. Permite prioritizarea traficului, prin existența a patru cozi de prioritate pentru diferite tipuri de trafic;
    - IOT Mode – permite o mai bună comunicare cu dispozitivele Linksys N;

C. Security Monitor

Permite monitorizarea rețelei wireless prin intermediul unei aplicații instalate pe PCul administratorului. Informațiile furnizate de către aplicație sunt legate de detecția şi clasificarea clienților şi a AP-urilor wireless.

- Wireless Security Monitor: activarea/dezactivarea opțiunii de monitorizare;
- Security Monitor: permite crearea unor conturi pentru utilizatorii aplicației;

D. Administration

- Management: opțiuni de administrare şi management;
- Log: permite setarea unei adrese de email, unde se vor trimite notificări legate de starea AP-ului şi selectarea evenimentelor ce vor fi transmise;
- Factory default
- Firmware Upgrade
- Reboot
- Config Management: permite salvarea/încărcarea configurației AP-ului.

E. Status

- Oferă informații despre statusul AP-ului.

2.5. Configurări avansate Linksys WRT350N *Wireless-N Gigabit Router*

2.5.1. Expunerea unor aplicații către utilizatori externi

Paşii necesari pentru expunerea unor Servere de Aplicații [2]

- Accesare utilitar Web.
- Accesare Tab Applications & Gaming -> Port Range Forwarding

Application Name	**Start and End Port**	**Protocol**	**To IP Address**	**Enabled**
FTP server	21 to 21	TCP	Adresa Server FTP (de ex. 192.168.1.5)	x
Web Server	80 to 80	Both	Adresa Web Server (de ex. 192.168.1.6)	x
Counter Strike	44000 to 44000	Both	Adresa Web Server (de ex. 192.168.1.10)	x

2.5.2. Expunerea unui PC către utilizatorii externi (DMZ)

Utilizarea acestei opțiuni (DMZ) este utilă dacă aplicațiile de pe PC-ul care se doreşte a fi expus necesită deschiderea unui număr prea mare de porturi, sau nu se cunosc cu exactitate porturile care trebuie expuse.

Se recomandă dezactivarea tuturor intrărilor de forwarding înainte de a utiliza opțiunea DMZ, deoarece opțiunea de DMZ este cea mai puțin prioritară dintre opțiunile de expunere către utilizatorii externi.

Paşii necesari pentru expunere utilizând opțiunea DMZ:

- Accessare utilitar Web.
- Accesare Tab Applications & Gaming -> Port Range Forwarding
- Dezactivarea intrărilor definite
- Accesare Tab Applications & Gaming -> DMZ
- Selectare Enable
- Selectare PC (selectarea se poate realiza utilizând adresa IP sau MAC a PC-ului)
    - după adresă IP: completare câmp Destination IP Address
    - după adresa MAC: completare câmp Destination MAC Address

2.5.3. Securizarea dispozitivului – Best Practices

Următorii paşi ar trebui urmați de către administratorul dispozitivului wireless pentru a creşte siguranța rețelei wireless:

1. modificarea SSID-ului implicit

2. dezactivarea opțiunii de SSID broadcast

3. modificarea parolei implicite pentru contul de Administrator şi utilizarea unei chei puternice

4. limitarea numărului de clienți care se pot conecta

5. utilizarea filtrelor MAC

6. modificarea periodică a parolelor utilizate

7. utilizarea unor standarde de criptare avansate / servere de autentificare

2.5.4. Ajustarea performanțelor dispozitivelor 802.11

Standardele 802.11 prezintă rate de transfer maxime de până la 300 Mbps (ex. 802.11n). Însă aceste rate de transfer maxime sunt rareori atinse datorită informațiilor adiționale adăugate de către protocoalele de

comunicaţie 802.11. Pentru a estima rata de transfer efectivă, în practică aceasta poate fi considerată ca fiind ½ din rata maximă de transfer specificată de producător.

Îmbunătăţirea performanţele reţelelor fără fir 802.11 se poate realiza prin două metode:

a. modificarea mediului fizic;

b. ajustarea parametrilor administrativi ai dispozitivelor.

Modificarea mediului fizic presupune schimbarea locaţiei punctelor de acces, înlocuirea antenelor dispozitivelor cu antene cu câştig ridicat, adăugarea unor amplificatoare etc., deci modificarea unor elemente externe.

Dispozitivele 802.11 permit, de asemenea, modificarea unor parametri administrativi pentru optimizarea utilizării resursei RF. Găsirea unor valori optime pentru aceşti parametrii presupune însă un grad ridicat de experienţă practică.

Paşii necesari pentru ajustarea parametrilor administrativi pentru ruterul Linksys WRT350N Wireless-N Gigabit Router sunt următorii:

- Accessare utilitar Web.
- Accesare Tab Wireless -> Advanced Wireless Settings

Principalii parametri administrativi ajustabili sunt: Becon Interval, DTIM Interval, Fragmentation Threshold, RTS Threshold.

<u>Becon Interval</u>

Cadrele Beacon au un rol fundamental în comunicarea în mod infrastructură. Cadrele Beacon definesc zona de acoperire a unui BSS, deoarece întreaga comunicaţie din cadrul unui BSS este trecută prin Access Point. Staţiile client vor asculta aceste cadre pentru a găsi AP-urile din zonă şi vor utiliza nivelul de putere al semnalului recepţionat pentru a monitoriza calitatea semnalului şi pentru a decide cărui AP din ESS se vor asocia. Însă

transmiterea cadrelor Beacon conduce la un consum al capacității liniei. Scăderea valorii parametrului Becon Interval conduce la creşterea fiabilității, deoarece APul se va anunța mai des, ajutând, de asemenea, nodurile mobile care îşi schimbă rapid locația. Creşterea valorii parametrului Becon Interval va conduce la o scădere a consumului dispozitivului şi la o creştere a ratei de transfer (intervalul ocupat de cadrele Beacon nu poate fi utilizat pentru transmiterea de date).

DTIM Interval

Parametrul DTIM (Delivery Traffic Indication Map) este configurat la nivelul APului şi, alături de parametrul TIM, este transmis prin cadrele Beacon. Cadrele unicast care sunt salvate în buffer sunt transmise clienților ca răspuns la o interogare din partea acestora. Pentru a recepționa cadrele broadcast sau multicast salvate în buffer, clienții sunt anuntați asupra momentului transmisiei prin parametrul DTIM. Creşterea parametrului poate conduce la o scădere a consumului dispozitivelor mobile, însă va conduce la o creştere a utilizării zonelor buffer şi la întârzieri în recepție, fapt ce poate afecta anumite aplicații cu constrângeri de timp.

Fragmentation Threshold (Prag de fragmentare)

În cadrul protocolul 802.11, cadrele mai mari decât pragul de fragmentare (implicit 2346 bytes) vor fi fragmentate. Scăderea acestui parametru poate avea un efect benefic asupra ratei de transfer într-un mediu puternic afectat de interferențe, deoarece se vor retransmite doar fragmentele pierdute din cadrul inițial. O scădere prea mare a valorii pragului va afecta rata de transfer, datorită timpului necesar confirmării fiecărui fragment retransmis, iar o creştere a valorii pragului va conduce, de asemenea la scăderea ratei de transfer datorită necesității de retransmisie a unui cadrul de dimensiuni mari. Modificarea Fragmentation Threshold se realizează, de obicei, în paralel cu modificarea parametrului RTS Threshold.

RTS Threshold (Prag RTS)

Unul din mecanismele de bază ale 802.11 este reprezentat de utilizarea cadrelor RTS/CTS. Cadrele care au dimensiunea mai mare decât Pragul

RTS trebuie supuse mecanismului RTS/CTS, pentru minimizarea interferențelor. În mod implicit acest prag are valoare de 2346 bytes. Scăderea pragului poate fi justificată de un număr mare de retransmisii de cadre sau de o rată de transfer scăzută.

3. Aplicații practice

3.1. Se conecta AP-ul Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet la rețeaua de test din cadrul laboratorului, conform paşilor descrişi în cadrul lucrării.

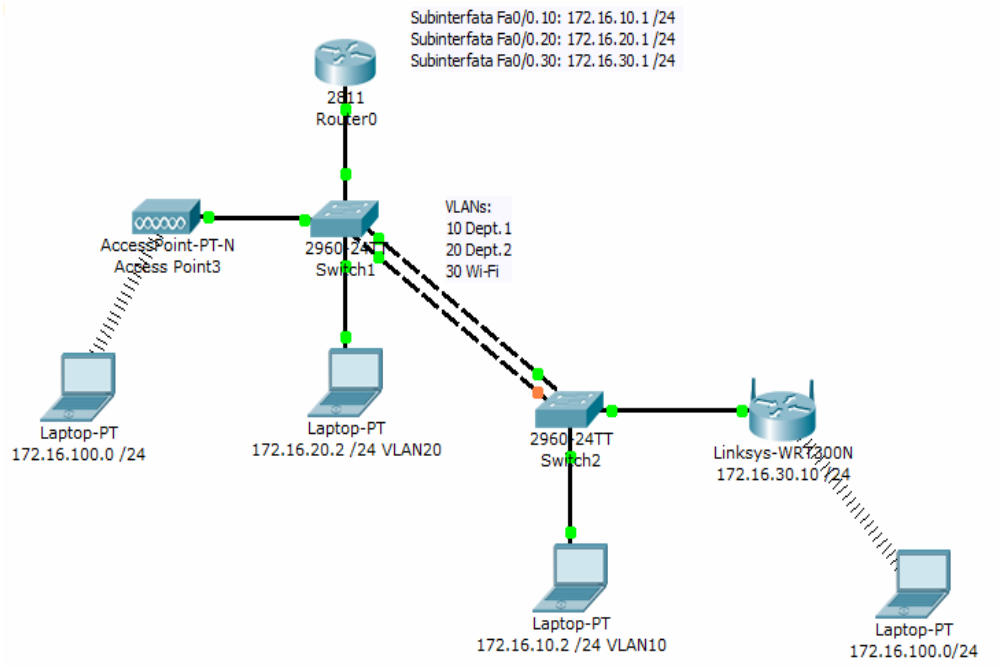
3.2 Se va configura şi se va securiza AP-ul Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet utilizând utilitarul Web.

3.3 Se va ajusta funcționarea ruterului Linksys WRT350N Wireless-N Gigabit Router conform paşilor de la punctul 2.3.

3.4 Se va testa conectivitatea la noua rețea wireless creată, prin conectarea stațiilor din cadrul laboratorului utilizând adaptoarele Linksys Wireless N USB, PCMCIA şi PCI. Pentru testare, se va utiliza utilitarul ping şi se vor testa opțiunile Security Monitor şi Log.

3.4 Se va configura topologia fizică din figura de mai jos şi se va testa conectivitatea între dispozitive, utilizând următorii parametrii:

Dispozitiv		**Adresa IP**	**Subnet mask**	**Default Gateway**
Router	Internet	172.16.10.2	255.255.255.0	172.16.10.1
	Wireless	172.16.100.10	255.255.255.0	-
PCs, Laptop		172.16.100.x Dinamic (DHCP)	255.255.255.0 Dinamic (DHCP)	172.16.100.10 Dinamic (DHCP)



Dispozitiv	SSID	Canal Standard	Securizare Wireless	Parola Securizare Wireless	Parola Remote Management
Router Wireless	Wi-Fi	11	WPA2 Personal	Cisco1234	Pass1234

Bibliografie:

[1] Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet User Manual
[2] Linksys WRT350N Wireless-N Gigabit User Manual
[3] Cisco CCNA LAN Switching and Wireless Course

VIII. Configurarea rețelelor wireless: Configurare VPN

1. Obiective

Capitolul de față îşi propune prezentarea noțiunilor de bază legate de VPN (Virtual Private Network) precum şi a protocoalelor şi a modurilor de încapsulare a datelor folosite în cadrul VPN; în partea a doua a lucrării se va configura o rețea VPN wireless între un calculator şi un router wireless.

2. Considerații teoretice

2.1. Generalități

VPN (Virtual Private Network) este o conexiune privată între două sau mai multe rețele sau calculatoare care trimit date protejate peste o rețea publică de date. Rețeaua virtuală privată oferă astfel posibilitatea utilizatorilor să acceseze rețeaua locală a companiei într-un mod sigur şi protejat, folosind o infrastructură de rețea publică, aşa cum este internetul [1].

VPN este un serviciu ce oferă securitate, conectivitate sigură peste o rețea partajată, menținând aceeaşi securitate şi aceleaşi politici de management ca şi într-o rețea privată. Clienții împart infrastructura, nefiind nevoie să folosească linii private dedicate pentru a-şi construi rețeaua.

VPN asigură traficul printr-o rețea publică utilizând criptare avansată şi tunelare pentru a proteja confidențialitatea informației, integritatea datelor şi autentificarea utilizatorilor.

Avantajele VPN sunt costul scăzut, flexibilitatea ridicată, managementul simplu şi utilizarea topologiei tunel. De asemenea folosirea VPN extinde conectivitatea geografică, reduce costurile operaționale în comparație cu rețeaua tradițională WAN, reduce timpul de tranzit şi costurile de transport

pentru utilizatorii aflați la distanță, simplifică topologia rețelei în anumite cazuri şi limitează accesul la rețeaua țintă. Prin VPN se pot integra mai multe aplicații: transfer de date, voce (voice over IP), videoconferințe. VPN oferă securitate (informațiile care circulă prin VPN sunt protejate prin diferite tehnologii de securitate, cum ar fi criptarea, autentificarea), mobilitate (angajații mobili, precum şi partenerii de afaceri, se pot conecta la rețeaua companiei într-un mod sigur, indiferent de locul în care se află), scalabilitate (atunci când apare o nevoie permanentă de angajați mobili şi conexiuni securizate cu partenerii strategici).

2.2. Tipuri de VPN

Există mai multe tipuri de rețele VPN:

2.2.1. Intranet VPN

Este un canal de comunicație privat în cadrul unei companii care poate sau nu să implice traversarea unui WAN; prin intermediul VPN de tip Intranet se pot conecta filialele sau birourile regionale la sediul central al companiei. Este dezvoltat pentru utilizatorii care au privilegii de acces la rețeaua internă a organizației, iar conexiunile prin care se realizează sunt de obicei conexiuni permanente.

2.2.2. Extranet VPN

O rețea virtuală privată de tip extranet este un canal de comunicație privat şi securizat între două sau mai multe companii ce poate implica traversarea unei rețele publice (internet) sau a unui alt WAN (Wide Area Network).

Extranet VPN realizează conexiunea între o corporație şi partenerii strategici de afaceri (distribuitori, furnizori, clienți), pentru a le permite acestora accesul sigur la o parte a rețelei interne a companiei. Diferența față de Intranet VPN este faptul că Extranet VPN permite accesul utilizatorilor din exteriorul companiei.

2.2.3. Remote acces VPN

Acestea mai sunt numite şi VPDN (Virtual Private Dial-up Network). Un client aflat la distanță care doreşte să acceseze rețeaua internă a companiei se conectează la un server local care e legat la rețeaua publică. Clientul VPN stabileşte legătura cu serverul VPN (care se află la sediul central al companiei). După stabilirea conexiunii, comunicația clientului cu rețeaua companiei peste rețeaua publică este la fel de sigură ca şi cum clientul s-ar afla în rețeaua locală internă.

O rețea virtuală poate fi stabilită la inițiativa clientului sau a unui server de acces.

În primul caz, utilizatorii de la distanță utilizează aplicații de tip client VPN pentru a stabili un tunel securizat peste rețeaua partajată a unui ISP cu compania.

În al doilea caz se utilizează un Server de Acces la Rețea (Network Access Server – NAS) de către ISP. Serverul de Acces la Rețea va stabili tunelul securizat la rețeaua privată a întreprinderii; se pot stabili sesiuni multiple inițiate de către utilizator.

După modul în care o rețea VPN se bazează pe securitatea liniei de date, rețelele virtuale pot fi clasificate în:

- Secure VPN
- Trusted VPN
- Hybrid VPN

Secure VPN

Rețelele Secure VPN au următoarele caracteristici:

- Trafic criptat şi autentificat.

- Proprietățile de securitate trebuie să fie agreate de către toate părțile dintr-un VPN (datorită faptului că orice tunel are 2 capete, administratorii de la fiecare capăt trebuie să agreeze proprietățile de autentificare).

- Nimeni din exterior nu trebuie să afecteze proprietățile de securitate.

Rețelele Secure VPN sunt utilizate pentru accesul remote, în cazul în care locația de unde se conectează utilizatorul nu poate fi controlată de administratorul de rețea.

Protocoale folosite:

- IPsec cu criptare în modurile tunel si transport. Securitatea poate fi setată manual sau cu ajutorul protocolului IKE (Intenet Key Exchange);
- IPsec în interiorul L2TP (descris in RFC 3193) – are o dezvoltare importantă pentru VPN-ul de tip remote access;
- SSL (Secure Socket Layer).

Trusted VPN

Rețelele trusted VPN au următoarele caracteristici:

- Căile de comunicație sunt specificate şi controlate de către ISP.
- De obicei este imposibil ca un client să ştie căile utilizate de către Trusted VPN deoarece rutarea traficului pe o cale sigură se face de către ISP.
- Doar provider-ul poate crea sau modifica o cale, poate schimba, introduce sau şterge datele de pe o cale VPN;
- Rutarea şi adresarea utilizate în Trusted VPN trebuiesc stabilite înainte de crearea VPN.

Tehnologii folosite: circuite ATM, circuite Frame-Relay, MPLS (Multiprotocol Label Switching).

VPN hibride

Rețelele VPN Secure asigură securitatea fără garantarea căilor; cele trusted asigură proprietățile pentru o cale, cum ar fi QoS, dar nu şi securitatea față de spionarea si modificarea datelor.

Rețelele VPN hibride combină cele două tehnologii (trusted si secure)

2.3. Componente VPN

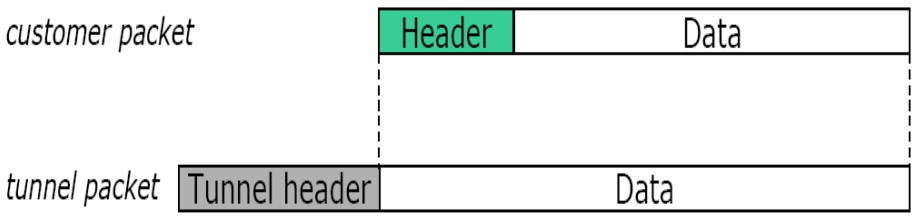
2.3.1. Tunneling

Conceptul de “tunneling” reprezintă transmiterea datelor în cadrul unei rețele publice astfel încât aceasta să nu realizeze faptul că transmisia (transportul de informații) e parte a unei rețele private.

Se realizează prin încapsularea datelor rețelei private şi crearea unui protocol care să nu permită accesul nimănui la aceste date. Tunelul se realizează între două rețele locale (LAN-LAN) sau între o rețea locală şi un client (LAN-Client), cu observația că unul din capete trebuie să fie rețea.

Tunelarea se realizează prin încapsularea unui pachet (datele sau inclusiv headerul) într-un alt pachet (se adaugă un header de tunel).

Adresele sursă şi destinatie ale headerului de tunel definesc unde se termină tunelul (terminale). Terminalele pot fi: router, gateway, NAS sau calculator cu VPN.

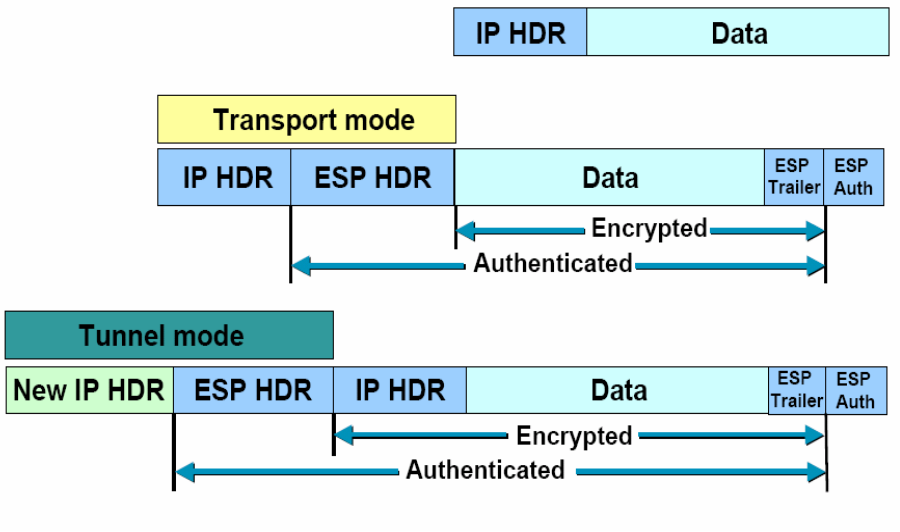


2.3.2 Protocoale folosite în VPN

IPSec

Are 2 moduri de operare: transport şi tunel.

În modul transport se încapsulează (şi se criptează) datele din pachetul IP, se adaugă headerul ESP (Encapsulation Security Protocol), după care se pune la începutul pachetului headerul IP.



În modul tunel se încapsulează şi se criptează întregul pachet IP (inclusiv headerul), apoi se adaugă headerul ESP iar în final se adaugă un nou header IP.

PPTP (Point-to-Point Tunneling Protocol)

Este un protocol de tunelare al protocolului PPP (Point-to-Point Protocol). Sunt create voluntar tunele inițializate de către client încapsulând datele în pachete IP pentru transmiterea prin internet sau prin alte rețele bazate pe protocolul TCP/IP. PPTP este uşor de implementat, dar nu este la fel de sigur ca si IPSec.

SSL (Secure Socket Layer)

SSL foloseşte certificări pentru autentificare, algoritmi de criptare cu perechi de chei publice-private (chei furnizate de serverul SSL).

SSL oferă mai multe măsuri de securitate prin numerotarea tuturor înregistrărilor cu numere de secvență în MAC-uri, prin folosirea unui mecanism de sumarizare a mesajului extins prin folosirea cheilor.

Protocolul SSL asigură o protecție bună împotriva unor tipuri cunoscute de atacuri (incluzând atacuri de tip "man in the middle") şi realizează autentificarea bidirecțională (atât a clientului cât şi a serverului).

L2F (Layer 2 Forwarding)

Protocolul a fost creat de Cisco şi foloseşte orice formă de autentificare suportată de PPP; trimite prin infrastructura rețelei sesiunile PPP (Point-to-Point) prin crearea unor tunele inițializate de către Network Access Server.

L2TP (Layer 2 Tunelling Protocol)

Este produsul parteneriatului dintre PPTP Forum, Cisco si IETF (Internet Engineering Task Force). A fost proiectat pentru a elimina limitarile IPSec pentru configurațiile CLIENT-LAN si LAN-LAN

Protocolul extinde PPP şi este compus din PPTP şi L2F (Layer 2 Forwarding); de asemenea suportă IPSec.

MPLS (MultiProtocol Label Switching)

Caracteristici:

- Folosirea nivelului 2 de către clienții VPN pentru rutarea proprie;

- Folosirea nivelului 3 de către clienții VPN ce doresc să elimine programele din rutarea lor.

GRE (Generic Route Encapsulation)

Este un protocol de încapsulare ce pune la dispoziție un framework pentru crearea pachetului de transport; include informații despre tipul pachetului încapsulat şi informații despre conexiunea dintre client si server.

2.3.3. Securitatea în VPN

Criptarea

Tehnologiile de criptare sunt extrem de eficiente în asigurarea segmentării şi virtualizării necesare pentru conectivitatea VPN şi pot fi aplicate pe oricare nivel al stivei de protocoale.

Pentru criptare se folosesc mai mulți algoritmi de criptare

- DES - Data Encryption Standard – chei pe 56 de biți
- Triple-DES – de 3 ori mai multe chei
- RSA - Rivest Shamir Adleman
- HMAC (Hash-based Message Authentication Code), MD5 (Message Digest Algorithm 5), SHA (Secure Hash Algorithm) – pentru autentificarea pachetelor
- IDEA (International Data Encryption Algorithm)

Firewall

Firewall-ul este ca o barieră între rețeaua privată şi internet; are ca scop monitorizarea parametrilor traficului din rețea şi protejarea rețelelor de accesul neautorizat.

Un firewall poate fi un software sau un echipament hardware care filtrează informațiile.

La nivel pachet, firewall-ul verifică sursa şi destinația, iar firewall-urile la nivel aplicație se comportă ca un host între rețeaua organizației şi internet.

După modul de funcționare, firewall-urile pot fi:

- *Packet filtering* – pachetele sunt analizate de un set de filtre, fiind acceptate doar cele care trec de acestea.
- *Proxy service* – informația de pe internet este primită şi trimisă prin firewall.
- *Stateful inspection* – examinează doar anumite părți ale pachetelor şi le compară cu o bază de date existentă.

Un firewall poate proteja rețeaua de: remote login, application backdoors, SMTP session hijacking, operating system bugs, atacuri de tip denial of service, e-mail bombs, viruşi, spam, macros.

Servere AAA (Authentication, Authorization and Accounting)

Sunt folosite pentru acces mai sigur într-un mediu remote-access VPN. Când o cerere de stabilire a unei conexiuni vine de la un client dial-up, aceasta este trimisă de proxy către serverul AAA care realizează autentificarea (“cine eşti”), autorizarea (“ce ați este permis”) şi accounting (“ceea ce faci”).

Prin autentificare se determină dacă emițătorul este persoana autorizată şi dacă datele au fost redirecționate sau corupte; se autentifică utilizatorul, sistemul şi datele.

Standardul curent de comunicare cu un server AAA se realizează prin Remote Authentication Dial-In User Service (RADIUS).

În funcție de tipul VPN (remote-acces, site-to-site) sunt necesare următoarele componente:

- Client software pentru fiecare utilizator remote;
- Hardware dedicat: VPN router, VPN concentrator sau Secure Pix Firewall;
- NAS(Network Access Server) folosit de ISP pentru accesul remote-user.
- Rețea VPN şi centru de management al politicilor.

3. Aplicații practice

3.1. Folosind routere wireless se pot implementa următoarele tipuri de VPN:

Router la router (LAN-LAN)

Un utilizator poate folosi conexiunea obişnuită de internet şi un router wireless pentru a stabili o rețea virtuală spre un alt router VPN; routerul utilizatorului va trebui să aibă aceleasi setări pentru VPN ca şi routerul la care se va conecta. La stabilirea rețelei virtuale cele două routere vor crea un tunel VPN, folosind criptarea datelor. Deoarece rețeaua virtuală este conectată prin internet, nu conteaza distanță la care se află routerele.

Calculator la router (CLIENT-LAN)

Un utilizator mobil se poate conecta printr-un modem la routerul VPN; dacă pe calculatorul utilizatorului mobil este instalat clientul de VPN, iar adresa IP a calculatorului este cea din rețeaua unde este conectat, calculatorul utilizatorului mobil se comportă ca şi cum ar fi conectat direct la rețeaua unde este routerul VPN, cu toate facilitățile oferite de rețeaua securizată; deoarece VPN foloseşte legătura la internet, distanța între echipamente nu are importanță.

În continuare se va stabili o rețea VPN şi se va configura un canal securizat de comunicație în cadrul acestei rețele private între două echipamente wireless (un calculator şi un router).

Programul pentru instalarea VPN funcționează cu un router cu 4 porturi gigabit configurat pentru a accepta conexiuni VPN. Pentru configurarea setărilor clientului VPN pentru router se vor efectua următorii paşi:

1. Se selectează tab-ul VPN
2. Se selectează tab-ul „Conturi client VPN”(VPN Client Accounts)
3. Se introduce numele utilizatorului şi parola (inclusiv reconfirmarea parolei)
4. Se selectează butonul „Add/Save”
5. Se selectează căsuța „Active” pentru clientul VPN nr. 1
6. Se salveaza setările (butonul „Save Settings”)

Instalarea programului pentru configurarea VPN:

Instalare de pe CD-ROM:

1. Se selectează „Install Quick VPN”

Descărcarea fişierelor şi instalarea de pe internet:

1. Se accesează pagina www.linksys.com
2. Se selectează „Business Solutions”, apoi „Router/VPN Solutions”, apoi „RSV4000”
3. În tab-ul „More information” se selectează „Linksys Quick VPN Utility”
4. Se salvează fişierul .zip pe calculator şi se despachetează arhiva

5. Se lansează fisierul executabil şi se urmăresc instrucțiunile de pe ecran; după instalare se trece la configurare

Configurarea VPN folosind programul „Linksys QuickVPN”

1. Se deschide programul de configurare (care tocmai a fost instalat)
2. Se foloseşte un nume pentru profil, apoi se introduce numele utilizator şi parola atribuită
3. Câmpul „Server address” se completează cu adresa IP sau numele de domeniu al routerului VPN şi apoi se salvează profilul; se pot seta mai multe profiluri dacă se doreşte stabilirea de tuneluri cu mai multe site-uri; doar un singur tunel poate fi activ la un moment dat
4. Se selectează butonul „Connect” (vor apare ferestre care indică stabilirea conexiunii, activarea politicilor, verificarea rețelei, după care la realizarea conexiunii va apare ecranul de stare, iar icon-ul QuickVPN va deveni verde şi va afişa adresa IP a capătului tunelului precum şi alte informații.
5. Pentru terminarea conexiunii se selectează butonul „Disconnect”

Configurarea unui tunel IPSec între două routere

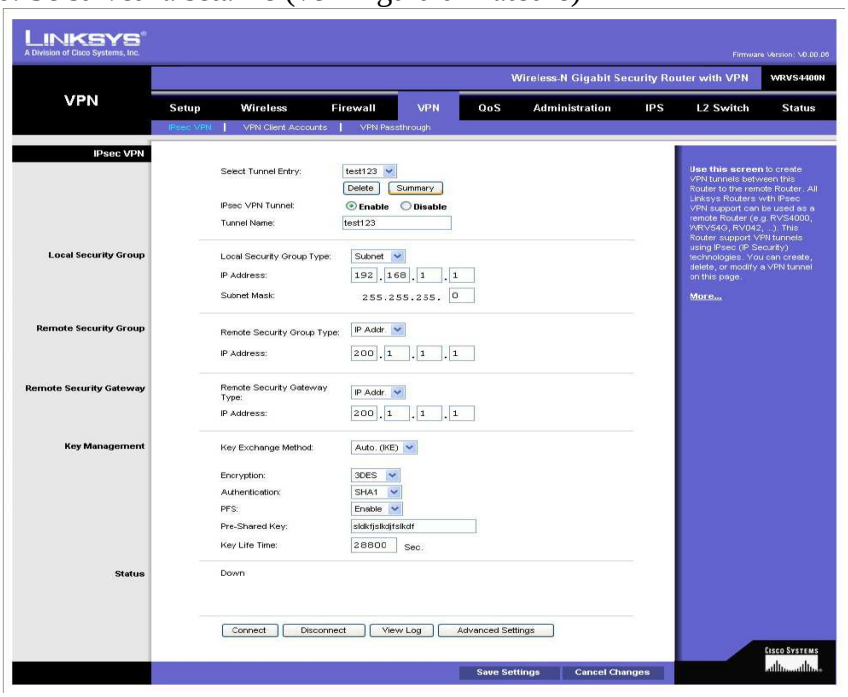
Sunt necesare două calculatoare pentru a testa tunelul; topologia între cele două routere (prin internet) poate fi vazută ca o legătură între cele două calculatoare; ca şi echipamente este nevoie de cele două calculatoare şi de două routere conectate la internet.

Configurarea setărilor VPN pentru routere

Configurarea routerului 1

1. Se lansează un browser de pe stația 1

2. Se introduce adresa IP a routerului 1 (implicit aceasta este 192.168.1.1)
3. Se introduce numele utilizator şi parola
4. Se selectează tab-ul „VPN”, apoi „IPSec VPN”
5. La setarea „VPN Tunnel” se selectează „Enabled”
6. Se dă un nume tunelului respectiv
7. La „Local secure group” se selectează „Subnet” şi se introduce adresa IP şi masca pentru routerul 1
8. La „Remote secure group” se selectează „Subnet” şi se introduce adresa IP şi masca pentru routerul 2 (subrețeaua routerului 2 trebuie să fie diferită de cea a routerului 1)
9. Pentru „Remote secure gateway” se selectează „IP addr” şi se introduce adresa IP pentru WAN a routerului 2
10. Se salvează setările (vezi figura următoare)

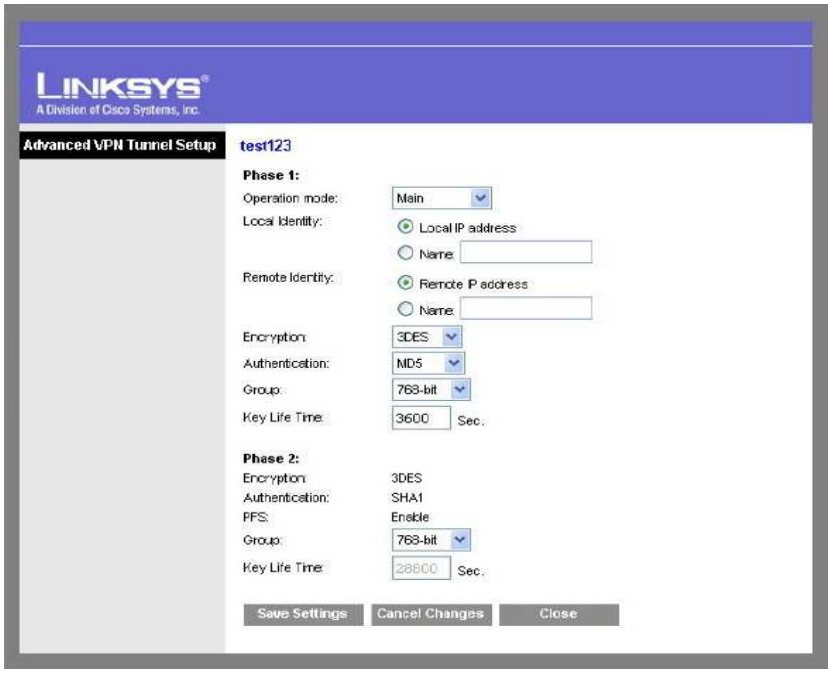


Configurarea setărilor pentru gestionarea cheilor

Configurarea routerelor (ambele routere se configurează parcurgând următorii paşi):

1. Din ecranul „IPSec VPN” se selectează „3DES” din meniul „Encryption”

2. Se selectează apoi „MD5” din meniul „Authentication”
3. Se păstrează metoda implicită de schimare a cheilor (Key Exchange) la valoarea „Auto (IKE)”
4. Se selectează „Pre-shared key” şi se introduce un şir de caractere
5. De la setările „PFS” se selectează „Enabled”
6. Se pot face şi setări mai avansate de la butonul „Advanced Settings”; apoi se salvează configurația (butonul „Save settings”) şi se trece la configurarea routerului 2 parcurgând aceiaşi paşi ca la configurarea routerului 1.
7. În fereastra de configurare avansată (Advanced VPN Tunnel setup) se păstrează modul de operare implicit („Main”)
8. Pentru faza 1 se selectează „3DES” din meniul „Encryption”, apoi „MD5” din meniul „Authentication”
9. Se selectează „1024-bit” din meniul „Group”, apoi se setează câmpul „Key life time” la valoarea 3600
10. Pentru faza 2, valorile pentru câmpurile „Encryption”, „Authentication” şi PFS” sunt cele setate în ecranul „VPN”; apoi se selectează „1024-bit” în meniul „Group”
11. Se păstrează valoarea implicită a timpului de viață a cheii („Key life time) la 28800 şi se salvează setările atât cele din ecranul de configurare avansată a tunelului cât şi cele din ecranul „IPSec VPN” (vezi figura următoare)



Configurarea stațiilor:

1. Ambele calculatoare se setează pentru a primi adresa DHCP
2. Se verifică cu comanda „ping” conectivitatea între ele

Dacă aceasta există, acest lucru înseamnă că tunelul VPN este configurat corect. Se pot testa apoi alți algoritmi de criptare, autentificare sau alte setări pentru gestionarea cheilor.

Bibliografie:

[1] Retele Virtuale Private,
http://www.netaccess.ro/retele_virtuale_private.html
[2] Cisco CCNA Security courses
[3] Wireless-N Gigabit Security with VPN WRVS4400N User manual

IX. Securitatea în rețele wireless şi mobile

1. Obiective

Capitolul de față îşi propune prezentarea noțiunilor de bază legate de ACL (Access Control List), IPS (Intrusion Prevention System), firewall, protocoalele de securizare WEP (Wired Equivalent Privacy), WPA (WiFi Protected Access), WPA2, Kerberos.

2. Considerații teoretice

2.1. Generalități

În rețelele wireless în care semnalul se propagă în mod broadcast este dificil să se urmărească unde ajunge semnalul, acesta putând parcurge o distantă de câteva zeci de metri de punctul de acces. Un hacker care caută conexiuni nesecurizate poate intra într-o rețea chiar şi dintr-o maşină parcată pe stradă. Acest lucru nu înseamnă că nu trebuiesc folosite rețelele wireless, ci doar că trebuie să se ia masuri de precauție de bază pentru a nu permite atacatorilor să ajungă la informații personale. Dintre aceste măsuri amintim:

- Schimbarea ID-ului de sistem: dispozitivele wireless au un ID implicit numit Service Set Identifier (SSID); acesta este bine să fie schimbat de la cel implicit, astfel încât echipamentul să nu fie uşor de găsit.

- Dezactivarea broadcastingului identificatorului (Disable SSID broadcast): deoarece utilizatorii care au drepturi în rețea cunosc acest identificator acesta nu trebuie să fie pus în regim broadcast.

- Folosirea criptării: WEP – (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) sunt protocoale ce criptează datele astfel încât doar destinatarul să poată să le citească. Dacă este posibil trebuie folosită criptarea WPA deoarece aceasta este mai sigură decât

criptarea WEP, chiar dacă şi WPA poate fi expus atacurilor de tip DoS (Denial of Service).

- Restricționarea traficului nenecesar: multe rețele cablate sau fără fir au firewall-uri predefinite. Aceste firewall-uri nu sunt printre cele mai avansate dar ajută la crearea unei zone relativ sigure.

- Schimbarea parolei implicite de administrare: acest lucru ar trebui făcut pe toate dispozitivele hardware şi software, parolele implicite fiind uşor de găsit deoarece mulți utilizatori nu le schimbă şi sunt primele pe care hackerii le încearcă.

- Folosirea update-urilor pe calculator. Calculatoarele necesită firewall-uri instalate precum şi programe antivirus care trebuiesc sa aibă semnăturile de viruşi la zi.

2.1.1 WEP (Wired Equivalent Privacy)

Este un protocol de securitate standard pentru rețelele de tip 802.11. A fost introdus în 1997 şi a fost înlocuit de WPA şi WPA2. Metoda de autentificare este destul de slabă, motiv pentru care acest protocol a fost înlocuit. WEP are câteva probleme de securitate care pot compromite rețeaua wireless:

- Atacuri pasive pentru decriptarea traficului – se bazează pe analize statistice
- Atacuri active pentru introducerea de trafic nou de pe stațiile mobile neautorizate
- Atacuri active pentru decriptarea traficului

Cea mai mare problemă apare când utilizatorul nu foloseşte nici măcar securitatea WEP; chiar dacă este un protocol mai slab de securitate este mai bun decât nimic.

O altă problemă la folosirea protocolului WEP o constituie faptul că utilizatorii uită să schimbe cheile în mod periodic. Cu mulți utilizatori într-o rețea fără fir, partajarea aceleiaşi chei pentru perioade mari de timp este o mare vulnerabilitate a securității. WEP foloseşte parole care se introduc manual la ambele capete (chei pre-partajate – preshared); WEP foloseşte

algoritmul de criptare RC4 specificând o cheie pe 40 biți care a fost ulterior mărită la 104 biți.

2.1.2. WPA şi WPA2 (Wi-Fi Protected Access)

WPA este un protocol de securitate pentru rețelele 802.11 care a fost dezvoltat pentru a înlocui WEP şi respectă standardele 802.11.i. WPA şi WPA2 folosesc o ierarhie de chei care generează chei noi de criptare de fiecare dată când un dispozitiv mobil se conectează la un punct de acces. Protocoalele EAP (Extensive Authentication Protocol) şi RADIUS (Remote Authentication Dial-in User Service) se folosesc pentru o autentificare mai puternică. Un server RADIUS oferă generarea automată a cheilor precum şi autentificarea. Pentru utilizatorii care nu au un server de autentificare, WPA poate fi folosit în modul cheilor pre-partajate (Preshared key – PSK) care necesită ca o cheie secretă să fie introdusă manual atât pe Access Point cât şi pe fiecare calculator. Din cheia secretă se vor genera ulterior cheile de criptare.

WPA2 foloseşte protocolul de criptare AES-CCMP (AES-Counter Mode CBC-MAC Protocol), protocol care este mai sigur şi care a fost proiectat special pentru rețelele wireless. Dispozitivele care folosesc modul WPA2 nu mai sunt compatibile cu cele care folosesc WEP.

2.1.3. Kerberos

Kerberos este o metodă sigură pentru autentificarea unei cereri de servicii într-o rețea de calculatoare. A fost dezvoltat de Athena Project de la MIT (Massachusetts Institute of Technology).

Kerberos permite utilizatorului să ceară un tichet criptat de la un proces de autentificare care poate fi folosit pentru a cere anumite servicii de la un server. Parola utilizatorului nu trebuie să treacă prin rețea. Kerberos verifică parolele o singură dată. Când utilizatorul se conectează la un sistem Kerberos, parola este criptată şi trimisă serviciului de autentificare din centrul de distribuție a cheilor (KDC – Key Distribution Center). Dacă

autentificarea are loc cu succes KDC generează un tichet care este trimis înapoi utilizatorului. De fiecare dată când utilizatorul doreşte să acceseze un serviciu se oferă tichetul master centrului de distribuțiilor a cheilor pentru a obține un tichet serviciu pentru serviciul respectiv. Această metodă face parolele mai sigure prin trimiterea lor doar o dată la logare.

2.1.4. IPS (Intrusion Prevention System)

IPS este o tehnologie avansată pentru a proteja rețeaua de atacuri. Se foloseşte în combinație cu firewall, liste de access bazate pe IP, NAPT (Network Address Port Translation) şi rețele virtuale (VPN) pentru a obține o securitate cât mai mare. IPS funcționează oferind detecție în timp real. Un router wireless securizat filtrează în mod activ şi ignoră pachetele TCP, UDP, ICMP şi poate termina conexiunile TCP. Acest lucru protejează stațiile şi serverele care folosesc sisteme de operare diferite de atacuri în rețea.

IPS nu poate totuşi să prevină atacurile generate de ataşamentele la e-mailuri.

Controlul protocoalelor P2P (peer to peer) şi IM (Instant Messaging) permite administatorului de rețea să nu permită utilizatorilor să acceseze aceste protocoale pentru a comunica pe internet. Administratorul va putea stabili politicile companiei privind modul în care utilizatorii folosesc internetul. Partea importantă a unui IPS este fişierul cu semnături, acesta fiind similar cu fişierul de definiții pentru viruşi al unui program antivirus.

IPS foloseşte acest fişier pentru a vedea dacă anumite pachete care sosesc la router se potrivesc cu un anumit set de reguli. De regulă un router echipat cu un fişier de semnături versiunea 1.1.4. poate să accepte un set de 1048 de reguli din următoarele categorii: DoS, Buffer Overflow, cal troian, P2P, Instant Messaging, viruşi.

2.1.5. Liste de control al accesului (ACL – Access Control List)

ACL reprezintă un set de reguli asociate cu un fişer, director sau resursă de rețea care definesc permisiunile pe care utilizatorii, grupurile, procesele sau dispozitivele le au pentru a accesa rețeaua. O lista de control al accesului este un tabel care indică sistemului de operare ce reguli de acces are fiecare utilizator asupra anumitui obiect din sistem, cum ar fi un director sau un fişier individual. Fiecare obiect are un atribut de securitate pentru a identifica accesul asupra lui. Lista conține intrări pentru fiecare utilizator privind privilegiile de acces. Privilegiile cele mai întâlnite permit posibilitatea de a citi un fişier sau a fişierelor dintr-un director, de a scrie un fişier, de a executa un fişier. Sistemele de operare folosesc liste de control al accesului, acestea fiind implementate diferit în fiecare sistem de operare.

La nivelul filtrării traficului listele de acces pot specifica anumite adrese sau anumite protocoale pe care se poate restricționa traficul în funcție de sensul specificat (in sau out) şi se aplică de regulă pe interfețele routerelor.

2.1.6. Firewall (Stateful Packet Inspection)

În literatura de specialitate, în diverse standarde şi referințe bibliografice au fost identificate o multitudine de definiții ale conceptului. Câteva definiții reprezentative ale conceptului de *firewall* sunt: un firewall este un agent care îngrădeşte traficul de rețea într-un anumit mod, blocând traficul pe care îl consideră nepotrivit şi/sau periculos; un firewall este un sistem sau un grup de sisteme care aplică o politică de control al accesului între două rețele; un firewall creează o barieră prin care traficul, în fiecare direcție, trebuie să treacă. O politică de securitate a firewall-ului va decide care tip de trafic este autorizat să treacă în fiecare direcție.

Pe baza acestor definiții putem extrage câteva caracteristici generale, pe care un sistem firewall trebuie sa le încorporeze şi anume:

- traficul unei rețele, indiferent de direcție (interior <–> exterior) trebuie sa treacă prin firewall;

- doar traficul autorizat poate trece prin firewall;
- firewall-ul implementează politici de securitate;
- firewall-ul permite monitorizarea traficului.

Patru tehnici generale pe care un firewall le utilizează, pentru controlul accesului, sunt:

- *controlul serviciului* – determină tipurile de servicii Internet care pot fi accesate, filtrarea lor putându-se realiza pe baza adreselor IP, a numărului de port, prin utilizarea unor aplicații proxy care vor interpreta cererile serviciilor, înainte de a le înainta;
- *controlul direcției* - determină direcția pe care un anumit tip de serviciu are acces prin firewall;
- *controlul utilizatorilor* – controlează accesul utilizatorilor interni ai rețelei la anumite tipuri de servicii; pentru utilizatorii externi este necesară implementarea unor tehnici de autentificare securizată;
- *controlul comportamentului* – controlează modul în care anumite servicii sunt folosite.

Trei tipuri principale de firewall-uri sunt descrise în literatura de specialitate: filtre de pachete, proxy-uri la nivel aplicație şi filtre bazate pe inspecția de tip statefull a pachetelor.

Filtru de pachete: Acest tip de sistem firewall se bazează pe aplicarea unui set de reguli asupra tuturor pachetelor IP care sunt recepționate sau transmise. Setul de reguli se bazează pe verificarea informațiilor conținute în cadrul pachetelor şi aplicarea unei politici de tip discard/forward.

Proxy la nivel aplicație. Acest tip de firewall presupune existența unei entități intermediare, care va prelua cererile clienților, le va procesa şi le va înainta în numele clientului către hosturile remote. Proxy-ul va respinge acele cereri de servicii pentru care nu există reguli, sau care încalcă regulile definite.

Avantajul acestei metode este reprezentat de nivelul de izolare introdus pentru clienți, față de exteriorul rețelei. Astfel, stațiile clienților îşi vor păstra anominatul, deoarece toate cererile acestora vor fi prelucrate prin intermediul proxy-ului. Aceasta este o măsură pentru creşterea securității clienților rețelei. Un dezavantaj al acestui sistem de firewall îl reprezintă overheadul de procesare introdus pe fiecare conexiune

Inspecția de tip statefull a pachetelor. Inspecția de tip statefull a pachetelor aduce îmbunatățiri de securitate filtrelor de pachete, fără a introduce în rețea o încărcare de procesare care să conducă la scăderea vitezei de transmisie. Acest tip de filtru va păstra o evidență a sesiunilor de rețea active. De asemenea, se utilizează timeout-uri configurabile pentru eliminarea, din evidență, a sesiunilor inactive.

Pachetele ICMP sunt folosite pentru a raporta informații legate de starea rețelei. Însă pachetele ICMP pot fi utilizate de utilizatorii externi pentru a afla topologia rețelei interne, sau pentru a încerca atacuri de tip DoS (Denial Of Service). Pentru evitarea acestor probleme, ruterele vor păstra o tabelă cu cererile ICMP care sunt originare din interiorul rețelei private, pentru a putea face o potrivire cu răspunsurile ICMP care vor sosi din exteriorul rețelei. Astfel, doar pachetele ICMP care au un corespondent în tabela ruterului vor fi permise.

3. Aplicații practice

În continuare se vor configura elemente legate de securitatea rețelelor wireless (configurarea unui firewall, crearea de liste de acces, configurarea unui IPS).

Se va începe prin conectarea stației la routerul wireless. Acest lucru se va face de preferat pe un port cu cablu sau (deşi nu este recomandat) se poate realiza conexiunea şi fără fir. Se va deschide interfața web de configurare a routerului aastfel: se va lansa un browser şi se va introduce adresa routerului (192.168.1.1). După autentificarea utilizatorului (nume şi parolă – userul inițial este „admin” iar parola implicită este tot „admin”).

În fereastra de configurare vor apare nouă taburi principale: setup, wireless, firewall, VPN, QoS, Administration, IPS, Layer 2 Switch şi status. Dintre acestea le detaliem pe cele folosite în acest laborator.

Firewall

Tabul „firewall” se foloseşte pentru configurarea de bază a setărilor firewall-ului, liste de acces IP şi NAPT (Network Address Port Translation) pentru securitatea rețelei.

- Setări de bază (Basic settings). Aici se configurează setăle de bază ale firewall-ului.

- Liste de acces bazate pe IP (IP Based ACL). Se definesc listele de acces bazate pe IP pentru a bloca anumite hosturi, rețele sau anumite protocoale (servicii).

- Politica de acces la internet (Internet access policy). Din acest ecran se pot stabili reguli pentru a permite blocarea sau accesul din router spre anumite adresa.

- Single port forwarding. Aici se pot seta servicii publice sau alte aplicații Internet specializate pe un singur port de rețea.

- Port range forwarding. Se floseşte pentru setarea serviciilor publice sau a altor aplicații specializate din rețea pe un anumit domeniu de porturi.

Configurarea detaliată a firewall-ului:

- Firewall SPI (Stateful packet inspection). La activarea acestei opțiuni routerul va efectua o inspecție mai amănunțită a pachetelor asupra întregului trafic ce trece prin router şi va ignora toate pachetele care nu urmăresc comportamentul predefinit.

- Protecție DoS – Denial of service (DoS) protection. La activare routerul va preveni atacurile DoS care provin din Internet.

- Blocarea cererilor WAN (Block WAN request). La activare routerul va ignora cererile „ping” din exteriorul rețelei.

- Configurare de la distanță (Remote management). La activarea opțiunii routerul va permite configurarea sa de la distanță (implicit opțiunea este dezactivată).

- HTTPS. Această opțiune se folosește la configurarea la distanță. Prin activarea opțiunii, pagina de configurare a routerului va putea fi accesată doar folosind HTTPS (HTTP Secure) în loc de HTTP; se vor folosi algoritmi de criptare SSL (Secure Socket Layer).

- Trecerea traficului multicast (Multicast pass through). Prin activarea acestei opțiuni routerul va permite traficului multicast să intre în rețeaua locală dinspre Internet.

- MTU (Maximum Transmission Unit). Se setează valoarea maximă a pachetelor la nivel IP manual sau automat. MTU la Ethernet este 1500 octeți. Implicit este „auto”.

- Restricționarea componentelor web (restrict web features). Se selectează componentele din paginile web care trebuie să fie restricționate, de exemplu cookies, controale activex, java.

IPS (Intrusion Prevention System)

Se va folosi acest ecran pentru configurări avansate ale sistemului de prevenire a intruziunilor din router. Routerul are încorporat un sistem de prevenire a intruziunilor. IPS se poate folosi împreună cu firewall, liste de acces, rețele virtuale pentru a obține securitate maximă.

- Configurare (Configure). Porneşte sau opreşte funcționarea IPS.

- P2P/IM (Peer to Peer sau Instant Messaging). Permite sau blochează traficul specific rețelelor peer to peer sau aplicațiile de tip Instant Messaging.

- Rapoarte (Report). Se pot vizualiza rapoarte despre traficul din rețea şi atacuri.

- Informații (Information). Se afişează versiunea fişierului de semnături al sistemului IPS.

- În continuare se descriu parametrii folosiți la configurarea IPS.

- Funcționarea IPS (IPS Function). Se poate activa sau dezactiva funcționarea IPS.

- Detectarea anormală (Abnormally detection). Se pot configura opțiuni pentru HTTP, FTP, Telnet, RPC (Remote Procedure Call), toate acestea putând fi subiectul atacurilor pe protocoalele respective. Implicit setăile lor sunt inactive (Disable).

- Butonul de actualizare a semnăturilor ajută la o protecție mai bună, fişierul de semnături IPS fiind actualizat la câteva zile. Acest fişier trebuie descărcat de pe pagina www.lynksys.com folosind butonul „Browse”, apoi cu butonul „Update” se va actualiza fişierul.

Ecranul de configurare pentru P2P/IM (Peer to Peer, respectiv Instant Messaging) permite administratorului de sistem să stabilează politici pentru folosirea aplicațiilor de tip P2P sau de tip IM. Când utilizatorii descarcă fişiere folosind programe P2P lățimea de bandă a portului WAN este complet folosită. Se poate permite blocarea anumitor aplicații de tip P2P. Folosirea programelor de tip Instant Messsenger poate fi blocată.

Ecranul „Rapoarte (Report)” oferă informații despre starea rețelei, inclusiv traficul în rețea şi atacurile întâlnite, informațiile sunt şi sub formă de diagrame sau tabele.

DMZ (Demilitarized Zone)

Ecranul DMZ permite ca o stație locală să fie expusă spre Internet pentru folosirea serviciilor cu un anumit scop, cum ar fi videoconferințe. Opțiunea „DMZ hosting” trimite traficul simultan spre toate porturile unei stații specificate spre deosebire de „Port range forwarding” care trimite traficul spre maxim 10 porturi.

- Activare (Enable). Se foloseşte pentru pornirea sau oprirea componentei DMZ.

- DMZ host IP address. Se introduce adresa stației care va fi expusă în zona demilitarizată.

Securitate wireless (Wireless Security)

- Modul de securitate (Security mode). Permite alegerea modului de securitate folosit: WPA personal, WPA2 personal, WPA2 mixt, WPA enterprise, WPS2 enterprise etc.

- Izolarea stațiilor din acelaşi SSID (Wireless isolation within SSID). Când opțiunea este dezactivată, calculatoarele wireless care sunt asociate cu acelaşi identificator de rețea (SSID) se pot vedea una pe cealaltă şi pot transfera fişiere între ele. Prin activarea opțiunii stațiile nu vor putea să se vadă una pe cealaltă.

WPA Personal

- Algoritmi WPA (WPA Algorithms). Se poate selecta algoritmul de criptare folosit de WPA: TKIP sau AES.

- Cheia partajată WPA (WPA shared key). Se introduce o cheie de 8-63 de caractere.

- Timpul de reînoire a cheii (Time renewal key). Se introduce o valoare de timp care specifică routerului cât de des se schimbă cheia de criptare (implicit 3600 sec).

WPA2 Personal

- Algoritmi WPA: WPA2 foloseşte AES pentru criptarea datelor. Restul configurărilor sunt aceleaşi ca la WPA-Personal.

WPA Enterprise

Se poate folosi WPA împreună cu un server RADIUS pentru autentificarea clienților (dacă acesta este disponibil). Se vor configura următorii parametrii:

- Adresa IP a serverului RADIUS (RADIUS server IP address).

- Portul serverului RADIUS (RADIUS Server port).

- Algoritmul WPA (WPA Algorithms). WPA oferă două metode de criptare: TKIP sau AES. Se selectează algoritmul WPA folosit (implicit este TKIP).

- Cheia secretă partajată (Shared Secret). Se introduce cheia secretă folosită de routerul wireless şi serverul RADIUS.

- Timpul de reinoire a cheii se configurează ca în cazul metodelor de mai sus.

WPA2 Enterprise

Funcționează în acelaşi mod cu WPA Enterprise (WPA2 foloseşte tot timpul AES pentru criptarea datelor.

WPA2 Enterprise Mixed

Acest mod de securitate permite trecere de la WPA Enterprise la WPA2 Enterprise. Pot să existe stații care folosesc WPA Enterprise sau stații care folosesc WPA2 Enterprise. Routerul va alege automat algoritmul de criptare folosit de fiecare stație. Semnificația parametrilor este în general aceeaşi ca şi în cazul algoritmilor precedenți.

WEP

Acest mod de securitate nu este recomandat datorită protecției mai puțin sigure. Utilizatorii sunt îndemnați să folosească WPA sau WPA2.

- Tipul autentificării (Authentication type). Se alege tipul de autentificare 802.11: sistem deschis (Open system) sau cheie partajată (Shared key).

- Cheia transmisă implicită (Default Transmit key). Se selectează cheia folosită pentru criptarea datelor.

- Criptarea WEP (WEP Encryption). Se alege nivelul de criptare WEP: 64 biți sau 128 biți).

- Parolă (Passphrase). Se foloseşte când se doreşte generarea cheilor WEP folosind o parolă de criptare.

Liste de control al accesului bazate pe IP – IP based ACL (Access Control List)

Ecranul arată un sumar al configurării listelor de acces bazate pe IP. Listele de acces sunt folosite pentru a restricționa traficul prin router atât spre exterior cât şi spre interior. Există două metode de restricționare a accesului: se pot bloca diferite tipuri de trafic conform definițiilor din listele de acces sau se poate permite doar un anumit tip de trafic (politici de specificare a ceea ce e permis şi implicit interzicerea restului traficului, sau specificarea traficului interzis şi implicti acceptare restului traficului).

Regulile din listele de acces vor fi citite conform cu prioritatea lor. Listele de acces sunt folosite cu precauție. Există două liste de acces care nu pot fi şterse. Prima regulă este să permită tot traficul din rețeaua intenă spre router. A doua regulă va permite tot traficul venind dinspre portul exterior (WAN). Aceste două reguli au cea mai mică priritate, deci fără a adăuga reguli de restricționare a traficului, tot traficul va fi permis prin router în ambele direcții.

Regula va fi activată când se bifează butonul de activare (Enable) şi când se vor potrivi data şi timpul menționate. Dacă oricare din aceste condiții nu se îndeplinesc regula nu va fi folosită pentru filtrarea pachetelor.

În continuare se descriu setările de la configurarea listelor de acces:

- Prioritatea (Priority). Se defineşte ordinea în care regula este verificată față de prima regulă: cu cât numărul este mai mic, cu atât regula are prioritate mai mare. Regulile implicite vor fi tot timpul verificate ultimele.

- Activare (Enable). Aici se defineşte dacă regula este activă sau nu. Se pot defini reguli în lista de control a accesului dar acestea pot fi într-o stare inactivă. Administratorul poate decide dacă o anumită regulă este activă sau nu prin bifarea căsuței „enable”.

- Acțiunea (Action). Se defineşte efectul regulii asupra traficului. Poate avea acțiunea de permitere (allow) sau de interzicere (deny) a traficului. Dacă regula se potriveşte iar acțiunea este „allow”

pachetul va fi trimis mai departe. Dacă regula se potriveşte iar acțiunea este „deny”, pachetul va fi ignorat.

- Serviciu (Service). Se pot selecta servicii predefinite sau se pot crea servicii noi cu butonul „Service management”. Odată definite servicii noi acestea vor apare în lista de servicii. Se poate de asemenea selecta „all” pentru a permite sau bloca tot tipul de trafic IP. Interfața grafică pentru definirea serviciilor utilizator poate fi accesată din ecranul „Regulă nouă (New rule)” cu butonul „Gestionarea serviciilor (Service management)”.

- Interfața sursă (Source interface). Se poate selecta interfața asupra căreia se va aplica lista: LAN, WAN sau oricare (any).

- Sursa (Source). Se selectează adresa IP sursă cu care trebuie potrivită regula. Se poate selecta o singură adresă IP, un domeniu de adrese sau o rețea întreagă (prin specificarea adresei de rețea şi a măştii) sau chiar valoarea „any” specificând orice adresă IP.

- Destinația (Destination). Se selectează adresa IP destinație în acelaşi mod ca la adresa sursă.

- Timpul (Time). Se defineşte perioada de timp în care regula va fi activă şi se foloseşte împreună cu parametrul „Data (Date)”. Se poate folosi şi valoarea „any” time şi „any” date.

- Editare (Edit). Cu acest buton se intră în ecranul de editare reguli şi se pot modifica regulile.

- Ştergere (Delete). Cu acest buton se şterge regula din ACL.

- Selectarea paginii (Page selection). Se pot selecta anumite pagini din lista de control al accesului sau se poate naviga între ele.

- Adăugare regulă nouă (Add new rule). Se foloseşte pentru crearea de noi reguli.

- Dezavarea tuturor regulilor (Disable all rules). Se dezactivează regulile definite de utilizator.

- Ştergerea tuturor regulilor (Delete all rules). Se şterg toate regulile definite de utilizator.

- Editarea unei reguli (Edit IP ACL rule). Se pot edita reguli. La o regulă nouă se poate folosi ca acțiune „allow” sau „deny” şi se vor completa următorii parametrii suplimentari.

- Log. La fiecare potrivire a unui pachet cu o regulă se va menționa în fişierul de log acest lucru.

- Managementul serviciilor (Service Managemet). Se foloseşte pentru adăugarea de noi tipuri de servicii în lista serviciilor.

- Programarea (Scheduling). Se introduce perioada de timp când regula va fi aplicată.

Politici de acces Intenet

Accesul la Internet poate fi gestionat de anumite politici de acces. O politică va conține patru componente: trebuie definită stația (adresa IP sau MAC) pe care se aplică politica, apoi permiterea sau interzicerea (allow sau deny) serviciului internet, data şi timpul când politica trebuie să fie activă precum şi adresa URL sau cuvintele cheie pentru aplicarea politicii.

Se poate crea o politică, şterge politica curentă, se pot şterge toate politicile sau se poate edita o politică folosind ecranul de editare a politicilor.

Pentru a crea o politică de acces la Internet se selectează numărul politicii din lista „Internet access policy”, apoi i se dă un nume politicii şi se selectează butonul de activare (enable); în continuare se va folosi butonul pentru selectarea listei stațiilor (Edit list of PCs) care vor fi afectate de această politică.

Dacă se doreşte blocarea accesului spre anumite site-uri se foloseşte componenta specifică numită „blocarea site-urilor după adresa URL (Website blocking by URL address)” sau blocarea după cuvinte cheie (Keyword). În primul vaz se va completa adresa URL sau numele de domeniu al site-urilor care se doresc a fi blocate, iar în al doilea caz se introduc cuvintele cheie din URL care vor produce blocarea acelui URL.

Folosind ecranele de configurare descrise mai sus se vor efectua diverse setări pentru a verifica funcționalitatea componenteleor de securitate ale routerului.

- Se vor testa diverse moduri de securitate în rețelele wireless;
- Se va configura firewall-ul astfel încât să restricționeze controale de tip activex şi java.
- Se vor implementa liste de acces pentru a verifica funcționalitatea lor prin interzicerea traficului de la anumite stații sau spre anumite stații pentru perioade definite de timp (se va verifica acest lucru prin testarea cu comanda „ping”, pachetele nu vor primi răspuns în timpul selectat la configurarea listelor de acces şi spre stațiile specificate).
- Se va configura prin politici de acces la Internet accesul doar a anumitor stații spre anumite adrese URL (inclusiv folosind cuvinte cheie pentru filtrarea mai multor adrese URL.
- Se va configura IPS pentru a bloca traficul de Instant Messaging.

Bibliografie

[1] Introduction to Wireless Network Security, http://netsecurity.about.com/od/hackertools/a/aa072004b.htm
[2] Wireless-N Gigabit Security with VPN WRVS4400N User manual
[3] PC Mag, http://www.pcmag.com
[4] Understanding WEP Weaknesses, http://eu.dummies.com/WileyCDA/how-to/content/understanding-wep-weaknesses.html
[5] Kerberos, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212437,00.html
[6] ACL, http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci213757,00.html
[7] Ramona Marfievici, Cosmin Ardelean, Adrian Peculea, Bogdan Iancu, Cristian Magherusan, coordonator Emil Cebuc, *Administrarea retelelor de calculatoare – indrumator de laborator*, 2009, 130 pagini, Editura U.T. Press, ISBN 978-973-662-500-8

X. Programarea dispozitivelor mobile: Comunicarea în rețea

1. Obiective

Obiectivele acestui capitol cuprind prezentarea fundamentelor teoretice referitoare la programarea aplicațiilor care comunică în rețea utilizând tehnologia Bluetooth, socketuri şi serviciile web.

2. Considerații teoretice

In anul 2011 statisticile arătau un număr de 4 miliarde de telefoane mobile la nivel global, dintre care 1,08 miliarde fiind smartphones [1].

Creşterea numărului de posesori de dispozitive mobile conectate la internet şi apariția standardelor de mare viteză (3G, 4G) a condus la explozia aplicațiilor de tip content-sharing, instant messaging, social networks, e-banking. Se estimează ca pana in anul 2014 internetul pe dispozitivele mobile va fi mai utilizat decât internetul pe sistemele desktop [2]. Din aceste considerente marea majoritate a aplicațiile moderne pun la dispoziție si o alternativa de accesare utilizând dispozitivele mobile.

Bluetooth s-a impus în industrie ca principala tehnologie pentru comunicarea dintre dispozitivele mobile pe distanțe scurte. Pentru comunicarea în Internet, două tehnici sunt extensiv utilizate: socketurile şi serviciile web.

2.1. Comunicarea în rețea utilizând tehnologia Bluetooth

Bluetooth este o tehnologie de cost şi putere redusă bazată tehnologia RF pentru comunicații pe distanțe scurte, reprezentând o alternativă la conexiunea cablată dintre diferite dispozitive electronice [3].

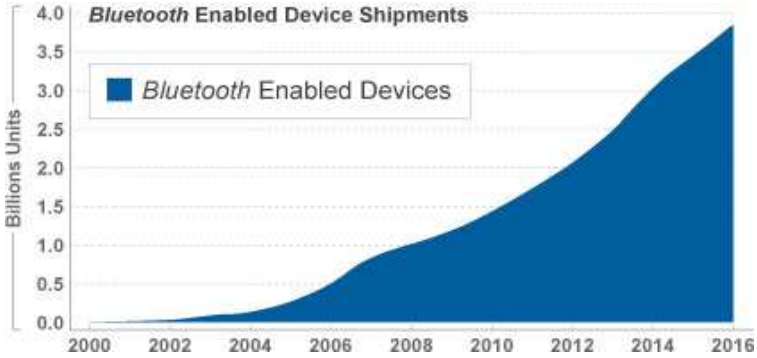


Figura 1. Evoluția tehnologiei Bluetooth [4]

Bluetooth a devenit tehnologia wireless cu cea mai mare rată de creştere, estimându-se că numărul dispozitivelor cu capabilități Bluetooth va ajunge la aproape 4 miliarde de unități.

Tabelul de mai jos prezintă evoluția şi versiunile tehnologiei Bluetooth:

Versiune	**Rata de date**
Bluetooth v1	până la 1 Mbit/s
Bluetooth v2 EDR (Enhanced Data Rate)	până la 3 Mbit/s
Bluetooth v3 HS (High Speed)	până la 24 Mbit/s bazat pe 802.11
Bluetooth v4	HS şi low energy

Tabelul 1. Versiuni Bluetooth

În [3] este descrisă arhitectura de bază şi principalele caracteristici ale nivelurilor care alcătuiesc tehnologia Bluetooth (fig. 2).

Nivelurile radio frecvență (RF) şi baseband corespund nivelului fizic al stivei de protocoale ISO/OSI. Dispozitivele Bluetooth operează în banda de frecvență liberă ISM 2,4 Ghz având următoarele caracteristici de bază:

- tehnică Frequency Hop Spread Spectrum (FHSS)
- modulație Gaussian shaped binary FSK (în mod EDR - $\pi/4$-DQPSK şi 8DPSK)

- distanțe între 10m şi 100 m
- conexiune ad-hoc

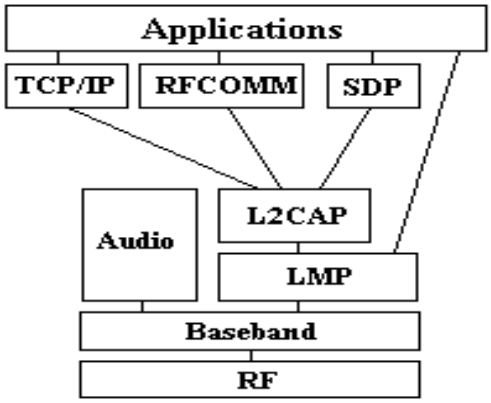


Figura 2. Arhitectura Bluetooth BR/EDR [3]

Conexiunile Bluetooth sunt de două tipuri: punct la punct sau punct la multipunct. Mai multe dispozitive Bluetooth care împart acelaşi canal formează un piconet. Dispozitivul care inițiază conexiunea va funcționa în mod master, celelalte dispozitive care vor participa la conexiune fiind în mod slaves. Mai multe piconet-uri pot forma o rețea denumită scatternet (fig. 3).

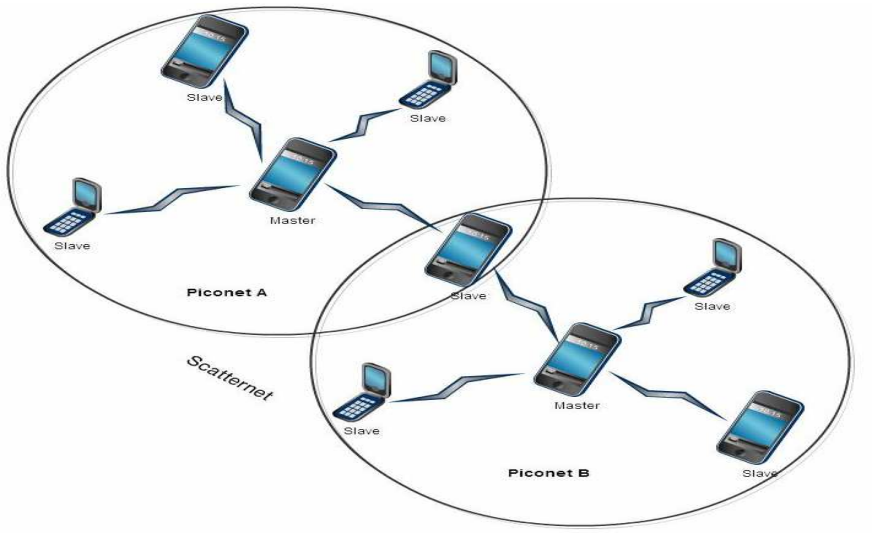


Figura 3. Tipuri de rețele Bluetooth

Nivelurile LMP şi L2CAP corespund nivelului legătură de date al stivei ISO-OSI. Protocolul Link Management Protocol (LMP) din cadrul nivelului Link Manager este responsabil configurarea, autentificarea, criptarea legăturii de comunicaţie. Dispozitivele Bluetooth sunt împărţite în trei clase de putere:

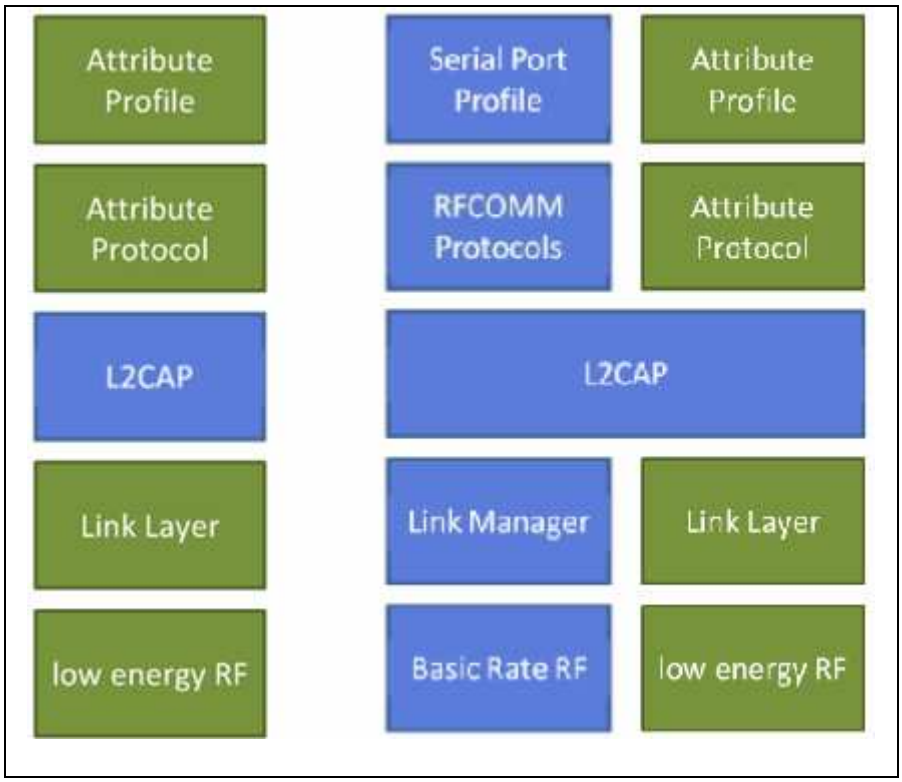
Clasa	Putere maximă
1	20 dBm (100mW)
2	4 dBm (2.5 mW)
3	0 dBm (1 mW)

Nivelul Logical Link Control And Adaptation Layer Protocol (L2CAP) furnizează servicii de date orientate pe conexiune (ex. transmisii audio) sau fără conexiune (ex. transmisii de date) către nivelurile superioare şi serviciu de multiplexare de protocoale.

RFCOMM este un protocol pentru emularea portului serial RS232, permiţând până la 60 de conexiuni simultane între două dispozitive Bluetooth.

Protocolul Service Discovery Protocol (SDP) descoperirea serviciilor din proximitatea Bluetooth, însă nu şi accesarea acestora.

Arhitectura versiunii 4.0 este prezentată în figura 4. Faţă de versiunile anterioare, versiunea 4.0 pune la dispoziţie două tipuri de dispozitive: single mode - care corespund dispozitivelor compatibile noii tehnologiei low-energy şi dual mode - care corespund dispozitivelor compatibile atât tehnologiei anteriore 4.0, cât şi cu tehnologiei low-energy.



a. single mode b. dual mode

Figura 4. Arhitectura Bluetooth 4.0 [5]

2.2. Comunicarea în rețea utilizând socketuri

Un socket reprezintă un capăt de comunicație a unei legături de comunicație bidirecțională între două programe care rulează în rețea [6].

Un socket de rețea reprezintă o combinație a unei adrese IP si a unui număr de port de nivel transport. Un socket de rețea are asociat un identificator unic pentru a permite conexiuni multiple între hosturi. Elementele care definesc în mod unic un socket de rețea sunt:

adresa IP sursă	**adresa IP destinație**	**port sursă**	**port destinație**	**protocol**

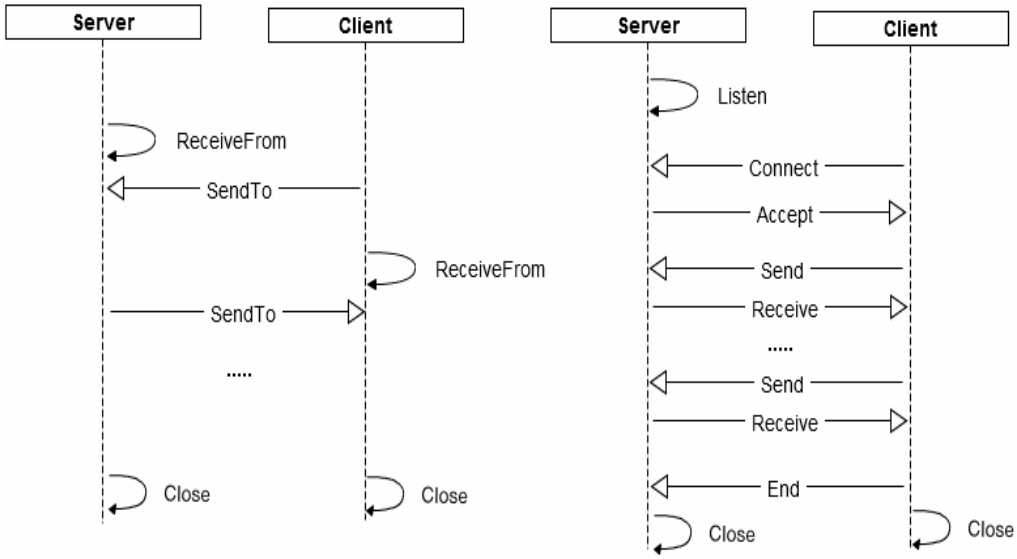
Un număr de porturi - well-known ports (porturi bine cunoscute), sunt rezervate pentru servicii de rețea specifice (FTP – 21, TELNET – 23, DNS – 53, HTTP – 80 etc). Lista completă a porturilor asignate de către Autoritatea

pentru Asignarea Numerelor în Internet (IANA) se găseşte la adresa: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml.

Socket-urile de rețea pot fi de mai multe tipuri, în funcție de protocolul de nivel transport utilizat. Două tipuri de socketuri de rețea sunt socketurile datagramă şi socketurile stream.

Socket-urile datagramă se bazează pe protocolul de nivel transport UDP (User Datagram Protocol) şi sunt cunoscute ca socketuri fără conexiune. Cele mai cunoscute aplicațiile care utilizează acest tip de socket sunt: streaming multimedia, telefonie IP sau jocurile online.

Complementar, socket-urile stream se bazează pe protocolul de nivel transport TCP (Transmission Control Protocol) şi sunt cunoscute ca socket-uri orientate pe conexiune. Cele mai cunoscute aplicațiile care utilizează acest tip de socket sunt: email, transfer de fişiere (ftp) sau web.



a. Comunicare Socket UDP b. Comunicare Socket TCP

Figura 5. Comunicare socket

Figura 5 si tabelele 2, 3 descriu paşii necesare realizării comunicației dintre un client şi un server utilizând socket-uri de rețea de tip datagramă, respectiv stream.

Operație	**Comunicare Socket UDP**	
	Server	**Client**
Socket	Creare socket server	Creare socket client
SendTo/ReceiveFrom	Serverul poate recepționa/transmite date (Protocolul UDP nu garantează transmiterea sigura si in ordine a datelor)	Clientul poate transmite/recepționa date (Protocolul UDP nu garantează transmiterea sigura si in ordine a datelor)
	Nu exista o conexiune. Fiecare datagrama este rutata individual	
Close	Serverul închide socketul (opțional)	Clientul închidere socketul

Tabelul 2. Comunicarea în rețea utilizând socket-uri UDP

Operație	**Comunicare Socket TCP**	
	Server	**Client**
Socket		Creare socket client
Listen	Aşteaptă cereri de conexiune de la clienți	
Connect		Cerere de conectare la server
Accept	Accepta conexiunea cu clientul	
Send/Receive	Serverul poate recepționa/transmite date (Protocolul TCP garantează transmiterea fiabila si in ordine a datelor)	Clientul poate transmite/recepționa date (Protocolul TCP garantează transmiterea fiabila si in ordine a datelor)
	Aceste operații se pot avea loc atât timp cat conexiunea este activa	
End		Clientul semnalizează terminarea conexiunii
Close	Serverul poate închide conexiunea (opțional)	Clientul închidere socketul si termina conexiunea

Tabelul 3. Comunicarea în rețea utilizând socket-uri TCP

2.3. Comunicarea în rețea utilizând servicii web

2.3.1. Arhitectura SOAP

Arhitectura orientată pe servicii (Service-Oriented Architecture – SOA) reprezintă un stil arhitectural pentru construirea de aplicații software care folosesc serviciile disponibile într-o rețea, cum ar fi web. Un serviciu reprezintă o implementare a unei funcționalități business bine definită, iar astfel de servicii pot fi consumate de către clienți în diverse aplicații sau procese business. [7].

O caracteristică de bază a SOA este separarea interfeței serviciului – care este independentă de platformă, de partea de implementare – care este specifică fiecărei platforme.

Arhitectura SOA utilizează paradigma find-bind-execute (fig. 6). Această paradigmă presupune existența a trei componente de bază: furnizorii de servicii (service providers), registrul public şi consumatorii de servicii (service consumers). Furnizorii de servicii înregistrează serviciile în registrul public, de unde consumatorii vor putea găsi şi utiliza serviciile web.

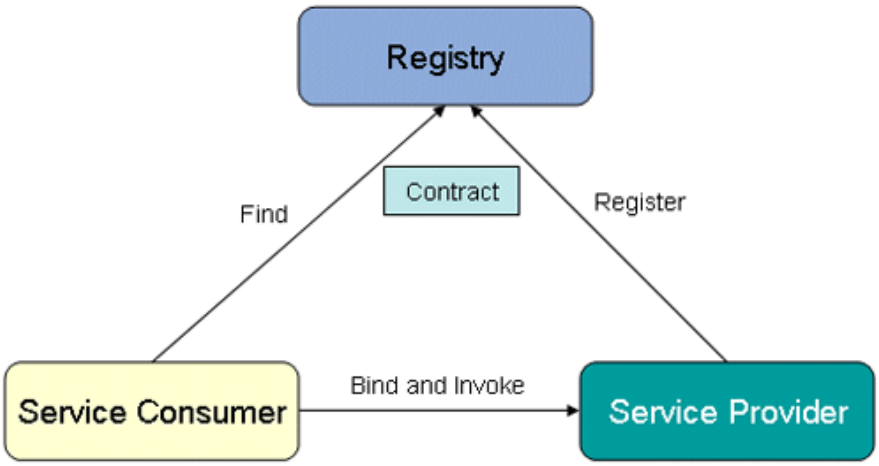


Figura 6. Paradigma *find-bind-execute* [7]

Serviciile Web permit accesul la o largă varietate de date prin intermediul Internetului. Caracteristica lor de interoperabilitate se bazează

pe un set de standard XML – SOAP, WSDL şi UDDI. SOAP (Simple Object Access Protocol) este un protocol XML care permit aplicațiilor să realizeze schimbul de informații utilizând protocolul HTTP. Limbajul (pe baza XML) utilizat pentru descrierea şi accesul la serviciile web este WSDL (Web Services Description Language). UDDI (Universal Description, Discovery and Integration) este un registru de interfețe web descrise prin WSDL.

2.3.2. Arhitectura REST

REST (REpresentational State Transfer) defineşte un set de principii arhitecturale prin care se pot proiecta servicii Web care se concentrează asupra resurselor unui sistem, inclusiv modul în care starea resurselor este abordată şi transferată prin HTTP de o gamă largă de aplicații client scrise în diferite limbaje [8].

SOAP	**REST**
Un contract formal trebuie să fie stabilit pentru a descrie interfața serviciilor web oferite	Serviciile web sunt fără stare (stateless)
Arhitectura trebuie să abordeze cerințe nefuncționale complexe (adresare, securitate etc)	O infrastructură cache poate fi utilizată pentru creşterea performanțelor
Arhitectura abordează prelucrare şi invocare asincronă	Producătorul de servicii şi consumator de servicii trebuie să aibă o înțelegere reciprocă asupra contextul şi conținutul transferat Serviciile pot fi expuse utilizând XML şi consumate de pagini HTML fără a modifica semnificativ arhitectura site-ul web existent

Tabelul 4. SOAP vs. REST

Implementarea unor servicii web REST urmareşte patru principii de bază: utilizarea explicită a metodelor HTTP, lipsa stării (stateless), identificare prin URL-uri a serviciilor şi transferul lor utilizând XML şi/sau JavaScript Object Notation (JSON).

În cadrul tabelului 4 sunt prezentate cazurile când este oportună utilizarea serviciilor web SOAP şi REST [9].

Bibliografie

[1] H. Richmond, *The Growth of Mobile Marketing and Tagging*, http://tag.microsoft.com/community/blog/t/the_growth_of_mobile_marketing_and_tagging.aspx

[2] E. Lemenager, *NFC mobile gaming makes simple real-life games interactive*, http://tag.microsoft.com/community/blog/t/nfc_mobile_gaming.aspx

[3] H. Wang, *Overview of Bluetooth Technology*, http://www.m2mgsm.com/download/BT/docs/general/Bluetooth_Overview.pdf

[4] Bluetooth SIG, http://www.bluetooth.com/Pages/SIG-Membership.aspx

[5] R. Heydon, *Training videos – Architecture*, https://www.bluetooth.org/OTV/4-Architecture/

[6] All about sockets, http://docs.oracle.com/javase/tutorial/networking/sockets/definition.html

[7] SOAP Tutorial, http://www.w3schools.com/soap/default.asp

[8] A. Rodriguez, *RESTful Web services: The basics*, http://www.ibm.com/developerworks/webservices/library/ws-restful/

[9] S. Tyagi, *RESTful Web Services*, http://www.oracle.com/technetwork/articles/javase/index-137171.html

XI. Programarea dispozitivelor mobile: Windows Phone 7

1. Obiective

Obiectivele acestui capitol cuprind prezentarea platformei Windows Phone Application, a arhitecturii Windows Phone 7 şi a fundamentelor necesare pentru programarea dispozitivelor mobile Windows Phone 7.

2. Considerații teoretice

Platforma Windows Phone Application permite creare aplicațiilor care rulează pe sistemul de operare Windows Phone 7. Dezvoltarea aplicațiilor se realizează utilizând framework-ul .NET , prin instalarea Windows Phone Developer Tools care conține Visual Studio 2010 Express for Windows Phone, XNA Game Studio 4.0 şi emulatorul Windows Phone Emulator. [1]

Platforma Windows Phone Application pune la dispoziția dezvoltatorilor două framework-uri [2]: Silverlight for Windows Phone framework – pentru aplicații bazate pe XAML şi XNA framework – pentru dezvoltarea de jocuri.

Figura 1 prezintă arhitectura care stă la baza Windows Phone 7: Silverlight for Windows Phone framework, XNA framework şi setul de caracteristici puse la dispoziție pentru dezvoltarea de aplicații WP7.

În [3] se prezintă structura hardware unui dispozitiv Windows Phone 7 (şi a emulatorului pentru dezvoltare). Dispozitivul este format dintr-un display multi-touch şi trei butoane: Back, Start, Search (fig. 2). Butonul Back permite navigarea prin paginile aplicațiilor sau terminarea unei aplicații, dacă utilizatorul se găseşte în pagina principală a aplicației. Butonul Start permite revenirea la ecranul de start al telefonului, iar butonul Search permite căutarea unei caracteristici. De asemenea, dispozitivul pune

la dispoziția utilizatorilor şi a dezvoltatorilor o serie de senzori şi servicii: Wi-Fi, Camera foto/video, Accelerometru, Locație, Notificaficări Push.

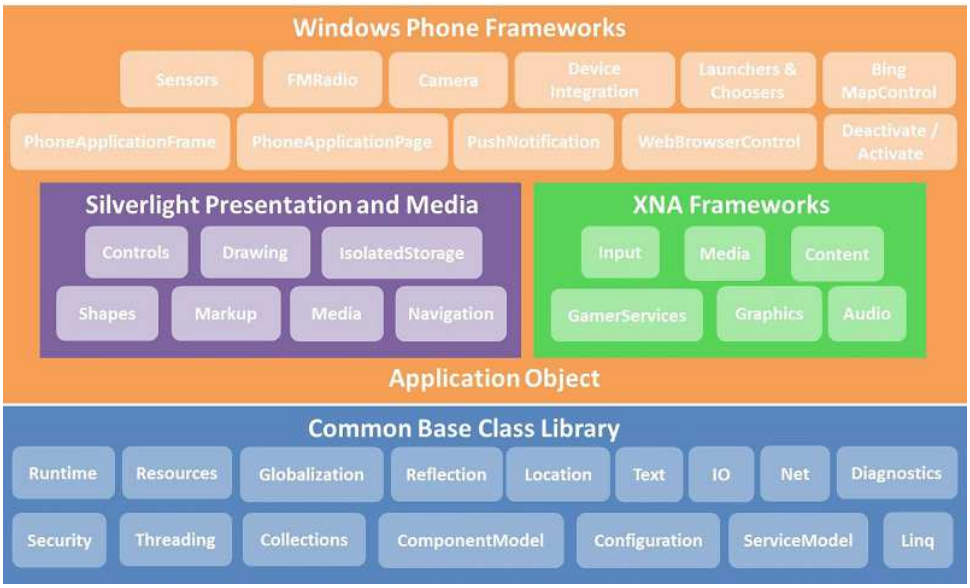


Figura 1. Arhitectura Windows Phone 7 [2]:

Figura 2. Structura hardware a unui dispozitiv Windows Phone 7

Pentru instalarea aplicațiilor dezvoltate pe dispozitivul mobil acesta trebuie înregistrat în portalul Windows Phone 7 [1].

3. Crearea aplicațiilor utilizând Windows Phone 7 - Silverlight

Pentru creare unei aplicații Windows Phone 7 – Silverlight se va crea un nou proiect urmărind pașii:

File - > New Project -> Windows Phone Application

Name: My first App

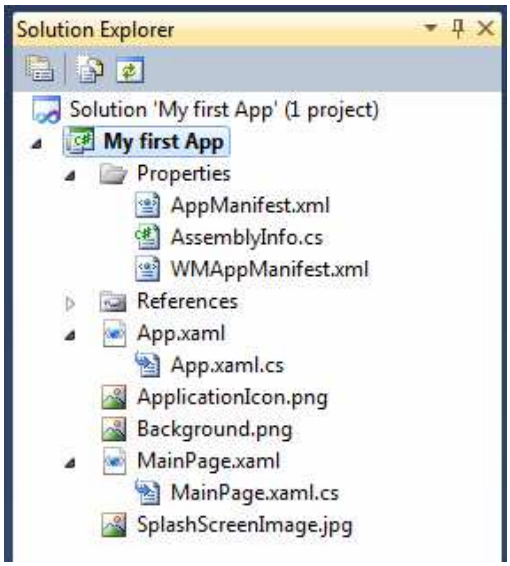


Figura 5. Solution Explorer Windows Phone 7

Figura 5 prezintă Solution Explorer împreună cu principalele fișiere Extensible Application Markup Language (XAML) și C# asociate ale unei aplicații Windows Phone 7 Silverlight. În continuare va fi descris succint rolul și structura acestora.

- *WMAppManifest.xml*
    - Title = " My first App " reprezintă numele proiectului; acest nume va fi afișat de către emulator/dispozitiv în lista de aplicații puse la dispoziția utilizatorilor

- Capabilities reprezintă lista de senzori şi servicii ce pot fi utilizate.

- *App.xaml cu App.xaml.cs*

  - App.xaml.cs: Toate programele conțin o clasă App derivată din Application şi este utilizată pentru acțiuni la nivelul întregii aplicații.

  - Structura App.xaml.cs

```
namespace My_first_App
{
public partial class App : Application
        {
        public App()
                { …
                InitializeComponent();
                …
                }
        …
        }
}
```

  - App.xaml: utilizat pentru stocarea de resurse *la nivelul întregii aplicații*

    Principalul atribut este elementul de root Application, din care derivă clasa App.

    Un alt atribut important al acestui fişier este x:Class. În cadrul aplicației x:Class="My_first_App.App"se interpretează astfel: clasa App din cadrul namespace-ului My_first_App este derivată din elementul de root – clasa Application.

    În momentul parsării App.xaml se va genera un fişier App.g.cs (g = generated) localizat în subdirectorul \obj\Debug şi care împreună cu App.xaml.cs alcătuiesc clasa App.

    În momentul rulării, clasa App va crea un obiect de tip PhoneApplicationFrame, care va juca rolul unui pseudo web browser, pentru a permite navigarea către obiectul MainPage, iar apoi spre alte pagini create.

- *MainPage.xaml cu MainPage.xaml.cs.*

  - MainPage.xaml.cs: defineşte clasa MainPage care derivă din clasa Silverlight PhoneApplicationPage. Elementele definite în această clasă vor fi afişate pe ecranul dispozitivului.

  - Structura MainPage.xaml.cs

```
namespace My_first_App
{
        public partial class MainPage : PhoneApplicationPage
        {
                public MainPage ()
                {
                InitializeComponent();
                }
        }
}
```

  - MainPage.xaml: Fişierul conține o structură ierarhică care defineşte elementele ce vor fi afişate pe ecranul dispozitivului (Grid, StackPanel, TextBlock etc). Fiecare pagină a aplicațiilor dezvoltate va avea o structură asemănătoare.

- *ApplicationIcon.png* şi *Background.png* sunt fişierele utilizate de către dispozitiv pentru a identifica vizual aplicația dezvoltată.

- *SplashScreenImage.jpg* este imaginea afişată la încărcarea aplicației.

Instalarea aplicației

În directorul \bin\Debug se va găsi o arhivă cu extensia XAP (compresie ZIP) denumită My_first_App.xap. Această arhivă este instalată în emulator sau în dispozitivul Windows Phone7.

Rularea primei aplicații

Se va selecta meniul Debug menu -> Start Debugging sau se apasă tasta F5.

4. Aplicații practice

4.1.1. Se va crea şi rula aplicația creată urmând paşii de la punctul 3. Identificați paşii urmați şi metodele utilizate.

4.1.2. Se va modifica fişierul MainPage.xaml astfel încât aplicația să afişeze pe ecran textul din figura 2.

4.1.3 Se va modifica fişierul MainPage.xaml astfel încât orientarea aplicației sa se modifice la schimbarea orientării telefonului (Portrait to Landscape)

4.1.4. Se va crea un nou proiect cu mai multe pagini si care va permite navigarea intre aceste pagini.

Observații privind crearea unor noi pagini şi navigarea către acestea:

1. Crearea unei noi pagini se realizează prin selectarea Project-> Add New Item, iar apoi a tipului de pagină dorit.
2. Navigarea din pagina “MainPage.xaml” către o altă pagină denumită “SecondPage.xaml” se realizează prin apelarea: NavigationService.Navigate(new Uri("/SecondPage.xaml", UriKind.Relative));
3. Navigarea din pagina “SecondPage.xaml” înapoi către pagina “MainPage.xaml” se realizează prin apelarea: NavigationService.GoBack() sau prin apăsarea butonul Back al dispozitivului.

4.2. Se va rula proiectul Netw. Info Status care permite vizualizarea informațiilor referitoare la starea rețelelor wifi, celulare etc. Identificați paşii urmați şi metodele utilizate.

4.3. Se vor rula aplicațiile client puse la dispoziție de către librăria MSDN, împreună cu sursele de server TCP şi server UDP puse la dispoziție. Se vor identifica paşii urmați şi metodele utilizate.

Aplicația client TCP Socket:	http://msdn.microsoft.com/en-us/library/hh202858(v=vs.92).aspx
Aplicația client UDP Socket:	http://msdn.microsoft.com/en-us/library/hh202864(v=vs.92).aspx

Observații privind utilizarea socket-urile de rețea în Windows Phone 7

1. Operația de conectare a clientului Windows Phone la un server TCP este o operație asincrona.
2. Operația de recepționare/transmitere a unui pachet de către clientul Windows Phone de la/către un server TCP este o operație asincrona

4.4.1. Se va rula aplicația care utilizează serviciul web RESTful freegeoip (http://freegeoip.net/static/index.html) pentru geolocația adresei IP sau a unui site web. Identificați pașii urmați şi metodele utilizate.

4.4.2. Se va modifica aplicația astfel încât răspunsul serviciului web să fie afişat într-o pagină nouă.

Observații pentru transmiterea parametrilor între pagini

1. Pentru transmiterea parametrilor către o nouă pagină utilizați QueryString.

http://msdn.microsoft.com/en-us/library/windowsphone/develop/ff626521(v=vs.92).aspx

2. Identificați alte metode pentru transmiterea parametrilor între paginile unei aplicații WP7.

Bibliografie:

[1] Windows Phone Dev Center, http://dev.windowsphone.com/en-us
[2] Application Platform Overview for Windows Phone, http://msdn.microsoft.com/en-us/library/windowsphone/develop/ff402531(v=vs.92).aspx
[3] C. Petzold, Programming Windows Phone 7, http://blogs.msdn.com/b/microsoft_press/archive/2010/10/28/free-ebook-programming-windows-phone-7-by-charles-petzold.aspx

XII. Programarea dispozitivelor mobile: Android

1. Obiective

Obiectivele acestui capitol cuprind prezentarea platformei, a arhitecturii şi a fundamentelor necesare pentru programarea dispozitivelor mobile Android.

2. Considerații teoretice

Sistemul Android pune la dispoziția dezvoltatorilor o platformă open-source şi un mediu de dezvoltare pentru aplicații specifice dispozitivelor mobile.

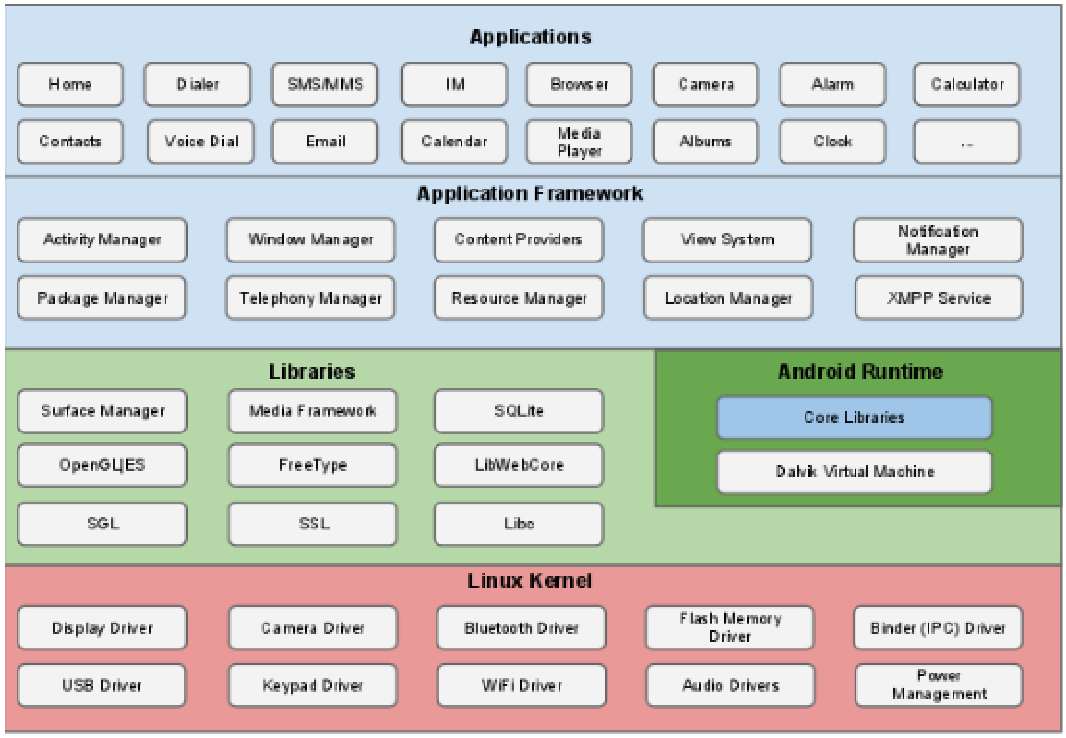


Figura 1. Arhitectura Android [1]

Arhitectura de baza a sistemului de operare Android (fig. 1) conține următoarele niveluri [1]:

- Nivel aplicații (scrise in limbajul java, executate in Dalvik)
- framework servicii şi librarii (majoritatea scrise in limbajul java şi executate in maşina virtuala)
- librarii native libraries, daemon şi servicii (scrise in limbajul C or C++)
- kernel Linux, care include diversele drivere

Cele două tipuri de aplicații care extind funcționalitățile de bază Android sunt aplicațiile preinstalate şi aplicațiile dezvoltate de către utilizatori (acestea se pot descărca şi instala de pe site-ul Google Play).

Dezvoltarea, testarea şi instalarea unei aplicații Android urmăreşte următorii paşi prezentați in figura 2 [2]:

1. instalarea şi configurarea dispozitivelor virtuale (Android Virtual Devices - AVDs) şi conectarea dispozitivelor hardware
2. dezvoltarea aplicației Android
3. testarea şi depanarea aplicației dezvoltate (se va crea un pachet .apk care va fi instalat şi rulat pe emulator sau dispozitivul hardware)
4. publicarea aplicației în mod release şi pe site-ul Google Play (opțional)

Pentru dezvoltarea aplicațiilor Android este necesară instalarea platformei Android şi a unui mediu de dezvoltare. Paşii necesari a fi urmăriți sunt [3]:

1. Descărcarea Android SDK.
2. Instalarea plugin-ului ADT pentru Eclipse (mediul Eclipse IDE se consider a fi instalat).
3. Descărcarea celor mai recente variante de utilitare şi SDK utilizând SDK Manager.

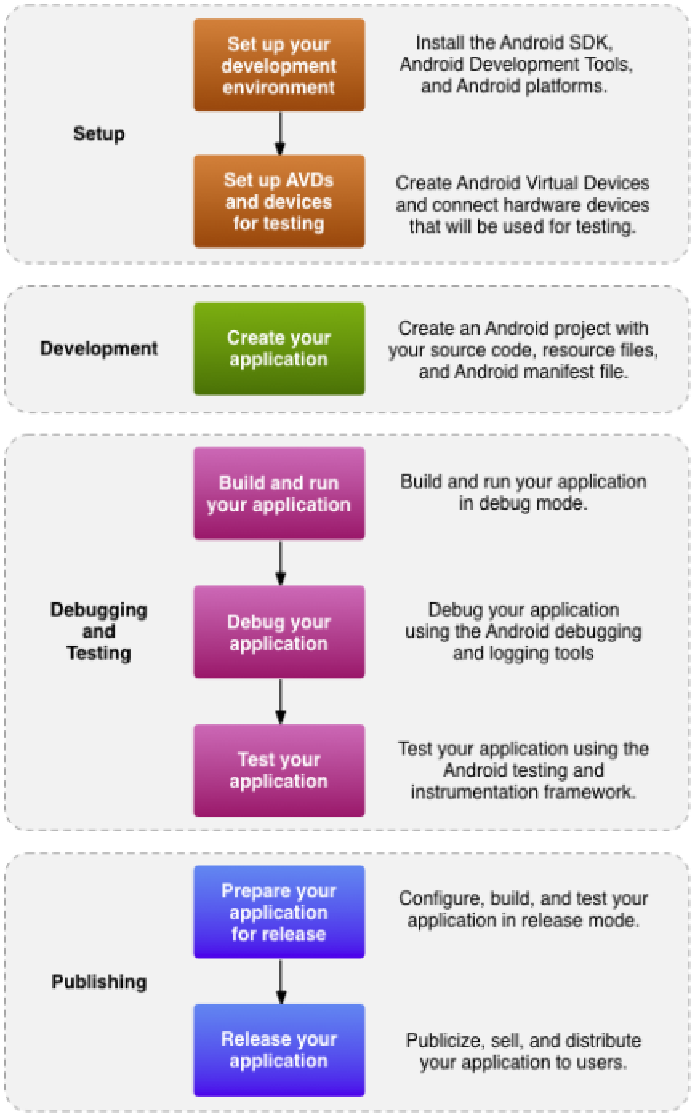
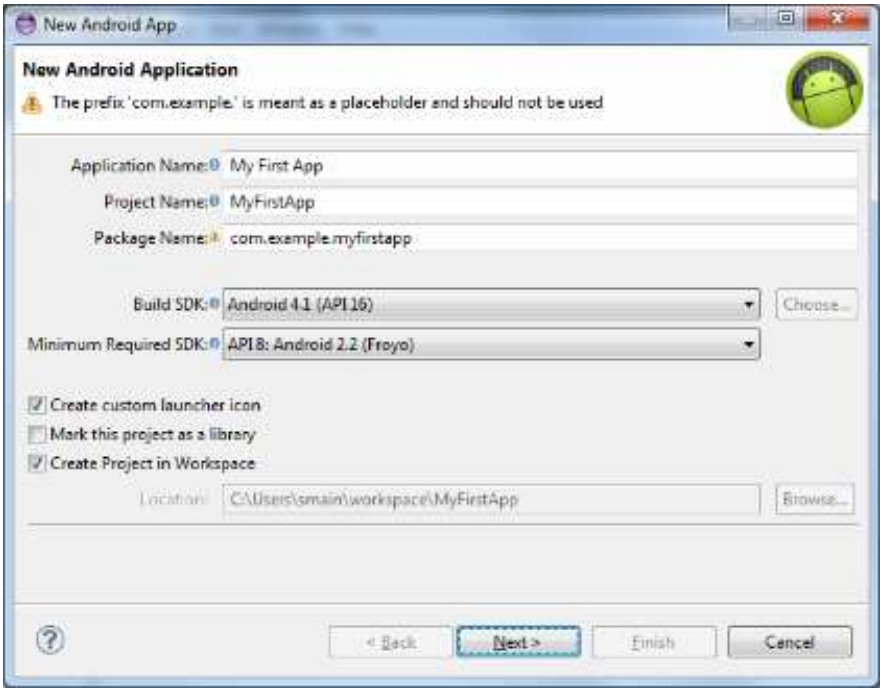


Figura 2. Procesul de dezvoltare al aplicațiilor Android [2]

3. Crearea aplicațiilor Android utilizând mediul de dezvoltare Eclipse

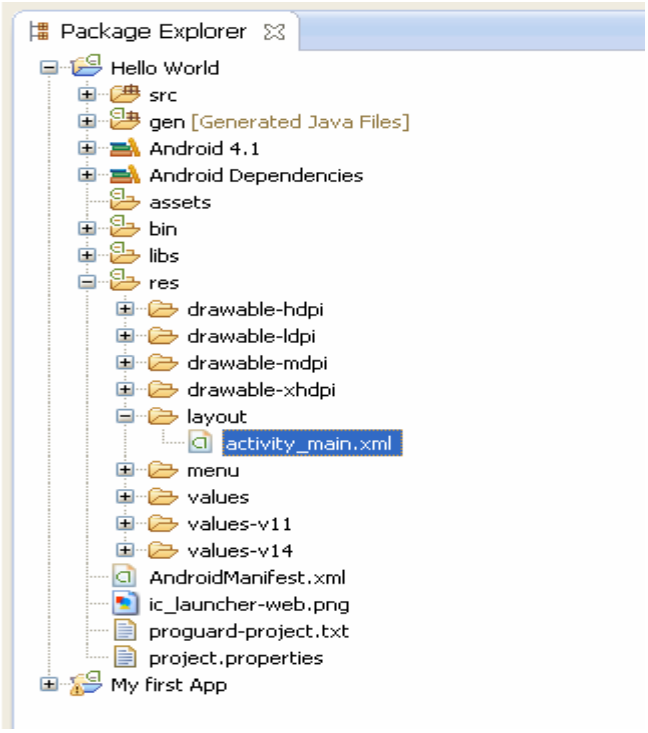
În descrierea modului de creare şi rulare a unui proiect Android se consideră utilizarea mediul de dezvoltare Eclipse şi a emulatorului aferent. În mediul de dezvoltare Eclipse, pentru creare unei simple aplicații se vor urmării următorii paşi:

1. click New Android App Project din cadrul toolbar



2. se va selecta un şablon de activitate (în acest caz BlankActivity)
3. click Next
4. click Finish.

Structura proiectului Android creat cuprinde următoarea structură de directoare şi fişiere:



- AndroidManifest.xml
  - cuprinde caracteristicile fundamentale şi definiția componentelor aplicației
- src/
  - cuprinde principalele fişierele sursă ale aplicației
- gen/
  - cuprinde fişierele sursă ale aplicației generate automat
- res/
  - cuprinde subdirectoarele cu resursele aplicației;
    - drawable-…/ - directoare cu obiecte drawable (ex. bitmaps) pentru diferite tipuri de ecrane.
    - layout/ - director cu fişierele ce definesc interfața utilizator
    - values/ - director cu fişiere care conțin o colecție de resurse (ex. definire de string-uri, stiluri)

Rularea primei aplicații utilizând emulatorul

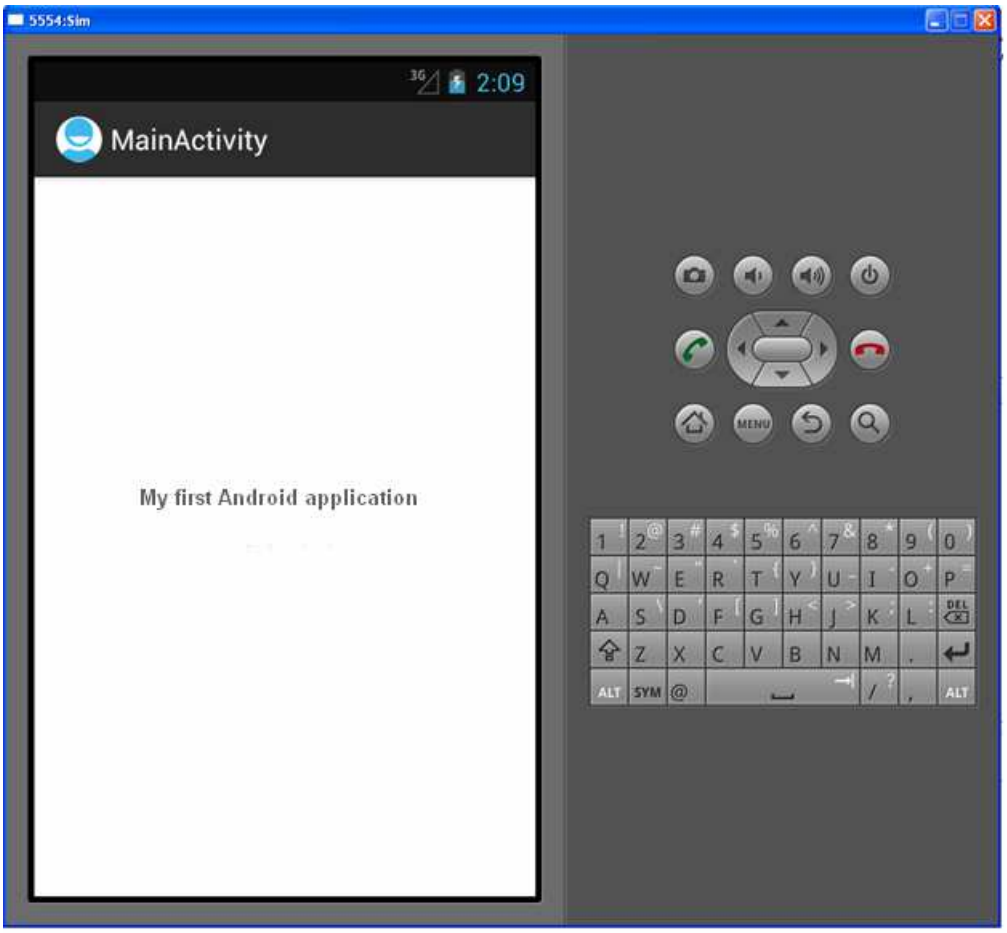


Figura 3. Emulatorul Android

Pentru rularea unei aplicații Android utilizând emulatorul, inițial e necesară crearea unui Dispozitiv Virtual (Android Virtual Device - AVD) care permite modelarea unor diferite tipuri de dispozitive:

1. se va lansa Android Virtual Device Manager din toolbar
2. click New
3. se vor completa detaliile pentru AVD
4. click Create AVD.
5. se va selecta noul AVD creat din Android Virtual Device Manager
6. click Start
7. click Run din toolbar

Pentru rularea pe dispozitive reale se va consulta tutorialul [4].

In [5] sunt descrise cele patru posibile component ale unei aplicații Android. O aplicație poate utiliza una sau mai multe componente, acestea fiind instanțiate de către sistemul de operare:

Funcționalitate	Clasa Java de bază	Exemple
Axat pe lucruri pe care un utilizator le poate face	Activity	Editarea unui text, jucarea unui joc
Proces de background	Service	Redare muzică, actualizarea unei pictograme
Recepționare mesaje	BroadcastReceiver	Declanşarea alarmei datorită unui eveniment
Stocare şi preluare date	ContentProvider	Deschiderea unui contact din telefon

Interfața grafică utilizator a unei aplicații Android este construită dintr-o ierarhie de obiecte View (ex. TextView, Button) sau ViewGroup (ex. Layout) conform figurii de mai jos:

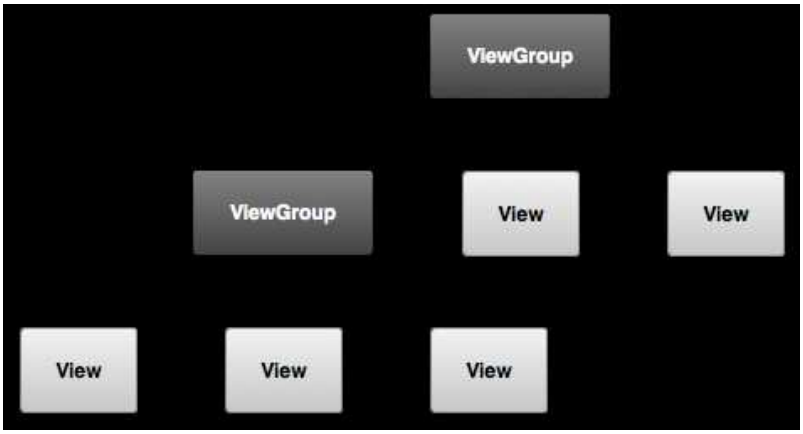


Figura 4. Ierarhia de obiecte GUI [6]

Interfața grafică utilizator a activității definite se regăseşte în fişierul `activity_main.xml` din cadrul directorului `res/layout/`

Semnul + înaintea tipului de resursă este necesar când se defineşte un ID de resursă pentru prima dată. Semnul @ este necesar atunci când se face referire la orice obiect resursă XML. Acesta este urmat de tipul de resursă (id, în acest caz), un slash, apoi numele resursei (*editTextNew).*

Exemplu:

```
<EditText android:id="@+id/editTextNew"
android:text="@string/hello_world"/>
```

Tip resursă	Nume resursă
id	editTextNew
string	hello_world

Observație:

1. În Eclipse, secvența Ctrl + Shift + O se poate utiliza pentru a importa clasele lipsă, necesare la adăugarea unei noi resurse.

4. Aplicații practice

4.1.1. Se va crea şi rula aplicația creată urmând paşii de la punctul 3. Identificați paşii urmați şi metodele utilizate.

4.1.2. Se va modifica fişierul res/layout/activity_main.xml astfel încât aplicația să afişeze pe ecran textul din figura 2.

4.1.4. Se va crea un nou proiect cu mai multe activități şi care va permite navigarea intre aceste pagini.

Observații privind crearea unor noi activități şi navigarea către acestea:

1. Crearea unei noi pagini se realizează prin selectarea Project-> Add New Item, iar apoi a tipului de pagină dorit.
2. Un obiect de tip Intent este utilizat pentru legarea unor componente separate la runtime (de exemplu două activități). În cele mai multe cazuri un obiect Intent este utilizat pentru a porni o altă activitate.
3. Navigarea din activitatea curentă către o altă se realizează prin apelarea: *startActivity(intent)*, unde intent este Intent-ul creat la pasul anterior.
4. Navigarea către activitatea inițială se realizează prin apelarea metodei *finish()* sau prin apăsarea butonul Back al dispozitivului.

4.2. Se va rula proiectul Netw. Info Status care permite vizualizarea informațiilor referitoare la starea rețelelor wifi, celulare etc. Identificați pașii urmați și metodele utilizate.
Observație:

1. pentru efectuarea operațiilor de rețea se vor adăuga următoarele linii in AndroidManifest.xml

```
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission
android:name="android.permission.ACCESS_NETWORK_STATE"/>
```

4.3. Se vor rula aplicațiile server și client puse la dispoziție. Se vor identifica pașii urmați și metodele utilizate.

4.4.1. Se va rula aplicația care utilizează serviciul web RESTful freegeoip (http://freegeoip.net/static/index.html) pentru geolocația adresei IP sau a unui site web. Identificați pașii urmați și metodele utilizate.

4.4.2. Se va modifica aplicația astfel încât răspunsul serviciului web să fie afișat într-o activitate nouă.

Bibliografie:

[1] Android Security Overview, http://source.android.com/tech/security/index.html
[2] Android Developers website, http://developer.android.com/tools/workflow/index.html
[3] Android Developers website , http://developer.android.com/training/basics/firstapp/index.html
[4] Android Developers website, http://developer.android.com/training/basics/firstapp/running-app.html#RealDevice
[5] J. Steele, N. To, *The Android Developer's Cookbook - Building Applications with the Android SDK*, Addison-Wesley, 2011.
[6] Android Developers website, http://developer.android.com/training/basics/firstapp/building-ui.html

© TWDM 2012

EDITURA U.T.PRESS
Str Republicii nr. 107, CP 42, OP 2
e-mail: utpress@biblio.utcluj.ro
http://www.utcluj.ro/editura

2012