6.3 WiFi: LAN-uri fără fir 802.11

LAN-urile fără fir reprezintă cea mai răspândită tehnologie de acces Internet fără fir fiind prezente la locul de muncă, în mediul casnic, în instituții de educație, localuri, aeroporturi şi parcuri. Deşi în anii 90 au fost dezvoltate mai multe tehnologii şi standarde pentru rețele locale fără fir doar una dintre ele s-a detaşat: LAN-uri fără fir IEEE 802.11, cunoscută şi sub numele de WiFi. În această secțiune vom studia detaliile LAN-urilor fără fir 802.11, examinând protocolul de acces la mediu, structura cadrului, precum şi interconectarea LAN-urilor 802.11 cu LAN-urile Ethernet cablate.

Există mai multe standarde 802.11 pentru LAN-uri fără fir: 802.11b, 802.11a, 802.11g şi 802.11n. Caracteristicile acestora sunt sintetizate in Tabelul 6.1. În acest moment sunt disponibile inclusiv dispozitive bi-standard 802.11a/g, tri-standard 802.11a/b/g şi chiar 802.11a/b/g/n.

Standard	Banda de frecvență (aprox)	Rata de transfer maximă	Bandă ocupată
802.11b	2,4 GHz	Pană la 11Mbps	22MHz
802.11a	5 GHz	Până la 54Mbps	22MHz
802.11g	2,4GHz	Pană la 54Mbps	22MHz
802.11n	2,4 şi 5GHz	Până la 495Mbps	22 sau 40MHz

Tabelul 6.1 Standardele 802.11

Standardele din familia 802.11 au o serie de caracteristici comune:

- folosesc acelaşi protocol de acces la mediu, CSMA/CA (pe care îl vom analiza în scurt timp);
- folosesc aceeaşi structură a cadrelor la nivel legătură de date;
- au posibilitatea de reducere a ratei de transfer în scopul creşterii distanței de comunicație;
- permit operarea atât în modul infrastructură cât şi în modul ad hoc.

După cum se poate observa în Tabelul 6.1 există deosebiri majore în ceea ce priveşte nivelul fizic.

LAN-urile fără fir 802.11b au o rată de transfer de până la 11 Mbps şi folosesc banda de frecvențe ISM nelicențiată de 2,4GHz partajând spectrul de frecvențe cu telefoanele ce operează în aceeaşi bandă precum şi cuptoarele cu microunde. LAN-urile 802.11a oferă rate de transfer semnificativ mai mari însă folosesc şi frecvențe mai mari. Prin operarea la frecvențe mai mari LAN-urile 802.11a au arii de acoperire mai mici pentru acelaşi nivel de putere al emițătorului iar problemele cauzate de propagarea multicale sunt mai pregnante. LAN-urile 802.11g operează în

aceeaşi bandă de frecvenţe ca si 802.11b fiind compatibile cu acestea însă oferă rate de transfer mai mari similare cu 802.11a.

Cel mai recent dintre standarde este 802.11n. Acesta foloseşte antene cu intrare multiplă şi ieşire multiplă (eng. multiple input multiple output, MIMO); mai exact se folosesc două sau mai multe antene la emisie şi două sau mai antene la recepție acestea transmițând/recepționând semnale diferite.

6.3.1 Arhitectura 802.11

Figura 6.7 ilustrează principalele componente ale arhitecturii LAN-urilor fără fir 802.11. Elementul fundamental al arhitecturii 802.11 este **setul de servicii de bază** (eng. basic service set, BSS). Un BSS constă din una sau mai multe staţii fără fir şi o **staţie de bază**, cunoscută în terminologia 802.11 sub numele de **punct de acces** (eng. acces point, AP).

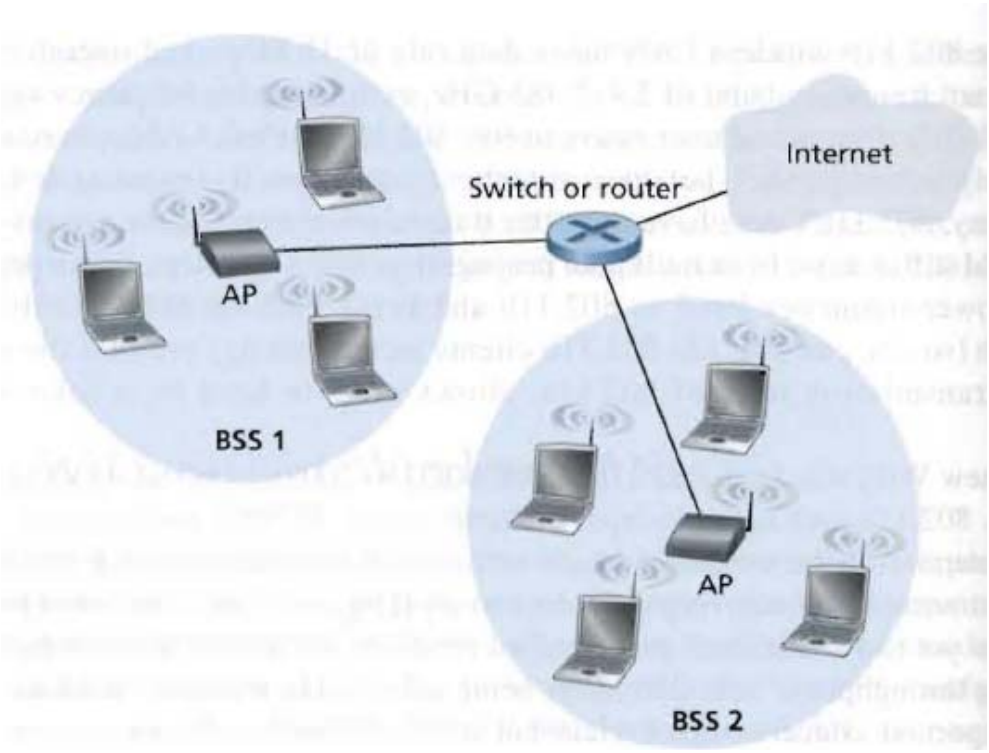


Figura 6.7 Arhitectura IEEE 802.11

Figura 6.7 prezintă AP-ul din fiecare BSS conectat la un dispozitiv de interconectare (ruter sau switch) care la rândul său este conectat la Internet. Într-o rețea casnică există un AP şi un ruter (de regulă integrate formând o singură unitate) care conectează BSS-ul la Internet.

La fel ca şi în cazul dispozitivelor Ethernet, fiecare staţie 802.11 are o adresă MAC stocată în firmware-ul adaptorului (interfață de rețea 802.11). Fiecare AP are de asemenea o adresă MAC pentru interfață radio. La fel ca în cazul Ethernet adresele MAC sunt administrate de IEEE fiind (teoretic) unice global.

Aşa cum s-a menționat în Secțiunea 6.1, LAN-urile fără fir care folosesc puncte de acces sunt referite ca LAN-uri fără fir cu infrastructură, infrastructura fiind punctul de acces împreună cu infrastructura Ethernet cablată care interconectează punctul de acces şi ruterul. Stațiile 802.11 se pot grupa pentru a forma o *rețea ah hoc* – o rețea fără un control centralizat şi fără conexiuni cu lumea exterioară. Rețeaua este formată „din zbor" existând dispozitive mobile aflate în proximitate care au nevoie să comunice însă nu există o infrastructură de rețea in acea locație. Rețelele ad hoc se pot forma de exemplu când o serie de utilizatori cu laptop-uri (la o conferință, în tren etc) doresc să transfere date în absența unui punct de acces. In continuare ne vom îndrepta atenția asupra rețelelor fără fir bazate pe infrastructură.

Figura 6.8 O rețea 802.11 ad hoc

Canalele şi asocierea

Orice stație gazdă 802.11 trebuie mai întâi să se asocieze la un punct de acces înainte de a putea trimite sau recepționa date. Deşi toate standardele 802.11 folosesc asocierea în continuare vom discuta chestiunea în contextul IEEE 802.11b/g.

Atunci când un administrator de rețea instalează un AP, el asignează punctului de acces un identificator al setului de servicii (eng. Service Set Identifier, SSID) format din una-două cuvinte. (Spre exemplu in Windows XP „view available networks" afişează o listă cu punctele de acces din zonă). Administratorul trebuie să aloce de asemenea un canal radio punctului de acces. Pentru a înțelege numerele de canale reamintiți-vă că 802.11 operează în banda de frecvențe de la 2,4GHz la 2,485GHz. În cadrul acestei benzi de 85MHz sunt definite 13 canale parțial suprapuse aşa cum este indicat în figura de mai jos. Oricare două canale nu sunt suprapuse doar dacă sunt separate de mai mult de patru canale. Spre exemplu setul de canale 1, 6 şi 11 nu se suprapun. Aceasta înseamnă că prin instalarea a trei puncte de acces 802.11b în aceeaşi locație fizică urmată de interconectarea

acestora printr-un switch se poate crea un LAN fără fir cu o rată totală maximă de transfer de 33 Mbps.

După înțelegerea canalelor 802.11 vom trece la descrierea unei situații interesante (foarte des întâlnită) şi anume jungla WiFi. O **junglă WiFi** reprezintă o locație fizică unde o gazdă fără fir recepționează semnale suficient de puternice de la două sau mai multe AP-uri.

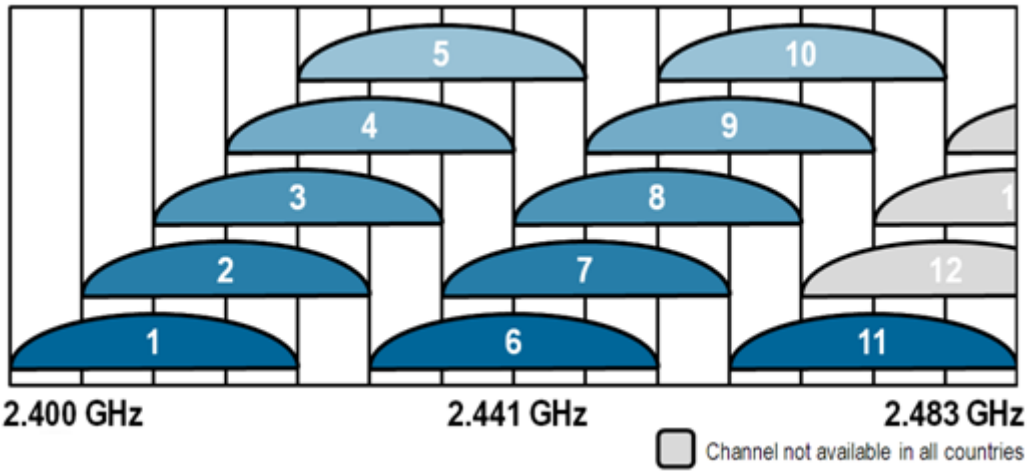


Figura. Canalele 802.11

Spre exemplu în multe locuri publice (şi nu numai) o gazdă fără fir poate recepționa semnale de la mai multe AP-uri. Unul dintre punctele de acces poate fi administrat de o cafenea iar altul poate fi într-un apartament din apropierea cafenelei. Fiecare din aceste AP-uri poate fi localizat într-o subrețea IP diferită fiind-ui asignat un canal în mod independent.

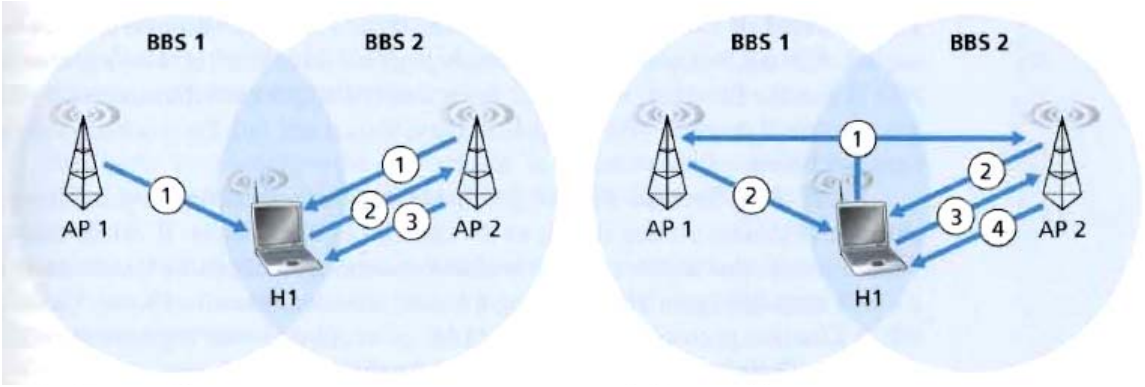
Să presupune că vă cineva intră cu laptop-ul într-o astfel de junglă dorind sa acceseze Internet-ul şi că există cinci puncte de acces. Pentru a avea acces la Internet stația trebuie să se alăture unei singure subrețele şi în consecință trebuie să se **asocieze** la exact un singur punct de acces. Mai exact doar punctul de acces asociat va trimite cadre de date către stația fără fir, iar stația fără fir va trimite cadre de date spre Internet doar prin intermediul AP-ului asociat. Cum se asociază însă stația cu un anumit AP, şi de unde ştie stația ce punct de acces există?

Standardul 802.11 impune ca fiecare AP să trimită periodic **cadre baliză** (eng. beacon frame) care includ SSID-ul AP-ului, adresa sa MAC, canalul radio precum şi alți parametri. Cunoscând acest fapt stația va baleia cele 13 canale în căutarea cadrelor baliză (este posibil ca unele AP-uri să transmită inclusiv pe acelaşi canal). Având cunoştință de existența punctelor de acces (prin intermediul cadrelor baliză) stația (sau utilizatorul) va selecta pe unul dintre ele pentru asociere.

Standardul 802.11 nu specifică un algoritm pentru selectarea punctului de acces pentru asociere; algoritmul este lăsat la latitudinea dezvoltatorilor de firmware şi software. În mod tipic gazda alege punctul de acces ale cărui cadre baliză sunt recepționate cel mai puternic. Deşi existenta unui semnal puternic este bună, puterea semnalului nu este singura caracteristică a punctului de acces care va determina performanța pentru gazda. În particular, este posibil ca AP-ul selectat să

aibă un semnal puternic dar să fie supraîncărcat cu alte gazde (care partajează lărgimea de banda a acelui AP) iar un AP neîncărcat să nu fie selectat datorită semnalului mai slab.

Procesul de scanare a canalelor şi ascultare a cadrelor baliză este cunoscut ca **scanare pasivă** (Figura 6.9a). O gazdă fără fir poate efectua şi o **scanare activă** difuzând cadre de probă care vor fi recepționate de toate AP-urile din aria de acoperire aşa cum este indicat în Figura 6.9b. Gazdă fără fir poate apoi selecta punctul de acces pentru asociere din cele care răspund la interogare.



a. Scanare pasivă
1. Cadre baliză trimise de AP
2. Trimitere cadru Cerere Asociere: H1 -> AP selectat
3. Trimitere cadru Răspuns Asociere: AP selectat -> H1

a. Scanare activă
1. Cadru de sondare difuzat de H1
2. Cadru răspuns la sondare trimis de AP
3. Trimitere cadru Cerere Asociere: H1 -> AP selectat
4. Trimitere cadru Răspuns Asociere: AP selectat -> H1

Figura 6.9 Scanarea activă şi pasivă în căutarea punctelor de acces

După selectarea unui punct de acces în vederea asocierii stația trimite un cadru de cerere de asociere către AP iar punctul de acces răspunde cu un cadrul de răspuns la asociere. Acest al doilea proces de negociere este necesar inclusiv atunci când se foloseşte scanarea activă, întrucât punctul de acces care a răspuns la cererea de probă inițială nu ştie care din punctele de acces care au furnizat răspunsuri va fi selectat pentru asociere. [După asocierea la AP, stația se va alătura subrețelei (în sensul adresării IP) de care aparține punctul de acces. De regulă gazda va face o cerere DHCP pentru obținerea unei adrese IP. După obținerea adresei gazda respectivă este văzută de restul stațiilor ca orice altă gazdă din subrețeaua respectivă.

Pentru ca o stație să se poată asocia la un AP este posibilă solicitarea unei autentificări prealabile. Rețelele 802.11 pun la dispoziție pentru o serie de alternative pentru autentificare şi acces. O abordare este permiterea accesului pe baza adresei MAC; o altă abordare este furnizarea unei parole sau a unui nume de utilizator şi a unei parole. De regulă, AP-ul comunică cu un server de autentificare, punctul de acces transferând informația între stația capăt şi serverul de autentificare folosind un protocol cum ar fi RADIUS [RFC 2865] sau DIAMETER [RFC 3588]. Separarea autentificării de punctul de acces permite folosirea unui singur server pentru mai multe AP-uri,

centralizând decizia de autentificare şi acces (adesea sensibilă) pe un singur server, menținând redus costul şi complexitatea AP-urilor.]

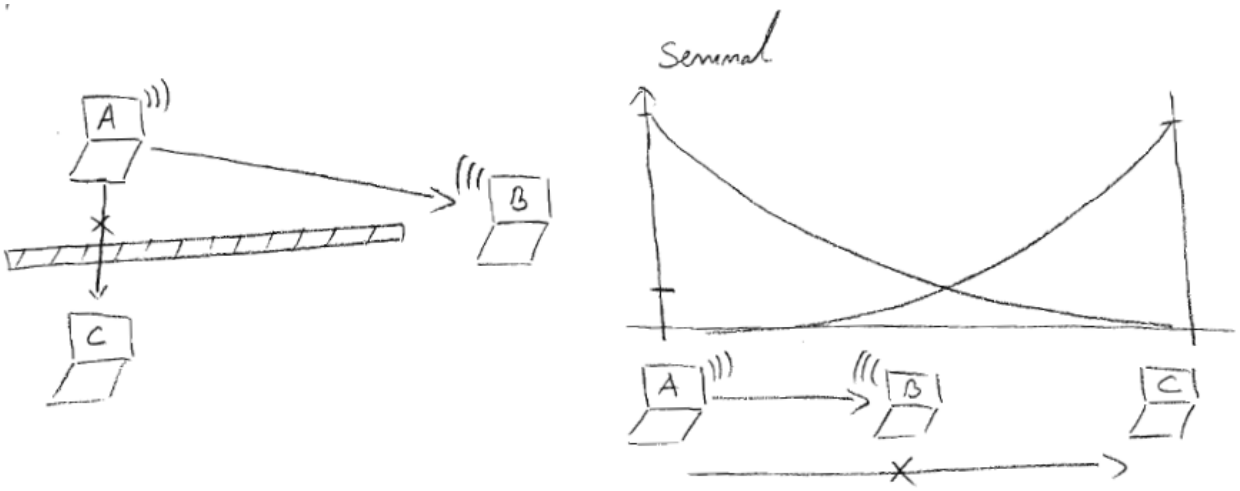
6.3.2 Protocolul MAC 802.11

După ce o stație s-a asociat la un punct de acces aceasta poate începe să trimită şi să recepționeze cadre spre şi de la punctul de acces. Întrucât pot exista mai multe stații care doresc să transmită în acelaşi timp folosind acelaşi canal este necesar un protocol de acces multiplu pentru coordonarea transmisiilor. Aici o **stație** este fie o gazdă fără fir fie un punct de acces. În mare există trei clase de protocoale cu acces multiplu: partiționarea canalului (inclusiv CDMA), acces aleator si acces pe rând. Inspirați de succesul Ethernet-ului şi al protocolului său cu acces aleatoriu proiectanții 802.11 au ales pentru LAN-urile fără fir 802.11 un protocol cu acces aleatoriu. Protocolul cu acces aleatoriu este **CSMA cu evitarea coliziunilor** sau pe scurt CSMA/CA. La fel ca şi în cazul CSMA/CD de la Ethernet CSMA din CSMA/CA implică acces multiplu cu detecția purtătoarei, ceea ce înseamnă că fiecare stație înainte de a transmite mai întâi ascultă canalul iar în cazul în care acesta este ocupat îşi amână transmisia. Deşi atât Ethernet-ul cât şi 802.11 utilizează accesul aleatoriu cu detecția purtătoarei, cele două protocoale MAC au diferențe importante. În primul rând, în loc de a utiliza detecția coliziunilor 802.11 foloseşte o tehnică de evitare a coliziunilor. În al doilea rând datorită ratei mari de eroare la nivel de bit pe canalele fără fir, 802.11 foloseşte o schemă de confirmări şi retransmisii la nivel legătură de date. Vom descrie mai jos schema de evitare a coliziunilor şi confirmare la nivel legătură de date.

În cazul algoritmului Ethernet de detectare a coliziunilor, stația ascultă canalul în timp ce transmite. Dacă în timp ce transmite stația detectează că o altă stație transmite, aceasta abandonează transmisia şi încearcă să retransmită după ce aşteaptă un scurt interval de timp aleatoriu. Spre deosebire de protocolul Ethernet (IEEE 802.3), protocolul MAC 802.11 nu implementează detecția coliziunilor din două motive:

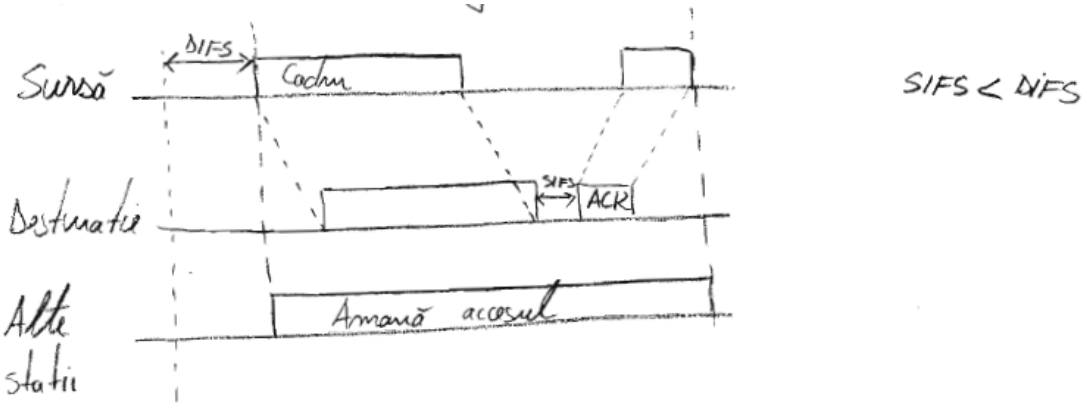
- Abilitatea de a detecta coliziuni impune ca stația să fie capabilă să transmită şi să recepționeze (pentru a detecta dacă o altă stație transmite simultan) în acelaşi timp. Întrucât puterea semnalului recepționat este foarte mică în raport cu semnalul transmis este foarte costisitoare construirea de hardware cate să poată detecta coliziuni.

- Chiar dacă adaptorul ar putea transmite şi recepționa în acelaşi timp (şi ar abandona transmisia în cazul în care canalul este ocupat), adaptorul tot nu ar putea detecta toate coliziunile datorită problemei stației ascunse.



Deoarece LAN-urile fără fir 802.11 nu utilizează detecția coliziunilor, odată ce o stație începe să transmită un cadru, *aceasta va transmite cadrul in totalitate*. Aşa cum era de aşteptat transmiterea integrală a cadrelor (şi mai ales a cadrelor lungi) atunci când coliziunile sunt frecvente poate degrada semnificativ performanță protocolului de acces multiplu. Pentru a reduce probabilitatea de coliziune 802.11 foloseşte câteva tehnici de evitare a lor.

Înainte de a examina evitarea coliziunilor, să examinăm mai întâi schema 802.11 de **confirmări la nivel legătură de date**. Atunci când o stație dintr-un LAN fără fir transmite un cadru, este posibil ca acesta să nu ajungă intact la destinație. Pentru a trata cazurile deloc neglijabile de eşec protocolul MAC 802.11 foloseşte confirmări la nivel legătură de date. Aşa cum se poate observa în Figura 6.10 atunci când o stație recepționează un cadru având CRC-ul corect, aceasta aşteptă un scurt interval de timp denumit **interval scurt inter-cadru** (eng. Short Interf-frame Space, SIFS) după care trimite un cadru de confirmare. Dacă stația emițătoare nu recepționează confirmarea într-un interval specificat consideră că a avut loc o eroare şi retransmite cadrul folosind protocolul CSMA/CA pentru accesarea canalului. Dacă nu se recepționează o confirmare după un număr fixat de retransmisii atunci cadrul este abandonat.



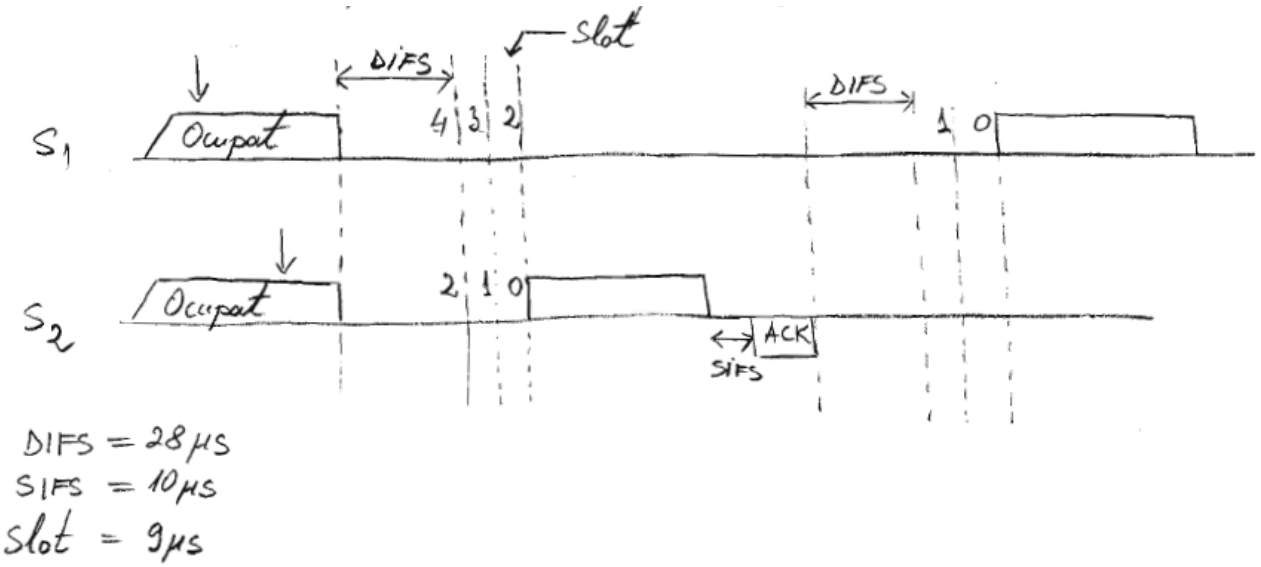
După discutarea confirmărilor la nivel legătură de date suntem în măsură să descriem protocolul CSMA-CA 802.11. Presupunem că o stație are de transmis un cadru.

1. În cazul în care canalul este detectat ca fiind liber pentru o durată mai mare sau egală cu DIFS (Distributed Inter-frame Space, Intervalul inter-cadru distribuit) stației i se permite să transmită.

2. Dacă mediul este ocupat, stația alege un număr aleatoriu ce desemnează un interval de timp fără transmisii ce trebuie să se scurgă înainte de a începe transmisia. Timpul este cuantificat iar contorul este decrementat cu o unitate pe parcursul fiecărei cuante în care mediul este detectat ca inactiv.

3. În momentul în care contorul atinge valoarea zero stația transmite întreg cadrul şi aşteaptă confirmarea.

4. Dacă se recepționează confirmarea stația va şti ca acel cadru a fost recepționat corect. Dacă stația are alt cadru de transmis aceasta începe procedura CSMA/CA la pasul 2. Dacă nu se recepționează confirmarea stația reintră în faza de regresie exponențială de la pasul 2 alegând contorul de regresie dintr-un interval mai mare.



În cazul protocolului cu acces multiplu CSMA/CD o stație începe să transmită imediat ce sesizează canalul ca fiind liber. În cazul CSMA/CA însă stația îşi amână transmisia, numărând descrescător, chiar dacă se detectează canalul liber. În continuare vom prezenta motivația pentru aceste abordări diferite.

Considerăm două stații, ambele având cadre de transmis, insă nici una dintre ele nu transmite imediat întrucât fiecare sesizează că o a treia stație deja transmite. În cazul utilizării CSMA/CD ambele stații ar începe să transmită imediat ce a treia stație eliberează canalul. Acest fapt duce în mod sigur la apariția unei coliziuni, ceea ce în cazul CSMA/CD nu este o problemă serioasă întrucât ambele stații vor detecta coliziunea abandonând transmisiile. În cazul 802.11 situația este diferită. Deoarece 802.11 nu detectează coliziunile, un cadru implicat intr-o coliziune va fi transmis în totalitate deşi acesta nu mai este utilizabil. Obiectivul pentru 802.11 este deci evitarea pe cat posibil

a coliziunilor, în punctul în care este cel mai probabil ca acestea să apară şi anume imediat după eliberarea mediului. Deci staţiile care folosesc CSMA/CA şi sesizează canalul ca fiind ocupat, vor intra după eliberarea canalului într-o fază de regresie exponenţială cu speranţă că vor alege valori diferite ale contorului. Dacă se întâmplă aşa, o staţie va începe mai repede să transmită, celelalte staţii vor sesiza transmisia şi vor suspenda numărătoarea descrescătoare până la eliberarea canalului. Astfel se pot evita coliziuni costisitoare. Bineînţeles că există posibilitatea apariţiei unor coliziuni dacă valorile alese sunt egale sau apropiate astfel încât semnalul să nu se propage la toate staţiile care vor să transmită sau datorită staţiilor ascunse.

Soluţionarea problemei staţiei ascunse

Protocolul MAC 802.11 include o schema opţională de rezervare care ajută la evitarea coliziunilor chiar şi în prezenţa unor terminale ascunse. Vom investiga problema în contextul din Figura 6.11, unde două staţii sunt se găsesc în aria de acoperire a punctului de acces (asociate la acest AP). Datorită atenuării semnalul staţiilor fără fir este limitat în interiorul cercului având centrul la staţie. Astfel fiecare staţie fără fir este ascunsă de cealaltă, insă nici una nu e ascunsă faţă de AP.

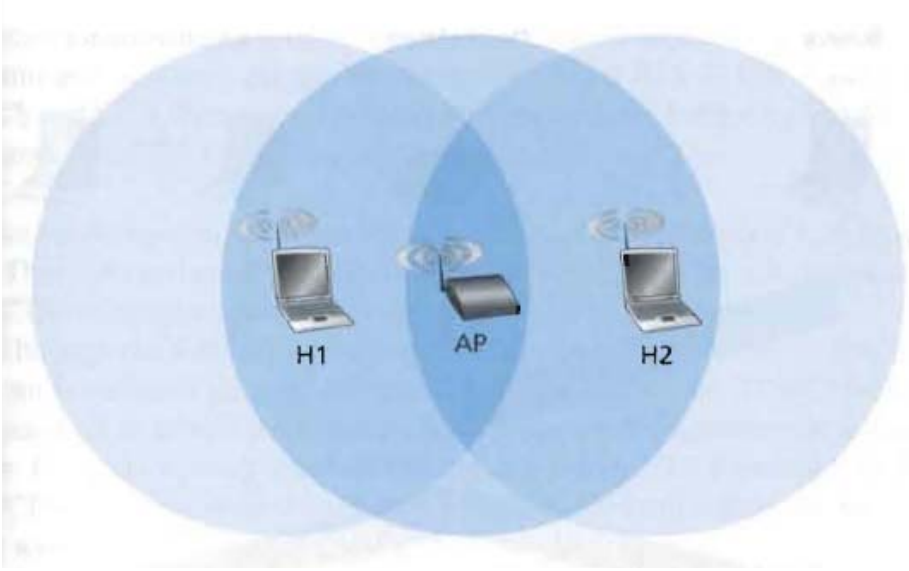


Figura 6.11 Exemplu de terminale ascunse: H1 este ascuns de H2 şi vice versa

Să presupunem că Staţia H1 efectuează o transmisie iar la jumătatea cadrului, Staţia H2 doreşte să trimită un cadru către AP. H2 nu sesizează transmisia de la H1 ceea ce duce la apariţia unei coliziuni. Canalului este irosit pe întreaga durată a transmisie lui H1 cît si pe durata transmisie lui H2.

Pentru a evita astfel de probleme protocolul IEEE 802.11 permite unei staţii să folosească două cadre scurte de control RTS (Request to Send) şi CTS (Clear to Send) pentru a *rezerva* accesul la canal. Atunci când o staţie doreşte să transmită un cadru de DATE, aceasta poate trimite mai întâi

un cadru RTS către AP indicând timpul total necesar pentru transmiterea cadrului de DATE şi a cadrului de confirmare (ACK). După recepționarea cadrului RTS, punctul de acces va răspunde prin difuzarea unui cadru CTS. Cadrul CTS are două scopuri: dă emițătorului permisiunea explicită de a transmite şi instruieşte celelalte stații să nu transmită pe durata rezervată.

Astfel în Figura 6.12, înainte de a transmite cadrul de DATE, H1 difuzează un cadru RTS, care este recepționat de toate stațiile din cerc, inclusiv AP-ul. Punctul de acces va răspunde cu un cadru CTS, care este auzit de toate stațiile din raza sa de acțiune , inclusiv H1 şi H2. După recepționarea CTS-ului stația H2 nu va transmite pe durata specificată in CTS chiar daca sesizează canalul liber.

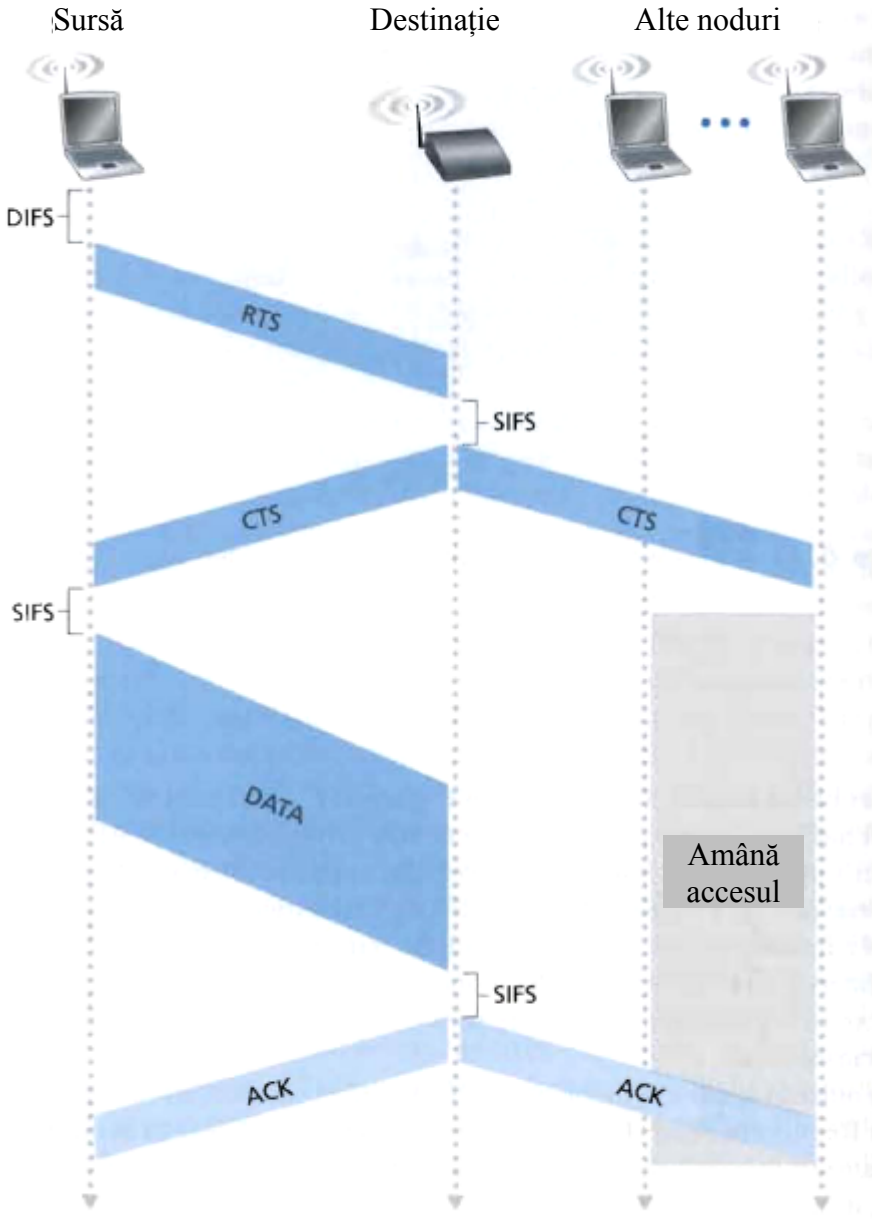


Figura 6.12 Evitarea coliziunilor folosind cadre RTS şi CTS

Folosirea RTS-CTS poate îmbunătății performanța în două moduri:

- se rezolvă problema staţiei ascunse, întrucât cadrele de DATE sunt transmise doar după rezervarea canalului
- întrucât cadrele RTS şi CTS sunt scurte, o coliziune care implică un cadru RTS sau CTS va ocupa canalul doar pentru o durată mică. După transmiterea corectă a cadrelor RTS şi CTS, cadrul de DATE şi confirmarea sa nu vor suferi coliziuni.

Deşi schimbul RTS-CTS poate ajuta la reducerea coliziunilor acesta introduce întârzieri care consumă resursele canalului. Din acest motiv schimburile RTS-CTS se folosesc doar pentru a rezerva canalul înaintea unor cadre de DATE lungi. În practică fiecare staţie fără fir are configurat un prag, schimbul RTS-CTS fiind folosit doar pentru cadre a căror lungime depăşeşte acest prag. În mod implicit, de cele mai multe ori acest prag este mai mare decât lungimea unui cadru de lungime maximă făcând ca mecanismul RTS-CTS să nu fie utilizat.

6.3.3 Structura cadrelor IEEE 802.11

Pentru a face faţă provocărilor apărute ca urmare a utilizării unui mediu fizic fără fir, au fost adoptate câteva măsuri unice ce nu se găsesc la reţelele cablate (IEEE 802.3). Printre acestea se numără utilizarea a trei tipuri de cadre: de management, de control şi de date. Structura unui cadru 802.11 generic este prezentată în Figura 6.13. Anumite tipuri de cadre nu folosesc toate câmpurile prezente, însă păstrează structura de bază. La momentul adoptării standardului, acest format a fost considerat cel mai bun compromis între eficienţă şi funcţionalitate.

Deşi cadrele 802.11 partajează o serie de caracteristici comune cu cadrele Ethernet, acestea conţin şi o serie de câmpuri specifice utilizării pe legături fără fir. Numerele de deasupra câmpurilor cadrului reprezintă lungimile câmpurilor exprimate in *octeţi*; numerele de deasupra subcâmpurilor din câmpul control cadru reprezintă lungimile subcâmpurilor exprimate în *biţi*. În continuare vom examina câmpurile cadrului precum şi câteva din cele mai importante subcâmpuri din câmpul control cadru.

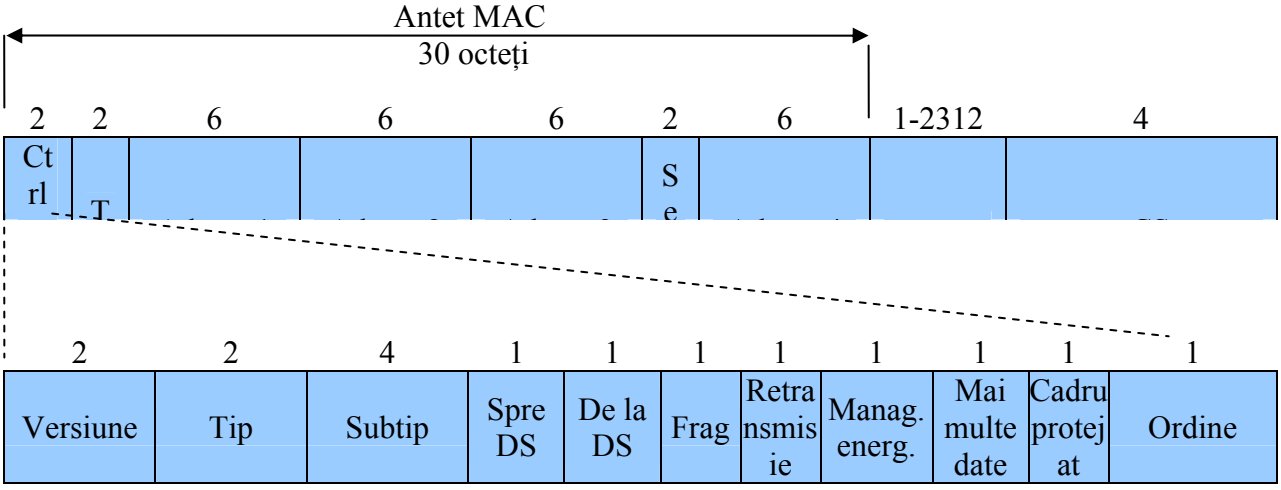


Figura 6.13 Formatul cadrelor IEEE 802.11

Încărcătura utilă şi CRC-ul

Elementul centra al cadrului este încărcătura utilă, care constă de regulă dintr-o datagramă IP sau un mesaj ARP. Deşi dimensiunea maximă a acestui câmp este de 2312 octeți, în mod tipic nu se depăşesc 1500 de octeți pentru a se asigura compatibilitatea cu cadrele Ethernet. La fel ca şi în cazul Ethernet cadrul se încheie cu o sumă de control cu redundantă ciclică pe 32 de biți. Aşa cum s-a menționat rata de eroare la nivel de bit în cazul LAN-urilor fără fir este mai mare decât în cazul LAN-urilor cablate, ceea ce face ca CRC-ul să fie mult mai util în acest caz.

Câmpurile de adrese

Probabil cea mai surprinzătoare diferență în structura cadrelor 802.11 este faptul că acestea au *patru* câmpuri de adresă, fiecare putând îngloba o adresă MAC de 6 octeți. De ce sunt necesare patru adrese? Nu ar fi fost suficiente adresa MAC destinație şi adresa MAC sursă ca la Ethernet? Pentru interconectare -- transportul unei datagrame de nivel rețea de la o stație fără fir la interfață ruterului prin intermediul punctului de acces -- sunt necesare trei câmpuri de adresă. A patra adresă este necesară atunci când se transmit cadre între punctele de acces (prin interfețele radio) ce formează un sistem de distribuție ad-hoc fără fir. Întrucât vom avea în vedere doar rețelele bazate pe infrastructură, ne vom concentra doar pe primele trei câmpuri de adresă. Standardul 802.11 defineşte aceste câmpuri astfel:

- *Adresa 2* reprezintă adresa MAC a stației care transmite cadrul. Astfel dacă acel cadru este transmis de o stație aceasta va insera adresa sa MAC în câmpul Adresa 2. În mod similar dacă acel cadru e transmis de un punct de acces, în câmpul Adresa 2 se va regăsi adresa MAC a AP-ului.
- *Adresa 1* este adresa MAC a stației care trebuie să recepționeze cadrul. Astfel dacă acel cadru e transmis de o stație câmpul Adresa 1 conține adresa MAC a punctului de acces destinație. În mod similar dacă AP-ul transmite cadrul atunci câmpul Adresa 1 conține adresa MAC a stației fără fir destinație.
- Pentru a înțelege *Adresa 3* amintiți-vă ca BSS-ul (constând din AP şi stații fără fir) este parte a unei subrețele, această subrețea fiind conectată la alte subrețele prin interfața unui ruter. Adresa 3 conține adresa MAC a interfeței ruterului.

În vederea clarificării scopului Adresei 3, vom proceda la studierea unui exemplu de interconectare având la bază Figura 6.14. În această figură există două puncte de acces, fiecare fiind responsabil de o serie de stații fără fir. Fiecare punct de acces are o conexiune directă la ruter, care este conectat mai departe de la Internet. Trebuie să avem în vedere faptul că AP-urile sunt dispozitive de nivel legătură de date; acestea nu operează cu adrese IP şi nici nu „înțeleg" semnificația acestora. Să considerăm transmiterea unei datagrame de la interfața R1 a ruterului la

stația fără fir H1. Ruterul nu are cunoştință de faptul că există un AP între el şi H1; din perspectiva lui ruterului, H1 este o stație ca oricare alta din subrețele conectate la ruter.

- Ruterul care cunoaşte adresa IP a lui H1 (adresa destinație din datagrama IP), foloseşte APR-ul pentru a determina adresa MAC a lui H1, la fel ca intr-un LAN Ethernet obişnuit. După obținerea adresei MAC a lui H1, interfața R1 a ruterului încapsulează datagrama întru-un cadru Ethernet. Câmpul adresa sursă al cadrului conține adresa MAC a lui R1 iar câmpul adresă destinație conține adresa MAC a lui H1.
- După ce cadrul Ethernet ajunge la AP, înainte de transmisia cadrului pe canalul radio, punctul de acces converteşte cadrul Ethernet 802.3 într-un cadru 802.11. AP-ul completează Adresa 1 şi Adresa 2 cu adresa MAC a lui H1 şi respectiva propria adresă MAC, aşa cum s-a menționat mai sus. La Adresa 3 punctul de acces înscrie adresa MAC a lui R1. În acest mod H1 poate determina (din Adresa 3) adresa MAC a interfeței ruterului care a trimis datagrama în subrețea.

Să vedem acum ce se întâmplă în momentul în care stația fără fir H1 răspunde, prin transmiterea unui cadru de la H1 la R1.

- H1 creează un cadru 802.11, completând câmpurile Adresa 1 şi Adresa 2 cu adresa punctului de acces şi respectiv adresa proprie aşa cum s-a menționat în prealabil. La adresa 3, H1 inserează adresa MAC a lui R1.

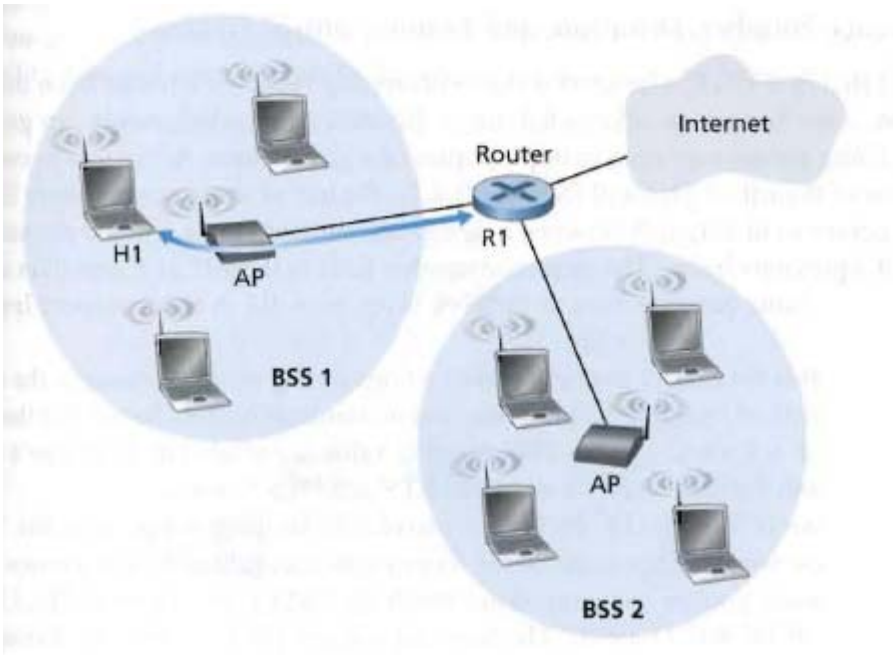


Figura 6.14 Utilizarea câmpurilor de adrese în cadrele 802.11: Trimiterea de cadre între H1 şi R1

- După recepționarea cadrului 802.11 punctul de acces în converteşte într-un cadru Ethernet. Adresa sursă pentru acest cadru va fi adresa MAC a lui H1 iar adresa destinație va fi adresa

MAC a lui R1. În acest fel adresa 3 permite AP-ului să determine adresa destinație corespunzătoare atunci când creează cadrul Ethernet.

Pe scurt Adresa 3 joacă un rol crucial pentru interconectarea BSS-ului la o rețea LAN cablată.

Numărul de secvență, durata şi câmpurile control cadru

Conform standardului 802.11 atunci când o stație recepționează corect de la o altă stație un cadru care ii este adresat aceasta trimite în scurt timp o confirmare. Întrucât confirmările se por pierde, stația emițătoare poate trimite mai multe copii ale aceluiaşi cadru. Folosirea numerelor de secvență permite receptorului să distingă între cadrele nou transmise şi retransmisiile unui cadru anterior. Numărul de secvență din cadrele 802.11 serveşte aceluiaşi scop aici la nivel legătură de date ca şi în cazul numerelor de secvență de la nivel transport (Capitolul 3).

Protocolul 802.11 permite unei stații să solicite rezervarea canalului pentru o perioadă de timp care include timpul necesar transmiterii cadrului precum şi timpul necesar transmiterii confirmării. Valoarea acestei durate este inclusă în câmpul durată (atât pentru cadrele de date cât şi pentru cadrele RTS şi CTS).

Aşa cum este indicat în Figura 6.13 câmpul control cadru include mai multe subcâmpuri. Vom spune doar câteva cuvinte despre cele mai importante dintre acestea; pentru o discuție completă se pot consulta specificațiile 802.11 [Held 2001; Crow 1997; IEEE 802.11 1999]. Câmpurile *tip* şi *subtip* se folosesc pentru diferențierea cadrelor de asociere, RTS, CTS, ACK sau date. Câmpurile *De la* şi *Spre* sunt folosite pentru a defini semnificația diverselor câmpuri de adrese (Semnificațiile se modifică în funcție de utilizarea modurilor ad-hoc sau infrastructură iar în cazul modului infrastructură dacă stația sau punctul de acces trimite cadrul). În final câmpul WEP indică dacă se utilizează sau nu criptarea.

6.3.4 Mobilitate în cadrul aceleiaşi subrețele IP

Pentru a creşte acoperirea fizică a LAN-urilor fără fir companiile şi universitățile instalează adesea mai multe BSS-uri în aceeaşi subrețea IP. Acest fapt ridică problema mobilității între BSS-uri -- cum se deplasează stațiile de la un BSS la altul menținând conexiunea TCP. Aşa cum vom vedea în această subsecțiune, atunci când BSS-urile fac parte din aceeaşi subrețea, mobilitatea este tratată într-o manieră simplă. Atunci când stațiile se deplasează între subrețele sunt necesare protocoale mult mai sofisticate pentru managementul mobilității, care vor fi studiate în Secțiunile 6.5 şi 6.6.

În continuare vom studia mobilitatea între BSS-uri din aceeaşi subrețea pe baza unui exemplu specific. Figura 6.15 prezintă două BSS-uri interconectate şi o stație care deplasează din BSS1 spre BSS2. Deoarece în acest exemplu dispozitivul de interconectare nu este un ruter, toate stațiile din

cele două BSS-uri, inclusiv AP-urile fapt parte din aceeaşi subrețea IP. Atunci când H1 se deplasează din BSS1 în BSS2 aceasta îşi poate păstra adresa IP precum şi toate conexiunile TCP deja stabilite. Dacă dispozitivul de interconectare ar fi fost un ruter atunci H1 ar fi trebuit să obțină o nouă adresă IP din rețeaua în care s-a deplasat. Modificarea adresei ar fi perturbat (şi eventual terminat) toate conexiunile TCP de la H1. În Secțiunea 6.6 vom examina modul în care un protocol de management al mobilității la nivel rețea, cum ar fi *mobile IP*, poate fi folosit pentru a evita astfel de probleme.

Ce se întâmplă exact atunci când stația H1 se deplasează din BSS1 în BSS2? Pe măsură ce H1 se îndepărtează de AP1, stația H1 va detecta reducerea puterii semnalului recepționat şi va începe să scaneze în căutarea unui semnal mai puternic. H1 va recepționa cadrele baliză de la AP2 (care în unele corporații sau universități va avea acelaşi SSID ca si AP1). H1 se va dezasocia de la AP1 şi se va asocia la AP2, păstrându-şi adresa IP precum şi conexiunile TCP stabilite.

Mai sus am discutat problema transferului de legătură din perspectiva stației gazdă şi a punctului de acces. Dar ce se întâmplă cu switch-ul din Figura 6.15? Cum va şti că stația s-a deplasat de la un AP la altul? Din Capitolul 5 se ştie că switch-urile sunt echipamente care auto-învață construindu-şi automat tabelele de comutare. Această auto-învățare rezolvă într-un mod simplist deplasările ocazionale (de exemplu când un angajat este transferat de la un departament la altul); cu toate acestea switch-urile nu au fost proiectate pentru a suporta utilizatori cu un grad înalt de mobilitate care doresc să-şi păstreze conexiunile TCP pe parcursul şi după deplasarea între BSS-uri.

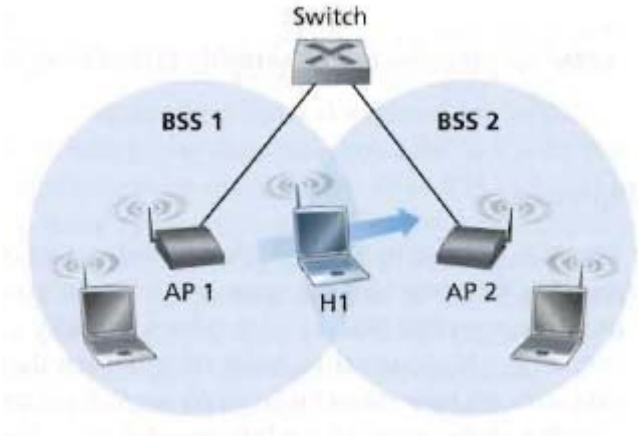


Figura 6.15 Mobilitate în cadrul aceleiaşi subrețele

Pentru aprecierea problemei, trebuie avut în vedere că înainte de deplasare, switch-ul deține o intrare în tabela de comutare care asociază adresa MAC a lui H1 cu interfața prin care această stație e accesibilă (interfața spre AP1). Dacă inițiat H1 se găseşte în BSS1 atunci o datagramă adresată lui H1 va fi direcționată spre H1 via AP1. După asocierea la AP2 însă cadrele trebuie direcționate spre AP2. O soluție este ca AP2 să trimită către switch imediat după noua asociere un cadru Ethernet de

difuzare având ca sursă adresa MAC a lui H1. La recepționarea cadrului switch-ul acesta va actualiza tabela de comutare, permițând ca H1 să fie accesat via AP2. Grupul de lucru IEEE 802.11f dezvoltă un protocol inter-AP pentru soluționarea unor astfel de probleme.

6.3.5 Elemente avansate in IEEE 802.11

Vom încheia discuția despre IEEE 802.11 printr-o scurtă prezentare a două capabilități avansate prezente la rețelele 802.11. Aşa cum vom vedea aceste capabilități nu sunt specificate complet în standardul 802.11, ele fiind posibile prin mecanisme specificate în standard. Aceasta permite diverşilor producători implementarea acestor capabilități prin abordări proprii, stimulând concurența.

Adaptarea ratei de transfer

Din Figura 6.3 se poate observa că diversele tehnici de modulație (ce asigură rate de transfer diferite) sunt adecvate pentru diverse scenarii de SNR. Să considerăm de exemplu un utilizator mobil 802.11 care se află la o distanță de 20 de metri de stația de bază, având un raport semnal zgomot bun. Dat fiind SNR-ul mare, utilizatorul poate comunica cu stația de bază folosind o tehnică de modulație de la nivel fizic ce asigură rate de transfer ridicate menținând erorile la nivel de bit scăzute. Să considerăm acum că utilizatorul devine mobil, depărtându-se de stația de bază; SNR-ul începe să scadă pe măsura creşterii distanței față de stația de bază. Într-un astfel de caz dacă tehnica de modulație utilizată de protocolul 802.11 între stația de bază şi utilizator nu se modifică, BER-ul va deveni inacceptabil pe măsura scăderii SNR-ului ajungându-se la situația în care nici un cadru transmis nu mai este recepționat corect.

Din acest motiv, majoritatea implementărilor 802.11 dispun de capabilitatea adaptării ratei de transfer care selectează în mod adaptiv tehnica de modulație de la nivel fizic pe baza condițiilor de canal curente sau recente. Spre exemplu dacă un nod transmite două cadre consecutive fără a primi o confirmare (indicație implicită a erorilor), rata de transfer este redusă automat la următoarea din listă. Dacă 10 cadre consecutive sunt confirmate sau dacă expiră cronometrul de la ultima reducere a ratei atunci rata de transfer este crescută la următoarea din listă. Mecanismul de adaptare a ratei de transfer este similar algoritmului TCP de control al congestiei, folosind sondarea -- atunci când condițiile sunt bune (se recepționează confirmări) rata de transfer este crescută până când se întâmplă ceva „rău”; când se întâmplă ceva rău rata de transfer este redusă.

Managementul energetic

Principalul avantaj al rețelelor fără fir este că accesarea rețelei nu impune ca nodurile să se afle într-o locație particulară. Pentru a beneficia la maxim de mobilitate, locația nodurilor nu trebuie

să fie limitată de existența unor cabluri de alimentare cu energie electrică. În acest caz, mobilitatea presupune ca nodurile să fie alimentate de la baterii. Se ştie că bateriile pot stoca cantități limitate de energie, fiind necesară reîncărcarea lor periodică prin conectarea la rețea, timp în care utilizatorul nu poate beneficia de mobilitate.

Multe din aplicații necesită durate lungi de funcționare, fără sacrificarea conectivității. Un transceptor radio poate fi activ (transmisie, recepție, aşteptare) sau in adormire. Algoritmii de economisire a energiei încearcă să mențină transceptorul cât mai mult timp în modul adormire, unde consumul este mult mai mic, însă în acelaşi timp este păstrată conectivitatea. Acest fapt este posibil în situația în care nodul mobil nu recepționează sau nu transmite în mod continuu date, schimburile de informații având loc sporadic.

Standardul 802.11 pune la dispoziție capabilități de management energetic pentru minimizarea timpului în care circuitele de aşteptare recepție, recepție şi transmisie sunt în funcțiune. Algoritmul de management energetic 802.11 funcționează astfel: Un nod poate alterna explicit între starea de activitate şi inactivitate (adormire). Un nod va anunța punctul de acces că trece în adormire prin setarea în 1 a bitului management energetic din antetul cadrului 802.11. La nod există un cronometru care activează recepția cu puțin timp înainte ca AP-ul să transmită cadrul baliză (cadrele baliză sunt emise de regulă la 100ms). Întrucât punctul de acces cunoaşte faptul că nodul va trece în adormire (prin intermediul bitului management energetic) acesta (AP-ul) nu va transmite cadrele destinate nodului respectiv ci le va stoca pentru o transmisie ulterioară.

Un nod îşi va activa recepția (tranziția durează cca 250 microsecunde) cu puțin timp înainte ca AP-ul să transmită cadrul baliză. Cadrele baliză transmise de punctul de acces conțin o listă de noduri care au cadre stocate la punctul de acces. Dacă nodul nu are cadre stocate acesta poate trece din nou în adormire. În caz contrar nodul poate solicita explicit printr-un cadru special livrarea mesajelor stocate la punctul de acces. Pentru un interval inter baliză de 100 msec şi un timp de tranziție (trezire) de 250 microsecunde precum şi un timp similar de recepționare şi analiză a cadrului baliză un nod care nu are cadre de transmis sau recepționat poate rămâne în adormire circa 99% din timp, rezultând o economie semnificativă de energie.