Tema 4. Medii de comunicare fără fir

Reţeaua fără fir (wireless) este reţeaua care nu utilizează cabluri între dispozitive.

Tipuri de reţele fără fir:

- infraroşu: această tehnologie operează cu dispozitive cum ar fi calculatoare, notebook, PDA- uri şi telecomenzi. Este utilizată pentru conectarea unor echipamente care nu se deplasează în timp ce se realizează transfer de date, operând în spectrul invizibil, situat după roşu din spectrul vizibil. Ca şi lumina nu poate străpunge obiectele opace şi are o rază de acoperire mult mai mică. O metodă pentru comunicaţia în infraroşu este specificată de IrDA (Infrared Data Association), folosită pe distanţe scurte, cu consum redus de energie, această tehnologie presupune existenţa unui câmp vizual fără obstacole între dispozitivele care realizează comunicarea. Sistemele care folosesc infraroşu lucrează cu lungimi de undă între 850 şi 950 nm. Aceste sisteme se utilizează în interiorul clădirilor şi operează cu transmisiune nedirecţională. Staţiile pot recepţiona transmisiuni în vizibilitate directă sau reflectate;

- bluetooth (PAN) – este o reţea fără fir personală, care creează o cale prin care se poate face schimb de informaţii între telefoane mobile, laptop-uri, calculatoare personale, imprimante, camere digitale şi console sigure, printr-o frecvenţă radio de rază mică. Dispozitivele bluetooth comunică între ele când se află în aceeaşi rază de acţiune. Sunt uşor de fabricat şi întregul proces consumă foarte puţină energie. Bluetooth a devenit un standard al industriei wireless comunicând prin unde radio cu o frecvenţă de aproximativ 2,45 gigahertzi. Aceasta este aceeaşi bandă utilizată de mai multe dispozitive industriale şi medicale dar şi casnice cum sunt dispozitivele de deschidere a uşilor de garaj şi aparetele de monitorizare a noilor născuţi. Când un dispozitiv ce rulează Bluetooth intră în raza de acţiune a altuia, are loc o mică conversaţie electronică. Acestea decid dacă trebuie să transfere informaţie şi dacă este cazul ele formează o mică reţea. Când se trimit date de pe un telefon pe altul, este un pic diferit. Persoana de la capătul receptor al conexiunii trebuie să-şi dea acordul pentru transfer, şi aici poate apărea o parolă. Aceste măsuri sunt luate din considerente de confidenţialitate şi securitate.

- Wi – Fi (LAN) – **Wireless Fidelity** – reţele care folosesc unde electromagnetice din domeniul radio. Este cel mai răspândit tip de retea, deoarece undele radio trec prin pereţi şi alte obiecte solide. Este o tehnologie construită pe baza standardelor de comunicaţie din familia IEEE 802.11 utilizate pentru reţele locale de comunicaţie fără fir la viteze echivalente cu cele ale reţelelor Ethernet. Raza de acoperire a unei reţele fără fir poate fi limitată la nivelul unei camere sau poate fi mai mare.

Toate reţelele 802 definesc subnivelul Media Access Control (MAC) şi nivelul fizic (PHY). Standardul 802.11 sau Wi – Fi specifică modul de conectare a reţelelor wireless şi se referă la un

grup de standarde 802.11a, 802.11b, 802.11g, 802.11n. Acestea specifică frecvenţele, vitezele şi alte capabilităţi ale diferitelor standarde Wi – Fi.

Standard	Lăţime bandă	Frecvenţă	Distanţă	Interoperabilitate
IEEE 802.11a	Până la 54 Mbps	Banda de 5 Ghz	150 ft (45.7 m)	Necompatibil cu 802.11b, 802.11g, 802.11n
IEEE 802.11b	Până la 11 Mbps	Banda de 2.4 Ghz	300 ft (91 m)	Compatibil cu 802.11g
IEEE 802.11g	Până la 54 Mbps	Banda de 2.4 Ghz	300 ft (91 m)	Compatibil cu 802.11b
IEEE 802.11n (Pre-standard)	Până la 540 Mbps	Banda de 2.4 Ghz	984 ft (300 m)	Compatibil cu 802.11b, 802.11g

Aspecte generale ale **Standardului IEEE 802.11**

Blocul fundamantal în arhitectura standardului 802.11 este reprezentat de Setul de Serviciu de Bază – BSS.

Acesta reprezintă un grup de staţii care lucrează conform uneia dintre funcţiile de coordonare: DCF sau PCF (Distributed Coordination Function sau Point Coordination Function).
Componentele reţelelor 802.11 sunt: staţie sau calculatorul cu placa de reţea wireless, punctul de acces (AP), mediul wireless, adică frecvenţa radio şi un sistem de distribuţie care înaintează cadrele către destinaţii. Punctele de acces sunt conectate la reţea folosind cabluri de cupru.

Aria geografică acoperită de BSS este numită Basic Service Area (BSA) şi este analogică unei celule din comunicaţiile celulare. Toate staţiile dintr-o BSS pot comunica direct cu oricare alte staţii din BSS.

Interferenţele care pot apărea între BSS vecine care utilizează aceeaşi parametrii pentru nivelul fizic (frecvenţă şi cod de împrăştiere) pot face ca anumite staţii să apară ascunse pentru celelalte staţii.
Conform standardului 802.11 se disting *două tipuri de reţele* locale:
- reţele ad-hoc (peer to peer adică punct la punct)
- reţele infrastructurale.

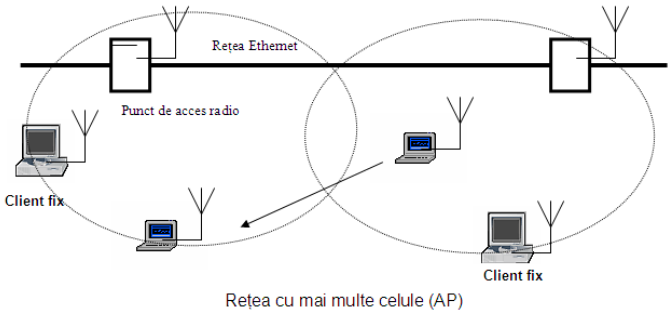
O reţea ad-hoc (BSS independente) este o grupare a staţiilor într-un singur BSS cu scopul comunicării inter-reţele fără ajutorul unei reţele infrastructurale. Orice staţie poate stabili o sesiune de comunicaţie directă cu altă staţie fără a fi necesară direcţionarea traficului printr-un punct de acces centralizat. Conectarea cu reţeaua cu fir se realizează prin intermediul unui calculator cu o aplicaţie software dedicată. În general, se realizează pentru o reţea cu un număr redus de calculatoare pe o suprafaţă mică. Calculatoarele trebuie configurate astfel încât să folosească acelaşi

canal radio. De obicei se folosesc astfel de reţele pentru diferite departamente sau ramuri ale companiilor.

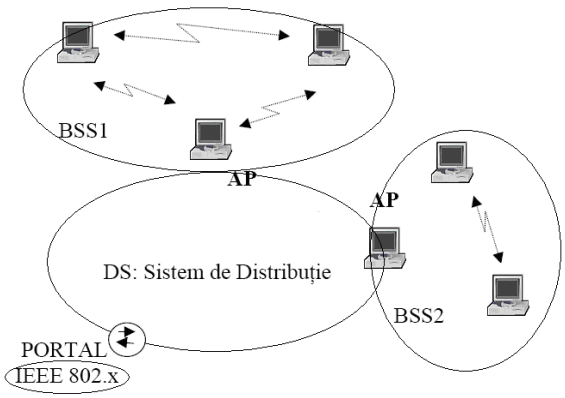
În opoziţie cu reţelele ad-hoc, *reţelele infrastructurale* au scopul să servească utilizatori cu servicii specifice şi cu extinderea zonei. Aceste reţele se constituie utilizându-se un AP. Acest mod de lucru permite o rază mai mare de acoperire prin utilizarea mai multor AP şi folosirea mai multor calculatoare în reţea. AP permite extinderea zonei prin conectarea între mai multe BSS formând un Set de Serviciu Extins (ESS).

ESS poate apare ca un BSS mai larg pentru subnivelul LLC (Logical Link Control) din fiecare staţie. ESS constă din mai multe BSS care pot coopera utilizând un sistem de distribuţie (DS) implementat independent (poate fi Ethernet LAN , token ring, LAN FDDI, MAN sau alt mediu fără fir IEEE 802.11).

Sistemul de distribuţie este utilizat pentru transferul pachetelor între diferite BSS. ESS poate oferi şi accesul pentru utilizatorii reţelei fără fir la o reţea cu fir cum ar fi Internetul.



Rețea cu mai multe celule (AP)



Exemplu de set de serviciu extins

Caracteristici generale ale comunicării fără fir

Avantaje

- Mobilitate – asigură conectarea fără dificultăţi atât a clienţilor staţionari, cât şi a clienţilor mobili;
- Scalabilitate – suportă conectarea unui număr mare de echipamente noi şi sporirea razei de acţiune;
- Flexibilitate – oferă conectivitate fără întreruperi clienţilor;

- Costuri reduse – costurile echipamentelor scad continuu pe măsură ce tehnologia avansează;
- Timp redus de instalare – instalarea unui singur echipament oferă conexiune la reţea pentru un număr mare de clienţi;
- Fiabilitate în condiţii grele – uşor de instalat în condiţii de urgenţă.

Dezavantaje şi limitări:

- Interferenţe – tehnologia Wireless este sensibilă la interferenţe electromagnetice cauzate de majoritatea echipamentelor electronice: telefoane mobile, cuptoare cu microunde, televizoare sau alte echipamente wireless;
- Securitatea datelor – tehnologia wireless LAN are drept scop principal să asigure accesul la date nu securizarea acestora. Mai mult, tehnologia wireless poate constitui o breşă nesecurizată a întregii reţele;
- Evoluţia tehnologică – tehnologia cu fir LAN evoluează în mod continuu. Tehnologia wireless LAN încă nu oferă viteza şi fiabilitatea reţelelor cu fir.

Pentru a rezolva problemele legate de transmisiune se pot folosi două variante de organizare (funcţii) a reţelei:

• **DCF (Distributed Coordination Function)** care este similară organizării din reţelele de comutare de pachete şi este destinată transferului asincron de date;

• **PCF (Point coordination Function)** care se bazează pe interogări controlate de punctul de acces şi care este destinată transmisiunilor sensibile la întârzieri;

Specificaţiile standardului IEEE 802.11 prevăd trei variante de implementare pentru nivelul fizic:

• folosind spectru împrăştiat cu salt de frecvenţă (FHSS),

• folosind spectru împrăştiat cu secvenţă directă (DSSS)

• folosind radiaţii în infraroşu (IR).

Sistemele care au la bază FHSS utilizează banda ISM (Industrial, Scientific and Medical band) de 2,4GHz. Primul canal are frecvenţa centrală de 2,402 GHz iar celelalte canale sunt distanţate cu 1 MHz. Sunt precizate trei seturi de secvenţe de salt cu câte 26 de secvenţe pe set. Aceasta permite coexistenţa mai multor BSS în aceeaşi zonă geografică ceea ce poate fi important pentru evitarea congestiilor şi pentru maximizarea transferului de date în BSS. Motivul pentru care sunt trei seturi diferite constă în evitarea perioadelor prelungite cu coliziuni între secvenţele de salt dintr-un set. Sistemele care folosesc DSSS utilizează de asemenea banda ISM de 2,4 GHz.

Mediul de transmisiune poate opera în două moduri:

• *modul concurenţial CP* (contend period), când staţiile îşi dispută accesul la canal pentru fiecare pachet transmis

• *modul neconcurenţial CFP*, când utilizarea mediului este controlată de AP.

O problemă pentru utilizatorii de reţea este lăţimea de bandă pe care o au la dispoziţie. Viteza de transfer este prestabilită de utilizatori sau rezultă în urma negocierii celor două echipamente fără fir. La fiecare pachet recepţionat se transmite un mesaj de confirmare a recepţiei (acknowledge). În concluzie, pentru un pachet de date e nevoie de două pachete, de aceea viteza de transfer se reduce la jumătate, aceasta este situaţia ideală, când nu apar erori de transmisie. Dar dacă canalul de transmisie este perturbat de alte echipamente viteza scade şi pot apărea şi apar retransmisii de pachete care reduc lăţimea de bandă. În situaţiile acestea ar putea fi utilizat un analizor de spectru, care ne poate da informaţii despre perturbările care apar pe canal, dar fiind un echipament costisitor, se recomandă folosirea altor canale, dacă apar probleme. Un alt aspect de care trebuie să ţinem cont este numărul de dipozitive wireless folosite. Având în vedere că un access point este asemănător cu un hub, trebuie respectate indicaţiile furnizorului de access point, deoarece lăţimea de bandă se împarte la toţi utilizatorii care comunică simultan. Din cauza coliziunilor care por apărea între două sau mai multe pachete, ceea ce înseamnă că două sau mai multe echipamente vor să transmită simultan date, lăţimea de bandă reală poate scădea.

IEEE 802.11 acceptă trei tipuri de cadre:

• de management (pentru asocierea staţiilor cu AP, sincronizare şi autentificare),
• de control (pt. negocieri în timpul CP respectiv pt. confirmări în timpul CP şi spre sfârşitul CFP);
• de date (pentru transmisie de date şi date combinate cu interogări şi confirmări în timpul CFP).

Formatul cadrului cuprinde:

• adrese MAC de 48 de biţi pentru identificarea staţiilor,
• 2 octeţi pentru specificarea duratei cât canalul va fi alocat pentru transmiterea cu succes a unei MPDU (MAC Protocol Data Unit),
• câmpul de date cu posibilitate de criptare dacă protocolul opţional WEP(Wired Equivalent Privacy),
• 2 biţi pentru tipul cadrului (de control, de management sau de date))
• un CRC de 32 de biţi.

DCF este metoda fundamentală de acces utilizată pentru transferul asincron al datelor. Toate staţiile au implementată această variantă. Ea poate opera singură sau poate coexista cu PCF.

Subnivelul MAC utilizează procedura CSMA (Carrier Sense Multiple Access), ca şi în Ethernet, dar, fiind dificil de detectat coliziunile într-un mediu fără fire, în reţelele IEEE 802.11 se implementează evitarea coliziunilor - collision avoidance (CSMA/CA) şi nu detectarea lor. În mecanismul de acces de bază se utilizează procedeul confirmării cadrelor transmise. Dacă un cadru de confirmare (ACK) nu este recepţionat într-un anumit interval de timp, cadrul neconfirmat va fi retransmis.

Detecţia purtătoarei este făcută fizic, la interfaţa radio (physical carrier sensing) sau logic, la subnivelul MAC (virtual carrier sensing).

Detecţia fizică a purtătoarei se face detectând prezenţa altor utilizatori WLAN prin analiza tuturor pachetelor detectate şi prin detecţia activităţii în canal observând puterea relativă a semnalului ce poate proveni de la alte surse.

Detecţia virtuală a purtătoarei se face prin transmiterea unei informaţii cu privire la durata MPDU în antetul RTS (request to send), CTS (clear to send) şi în cadrele de date. MPDU este o unitate completă de date transmisă de subnivelul MAC nivelului fizic.

Această informaţie reprezintă timpul (în microsecunde) cât canalul va fi utilizat pentru transmiterea cu succes a datelor sau cadrelor de management, începând de la sfârşitul cadrului curent. Canalul e marcat *ocupat* dacă mecanismul de detecţie a purtătoarei (*fizic sau virtual*) indică acest lucru.

Avantajul DCF constă în aceea că asigură un acces cu şanse egale pentru toate staţiile. Totuşi ea nu poate garanta o întârziere minimă pentru staţiile cu servicii în timp real (pachete de voce sau video).

PCF este un serviciu opţional, orientat pe conexiune, care asigură transferul cadrelor neconcurenţial (contention-free CF). PCF se bazează pe coordonatorul de punct (PC) pentru realizarea interogărilor şi pentru a permite accesul staţiilor la canal. Funcţia de coordonare (PC) este realizată de AP (acces point) în interiorul fiecărui BSS.

PCF trebuie să coexiste cu DCF şi din punct de vedere logic este o organizare superioară acesteia. PCF se repetă după un interval stabilit de un parametru, CFP-Rate.

O parte din acest interval este alocată traficului PCF, iar timpul rămas este alocat DCF.

Securitatea datelor

Spre deosebire de Ethernet, mediul de transmisie aduce probleme de securitate suplimentară. Dacă în Ethernet, accesul la cablu se putea restricţiona prin ascunderea sau asigurarea zonelor prin care trece acesta, undele radio sunt mult mai dificil de controlat. Există mecanisme de bruiaj, care generează un zgomot electromagnetic ce acoperă frecvenţele folosite de reţelele 802.11, dar acestea nu pot funcţiona perfect, fără a afecta comunicaţiile legitime sau fără a lăsa breşe prin care se poate obţine acces în reţea. Cum la nivel fizic securitatea este dificil de asigurat, pentru obţinerea unui nivel de securitate acceptabil este obligatorie criptarea datelor şi controlul accesului la nivelele superioare celui fizic.

Tehnici simple de control al accesului

Accesul la reţea se poate controla şi prin unele tehnici simple, care pot avea un succes limitat, dar suficient pentru a îndepărta unele intruziuni ocazionale.

Pentru a asigura securitatea de bază a reţelelor wireless este necesară implementarea următoarelor funcţii:

• SSID (Service Set Identifiers)

• WEP (Wired Equivalent Privacy or Wireless Encryption Protocol)

• Filtrarea adreselor MAC (Media Acces Control).

SSID-ul este un cod ataşat tuturor pachetelor de date format dintr-un şir de 1-32 octeţi de obicei reprezentaţi prin caractere alfanumerice. Oprirea transmiterii acestui semnal ascunde prezenţa reţelei faţă de un potenţial atacator superficial, permiţând totuşi staţiilor care cunosc SSID-ul punctului de acces să se conecteze la reţea. Această soluţie nu este una de natură să protejeze sistemul de accesul unor intruşi mai riguroşi, deoarece interceptarea cadrelor transmise în reţea între punctul de acces şi staţiile conectate poate oferi informaţia necesară pentru accesarea reţelei.

O modalitate foarte slabă de securitate este de a dezactiva opţiunea de broadcast a SSIDului. În general un punct de acces îşi transmite SSID-ul la fiecare câteva secunde, astfel încât, dacă acesta este dezactivat o persoană neautorizată nu poate descoperi automat SSID-ul şi implicit punctul de acces. Dar, deoarece SSID-ul este inclus în pachete, este uşor pentru un intrus dotat cu echipament de monitorizare să-i descopere valoarea şi să se conecteze la reţea.

O altă tehnică la fel de simplă, dar la fel de ineficientă, este **filtrarea adreselor MAC**. Ca şi în Ethernet, dispozitivele de acces la reţea sunt identificate în mod unic de o adresă fizică (denumită şi adresă MAC). Un punct de acces poate fi configurat să nu permită accesul în reţea decât staţiilor care au una dintr-o listă finită de adrese MAC. Prin aceeaşi tehnică de ascultare a traficului legitim din reţea, însă, un intrus poate afla adresa MAC a unei staţii legitime, falsificând apoi această adresă şi obţinând accesul, pretinzând că este respectiva staţie.

WEP (Wired Equivalent Privacy or Wireless Encryption Protocol) este folosit pentru a securiza reţelele wireless IEEE 802.11 şi pentru a ameliora problema transmiterii continue a SSID-ului prin criptarea traficului dintre clienţii wireless şi punctul de acces.

Paşii autentificării WEP:

1.Staţia (STA) trimite o cerere de autentificare.

2.Punctul de acces (AP) generează un nonce şi îl trimite staţiei.

3.Staţia criptează nonce-ul cu cheia secretă comună şi îl trimite înapoi punctului de acces.

4.Punctul de acces compară datele criptate primite cu cele aşteptate şi apoi trimite înapoi cadrul de autentificare cu rezultatul.

Prima tehnică de criptare a cadrelor la nivelul legătură de date a fost WEP (Wired Equivalent Privacy), numele sugerând că a fost gândită cu scopul de a obţine o securitate a legăturii de date echivalentă cu cea a unei reţele Ethernet. Această tehnică fost folosită din 1997 până când a fost spartă în 2001 şi a încetat să mai fie considerată sigură din 2005 odată cu publicarea standardului de securitate IEEE 802.11i.

WEP folosea algoritmul RC4, cu o cheie constantă de-a lungul transmisiunii, în variantele pe 64 de biţi (cheie de 40 de biţi şi vector de iniţializare de 24) sau de 128 de biţi (cheie de 104 biţi şi vector de iniţializare de 24), controlul integrităţii datelor realizându-se printr-o sumă de control CRC. În modul de lucru cel mai sigur, cel cu cheie partajată, autentificarea staţiilor se făcea printr-un mecanism de challenge: după ce o staţie anunţă că doreşte să se autentifice, punctul de acces alege aleator un text clar şi îl trimite staţiei. Staţia criptează textul primit şi îl trimite înapoi punctului de acces; punctul de acces decriptează mesajul şi îl compară cu cel trimis iniţial, permiţând sau respingând accesul în consecinţă. După ce accesul este permis, transmisia cadrelor se face criptat cu cheia reţelei.

O demonstraţie a spargerii WEP a fost publicată în august 2001 de Scott Fluhrer, Itsik Mantin şi Adi Shamir, care au arătat slăbiciuni în planificarea cheilor din algoritmul RC4, slăbiciuni care permit atacuri în timp liniar asupra transmisiunilor care îl folosesc, pe baza lucrării prezentate cu o lună înainte, la conferinţa ACM din 2001, de către Nikita Borisov, Ian Goldberg şi David Wagner. Ulterior, aplicaţii practice au demonstrat că atacul Fluhrer-Mantin-Shamir este uşor realizabil practic. La nivelul anilor 2005, o criptanaliză WEP cu unelte disponibile public necesită un timp de ordinul minutelor, atacuri îmbunătăţite reuşind de atunci şi în mai puţin de un minut. Ca o măsură temporară de sporire a securităţii pentru dispozitivele ce nu suportă programe de securitate avansate a fost elaborat WEP2. O altă variantă a acestui protocol este WEP Plus elaborat de Agere Systems. Această variantă este într-adevăr eficientă doar dacă este folosită la ambele capete ale conexiunii, condiţie ce nu poate fi întotdeauna realizată ceea ce face ca WEP Plus să fie limitat în privinţa securităţii.

Ca răspuns la spargerea WEP, Wi-Fi Alliance a produs în 2003 specificaţia WPA (Wi-Fi Protected Access), în care a adresat problemele primare ale WEP. În WPA, s-a păstrat algoritmul de criptare simetrică RC4, dar s-a introdus în schimb TKIP (Temporary Key Integrity Protocol), o tehnică de schimbare a cheii de criptare pe parcursul sesiunii de lucru şi s-a înlocuit suma de control CRC-32 din WEP cu algoritmul Michael, deoarece cu CRC recalcularea sumei de control unui cadru alterat nu necesita cunoaşterea cheii de criptare.

IEEE a preluat specificaţia WPA şi a elaborat în 2004 pe baza ei standardul IEEE 802.11i, standard care stabileşte o politică de criptare cunoscută sub numele de WPA2. În WPA2, algoritmul de criptare RC4 este înlocuit şi el cu mai puternicul algoritm AES, iar suma de control a cadrului este calculată cu ajutorul CCMP, un cod mai sigur decât CRC şi decât algoritmul Michael. WPA şi WPA2 pot funcţiona în două moduri distincte. Cel mai simplu dintre acestea, folosit în general la reţele personale, presupune configurarea staţiilor cu ajutorul unei parole de acces, parolă din care se calculează cheile de criptare cu ajutorul funcţiei PBKDF (Password-Based Key Derivation Function). În celălalt mod, WPA2 autentifică staţiile de lucru cu ajutorul unui server RADIUS.

Testarea reţelelor fără fir

Mai multe celule sunt conectate între ele, printr-o reţea de distribuţie, realizată de obicei prin cablu, formând un ESS (Extended Service Set) sau un domeniu. În acest domeniu un calculator mobil (un client) se poate deplasa de la o celulă la alta fără a pierde conexiunea cu reţeaua. Aceasta este semnificaţia termenului de roaming în noul context.

În acest scop staţia mobilă:

• va monitoriza permanent calitatea legăturii cu celula folosită.

• va începe căutarea de noi celule atunci când calitatea comunicaţiei scade sub un prag prestabilit

• va folosi un ID diferit în fiecare celulă, acesta fiind impus de către sistem.

Uzual, roaming-ul nu este posibil între secţiuni diferite ale reţelei interconectate cu ajutorul unor Routere sau Gateway-uri, dar există sisteme ce oferă şi această facilitate.

În fiecare celulă dintr-o reţea care acceptă acest serviciu, se transmite permanent un mesaj baliză care conţine următoarele informaţii: ID-ul domeniului, ID-ul celulei, informaţii despre calitatea comunicaţiei, informaţii despre celulele vecine.

În general, pentru orice echipament wireless, fie acesta o staţie bază – fie o staţie client, antenele sunt cele care oferă robusteţe şi flexibilitate, cele care optimizează anumite aplicaţii, cum ar fi legătura între mai multe clădiri. Întrucât mediul fără fir este unul foarte dinamic, prin folosirea unor antene direcţionale se poate influenţa modalitatea de propagare a semnalului radio. Astfel, energia şi caracteristica unui semnal pot fi direcţionate de-a lungul unui culoar îngust în loc să se lovească de pereţi, ceea ce ar duce la o risipă de energie sau poate cauza interferenţe nedorite. Antenele omnidirecţionale emit undele radio în toate direcţiile (sferă) în timp ce antenele unidirecţionale concentrează semnalul pe o direcţie preferenţială dată de orientarea antenei. Cu cât unghiul de emisie este mai mic, cu atât mai mare este distanţa acoperită. Avantajul antenelor omnidirecţionale constă în faptul că antena clientului nu trebuie să fie foarte precis orientată, fiind suficient să se afle în aria de acoperire a antenei staţiei bază. Dezavantajele sunt numeroase: risipă de putere de emisie, securitate scăzută datorită riscului ridicat de interceptare a undelor radio. Antenele unidirecţionale se situează pe o poziţie mai bună în ceea ce priveşte folosirea mai eficientă a puterii de emisie dar şi a riscului mai scăzut de interceptare a transmisiei. Dezavantajul lor constă în faptul că acordarea antenelor bază-client trebuie făcută foarte precis şi dimensiunea este semnificativă. Diversitatea antenelor oferă beneficii substanţiale implementărilor LAN fără fir, cum ar fi luxul folosirii mai multor antene sau posibilitatea de a alege cel mai bun tip de antenă pentru o locaţie dată. Pentru aceasta este nevoie de o bună cunoaştere a proprietăţilor semnalului radio şi a modalităţilor de amplasare corectă a antenelor radio. În practică, antenele amplasate prea aproape una de alta vor duce la o degradare a performanţei receptorului. Utilizarea diferitelor tipuri de antenă are, de asemenea, impact şi asupra metodei, dar şi a rezultatelor monitorizării unei locaţii. În

practică, antenele unidirecţionale se folosesc numai pentru legături fixe de tipul punct-la-punct, cum ar fi cazul unui bridge sau router de tip wireless.

Staţiile bază au deschiderea antenei de obicei de la 60 pînă la 360 de grade, asigurând conectivitatea clienţilor pe o anumită arie. Ele pot fi legate la o reţea cablată prin fibră optică, cabluri metalice sau chiar relee radio. Staţiile client au antene cu deschidere mult mai mică şi trebuie orientate spre BSS-uri.