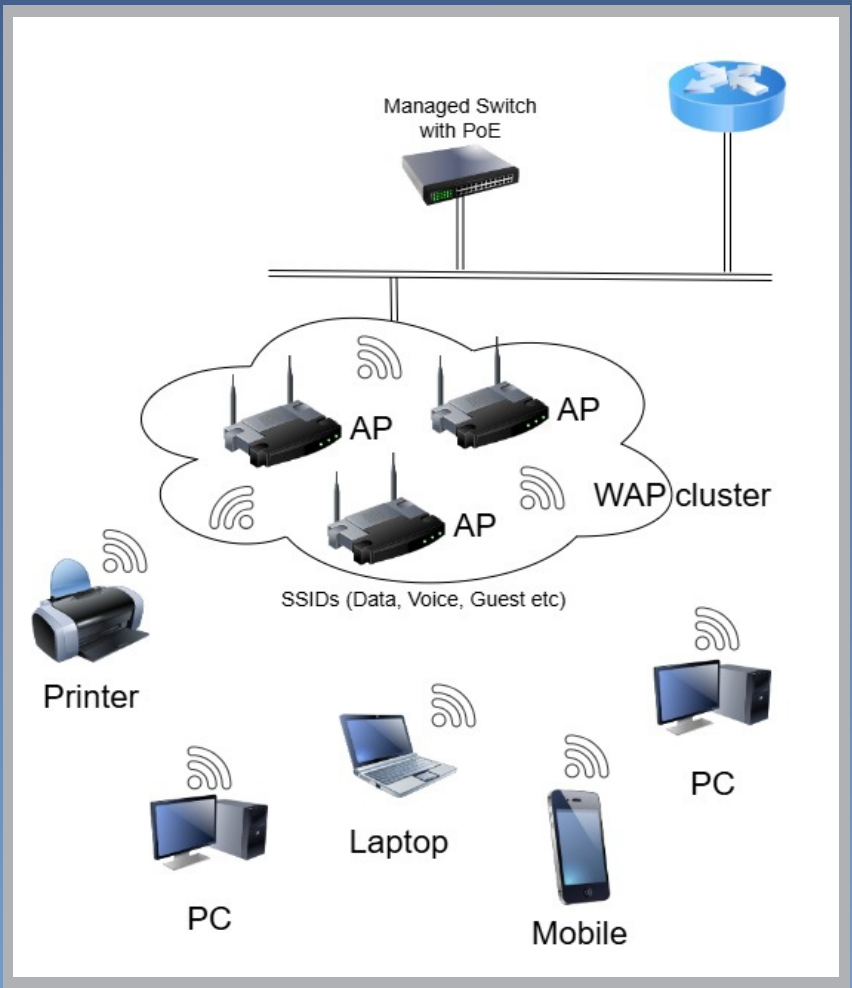
Bogdan IANCU, Adrian PECULEA

***Coordonatori*: Emil CEBUC, Vasile DĂDÂRLAT**

Tehnologii Wireless și Dispozitive Mobile

APLICAȚII PRACTICE



U.T.PRESS
Clij-Napoca, 2025
ISBN 978-606-737-755-2

Bogdan IANCU Adrian PECULEA

Coordonatori: Emil CEBUC, Vasile DĂDÂRLAT

Tehnologii Wireless şi Dispozitive Mobile

APLICAŢII PRACTICE

U.T.PRESS
Cluj - Napoca, 2025
ISBN 978-606-737-755-2

Editura U.T.PRESS
Str. Observatorului nr. 34
400775 Cluj-Napoca
Tel.: 0264-401.999
e-mail: utpress@biblio.utcluj.ro
www.utcluj.ro/editura

Recenzia: Prof.dr.ing. Ionuț Anghel
Conf.dr.ing. Lia-Anca Hangan

Pregătire format electronic on-line: Gabriela Groza

ISBN 978-606-737-755-2

Prefaţă

Rețelele wireless și dispozitivele mobile sunt esențiale în viața modernă, susținând comunicații rapide, soluții IoT și infrastructuri complexe, în continuă evoluție, cu noi oportunități și provocări. Această a **doua ediție** a cărții **Tehnologii Wireless și Dispozitive Mobile. Aplicații Practice** își propune să ofere cititorilor o abordare clară și aplicată asupra principiilor, configurațiilor și instrumentelor esențiale pentru înțelegerea și implementarea soluțiilor wireless moderne. Structurată în douăsprezece capitole, lucrarea acoperă aspecte fundamentale, de la principii RF și tehnologii de antene, până la securitatea rețelelor wireless și programarea dispozitivelor mobile.

Primele capitole introduc cititorul în fundamentele RF, explorând conceptele esențiale legate de propagarea semnalului, interferențe și caracteristicile antenelor. Următoarele secțiuni detaliază analiza mediului RF folosind instrumente profesionale precum Netscout/netAlly AirCheck G2 Wireless Tester, Fluke Etherscope Series II Network Assistant și Fluke Analyze-Air, facilitând diagnosticarea și optimizarea performanței rețelelor wireless.

Lucrarea continuă cu o prezentare practică a configurării rețelelor wireless, de la setări de bază și avansate, până la implementarea soluțiilor VPN pentru acces securizat la distanță. Într-o lume din ce în ce mai vulnerabilă la atacuri cibernetice, un capitol esențial este dedicat securității rețelelor wireless și mobile, oferind strategii de protecție împotriva amenințărilor moderne.

Ultimele capitole sunt destinate programării dispozitivelor mobile, explorând metodele de comunicare în rețea și dezvoltarea aplicațiilor pentru platforma Android. Aceste secțiuni sunt esențiale pentru inginerii și dezvoltatorii care doresc să creeze aplicații eficiente și sigure pentru dispozitive mobile conectate la rețele wireless.

Prin această ediție revizuită și actualizată, cartea se adresează studenților, specialiștilor IT, administratorilor de rețea și dezvoltatorilor de aplicații mobile, oferindu-le o resursă valoroasă de învățare și practică. Fie că este vorba despre proiectarea unei rețele wireless, optimizarea performanței acesteia sau dezvoltarea de aplicații mobile conectate, cititorii vor găsi în această lucrare soluții concrete și exemple aplicate.

Autorii,

Cluj-Napoca, 2025

Cuprins

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 unităţilor de măsură şi a fundamentelor matematice necesare pentru proiectarea şi evaluarea reţelelor 802.11.

2. Consideraţii teoretice

2.1. Semnale RF

În cadrul comunicaţiilor de date în reţelele cablate, mediile de transmisie utilizate au fost, în ordinea apariţiei, cablurile coaxiale, cablurile torsadate şi fibra optică. Pentru transmiterea datelor (biţi de informaţie) 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 semnale electrice, iar în cazul fibrei optice s-a optat pentru transmiterea informaţiei sub formă de impulsuri optice. IEEE 802.11, cunoscut ca şi Wireless Fidelity (Wi-Fi), este standardul pentru comunicaţii în reţelele locale de calculatoare (LAN) care utilizează frecvenţele radio (radio frequencies – RF). Wi-Fi include în plus față de IEEE 802.11 și metodele de autentificare și criptare acceptate pentru interoperabilitate. IEEE 802.11 standardizează doar nivelul fizic și legătură de date din Modelul ISO-OSI.

Pentru a transmite date de la un emiţător la un receptor, semnalul RF trebuie manipulat astfel încât, staţia receptoare să poate face diferenţa 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).

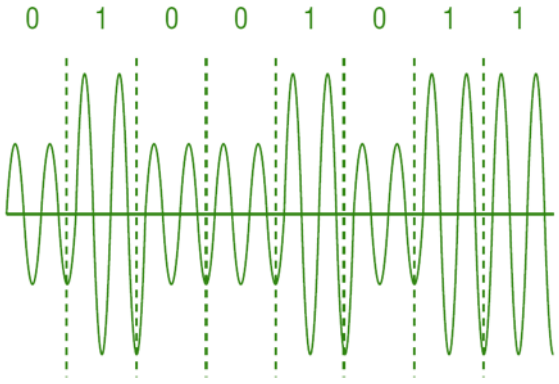


Figura 1. Tehnica ASK [1]

Modularea în amplitudine (Amplitude Shift Keying), utilizează modificarea amplitudinii semnalului pentru reprezentarea valorilor binare (fig. 1). Această tehnică este dificil de utilizat deoarece, semnalele RF pot fi afectate de zgomot sau interferenţe, ceea ce conduce la modificări ale amplitudinii semnalului iniţial. Astfel, este posibil ca receptorul sa interpreteze în mod eronat semnalul primit.

Modularea în frecvenţă (Frequency Shift Keying), variază frecvenţa semnalului pentru reprezentarea valorilor binare (fig. 2). Tehnica FSK a fost utilizată în primele standarde 802.11, fiind mai puţin practică, datorită resurselor de calcul necesare pentru procesarea unor semnale foarte rapide.

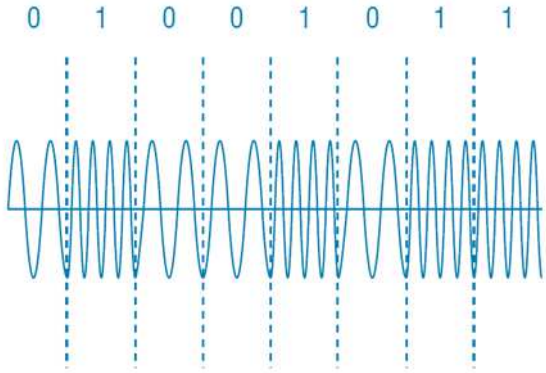
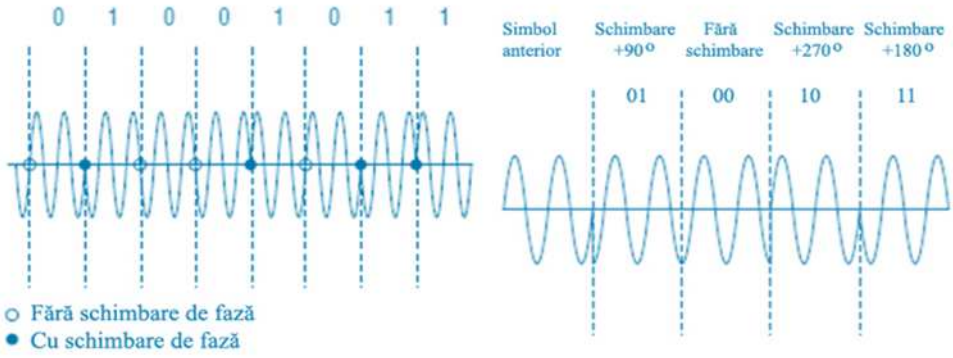


Figura 2. Tehnica FSK [1]

Modularea în fază (Phase Shift Keying), variază faza semnalului pentru reprezentarea valorilor binare (fig. 3). Tehnica PSK este larg utilizată în standarde 802.11.



a. b.

Figura 3. Tehnicile a.PSK şi b.QPSK [1]

Variante mai avansate ale acestei tehnici există, cum ar fi Quadrature Phase Shift Keying (QPSK), 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. Pentru a crește rata de transmisie, sistemele moderne folosesc modulații de tip QAM (Quadrature amplitude modulation) care folosesc o combinație de amplitudine și fază. Astfel, 16-QAM (Fig. 4) poate coda 4 biți, 64-QAM poate coda 6 biți, 128-QAM poate coda 8 biți, șamd.

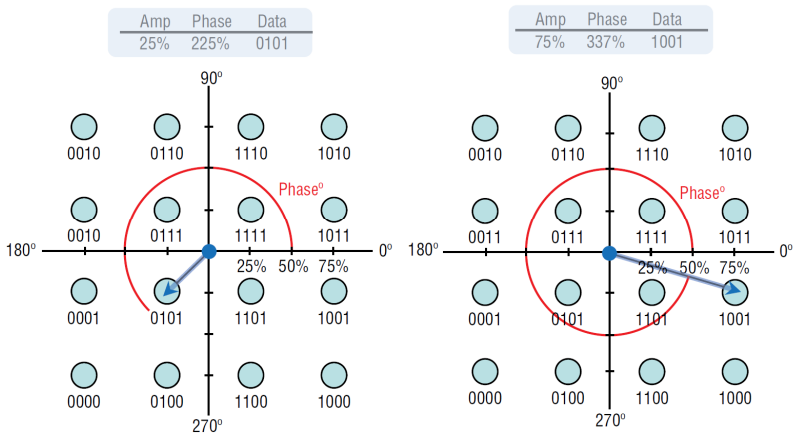


Figura 4. Exemplu 16-QAM [1]

Un sistem wireless de bază este compus din următoarele elemente: transmiţător, receptor, cablu de antenă, antene şi semnalul RF propagat (fig. 5).

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.

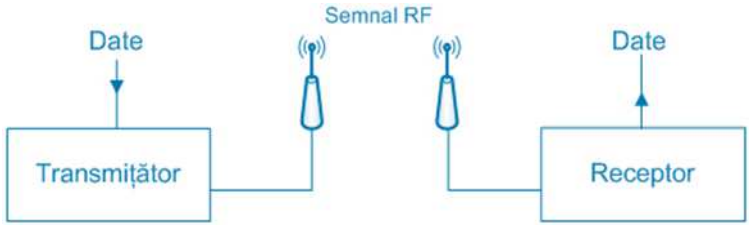


Figura 5. Comunicaţia wireless

Diferiţi factori pot influenţa modul de propagare a semnalului RF prin diferite medii [1]: absorbţia, reflexia, dispersia, refracţia, difracţia, atenuarea, amplificarea etc.

Absorbţia 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. Absorbţia conduce la atenuarea semnalului iniţial.

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

Dispersia poate fi descrisă ca fiind o reflexie multiplă (în multiple direcţii). Aceasta are loc când semnalul RF întâlneşte o suprafaţă neuniformă.

Fenomenul de refracţie se produce, în principal, datorită condiţiilor atmosferice (fig. 6). Acest fenomen poate fi definit ca, curbarea unui semnal RF la trecerea printr-un mediu cu o densitate diferită, provocând modificarea direcţiei undei. Câteva cauze ale refracţiei 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 suprafaţa pământului. Însă există şi cazuri în care semnalul poate fi refractat în atmosferă. Fenomenul de refracţie este foarte important în legăturile exterioare pe distanţe lungi.

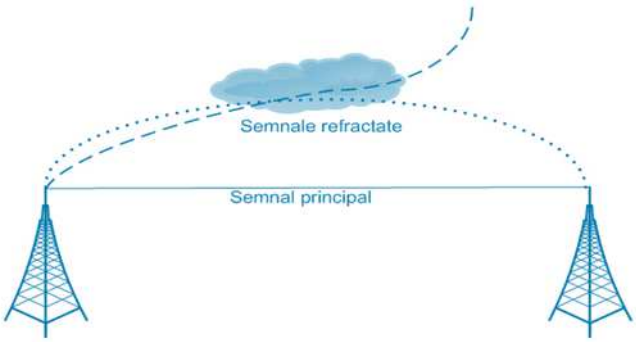


Figura 6. Fenomenul de refracţie

Un alt element important, alături de refracţie este fenomenul de difracţie, care se defineşte 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 funcţie de dimensiunile şi caracteristicile obstacolului şi în funcţie de caracteristicile semnalului RF, această zonă poate deveni o zonă fără acoperire sau, o zonă unde semnalul este recepţionat deteriorat.

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

Tabelul 1. Comparaţie material – atenuare [1]

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

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

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

unde FSLP – măsurat în dB, D – distanţa în km dintre antene şi f – frecvenţa în MHz. FSPL reprezintă o valoare ideală, deoarece este calculat considerând un spaţiu fără obstacole.

Pentru un calcul mai precis, la formula de mai sus, se poate adăuga câștigul/amplificările antenelor (la transmisie G_{tx} sau recepție G_{rx}), și pierderile cablurilor/echipamentelor utilizate pentru a transmite (la transmisie P_{tx} sau recepție P_{rx}). Astfel, formula devine:

$$FSLP = 32.4 + 20\log_{10}(f) + 20\log_{10}(D) + P_{tx} + P_{rx} - G_{tx} - G_{rx}$$

O altă problemă este datorată fenomenului de multicale (multipath). Acesta este un fenomen de propagare care presupune apariţia mai multor căi ale unui semnalului la receptor, simultan sau la intervale de câteva nanosecunde, datorită reflexiei, dispersiei sau difracţiei. De cele mai multe ori, acest fenomen conduce la alterarea semnalului primit (fig. 7). Un efect al fenomenului de multicale este amplificarea semnalului, cu condiţia ca multiplele semnale să ajungă la receptor în acelaşi timp şi în fază.

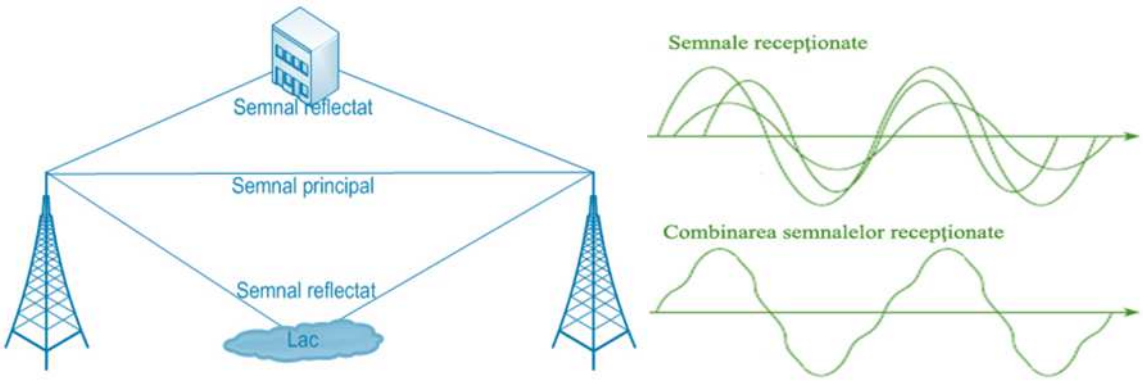


Figura 7. Fenomenul de multicale

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 unităţi de măsură, ci unităţi de comparaţie, utilizate pentru a reprezenta diferenţa dintre două valori (ex. diferenţa de putere dintre două AP-uri). Un decibel (db) reprezintă a 10 parte dintr-un bel (B) şi se calculează conform formulei:

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

, 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 proprietăţi când sunt măsurate în toate direcţiile – radiază uniform în toate direcţiile). 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 a compara un semnal cu 1 miliwatt de putere se utilizează dBm (decibeli relativ la 1 miliwatt). Diferenţa dintre dBm si celelalte unităţi prezentate este faptul că, dBm este o măsura de putere, nu de comparaţie. 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

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

Legea pătratului invers

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

, unde I – puterea la distanţa r, P – puterea iniţială, r – distanţa de referinţăfaţa de sursă.

2.3. Componente RF

Figura 8 prezintă, în mod sumar, componentele RF utilizate în transmisia fără fir: transmiţător-receptor, cablul de antenă, IR, EIRP, antena şi undele radio.

IR (Intentional Radiator) este definit ca un dispozitiv care generează şi emite în mod intenţionat energie în frecvenţă prin radiaţie sau inducţie. Acesta este alcătuit din toate componentele dintre transmiţător 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).

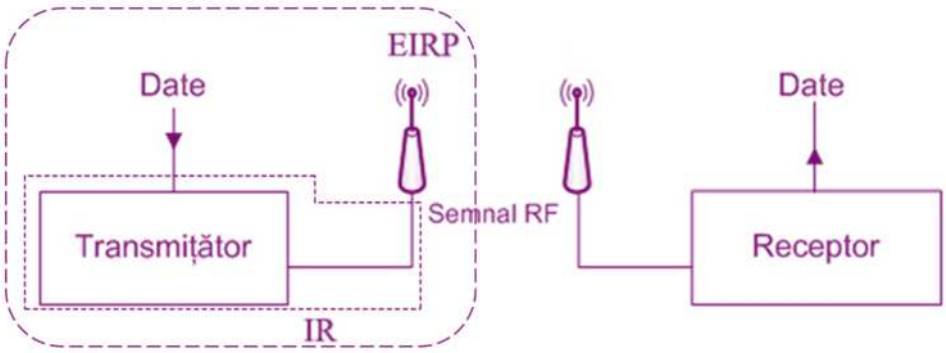


Figura 8. Componentele RF

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

RSSI este un parametru opţional 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 recepţionată. RSSI este unul dintre indicatorii utilizaţi 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 mulţi producători este dificilă.

SOM, cunoscut şi sub numele de link buget, este modul de calcul a cantităţii de semnal RF recepţionat. 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 influenţe externe. Pentru a ţine cont de această fluctuaţie, este o practică comună de a adăuga între 10 - 20 de dBs la valoarea senzitivităţii receptorului. Creşterea marginii de atenuare conduce la creşterea fiabilităţii legăturii.

3. Aplicaţii practice

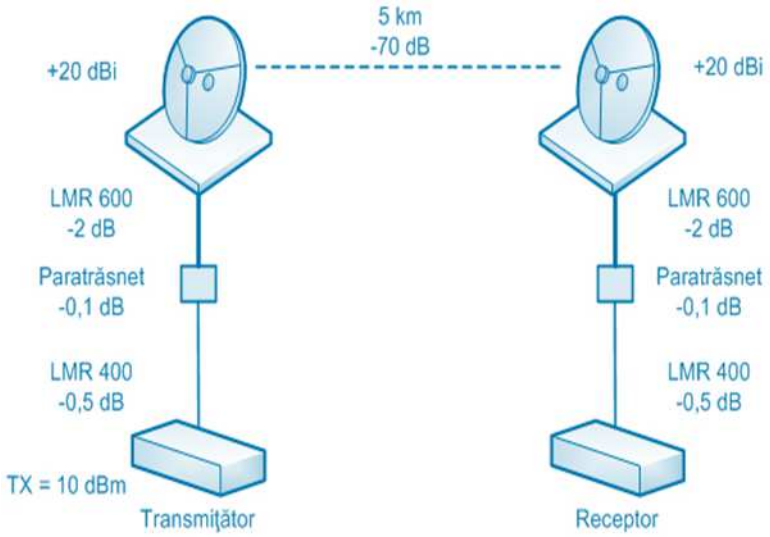
3.1. Se vor discuta caracteristicile semnalelor RF şi a principalelor componente de radio frecvenţă.

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

3.3. Se consideră un AP care generează un semnal de 40mW la o distanţă de 1 metru. Calculaţi puterea semnalului la o distanţă de 10 m, faţă de punctul de origine.

3.4. Se consideră un AP care generează un semnal de 20 dB. Acesta transmite, utilizând o antenă dipol 5dB, un semnal către un laptop aflat la o distanţă de 50 m, care introduce un FSPL egal cu -73.98 dB. Antena laptopului aduce un câştig de 2.14 dB. Senzitivitatea receptorului este de -71 dB (la 54 Mbps). Calculaţi puterea semnalului recepţionat şi valoarea parametrul SOM.

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



Sensibilitatea receptorului se consideră a fi de – 15 dBm. Calculaţi valoarea parametrului SOM (LMR reprezintă cablu coaxial cu pierderi reduse – Low-Loss Coaxial Cables).

Bibliografie:

[1] D. Coleman, D. Westcott, CWNA Certified Wireless Network Administrator Study Guide, Sybex Wiley Publishing, 2021.
[2] Cisco CCNA v7, https://www.netacad.com/

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 comunicaţia RF şi înţelegerea conceptelor matematice de bază necesare instalării antenelor de comunicaţie.

2. Consideraţii teoretice

2.1. Concepte de bază

Pentru realizarea procesului de comunicare între două sau mai multe transceivere, semnalul de frecvenţă radio (RF) trebuie să fie emis din antena transmiţătorului cu suficientă putere, astfel încât să fie recepţionat şi înţeles 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 influenţă majoră în cadrul comunicării şi determină dacă aceasta s-a realizat sau nu cu succes [1].

Dimensiunea unei antene este invers proporţională cu frecvenţa suportată: cu cât frecvenţa este mai mare, antena va fi mai scurtă. În mod clasic, dimensiunea minimă a unei antene, la orice frecvenţă, este de ½ din lungimea de undă λ. De exemplu, la frecvenţa de 2,4GHz, unde λ = 12,5 cm, lungimea unei antene dipol va fi de 6 cm; la frecvenţa de 5GHz, unde λ = 6 cm, lungimea unei antene dipol va fi de 3 cm). Formula pentru calculul este $\lambda = c / f$, unde λ - lungimea de undă (m), c - viteza luminii 299,792,458 (m/s), f – frecvența (Hz).

Două tipuri de câştig de semnal sunt utilizate în comunicaţiile RF: câştig activ și câştig pasiv. În cazul în care puterea este crescută utilizând anumite dispozitive electrice, cum ar fi un emiţător 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 direcţie, creşterea se va numi câştig pasiv. Câştigul pasiv este obţinut prin focalizarea puterii existente, iar câştigul activ este obţinut prin adăugare de putere.

În comerţ 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, ţinând cont de factorii din mediul înconjurător, care ar putea denatura semnalul.

Producătorii pun însă, la dispoziţia potenţialilor cumpărători, şabloane de radiaţie, cunoscute sub numele de diagrame de azimut şi de elevaţie. Şabloanele de radiaţii sunt create în medii controlate, unde rezultatele nu pot fi denaturate de influenţe externe şi reprezintă un

model de semnal care este radiat de un anumit model de antenă. Graficul arată puterea semnalului în fiecare locaţie relativ la fiecare altă locaţie, şi nu în raport cu o distanţă absolută de la antena sau cu un nivel absolut de putere.

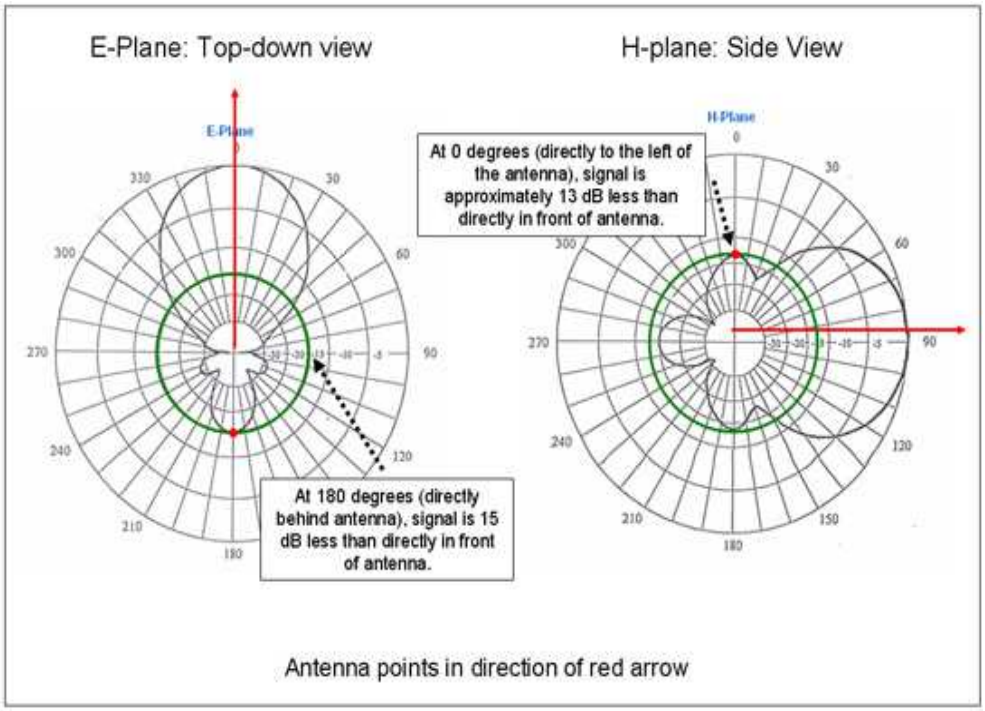


Fig. 1. Azimut şi elevaţie [2]

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

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 lăţimii fascicolului. Definiţia lăţimii fascicolului (cunoscută şi sub numele de lăţimea fascicolului la jumătate de putere) este unghiul dat de şablonul antenei (fascicolul) unde puterea relativă este la sau de peste 50% din puterea maximă.

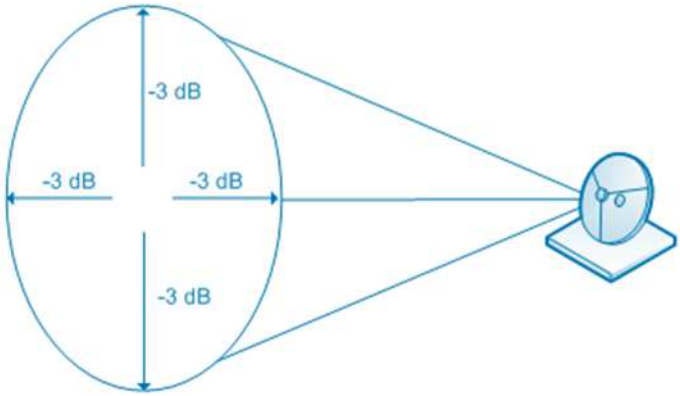


Fig. 2. Lăţimea fascicolului

Este important de reţinut că, deşi cea mai mare parte a semnalului RF generat este concentrat în zona lăţimii 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	Lăţime fascicol Orizontal (în grade)	Lăţime fascicol Vertical (în grade)
Omni-direcţională	360	7 – 80
Yagi	30 – 78	14 - 64
Parabolică	4 – 25	4 - 21

Tabelul 1. Lăţime 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 lăţimii fascicolului pentru diferite tipuri de antene.

2.2. Categorii de antene

Există trei mari categorii de antene: antene omni-direcţionale – concepute pentru a furniza acoperire în toate direcţiile, antene semidirecţionale – concepute pentru a furniza acoperire pe o anumită direcţie, însă pe o arie mai mare de acoperire şi antene ultra-direcţionale - concepute pentru a furniza acoperire pe o anumită direcţie [1].

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

Antene omni-direcţionale

Aceste tipuri de antene radiază semnalul RF în toate direcţiile. O antenă omni-direcţională 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 majorităţii 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-direcţionale 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). Lăţimea orizontală a fascicolului, pentru antenele omni-direcţionale este întotdeauna de 360 de grade, iar cea verticală variază, în funcţie antenă, între 7 şi 80 de grade.

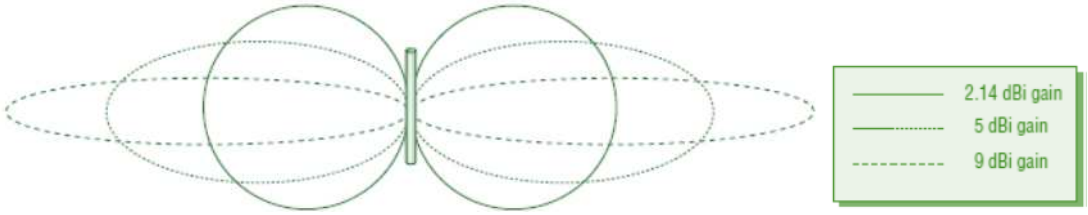


Figura 3. Şablon de radiaţie verticală a antenelor omni-direcţionale

Datorită acoperirii verticale foarte înguste, antenele omni-direcţionale de mare câştig trebuie instalate doar în situaţiile 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 recepţiona un semnal scăzut. Pentru instalarea interioară se alege, în mod uzual, o antenă omni-direcţională de câştig scăzut, aproximativ 2.14 dBi. Antenele omni-direcţionale de mare câştig se construiesc prin multiple antene dipol, suprapuse una peste alta, şi poartă numele de antene colineare.

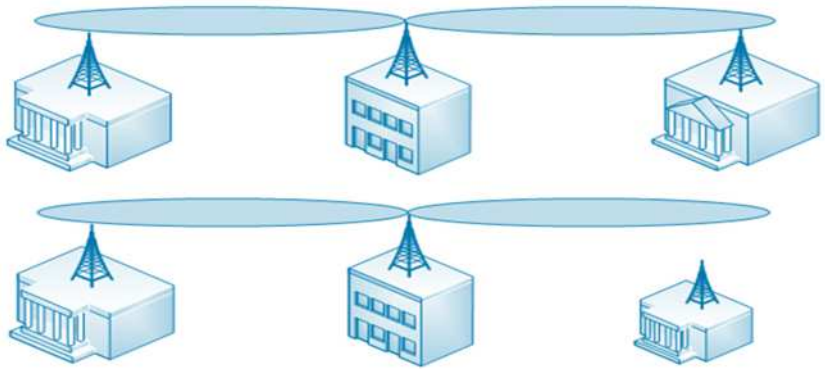


Figura 4. Cazuri de instalare în mediul exterior

Antenele omni-direcţionale sunt utilizate în mod frecvent în medii punct la multipunct. Antena omni-direcţională va fi conectată la un dispozitiv (AP) plasat în centrul dispozitivelor

client, pentru a oferi o acoperire cât mai largă. Antenele omni-direcţionale de mare câştig pot fi utilizate şi în exterior pentru a conecta mai multe clădiri într-o configuraţie punct la multipunct. O astfel de antenă va fi poziţionată pe o clădire centrală, iar pe celelalte clădiri se vor instala antene direcţionale îndreptate către clădirea centrală (fig. 4).

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

Antene semi-direcţionale

Antenele semi-direcţionale sunt proiectate pentru a radia semnalul RF spre o anumită direcţie. Sunt utilizate pentru distanţe mici şi medii, folosind ca bridge de reţea 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 direcţională în exterior pentru conexiuni punct la punct pe distanţe 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 lăţimea fascicolului orizontală de până la 180 de grade, doar o parte redusă de semnal va fi radiată în exteriorul clădirii. Utilizarea antenelor semi-direcţionale în interiorul clădirilor conduce la reducerea reflexiilor, minimizând efectele negative ale fenomenului de multicale. Pentru telefoanele mobile, senzorii IoT și alte dispozitive de comunicație wireless de mici dimensiuni se utilizează antene PIFA (Planar Inverted-F Antenna) din categoria antenelor F inversate, reprezentând un tip de antenă patch.

Din categoria antenelor yagi fac parte antenele clasice de televiziune de pe clădiri. Diferenţa faţă 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 recepţiona doar o gamă îngustă de frecvenţe. Antenele yagi sunt utilizate pentru comunicaţii punct la punct pe distanţe scurte sau medii, de până la 3 km. Un avantaj al antenelor semidirecţionale este posibilitatea instalării pe clădiri, la înălţime, inclinate în jos către aria de acoperire.

Antene ultra-direcţionale

Antenele ultra-direcţionale sunt utilizate strict pentru comunicaţiile punct la punct, de exemplu, pentru a furniza o legătură între două clădiri. Acestea pun la dispoziţie cele mai înguste lăţimi de fascicol dintre toate tipurile de antene. Există două tipuri de antene ultra-direcţionale: antene cu vas parabolice şi antene grid. Datorită câştigului foarte mare al acestora tipuri de antene, sunt ideale pentru comunicaţii pe distanţe mari, de până la 58 km. Însă datorită distanţelor lungi şi a lăţimii de fascicol înguste, antenele ultra-direcţionale sunt afectate de vânt, orice deviere a antenei conducând la o recepţie defectuoasă sau la întreruperea comunicaţiei. De aceea, indiferent de tipul de antenă instalat, calitatea montării va determina calitatea recepţiei.

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 mulţi utilizatori (sunt specializate, costisitoare şi nu sunt create special pentru 802.11), sau antenele sectoriale (antene semi-direcţionale, de câştig ridicat, utilizate frecvent în comunicaţiile celulare).

Este important de menționat că dispozitivele IEEE 802.11 sunt limitate la o valoare maximă de transmisie. Tabelul de mai jos (Tabel 2) sumarizează valorile EIRP maxime în spectrul 2,4GHz si 5GHz, conform standardelor ETSI în Europa [3]:

	2,4 GHz	5GHz RLAN band 1 (5,150 – 5,350 GHz) Interior	5GHz RLAN band 2 (5,470 – 5,725 GHz) Interior/Exterior	RLAN band 3 / Broadband Radio Access Networks (BRAN) (5,725 – 5,875 GHz)
EIRP	20 dBm (100 mW)	23 dBm (200 mW)	30 dBm (1000 mW)	36 dBm (4000 mW)

Tabelul 2. Valori maxime EIRP

2.3. Concepte pentru comunicaţia punct la punct

În general, comunicaţia punct-la-punct trebuie să aibă la dispoziţie o linie de vedere (line of sight – LOS) neobstrucţionată între două antene. În cazul comunicaţiilor RF acest lucru nu este suficient, deoarece este necesar ca şi zona din jurul LOS să fie fără obstrucţii. Aceasta zona din jurul LOS este cunoscută sub numele de zona Fresnel şi este adesea menţionată 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 influenţă neglijabilă.

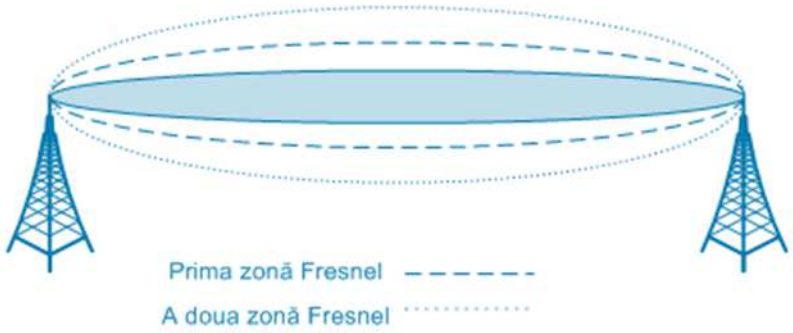


Figura 6. Zone Fresnel

Dacă prima zonă Fresnel este obstrucţionată, chiar şi parţial, integritatea comunicaţiei RF ar putea fi influenţată negativ, şi ar putea conduce la scăderea puterii semnalului recepţionat sau chiar la sistarea comunicaţiei. 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 distanţei:

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

, r – raza (m); D – distanţa (km), F – frecvenţa (GHz)

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

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

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

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

F – frecvenţa (GHz), N – zona Fresnel

Formula (1) este utilizată pentru a putea calcula la ce înălţime minimă faţă 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 ţinut cont şi de curbura pământului, care acţionează ca un obstacol, pe distanţe mari.

Parametrul *voltage standing wave ratio (VSWR)* este o măsură a modificărilor în impedanţă pentru un semnal AC [1]. Aceste modificări există datorită nepotrivirii sau variaţiei impedanţei dintre dispozitivele unui sistem de comunicaţii RF. Când un transmiţător generează un semnal radio AC, semnalul parcurge cablul către antenă. Însă, datorită nepotrivirii impedanţelor dintre cablu şi antenă, o parte din energie este reflectată înapoi către

transmiţător. VSWR este o relaţie numerică între valoarea maximă măsurată a tensiunii, generată de transmiţător, şi valoarea minimă măsurată a tensiunii, recepţionată de antenă. VSWR este, prin urmare, un raport de nepotrivire de impedanţă, cu 1:1 fiind optim (nu există nepotriviri de impedanţă), 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 impedanţelor echipamentelor utilizate şi verificarea mufării şi instalării corecte a acestora. Tabelul 3 prezintă efectul VSWR pentru grade diferite de nepotrivire de impedanţă.

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 3. Pierderi datorate VSWR [1]

2.4. Componente şi accesorii pentru antene

Cabluri RF

Următoarele aspecte trebuie luate în considerare în momentul alegerii cablurilor:
- impedanţa cablului (VSWR)
- gama de frecvenţe suportate
- pierderile introduse (dB)
- atenuare

Conectori RF

Următoarele aspecte trebuie luate în considerare în momentul alegerii conectorilor:
- impedanţa conectorului (VSWR)
- gama de frecvenţe 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 recepţie RF. LNA-urile amplifică semnalul recepţionat şi cresc puterea acestuia peste nivelul de zgomot produs de circuite ulterioare, oferind un câştig constant pe o anumită gamă de frecvenţe. Datorită faptului că semnalele recepţionate sunt de intensitate redusă şi includ zgomot considerabil, performanţa 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 frecvenţă, pentru a creşte SNR-ul sistemului de comunicaţie şi, de asemenea, pentru a îmbunătăţi 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 unidirecţional sau bidirecţional
- instalare aproape de antenă, pentru a compensa pierderea pe cablu

Atenuatoare RF

Atenuatoare sunt folosite într-o mare varietate de aplicaţii 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

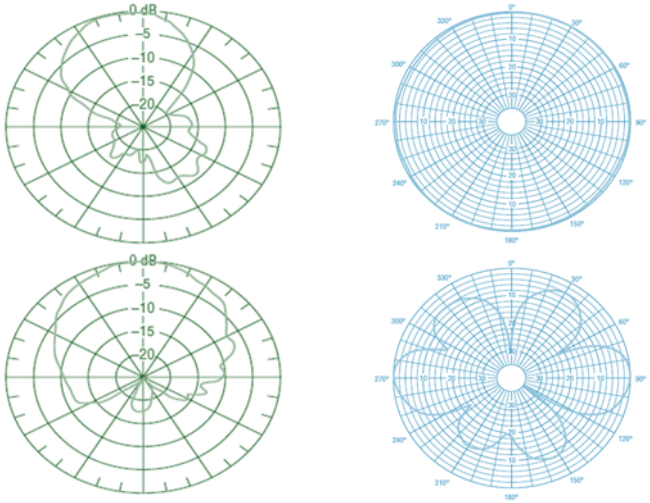
- protejează împotriva descărcărilor electrice
- instalare aproape de antenă

3. Aplicaţii practice

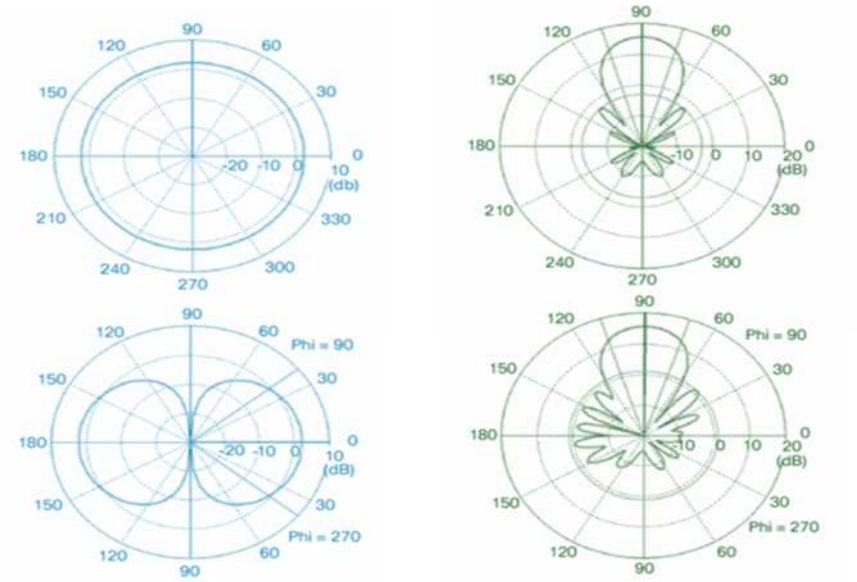
3.1. Se vor discuta principalele caracteristicile ale antenelor RF.

3.2. Vizualizați comportamentul undelor electromagnetice folosind utilitarul EMANIM: https://emanim.szialab.org/index.html

3.3. Interpretaţi diagramele de azimut şi elevaţie de mai jos. Ce tip de antenă prezintă acest tip de şablon radio?



a. b.



c. d.

3.4. Se consideră o legătură de comunicaţie punct la punct între două antene pe o distanţă de 10 km, utilizând o frecvenţă de 5.7 GHz. La ce înălţime minimă faţă de sol trebuie instalate antenele? Care ar fi valoarea utilizată în practică?

3.5. Se consideră o legătură de comunicaţie punct la punct între două antene pe o distanţă de 18 km, utilizând o frecvenţă de 2.4 GHz. La o distanţă de 4 km se află un obstacol înalt de 200 m. La ce înălţime minimă faţă de sol trebuie instalate antenele? Care ar fi valoarea utilizată în practică? Care este influenţa curburii pământului?

Bibliografie:

[1] D. Coleman, D. Westcott ,*CWNA Certified Wireless Network Administrator Study Guide*, Sybex Wiley Publishing, 2021.
[2] Essential Wi-Fi, http://www.connect802.com/e_images/E/antenna_graphs.jpg
[3] WLAN: Maximum Transmission Power (ETSI) https://wlan1nde.wordpress.com/2014/11/26/wlan-maximum-transmission-power-etsi/
[4] Cisco CCNA v7, https://www.netacad.com/

III. Conectarea la reţea

1. Obiective

Obiectivul acestui capitol este prezentarea principalelor topologii fără fir şi 802.11, a dispozitivelor utilizate în comunicaţia wireless şi înţelegerea modalităţilor de configurare şi testare a conexiunilor wireless în sistemele de operare Windows şi Linux.

2. Consideraţii teoretice

2.1. Topologii wireless

Standardul IEEE 802.11 se referă la reţelele locale de comunicaţii (LAN) cu ajutorul frecvenţelor radio (RF) [1]. Alături de reţelele 802.11, există alte tehnologii şi standarde de comunicaţii 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 Local Area Network(WLAN) și Wireless Personal Area Network (WPAN).

O reţea de arie largă (WAN) acoperă o vastă arie geografică. O reţea WAN poate acoperi o regiune, o ţară, și poate fi extinsă la nivel global. 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 comunicaţiile cu fir WAN includ Frame Relay, ATM, MPLS, etc. O reţea de arie largă fără fir (WWAN) acoperă, de asemenea, zone geografice întinse utilizând un mediu wireless. Reţelele WWAN utilizează, în general, tehnologiile reţelelor 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 laptopurile sau telefoanele mobile, însă ratele de date şi lăţimea de bandă ale acestor tehnologii sunt relativ mai lente, în comparaţie cu alte tehnologii fără fir, cum ar fi 802.11. Cu toate acestea, există noi tehnologiile celulare cu rate de transfer de date îmbunătăţite, de exemplu 5G. De asemenea, noi protocoale, precum LoRaWAN, sunt utilizate pentru interconectarea sistemelor (Intenet of Things) IoT [3]. Este important de reţinut însă, că infrastructura 802.11 nu poate fi utilizată ca un WWAN.

O reţea metropolitană fără fir (WMAN) oferă o acoperire unei zonei metropolitane, cum ar fi un oraş. De tehnologia comunicaţiei fără fir WMAN este asociat standardul, definit de grupul 802.16 - acces fără fir în bandă largă, cunoscut sub numele de Worldwide Interoperability for Microwave Access (WiMAX). WiMAX este un competitor al serviciilor în bandă largă DSL sau cablu. De asemenea, tehnologiile celulare cu rate de transfer de date îmbunătăţite, de exemplu 5G, sunt utilizate pentru a oferi conectivitate în zonele urbane. Adițional, rețelele fără fir de tip mesh (WMN) sunt utilizate în contextul orașelor inteligente.

O reţea personală fără fir (WPAN) este o reţea de calculatoare fără fir utilizată pentru comunicarea între diferite dispozitive aflate în imediata apropiere a unui utilizator. Diferite dispozitive, cum ar fi laptop-urişi telefoanele mobile pot comunica între ele folosind o varietate de tehnologii fără fir. Cele mai frecvente tehnologii fără fir în domeniul reţelelor WPAN sunt tehnologiile Bluetooth (802.15.1), infraroşu (IrDA), ZigBee și, în anumite cazuri de utilizare, tehnologia NFC – Near Field Communication. Transmisia în infraroşu utilizează un mediu bazat pe unde optice, în timp ce Bluetooth folosește un mediu de frecvenţe radio. ZigBee (802.15.1) este o altă tehnologie RF care are un potenţial de cost scăzut de reţea fără fir între dispozitive, într-o arhitectură WPAN.

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

Figura 1 ilustrează principalele diferenţe dintre aceste tehnologii, punând în evidenţă nivelul de acoperire şi exemple de tehnologiile utilizate:

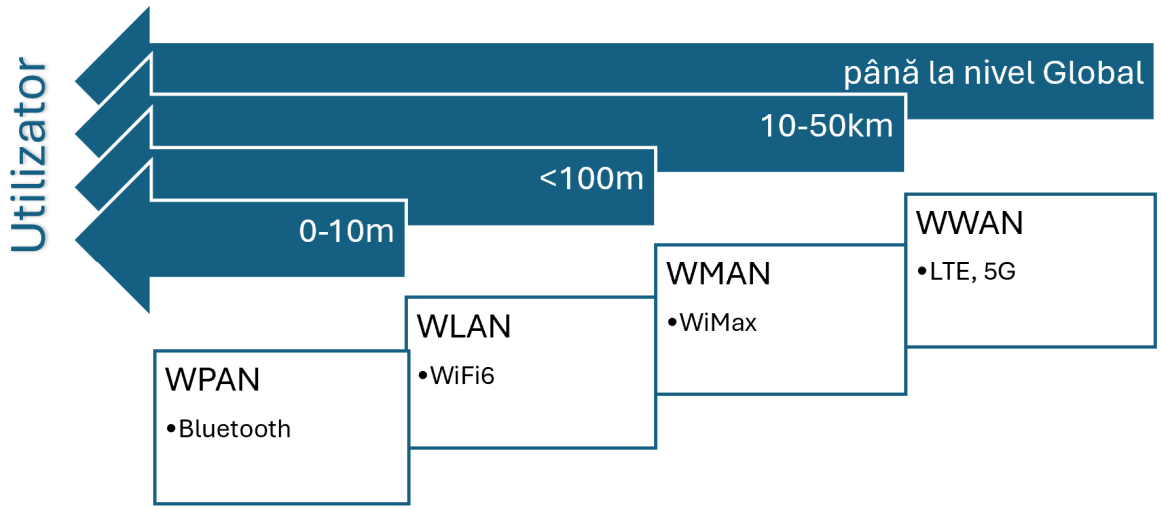


Figura 1. Topologii fără fir

2.1. Topologii 802.11

IEEE defineşte tehnologiile 802.11 referitoare la nivelul Fizic şi la subnivelul MAC al nivelului Legăturii de Date (reamintiţi-vă modelul ISO / OSI).

Principalele amendamente 802.11 sunt [2]: 802.11a , 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax şi, recent 802.11be. Aceste tehnologii operează în banda de frecvențe 2.4GHz *Industrial, Scientific, and Medical (ISM),* 5GHz *Unlicensed National Information Infrastructure (U-NII)* și, recent 6GHz . Banda 2.4 GHz ISM este mult mai aglomerată decât 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 potenţiale de interferenţă.

Obiectivul standardului 802.11n, cunoscut ca Wi-Fi 4, a fost de a creşte rata de transfer atât în banda de frecvenţă 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) împreună cu Orthogonal Frequency Division Multiplexing (OFDM). Tehnologia MIMO foloseşte antene multiple pentru recepţie 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 îmbunătăţirea ratei de transfer şi a ariei de acoperire.

Standardul 802.11ac, cunoscut și sub numele de Wi-Fi 5, utilizează banda de frecvență de 5GHz și are o posibilă o rată de transfer de până la 6.9 Gbps. Standardul a marcat introducerea tehnologiei multi-user MIMO (MU-MIMO) care permite transmiterea simultană a unui semnal către mai mulți clienți în cadrul aceluiași canal. 802.11ac permite utilizarea mai multor fluxuri spațiale (spatial streams sau spatial multiplexing) pentru a îmbunătăți performanța rețelei fără fir. Fluxurile spațiale reprezintă fluxurile independente de date care pot fi transmise simultan între un punct de acces si un dispozitiv client.

Standardul 802.11ax, cunoscut și sub numele de Wi-Fi 6 utilizează benzile de frecvență 2,4GHz și 5GHz și are o posibilă o rată de transfer de până la 9.6 Gbps. Standardul a adus o noua tehnologie de multiplexare denumită Orthogonal Frequency-Division Multiple Access (OFDMA). Extensia standardului 802.11ax, denumită Wi-Fi 6E, utilizează și banda de frecvență 6GHz. Standardul a adus și îmbunătățiri la nivel de securitate prin suport WPA3.

Standardele viitoare, precum 802.11be (Wi-Fi 7) vor aduce îmbunătățiri ale ratei de transfer - teoretic până la 46 Gbps, a ariei de acoperire și scăderea latenței de transmisie.

Tabelul 1 sumarizează caracteristicile amendamentelor 802.11 a, b, g, n, ac, ax:

	802.11a	802.11b	802.11g	802.11 n Wi-Fi4	802.11ac Wi-Fi5	802.11ax Wi-Fi6/6E
Frecvenţa	5 GHz	2.4 GHz	2.4 GHz	2.4, 5 GHz	5 GHz	2.4, 5, 6 GHz
Tehnologie de transmisie	*OFDM*	HR-DSSS	*OFDM, DSSS*	*OFDM, MIMO*	*OFDM, MU-MINO*	*OFDMA*
Rate de Transfer	până la 54 Mbps	până la 11 Mbps	până la 54 Mbps	până la 600 Mbps	până la 6.9 Gbps	până la 9.6 Gbps
Standardizat	*1999*	*1999*	*2003*	*2008*	*2014*	*2019/2020*

Tabelul 1. Comparaţie 802.11 a, b, g, n, ac, ax

În IEEE 802. 11 sunt definite două moduri de operare: mod infrastructură şi mod ad-hoc [4].

În *modul Infrastructură* (fig. 2), reţeaua fără fir este formată din cel puţin un punct de acces (AP) conectat la infrastructura reţelei cablate şi un set de staţii wireless. Un punct de acces controlează modul de criptare în reţea şi poate înainta sau ruta traficul wireless către o reţea cablată sau în Internet. Această configuraţie este denumită Basic Service Set (BSS). Punctele de acces care acţionează ca routere pot, de asemenea, atribui adrese IP către staţii 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.

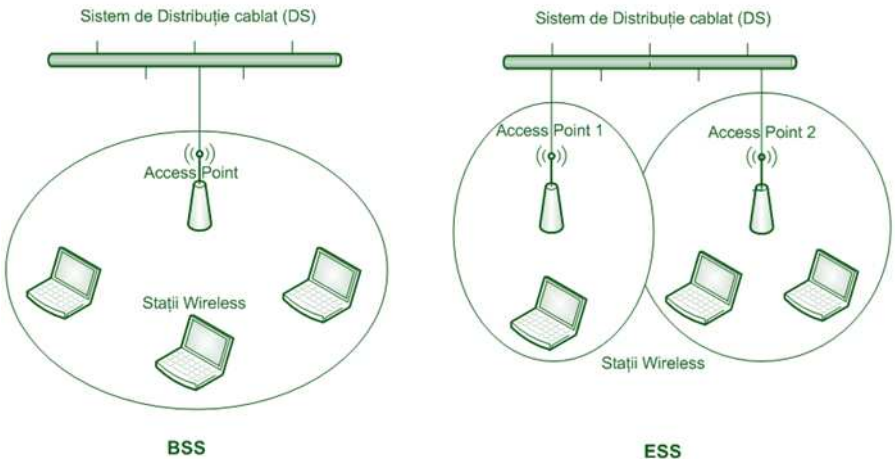


Figura 2. Mod Infrastructură

Un Extended Service Set (ESS) este alcătuit din două sau mai multe BSS-uri care formează o singură subreţea. Traficul este înaintat de la un BSS la altul, pentru a facilita circulaţia staţiilor wireless între BSS-uri. Aproape întotdeauna, sistemul de distribuţie (DS) care conectează aceste reţele este un LAN Ethernet. Există însă şi sisteme de distribuţie fără fir (WDS) care conecteză AP-urile. Deoarece marea majoritate a reţelelor fără fir necesită conectarea la reţeaua 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 reţea – *Service Set Identifier (SSID)* sau *Extended Service Set Identifier (ESSID)*. Există posibilitatea ca AP-urile dintr-un ESS să aibă nume de reţea diferite, şi totuşi sa aparţină de acelaşi ESS.

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

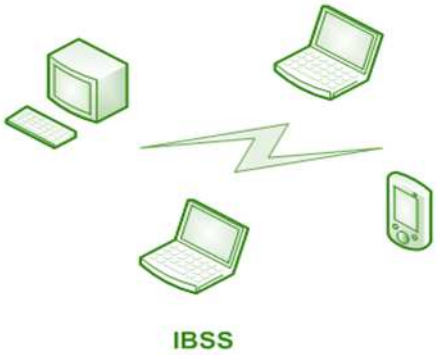


Figura 3. Mod Ad-Hoc

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

2.2. Dispozitive wireless

O *staţie client* este definită ca un card radio, care nu este folosit într-un AP. Staţiile 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 reţea wireless. Într-o reţea cablată, echivalentul acestui dispozitiv îl reprezintă în general, switch-ul de rețea.

Un access point poate fi privit ca un hub wireless, însă cu câteva îmbunătăţiri, prezentând şi capabilităţi de switch. Principala funcţie a unui AP este funcţia de bridging, direcţionând traficul, fie la backbone-ul reţelei, fie înapoi în mediul fără fir. O staţie 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 PCIe, 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.

Figura 4. Exemplu de adaptoare wireless Linksys

Pentru dispozitivele desktop, *adaptoarele radio PCIe* (Peripheral Component Interconnect Express) 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 menţionat faptul că, cardurile radio 802.11 folosite ca şi clienţi, se utilizează şi în alte tipuri de dispozitive mobile, console de jocuri, telefonie VoIP wireless, senzori, etc.

Majoritatea sistemelor moderne, indiferent dacă sunt laptopuri, desktopuri, sisteme All-in-One, tablete sau smartphone-uri, sunt echipate în mod standard cu interfețe de comunicație wireless, eliminând necesitatea utilizării unor adaptoare suplimentare.

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

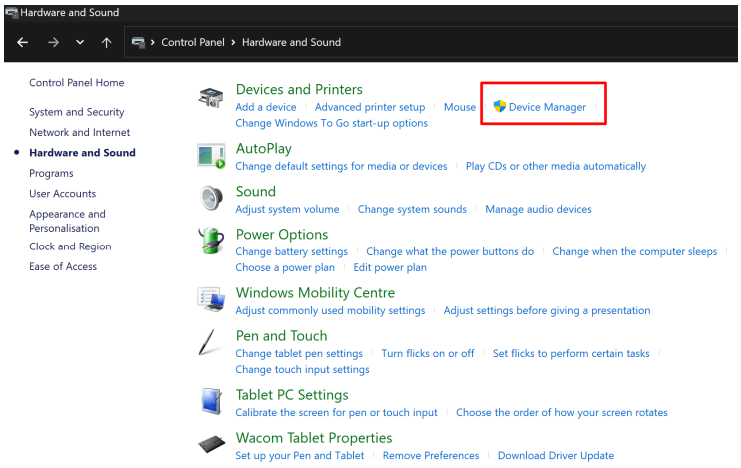
În cadrul sistemelor de operare Windows, instalarea unui dispozitiv de comunicare fără fir se efectuează în mod similar cu instalarea unui dispozitiv de comunicaţie cu fir. Instalarea şi configurarea stivei de protocoale TCP/IP, cât si principalele comenzi pentru testarea conectivităţii unei reţele de calculatoare, sunt considerate cunoscute din cadrul laboratorului "Reţele de calculatoare" [5].

Windows 11

Sistemul de operare Windows 11 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 va utiliza software-ul de instalare sau, se vor descărca de pe site-ul producătorului driver-ele aferente.

Verificarea adaptoarelor instalate se realizează urmărind următorii paşi:

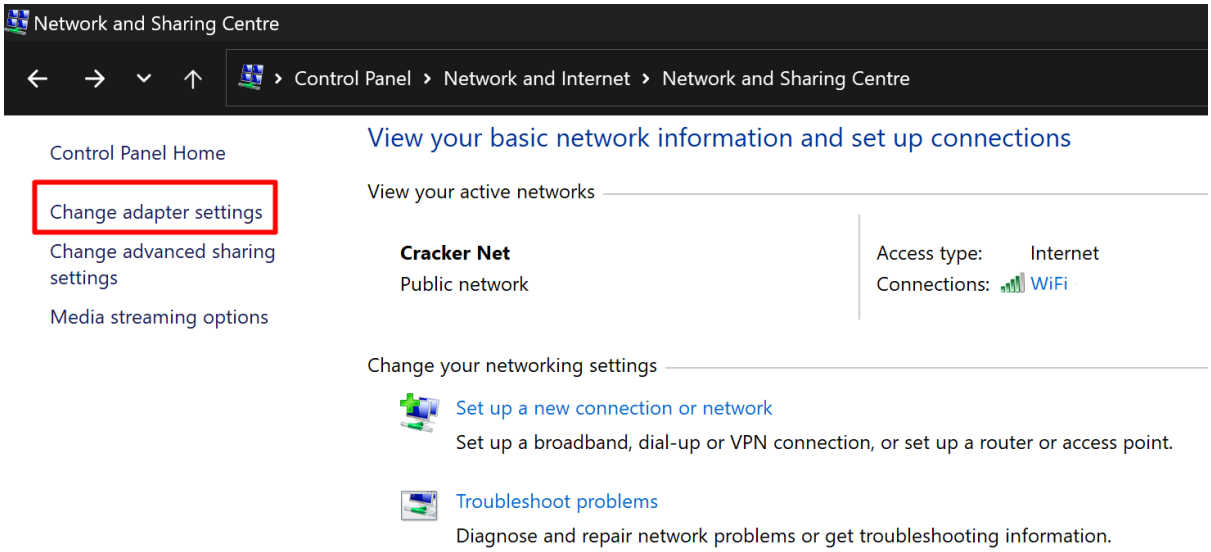
- click *Start* menu, se caută Control *Panel* App, se selectează selectaţi opţiunea *Hardware and Sound* şi *Device Manager*



- click simbolul (+) de la linia *Network adapters*
- adaptoarele wireless instalate trebuie să apară în această listă

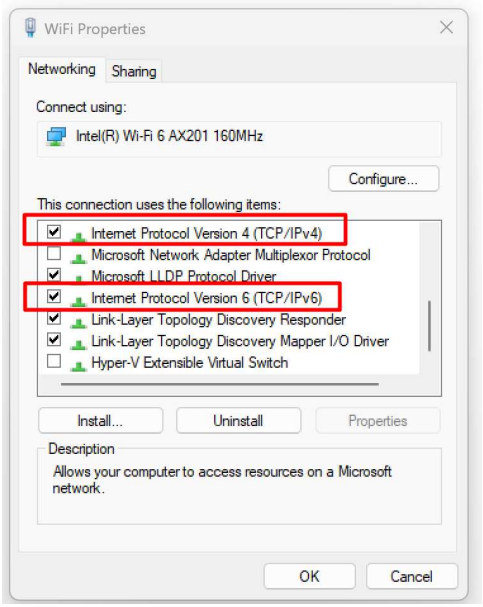
Configurarea adaptoarelor instalate se realizează urmărind următorii paşi:

- se caută Control *Panel* App, se selectează selectaţi opţiunea *Network and Internet*, apoi *Network and Sharing Centre* și *Change Adapter Settings*



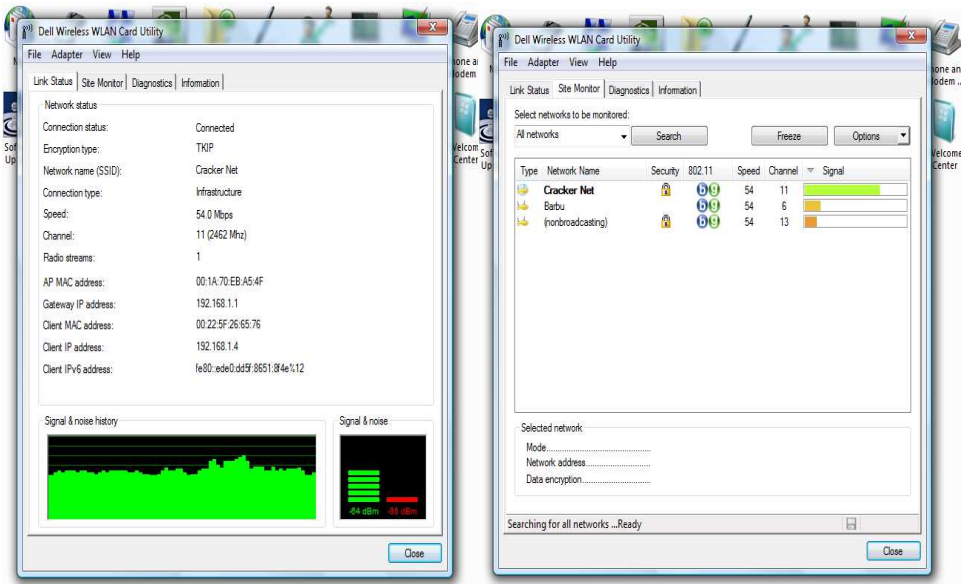
- right-click pe numele adaptorului de reţea wireless şi selectaţi opţiunea *Properties*

- verificaţi ca opţiunile *Internet Protocol Version 4 (TCP/IPv4)* şi *Internet Protocol Version 6 (TCP/IPv6)* să fie selectate

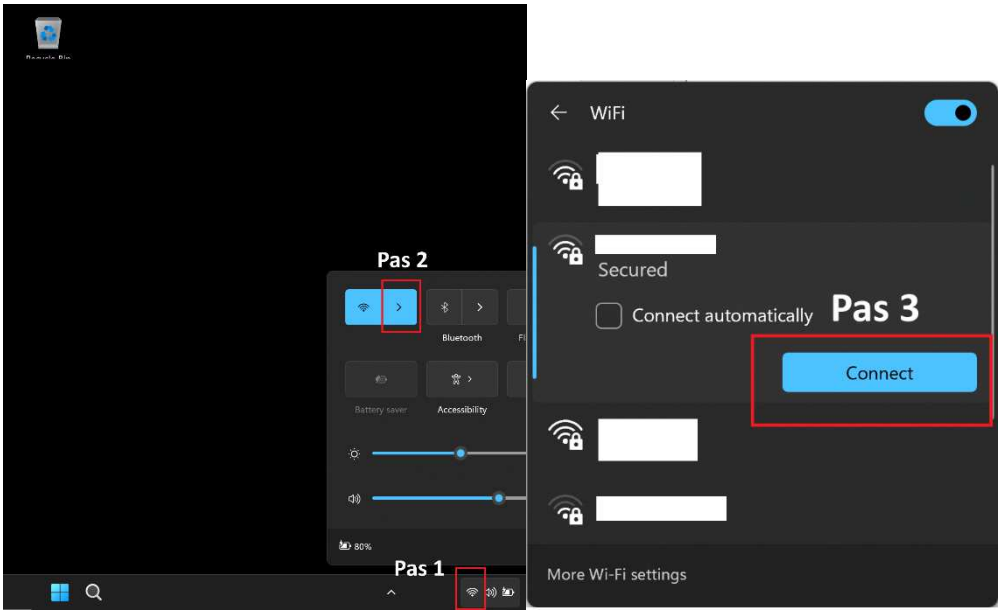


- selectaţi *Internet Protocol Version 4 (TCP/IPv4)* şi *Internet Protocol Version 6 (TCP/IPv6* şi apoi *Properties* pentru a configura opţiunile TCP/IP, asemenea unui dispozitiv de reţea cablat.

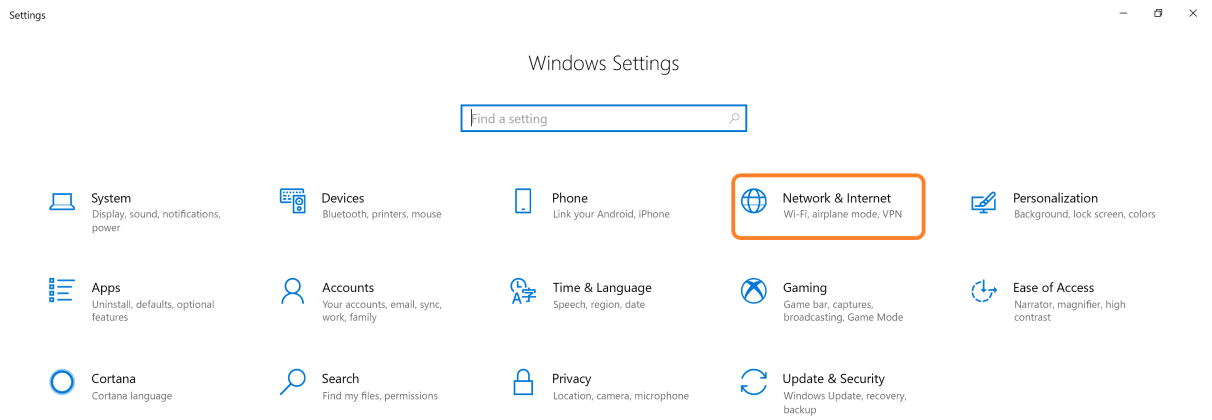
Marea majoritatea a producătorilor de plăci wireless, pun la dispoziţia utilizatorilor diferite programe pentru monitorizarea şi diagnosticarea conexiunilor wireless (exemplu utilitar pentru Dell Wireless Card):

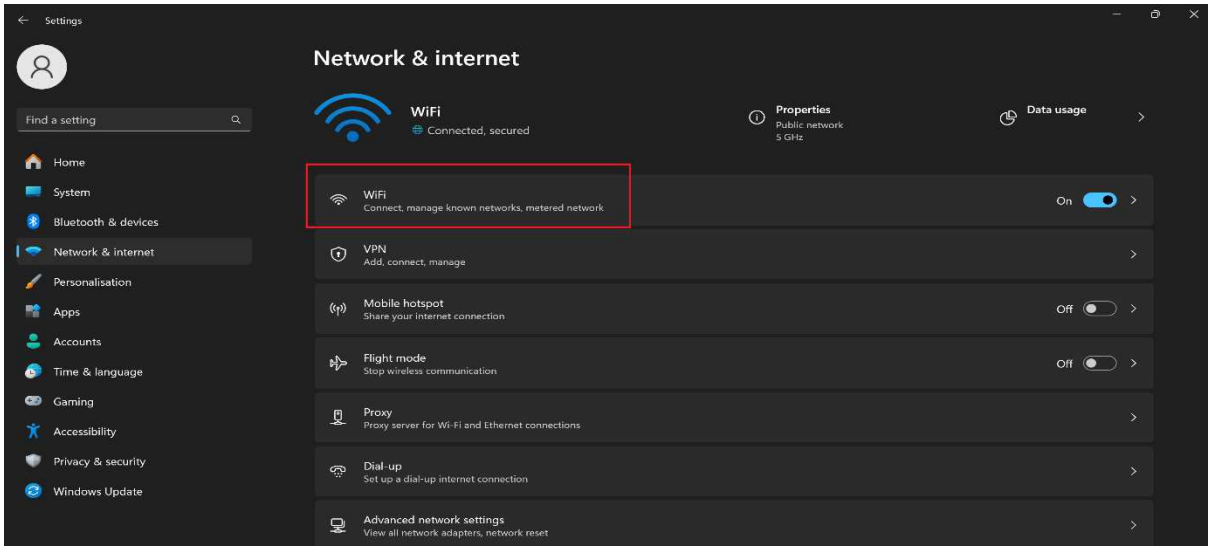


Pentru conectarea la o rețea WiFi și pentru vizualizarea informațiilor despre aceste rețele, se pot urma mai multe metode. Prima metodă presupune utilizarea icoanei de rețea (network icon) disponibilă în bara Taskbar, alegerea rețelei dorite, click pe butonul *Connect*, se introduce parola (sau alte credențiale), apoi click pe butonul *Next*.

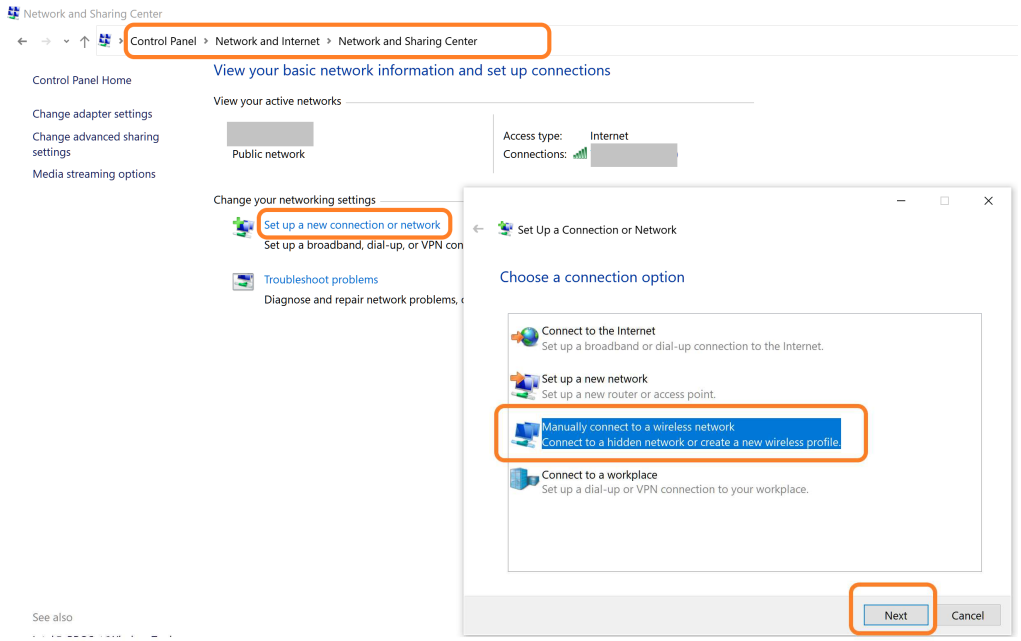


Cea de-a doua metodă presupune accesarea setărilor Windows prin secvența de pași: Start -> *Windows Settings* -> *Network and Internet* sau Start -> *Settings* -> *Network and Internet* -> *WiFi* -> *Show available Networks*. Mai apoi, se repetă pașii din prima metodă prezentată.

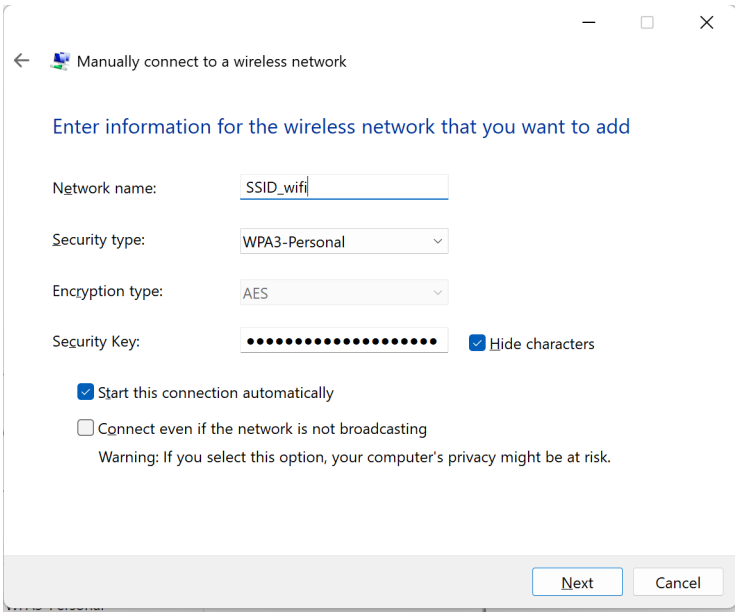




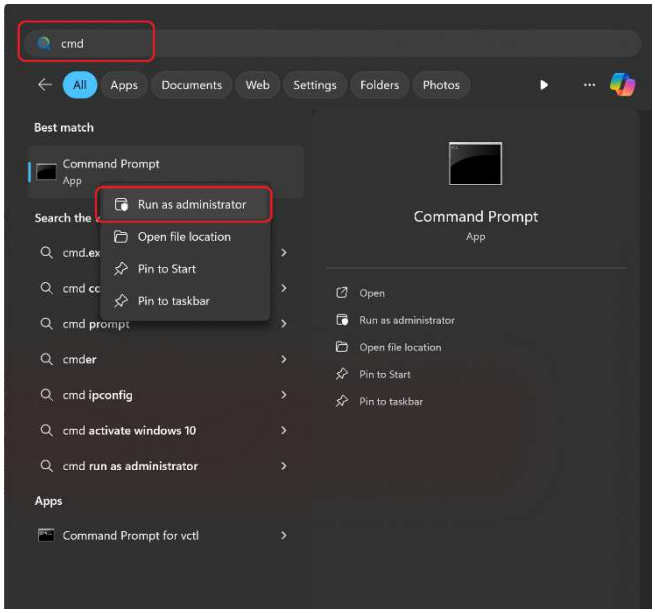
Pentru conectarea manuală la o rețea fără fir se vor urma pașii: Start -> *Control Panel* -> *Network and Internet* -> *Network and Sharing Center* -> *Set up a new connection or network*



Se vor introduce numele rețelei la care se dorește conectarea, se alege tipul de securitate folosit (preferabil soluții WPA3) și se introduc credențialele (parola sau altă metodă).



După instalarea și conectarea la rețelele de comunicație fără fir, următorul pas este vizualizarea informațiilor despre plăcile de rețea pentru a verifica corectitudinea configurațiilor. Vizualizarea se poate face fie utilizând *command prompt* sau utilitarul *netsh*. Pașii pentru utilizarea *command promt* sunt: click Start -> scriem comanda *cmd* în bara de căutare, iar apoi click dreapta pe icoana respectivă și se alege *Run as administrator*. În command prompt se va rula comanda *ipconfig /all* și se vor căuta plăcile de rețea *Wireless LAN adapter WiFi*.



Odată ajunși în consola *command prompt*, se poate utiliza utilitarul *netsh* (network shell). Comenzile uzuale sunt:

>*netsh* wlan show interface
>*netsh* wlan show profile
>*netsh* wlan show networks
>*netsh* wlan show wlanreport

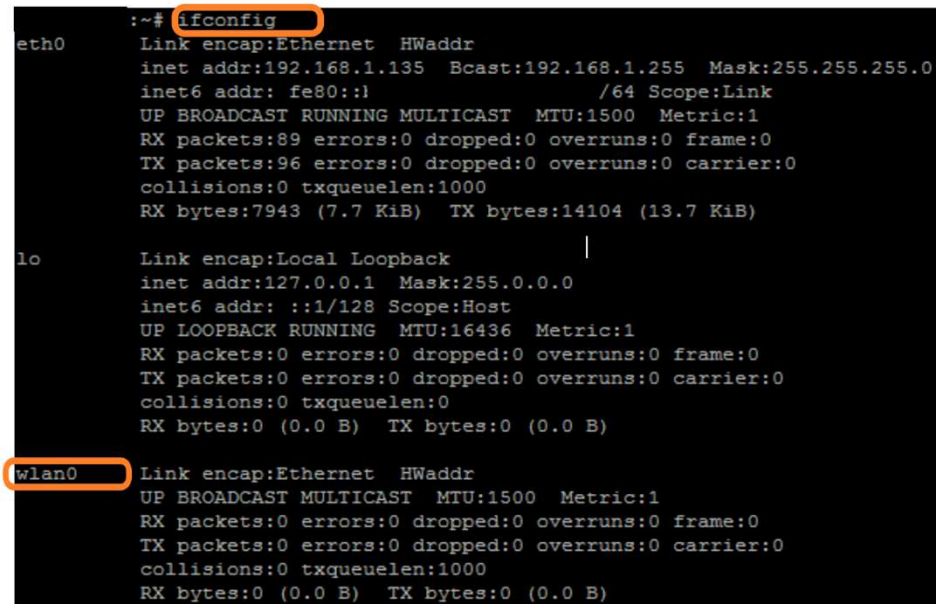
Linux

PCMCIA

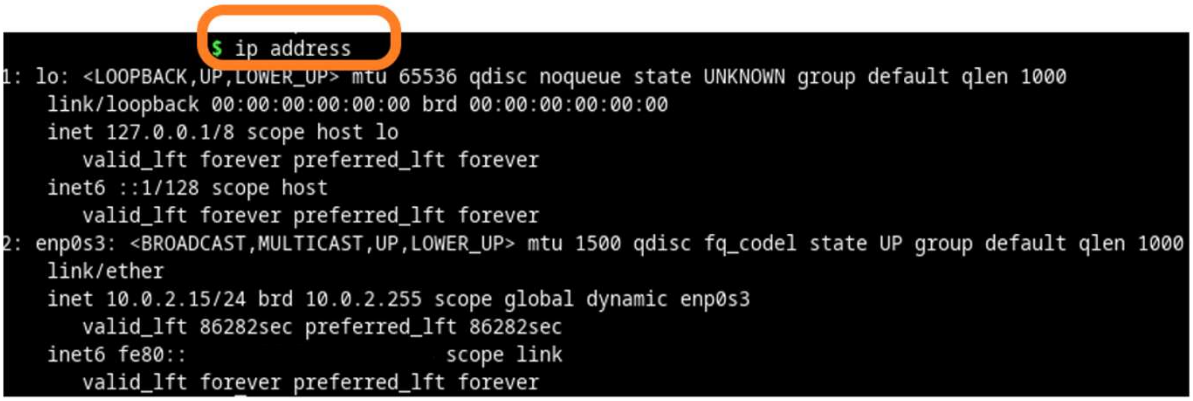
- Instalare
- Verificare si control
  - [...]#cardctl eject 0
  - [...]#cardctl insert 0
  - Vizualizare Card Information Structure (CIS):
    - [...]#cardctl info 0
    - [...]#cardctl ident 0
    - [...]#dump_cis
  - [...]#cardctl status 0
  - [...]#cardctl config 0

Wireless Network Adapters

- Vizualizare informaţiilor se face utilizând setul de comenzi disponibile în pachetul *net-tools* (ifconfig, route, nameif, iwconfig, netstat, etc) și în pachetul *iproute2util* (ip)
  - [...]#ifconfig



  - [...]#iwconfig
  - [...]#ip



- Căutare reţele
  - [...]#iwlist eth1 scan
- Căutarea unei reţele (căutare după SSID)
  - [...]#iwconfig ath0 essid “SSID Reţea”
  - [...]#ifconfig ath0 up
  - [...]#iwconfig ath0
- Vizualizare informaţii canale disponibile
  - [...]#iwlist ath channel
- Selectarea frecvenţei/canalului (pentru plăci care nu au suport de scanare)
  - [...]#iwconfig ath0 freq 2.462G
  - [...]#iwconfig ath0 channel 11
- Setarea modului reţelei
  - [...]#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

Exemplu de configurare WiFi:

ifconfig wlan0 up

- comada pentru activarea interfetei wireless

iwlist wlan0 scan

- comanda pentru vizualizarea retelelor wireless disponibile

iwconfig wlan0 essid WIFI_NETW key SEC_KEY

- comanda pentru configure, unde WIFI_NETW este numele retelei la care se doreste conectarea si SEC_KEY este cheia de securitate pentru acea retea

dhclient wlan0

- comanda pentru cerere adresa IP prin protocolul DHCP

3. Aplicaţii practice

3.1. Se vor discuta caracteristicile principalelor topologii 802.11.

3.2. Se vor instala, configura şi testa, utilizând sistemul de operare Windows 11, diferite dispozitive de comunicaţie wireless: PCI/PCIe adapter, PCMCIA adapter, USB adapter.

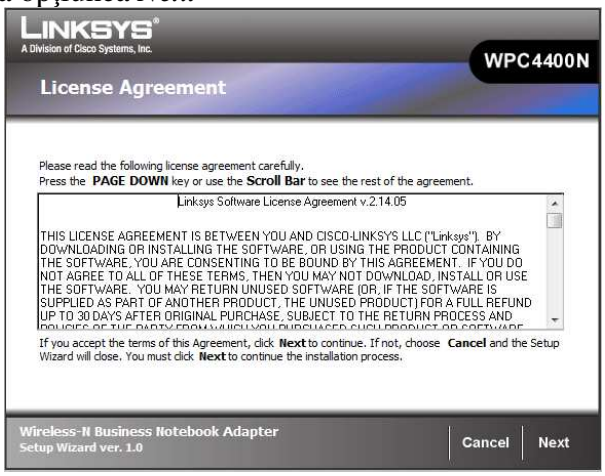
Instalarea şi configurarea PCI adapter (Linksys Wireless-N WMP300N)

- se va utiliza software-ul de instalare (Setup Wizzard software)
- 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)

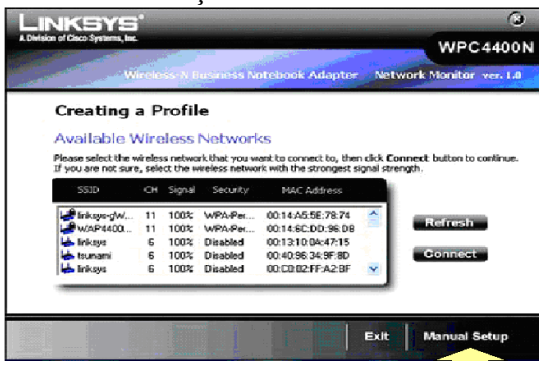
- se va utiliza software-ul de instalare (Setup Wizzard software)
- se va selecta opţiunea *Click Here To Start*

- se va selecta opţiunea *Next*



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

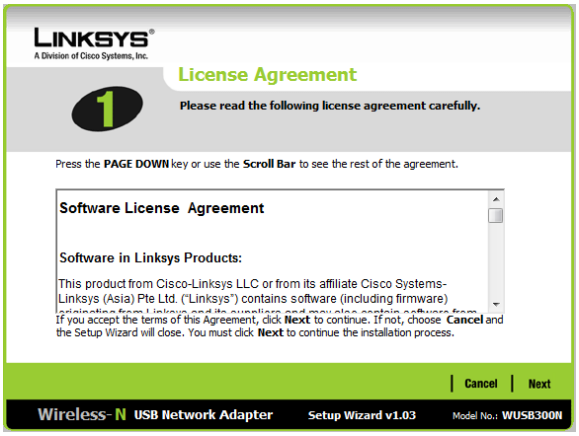
- pentru Windows, va apărea fereastra *Found New Hardware Wizard*, unde se va selecta opţiunea *Next*, iar apoi, în următoarea fereastră *Install Software Automatically (Recommanded)*
- se va realiza conexiunea la reţeaua wireless dorită



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

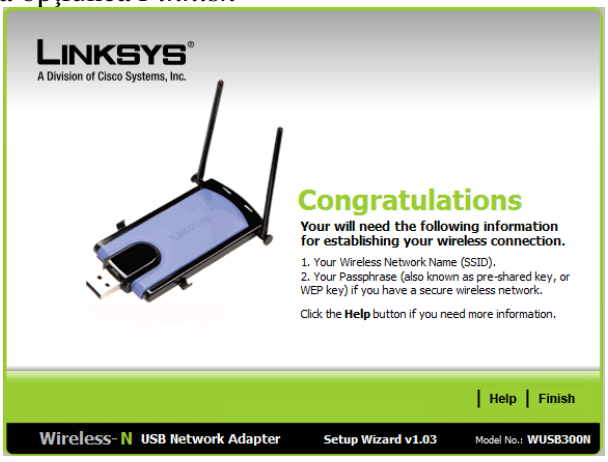
- se va utiliza software-ul de instalare (Setup Wizzard software)
- se va selecta opţiunea *Click Here To Start*

- 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 opţiunea *Finnish*



- se va realiza conexiunea la reţeaua 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 comunicaţie wireless: PCI/PCIe adapter, PCMCIA adapter, USB adapter.

3.4 Se vor conecta dispozitivele client la rețeaua wireless și se vor vizualizarea informațiile WiFi utlizând sistemele de operare Windows și Linux.

Bibliografie:

[1] M. Gast, *802.11 Wireless Networks: The Definitive Guide*, O'Reilly, 2002, 2005.
[2] D. Coleman, D. Westcott ,*CWNA Certified Wireless Network Administrator Study Guide*, Sybex Wiley Publishing, 2021.
[3] LoRaWAN, https://lora-alliance.org/about-lorawan/
[4] Cisco CCNA v7, https://www.netacad.com/
[5] A. Peculea, B. Iancu, S. Buzura, V. Rațiu, coord. V. Dădârlat, E. Cebuc, *Retele de calculatoare. Aplicatii practice*, Ed. U.T. Press, ISBN: 978-606-737-730-9, 2024.
[6] Wi-Fi Alliance, https://www.wi-fi.org/

IV. Analiza mediului RF: Netscout/netAlly AirCheck G2 Wireless Tester

1. Obiective

Obiectivul acestui capitol este prezentarea modului de utilizare a instrumentului de testare Netscout AirCheck G2 pentru analiza dispozitivelor şi a traficului în reţelele fără fir, precum și depanarea reţelelor fără fir.

2. Consideraţii teoretice

2.1. Introducere

Dispozitivul Netscout/netAlly AirCheck G2 (fig. 1) este destinat analizei și depanării problemelor din reţelele fără fir de tip 802.11 (802.11b/g/n/ax în banda de frecventă 2.4GHz și 802.11a/n/ac/ax în banda de frecventă 5GHz). Poate fi folosit, de către specialiștii IT, în diferite medii de lucru, de la spații de locuit și birouri până la spații industriale și locații publice.

Figura 1. Netscout/netAlly AirCheck G2 [1]

Câteva avantaje ale utilizării dispozitivului Netscout/netAlly AirCheck G2 sunt:

- rezolvarea problemelor de conectivitate, configurare și performanță în rețelele 802.11 (inclusiv 802.11ac si 802.11ax), într-un mod eficient,
- existența serviciul cloud Link-Live [2], care permite salvarea, vizualizarea și organizarea rezultatelor testelor efectuate în mediul online, indiferent de locația specialistului

- existența aplicației Windows AirCheck G2 Manager, care permite crearea profilelor de testare, salvarea și analiza rezultatelor testelor, precum și generarea rapoartelor necesare
- integrarea cu aplicația AirMapper™ Site Survey [3] care permite realizarea unor măsurători Wi-Fi bazate pe locație și creearea unor hărți vizuale cu valorile performanțelor măsurate. Aplicația se integrează și cu serviciul cloud Link-Live.

2.2. Descrierea interfeţelor dispozitivului

Figura 2 prezintă porturile fizice ale dispozitivului, explicând principalele caracteristici şi interfețe fizice ale dispozitivului:

- RJ-45 Ethernet Port 10/100/1000 Mbps, pentru efectuare de teste Ethernet în rețele cablate (inclusiv PoE) și pentru descoperirea accesoriilor pentru teste Ethernet (de exemplu iPerf Tester, [4])
- USB Port 1, pentru conectivitate cu periferice USB (500 mA)
- Micro USB Port 2, pentru comunicarea cu aplicația AirCheck G2 Manager
- USB Port 3, pentru conectivitate cu periferice USB (200 mA)
- External Antenna Connector, conector pentru conectarea antenelor externe
- Touchscreen – ecran tactil
- Power Button and LED – pentru pornirea/oprirea dispozitivului

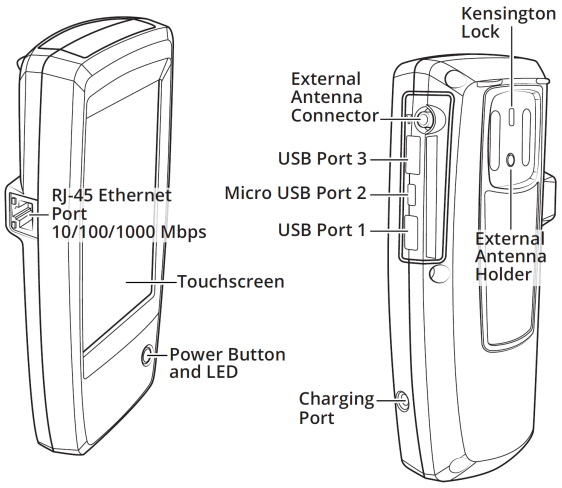


Figura 2. Porturi fizice Netscout/netAlly AirCheck G2 [5]

Analiza dispozitivelor şi a traficului în reţelele fără fir, precum și depanarea reţelele lor se poate realiza utilizând cele 5 funcții principale (Networks, Channels, Access Points, Clients și Interferers) și 2 teste rapide (AutoTest și Ethernet Test). Figura 3 prezintă ecranul principal al dispozitivului, împreună cu principalele funcționalități şi tipuri de teste ce pot fi rulate.

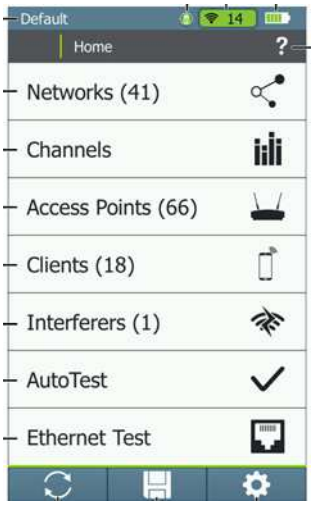
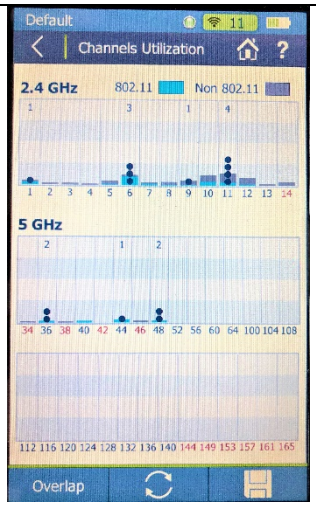


Figura 3. Ecranul principal al Netscout/netAlly AirCheck G2 [5]

Dispozitivul pune la dispoziția specialiștilor următoarele funcționalități principale:

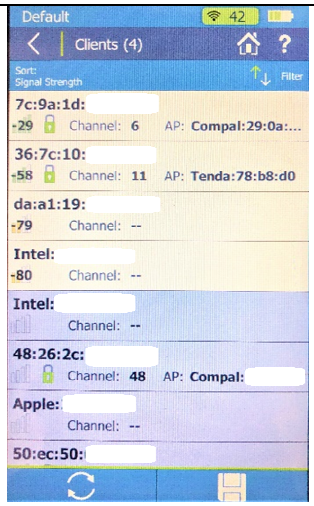
1. Networks (*Rețele*):
- funcție utilizată pentru descoperirea și afișarea rețelelor wireless
- se afișează lista SSID-urilor descoperite, puterea semnalului pentru fiecare AP descoperit (dBm), nivelul de securitate și parametru SNR (dB) pentru cel mai puternic AP din rețeaua descoperită
- permite găsirea rețelelor în mod infrastructură (descoperibile sau ascunse) sau în mod ad-hoc

2. Channels (*Canale*):
- permite vizualizarea utilizării canalelor wireless (2.4 GHz și 5 GHz).
- scopul funcției este să ajute utilizatorii să identifice canale aglomerate sau interferențe, oferind posibilitatea de a optimiza performanța rețelelor wireless prin ajustarea configurărilor de canal.



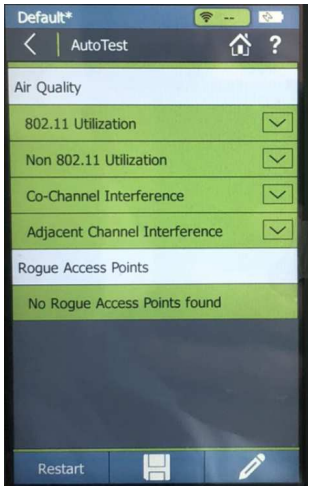
3. Access Points (*Puncte de acces*):
- funcție utilizată descoperirea și vizualizarea punctelor de acces (APs)
- poate scana și afișa toate punctele de acces Wi-Fi dintr-o anumită zonă, fie ele autorizate sau neautorizate

4. Clients (*Clienți*):
- permite descoperirea și vizualizarea clienților wireless asociați sau neasociați

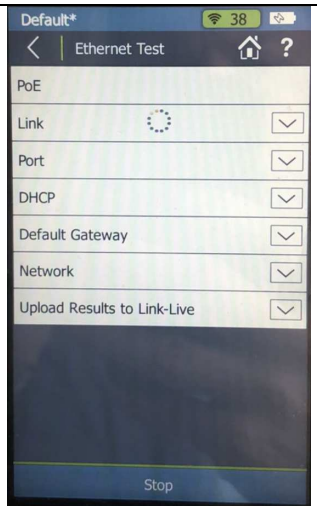


5. Interferers (*Perturbatori*):
- funcția permite descoperirea și vizualizarea echipamentelor care pot cauza interferențe în rețelele 802.11 (Bluetooth și alte echipamente wireless non 802.11)

6. Autotest:
- permite rularea unui set automat de teste pentru verificarea rețelei



7. Ethernet Test (*Test Ethernet*):
- este funcția ce permite verificarea parametrilor conexiunii cablate și a sistemului de distribuție care conectează un AP;
- rezultatelor testelor pot fi trimise către serviciul de Cloud Link-Live prin intermediul conexiunii cablate

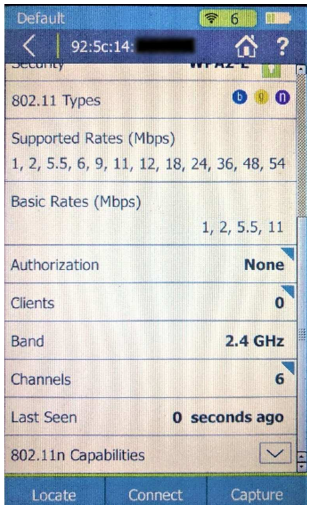


2.3. Descrierea detaliată funcțiilor dispozitivului

AirCheck G2 poate oferi informații detaliate despre punctele de acces Wi-Fi detectate în rețea. Aceste date permit identificarea rapidă a punctelor de acces neautorizate sau a problemelor de acoperire.

Acces Point details (Detalii punct de acces)

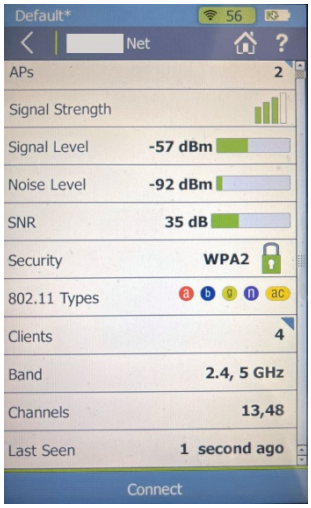
- oferă detalii despre standardele Wi-Fi utilizate (802.11a/b/g/n/ac), lățimea de bandă puterea semnalului, canalul pe care funcționează punctul de acces, etc;
- afișează informații despre metodele de securitate utilizate de fiecare punct de acces (WEP, WPA, WPA2, etc.)



AirCheck G2 poate afișa informații complete despre rețelele Wi-Fi disponibile. Aceste detalii ajută la evaluarea performanței și securității rețelei.

Network details (Detalii rețele)

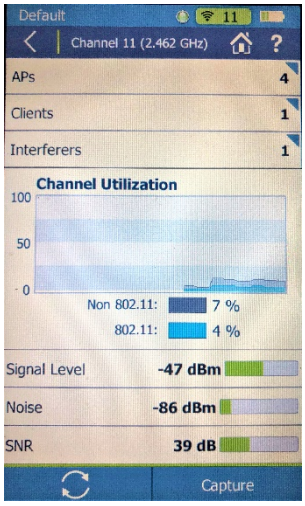
- oferă o imagine detaliată a stării și configurării unei rețele selectate
- se pot vizualiza: SSID-ul rețelei afișate, numărul de puncte de acces detectate pe această rețea, puterea semnalului celui mai puternic punct de acces din rețea, nivelul semnalului în dbm de la cel mai puternic punct de acces, nivelul de zgomot în dBm din mediu, raportul semnal-zgomot (SNR), starea de securitate a rețelei, standardele 802.11 utilizate de punctele de acces din rețea, numărul de clienți Wi-Fi descoperiți pe rețea, banda radio utilizată de rețea: 2,4 GHz, 5 GHz sau ambele și canalele Wi-Fi utilizate de rețea.



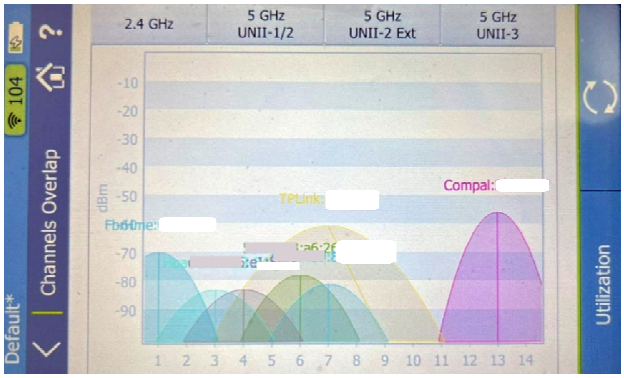
AirCheck G2 oferă informații despre utilizarea canalelor Wi-Fi. Această funcție permite utilizatorilor să analizeze suprasolicitarea canalelor și să optimizeze distribuția frecvențelor pentru a îmbunătăți performanța rețelei.

Channel details (Detalii canal):

- funcția are rolul de a furniza informații detaliate despre canalul wireless ales în mediul de testare
- se pot vizualiza: numărul de puncte de acces descoperite pe canal, numărul de clienți Wi-Fi descoperiți pe canal, numărul de dispozitive potențial interferente descoperite pe canal, nivelul semnalului în timp real (în dBm) al celui mai puternic semnal de punct de acces pe canal, nivelul de zgomot și raportul semnal-zgomot măsurat în timp real.



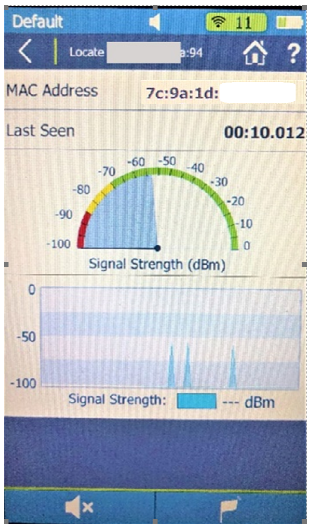
- permite vizualizarea încărcării canalelor wireless detectate în mediul de testare, prin opțiunea Overlap (*Suprapunere*)



Funcția de localizare permite identificarea și găsirea fizică a unui punct de acces sau a unui client Wi-Fi. AirCheck G2 utilizează intensitatea semnalului pentru a ghida utilizatorul către dispozitivul căutat, facilitând localizarea rapidă a surselor de interferență sau a punctelor de acces neautorizate.

Locate (Localizare):

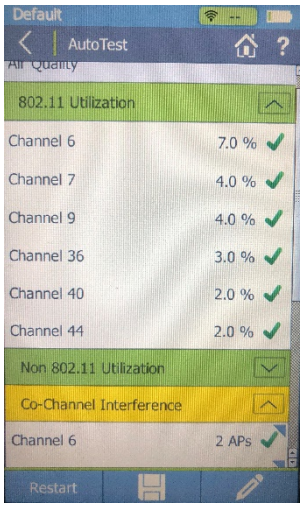
- opțiunea are rolul de a ajuta utilizatorii să identifice și să localizeze dispozitivele wireless, cum ar fi punctele de acces sau clienții wireless, prin măsurarea intensității semnalului (RSSI).



AirCheck G2 oferă un test automat care verifică rapid starea și performanța unei rețele wireless, pentru a evalua rapid dacă rețeaua funcționează în parametri optimi

Auto-test (Air Quality) details (Detalii auto-test (Calitatea aerului)):

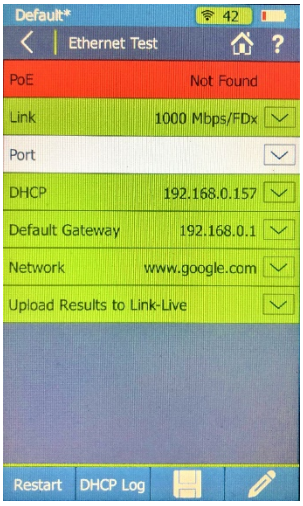
- măsurătorile includ utilizarea canalelor 802.11, utilizarea canalelor non-802.11, interferența co-canal și interferența între canale adiacente

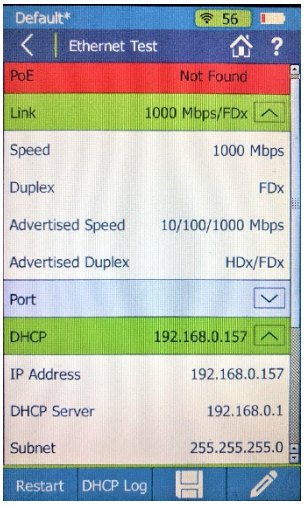


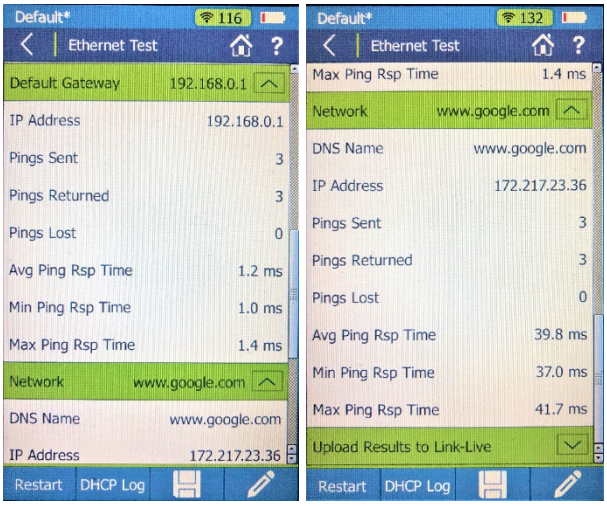
AirCheck G2 permite diagnosticarea conexiunilor Ethernet prin verificarea dacă link-ul fizic este stabilit, dacă sunt detectate capabilități PoE (Power over Ethernet), și dacă dispozitivul poate obține o adresă DHCP. De asemenea, oferă informații despre switch-ul la care este conectat dispozitivul (nume, model, MAC, IP, port și VLAN).

Ethernet Test details (Detalii test Ethernet)

- indică dacă au fost detectate capabilități PoE pe legătura curentă.
- arată dacă a fost stabilită o legătură Ethernet la nivelul Layer-2.
- afișează numele switch-ului, modelul, adresa MAC, adresa IP, numărul portului și ID-urile VLAN.
- arată dacă a fost obținută o adresă DHCP și dacă AirCheck G2 poate să facă ping către gateway-ul implicit și o țintă de rețea definită de utilizator (de ex. www.google.com)
- arată dacă rezultatele testului au fost transmise către Link-Live Cloud Service







2.4. Ghid de bune practici pentru analiza și depanarea rețelelor wireless

Cele mai frecvente probleme/nelămuriri ale utilizatorilor și a administratorilor de rețea sunt:

- Clienții nu se pot conecta la rețeaua wireless
- Clienții sunt deconectați
- Rețeaua funcționează greu și conexiunea este lentă

Pornind de la principalele probleme/nelămuriri ale utilizatorilor și a administratorilor de rețea, se pot utiliza o multitudine de abordări și teste pentru a rezolva situațiile apărute în practică. Intotdeauna este necesară o abordare sistematică pentru identificarea cauzei și implementarea soluțiilor potrivite. Utilizând dispozitivul Netscout/netAlly AirCheck G2 Wireless Tester se pot folosi funcționalitățile acestuia (opțiunile Networks, Channels, Access Points, Interferers și Ethernet Test) pentru rezolvarea acestor probleme. Pentru depanarea problemelor Wi-Fi, se pot utiliza abordări top-down sau bottom-up, în funcție de natura problemei și de preferințele echipei de depanare. Mai jos, se vor prezenta posibilele abordări, cu mențiunea că aceste soluții nu sunt exhaustive și se pot aplica și altor scenarii.

1. Clienții nu se pot conecta la rețeaua wireless

Posibilele cauze ale problemelor de conectare la rețeaua wireless includ un semnal Wi-Fi slab sau interferențe, o configurație incorectă a punctului de acces (AP) sau a dispozitivului client, congestia rețelei din cauza suprasolicitării canalelor, probleme legate de serviciile de rețea, cum ar fi DHCP, DNS sau conexiunea la internet, precum și probleme cu infrastructura rețelei, cum ar fi legătura AP-ului către rețeaua cablată sau controlerul WLAN.

Verificați dacă dispozitivul client încearcă să se conecteze la SSID-ul corect, deoarece este posibil ca acesta să fie configurat cu un SSID incorect. De asemenea, este important să verificați acoperirea semnalului și raportul semnal-zgomot (SNR) pentru rețea, întrucât un semnal slab sau interferențele pot genera probleme de conectare. Asigurați-vă că punctul de acces suportă standardele Wi-Fi corespunzătoare (802.11a/b/g/n/ac/ax) și că dispozitivul client este compatibil cu acestea. În plus, verificați dacă setările de securitate ale rețelei

(WPA2, WPA3 etc.) și ale dispozitivului client sunt compatibile pentru a evita eventualele dificultăți de autentificare.

Dacă dispozitivul client este conectat la rețea, verificați dacă acesta primește adresele corecte de la serverul DHCP și asigurați-vă că dispozitivul poate comunica atât în rețea, cât și în afara acesteia. De asemenea, verificați dacă punctul de acces are o conexiune stabilă cu controlerul WLAN și cu rețeaua, dacă este înregistrat corect și dacă nu există probleme de comunicare între punctul de acces și infrastructura principală a rețelei.

2. Clienții sunt deconectați

Verificați dacă firmware-ul punctului de acces (AP) este actualizat și asigurați-vă că puterea semnalului este suficientă pentru a acoperi întreaga zonă de utilizare a clientului. O acoperire necorespunzătoare a semnalului poate duce la deconectări frecvente sau la o conexiune instabilă. Actualizați driverul adaptorului Wi-Fi al dispozitivului client și verificați corectitudinea setărilor de roaming și conexiune automată. Aceste ajustări pot îmbunătăți experiența de conectare și preveni întreruperile în momentul schimbării punctelor de acces (roaming).

Verificați dacă există congestie pe canalele utilizate de rețea. Un număr prea mare de clienți sau alte rețele care operează pe același canal pot cauza deconectări frecvente. De asemenea, verificați interferențele cauzate de dispozitive non-802.11, cum ar fi cuptoarele cu microunde, telefoanele fără fir sau alte echipamente care operează în frecvențele de 2,4 GHz și 5 GHz. Utilizarea unui instrument specializat, precum AirCheck G2, poate ajuta la identificarea acestor probleme. În cazul depistării unei suprasolicitări a canalelor, schimbarea acestora sau trecerea la banda de 5 GHz poate îmbunătăți stabilitatea conexiunii.

Verificați dacă există dispozitive neautorizate conectate la rețea, care ar putea suprasolicita punctul de acces sau genera interferențe. Aceste dispozitive pot cauza probleme de performanță și deconectări frecvente pentru ceilalți utilizatori ai rețelei. Consultați specialiștii în securitate cibernetică pentru a implementa măsuri adecvate de protecție și control al accesului.

3. Rețeaua Wi-Fi funcționează greu și conexiunea este lentă

Pentru a rezolva problema unei rețele Wi-Fi care funcționează greu, trebuie abordate mai multe aspecte, unele precizate anterior (congestie, infrastructură, securitate).

Reevaluați distribuția punctelor de acces și, dacă este necesar, adăugați AP-uri suplimentare sau redistribuiți utilizatorii pe alte AP-uri pentru a echilibra traficul.

Optimizarea configurării AP-urilor poate fi realizată prin setarea acestora să utilizeze o lățime de bandă de 20 MHz pe banda de 2,4 GHz, pentru a reduce interferențele cauzate de congestia acestei benzi. În același timp, pe banda de 5 GHz, este recomandat să configurați AP-urile să folosească 40 MHz sau mai mult, pentru a maximiza lățimea de bandă disponibilă

și a îmbunătăți performanța rețelei, având în vedere că această bandă este mai puțin aglomerată.

În plus, se recomandă să efectuați periodic verificări și teste de stabilitate pentru infrastructura rețelei, asigurându-vă că toate componentele funcționează în parametri optimi și că nu există probleme de conectivitate sau performanță.

3. Aplicaţii practice

3.1. Se vor experimenta opțiunile puse la dispozitie de catre AirCheck G2, utilizând configuraţia de test din cadrul laboratorului. Se va realiza o analiză a reţelelor WLAN 802.11 dispoznibile, se va monitoriza traficul şi se vor depana problemele din cadrul reţelor wireless detectate. Se vor salva capturile obţinute pentru analize ulterioare.

3.2. Se vor depana scenariile de test puse la dispoziție în cadrul laboratorului, urmând ghidul de bune practici descris în cadrul capitolului. Se va pune în evidenţă utilitatea AirCheck G2, atât pentru proiectarea şi instalarea reţelelor WLAN 802.11, cât şi pentru identificarea şi localizarea interferenţelor.

3.3 Analizați mediul RF utilizând AirCheck G2 din locația voastră și notați:

a. Câte rețele wireless ați descoperit?

b. În ce canale sunt aceste rețele configurate să funcționeze?

c. Cate dispozitive aveți în fiecare canal și care sunt numele lor? Sunt dispozitive autorizate sau dispozitive pe care nu le cunoașteți?

d. Care este puterea fiecărui dispozitiv detectat: signal quality (dB), RSSI (Received signal strength indication), etc?

e. Care ar fi frecvența și canalul optim în care să instalați un nou dispozitiv wireless, AP sau routerWiFi? (indicație: maximizați nivelul semnalului și minimizați nivelul de zgomot)

Bibliografie:

[1] netAlly AirCheck G2, https://www.netally.com/products/aircheck/
[2] Link-Live, https://www.netally.com/products/link-live/
[3] AirMapper Site Survey, https://www.netally.com/airmapper-site-survey/
[4] Test Accessory, Pocket iPerf Testing Tool, https://www.netally.com/products/testaccessory/
[5] NetAlly AirCheck™ G2 Wireless Tester User Manual, 10.2020, https://www.netally.com/wp-content/uploads/2020/10/AirCheck-G2-Quick-Start-English.pdf

V. 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 reţele WLAN 802.11a/b/g şi descoperire AP-uri 802.11n;
- monitorizare trafic reţea şi interfeţe de switch, localizarea celui mai apropiat switch pentru a afişa detaliile şi statisticile de port;
- descoperire dispozitive de infrastructură wired şi wireless şi configuraţiile acestora;
- identificare VLAN-uri pentru vizualizarea stărilor interfeţelor, detaliile staţiilor conectate;
- descoperire sub-reţelele şi catalogarea elementelor din reţea după adresa de IP, domeniu de NetBIOS sau reţele IPX;
- interfata touch-screen;
- sistem de operare Linux;

2.2. Descrierea interfeţelor dispozitivului

Produsul Fluke Networks EtherScope Network Assistant este un instrument mobil utilizat pentru depanarea şi întreţinerea reţelelor WLAN şi LAN, care pune la dispoziţia administratorilor de reţea 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 interfeţe ale dispozitivului:

- buton On/Off/Stand-by
- stilou grafic pentru interfaţa touch-screen
- led-uri care indică funcţionarea dispozitivului
- port serial, utilizat pentru conectarea şi configurarea unor dispozitive de reţea (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 interfeţele de reţea ale dispozitivului:

Figura 3. Fluke EtherScope Series II Network Assistant – interfeţe de reţea [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 reţele wired, bazate pe cabluri torsadate (10/100/1000 Mbps)
- interfaţă SFP, utilizată pentru conectarea unui transciever de fibră optică pentru conectarea directă la reţele de fibră optică (1000 Mbps)

2.3. Descrierea interfeţei 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 dispoziţie 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 opţiuni de depanare şi testare a reţelei
-  buton pentru accesarea informaţiilor referitoare la un test specific
-  buton pentru accesarea testelor pentru reţeaua wired

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

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

2.4. Depanarea reţelelor wireless

Dispozitivul Fluke EtherScope Series II Network Assistant pune la dispoziţia administratorilor de reţea şi opţiunea de analiză şi depanare a reţelelor fără fir. Slotul 1, descris anterior, permite instalarea unui card wireless utilizând interfaţa PCMCIA.

Paşii care trebuie urmaţi pentru depanarea reţelelor fără fir sunt următorii:

- instalarea unui adaptor wireless Fluke 802.11 a/b/g

- pornirea dispozitivului şi selectarea opţiunii *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 opţiunii WLAN Test, în panoul central al dispozitivul EtherScope Network Assistant vor fi afişate testele efectuate (fig. 4).

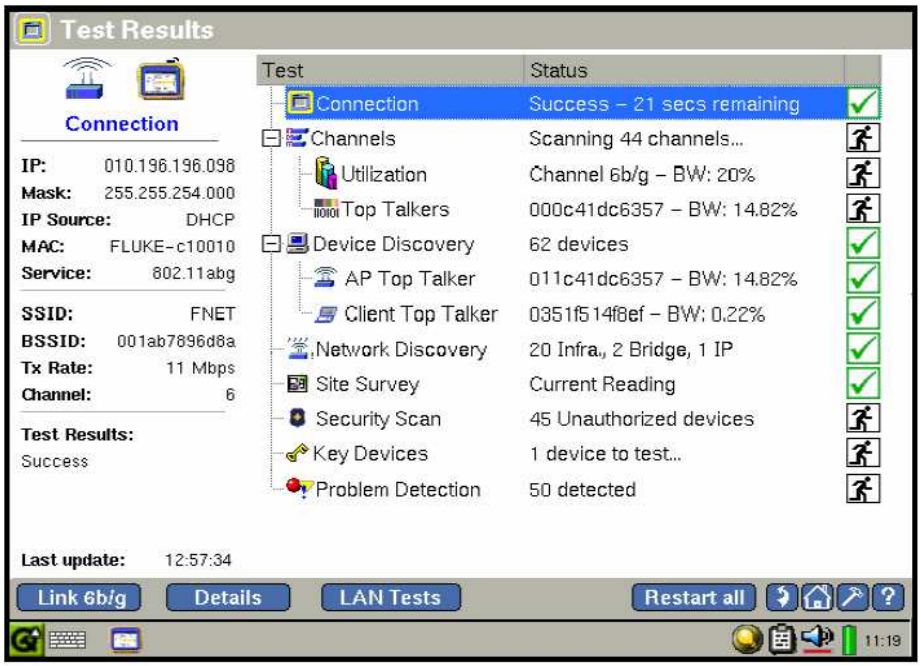


Figura 4. Vizualizare rezultate AutoTest

Icoanele din partea dreaptă a panoului central prezintă statusul fiecărui test in curs, semnificaţiile 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 reţea o privire a ansamblu asupra configuraţiei reţelei şi a posibilelor probleme.

Pictograma	Semnificaţie
	Test în curs de execuţie
	Test care nu se execută
	Test terminat cu succes
	Test terminat cu eşec

Tabelul 1. Status teste

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

Autotestul conţine următoarele verificări:

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

Alte opţiuni 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 ţării în care este utilizat dispozitivul
- Instrument Security: setarea securităţii 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).

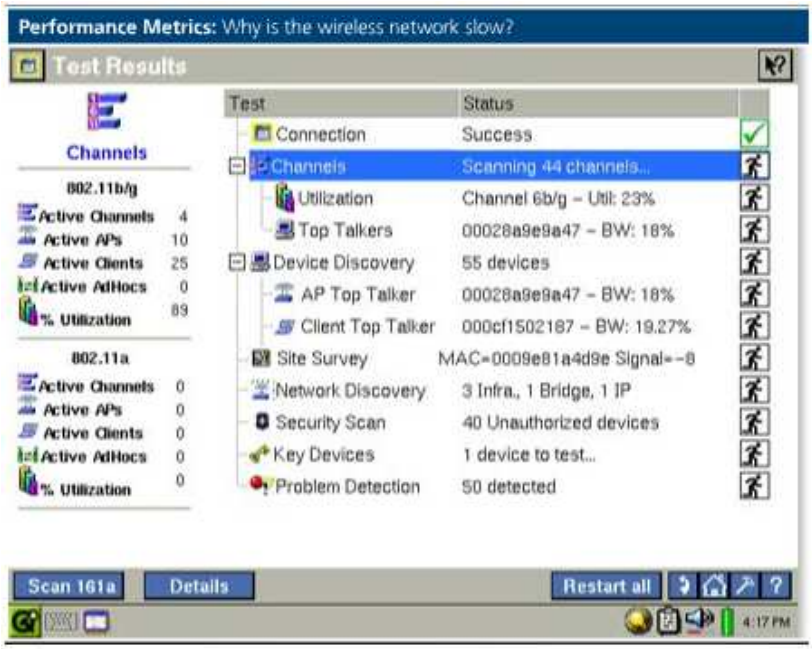


Figura 5. Test Scanare Canale RF

Panoul preview va afişa informaţii 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 diferiţi parametri de calitate, pentru fiecare canal detectat, se va selecta opţiunea Details din cadrul panoului toolbox. Următoarele statistici sunt disponibile în cadrul acestei opţiuni:

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

Submenirile *Utilization* şi *Top Talkers* furnizează informaţii care sunt utile pentru verificarea şi depanarea problemelor de trafic şi de performanţă în reţea. Opţiunea *Utilization* oferă statistici referitoare la cantitatea şi tipul de trafic pe canalele detectate, iar opţiunea *Top Talkers* oferă statistici referitoare la dispozitivele care utilizează reţeaua.

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

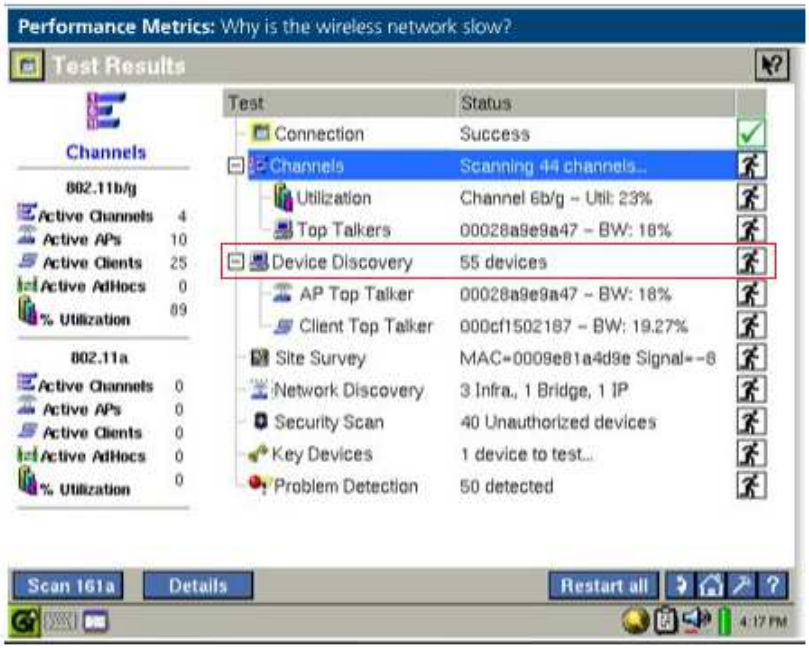


Figura 6. Test Descoperire Dispozitive

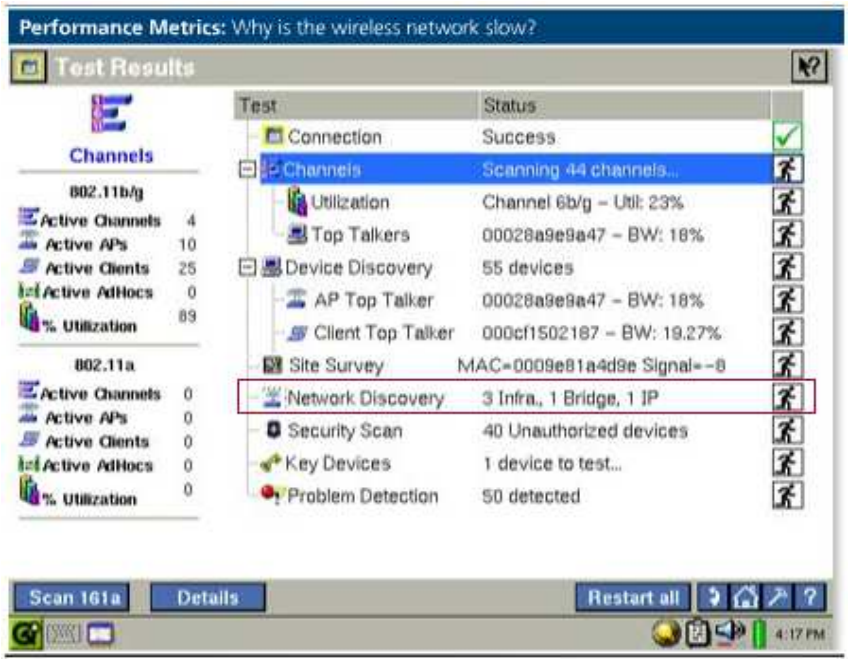
În panoul preview se va afişa o listă de categorii de dispozitive şi numărul acestora. Datorită faptului că un dispozitiv poate juca mai multe roluri, numărul total de dispozitive din fiecare categorie va putea fi mai mare decât numărul dispozitivelor existente (fig. 6).

La selectarea opţiunii 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, informaţii 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 informaţiile disponibile despre un anumit dispozitiv descoperit, se va selecta dispozitivul şi se va selecta opţiunea Details din cadrul panoului toolbox.

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

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



c. Figura 7. Test Descoperire Configuraţii de Reţea

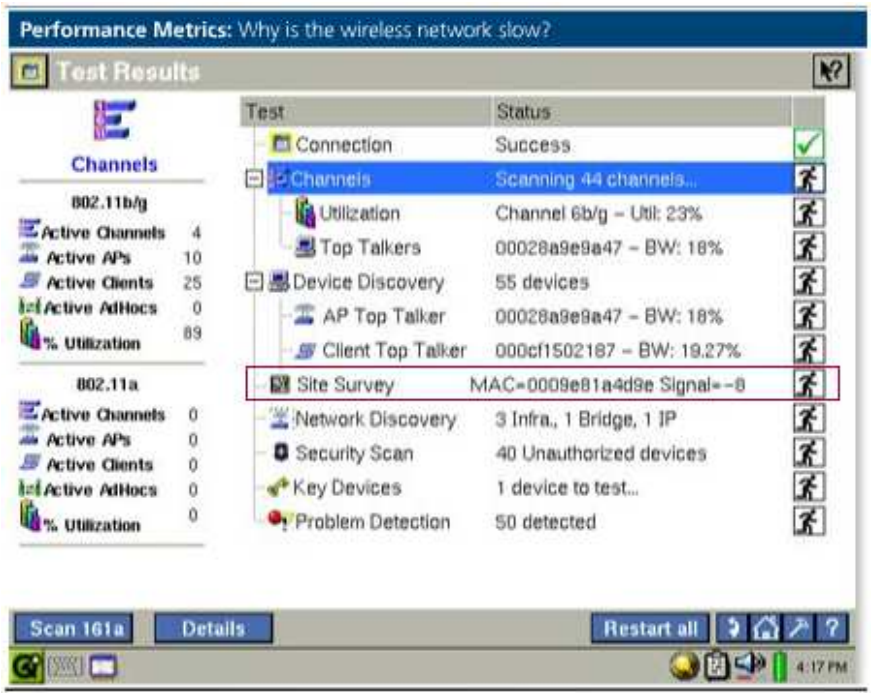


Figura 8. Test Examinare Reţea

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 această opţiune va fi configurată în funcţie de necesităţile administratorului de reţea.
f. **Problem detection** – acest test poate fi utilizat pentru a determina dispozitivele care prezintă probleme. Panoul preview oferă informaţii legate de următoarele probleme: Erori/ Avertismente/ Mesaje Info/ Probleme rezolvate. Pentru vizualizarea acestor informaţii se va selecta opţiunea 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]

Execuţia testelor de diagnostic

Dispozitivul EtherScope Network Assistant pune la dispoziţie diferite informaţii referitoare la staţii, dispozitive şi servicii de reţea şi, de asemenea, teste pentru verificarea conectivităţii şi a performanţelor reţelei.

Teste disponibile pot fi accesate în două moduri:

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

   Testele disponibile:

   • Ping – utilizat pentru testarea conectivităţii 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 opţiunii 

. 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/recepţie
   • Problems – problemele detectate
   • Trace Route - utilizat pentru a vizualiza calea parcursă până la un anumit dispozitiv
   • Ping – utilizat pentru testarea conectivităţii 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. Aplicaţii practice

3.1. Se vor experimenta testele WLAN ale dispozitivului Fluke EtherScope Network Assistant, utilizând configuraţia de test din cadrul laboratorului. Se va realiza o analiză a reţelelor WLAN 802.11a/b/g, se va monitoriza traficul şi se vor depana problemele din cadrul reţelor wireless detectate. Se vor pune în evidenţă diferenţele dintre reţelele wired şi wireless, şi problemele specifice reţelelor 802.11. Se vor crea rapoarte pentru fiecare test rulat.

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

Bibliografie:

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

VI. 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 reţea al dispozitivelor, gradul lor de utilizare, cât şi utilizarea pe canale, sunt evidenţiate în graficele pe care Analyze Air le pune la dispoziţia administratorilor de reţea.

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

2.2. Descrierea modului de funcţionare

Fluke AnalyzeAir pune la dispoziţia 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 opţiuni 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).

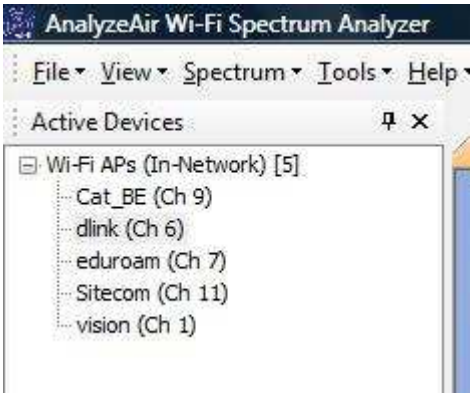


Figura 3. Modul Active Devices

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).

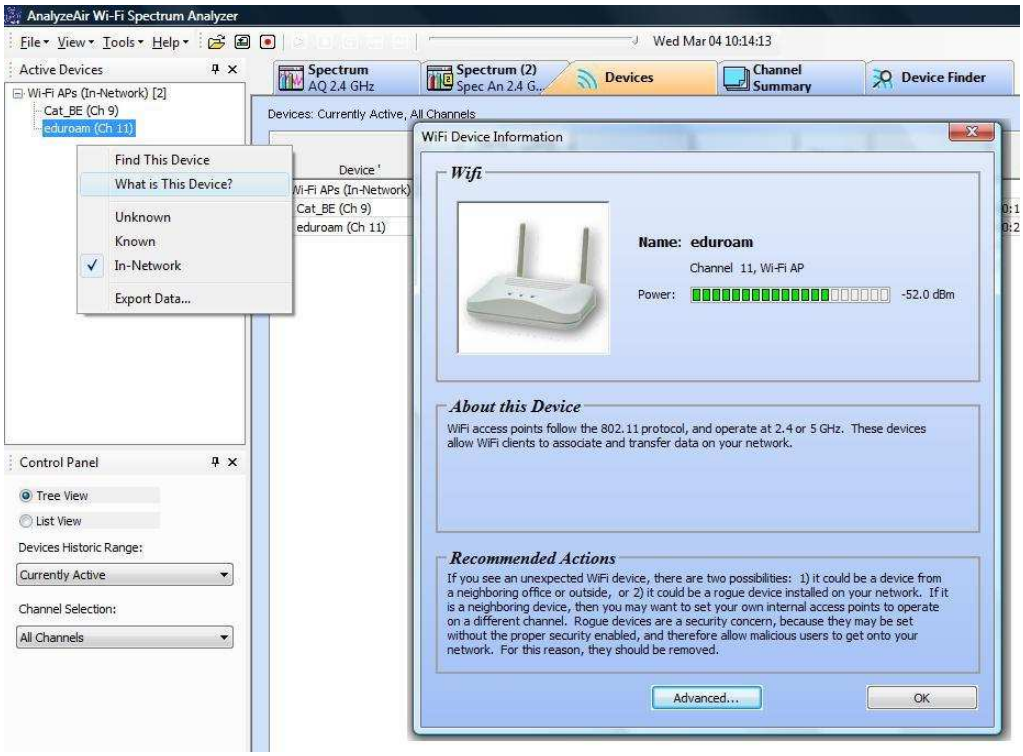


Figura 4. Descoperire dispozitiv

B. Spectrum Plots

Acestă opţiune oferă cinci tipuri de grafice care prezintă în timp real activitatea RF în funcţie de frecvenţă şi, de asemenea, variaţii în activitatea RF pe intervale scurte de timp. Aceste grafice sunt unelte esenţiale pentru întelegerea şi analiza mediului în care WLAN-ul

funcţionează. 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 (waţi sau dBm), ci mai degrabă în termeni care indică cât de multă putere RF este prezentă în sens operaţional sau funcţional. Scopul este de a avea o măsură de putere RF care să sugereaze cât de mult impact va avea puterea RF asupra performanţei reţelei.

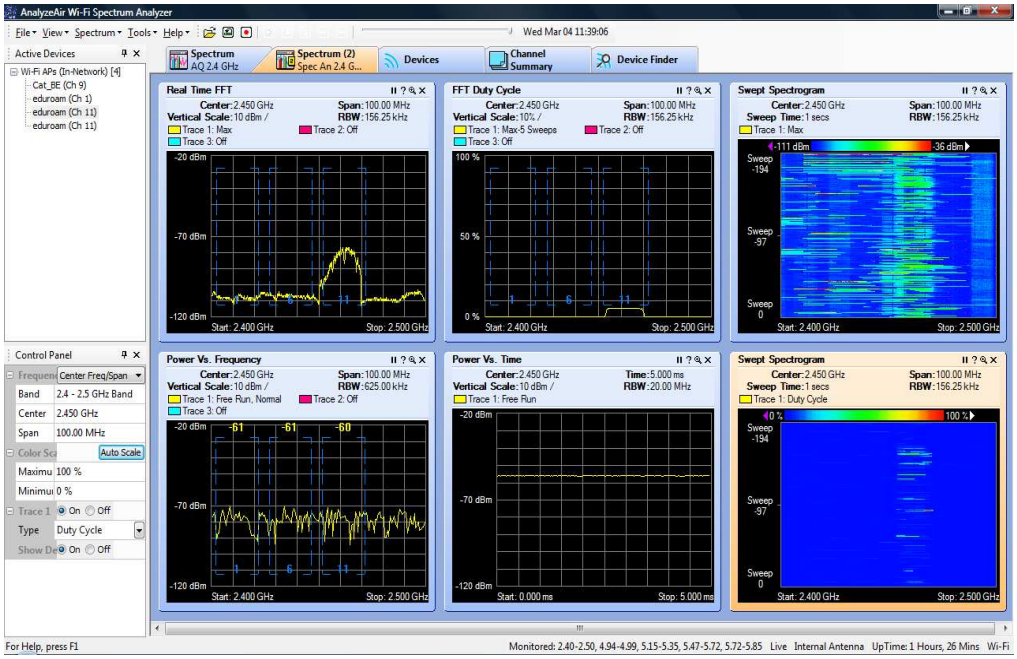
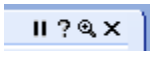


Figura 5. Spectrum plots

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 funcţie de frecvenţă. 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 frecvenţe. 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 funcţie de timp. Intervalul de timp utlizat în această analiză este foarte scurt (de ordinul milisecundelor).

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

C. Spectrum Charts

Acest display oferă informaţii generalizate către inginerul de reţea, pe când Spectrum Plots oferă informaţii mai uşor de înţeles de către experţii RF. Diagrame ca *Devices vs. Time* şi *Channel Utilization vs. Time* pot oferi informaţii legate de momentele când reţeaua wireless este afectată mai mult de interferenţe, iar diagrame ca *Devices vs. Channel* şi *Channel Utilization* pot oferi informaţii generale referitoare la modul în care diferite canale pot fi afectate de activitatea RF.

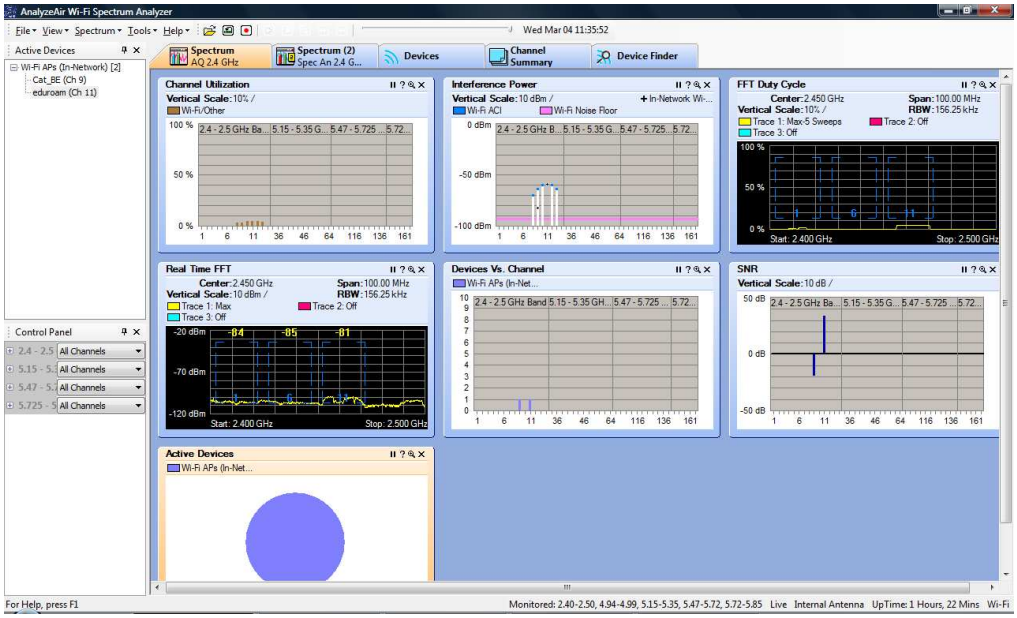


Figura 6. Spectrum charts

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 aparţine 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 anumiţi 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 funcţie 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 funcţie de timp.
- *Intereference Power* reprezintă un bar chart care va afişa puterea pe fiecare canal selectat. Înalţimea fiecărei bare va indica puterea tuturor semnalelor de interferenţă. 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 recepţionat 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 informaţii detaliate referitoare la dispozitivele de reţea şi la dispozitivele care interferează cu reţeaua wireless (fig. 7). O opţiune importantă este reprezentată de posibilitatea de a avea un istoric al dispozitivelor detectate, nu doar a celor detectate la momentul curent.

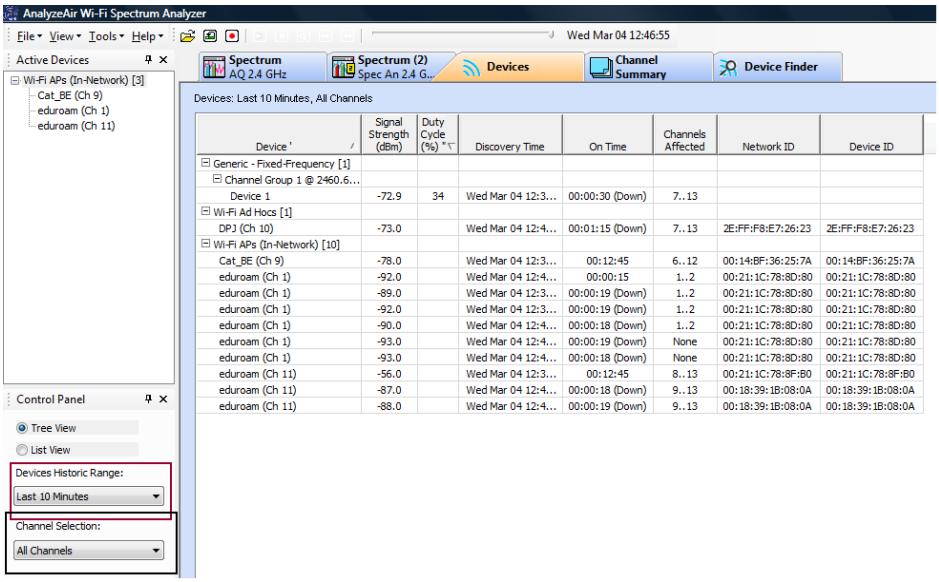


Figura 7. Devices view

E. Channel Summary

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

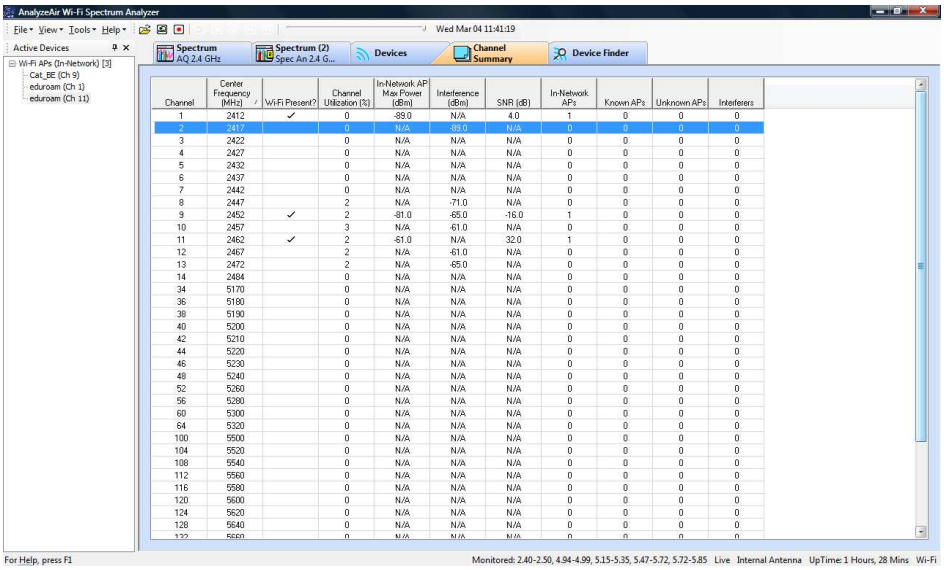


Figura 8. Channel summary

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

F. Device Finder

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

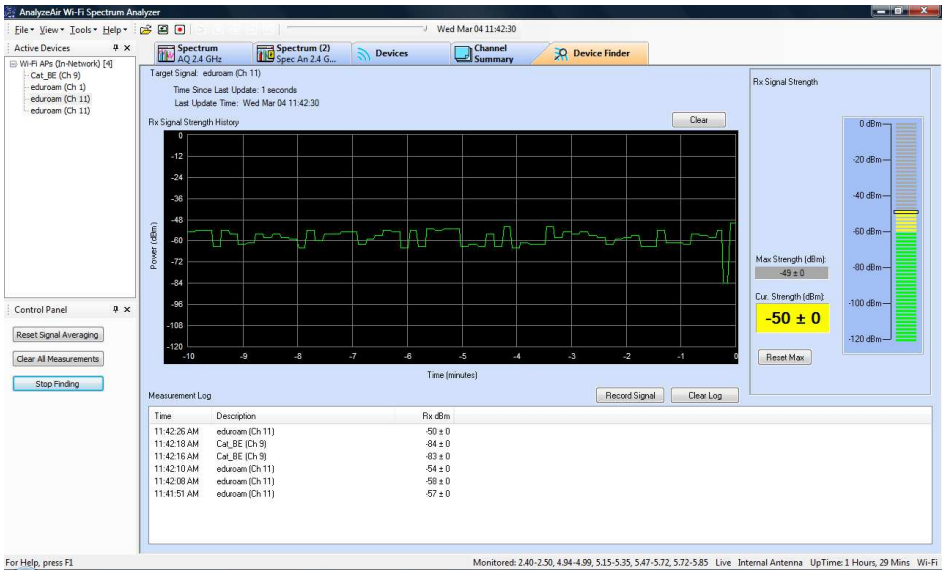


Figura 9. Device Finder

2.3. Descrierea opţiunilor de funcţionare

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

- *Sensors and Antennas*: opţiune pentru selectarea tipului de senzor utilizat pentru obţinerea de date (Internal/Extenal PC Card Antenna)
- *Console Settings*: opţiune pentru modificarea modului în care Analyze-Air afişează datele.
- *Band and Channel Settings*: opţiune 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*: opţiune 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:* opţiune pentru configurări SNMP

3. Aplicaţii practice

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

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

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, Laptop, etc.).

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.

VII. Configurarea reţelelor wireless: Configurări de bază

1. Obiective

Obiectivul acestui capitol este prezentarea modului de instalare şi configurare a unui ruter wireless și a unui punct de acces wireless (Linksys *WRT350N* Wireless-N Gigabit with Storage Link și Cisco WAP150 Wireless-AC/N Dual Radio Access Point with PoE). Se vor descrie principalele caracteristici ale dispozitivelor, modalităţile de funcţionare, precum şi avantajele/dezavantajele introduse de acestea în rețelele wireless.

2. Consideraţii teoretice

2.1. Linksys WRT350N Wireless-N Gigabit with Storage Link

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 reţele locale de calculatoare.

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

Principalele caracteristici ale dispozitivului sunt:

- Transmisie în tehnologie Wireless N (MIMO);
- Frecvenţă de operare: 2.4 - 2.5 GHZ;
- Internet Gigabit Router şi Switch cu 4 port-uri 10/100/1000;
- Wireless Access Point cu rază mărită de acţiune;
- Securitate avansată prin Firewall SPI, criptare pe 256 de biţi;
- 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;

Descrierea interfeţelor dispozitivului

Figura 2 prezintă o vedere frontală a dispozitivului. Led-urile dispozitivului permit o diagnosticare rapidă a funcţionării 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/recepţionează 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]

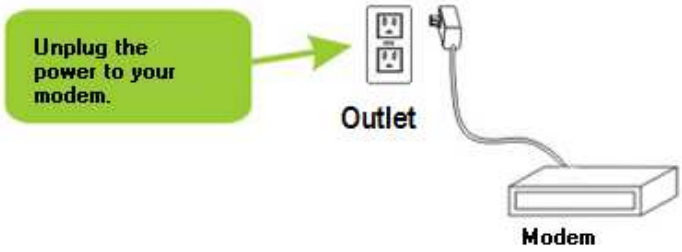
Figura 3 prezintă o vedere a interfeţele de reţea/USB ale dispozitivului:

- *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 reţea;
- *Reset* – buton pentru resetarea la configuraţia implicită;

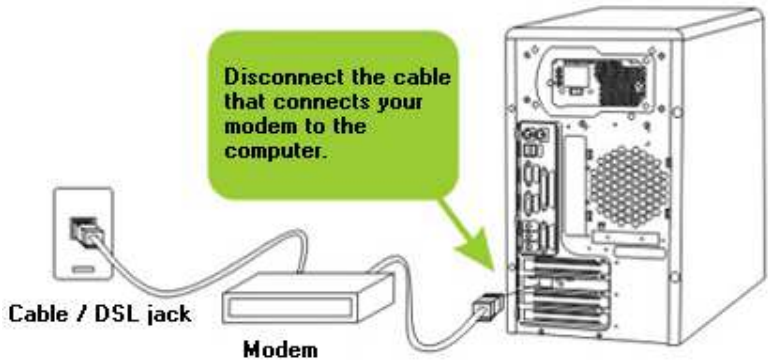
Figura 3. Interfeţe de reţea/USB [1]

Conectarea şi configurarea ruterului Linksys WRT350N Wireless-N Gigabit

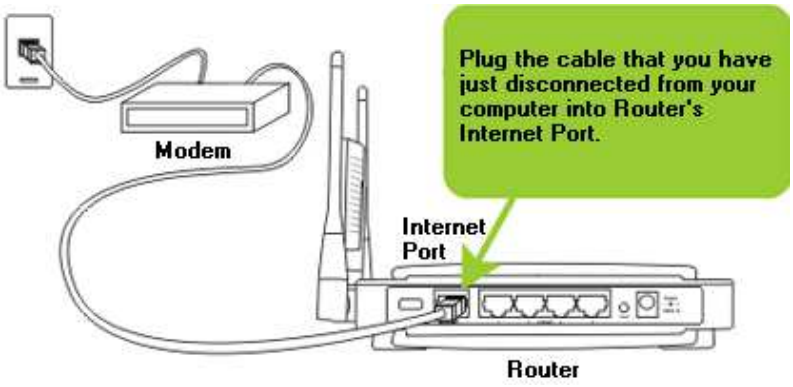
Figura 4 [1] prezintă paşii care trebuie urmaţi pentru conectarea ruterului la sistemul de distribuţie cablat/modem. La sfârşitul pasului f, led-urile frontale vor indica activitatea ruterului.



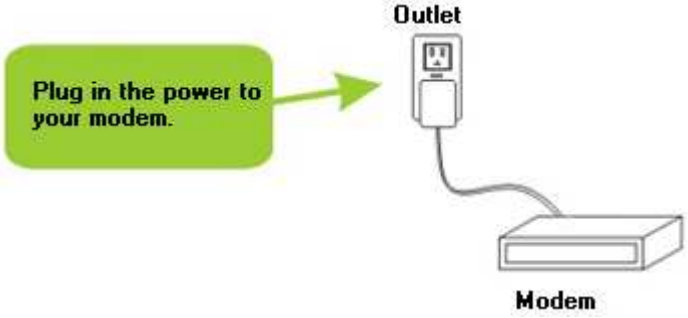
Pas a.



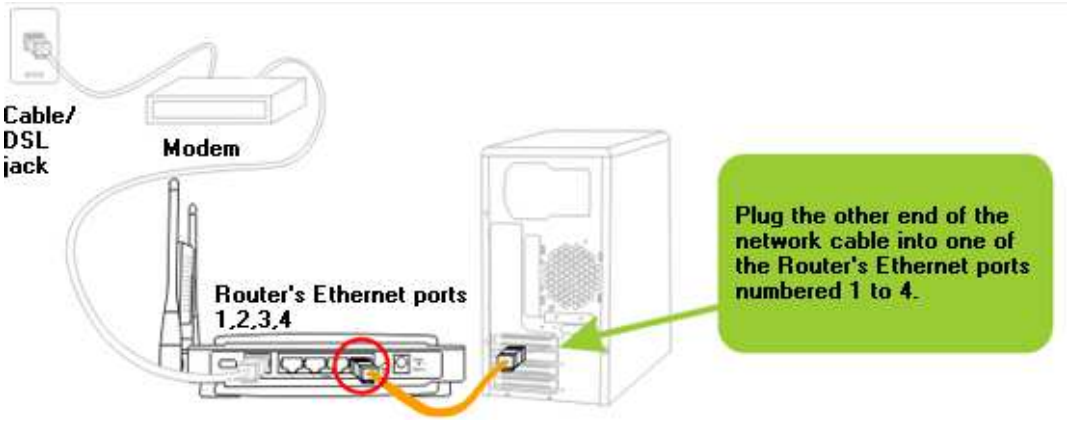
Pas b.



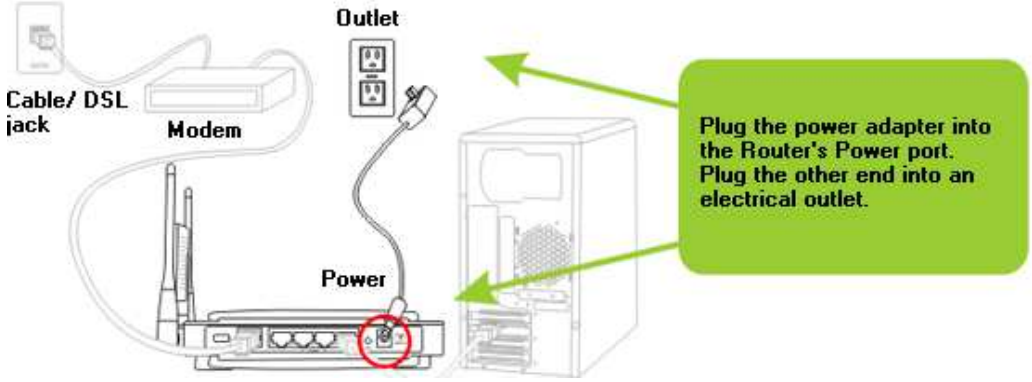
Pas c.



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 software-ul pe care se află un Wizzard, şi care descrie modalitatea de configurare pas cu pas;

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

Tab	Funcţie
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 aplicaţii
Administration	Setări dispozitiv
Status	Informaţii dispozitiv

Tabelul 1. Tab-uri de opţiuni

Diferenţa principală dintre cele două modalităţi constă în faptul că, configurarea utilizând Setup software-ul permite doar câteva setări de bază, pe când utilitarul web permite setarea tuturor opţiunilor disponibile. Această lucrare descrie modul de configurare bazat pe utilizarea utilitarul web. Tabelul 1 prezintă o descriere sumară a tab-urilor principale de opţiuni.

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:

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

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

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

În continuare se vor descrie tab-urile de opţiuni, împreună cu subopţiunile de configurare:

A. Setup

- Basic Setup: pentru a introduce informaţiile pentru conexiunea Internet, furnizate de către ISP;
- DDNS: permite activarea opţiunii Dynamic Domain Name System (permite asocierea unui host fix şi a unui nume de domeniu la o adresă Internet IP dinamică);

- MAC Address Clone: opţiune pentru clonarea unei adrese MAC pe ruter;
- Advanced Routing: opţiune pentru configuraţii de rutare statică/dinamică;

B. Wireless

- Basic Wireless Settings: setări de bază ale reţelei wireless (nume, canal, etc);
- Wireless Security: configurarea setărilor de securitate pentru reţeaua wireless;
- Wireless MAC Filter: restricţionarea accesului la reţeaua wireless prin filtrarea adreselor MAC ale staţiilor client;
- Advanced Wireless Settings: opţiune pentru configuraţii avansate, pentru administratorii de reţea:
    - AP Isolation: această opţiune permite izolarea clienţilor şi a dispozitivelor wireless din cadrul reţelei. Acestea nu vor putea comunica între ele, ci doar cu ruterul;
    - Authentication Type: opţiunea Shared Key se va selecta doar dacă receptorul şi transmiţătorul 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 funcţie de vitezele suportate de dispozitivele wireless);

C. Security

- Firewall: opţiune 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 partiţiile discului ataşat;
- Administration: administrarea utilizatorilor/grupurilor care pot accesa partajările;
- Media Server: opţiune pentru activarea serverului media încorporat în ruter;
- FTP Server: configurarea ruterului ca server FTP local;

E. Access Restrictions

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

F. Applications & Gaming

- Single Port Forwarding: opţiune pentru port mapping şi forwarding pentru un singur port de serviciu;
- Port Range Forwarding: pentru accesul unor servicii publice/aplicaţii 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: opţiuni de Quality of Service.

G. Administration

– opţiuni de administrare şi management ruter;

H. Status

– informaţii despre statusul ruterului şi a reţelei locale;

2.2. Cisco WAP150 Wireless-AC/N Dual Radio Access Point with PoE

Dispozitivul Cisco WAP150 (fig. 6) face parte din seria Cisco Small Business 100 Series Wireless Access Points, fiind conceput pentru utilizarea în mediul de business, pentru organizații de dimensiuni mici. Pentru organizații de dimensiuni medii și mari sau pentru mediul industrial se pot utiliza echipamentele din seria Cisco Catalyst 9100 Access Points sau seria Meraki.

Figura 6. Cisco WAP150: vedere panou frontal posterior [3]

Principalele caracteristici ale APului Cisco WAP150 sunt:

- Standardul Wi-Fi utilizat este 802.11ac Wave 1, oferind performanțe avansate
- Dispozitivul funcționează pe frecvențele 2,4 GHz și 5 GHz (tehnologie dual radio)
- Rata de transfer a datelor ajunge la 867 Mbps pentru 802.11ac și 300 Mbps pentru 802.11n
- Fiecare radio poate susține până la 64 de clienți asociați simultan
- Pentru acoperire extinsă, clusterul poate include un maximum de 4 puncte de acces WAP150
- Dispozitivul este echipat cu un port GigabitEthernet compatibil cu Power over Ethernet (PoE)

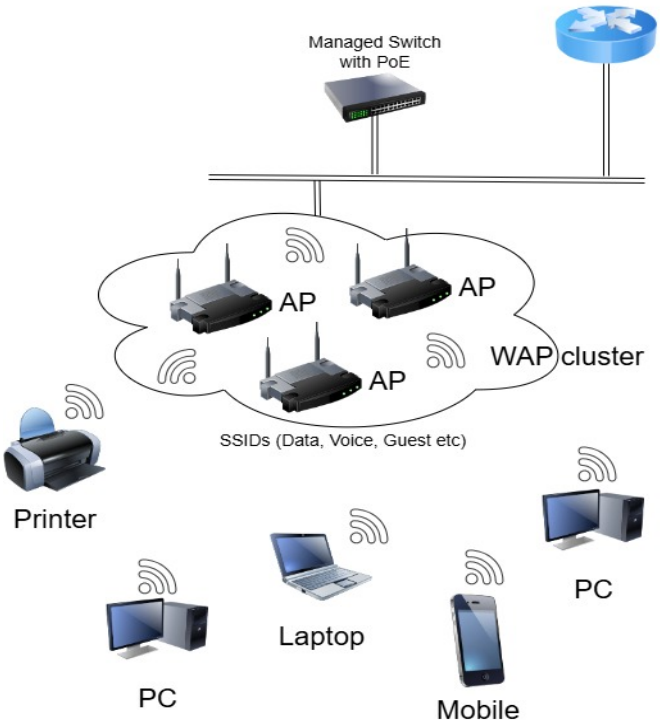


Figura 7. Exemplu de topologie cu cluster WAP150

Configurarea inițială se poate realiza utilizând fie o conexiune cu fir (cablată), fie una wireless. Configurația implicită a Cisco WAP150 are modulul Wi-Fi activat, iar pentru configurare se utilizează SSID-ul WAP150 (CiscoSB-Setup) cu cheia de acces cisco123. Pentru configurația cablată se va conecta un cablul Ethernet de la portul Ethernet (LAN) al dispozitivului Cisco WAP150 la portul Ethernet al unui switch, router sau PC (fig. 7).

Pentru configurarea inițială se vor utiliza următorii parametri pentru a lansa Access Point Setup Wizard (fig. 8):

- Adresa IP a WAP150: adresă IP asignată de un server DHCP în rețeaua 192.168.1.0 cu NM 255.255.255.0; dacă nu există un server DHCP (sau APul nu reușește să primească o adresa IP în 60 de secunde) acesta va utiliza adresa IP statică 192.168.1.245 cu NM 255.255.255.0;
- PC-ul utilizat pentru configurare trebuie sa fie în aceeași rețea cu APul (adresă IP asignată de un server DHCP în rețeaua 192.168.1.0 cu NM 255.255.255.0)
- Username: cisco
- Password: cisco

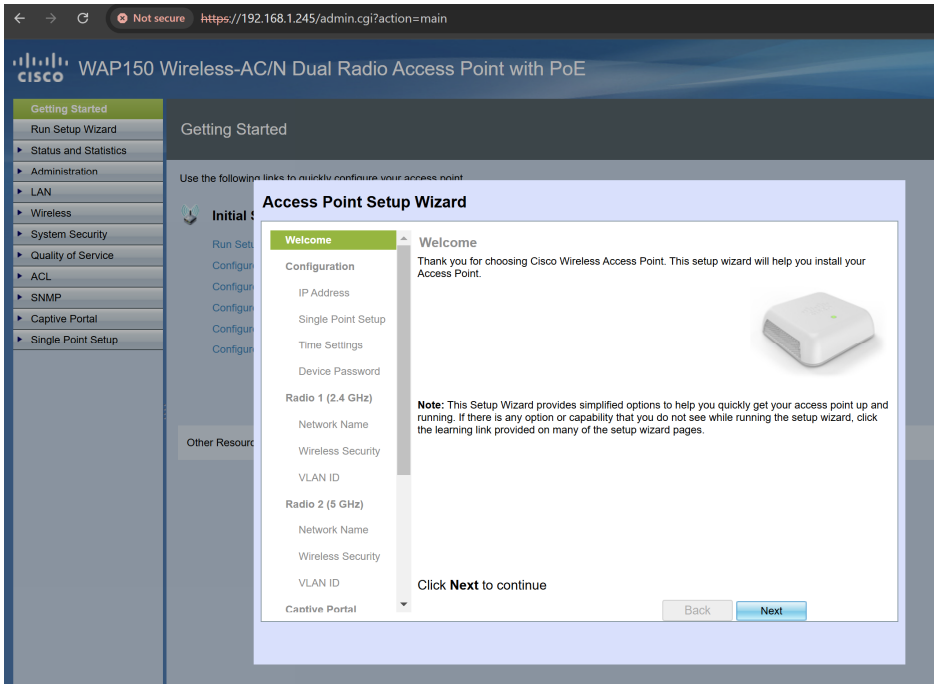


Figura 8. WAP150 Access Point Setup Wizard

Observație: pentru a gasi adresa IP a APului, asignată de serverul DHCP se pot utiliza pașii de mai jos:

- notați adresa MAC a APului (se regăsește pe eticheta acestuia)
- din command promt (cmd) sau terminal, rulați comanda ping catre adresa 192.168.1.255
- rulați comanda arp -a (căutați adresa MAC a punctului de acces și notați adresa sa IP).
- alternativ, puteti utiliza un utilitar care scanează rețeaua în intervalul 192.168.1.1 - 192.168.1.254 (de ex. utilitarul Nmap sau Angry IP Scanner)

Adresa IP a punctului de acces poate fi configurată în două moduri (fig. 9): dinamic (opțiunea implicită, prin protocolul DHCP) sau static (configurarea manuală a adresei IP și a celorlalți parametri de rețea).

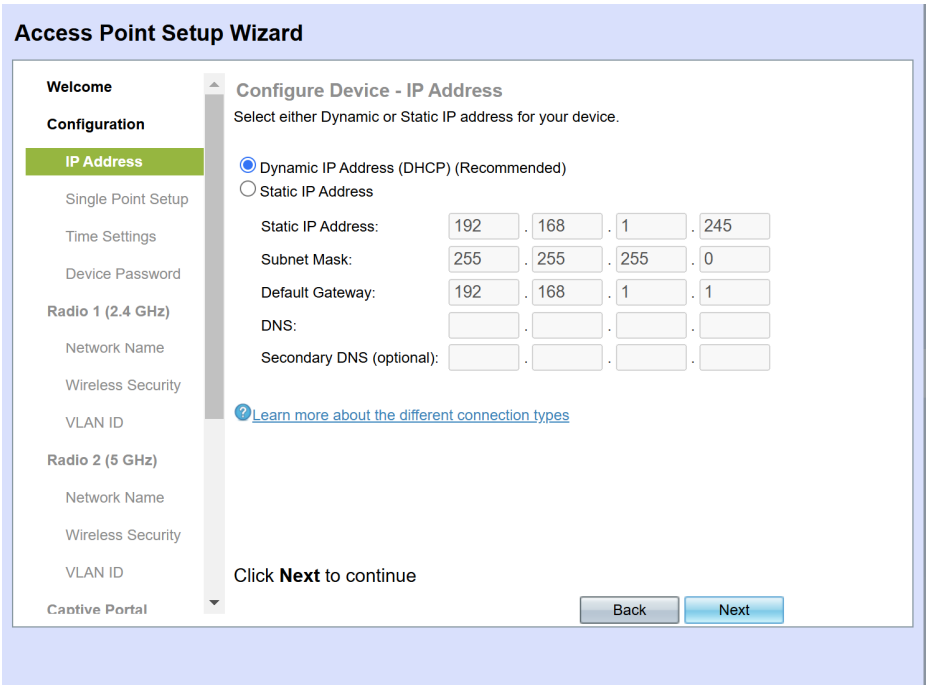


Figura 9. Configurarea adresei IP a dispozitivului

AP-ul Cisco WAP150 oferă o opțiune de clustering (fig. 10) – mai multe puncte de acces pot fi gestionate împreună ca un singur grup pentru a simplifica administrarea rețelei și pentru a oferi suport de scalabilitate. Un cluster poate include până la 4 puncte de acces Cisco WAP150, lucrând împreună pentru a acoperi o zonă mai mare sau pentru a oferi conectivitate suplimentară utilizatorilor. Clusterul poate susține până la 120 de dispozitive conectate simultan, distribuite pe cele 4 puncte de acces. Aceasta permite o gestionare eficientă a traficului și asigură o experiență optimizată utilizatorilor conectați.

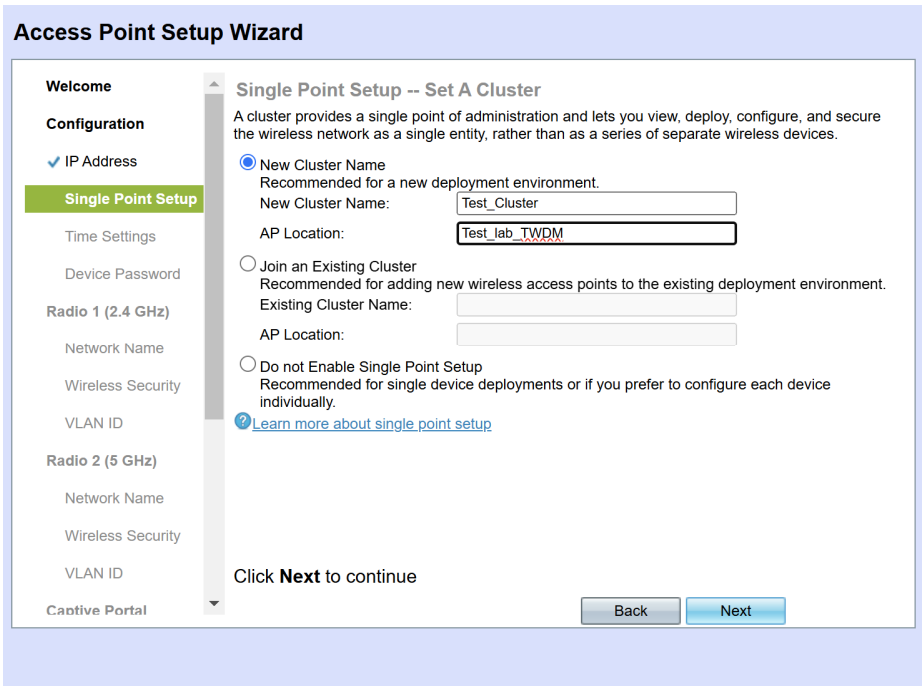


Figura 10. Crearea unui cluster și funcția Single Point Setup

Funcția Single Point Setup creează un cluster dinamic (un grup de dispozitive WAP) aflate în aceiași subrețea a unei rețele. Un cluster poate propaga informațiile de configurare către toate dispozitivele. Prin configurarea Single Point Setup pe un dispozitiv, setările acestuia sunt distribuite automat către celelalte dispozitive pe măsură ce acestea se conectează la cluster. Există și opțiunea ca AP-ul să se alăture unui cluster existent, prin introducerea numele grupului clusterului. Observație: este obligatoriu ca toate dispozitivele dintr-un cluster să fie de același model.

Configurarea corectă a timpului și datei pe un punct de acces este importantă pentru funcționarea precisă a fișierelor de log, autentificarea bazată pe certificate, sincronizarea între dispozitive și respectarea protocoalelor de rețea sau a reglementărilor de audit.

De asemenea, parola implicită a dispozitivului trebuie schimbată (fig. 11) pentru a preveni accesul neautorizat, a proteja rețeaua împotriva atacurilor cibernetice și a asigura conformitatea cu practicile de securitate.

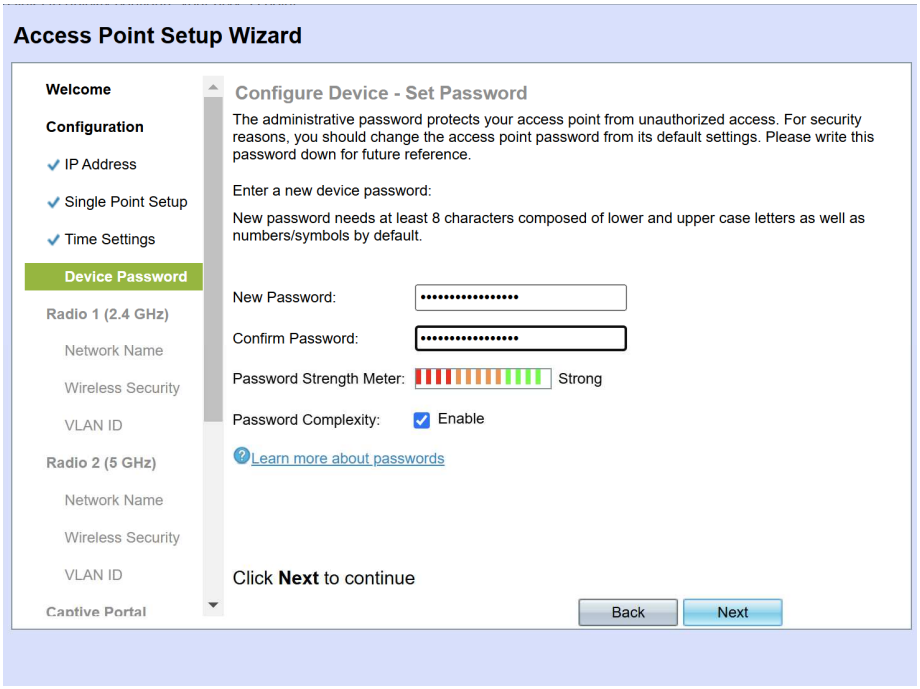


Figura 11. Schimbarea parolei implicite

Pasul următor este configurarea Radio 1, care utilizează banda de 2.4 GHz și Radio 2, care utilizează banda de 5 GHz pentru viteză mai mare dar cu o acoperire mai redusă (fig. 12 – 14). Se va introduce un nume de rețea care va servi drept SSID pentru rețeaua wireless implicită, se va specifica o cheie de securitate și tipul de securitate (implicit WPA2 Personal – AES; dacă dispozitivul permite, se recomandă utilizarea WPA3) și se va introduce ID-ul de VLAN pentru traficul recepționat pe rețeaua wireless. Punctele de acces virtuale (VAP) permit divizarea rețelei wireless LAN în diverse domenii de difuzare, similare cu VLAN-urile Ethernet. VAP-urile simulează multiple puncte de acces într-un singur dispozitiv fizic, fiecare VAP fiind identificat printr-un SSID.

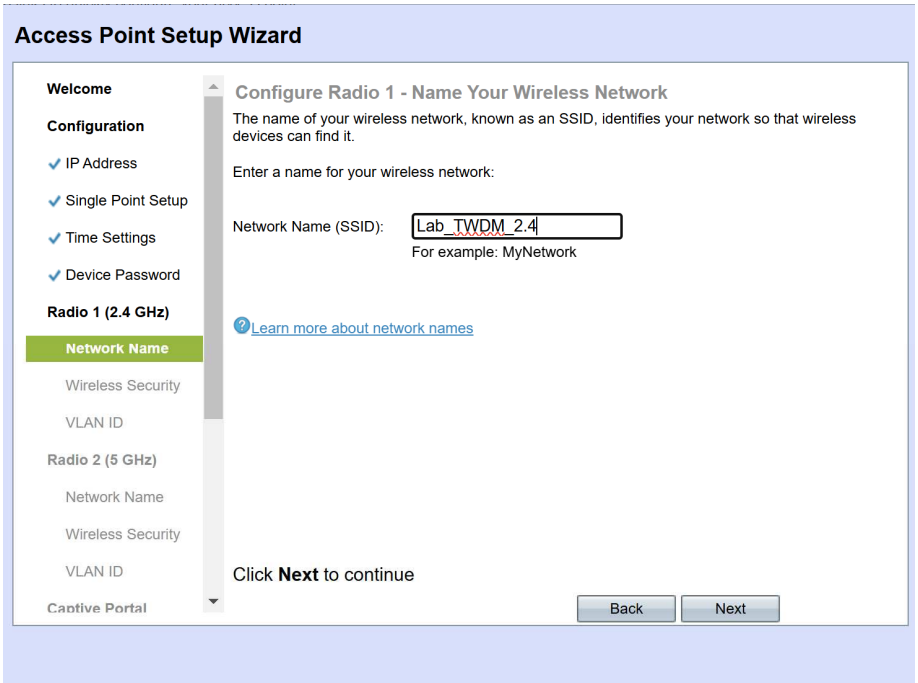


Figura 12. Configurare SSID

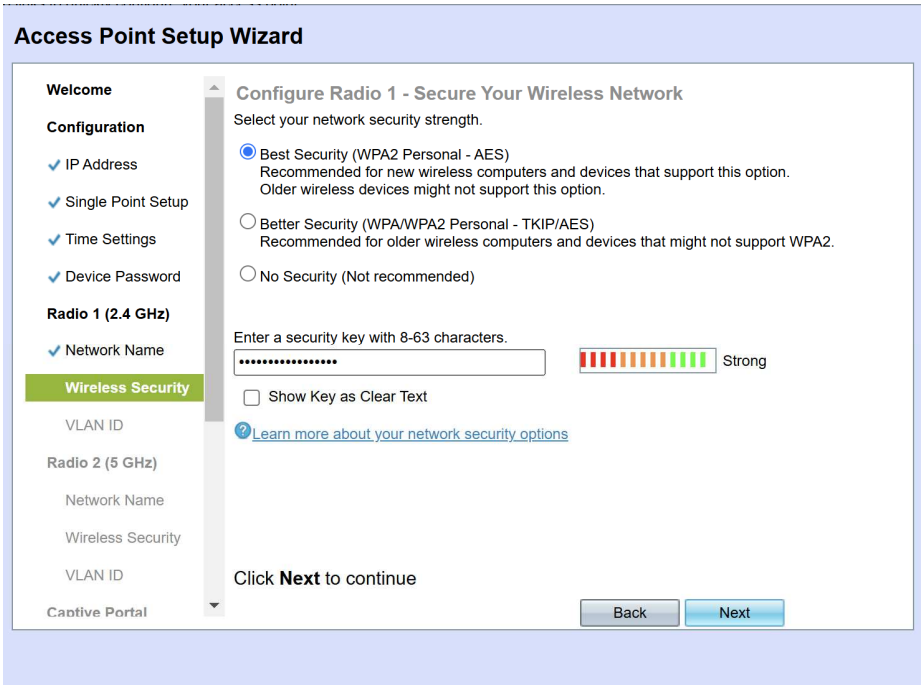


Figura 13. Configurare metodă de securitate

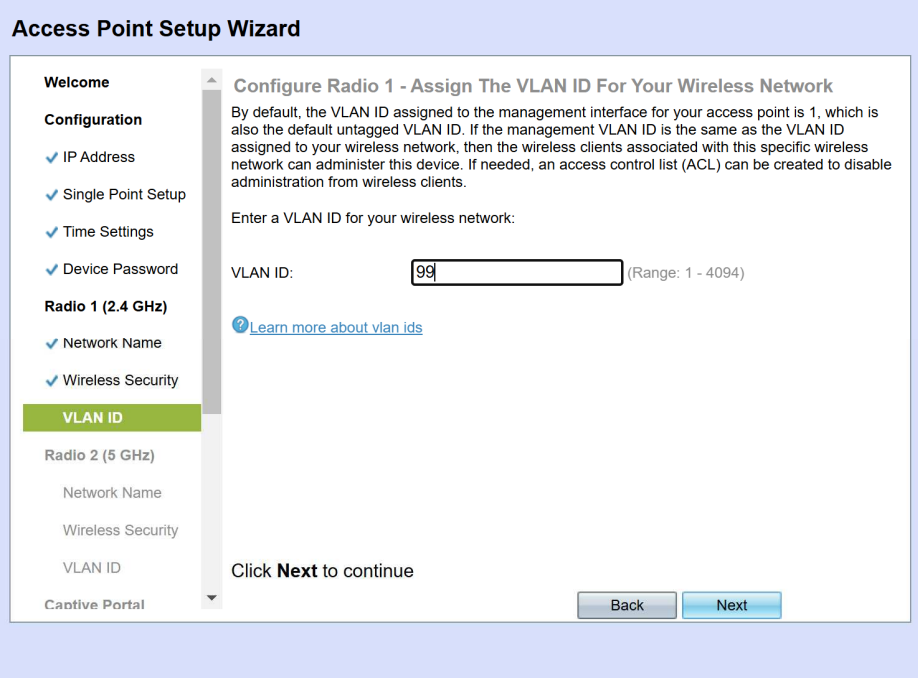
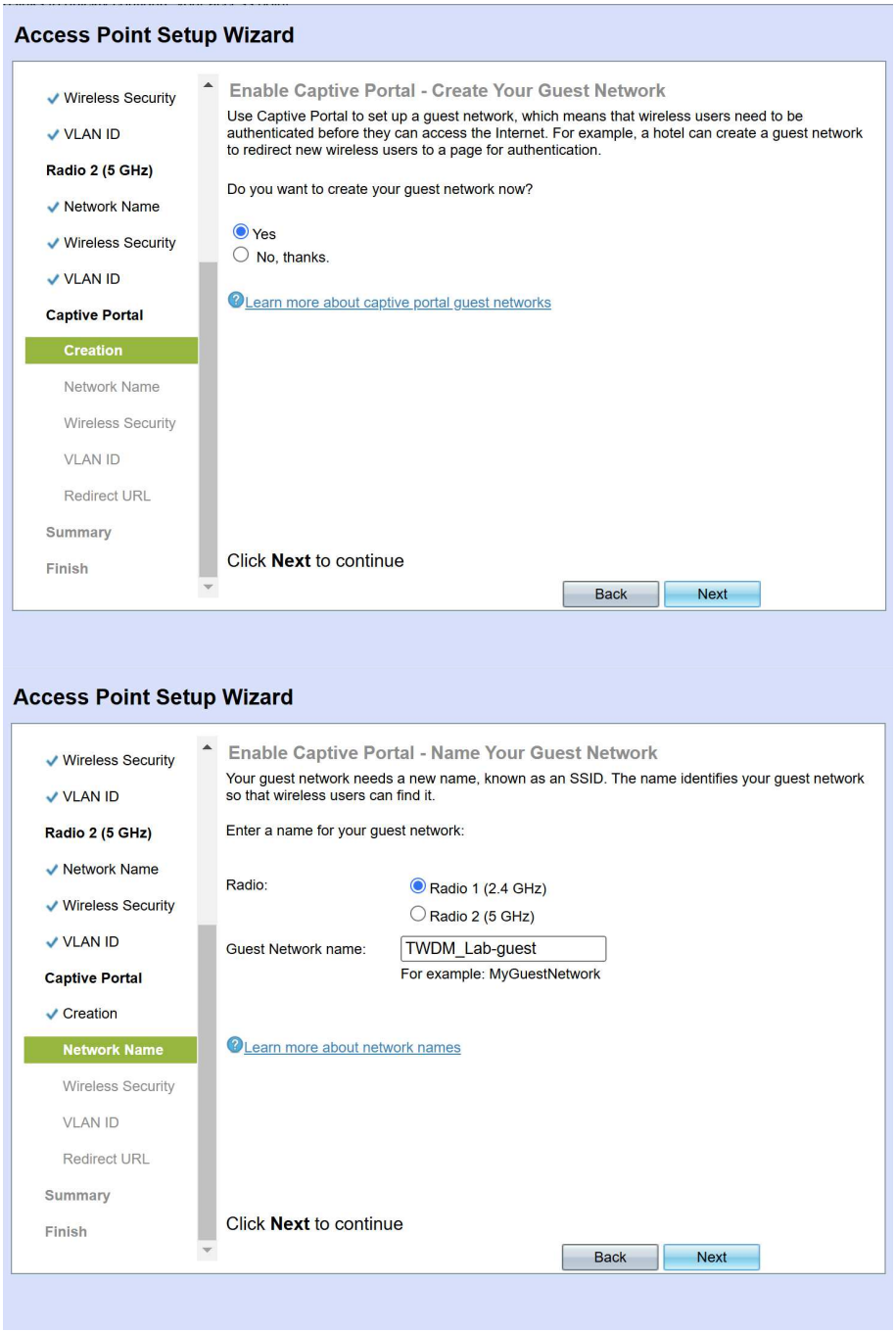
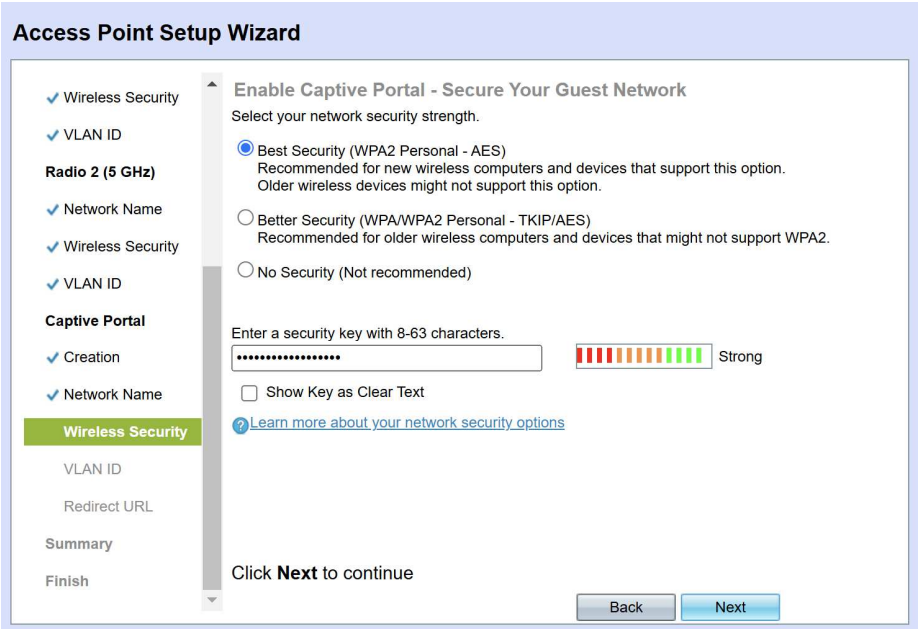
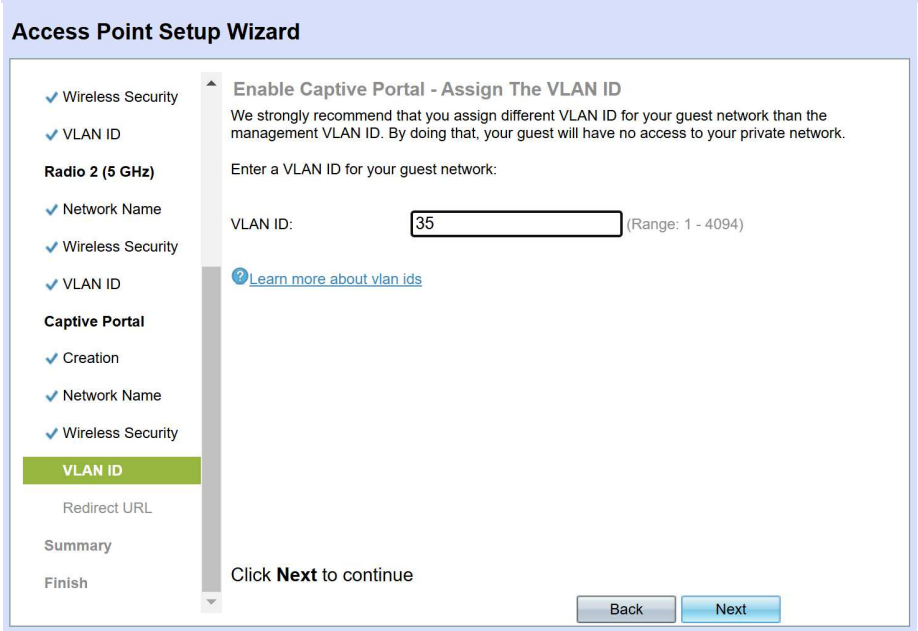


Figura 14. Configurare VLAN

Punctele de acces WAP150 permit oferirea unui acces WiFi securizat pentru oaspeți (Guest network), punând la dispoziție un *portal captiv (captive portal)* cu diverse opțiuni de autentificare, precum și posibilitatea de a seta drepturi, roluri și limite pentru lățimea de bandă. Un portal captiv este o interfață web care se afișează automat utilizatorilor atunci când încearcă să acceseze o rețea Wi-Fi publică sau privată și este folosit pentru a gestiona și controla accesul la rețea. Configurarea (fig. 15) presupune, similar cu pașii anteriori, specificarea unui nume pentru rețeaua de oaspeți, a unei chei de securitate, definirea unui VLAN ID pentru rețeaua de oaspeți. Opțional, se poate specifica o adresă URL de redirecționare a utilizatorii după autentificare.


Access Point Setup Wizard
Wireless Security
VLAN ID
Radio 2 (5 GHz)
Network Name
Wireless Security
VLAN ID
Captive Portal
Creation
Network Name
Wireless Security
VLAN ID
Redirect URL
Summary
Finish
Enable Captive Portal - Create Your Guest Network
Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.
Do you want to create your guest network now?
Yes
No, thanks.
Learn more about captive portal guest networks
Click Next to continue
Back
Next
Access Point Setup Wizard
Wireless Security
VLAN ID
Radio 2 (5 GHz)
Network Name
Wireless Security
VLAN ID
Captive Portal
Creation
Network Name
Wireless Security
VLAN ID
Redirect URL
Summary
Finish
Enable Captive Portal - Name Your Guest Network
Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.
Enter a name for your guest network:
Radio:
Radio 1 (2.4 GHz)
Radio 2 (5 GHz)
Guest Network name:
TWDM_Lab-guest
For example: MyGuestNetwork
Learn more about network names
Click Next to continue
Back
Next


Access Point Setup Wizard
Wireless Security
VLAN ID
Radio 2 (5 GHz)
Network Name
Wireless Security
VLAN ID
Captive Portal
Creation
Network Name
Wireless Security
VLAN ID
Redirect URL
Summary
Finish
Enable Captive Portal - Secure Your Guest Network
Select your network security strength.
Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.
Better Security (WPA/WPA2 Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.
No Security (Not recommended)
Enter a security key with 8-63 characters.
Strong
Show Key as Clear Text
Learn more about your network security options
Click Next to continue
Back
Next


Access Point Setup Wizard
Wireless Security
VLAN ID
Radio 2 (5 GHz)
Network Name
Wireless Security
VLAN ID
Captive Portal
Creation
Network Name
Wireless Security
VLAN ID
Redirect URL
Summary
Finish
Enable Captive Portal - Assign The VLAN ID
We strongly recommend that you assign different VLAN ID for your guest network than the management VLAN ID. By doing that, your guest will have no access to your private network.
Enter a VLAN ID for your guest network:
VLAN ID:
35
(Range: 1 - 4094)
Learn more about vlan ids
Click Next to continue
Back
Next

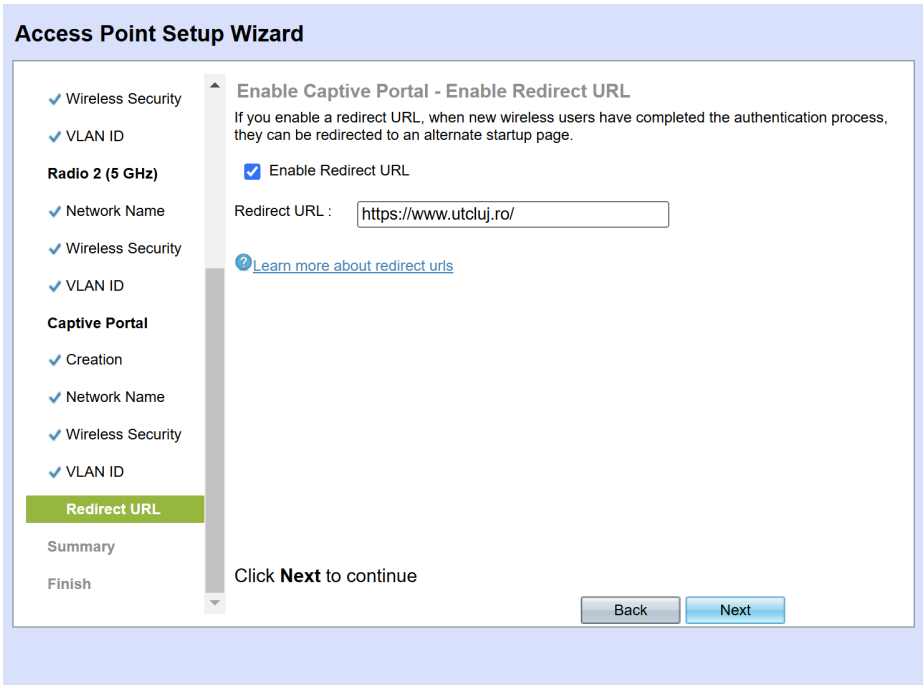
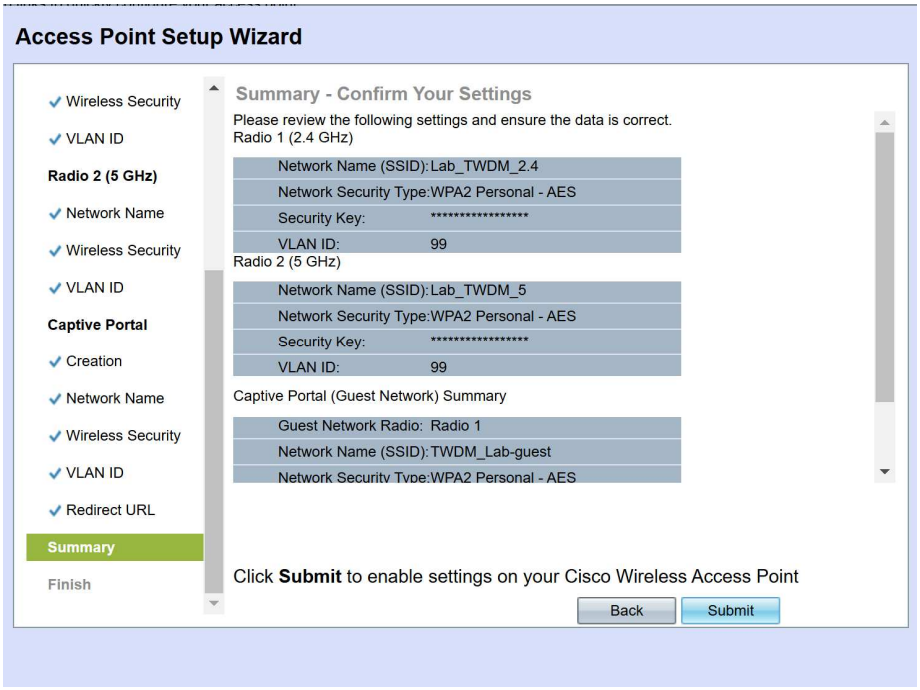


Figura 15. Configurarea opțiunii Captive Portal

Pagina de Sumar (Summary page) permite verificarea configurațiilor introduse și confirmarea acestora prin butonul Submit (fig. 16).



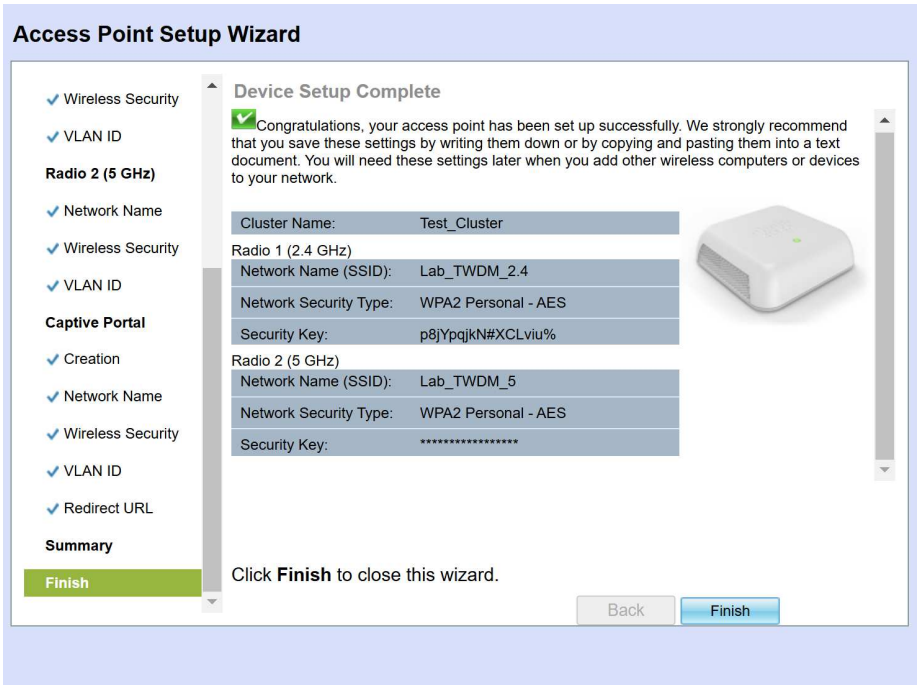


Figura 16. Pagini de sumar

Pentru o securitate sporită, dispozitivul Cisco WAP150 permite configurarea opțiunilor de SSID Broadcast - numele rețelei nu este afișat în lista de rețele disponibile, Channel Isolation - împiedică comunicarea directă între dispozitivele conectate la același SSID și MAC filter - utilizarea unei liste de adrese MAC pentru a controla accesul dispozitivelor la rețea. De asemenea, pentru optimizarea performanței rețelei prin direcționarea dispozitivelor către banda de 5 GHz se poate utiliza opțiune Band Steer.

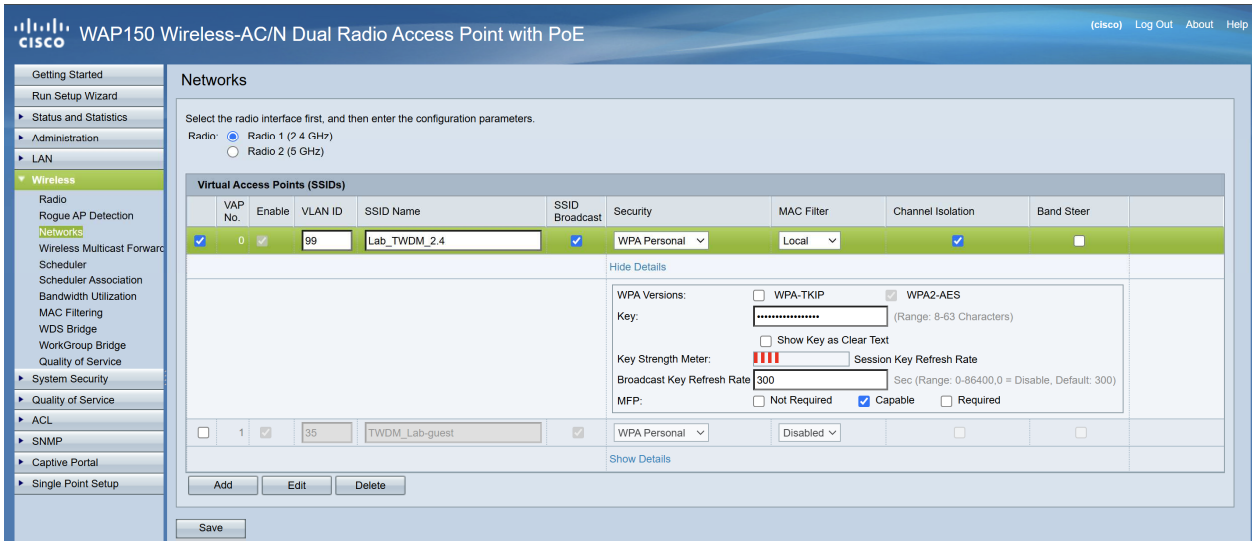


Figura 17. Configurarea opțiunilor SSID Broadcast, Channel Isolation și Band Steer

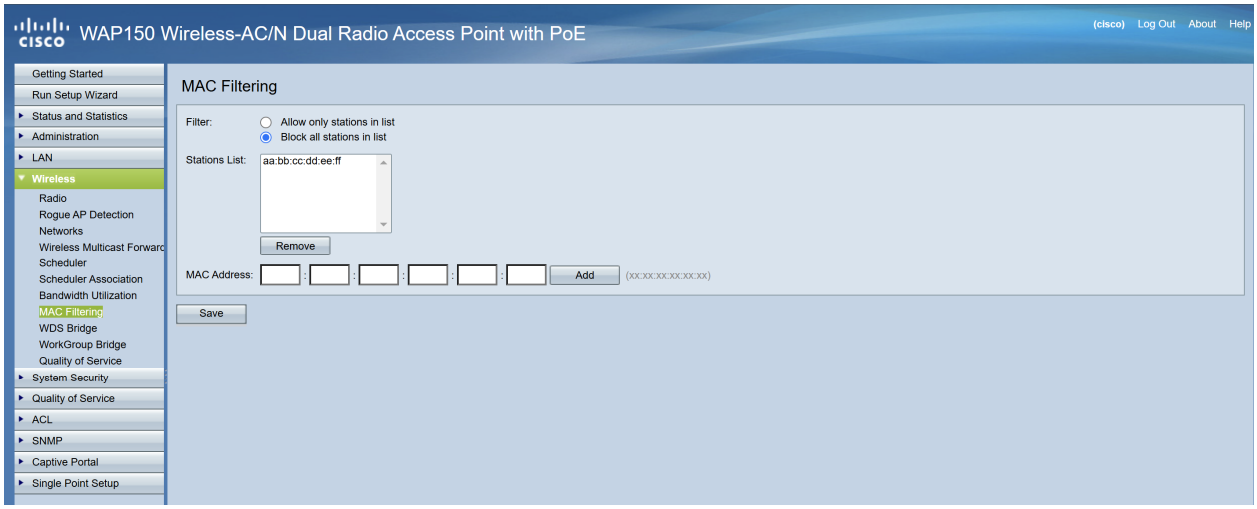


Figura 18. Configurarea opțiunii MAC Filter

Pe lângă aceste măsuri de securitate de bază, se recomandă și implementarea unor măsuri suplimentare care vor contribui la creșterea securității rețelei wireless.

3. Aplicaţii practice

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

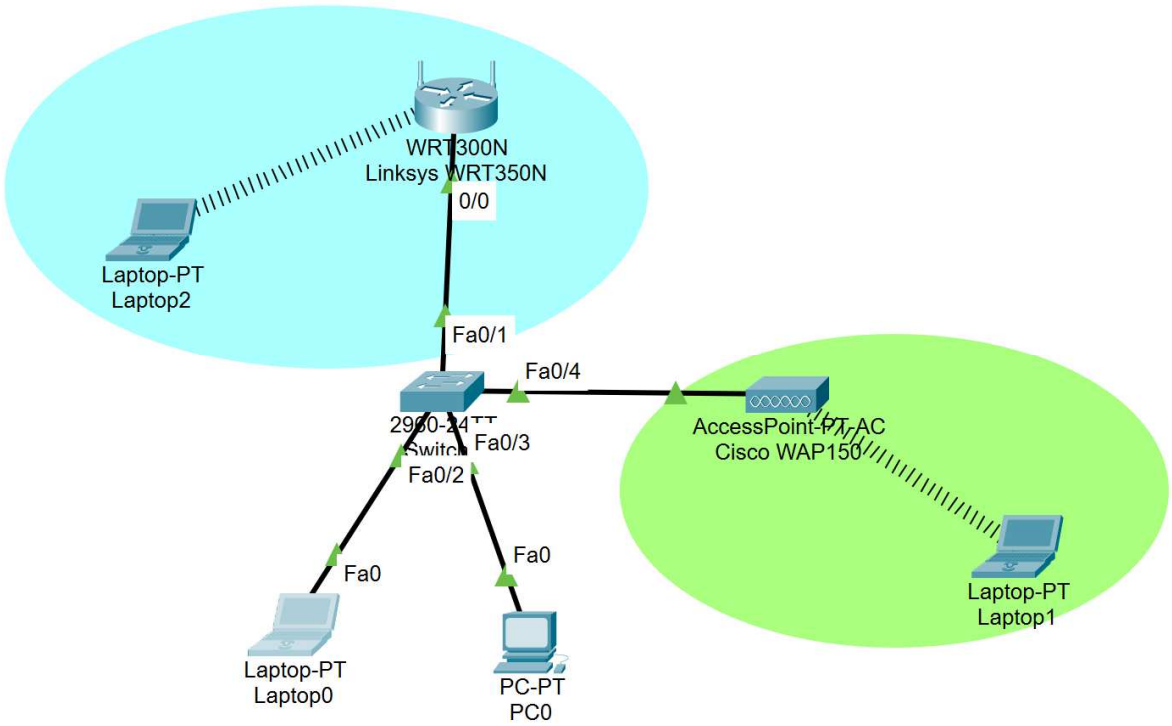
3.2 Se va configura şi se va securiza ruterul Linksys WRT350N Wireless-N Gigabit with Storage Link utilizând utilitarul Web. Se va ataşa un hard-disk/flash USB extern care se va partaja în reţea.

3.3 Se va conecta Cisco WAP150 la reţeaua de test din cadrul laboratorului, conform paşilor descrişi în cadrul lucrării și se va configura Cisco WAP150 ca Access Point pentru a extinde rețeaua wireless.

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

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

Dispozitiv		Adresa IP	Subnet mask	Default Gateway
Router	Internet	173.16.10.2	255.255.255.0	173.16.10.1
	Wireless	172.16.100.10	255.255.255.0	-
AP		Dinamic (DHCP) de la rețeaua wireless router	Dinamic (DHCP) de la rețeaua wireless router	Dinamic (DHCP) de la rețeaua wireless router
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
AP	Wi-Fi	Band Steer	WPA2 Personal	Cisco4321	Pass4321

Bibliografie:

[1] Linksys WRT350N Wireless-N Gigabit User Manual, https://downloads.linksys.com/downloads/userguide/WRT350N-EU-LA+v2+user+guide+Rev+A+web,0.pdf
[2] Cisco CCNA LAN Switching and Wireless Course
[3] Cisco WAP150 datasheet, https://www.cisco.com/c/en/us/products/collateral/wireless/small-business-100-series-wireless-access-points/datasheet-c78-736450.html

VIII. Configurarea reţelelor wireless: Configurări avansate

1. Obiective

Obiectivul acestui capitol este descrierea rolului punctelor de acces (AP) în cadrul reţelelor fără fir, prezentarea principalelor tipuri de AP-uri, caracteristicile lor, modalităţile de funcţionare şi prezentarea rolului controllerelor wireless. De asemenea, se vor prezenta conceptele PoE și metode alternative pentru extinderea ariei de acoperire. Se va expune modul de instalare şi configurare al unor puncte de acces (ex. Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet), precum şi, configurări avansate ale routerelor wireless (ex. Linksys WRT350N Wireless-N Gigabit). În plus, se vor prezenta principalele bune practici de securizare ale dispozitivelor wireless.

2. Consideraţii 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 reţea wireless. Într-o reţea cablată, echivalentul acestui dispozitiv îl reprezintă hub-ul. Un access point poate fi privit ca un hub wireless, însă cu câteva îmbunătăţiri, prezentând şi capabilităţi de switch. Principala funcţie a unui AP este funcţia de bridging, direcţionând traficul, fie la backbone-ul reţelei, fie înapoi în mediul fără fir. O staţie 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 reţele wireless în mod infrastructură.

Principalele tipuri de puncte de acces 802.11 includ AP-uri de tip standalone (independente) și AP-uri de tip lightweight (dependente de un controller wireless). AP-urile standalone sau autonome funcționează independent, fiind gestionate și configurate direct pe fiecare dispozitiv. Acestea sunt potrivite pentru rețele de dimensiuni mici, cu un număr limitat de AP-uri, deoarece necesită administrare individuală. AP-urile lightweight (LWAP) nu au toate funcțiile de administrare și control încorporate (ci doar funcții de bază) și sunt gestionate centralizat de un nod central, denumit controller wireless. Utilizarea unui controller wireless (Wirelesss LAN Controller - WLC) permite administrarea mai multor AP-uri dintr-un singur loc, pentru a asigura performanța și securitatea întregii rețele. Aceste AP-uri sunt utilizate în rețele de dimensiuni mari, cu mai multe dispozitive, care necesită o administrare complexă.

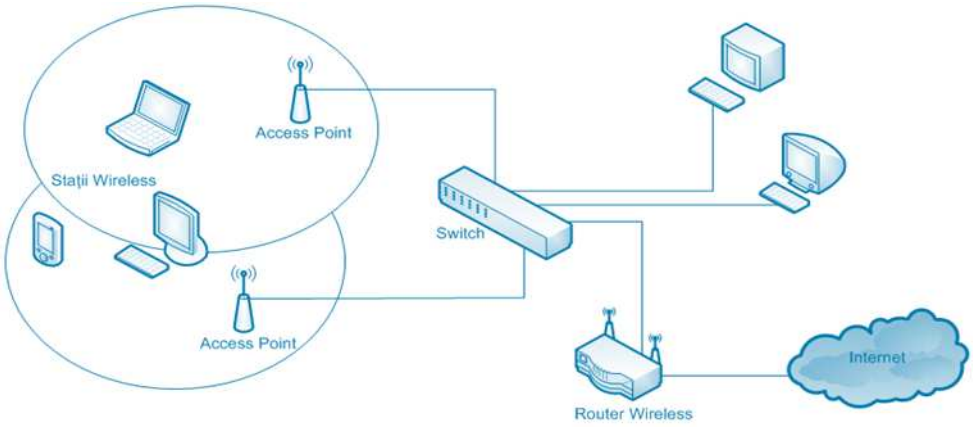


Figura 1. Exemplificarea conectării Punctelor de Acces

Un WLC are rolul de a acționa ca un punct central de management pentru access point-uri, facilitând configurarea și administrarea acestora dintr-o singură locație. Acesta poate gestiona până la câteva sute de AP-uri, în funcție de capacitatea sa, iar dispozitivele pot fi în aceeași subrețea sau într-o rețea complet diferită. Într-o rețea de dimensiuni mari, de tip enterprise, mai multe WLC-uri îndeplinesc funcția de management pentru LAP-uri.

WLC-urile pot fi dispozitive fizice amplasate în centrele de telecomunicații și oferă conectivitate directă pentru dispozitivele din rețea. Alternativ, WLC-urile pot fi soluții de tip cloud, care nu necesită instalarea unui echipament local, ci funcționează printr-o conexiune la internet. oluțiile de tip cloud oferă flexibilitate și scalabilitate, dar depind de o conexiune stabilă la rețea pentru a funcționa eficient (fig. 2). Un WLC îndeplinește o multitudine de funcții, cum ar fi administrarea centralizată a rețelei wireless, securitate avansată prin criptare și autentificare, optimizarea automată a performanței rețelei prin ajustarea dinamică a canalelor și a puterii semnalului, monitorizarea în timp real a traficului și dispozitivelor conectate, precum și suport pentru scalabilitate.

Control And Provisioning of Wireless Access Points (CAPWAP) [5] este un protocol de nivel 2, standardizat și interoperabil care facilitează gestionarea centralizată a AP-urilor dintr-o rețea de către un WLC. CAPWAP utilizează un model client-server, în care controllerul (WLC) funcționează ca server responsabil pentru gestionarea AP-urilor, iar AP-urile acționează ca clienți, conectându-se la controller pentru a primi configurații și a raporta informații despre starea lor.

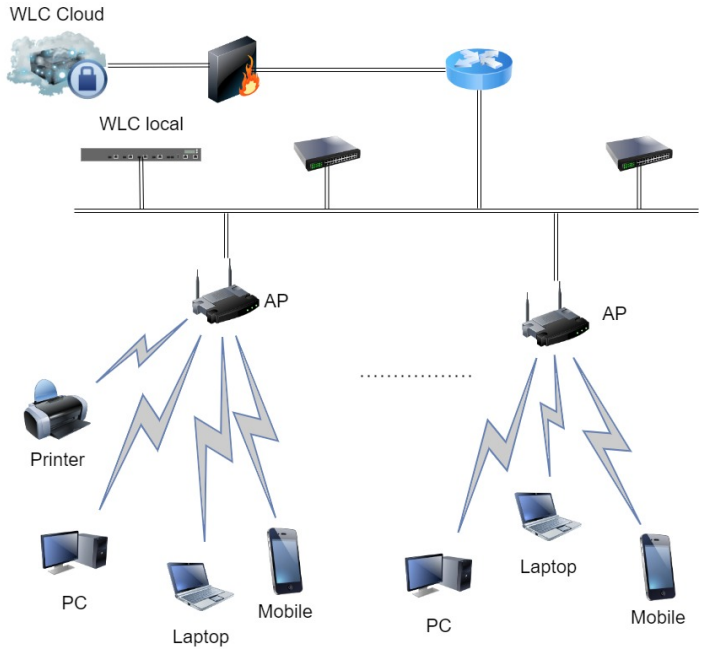


Figura 2. Exemplificare amplasare WLC local și în cloud

Un avantaj important adus reţelelor wireless, de către punctele de acces, îl reprezintă posibilitatea de Roaming pentru utilizatorii mobili. Condiţia prealabilă, care trebuie îndeplinită de către AP-uri şi staţiile 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.

Punctul de acces Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet (fig. 3) este o componentă Wi-Fi care permite conectarea, în mod infrastructură, a mai multor staţii fără fir la o reţea locală de calculatoare.

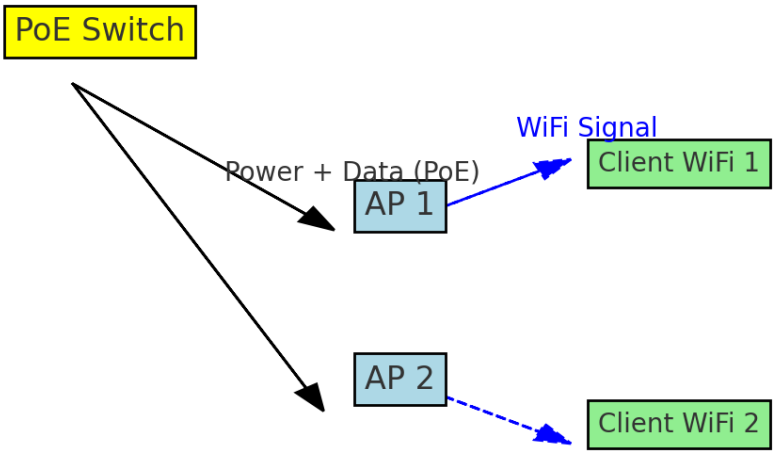


Figura 4. Exemplu de conectare a unor AP-uri prin PoE

Power over Ethernet PoE permite alimentarea dispozitivelor de rețea (în cazul nostru, puncte de acces) prin intermediul cablurilor Ethernet, utilizate în mod normal doar pentru

transmiterea datelor. PoE nu este o tehnologie proiectata pentru rețelele fără fir, însă este o tehnologie larg utilizată pentru alimentarea echipamentelor 802.11, în special APuri de tip business/enterprise (fig. 4). Acest lucru permite o instalare facilă a APurilor în locații în care nu sunt disponibile prize de alimentare.

Principalele standarde PoE sunt:

- PoE (IEEE 802.3af) – poate furniza până la 15,4W de energie.
- PoE+ (IEEE 802.3at) – poate furniza până la 30W de energie.
- PoE++ (IEEE 802.3bt) –poate furniza până la 90W de energie.

Figura 5. 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 acţiune;
- 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 interfeţelor dispozitivului

Figura 5 prezintă o vedere frontală a dispozitivului. Led-urile dispozitivului permit o diagnosticare rapidă a funcţionării 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/recepţionează 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/recepţionează date;

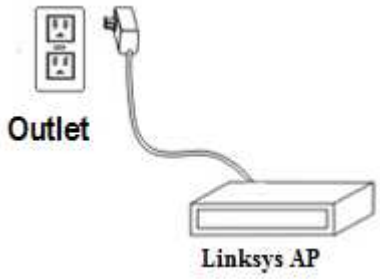
Figura 6. Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet [1]

Figura 6 prezintă o vedere din spate a dispozitivului:

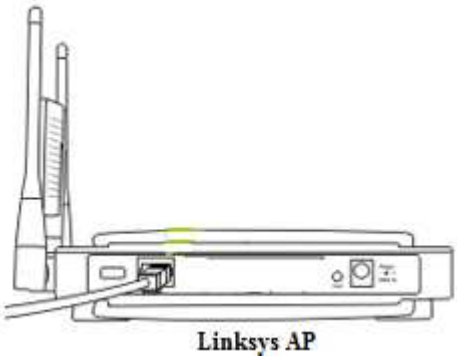
- *Alimentare* – alimentarea AP-ului prin adaptorul 12V DC;
- *Port RJ45* (*ETHERNET*) – utilizat pentru conectarea unor PC-uri sau a unor elemente de reţea;
- *Reset* – buton pentru resetarea la configuraţia implicită;

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

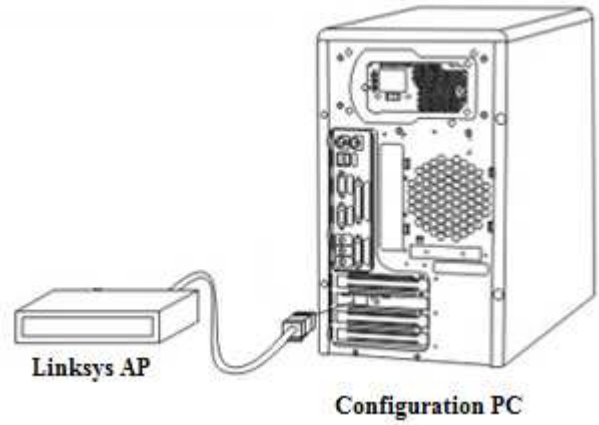
Figura 7 [1] prezintă paşii care trebuie urmaţi pentru conectarea AP-ului la sistemul de distribuţie cablat/PC-ul pentru configurare. La sfârşitul pasului d, led-urile frontale vor indica activitatea AP.



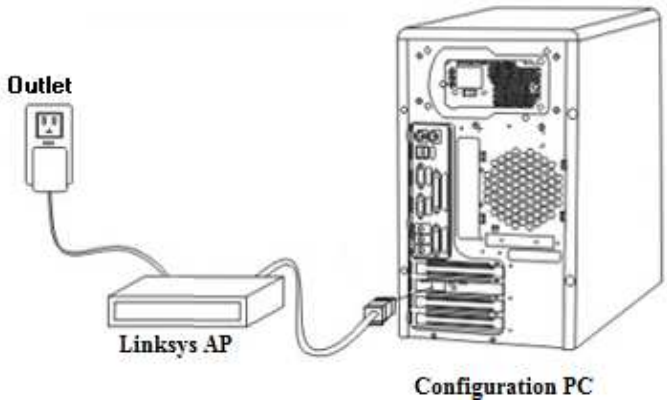
Pas a. Unplug the AP



Pas b. Conect the network cable to the AP



Pas c. Conect the network cable to the PC



Pas d. Plug the AP

Figura 7. Conectarea AP la PC [1]

Tab	Funcţie
Setup	Setări generale de conexiune
Wireless	Setări conexiune wireless
Security Monitor	Setări pentru aplicaţia de monitorizare
Administration	Setări dispozitiv
Status	Informaţii dispozitiv

Tabelul 1. Tab-uri de opţiuni [1]

Punctul de acces este proiectat pentru a fi funcţional 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 opţiunilor disponibile. Această lucrare descrie modul de configurare bazat pe utilizarea utilitarul web. Tabelul 1 prezintă o descriere sumară a tab-urilor principale de opţiuni:

2.4. Configurarea utilizând Utilitarul Web

Pentru a accesa utilitarul Web (configurare utilizând browserul web – fig.8), se va utilizaMicrosoft Edge sau Google Chrome, şi se va accesa http://192.168.1.245. Informaţiile implicite de conectare sunt:

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

Staţia de pe care se realizează configurarea se va seta cu o adresă IP statică, din aceeaşi subreţea ca şi AP-ul (192.168.1.0/24). Dacă în reţea există un server DHCP, acesta se va configura pentru a atribui adrese IP din aceeaşi subreţea 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 8. Conectarea la utilitarul Web

Principalele probleme întâmpinate la accesarea AP-ului sunt:

- Staţia de pe care se realizează configurarea nu este setată să utilizeze IP-uri statice din aceeaşi subreţea cu AP-ul;
- Serverul DHCP al reţelei nu este configurat pentru a atribui adrese IP din aceeaşi subreţea ca şi AP-ul.
- Nu se utilizează browserul corespunzător (IE, NN);
- Nivelul de securitate al browserului este prea ridicat, nepermiţând conectarea (verificare Security Level în IE);
- Firewall-ul staţiei blochează accesul la serviciile http (adăugare regulă de acces sau deactivarea temporară a firewall-ului);

- Probleme hardware (placă de reţea 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 informaţiile de reţea (adresa IP);
- Wireless -> Basic Wireless Settings: opţiune pentru a modifica numele reţelei şi pentru a seta un mod de securitate/parolă;
- Administration -> Management: opţiune pentru a schimba parola implicită.

În continuare se vor descrie tab-urile de opţiuni, împreună cu subopţiunile de configurare:

A. Setup

- Basic Setup: introducere informaţii legate de numele AP-ului;
    - Host Name: numele folosit pentru accesarea Utilitarului Web prin intermediul reţelei – 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 opţiuni 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 reţelei wireless (nume, canal, etc);
- Wireless Security: configurarea setărilor de securitate pentru reţeaua wireless;
- Wireless Connection Control: restricţionarea accesului la reţeaua wireless prin filtrarea adreselor MAC ale staţiilor client;
- Advanced Wireless Settings: opţiune pentru configuraţii avansate, pentru administratorii de reţea:
    - WMM – opţiune QoS, parte a 802.11e. Permite prioritizarea traficului, prin existenţa 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 reţelei wireless prin intermediul unei aplicaţii instalate pe PCul administratorului. Informaţiile furnizate de către aplicaţie sunt legate de detecţia şi clasificarea clienţilor şi a AP-urilor wireless.

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

D. Administration

- Management: opţiuni 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 configuraţiei AP-ului.

E. Status

- Oferă informaţii despre statusul AP-ului.

2.5. Configurări avansate Linksys WRT350N Wireless-N Gigabit Router

2.5.1. Expunerea unor aplicaţii către utilizatori externi

Paşii necesari pentru expunerea unor Servere de Aplicaţii [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 opţiuni (DMZ) este utilă dacă aplicaţiile 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 opţiunea DMZ, deoarece opţiunea de DMZ este cea mai puţin prioritară dintre opţiunile de expunere către utilizatorii externi.

Paşii necesari pentru expunere utilizând opţiunea 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 urmaţi de către administratorul dispozitivului wireless pentru a creşte siguranţa reţelei wireless.

- Administratorul ar trebui să modifice SSID-ul implicit și să dezactiveze opțiunea de SSID broadcast, reducând vizibilitatea rețelei.
- Parola implicită a contului de Administrator trebuie schimbată, iar pentru accesul rețelei să fie utilizată o cheie puternică.
- Limitarea numărului de clienți conectați, utilizarea unor standarde de criptare avansate și schimbarea periodică a parolelor adaugă un nivel suplimentar de control.
- Autentificare 802.1X se poate utiliza pentru controlul accesul utilizatorilor la rețea.
- Utilizarea opțiunilor de filtrare (liste de acces, filtre web) și adăugarea unui firewall adaugă un grad sporit de control a traficului de rețea și blocarea conținutului malițios.
- Utilizarea unor servicii de monitorizare și logare permit identificarea activităților suspecte, diagnosticarea problemelor de rețea și menținerea unui istoric.

2.5.4. Ajustarea performanţelor 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 informaţiilor adiţionale 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.

Becon Interval

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 capacităţii liniei. Scăderea valorii parametrului Becon Interval conduce la creşterea fiabilităţii, deoarece APul se va anunţa mai des, ajutând, de asemenea, nodurile mobile care îşi schimbă rapid locaţia. 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 clienţilor ca răspuns la o interogare din partea acestora. Pentru a recepţiona cadrele broadcast sau multicast salvate în buffer, clienţii sunt anunţaţi 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 recepţie, fapt ce poate afecta anumite aplicaţii 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 interferenţe, deoarece se vor retransmite doar fragmentele pierdute din cadrul iniţial. 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 necesităţii 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 interferenţelor. 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.

2.6 Metode alternative pentru extinderea ariei de acoperire

Pentru a extinde aria de acoperire a unei rețele fără fir, pentru situațiile în care nu se pot instala cabluri Ethernet și AP-uri, se pot utiliza dispozitive *Wi-Fi Extender* (repetoare WiFi) sau dispozitive *Power Line Adapters.*

Un dispozitiv Wi-Fi Extender captează semnalul Wi-Fi existent de la echipament (router wireless sau AP) și îl retransmite într-o zonă unde semnalul este slab sau inexistent. Principalele avantaje al utilizarii unui Wi-Fi Extender sunt costul redus și ușurința în instalare, însă poate reduce viteza, mai ales dacă semnalul captat și apoi retransmis nu este suficient de puternic (fig. 9). O alternativă pentru aceste echipamente este utilizarea unor echipamente Wi-Fi de tip mesh.

Figura 9. Exemplificare de utilizare a Wi-Fi Extender Edimax [6]

Dispozitivele Power Line Adapters (PLA) permit extinderea conexiunii de Internet în zone unde semnalul WiFi este slab sau inaccesibil, iar alte metode nu pot fi utilizate. PLA utilizează cablurile electrice existente într-o clădire pentru a transmite date. Un dipozitiv PLA poate crea inclusiv un punct de acces Wi-Fi pentru dispozitivele wireless din zonă. Principalul avantaj al acestei soluții este folosirea cablurilor electrice existente, evitând necesitatea de a instala noi cabluri de rețea. Însă, performanța lor poate fi afectată de calitatea și vechimea cablurilor electrice din clădire. În plus, dispozitivele trebuie să fie conectate la

același circuit electric (de obicei în aceeași clădire sau etaj). În Figura 10 este exemplificat un sistem PLA al companiei TP-Link:

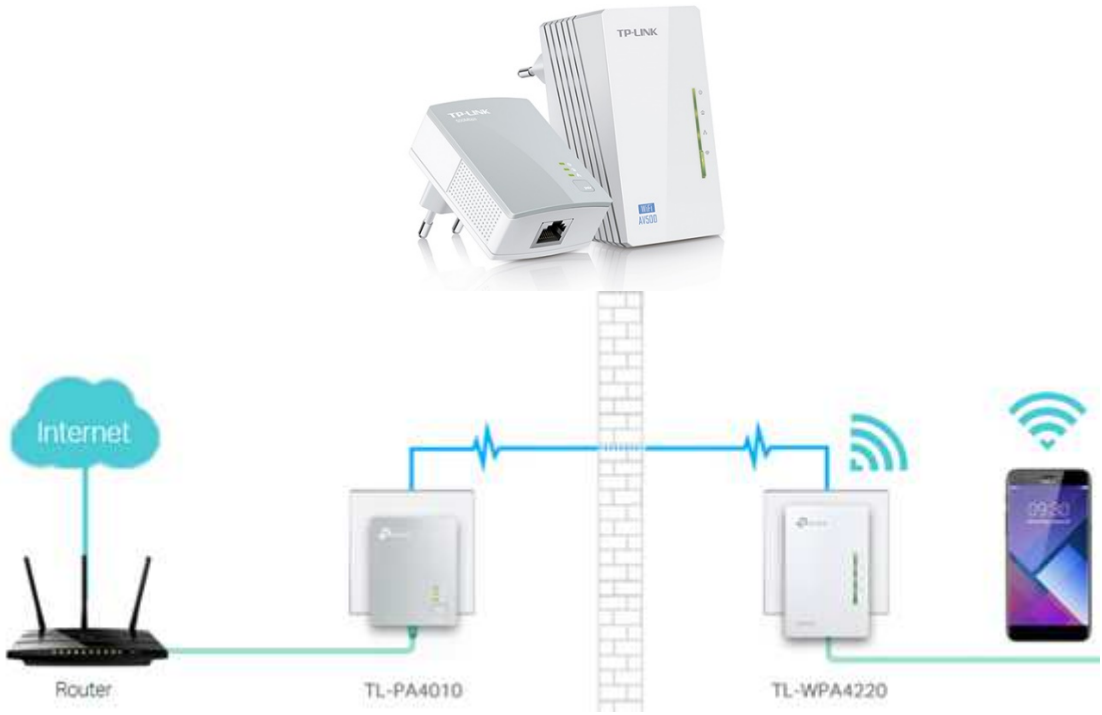


Figura 10. Exemplificare utilizare sistem PLA [7]

3. Aplicaţii practice

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

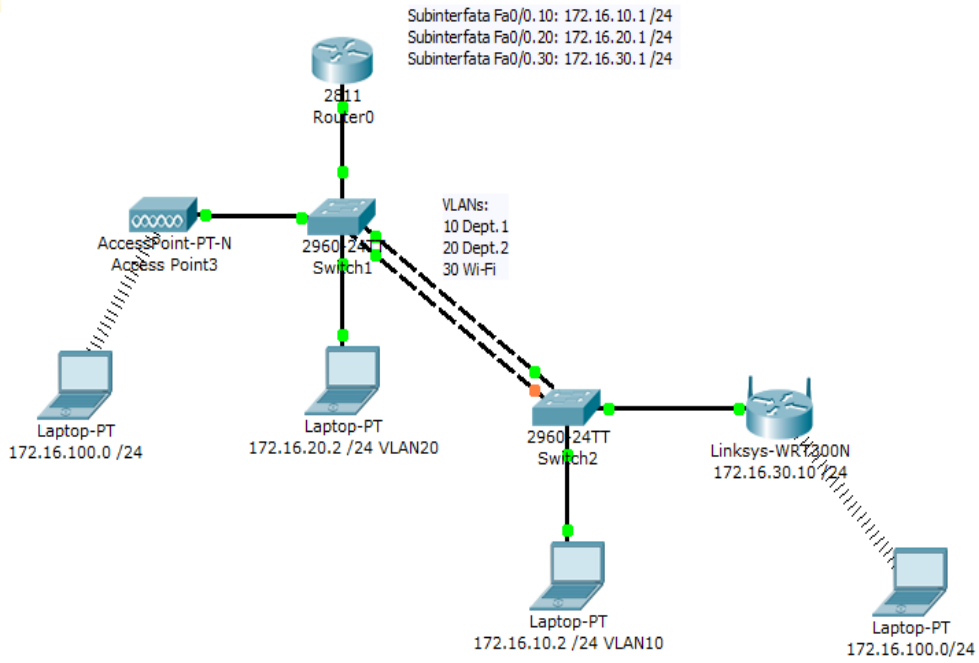
3.2 Se va configura şi se va securiza AP-ul Linksys WAP4400N Wireless-N Access Point with Power Over Ethernet utilizând utilitarul Web.

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

3.4 Se va testa conectivitatea la noua reţea wireless creată, prin conectarea staţiilor din cadrul laboratorului utilizând adaptoarele Wireless USB, PCMCIA şi PCI. Pentru testare, se va utiliza utilitarul ping şi se vor testa opţiunile 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 CCNA7 Switching, Routing, and Wireless Essentials, https://www.netacad.com/
[4] D. Coleman, D. Westcott, CWNA Certified Wireless Network Administrator Study Guide, Sybex Wiley Publishing, 2021.
[5] CAPWAP Protocol Specification, https://datatracker.ietf.org/doc/html/rfc5415
[6] Wi-Fi Extender Edimax, https://www.edimax.com/
[7] PLA TP-Link, https://www.tp-link.com/

IX. Configurarea reţelelor wireless: Configurare VPN

1. Obiective

Capitolul de faţă îşi propune prezentarea noţiunilor 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 reţea VPN wireless între un calculator şi un router wireless.

2. Consideraţii teoretice

2.1. Generalităţi

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

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

VPN asigură traficul printr-o reţea publică utilizând criptare avansată şi tunelare pentru a proteja confidenţialitatea informaţiei, 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 operaţionale în comparaţie cu reţeaua tradiţională WAN, reduce timpul de tranzit şi costurile de transport pentru utilizatorii aflaţi la distanţă, simplifică topologia reţelei în anumite cazuri şi limitează accesul la reţeaua ţintă. Prin VPN se pot integra mai multe aplicaţii: transfer de date, voce (voice over IP), videoconferinţe. VPN oferă securitate (informaţiile care circulă prin VPN sunt protejate prin diferite tehnologii de securitate, cum ar fi criptarea, autentificarea), mobilitate (angajaţii mobili, precum şi partenerii de afaceri, se pot conecta la reţeaua companiei într-un mod sigur, indiferent de locul în care se află), scalabilitate (atunci când apare o nevoie permanentă de angajaţi mobili şi conexiuni securizate cu partenerii strategici).

2.2. Tipuri de VPN

Există mai multe tipuri de reţele VPN, descrise în cele ce urmează:

2.2.1. Intranet VPN

Este un canal de comunicaţie 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 reţeaua internă a organizaţiei, iar conexiunile prin care se realizează sunt de obicei conexiuni permanente.

2.2.2. Extranet VPN

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

Extranet VPN realizează conexiunea între o corporaţie şi partenerii strategici de afaceri (distribuitori, furnizori, clienţi), pentru a le permite acestora accesul sigur la o parte a reţelei interne a companiei. Diferenţa faţă 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 distanţă care doreşte să acceseze reţeaua internă a companiei se conectează la un server local care e legat la reţeaua publică. Clientul VPN stabileşte legătura cu serverul VPN (care se află la sediul central al companiei). După stabilirea conexiunii, comunicaţia clientului cu reţeaua companiei peste reţeaua publică este la fel de sigură ca şi cum clientul s-ar afla în reţeaua locală internă.

O reţea virtuală poate fi stabilită la iniţiativa clientului sau a unui server de acces.

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

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

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

- Secure VPN
- Trusted VPN
- Hybrid VPN

Secure VPN

Reţelele Secure VPN au următoarele caracteristici:

- Trafic criptat şi autentificat.

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

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

Reţelele Secure VPN sunt utilizate pentru accesul remote, în cazul în care locaţia de unde se conectează utilizatorul nu poate fi controlată de administratorul de reţea.

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

Reţelele trusted VPN au următoarele caracteristici:

- Căile de comunicaţie 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

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

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

2.3. Componente VPN

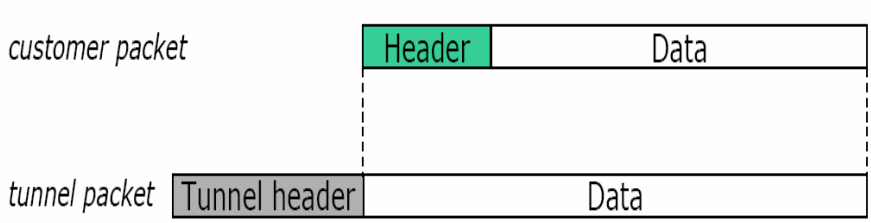
2.3.1. Tunneling

Conceptul de "tunneling" reprezintă transmiterea datelor în cadrul unei reţele publice astfel încât aceasta să nu realizeze faptul că transmisia (transportul de informaţii) e parte a unei reţele private.

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

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.

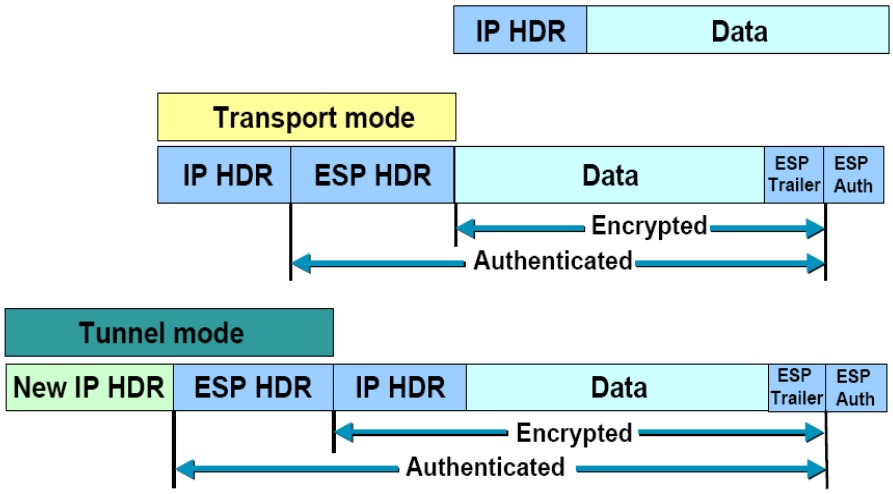


2.3.2 Protocoale folosite în VPN

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 iniţializate de către client încapsulând datele în pachete IP pentru transmiterea prin internet sau prin alte reţele 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 secvenţă în MAC-uri, prin folosirea unui mecanism de sumarizare a mesajului extins prin folosirea cheilor.

Protocolul SSL asigură o protecţie bună împotriva unor tipuri cunoscute de atacuri (incluzând atacuri de tip "man in the middle") şi realizează autentificarea bidirecţională (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 reţelei sesiunile PPP (Point-to-Point) prin crearea unor tunele iniţializate 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 configuraţiile 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 clienţii VPN pentru rutarea proprie;

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

GRE (Generic Route Encapsulation)

Este un protocol de încapsulare ce pune la dispoziţie un framework pentru crearea pachetului de transport; include informaţii despre tipul pachetului încapsulat şi informaţii 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 mulţi algoritmi de criptare

- DES - Data Encryption Standard – chei pe 56 de biţi
- 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 reţeaua privată şi internet; are ca scop monitorizarea parametrilor traficului din reţea şi protejarea reţelelor de accesul neautorizat.

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

La nivel pachet, firewall-ul verifică sursa şi destinaţia, iar firewall-urile la nivel aplicaţie se comportă ca un host între reţeaua organizaţiei şi internet.

După modul de funcţionare, firewall-urile pot fi:

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

Un firewall poate proteja reţeaua 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 iţi este permis”) şi accounting (“ceea ce faci”).

Prin autentificare se determină dacă emiţătorul este persoana autorizată şi dacă datele au fost redirecţionate 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 funcţie 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.
- Reţea VPN şi centru de management al politicilor.

3. Aplicaţii 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 reţea 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 reţelei virtuale

cele două routere vor crea un tunel VPN, folosind criptarea datelor. Deoarece reţeaua virtuală este conectată prin internet, nu conteaza distanţă 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 reţeaua unde este conectat, calculatorul utilizatorului mobil se comportă ca şi cum ar fi conectat direct la reţeaua unde este routerul VPN, cu toate facilităţile oferite de reţeaua securizată; deoarece VPN foloseşte legătura la internet, distanţa între echipamente nu are importanţă.

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

Programul pentru instalarea VPN funcţionează 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 căsuţa „Active” pentru clientul VPN nr. 1
6. Se salveaza setările (butonul „Save Settings”)

Instalarea programului pentru configurarea VPN:

Instalare de pe setup software:

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 instrucţiunile 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 reţelei, 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 informaţii.
5. Pentru terminarea conexiunii se selectează butonul „Disconnect”

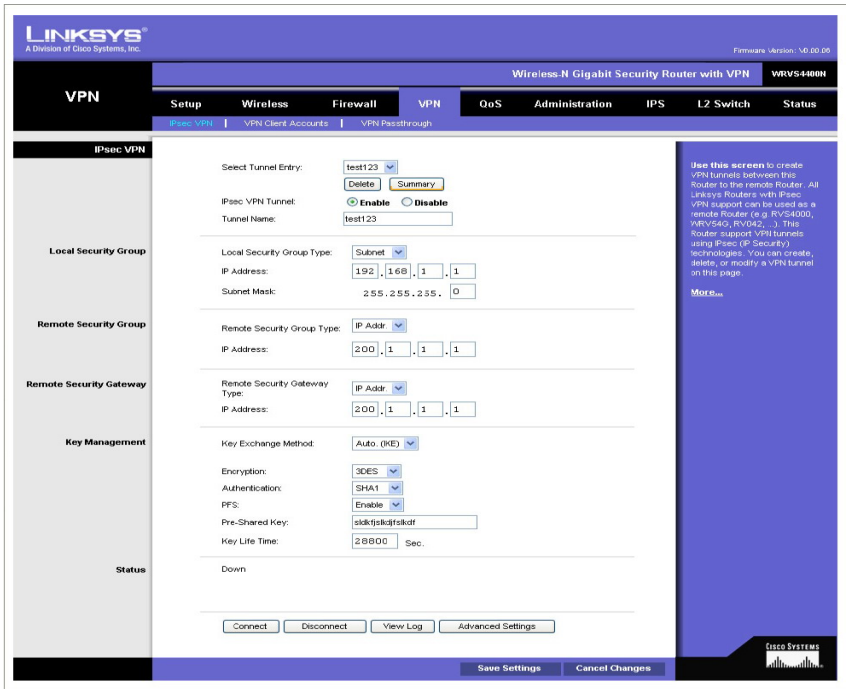
Configurarea unui tunel IPSec între două routere

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

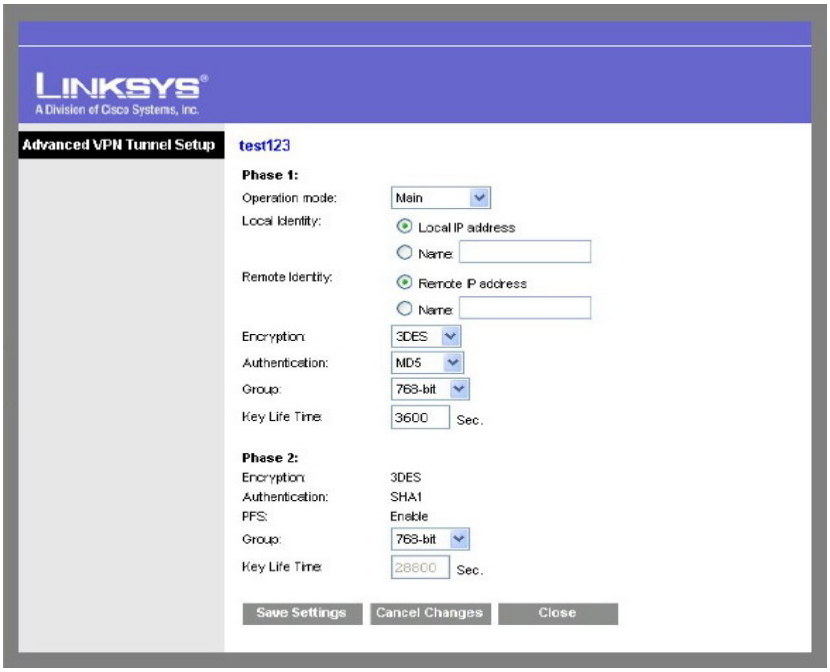
1. Se lansează un browser de pe staţia 1
2. Se introduce adresa IP a routerului 1 (implicit aceasta este 192.168.1.1)
3. Se introduce numele utilizator şi parola
4. Se selectează tab-ul „VPN”, apoi „IPSec VPN”
5. La setarea „VPN Tunnel” se selectează „Enabled”
6. Se dă un nume tunelului respectiv
7. 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 (subreţeaua 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 configuraţia (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 viaţă 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 staţiilor:

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 alţi 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

X. Securitatea în reţele wireless şi mobile

1. Obiective

Capitolul de faţă îşi propune prezentarea noţiunilor 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, WPA3 și Kerberos.

2. Consideraţii teoretice

2.1. Generalităţi

În reţelele 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 reţea chiar şi dintr-o maşină parcată pe stradă. Acest lucru nu înseamnă că nu trebuiesc folosite reţelele wireless, ci doar că trebuie să se ia masuri de precauţie de bază pentru a nu permite atacatorilor să ajungă la informaţii 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 identificat uşor de găsit (SSID-ul implicit este adesea asociat cu numele anumitor modele de routere și puncte de acces wireless).

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

- Folosirea criptării: dacă echipamentele suportă WPA3, acesta este cea mai bună opțiune. În caz contrar, WPA2-PSK cu criptare AES rămâne cea mai bună alegere disponibilă în majoritatea dispozitivelor actuale. WEP și WPA ar trebui evitat complet, deoarece nu mai oferă protecție reală împotriva atacurilor moderne.

- Restricţionarea traficului neesențial: multe reţele 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 mulţi 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 reţelele de tip 802.11. A fost introdus în 1997 şi a fost înlocuit de WPA, WPA2 şi WPA3. Metoda de autentificare este destul de slabă, motiv pentru care acest protocol a fost înlocuit. WEP are câteva probleme de securitate care pot compromite reţeaua wireless:

- Atacuri pasive pentru decriptarea traficului – se bazează pe analize statistice
- Atacuri active pentru introducerea de trafic nou de pe staţiile 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 mulţi utilizatori într-o reţea fără fir, partajarea aceleiaşi chei pentru perioade mari de timp este o mare vulnerabilitate a securităţii. 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 biţi care a fost ulterior mărită la 104 biţi.

2.1.2. WPA, WPA2 şi WPA3 (Wi-Fi Protected Access)

WPA este un protocol de securitate pentru reţelele 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 reţelele wireless. Dispozitivele care folosesc modul WPA2 nu mai sunt compatibile cu cele care folosesc WEP. În acest moment WPA3 este standardul recomandat pentru rețelele moderne datorită protecției sale superioare.

WPA3 este cel mai nou standard de securitate pentru rețelele Wi-Fi, lansat în 2018 de Wi-Fi Alliance. Acesta oferă protecție îmbunătățită împotriva atacurilor brute-force prin utilizarea protocolului SAE (Simultaneous Authentication of Equals) în locul metodei

tradiționale PSK (Pre-Shared Key). De asemenea, fiecare conexiune beneficiază de criptare individuală a datelor, sporind confidențialitatea utilizatorilor pe rețelele publice. WPA3 include și măsuri de securitate avansate pentru dispozitivele IoT, chiar și pentru cele cu resurse limitate. În varianta WPA3-Enterprise, standardul oferă criptare de 192 de biți, asigurând un nivel de securitate adecvat chiar și pentru utilizări guvernamentale.

2.1.3. Kerberos

Kerberos este o metodă sigură pentru autentificarea unei cereri de servicii într-o reţea 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 reţea. 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 distribuţie 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 distribuţiilor a cheilor pentru a obţine 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 reţeaua de atacuri. Se foloseşte în combinaţie cu firewall, liste de access bazate pe IP, NAPT (Network Address Port Translation) şi reţele virtuale (VPN) pentru a obţine o securitate cât mai mare. IPS funcţionează oferind detecţie 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 staţiile şi serverele care folosesc sisteme de operare diferite de atacuri în reţea.

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 reţea 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 definiţii 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 reţea care definesc permisiunile pe care utilizatorii, grupurile, procesele sau dispozitivele le au pentru a accesa reţeaua. 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 conţine 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 restricţiona traficul în funcţie de sensul specificat (in sau out) şi se aplică de regulă pe interfeţele routerelor.

2.1.6. Firewall (Stateful Packet Inspection)

În literatura de specialitate, în diverse standarde şi referinţe bibliografice au fost identificate o multitudine de definiţii ale conceptului. Câteva definiţii reprezentative ale conceptului de *firewall* sunt: un firewall este un agent care îngrădeşte traficul de reţea 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 reţele; un firewall creează o barieră prin care traficul, în fiecare direcţie, trebuie să treacă. O politică de securitate a firewall-ului va decide care tip de trafic este autorizat să treacă în fiecare direcţie.

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

- traficul unei reţele, indiferent de direcţie (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 aplicaţii proxy care vor interpreta cererile serviciilor, înainte de a le înainta;

- *controlul direcţiei* - determină direcţia pe care un anumit tip de serviciu are acces prin firewall;

- *controlul utilizatorilor* – controlează accesul utilizatorilor interni ai reţelei 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 aplicaţie şi filtre bazate pe inspecţia 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 recepţionate sau transmise. Setul de reguli se bazează pe verificarea informaţiilor conţinute în cadrul pachetelor şi aplicarea unei politici de tip discard/forward.

Proxy la nivel aplicaţie. Acest tip de firewall presupune existenţa unei entităţi intermediare, care va prelua cererile clienţilor, 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 clienţi, faţă de exteriorul reţelei. Astfel, staţiile clienţilor îşi vor păstra anominatul, deoarece toate cererile acestora vor fi prelucrate prin intermediul proxy-ului. Aceasta este o măsură pentru creşterea securităţii clienţilor reţelei. Un dezavantaj al acestui sistem de firewall îl reprezintă overheadul de procesare introdus pe fiecare conexiune

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

Pachetele ICMP sunt folosite pentru a raporta informaţii legate de starea reţelei. Însă pachetele ICMP pot fi utilizate de utilizatorii externi pentru a afla topologia reţelei 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 reţelei private, pentru a putea face o potrivire cu răspunsurile ICMP care vor sosi din exteriorul reţelei. Astfel, doar pachetele ICMP care au un corespondent în tabela ruterului vor fi permise.

3. Aplicaţii practice

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

Se va începe prin conectarea staţiei 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 interfaţa 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 iniţial 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 partea practică.

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 reţelei.

- 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, reţele 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 aplicaţii Internet specializate pe un singur port de reţea.
- Port range forwarding. Se floseşte pentru setarea serviciilor publice sau a altor aplicaţii specializate din reţea pe un anumit domeniu de porturi.

Configurarea detaliată a firewall-ului:

- Firewall SPI (Stateful packet inspection). La activarea acestei opţiuni routerul va efectua o inspecţie mai amănunţită a pachetelor asupra întregului trafic ce trece prin router şi va ignora toate pachetele care nu urmăresc comportamentul predefinit.
- Protecţie 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 reţelei.
- Configurare de la distanţă (Remote management). La activarea opţiunii routerul va permite configurarea sa de la distanţă (implicit opţiunea este dezactivată).

- HTTPS. Această opţiune se foloseşte la configurarea la distanţă. Prin activarea opţiunii, 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 opţiuni routerul va permite traficului multicast să intre în reţeaua locală dinspre Internet.

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

- Restricţionarea componentelor web (restrict web features). Se selectează componentele din paginile web care trebuie să fie restricţionate, 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, reţele virtuale pentru a obţine securitate maximă.

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

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

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

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

- În continuare se descriu parametrii folosiţi la configurarea IPS.

- Funcţionarea IPS (IPS Function). Se poate activa sau dezactiva funcţionarea IPS.

- Detectarea anormală (Abnormally detection). Se pot configura opţiuni 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 protecţie 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 aplicaţiilor de tip P2P sau de tip IM. Când utilizatorii descarcă fişiere folosind programe P2P lăţimea de bandă

a portului WAN este complet folosită. Se poate permite blocarea anumitor aplicaţii de tip P2P. Folosirea programelor de tip Instant Messsenger poate fi blocată.

Ecranul „Rapoarte (Report)" oferă informaţii despre starea reţelei, inclusiv traficul în reţea şi atacurile întâlnite, informaţiile sunt şi sub formă de diagrame sau tabele.

DMZ (Demilitarized Zone)

Ecranul DMZ permite ca o staţie locală să fie expusă spre Internet pentru folosirea serviciilor cu un anumit scop, cum ar fi videoconferinţe. Opţiunea „DMZ hosting" trimite traficul simultan spre toate porturile unei staţii 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 staţiei 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, WPA2 enterprise, WPA3, etc.
- Izolarea staţiilor din acelaşi SSID (Wireless isolation within SSID). Când opţiunea este dezactivată, calculatoarele wireless care sunt asociate cu acelaşi identificator de reţea (SSID) se pot vedea una pe cealaltă şi pot transfera fişiere între ele. Prin activarea opţiunii staţiile nu vor putea să se vadă una pe cealaltă.

WEP

Acest mod de securitate nu este recomandat datorită protecţiei mai puţin sigure. Utilizatorii sunt îndemnaţi să folosească WPA3.

- 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 biţi sau 128 biţi).
- Parolă (Passphrase). Se foloseşte când se doreşte generarea cheilor WEP folosind o parolă de criptare.

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 clienţilor (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

Funcţionează 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 staţii care folosesc WPA Enterprise sau staţii care folosesc WPA2 Enterprise. Routerul va alege automat algoritmul de criptare folosit de fiecare staţie. Semnificaţia parametrilor este în general aceeaşi ca şi în cazul algoritmilor precedenţi.

WPA3

- Utilizează SAE (Simultaneous Authentication of Equals) pentru autentificare mai sigură și asigură protecție împotriva atacurilor brute-force

- Protejează datele chiar și pe rețelele Wi-Fi deschise, prin criptare individualizată pe rețele publice.
- Utilizează criptare 192-bit pentru protecție avansată.
- Remediază vulnerabilitățile din WPA2, oferind protecție împotriva atacurilor KRACK.
- Suportă Wi-Fi Easy Connect (conectare prin cod QR), pentru configurare simplificată pentru dispozitive IoT

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 restricţiona traficul prin router atât spre exterior cât şi spre interior. Există două metode de restricţionare a accesului: se pot bloca diferite tipuri de trafic conform definiţiilor 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 precauţie. Există două liste de acces care nu pot fi şterse. Prima regulă este să permită tot traficul din reţeaua 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 restricţionare a traficului, tot traficul va fi permis prin router în ambele direcţii.

Regula va fi activată când se bifează butonul de activare (Enable) şi când se vor potrivi data şi timpul menţionate. Dacă oricare din aceste condiţii 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 faţă 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 căsuţei „enable”.
- Acţiunea (Action). Se defineşte efectul regulii asupra traficului. Poate avea acţiunea de permitere (allow) sau de interzicere (deny) a traficului. Dacă regula se potriveşte iar acţiunea este „allow” pachetul va fi trimis mai departe. Dacă regula se potriveşte iar acţiunea 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. Interfaţa grafică pentru definirea serviciilor utilizator poate fi accesată din ecranul „Regulă nouă (New rule)” cu butonul „Gestionarea serviciilor (Service management)”.

- Interfaţa sursă (Source interface). Se poate selecta interfaţa 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 reţea întreagă (prin specificarea adresei de reţea şi a măştii) sau chiar valoarea „any” specificând orice adresă IP.

- Destinaţia (Destination). Se selectează adresa IP destinaţie 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 acţiune „allow” sau „deny” şi se vor completa următorii parametrii suplimentari.

- Log. La fiecare potrivire a unui pachet cu o regulă se va menţiona 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 conţine patru componente: trebuie definită staţia (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 staţiilor (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 funcţionalitatea componenteleor de securitate ale routerului.

- Se vor testa diverse moduri de securitate în reţelele wireless;
- Se va configura firewall-ul astfel încât să restricţioneze controale de tip activex şi java.
- Se vor implementa liste de acces pentru a verifica funcţionalitatea lor prin interzicerea traficului de la anumite staţii sau spre anumite staţii 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 staţiile specificate).
- Se va configura prin politici de acces la Internet accesul doar a anumitor staţii 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

XI. Programarea dispozitivelor mobile: Comunicarea în reţea

1. Obiective

Obiectivele acestui capitol cuprind prezentarea fundamentelor teoretice referitoare la programarea aplicaţiilor care comunică în reţea utilizând tehnologia Bluetooth, socketuri şi serviciile web. Obiectivele prezentate vor fi aplicate în capitolul următor prin exerciții practice care vor permite implementarea mai multor metode de comunicare în rețea.

2. Consideraţii teoretice

Conform celor mai recente statistici [1], 70% din populația globală utilizează în prezent un telefon mobil, ceea ce indică o penetrare semnificativă a acestei tehnologii în viața cotidiană. În iulie 2024, numărul utilizatorilor „unici” de telefoane mobile a atins pragul impresionant de 5,68 miliarde, reflectând o creștere constantă a conectivității la nivel mondial. Creşterea numărului de posesori de dispozitive mobile conectate la internet şi apariţia standardelor de mare viteză (4G și 5G) a condus la explozia aplicaţiilor de tip mobil și, în special, a celor de streaming, social media, e-commerce și jocuri online.. Marea majoritate a utilizatorilor de internet la nivel global – 95,9% – utilizează un telefon mobil pentru a accesa internetul, fie și doar ocazional, conform [1]. În prezent, telefoanele mobile sunt responsabile pentru 56,9% din timpul petrecut online și generează 60% din traficul web mondial.

Tehnologia Bluetooth s-a afirmat ca standard dominant în industrie pentru comunicarea pe distanțe scurte între dispozitive mobile.. Pentru comunicarea în Internet, două tehnici sunt extensiv utilizate: socketurile şi serviciile web.

2.1. Comunicarea în reţea utilizând tehnologia Bluetooth

Datorită capacității sale de a oferi conexiuni stabile și eficiente din punct de vedere energetic, Bluetooth a devenit alegerea preferată pentru o gamă largă de aplicații, inclusiv transferul de date între smartphone-uri, conectarea căștilor wireless, a dispozitivelor portabile (wearables), a sistemelor audio și a accesoriilor inteligente. Bluetooth este o tehnologie de cost şi putere redusă bazată tehnologia RF pentru comunicaţii pe distanţe scurte, reprezentând o alternativă la conexiunea cablată dintre diferite dispozitive electronice [2].

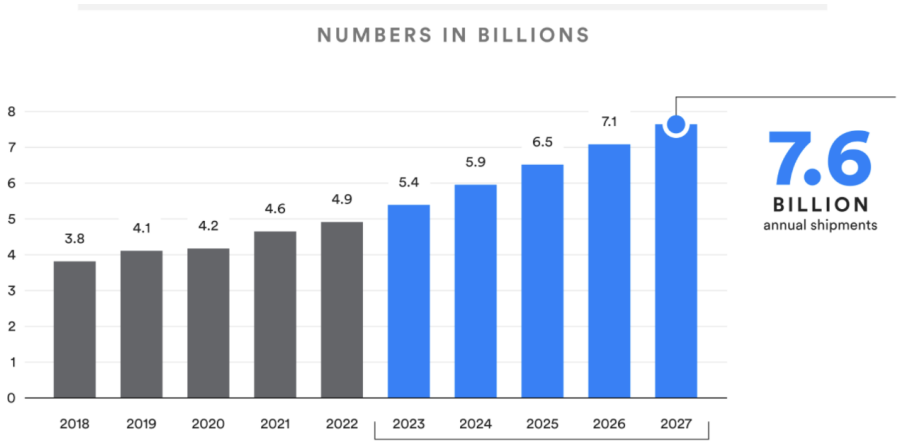


Figura 1. Numărul total de dispozitive Bluetooth livrate [3]

Bluetooth este o tehnologia wireless cu o rată de creştere rapidă (fig. 1), estimându-se că numărul dispozitivelor cu capabilităţi Bluetooth va depași 7 miliarde de unităţi.

Principalele tehnologii Bluetooth utilizate astăzi sunt Bluetooth Classic, folosit pentru aplicații cu transmisie continuă de date, și Bluetooth Low Energy (BLE), optimizat pentru un consum redus de energie, ideal pentru dispozitive portabile și IoT.

Tabelul de mai jos prezintă evoluţia şi versiunile tehnologiei Bluetooth:

Versiune	Rata de date
Bluetooth v1	până la 1 Mbps
Bluetooth v2 EDR (Enhanced Data Rate)	până la 3 Mbps
Bluetooth v3 HS (High Speed)	până la 24 Mbpsbazat pe 802.11
Bluetooth v4 – 4.0,4.1,4.2 (Enhanced Data Rate și Low Energy)	EDR până la 3 Mbps LE până la 1 Mbps
Bluetooth v5 - 5.0, 5.1, 5.2, 5.3, 5.4	EDR până la 50 Mbps LE până la 2 Mbps

Tabelul 1. Versiuni Bluetooth

Bluetooth Clasic sau Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) a fost proiectat pentru comunicare de tip punct la punct pentru transfer de date și audio streaming, pe distanțe reduse (0-10m).

Bluetooth low energy (BLE) a fost gândit ca un standard radio care să ofere o soluție optimizată pentru consum redus, costuri reduse, lățime de bandă redusă și complexitate redusă. A fost introdus, pentru prima dată, cu versiunea 4.0 a Bluetooth Clasic. BLE permite comunicare de tip punct la punct, broadcast și mesh pentru transfer de date, audio streaming, comunicare în rețea (ex. IoT) sau localizare. [4]

Cele două specificații (BR/EDR și BLE) nu sunt direct compatibile, însă, noile tipuri de dispozitive pot utiliza ambele specificații (dual mode devices).

Tabelul de mai jos oferă o vedere sumarizată a caracteristicilor celor două specificații:

	BR/EDR	BLE
Frecvență	Banda 2.4GHz ISM	Banda 2.4GHz ISM
Canale	79 canale	40 canale
Rata de date	1 Mbps; 2-3 Mbps	1 Mbps

Tabelul 2. Bluetooth clasic vs. low energy

Cu toate că există asemănări cu modelul TCP/IP, Bluetooth folosește propria sa stivă de protocoale. În [2] este descrisă arhitectura de bază Bluetooth clasică şi principalele caracteristici ale nivelurilor care alcătuiesc tehnologia Bluetooth (fig. 2).

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

- tehnică Frequency Hop Spread Spectrum (FHSS)
- modulaţie Gaussian shaped binary FSK (în mod EDR - π/4-DQPSK şi 8DPSK)
- distanţe între 10m şi 100 m
- conexiune ad-hoc

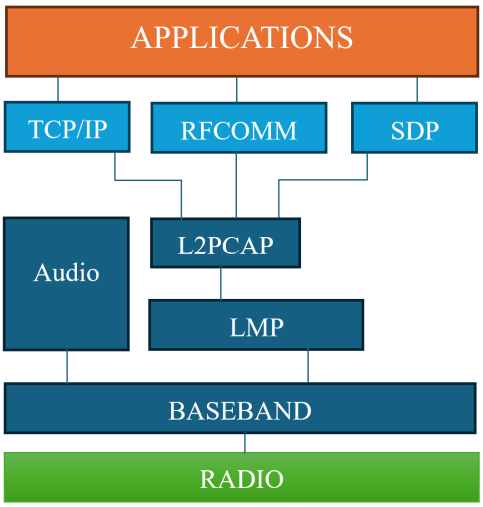


Figura 2. Arhitectura Bluetooth BR/EDR [2]

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 iniţiază conexiunea va funcţiona în mod master, celelalte dispozitive care vor participa la conexiune fiind în mod slaves. Mai multe piconet-uri pot forma o reţea denumită scatternet (fig. 3).

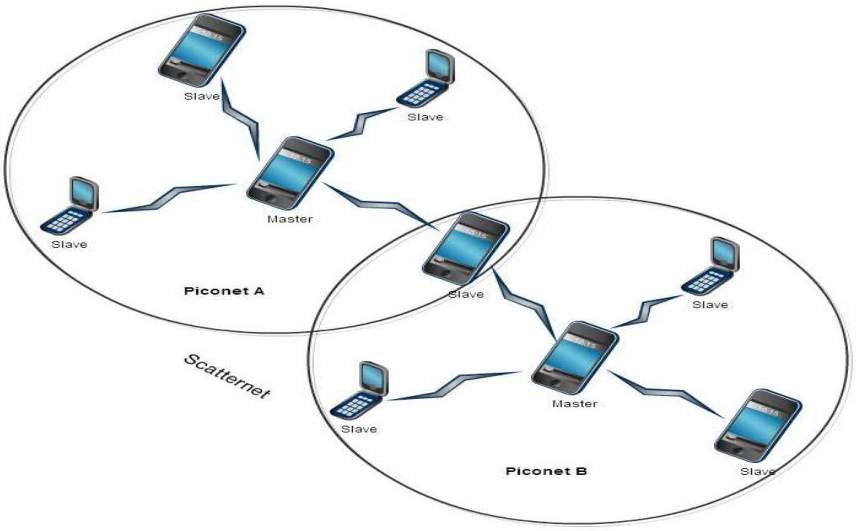


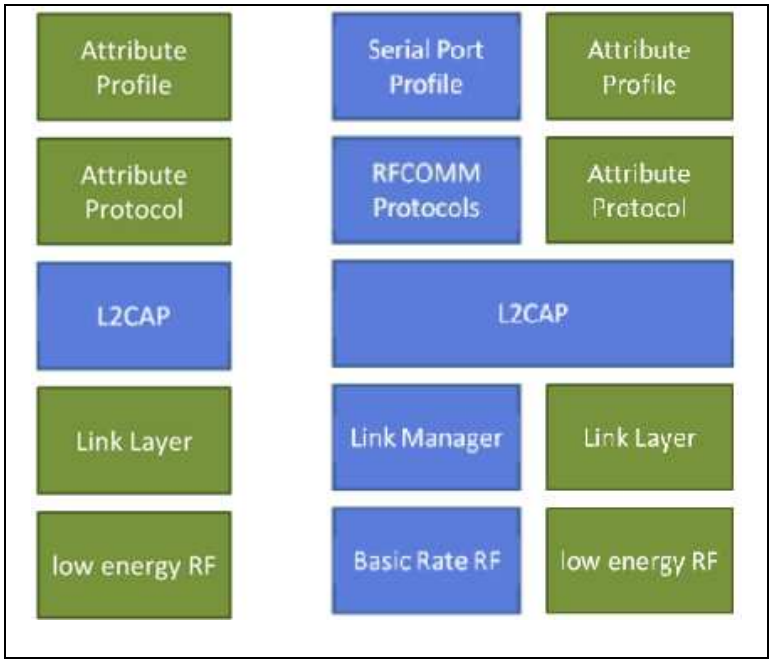
Figura 3. Tipuri de reţele Bluetooth

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]

Una dintre principalele caracteristici ale BLE este consumul extrem de eficient de energie. Stiva de protocoale Bluetooth Low Energy (BLE) este prezentată în [6]. Stiva BLE este împărțită în trei componente principale: nivelul Controlor (Controller), nivelul Gazdă (Host) și nivelul Aplicație (Application). Separarea nivelurilor Control și Gazdă, precum și existența unei interfețe pentru comunicarea între cele două niveluri (Host Controller Interface - HCI) permit implementarea funcționalităților lor în componente fizice distincte.

Nivelul Controller are rol în gestionarea comunicării dintre dispozitive. Subnivelul Physical Layer este responsabil pentru transmiterea și recepționarea datelor prin mediul fizic, utilizând nivelul radio. Subnivelul Link Layer gestionează logica de control a conexiunii dintre două dispozitive BLE, precum și securitatea transmisiei de date. Subnivelul Isochronous Adaptation Layer permite dispozitivelor să gestioneze fluxuri de date sensibile la latență și care au nevoie de sincronizare precisă.

Interfața HCI permite schimbul de comenzi, date și evenimente, prin comunicare bidirecțională între nivelurile Controller și Host. La nivelul Host sunt specificate o serie de protocoale. Logical Link Control and Adaptation Protocol (L2CAP) funcționează ca un multiplexor de protocol, direcționând corect protocoalele către componentele corespunzătoare și efectuând segmentarea și reasamblarea PDU/SDU între straturile adiacente. Security Manager Protocol (SMP) în BLE are rolul de a gestiona autentificarea, asocierea și criptarea între dispozitive, asigurând o conexiune securizată și protejând datele transmise împotriva accesului neautorizat.

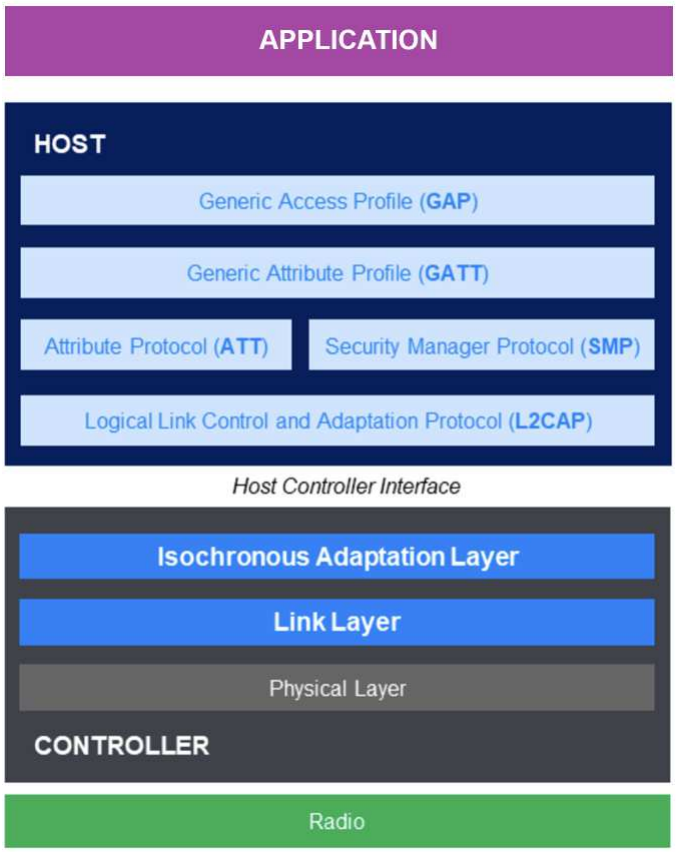


Figura 5. Stiva de protocoale BLE [7]

Attribute Protocol (ATT) definește modul în care datele sunt organizate, accesate și schimbate între dispozitive, utilizând un model client-server bazat pe attribute. Generic Attribute Profile (GATT) definește tipuri de date la nivel înalt (servicii, caracteristici și descriptori), în termeni de atribute din tabelul de atribute, precum și proceduri de nivel superior pentru utilizarea ATT în lucrul cu tabelul de atribute. Generic Access Profile (GAP) definește modul în care dispozitivele BLE comunică între ele atunci când se află într-o stare neconectată, precum și modurile și nivelurile de securitate.

2.2. Comunicarea în reţea utilizând socketuri

Un socket reprezintă un capăt de comunicaţie a unei legături de comunicaţie bidirecţională între două programe care rulează în reţea [8].

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

Adresa IP sursă	**Adresa IP destinaţie**	**Port sursă**	**Port destinaţie**	**Protocol**

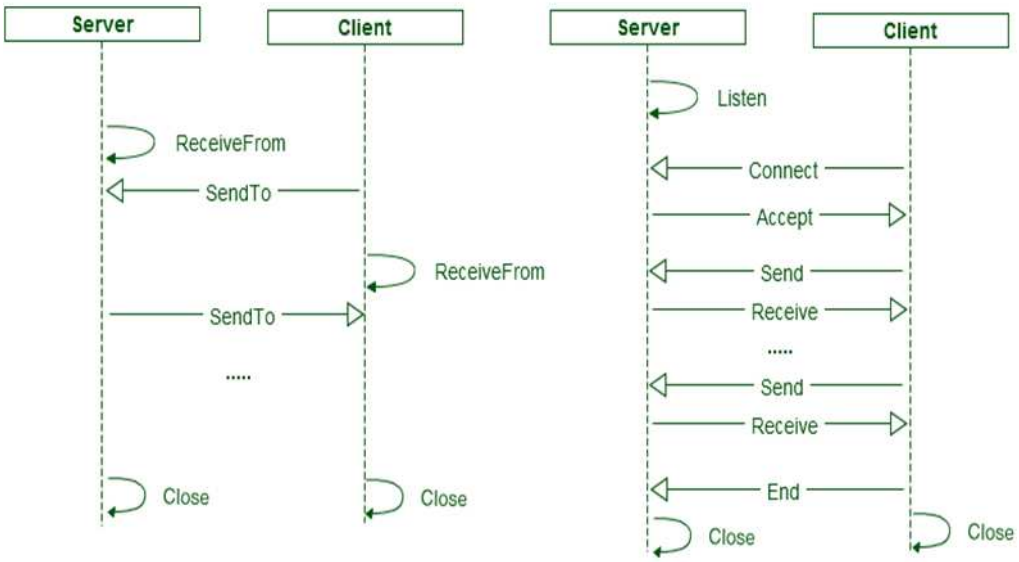
Un număr de porturi - well-known ports (porturi bine cunoscute), sunt rezervate pentru servicii de reţea specifice (FTP – 21, TELNET – 23, DNS – 53, HTTP – 80 etc). Lista

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 reţea pot fi de mai multe tipuri, în funcţie de protocolul de nivel transport utilizat. Două tipuri de socketuri de reţea 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 aplicaţiile 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 aplicaţiile 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 comunicaţiei dintre un client şi un server utilizând socket-uri de reţea de tip datagramă, respectiv stream.

Operaţie	Comunicare Socket UDP	
	Server	Client
Socket	Creare socket server	Creare socket client
SendTo/ReceiveFrom	Serverul poate recepţiona/transmite date (Protocolul UDP nu garantează transmiterea sigura si in ordine a datelor)	Clientul poate transmite/recepţiona 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 (opţional)	Clientul închidere socketul

Tabelul 2. Comunicarea în reţea utilizând socket-uri UDP

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

Tabelul 3. Comunicarea în reţea utilizând socket-uri TCP

2.3. Comunicarea în reţea utilizând servicii web

2.3.1. Arhitectura SOAP

Arhitectura orientată pe servicii (Service-Oriented Architecture – SOA) reprezintă un stil arhitectural pentru construirea de aplicaţii software care folosesc serviciile disponibile într-o reţea, cum ar fi web. Un serviciu reprezintă o implementare a unei funcţionalităţi business bine definită, iar astfel de servicii pot fi consumate de către clienţi în diverse aplicaţii sau procese business. [9].

O caracteristică de bază a SOA este separarea interfeţei 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 existenţa 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.

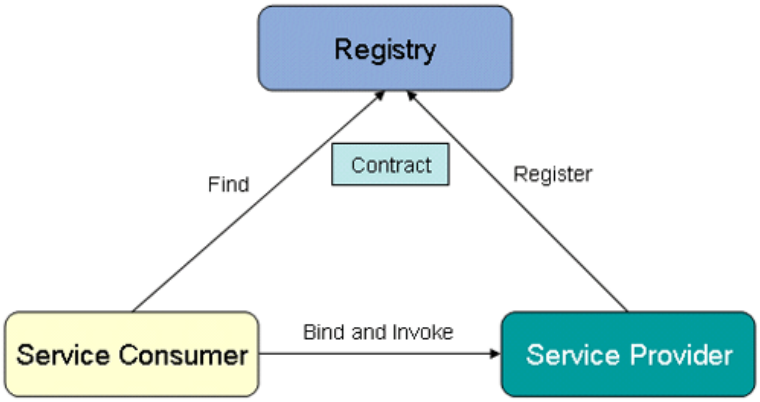


Figura 6. Paradigma *find-bind-execute* [9]

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 aplicaţiilor să realizeze schimbul de informaţii 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 interfeţe 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 [10].

Implementarea unor servicii web REST urmărește 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).

SOAP	REST
Un contract formal trebuie să fie stabilit pentru a descrie interfaţa serviciilor web oferite	Serviciile web sunt fără stare (stateless)
Arhitectura trebuie să abordeze cerinţe nefuncţionale complexe (adresare, securitate etc)	O infrastructură cache poate fi utilizată pentru creşterea performanţelor
Arhitectura abordează prelucrare şi invocare asincronă	Producătorul de servicii şi consumator de servicii trebuie să aibă o înţelegere reciprocă asupra contextul şi conţinutul 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

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

Bibliografie

[1] Digital Around the World, https://datareportal.com/global-digital-overview
[2] H. Wang, Overview of Bluetooth Technology, http://www.m2mgsm.com/download/BT/docs/general/Bluetooth_Overview.pdf
[3] 2023 Bluetooth Market Update https://www.bluetooth.com/2023-market-update/
[4] Bluetooth Technology Overview, https://www.bluetooth.com/learn-about-bluetooth/tech-overview/
[5] R. Heydon, Training videos – Architecture, https://www.bluetooth.org/OTV/4-Architecture/
[6] D. H Morais, 5G NR, Wi-Fi 6, and Bluetooth LE 5: A Primer on Smartphone Wireless Technologies, Springer, 2023rd edition, 2023
[7] The Bluetooth Low Energy Primer, https://www.bluetooth.com/bluetooth-resources/the-bluetooth-low-energy-primer/
[8] All about sockets, http://docs.oracle.com/javase/tutorial/networking/sockets/definition.html
[9] SOAP Tutorial, http://www.w3schools.com/soap/default.asp
[10] Rodriguez, A.: Restful web services: the basics, http://www.gregbulla.com/TechStuff/Docs/ws-restful-pdf.pdf

XII. Programarea dispozitivelor mobile: Android

1. Obiective

Obiectivele acestui capitol cuprind prezentarea platformei, a arhitecturii şi a fundamentelor necesare pentru programarea dispozitivelor mobile Android și a aplicațiilor de comunicare în rețea utilizând sistemul de operare Android.

2. Considerații teoretice

Sistemul Android pune la dispoziția dezvoltatorilor o platformă open-source și un mediu de dezvoltare pentru aplicații specifice dispozitivelor mobile, televizoarelor, brățări fitness si ceasuri inteligente.

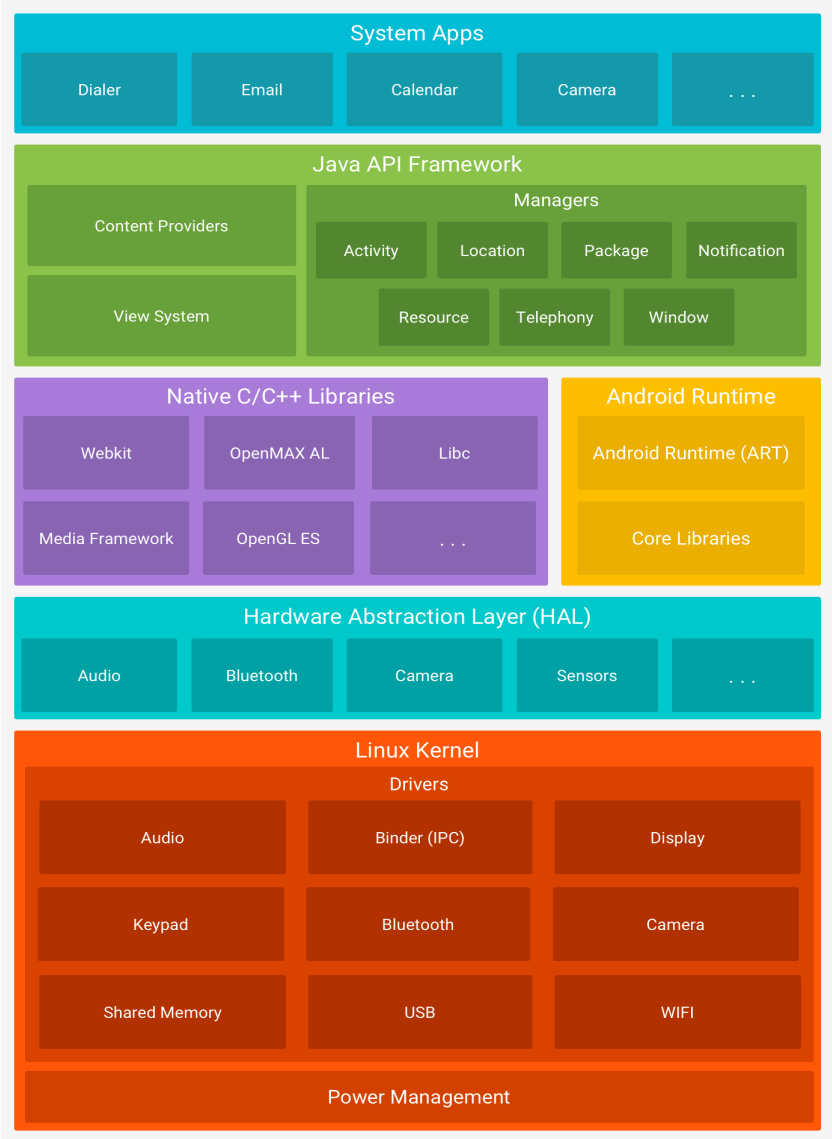


Figura 1. Stiva software Android [2]

Dispozitivele Android suportă diverse tehnologii de comunicare fără fir, incluzând rețele mobile (3G, 4G, 5G) pentru conectivitate rapidă, VPN pentru rețele private securizate și Wi-Fi cu funcții precum scanarea rețelelor, conectarea directă prin Wi-Fi Direct (P2P) sau Wi-Fi Aware (NAN), precum și măsurarea distanței prin Wi-Fi RTT. Bluetooth permite conexiuni tradiționale prin Bluetooth Classic, transfer eficient de date cu Bluetooth Low Energy (BLE) și sunet de înaltă calitate prin BLE Audio. NFC facilitează schimbul rapid de date și plățile contactless, iar UWB oferă localizare precisă între dispozitive. Android include suport pentru gestionarea apelurilor prin rețele mobile și eSIM, precum și conectivitate prin USB pentru utilizarea accesoriilor și a perifericelor. Aceste tehnologii permit o conectivitate flexibilă și eficientă pentru utilizatori și dezvoltatori. Documentatia oficiala a Android ofera o serie de API-uri pentru a putea folosi aceste capabilitati in aplicatii [1].

Stiva software a sistemului de operare Android (fig. 1) conţine următoarele niveluri [2]:

- Nucleul Linux (Linux Kernel): fundamentul platformei Android, care gestionează interacțiunea cu hardware-ul, securitatea, memoria, procesele și rețeaua.
- Stratul de abstractizare a hardware-ului (Hardware Abstraction Layer - HAL): interfețe standard pentru ca API-urile Android să poată accesa componente hardware precum camera, Bluetooth sau senzorii.
- Biblioteci native C/C++ (Native C/C++ libraries): includ componente esențiale scrise în C/C++, precum OpenGL ES pentru grafică, folosite de sistem și accesibile prin API-uri Java.
- Android Runtime (ART): motorul de execuție al aplicațiilor, care optimizează performanța prin compilare Ahead-of-Time (AOT) și Just-in-Time (JIT), gestionează memoria și suportă depanarea avansată.
- Cadrul API Java (Java API framework): instrumente esențiale pentru dezvoltarea aplicațiilor, inclusiv UI, gestionarea resurselor, notificări și interacțiunea între aplicații
- Aplicațiile de system (System Apps): set de aplicații esențiale (e-mail, mesagerie, calendar etc.), care funcționează atât pentru utilizatori, cât și ca servicii reutilizabile de către alte aplicații

Android Studio [3] este IDE-ul oficial pentru dezvoltarea aplicațiilor Android, oferind instrumente avansate bazate pe IntelliJ IDEA pentru a crește productivitatea dezvoltatorilor.

Aplicațiile Android pot fi dezvoltate în Kotlin, Java și C++. Android SDK compilează codul și resursele într-un APK sau App Bundle, utilizate pentru instalarea și rularea aplicației pe dispozitivele Android [4]. Android Studio utilizează Gradle ca sistem de compilare, iar Android Gradle Plugin (AGP) oferă funcționalități dedicate dezvoltării aplicațiilor Android. Tipurile de aplicaţii care extind funcţionalităţile de bază Android sunt aplicaţiile preinstalate şi aplicaţiile dezvoltate de către utilizatori (acestea se pot descărca şi instala de pe site-ul Google Play).

Fluxul pentru dezvoltarea unei aplicaţii Android urmăreşte următorii paşi prezentaţi în figura 2 [5]:

1. Setarea mediului de lucru – instalarea Android Studio și crearea unui nou proiect; utilizatorii pot parcurge un ghid pentru a învăța noțiuni fundamentale de dezvoltare Android.

2. Scrierea codului aplicației – utilizarea instrumentelor din Android Studio pentru scrierea codului, proiectarea interfeței și gestionarea resurselor pentru diverse dispozitive.
3. Compilare și rulare – construirea unui APK pentru testare pe emulator sau dispozitiv real; în această etapă, se pot crea variante de build și se poate optimiza dimensiunea aplicației.
4. Depanare, testare și optimizare – eliminarea erorilor, testarea performanței și analizarea utilizării resurselor (CPU, memorie, rețea) pentru optimizarea aplicației.
5. Publicare – crearea unui Android App Bundle, semnarea aplicației și pregătirea acesteia pentru publicare în Google Play Store.

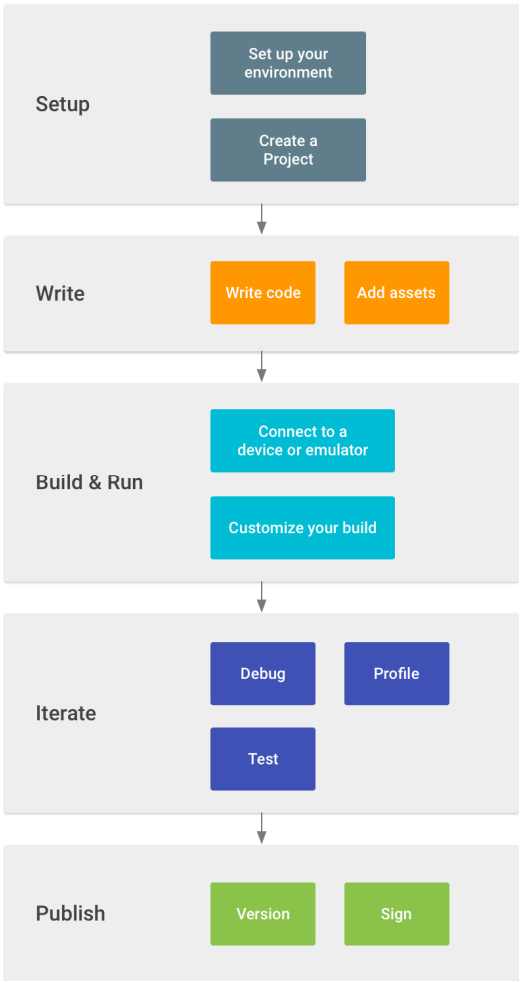


Figura 2. Fluxul de lucru pentru dezvoltarea unei aplicații Android [5]

Pentru dezvoltarea aplicațiilor Android este necesară instalarea Android Studio de pe site-ul oficial [6], ilustrat în imaginea de mai jos (fig. 3).

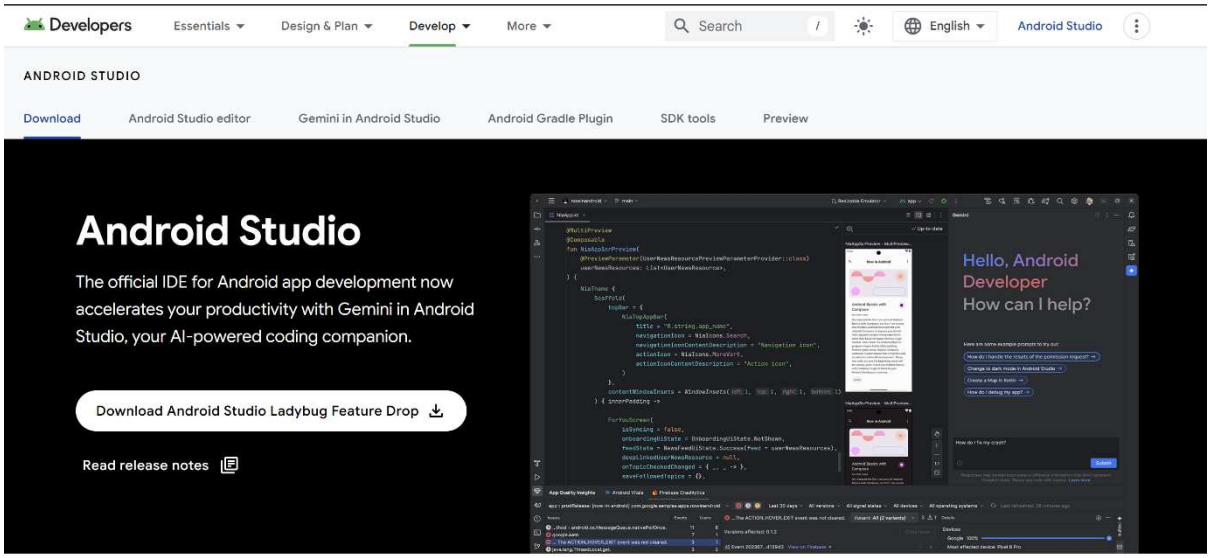


Figura 3. Pagina pentru descărcarea Android Studio [6]

3. Crearea aplicaţiilor Android

Android este un sistem de operare mobil care permite dezvoltarea aplicațiilor prin componente esențiale (fig. 4), fiecare având un rol specific. Aceste componente asigură structura aplicațiilor și facilitează crearea unor aplicații interactive și eficiente. Cele patru componente ale unei aplicații sunt [4]:

- Activități (Activities) – reprezintă interfața utilizatorului și fiecare ecran al aplicației (de exemplu: o pagină de autentificare sau un ecran principal);
- Servicii (Services) – rulează în fundal fără interfață vizuală, fiind utilizate pentru procese de lungă durată, cum ar fi redarea muzicii sau sincronizarea datelor;
- Receptori de difuzare (Broadcast Receivers) – detectează și răspund la evenimente de sistem în afara fluxului obișnuit al utilizatorului, precum schimbarea conexiunii la internet sau primirea unui SMS;
- Furnizori de conținut (Content Providers) – se ocupă cu gestionarea și partajarea datelor între aplicații (de exemplu: accesarea contactelor sau a fișierelor media);

Figura 4. Componentele unei aplicații Android

Aplicațiile Android pot fi testate fie pe un dispozitiv mobil inteligent, fie pe emulatorul Android, care vine instalat automat cu Android Studio. Emulatorul permite testarea pe diverse dispozitive și versiuni de API Android, fără a necesita dispozitive fizice.

Este important de specificat faptul că fiecare aplicație Android rulează într-un sandbox de securitate și are acces doar la componentele necesare, conform principiului privilegiului minim. Astfel, aplicațiile nu pot accesa părți ale sistemului fără permisiune, asigurând un mediu sigur. Fiecare aplicație rulează într-un proces separat, cu permisiuni care împiedică accesul direct la alte aplicații.

Totuși, sistemul Android poate activa componente din alte aplicații dacă i se trimite un *Intent* care specifică această intenție. Intent în Android este un mecanism de mesagerie folosit pentru a comunica între componente ale unei aplicații sau între aplicații. Există Intenturi Explicite, care lansează o componentă specifică, și Intenturi Implicite, care solicită o acțiune fără a specifica exact componenta. Un Intent conține informații precum acțiunea dorită, datele asociate, categorii, extra-uri și flag-uri. Intenturile sunt folosite pentru a deschide activități, a porni servicii sau a trimite broadcast-uri. Exemple comune includ deschiderea unui URL, trimiterea unui email sau partajarea unui mesaj.

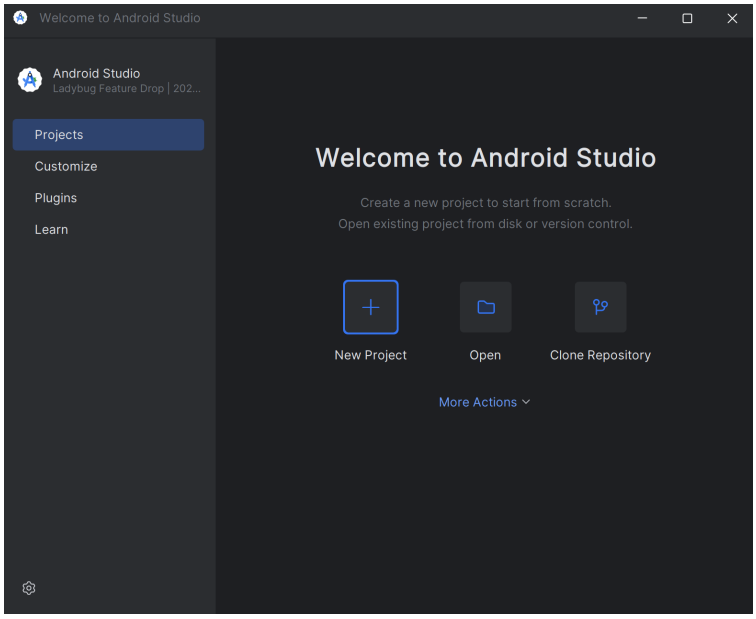


Figura 5. Crearea unui proiect nou Android

Pentru creare unei simple aplicații, utilizând Android Studio, se vor urma pașii de mai jos:

1. Pentru a crea un proiect nou (fig. 5), selectați opțiunea *New Project* în ecranul de bun venit al Android Studio sau din meniul principal File > New > New Project from the main menu. În ecranul *New Project*, puteți alege tipul de proiect (fig.6) din diverse categorii de dispozitive afișate în panoul *Templates*. Android Studio va include cod exemplu și resurse pentru a facilita dezvoltarea aplicației. După selecție, faceți clic pe *Next*.

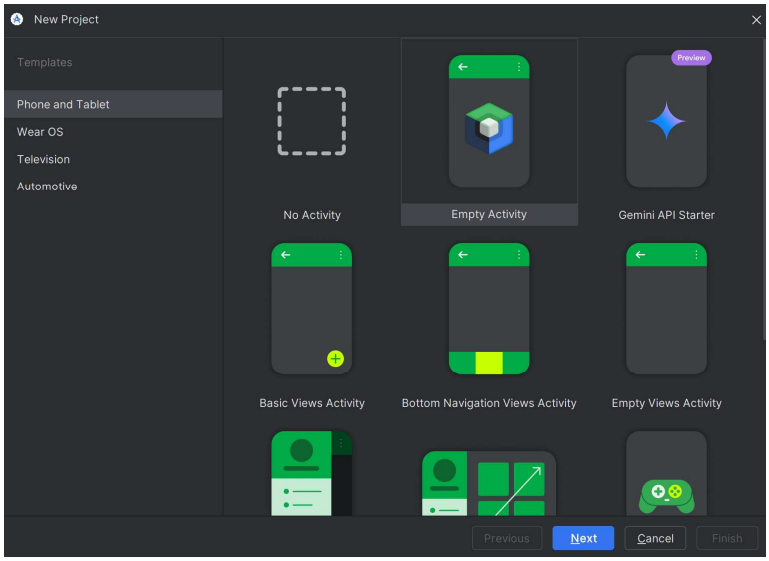


Figura 6. Alegerea tipului de proiect Android

2. Specificați numele proiectului (*Name*) și numele pachetului (*Package name*), care va servi drept spațiu de nume pentru resurse și ID-ul aplicației pentru publicare. De asemenea, specificați locația unde doriți să stocați proiectul local (*Save location*) și selectați nivelul minim al API-ului (*Minimum SDK*), echilibrând compatibilitatea cu dispozitivele mai vechi și accesul la funcționalități moderne ale Android (opțiunea *Help me choose* vă oferă mai multe informații). Apoi apăsați butonul *Finish* (fig. 7).

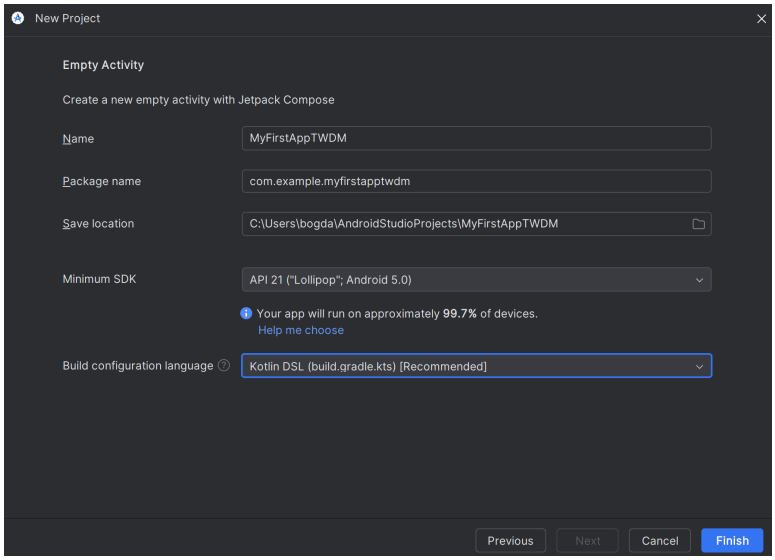


Figura 7. Configurația proiectului Android

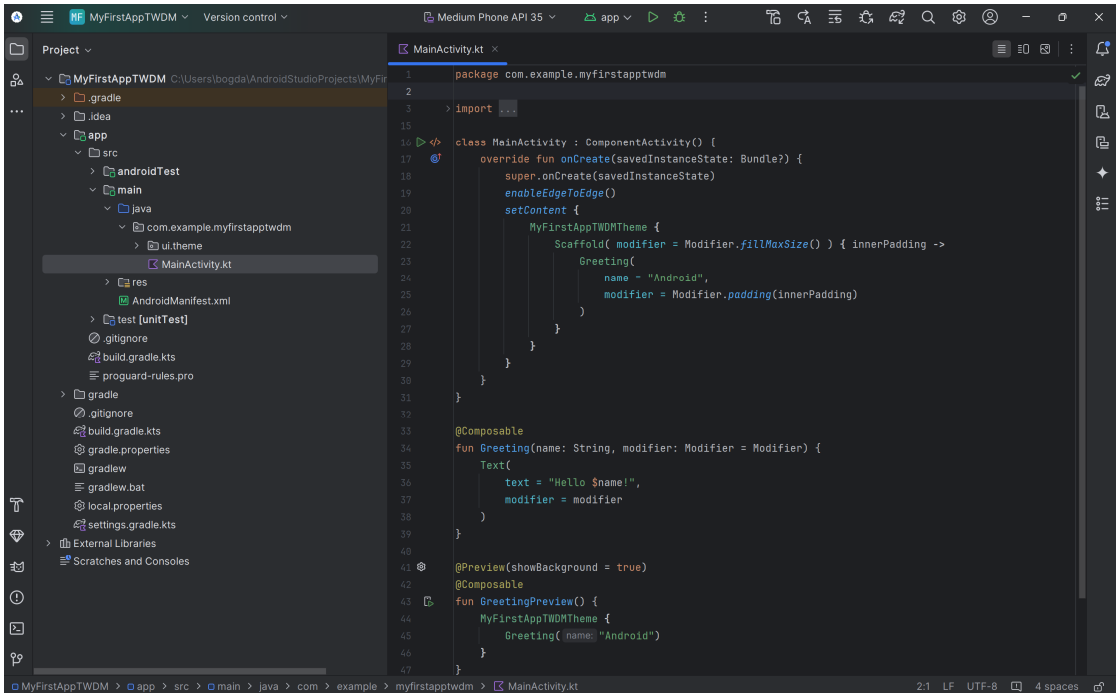


Figura 8. Structura unei aplicații Android

Fișierele unei aplicații Android sunt organizate în mai multe grupuri (fig.8):

- Codul sursă (/src/main/java/) – conține clasele aplicației scrise în Java/Kotlin.
- Resursele aplicației (/res/) – include fișiere XML pentru interfață, imagini, pictograme și valori statice.
- Manifestul (AndroidManifest.xml) – definește permisiunile, activitățile și componentele aplicației.
- Fișiere de compilare (build.gradle, gradle.properties) – conțin configurațiile pentru Gradle.
- Fișiere generate automat (/build/, /gen/) – includ artefactele de compilare și fișiere auxiliare.
- Biblioteci externe (/libs/) – conțin librării .jar sau .aar.
- Fișiere de resurse suplimentare (/assets/, /raw/) – stochează fonturi, baze de date și fișiere media.
- Fișiere de stocare internă (/data/data/com.numeaplicatie/) – conțin baze de date SQLite și setări ale aplicației.

Rularea primei aplicații utilizând emulatorul

Pentru a rula o aplicație Android pe un emulator în Android Studio, urmați acești pași:

- se accesează *Device Manager* și creează sau selectează un emulator cu configurația dorită (fig. 9).

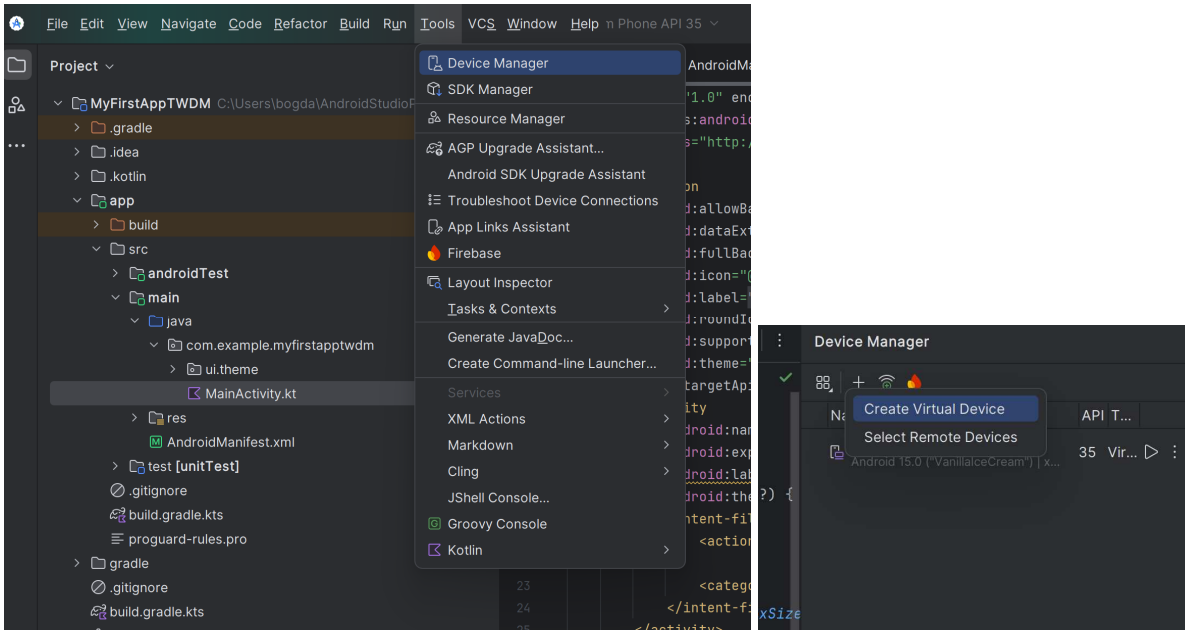


Figura 9. Alegerea emulatorului

- se rulează aplicația apăsând butonul Run (triunghi verde) sau se folosește combinația de taste Shift + F10.
- Se testează aplicația interacționând cu emulatorul (fig. 10).

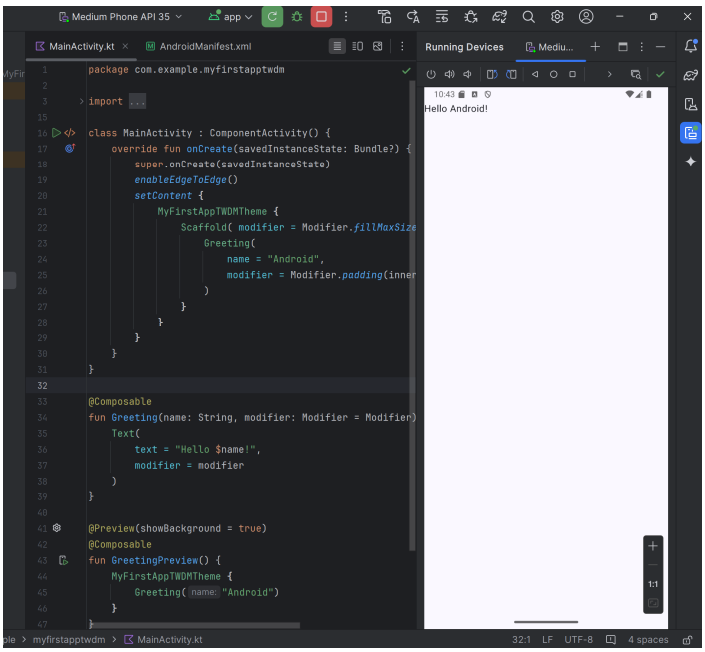


Figura 10. Exemplu de rulare pe emulator

Analizând structura aplicație vom identifica principalele fișiere și directoare, precum și conceptele de activitate, manifest și fragment.

Fișierele de cod sursă Kotlin ale aplicației, controlează logica, sunt definite în directorul app/src/main/java/com/example/myfirstapptwdm/, unde MainActivity.kt este punctul de

intrare. Manifestul AndroidManifest.xml care gestionează activitățile și permisiunile este localizat în directorul app/src/main/. Fișiere XML pentru definirea interfeței utilizatorului se regăsesc în directorul app/src/main/res/layout/. Resursele statice precum string-uri, culori, stiluri, etc se regăsesc în directorul app/src/main/res/values/.

O *Activitate* (fig. 11) este o componentă fundamentală a unei aplicații Android care reprezintă un ecran al interfeței utilizatorului. Fiecare activitate oferă o interacțiune distinctă și este gestionată de sistem în ciclul său de viață.

```
class MainActivity : ComponentActivity() {
    override fun onCreate(savedInstanceState: Bundle?) {
        super.onCreate(savedInstanceState)
        enableEdgeToEdge()
        setContent {
            MyFirstAppTWDMTheme {
                Scaffold( modifier = Modifier.fillMaxSize() ) { innerPadding ->
                    Greeting(
                        name = "Android",
                        modifier = Modifier.padding(innerPadding)
                    )
                }
            }
```

Figura 11. Exemplu de activitate

Fiecare activitate trebuie declarată în *AndroidManifest.xml* pentru ca sistemul să o poată recunoaște și lansa. Activitatea principală (MainActivity – fig. 12) trebuie să conțină un intent-filter pentru a fi punctul de start al aplicației.

```
    <activity
        android:name=".MainActivity"
        android:exported="true"
        android:label="MyFirstAppTWDM"
        android:theme="@style/Theme.MyFirstAppTWDM" >
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />

            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
```

Figura 12. Exemplu de activitate în AndroidManifest.xml

Fragmentul este o componentă reutilizabilă a UI-ului care rulează în cadrul unei Activități, fără a necesita o declarație în manifest. Interfaţa grafică utilizator a unei aplicaţii Android este construită dintr-o ierarhie de obiecte View - (ex. TextView, Button) sau ViewGroup (ex. Layout) conform figurii de mai jos (fig. 13).

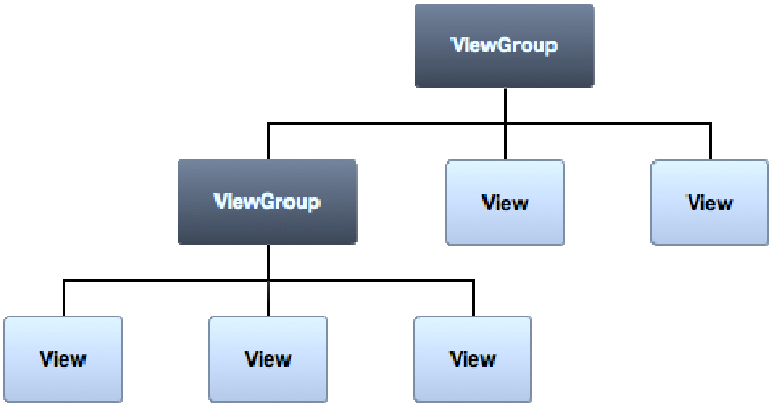


Figura 13. Ierarhia de obiecte GUI [7]

Un View reprezintă un element individual al interfeței grafice, cum ar fi un buton, un text sau o imagine. ViewGroup este un container care organizează și gestionează mai multe View-uri, permițând crearea unor structuri complexe de interfață. Interfaţa grafică utilizator a activităţii definite se regăseşte în fişierul *activity_main.xml* din cadrul directorului *res/layout/*.

Exemplu:

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

Tip resursă	Nume resursă
id	editTextNew
string	hello_world

Semnul + înaintea tipului de resursă este necesar când se definește 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).

4. Aplicații practice

4.1. Se va crea şi rula o primă aplicație Android urmând pașii disponibili pe pagina oficială: https://developer.android.com/codelabs/basic-android-kotlin-compose-first-app. Identificați pașii urmați, metodele utilizate și structura aplicației. Se va extinde proiectul cu mai multe activități care vor permite navigarea între aceste pagini.

4.2. Se va rula proiectul Network Info Status care permite vizualizarea informațiilor referitoare la starea rețelelor WiFi detectate. Aplicația scanează rețelele WiFi disponibile la deschidere și afișează utilizatorului informațiile despre acestea, după finalizarea scanării. Identificați pașii urmați și metodele utilizate.
Observație: se va actualiza AndroidManifest.xml cu permisiunile de securitate necesare.

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

4.4. Se va rula aplicația care utilizează serviciul web RESTful freegeoip (https://freegeoip.io/) pentru geolocaţia unei adrese IP sau a unui site web. Identificați pașii urmați și metodele utilizate. Se va modifica aplicația astfel încât răspunsul serviciului web să fie afișat într-o activitate nouă.

Bibliografie:

[1] Android Developers website, https://developer.android.com/develop/connectivity/overview
[2] Android Developers website, https://developer.android.com/guide/platform
[3] Android Developers website, https://developer.android.com/studio/intro
[4] Android Developers website, https://developer.android.com/guide/components/fundamentals
[5] Android Developers website, https://developer.android.com/studio/workflow
[6] Android Developers website, https://developer.android.com/studio
[7] Android Developers website, http://developer.android.com/training/basics/firstapp/building-ui.html