
Rețele wireless

Într-o rețea pe cablu, mediul este al tău și nimeni nu îl vede. Într-o rețea fără fir totul se schimbă: mediul este public, oricine din parcare poate asculta, două stații pot să nu se audă între ele deși vorbesc amândouă cu același punct de acces, iar coliziunile nu pot fi detectate - nici măcar în principiu. Fiecare dintre aceste probleme a cerut o soluție proprie, iar cursul acesta le ia pe rând, de la fizica undelor până la protocolul care hotărăște cine are voie să vorbească și la criptarea care ține parcare afară.

Din capitolul precedent.

- Pe un mediu **partajat**, două stații care transmit simultan produc o **coliziune**.
- **CSMA/CD** rezolva asta: ascultă, transmite, iar dacă detectezi coliziune, oprește-te și reîncearcă după un timp aleator.
- Un **domeniu de coliziune** este zona în care două transmisii se pot ciocni.
- Adresa MAC identifică o interfață; cadrul are sursă, destinație și CRC.
- **Modulația** transformă biții într-un semnal transmisibil pe mediu (cursul 1).

OBIECTIVELE CAPITOLULUI

- Să explicați compromisul dintre frecvență, acoperire și debit
- Să spuneți ce a crescut debitul de la 2 Mbps la peste 10 Gbps, pe patru pârghii
- Să distingeți FHSS, DSSS, OFDM și OFDMA
- Să planificați canalele într-o clădire cu mai multe puncte de acces
- Să folosiți corect termenii BSS, IBSS, ESS, SSID și BSSID
- Să explicați de ce CSMA/CD nu funcționează în aer și cum îl înlocuiește CSMA/CA
- Să descrieți problema stației ascunse și modul în care RTS/CTS o rezolvă
- Să alegeți mecanismul de securitate potrivit și să spuneți de ce cele „simple” nu sunt securitate

Astăzi vom vedea că CSMA/CD, mecanismul care a făcut Ethernet-ul posibil, **nu poate fi folosit** în aer. Nu pentru că cineva a decis altfel, ci pentru că fizica nu permite. Iar din această imposibilitate decurge aproape tot ce e specific la 802.11.

11.1 Fizica din spatele deciziilor

Rețelele wireless folosesc **microunde**, o felie din spectrul electromagnetic aflată aproximativ între 1 și 10 GHz. Alegerea nu e arbitrară: rezultă dintr-un compromis cu cinci termeni, pe care merită să îl aveți în minte de fiecare dată când cineva propune „o bandă mai bună”.

Tabelul 11.1 Fizica din spatele deciziilor.

Proprietate	Frecvențe mici	Frecvențe mari
Distanța de propagare	mare	mică
Penetrarea pereților	bună	slabă
Interferențe	multe - banda e aglomerată	puține
Lățime de bandă disponibilă	mică	mare
Costul echipamentelor	mic	mare

De ce frecvențele mari trec mai greu prin pereți. Lungimea de undă este invers proporțională cu frecvența. La 2,4 GHz ea este de circa **12,5 cm**; la 5 GHz, de circa **6 cm**.

O undă „ocoloște” mai ușor obstacolele mai mici decât lungimea ei de undă și este absorbită sau reflectată de cele comparabile ori mai mari. Un perete de 15 cm este, pentru unda de 12,5 cm, un obstacol pe care îl mai poate negocia; pentru cea de 6 cm, e un zid în toată puterea cuvântului.

Același motiv explică de ce radioul FM prinde în tunel, iar Wi-Fi-ul nu: la 100 MHz lungimea de undă e de trei metri.



Figura 11.1 Lungime de undă și buget de semnal.

Comparați 2,4 și 5 GHz la aceeași distanță: pierderea crește cu circa 6,4 dB doar din schimbarea frecvenței, fără niciun perete în plus. Aceasta este, în cifre, explicația pentru care banda de 5 GHz „nu ajunge la fel de departe” - deși puterea emisă e identică. Iar calculul de mai sus este pentru **spațiu liber**: într-o clădire reală se mai adaugă 3–5 dB per perete de gips-carton și 10–15 dB per perete de beton.

11.2 Benzile libere și cine le mai folosește

Tabelul 11.2 Benzile libere și cine le mai folosește.

Tehnologie	Bandă	Aplicație
LoRaWAN	868 MHz (UE)	IoT pe distanțe mari, consum foarte mic, debit minuscul
Zigbee	868 MHz și 2,4 GHz	automatizări, senzori, becuri inteligente
Bluetooth	2,4000 – 2,4835 GHz	periferice, distanțe scurte
Wi-Fi	2,4 / 5 / 6 GHz	rețele locale fără fir
Cuptorul cu microunde	2,45 GHz	nu comunică nimic, dar emite cu sute de wați

Toate acestea funcționează în **benzi ISM** (Industrial, Scientific and Medical), utilizabile fără licență și fără taxă, cu respectarea unor limite de putere. În România, alocările sunt reglementate de **ANCOM**.

Paradoxul benzilor libere. Faptul că banda este liberă explică **simultan** succesul enorm al Wi-Fi și aglomerația din ea. Oricine poate emite acolo, deci echipamentele sunt ieftine și se vând peste tot - și, din exact același motiv, într-un bloc de locuințe banda de 2,4 GHz este astăzi practic inutilizabilă la debit maxim.

Nu există administrator al benzii. Nu se poate reclama nimănui. Singura soluție e să treceți la 5 sau 6 GHz, unde e mai puțină lume - deocamdată.

11.3 Evoluția standardelor 802.11

Tabelul 11.3 Evoluția standardelor 802.11.

Generație	Standard	Bandă	Debit maxim	Modulație / acces	An
Wi-Fi 0	802.11	2,4 GHz	2 Mbps	FHSS / DSSS	1997
Wi-Fi 1	802.11b	2,4 GHz	11 Mbps	DSSS	1999
Wi-Fi 2	802.11a	5 GHz	54 Mbps	OFDM	1999
Wi-Fi 3	802.11g	2,4 GHz	54 Mbps	OFDM / DSSS	2003
Wi-Fi 4	802.11n	2,4 / 5 GHz	600 Mbps	OFDM + MIMO	2009
Wi-Fi 5	802.11ac	5 GHz	6,93 Gbps	OFDM, până la 8 fluxuri	2014
Wi-Fi 6	802.11ax	2,4 / 5 GHz	9,6 Gbps	OFDMA	2019
Wi-Fi 7	802.11be	2,4 / 5 / 6 GHz	~30 Gbps	OFDMA, 4096-QAM	2024

Creșterea de la 2 Mbps la 30 Gbps în mai puțin de trei decenii nu vine dintr-o singură invenție, ci din **patru pârgii** acționate simultan - toate cunoscute deja din cursul 1.

1. **Modulații tot mai dense.** De la BPSK și QPSK la 256-QAM (802.11ac) și 4096-QAM (802.11be). Fiecare pas crește numărul de biți per simbol - și cere, în schimb, un raport semnal-zgomot mai bun. De aceea debitul maxim se obține doar lângă punctul de acces.
2. **MIMO.** Mai multe antene care transmit simultan fluxuri spațiale independente. Patru fluxuri înseamnă, în condiții bune, de patru ori debitul - folosind exact aceeași bandă.
3. **Canale mai late.** De la 20 MHz la 40 MHz (802.11n), 160 MHz (802.11ac) și 320 MHz (802.11be). Banda dublă înseamnă debit dublu - dacă găsiți atâta spectru curat.
4. **Metode mai bune de acces multiplu.** Trecerea de la DSSS la OFDM și apoi la OFDMA.

De ce nu obțineți niciodată debitul de pe cutie. Cifrele din tabel sunt maxime teoretice, obținute cu numărul maxim de antene, la distanță zero, fără alt trafic. În practică se pierd:

- jumătate din debit pe **antetele și confirmările** protocolului (mediul e semiduplex, fiecare cadru cere ACK);
- încă o parte din **partajarea** cu celelalte stații din același BSS;
- încă o parte din **scăderea modulației** odată cu distanța.

Un „Wi-Fi 6 de 1200 Mbps” livrează, realist, 400–600 Mbps la câțiva metri și mult mai puțin în camera alăturată.



Figura 11.2 Pârghia și efectul ei.

11.4 Spreading și acces multiplu

De ce împrăștiem semnalul pe o bandă mai largă decât e nevoie. Pare o risipă: dacă informația încapă în 1 MHz, de ce să ocupăm 20?

Pentru că într-o bandă liberă zgomotul e **punctual și imprevizibil**: cuptorul cu microunde strică o felie, telefonul Bluetooth alta. Un semnal concentrat pe 1 MHz care nimerește peste zgomot este pierdut complet.

Un semnal **împrăștiat** pe 20 MHz pierde doar felia afectată, iar restul e suficient ca receptorul să reconstituie informația. În plus, energia fiind distribuită, semnalul e mai greu de detectat de cineva care nu știe ce caută - motiv pentru care tehnica vine, ca multe altele, din aplicații militare.

Tabelul 11.4 Spreading și acces multiplu.

Tehnică	Cum funcționează	Observație
FHSS Frequency Hopping	emițătorul „sare” între subbenzi după o secvență cunoscută ambelor capete	simplu, dar folosește o singură subbandă la un moment dat; Bluetooth încă îl folosește
DSSS Direct Sequence	fiecare bit este înlocuit cu o secvență fixă de <i>chipuri</i> , care ocupă tot canalul	semnalul se reface chiar dacă o parte din secvență e perturbată
OFDM	banda se împarte în multe subpurtătoare ortogonale , transmise simultan	foarte rezistent la reflexii multiple; baza tuturor standardelor moderne
OFDMA	subpurtătoarele sunt alocate utilizatorilor diferiți , simultan	Wi-Fi 6; transformă un mediu cu conținție într-unul planificat

Analogie pentru OFDM și OFDMA OFDM este un camion cu 64 de compartimente care pleacă spre o singură adresă. Chiar dacă trimiteți un plic mic, camionul pleacă tot. Dacă vreți să livrați la altcineva, așteptați următorul camion.

OFDMA încarcă în **același** camion pachete pentru mai mulți destinatari și le lasă pe rând, pe același drum. Nimeni nu mai așteaptă un camion întreg pentru un plic.

De aceea Wi-Fi 6 nu e mult mai rapid pentru un singur client, dar e dramatic mai bun într-o sală cu o sută de laptopuri - exact scenariul unei săli de curs.

Trei tipuri de „simultan”. MIMO = mai multe fluxuri, pe aceeași frecvență, separate **spațial** (antene diferite).

OFDM = mai multe subpurtătoare, pentru **un singur** utilizator la un moment dat.

OFDMA = aceleași subpurtătoare, împărțite între **mai mulți** utilizatori.

Se combină: un AP Wi-Fi 6 face toate trei în același timp.

11.5 Planificarea canalelor

Banda de 2,4 GHz are aproximativ 85 MHz utilizabili (2400 – 2485 MHz), iar un canal 802.11g ocupă circa **22 MHz**. Canalele sunt însă definite din 5 în 5 MHz - deci se **suprapun** masiv. Rezultă loc pentru exact trei rețele care nu se suprapun deloc: canalele **1, 6 și 11**.



Figura 11.3 Suprapunerea canalelor în banda de 2,4 GHz.

Puneți toate trei punctele de acces pe canalele 1, 6 și 11 - nicio suprapunere. Apoi mutați unul pe canalul 3 și priviți ce se întâmplă: se suprapune parțial și cu 1, și cu 6. A stricat două rețele în loc să evite una.

Greșeala „canalului 3”. Un administrator care alege canalul 3 „pentru că e liber” provoacă interferență parțială atât pe 1, cât și pe 6.

Iar suprapunerea **parțială** este mai gravă decât folosirea **aceluiași** canal. Două rețele pe canalul 1 se aud reciproc și își împart politicos mediul prin CSMA/CA: fiecare așteaptă când cealaltă vorbește. O rețea pe canalul 3 nu este auzită ca semnal valid, deci nimeni nu îi cedează mediul - pentru celelalte, este pur și simplu **zgomot**.

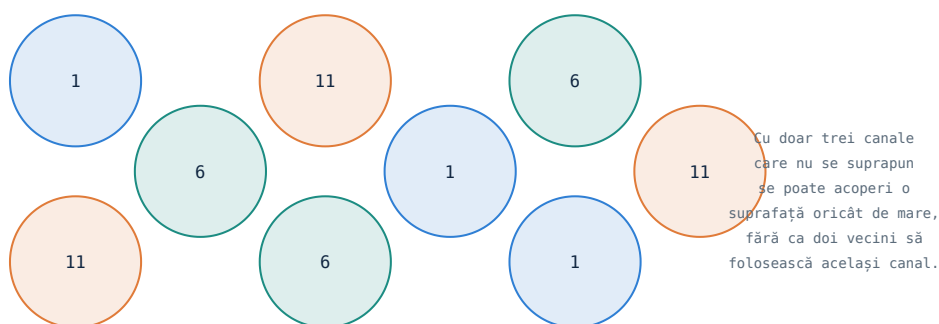


Figura 11.4 Reutilizarea canalelor într-o rețea cu mai multe puncte de acces. Este exact aceeași idee ca la celulele de telefonie mobilă, aplicată la scara unei clădiri.

La 5 GHz problema aproape dispare. Sunt disponibile peste 20 de canale de 20 MHz care nu se suprapun, deci planificarea devine banală. Prețul: acoperire mai mică, deci mai multe puncte de acces pentru aceeași clădire.

Atenție însă la canalele **DFS** (52–140): acolo Wi-Fi-ul este oaspete, iar radarele meteo sunt proprietarul. Dacă echipamentul detectează un radar, este obligat să părăsească imediat canalul - ceea ce înseamnă câteva secunde de întrerupere pentru toți clienții.

11.6 Organizarea unei rețele wireless

Tabelul 11.5 Organizarea unei rețele wireless.

Termen	Ce este
BSS - Basic Service Set	unitatea de bază: una sau mai multe stații plus cel mult un punct de acces
IBSS - Independent BSS	BSS fără punct de acces: rețea ad-hoc, stațiile vorbesc direct între ele
ESS - Extended Service Set	mai multe BSS-uri legate printr-un sistem de distribuție (de regulă rețeaua cablată)
BSSID	identificator de 48 de biți al unui BSS; într-o rețea cu AP este chiar adresa MAC a punctului de acces
SSID	numele rețelei, configurabil de administrator; ceea ce vede utilizatorul în listă



Figura 11.5 De la scanare la roaming.

Echipamentele tipice sunt: adaptoare wireless, puncte de acces, bridge-uri wireless (leagă două segmente cablate prin aer), repetitoare de semnal, antene direcționale sau omnidirecționale și, în instalațiile mari, **controlere WLAN** care administrează central zeci de puncte de acces *lightweight* - acestea din urmă neavând practic configurație proprie.

11.7 Accesul la mediu

Mediul wireless este partajat, exact ca vechiul cablu coaxial. Dar CSMA/CD nu poate fi folosit, din două motive fizice imposibil de ocolit:

De ce nu se poate detecta o coliziune în aer. Motivul 1. O stație nu poate asculta în timp ce transmite. Propriul semnal, la propria antenă, este cu **zeci de ordine de mărime** mai puternic decât orice ar putea recepționa de la distanță. E ca și cum ai încerca să auzi o șoaptă din cealaltă cameră în timp ce strigi.

Motivul 2. Chiar dacă ar putea, coliziunea se produce **la receptor**, nu la emițător. Două stații aflate la 100 m una de alta pot transmite fără să se deranjeze reciproc - dar semnalele lor se pot ciocni perfect la punctul de acces aflat între ele.

Pe cablu, ambele probleme dispar: semnalul e același pe tot firul și o stație își poate compara ce transmite cu ce se aude pe mediu.

Soluția este **CSMA/CA** - Collision *Avoidance* în loc de *Detection*. Dacă nu putem detecta coliziunile, le prevenim.



Figura 11.6 CSMA/CA, pas cu pas.

Tabelul 11.6 Accesul la mediu.

Funcție	Când se folosește	Cum decide cine transmite
DCF - Distributed Coordination Function	întotdeauna, inclusiv în rețele ad-hoc	distribuit, prin CSMA/CA: fiecare stație ascultă, așteaptă DIFS și un backoff aleator
PCF - Point Coordination Function	opțional, doar cu punct de acces	centralizat: AP-ul interoghează pe rând stațiile (polling), într-o perioadă fără contenție

PCF a rămas, practic, pe hârtie. Aproape niciun echipament comercial nu l-a implementat: era complicat și nu aducea destul. Ideea de acces **planificat de AP** a revenit însă, în altă formă și cu mult mai mult succes, prin **OFDMA** în Wi-Fi 6 - unde punctul de acces chiar programează cine transmite și pe ce subpurtătoare.

11.8 Cadrul 802.11



Figura 11.7 Cadrul 802.11 - apăsați pe câmpuri.

De ce patru adrese și nu două. Ethernet are nevoie de două: sursa și destinația, ambele pe același segment.

În aer, cadrul are **patru roluri** potențial diferite: cine îl emite acum, cine îl primește acum, de la cine provine originalul și pentru cine este destinat în final. Într-un BSS obișnuit trei sunt suficiente, pentru că AP-ul este mereu unul dintre capete. A patra apare doar când cadrul sare între două puncte de acces.

11.9 Două probleme care nu există pe cablu

Stația ascunsă

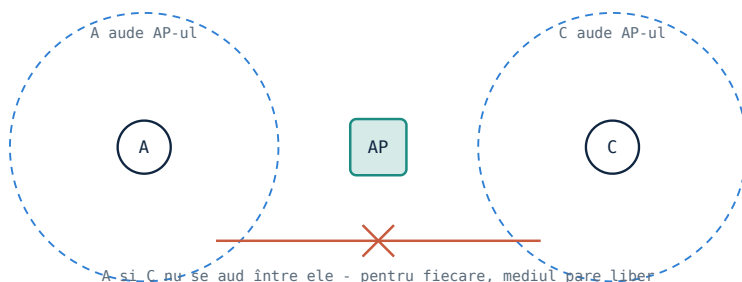


Figura 11.8 Problema stației ascunse. A și C sunt amândouă în raza AP-ului, dar nu în raza celeilalte. Ascultă mediul, îl găsesc liber și transmit simultan; coliziunea se produce la AP, unde niciuna dintre ele nu o poate observa.



Figura 11.9 RTS/CTS rezolvă stația ascunsă.

Stația expusă

Problema simetrică, și mai puțin cunoscută: o stație aude o transmisie și tace, **deși transmisia ei nu ar deranja pe nimeni** - pentru că destinatarii sunt în direcții opuse.

Rezultatul nu este o coliziune, ci **pierdere de capacitate**: mediul stă degeaba deși ar fi putut fi folosit. Soluțiile sunt folosirea de canale diferite, antene direcționale, sau coordonarea centralizată - adică exact ce face OFDMA în Wi-Fi 6.

Cele două probleme, în oglindă. Stația ascunsă: nu aud pe cineva pe care ar trebui să îl aud → transmit când nu trebuie → **coliziune**.

Stația expusă: aud pe cineva pe care nu ar trebui să îl iau în seamă → tac când aș putea vorbi → **capacitate irosită**.

Prima produce erori, a doua produce încetineală. Prima are o soluție standard (RTS/CTS), a doua nu.

11.10 Securitatea rețelelor wireless

Pe cablu, un atacator trebuie să intre în clădire. În aer, îi ajunge să fie în parcare. Diferența aceasta explică de ce securitatea wireless a fost, de la început, o problemă mai grea - și de ce primele soluții au eșuat spectaculos.

Mecanismele care nu sunt securitate

Tabelul 11.7 Mecanismele care nu sunt securitate.

Măsură	Ce pretinde	De ce nu ajunge
Reducerea puterii de emisie	semnalul nu iese din clădire	o antenă direcțională îl captează de la sute de metri; iar recepția e mult mai sensibilă decât emisia
Ascunderea SSID-ului	rețeaua devine invizibilă	SSID-ul apare în clar în cadrele de asociere ale clienților legitimi - e destul să aștepti unul
Filtrarea după adrese MAC	doar dispozitivele cunoscute intră	adresele MAC circulă neprotejate în fiecare cadru și pot fi copiate în câteva secunde

Ascunderea SSID-ului face rău, nu bine. Un dispozitiv configurat pentru o rețea ascunsă nu o poate găsi pasiv, deci trebuie să **întrebe activ**: emite continuu cadre *probe request* cu numele rețelei căutate.

Rezultatul: telefonul dumneavoastră strigă numele rețelei „ascunse” în fiecare cafe-nea, aeroport și stație de metrou prin care treceți. Ați ascuns rețeaua de la locul ei și ați anunțat-o peste tot altundeva.

Toate trei sunt utile ca măsuri de **igienă** - reduc zgomotul și tentativele oportuniste - dar niciuna nu oprește un atacator care știe ce face. Securitatea reală începe la criptare.

Tabelul 11.8 Mecanismele care nu sunt securitate.

Mecanism	Criptare	Autentificare	Statut
Open	niciuna	niciuna	doar pentru rețele publice, cu portal
WEP (1999)	RC4, cheie statică	cheie partajată	spart complet; se sparge în minute
WPA (2003)	TKIP	PSK sau RADIUS	soluție de tranziție, depășită
WPA2 (2004)	AES-CCMP	PSK sau 802.1X	încă acceptabil
WPA3 (2018)	AES, cadre de management protejate (PMF)	SAE în loc de PSK	recomandat

De ce a căzut WEP: vectorul de inițializare. WEP folosea RC4 cu o cheie fixă, la care adăuga un **vector de inițializare** (IV) de doar **24 de biți**, transmis în clar, pentru ca fiecare cadru să fie criptat diferit.

24 de biți înseamnă 16,7 milioane de valori. Într-o rețea încărcată, ele se epuizează în câteva ore - iar de la primul IV repetat se pot deduce informații despre cheie.

Mai rău: atacatorul nu trebuie să aștepte. Poate **injecta** trafic (retransmițând cereri ARP captate) ca să forțeze rețeaua să genereze IV-uri rapid. Din 2007, o rețea WEP se sparge în sub cinci minute, cu unelte publice.

Lecția generală: nu criptarea a fost slabă, ci **modul în care a fost folosită**.

Două îmbunătățiri ale WPA3 merită înțelese, pentru că rezolvă slăbiciuni concrete ale lui WPA2:

- **SAE** (Simultaneous Authentication of Equals) înlocuiește PSK-ul clasic. Cu WPA2-PSK, un atacator care captează strângerea de mână de patru pași poate încerca **offline**, la nesfârșit și fără să atingă rețeaua, dicționare întregi. Cu SAE, fiecare încercare de parolă cere o **interacțiune** cu rețeaua - deci atacul devine lent, detectabil și limitabil.
- **Perfect Forward Secrecy**. Cheia de sesiune se derivă din nou la fiecare conexiune, deci compromiterea parolei **nu** permite decriptarea traficului înregistrat anterior. Cu WPA2, cine avea parola și o captură veche putea citi tot.

DEFINIȚIA 11.1 (PERSONAL ȘI ENTERPRISE). În modul **personal**, toată lumea folosește aceeași parolă - dacă pleacă un angajat, trebuie schimbată pentru toți, pe toate dispozitivele. În modul **enterprise**, fiecare utilizator se autentifică individual, prin **802.1X** și un server **RADIUS**, cu credențiale proprii sau certificat.

Pentru orice rețea de organizație - inclusiv cea a unei facultăți - enterprise este singura variantă gestionabilă: se revocă un singur cont, nu se schimbă o parolă pentru trei mii de oameni.

Rogue AP și evil twin. Cea mai eficientă cale de atac nu este spargerea criptării, ci **păcălirea clientului**: se ridică un punct de acces cu același SSID și semnal mai puternic, iar dispozitivele se conectează singure.

Apărarea nu stă în parolă, ci în **autentificarea reciprocă** - clientul trebuie să verifice certificatul serverului RADIUS, exact ca un browser care verifică certificatul unui site HTTPS. Un dispozitiv configurat să nu valideze certificatul este vulnerabil oricât de puternică ar fi criptarea.

11.11 Greșeli frecvente

Greșeli frecvente.

„Am pus toate AP-urile pe canale libere, 1, 3, 5”

Canalele 3 și 5 se suprapun parțial cu 1 și 6, deci interferează cu tot.

Doar 1, 6 și 11 în banda de 2,4 GHz. Fără excepții.

„Am ascuns SSID-ul, deci rețeaua e mai sigură”

Nu e. Iar clienții își strigă numele rețelei peste tot în lume.

SSID vizibil, WPA3 sau WPA2 cu parolă lungă. Securitatea vine din criptare.

„Am pus canale de 40 MHz pe 2,4 GHz, ca să am debit dublu”

Un canal de 40 MHz ocupă aproape jumătate din bandă și strică ambii vecini.

20 MHz pe 2,4 GHz. Canalele late au sens doar pe 5 și 6 GHz.

„Debitul real e mult sub cel de pe cutie”

Normal: jumătate din timpul mediului se duce pe protocol, ACK-uri și partajare.

Așteptați-vă la 40–50% din cifra teoretică, în cel mai bun caz.

„Am adăugat un repetor ca să acopăr toată casa”

Un repetor retransmite ce aude pe același canal, deci înjumătățește debitul disponibil și ocupă mediul de două ori pentru fiecare cadru.

Un al doilea AP legat prin cablu, pe alt canal. Sau mesh cu radio dedicat.

„Filtrarea MAC ține intrușii afară”

Adresele circulă în clar în fiecare cadru și se pot clona în câteva secunde.

Utilă ca inventar, inutilă ca securitate.

„Am configurat WPA2-Enterprise, dar clienții nu verifică certificatul”

Un evil twin poate captura credențialele oricui.

Configurați explicit validarea certificatului serverului RADIUS pe toate dispozitivele.

11.12 Rezumat și glosar

Ce trebuie să rămână.

- Frecvență mai mare = debit mai mare, dar acoperire și penetrare mai mici. Nu există bandă „mai bună”.
- Debitul a crescut prin **modulație densă, MIMO, canale late și OFDMA**.
- În banda de 2,4 GHz există exact **trei** canale care nu se suprapun: 1, 6, 11.
- **SSID** = numele rețelei; **BSSID** = adresa MAC a unui AP. Roaming-ul păstrează primul și schimbă al doilea.
- CSMA/CD e imposibil în aer: nu poți asculta cât transmiți, iar coliziunea se produce la **receptor**.
- **CSMA/CA**: ascultă, DIFS, backoff aleator, transmite, așteaptă **ACK**.
- Câmpul **Durată** și **NAV**-ul sunt ascultarea „virtuală” a mediului.
- **RTS/CTS** rezolvă stația ascunsă, pentru că CTS-ul AP-ului e auzit de toți.
- Puterea redusă, SSID-ul ascuns și filtrarea MAC **nu sunt securitate**.
- **WPA3 cu SAE** este recomandarea; **Enterprise** este singura variantă gestionabilă într-o organizație.

Exerciții

1. De ce Wi-Fi folosește CSMA/CA în loc de CSMA/CD?
 - a. Pentru ca este mai rapid
 - b. Pentru ca o stație nu poate asculta în timp ce transmite, iar coliziunea se produce la receptor, nu la emitor
 - c. Pentru ca standardul IEEE interzice CD
 - d. Pentru ca nu există coliziuni în aer
2. La ce servește câmpul Durata din cadrul 802.11?
 - a. Măsoară cât a durat transmisia anterioară
 - b. Anunță cât timp va fi ocupat mediul, iar celelalte stații își setează NAV-ul pe această valoare
 - c. Indică vechimea cadrului
 - d. Stabilește intervalul dintre două beacon-uri
3. Ce rezolvă mecanismul RTS/CTS?
 - a. Problema stației expuse
 - b. Problema stației ascunse: CTS-ul AP-ului este auzit de toate stațiile din raza lui, inclusiv de cele care nu aud emitorul
 - c. Creșterea debitului
 - d. Criptarea traficului

4. De ce backoff-ul din CSMA/CA este aleator?
 - a. Ca sa economiseasca energie
 - b. Ca doua statii care au asteptat impreuna sfarsitul unei transmisii sa nu porneasca simultan
 - c. Pentru ca nu se poate masura timpul exact
 - d. Ca sa cripteze transmisia
5. Un administrator pune trei puncte de acces pe canalele 1, 3 si 6. Care este problema?
 - a. Nicio problema, sunt canale diferite
 - b. Canalul 3 se suprapune partial atat cu 1 cat si cu 6, deci interfereaza cu ambele
 - c. Trebuiau puse toate pe acelasi canal
 - d. Canalul 3 nu exista
6. De ce ascunderea SSID-ului nu este o masura de securitate?
 - a. Pentru ca reduce debitul
 - b. Pentru ca SSID-ul apare in clar in cadrele de asociere ale clientilor legitimi
 - c. Pentru ca nu functioneaza pe 5 GHz
 - d. Pentru ca il pot vedea doar administratorii
7. Doua puncte de acces din aceeasi retea, intr-un ESS, au:
 - a. Acelasi SSID si acelasi BSSID
 - b. Acelasi SSID, dar BSSID-uri diferite
 - c. SSID-uri diferite si acelasi BSSID
 - d. SSID-uri si BSSID-uri diferite
8. De ce a fost spart WEP?
 - a. Pentru ca AES era prea slab
 - b. Pentru ca vectorul de initializare avea doar 24 de biti si se repeta rapid, iar atacatorul putea forta generarea lui
 - c. Pentru ca nu folosea deloc criptare
 - d. Pentru ca parolele erau prea scurte
9. Ce aduce nou SAE, in WPA3, fata de PSK-ul din WPA2?
 - a. Cripoteaza mai rapid
 - b. Impiedica atacul de dictionar offline pe strangerea de mana captata
 - c. Elimina nevoia de parola
 - d. Creste raza de acoperire

Note bibliografice

Ultimul curs adună la un loc atacurile care funcționează **în interiorul** rețelei locale - inclusiv cele care exploatează chiar mecanismele studiate în cursurile 3 și 4, de la tabela CAM la protocolul STP - și configurațiile care le opresc.

Laboratorul 7 include construirea și securizarea unei rețele wireless în Packet Tracer, cu planificarea canalelor și WPA2-Enterprise.

- IEEE 802.11 - standardul complet, cu amendamentele a/b/g/n/ac/ax/be
- IEEE 802.11i - mecanismele de securitate care au devenit WPA2
- Wi-Fi Alliance - specificațiile WPA3 și cerințele de certificare
- ANCOM - reglementările pentru benzile ISM în România
- Matthew Gast, *802.11 Wireless Networks: The Definitive Guide*

Extras din volumul „Rețele Locale - Note de curs și lucrări de laborator”. Varianta online a acestui capitol conține figurile în formă interactivă.