Acesta este capitolul 9 — *Reţele IEEE 802* — al ediţiei electronică a cărţii *Reţele de calculatoare*, publicată la Casa Cărţii de Ştiinţă, în 2008, ISBN: 978-973-133-377-9.

Cartea, integrală, poate fi descărcată gratuit de la adresa
`http://www.cs.ubbcluj.ro/~rlupsa/works/retele.pdf`

Capitolul 9

Reţele IEEE 802

Vom studia în continuare standardul utilizat de cele mai multe reţele locale. IEEE 802 defineşte de fapt o familie de tipuri de reţele locale, dintre care cele mai des întâlnite sunt:

- reţele *Ethernet* (de 10, 100 sau 1000 Mbit/s), construite conform standardului IEEE 802.3;
- reţele numite *Wireless Ethernet*, conform standardului IEEE 802.11.

9.1. Reţele IEEE 802.3 (Ethernet)

Cele mai multe reţele locale (reţele cu întinderi geografice reduse, de până la câţiva kilometri) sunt construite pe baza standardului IEEE 802.3 [IEEE 802.3, 2005]. Astfel de reţele mai sunt numite, în mod curent, reţele *Ethernet* (denumirea standardului original, din care a fost dezvoltat standardul IEEE 802.3) sau reţele *UTP 10/100/1000* (UTP vine de la *unshielded twisted pairs — perechi torsadate neecranate* — şi desemnează tipul de cablu utilizat cel mai frecvent în instalaţiile actuale, iar 10/100/1000 sunt capacităţile posibile ale legăturilor, măsurate în megabiţi pe secundă).

Standardul este complex (are peste 1500 de pagini) şi a rezultat în urma unei evoluţii întinse pe mai mult de 20 de ani. În cele ce urmează vom trece în revistă aspectele mai importante.

Componentele din care se realizează o reţea Ethernet sunt:

Interfaţa de reţea sau *placa de reţea* (engl. *Network Interface Card — NIC*) este dispozitivul prin care se conectează un calculator la reţea.

Cablul magistrală. O reţea constrită cu cablu magistrală consta într-un cablu, format din două conductoare izolate între ele, la care sunt

conectate, în paralel, interfeţele de reţea ale calculatoarelor (fig. 9.1). În acest sistem, semnalul emis de orice interfaţă de reţea este recepţionat de toate celelalte interfeţe de reţea conectate la acel cablu.

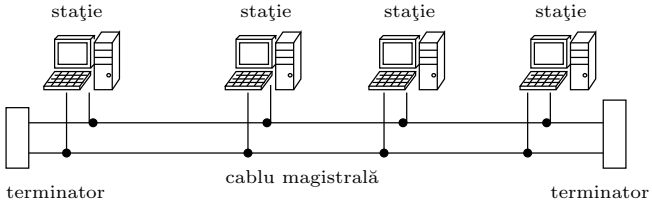


Figura 9.1: O reţea Ethernet construită cu un cablu magistrală

Comunicaţia se face prin pachete de dimensiune variabilă.

Două interfeţe care emit simultan îşi bruiază reciproc semnalele emise; este necesar deci un mecanism de control al accesului la mediu (vezi § 4.2). IEEE 802.3 alege soluţia cu detectarea coliziunilor şi retransmiterea pachetelor distruse de coliziuni.

Deoarece fiecare interfaţă de reţea „aude“ toate pachetele emise în reţea, este prevăzut un mecanism prin care interfaţa să identifice şi să livreze sistemului de operare numai pachetele ce îi sunt destinate. Anume, fiecare interfaţă de reţea are o adresă unică, numită *adresă fizică* sau *adresă MAC* şi fiecare pachet poartă adresa sursei şi adresa destinaţiei.

Repetorul (engl. *repeater*) este un dispozitiv care este conectat la mai multe cabluri de reţea şi copiază pachetele de date de pe fiecare cablu pe celelalte.

Repetorul este conectat la fiecare cablu de reţea întocmai ca o interfaţă de reţea a unui calculator. Interfaţa repetorului către cablul de reţea se numeşte *port*.

Oridecâteori repetorul recepţionează un pachet printr-unul dintre porturile sale (printr-unul din cablurile de reţea conectate la repetor), îl retransmite (repetă) pe toate celelalte cabluri de reţea conectate (toate cu excepţia celui prin care a intrat pachetul). Retransmiterea se face cu întârziere de ordinul duratei câtorva biţi, în orice caz mai puţin decât durata unui pachet. Dacă repetorul recepţionează simultan pachete prin două sau mai multe porturi, consideră că are loc o *coliziune* şi semnalizează acest lucru emiţând, prin toate porturile, un semnal special de anunţare a coliziunii. Acest semnal de coliziune se propagă în toată reţeaua.

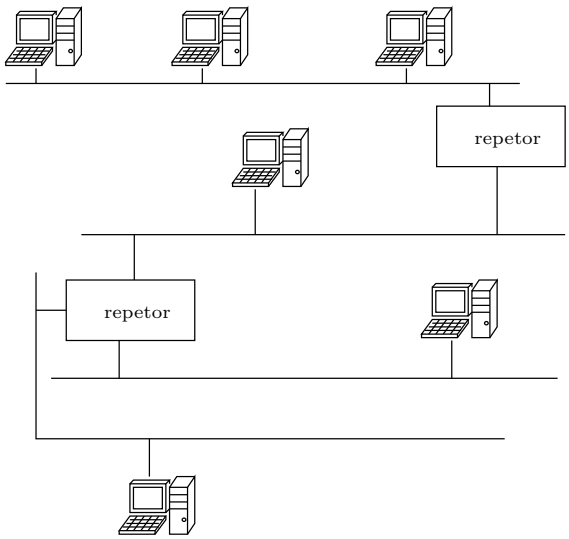


Figura 9.2: O reţea construită din mai multe cabluri magistrală interconectate prin repetoare.

Repetoarele permit construirea unei reţele întinse pe o distanţă mai mare decât lungimea maximă a unui singur cablu (lungime limitată de atenuarea semnalului pe cablu). O reţea construită cu repetoare este desenată în figura 9.2.

Odată cu ieftinirea repetoarelor, a devenit curentă utilizarea câte unui cablu pentru conectarea fiecărui calculator la un repetor. În acest fel, un cablu de reţea va avea legate la el doar două echipamente: fie o interfaţă de reţea şi un repetor, fie două repetoare, fie două interfeţe de reţea (în acest din urmă caz rezultă o reţea formată doar din două calculatoare). De regulă, cablul de legătură folosit în aceste cazuri este o legătură duplex (vezi mai jos) şi poate conecta doar două echipamente. Repetoarele utilizate în această situaţie se mai numesc *hub*-uri (engl. hub = butuc de roată).

Comutatoarele. Un *comutator* (eng. *switch*) este un dispozitiv asemănător cu un repetor, dar cu următoarele modificări:

- este capabil să memoreze câte un pachet întreg pentru fiecare port;
- dacă primeşte simultan două sau mai multe pachete, le memorează şi le retransmite pe rând;
- dacă este posibil, în loc să retransmită un pachet prin toate porturile comutatorului, îl retrimite doar pe calea către interfaţa de reţea

căreia îi este destinat pachetul (a se vedea § 9.1.5 pentru detalii).

Legăturile duplex. Cablurile de legătură între două echipamente pot fi făcute cu căi independente pentru cele două sensuri. Dacă şi echipamentele conectate sunt capabile să emită şi să recepţioneze simultan, este posibilă realizarea unei comunicaţii duplex între cele două echipamente.

Există în cadrul IEEE 802.3 mai multe sub-standarde legate de nivelul fizic, privitoare la cablurile de legătură între echipamente. Cu excepţia debitului de comunicaţie şi a existenţei sau absenţei posibilităţii comunicaţiei duplex, tipul cablului de legătură ales nu afectează restul reţelei.

Pentru echipamente capabile să funcţioneze după mai multe standarde privind nivelul fizic (debite diferite şi mod semi-duplex sau duplex), există un protocol de negociere al modului de transmisie la nivel fizic folosit; acesta va fi studiat în § 9.1.1 cu ocazia prezentării standardului 10 Base T.

9.1.1. Legături punct la punct prin perechi de conductoare

Grupăm la un loc studiul legăturilor punct la punct prin perechi de conductoare datorită multiplelor aspecte comune între toate tipurile de astfel de legături admise de standard.

Toate aceste variante de legături sunt gândite pentru a realiza un cablaj ieftin şi fiabil în interiorul unei singure clădiri.

În toate cazurile, mediul de transmisie este format din două sau patru perechi de conductoare torsadate. Cu cablurile recomandate de standard, lungimea maximă a unei legături este de 100 m.

Condiţiile de izolare electrică şi de pământare nu permit utilizarea sigură pentru legături aeriene prin exteriorul clădirilor. Pentru astfel de scopuri standardul recomandă utilizarea fibrelor optice.

Descriem în continuare particularităţile tuturor standardelor privitoare la nivelul fizic construit pe perechi torsadate.

10 Base T . Este o legătură duplex la 10 Mbit/s utilizând două perechi de conductoare torsadate, câte o perechie pentru fiecare sens (4 conductoare în total). Denumirea standardului vine de la viteza de comunicaţie (10 Mbit/s), codificarea (în banda de bază) şi tipul mediului (*Twisted pairs — perechi torsadate*).

Cablul de legătură constă, aşa cum am văzut, din 4 conductoare izolate. Conductoarele sunt împerecheate 2 câte 2 (formând deci 2 perechi). În cadrul fiecărei perechi, conductoarele sunt răsucite unul în jurul celuilalt

pentru reducerea interferenţelor cu câmpurile electromagnetice din jur. Caracteristicile electrice ale cablurilor, specificate prin standard, sunt în general îndeplinite de către tronsoanele de până la 100 m construite din cablurile folosite în mod curent pentru reţeaua telefonică şi clasificate, în sistemul american de telefonie, *UTP Cat 3*(UTP de la *Unshielded Twisted Pairs — perechi torsadate neecranate*, iar *Cat 3*, de la *Category 3*).

Dăm în continuare, cu titlu informativ, câteva caracteristici:

- impedanţa caracteristică: 100 Ω;
- atenuare: maxim 11,5 dB pentru tot tronsonul de cablu (de fapt acesta este parametrul care limitează lungimea unui tronson de cablu; dacă folosim un cablu cu atenuarea pe 200 m mai mică de 11,5 dB, putem cabla un tronson de 200 m cu astfel de cablu fără probleme);
- timpul de propagare al semnalului: maxim 1000 ns. Standardul cere, în plus, ca viteza de propagare să fie cel puţin $0{,}585 \cdot c$ (adică cel puţin de 0,585 de ori viteza luminii în vid).

Conectarea cablului la interfaţa de reţea sau la repetoare se realizează prin intermediul unui conector cu 8 pini, asemănător cu cel de telefon, standardizat sub numele RJ45.

Utilizarea pinilor este următoarea: emisia între pinii 1 şi 2 şi recepţia între pinii 3 şi 6. Pinii 4, 5, 7 şi 8 sunt neutilizaţi.

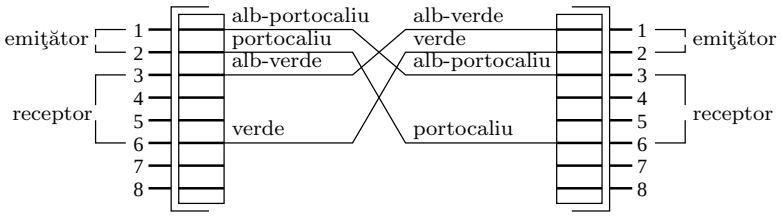
Conductoarele legate la emiţător la un capăt trebuie legate la receptor la celălalt capăt (fig. 9.3). Acest lucru se poate realiza în două moduri:

1. Legarea cablului la conectoare se face „în X“: pinul 1 de pe un conector se leagă la pinul 3 de pe celălalt conector, 2 cu 6, 3 cu 1 şi respectiv 6 cu 2, conform fig. 9.3(a)). Un astfel de cablu se numeşte *cablu inversor* sau *cablu X*.
2. Cablul este „unu-la-unu“(adică pinul 1 de pe un conector este legat cu pinul 1 de pe celălalt conector, 2 cu 2, 3 cu 3 şi 6 cu 6), iar inversarea se face în dispozitivul de la un capăt al cablului, prin legarea inversată a conectorului la circuite: pinii 1 şi 2 la receptor şi 3 şi 6 la emiţător, ca în fig. 9.3(b).

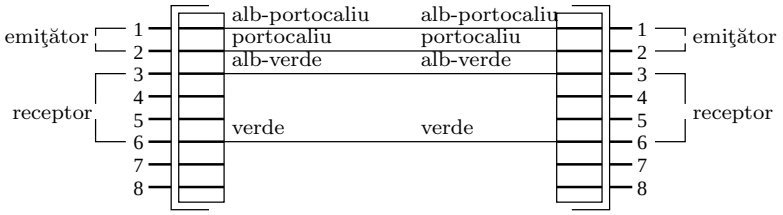
   Standardul recomandă inversarea legăturilor în conectoarele repetoarelor şi cere marcarea conectoarelor cu inversare printr-un simbol „X“.

Conectarea a două echipamente prevăzute cu inversare în conector se face cu ajutorul unui cablu inversor, ca în figura 9.3(c).

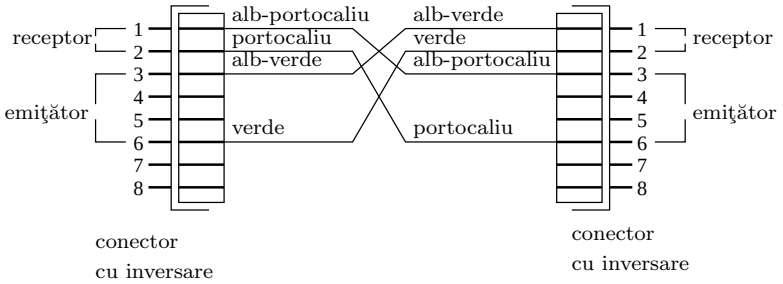
Există şi dispozitive care detectează automat pinii folosiţi la emisie şi recepţie. Aceste dispozitive sunt desemnate *auto MDI/MDIX*. Dacă la unul



(a) Inversare realizată în cablul de legătură



(b) Inversare realizată de unul dintre dispozitivele de la capete



(c) Conectarea a două echipamente prevăzute cu inversare în conector

Figura 9.3: Conectarea a două echipamente 10 Base T. Sunt date şi culorile standard pentru izolaţiile conductoarelor din cablu.

dintre capete se găseşte un astfel de dispozitiv, se poate utiliza atât cablu unu-la-unu cât şi cablu inversor, fără nici un fel de restricţii. Mecanismul de detectare a pinilor utilizaţi se bazează pe pulsurile pentru verificarea mediului, descrise mai jos.

Transmiterea biţilor se face în codificare Manchester. Cele două nivele de tensiune, la emiţător, sunt unul între 2,2 V şi 2,8 V şi celălalt între −2,2 V şi −2,8 V.

Pe lângă transmiterea informaţiei utile, standardul prevede emiterea periodică, de către fiecare echipament, a unui puls de testare a cablului. O interfaţă de reţea sau un repetor care nu primeşte periodic pulsuri de test de la celălalt capăt va „deduce“ că legătura nu este validă. Starea legăturii este semnalată printr-un led; de asemenea, plăcile de reţea semnalează starea legăturii printr-un bit de control ce poate fi citit de driver-ul plăcii de reţea.

O adăugire ulterioară la standard prevede ca în secvenţa de pulsuri de testare a cablului să se codifice disponibilitatea echipamentului ce le emite de a funcţiona în regim duplex sau la o viteză mai mare de 10 Mbit/s (adică conform unuia din standardele descrise mai jos). Un echipament capabil de comunicaţie duplex şi care este informat că echipamentul de la celălalt capăt este capabil de asemenea de comunicaţie duplex va intra automat în mod duplex.

Un echipament vechi, datând dinaintea acestei adăugiri la standard, va funcţiona numai în regim semiduplex. Păstrarea compatibilităţii este asigurată de faptul că echipamentul vechi va înţelege pulsurile doar ca testarea liniei, iar pulsurile generate de el este puţin probabil să coincidă întâmplător cu pulsurile de negociere a modului de transmisie.

100 Base Tx. Este foarte asemănător cu 10 Base T, dar obţine o viteză de transmisie de 100 Mbit/s.

Cablul constă tot din două perechi de conductoare torsadate, însă cu proprietăţi mai bune de transmitere a semnalului (obţine aceleaşi caracteristici de atenuare până la frecvenţe de 10 ori mai mari). Cablurile utilizate sunt cele desemnate *UTP Cat 5*. Lungimea maximă a unui tronson este de 100 m.

Conectoarele şi utilizarea pinilor sunt identice cu 10 Base T. Din acest motiv un cablu pentru 100 Base Tx poate fi întotdeauna utilizat la o legătură 10 Base T.

În general, echipamentele capabile să opereze conform standardului 100 Base Tx sunt capabile să lucreze şi cu 10 Base T. Stabilirea vitezei se face printr-un mecanism similar cu cel utilizat la 10 Base T pentru negocierea modului semiduplex sau duplex. Trebuie însă spus că mecanismul de negociere

nu testează şi calitatea cablului; din acest motiv, dacă legăm o placă de reţea de 100 Mbit/s la un hub sau switch de 100 Mbit/s printr-un cablu ce nu permite 100 Mbit/s (de exemplu *Cat 3* în loc de *Cat 5*), este necesar să configurăm manual viteza de 10 Mbit/s.

100 Base T4. Transmite 100 Mbit/s semi-duplex, utilizând cabluri *Cat 3*. Sunt necesare 4 perechi de conductoare (8 conductoare în total).

Câte o pereche de conductoare este rezervată pentru fiecare sens. Celelalte două perechi se utilizează în sensul în care are loc efectiv transmiterea informaţiei (adică, întotdeauna trei perechi sunt utilizate pentru transmiterea informaţiei şi a patra este temporar nefolosită).

Codificarea informaţiei este mai specială, utilizând 3 nivele de semnalizare în loc de obişnuitele 2 şi transmiţând simultan pe trei canale, pentru a obţine un semnal ce se încadrează în banda de trecere a unui cablu *Cat 3*.

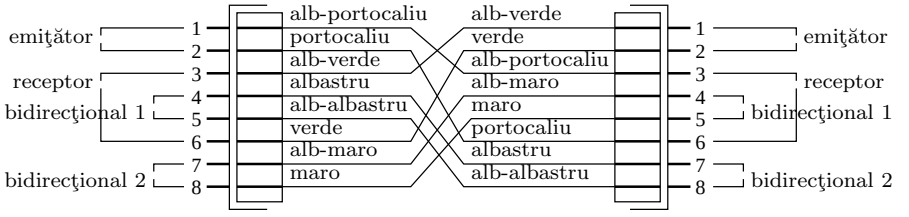


Figura 9.4: Utilizarea pinilor şi conectarea între echipamente la 100 Base T4.

Conectoarele sunt tot RJ45, cu următoarea utilizare a pinilor: emisie: pinii 1 şi 2; recepţie: 3 şi 6, bidirecţional 1: pinii 4 şi 5; bidirecţional 2: pinii 7 şi 8. Ca şi la celelalte cabluri, descrise mai sus, este necesară o încrucişare, realizată fie în cablu, fie în conectorul unuia dintre echipamente. Standardul cere inversarea atât a emisiei cu recepţia cât şi a celor două legături bidirecţionale (fig. 9.4).

Întrucât în majoritatea instalaţiilor sunt disponibile cabluri *Cat 5*, utilizarea standardului 100 Base T4 este extrem de rară.

100 Base T2. Transmite 100 Mbit/s duplex, utilizând două perechi *Cat 3*. Ca şi la 100 Base T4, se utilizează o codificare complicată, însă obţine performanţele lui 100 Base Tx pe cabluri identice cu cele folosite de 10 Base T.

Utilizarea lui este rară, datorită răspândirii cablului *Cat 5*.

1000 Base T. Transmite 1 Gbit/s duplex, utilizând 4 perechi *Cat 5*.

Legătura constă în patru perechi torsadate (8 conductoare) conforme *Cat 5*, de lungime maxim 100 m.

Se utilizează o schemă de codificare mai complicată, ce utilizează fiecare pereche de conductoare în regim duplex.

Conectoarele folosite sunt tot RJ45. Din raţiuni de compatibilitate, legăturile trebuie să realizeze aceeaşi inversare a unor perechi de fire ca şi la 100 Base T4 (fig. 9.4).

Majoritatea plăcilor de reţea şi celorlalte echipamente pentru reţele IEEE 802.3, produse recent şi desemnate *Ethernet gigabit*, implementează standardele 10 Base T, 100 Base Tx şi 1000 Base T.

1000 Base Cx. Transmite 1 Gbit/s duplex utilizând 2 perechi de conductoare de construcţie specală.

Se utilizează câte o pereche pentru fiecare sens.

Standardul permite două tipuri de conectoare: conectoare trapezoidale cu 9 pini (identice cu cele utilizate pentru porturile seriale) sau nişte conectoare cu 8 pini asemănătoare, dar incompatibile, cu RJ45.

Datorită incompatibilităţii cu 10 Base T şi 100 Base Tx, puţine echipamente utilizează 1000 Base Cx.

Realizarea practică a cablajelor

Cablurile *UTP Cat 5* folosite au de obicei 4 perechi de fire torsadate (8 fire în total), invelite toate într-o teacă protectoare. Doar 2 perechi (4 fire) sunt utilizate efectiv de legăturile 10 Base T şi 100 Base Tx.

În cadrul fiecărei perechi, unul din fire are izolaţia într-o culoare plină iar celălalt este combinat, alb alternând cu culoarea firului pereche. Culorile folosite pentru perechi sunt portocaliu, verde, albastru şi maro. Menţionăm că se comercializează, din păcate, şi cabluri în care firele ce ar trebui să fie colorate cu alb plus o culoare sunt doar albe şi, ca urmare, pentru a le identifica este necesar să se desfacă teaca protectoare pe o lungime suficient de mare pentru a vedea cum sunt torsadate firele (care cu care este împerecheat prin răsucire).

Schema de conectare standardizată este dată în tabela 9.1. Varianta „normal“ este utilizată la cablurile unu-la unu, precum şi la unul din capetele cablurilor inversoare. Varianta „inversat“ este utilizată la celălalt capăt al cablurilor inversoare. Varianta „semi-inversat“ a fost utilizată frecvent pentru al doilea capăt al cablurilor inversoare, dar nu funcţionează decât pentru reţele 10 Base T şi 100 Base Tx, care nu utilizează deloc perechile albastru şi maro. Pentru 1000 Base T, varianta „semi-inversat“ nu este prevăzută de standard; ca urmare unele echipamente funcţionează cu astfel de cabluri, iar alte echipamente nu funcţionează.

Nr. pin	Culoare		
	normal	inversat	semi-inversat
1	alb-portocaliu	alb-verde	alb-verde
2	portocaliu	verde	verde
3	alb-verde	alb-portocaliu	alb-portocaliu
4	albastru	alb-maro	albastru
5	alb-albastru	maro	alb-albastru
6	verde	portocaliu	portocaliu
7	alb-maro	albastru	alb-maro
8	maro	alb-albastru	maro

Tabelul 9.1: Ataşarea conectoarelor RJ45

Atragem atenţia că este foarte important să se respecte schema de conectare din următoarele motive:

- Răsucirea firelor afectează transmiterea semnalului şi sensibilitatea la paraziţi. Nerespectarea perechilor, adică utilizarea pentru un circuit a două fire care nu sunt împerecheate prin răsucire, duce la pierderi aleatoare de pachete, cu atât mai multe cu cât cablul este mai lung.
- Este necesar un efort inutil de mare pentru ataşarea corectă a conectorului la al doilea capăt, dacă ataşarea primului s-a făcut nestandard. Amatorii să se gândească la cazul când capătul cablat nestandard se găseşte într-un dulap înghesuit, iar capătul unde trebuie ataşat celălalt conector este câteva etaje mai sus sau mai jos...

Toate sistemele IEEE 802.3 ce utilizează perechi torsadate sunt proiectate pentru legături în interiorul unei singure clădiri. La cablurile trase prin exterior, descărcările electrice din atmosferă riscă să inducă în cablul de reţea tensiuni suficient de mari pentru a distruge plăcile de reţea sau hub-urile sau switch-urile ataşate. Pentru legături exterioare se recomandă utilizarea fibrelor optice.

9.1.2. Legături prin fibre optice

IEEE 802.3 standardizează mai multe tipuri de legături prin fibre optice. Toate acestea sunt foarte similare din punctul de vedere al logicii funcţionării; diferenţele sunt aproape în totalitate aspecte minore legate de realizarea nivelului fizic.

Toate legăturile pe fibră optică sunt punct-la-punct (nu magistrală). Există totuşi un echipament, numit *stea pasivă*, la care se pot conecta mai

multe plăci de reţea şi care distribuie semnalul transmis de o placă spre toate celelalte. Astfel, o stea pasivă se comportă întrucâtva similar cu un cablu magistrală.

O legătură punct la punct constă din două fibre optice, câte una pentru fiecare sens; astfel, fiecare legătură este capabile de transmisie duplex.

10 Base F: standardizează transmisia prin fibră optică la un debit de transmisie de 10 Mbit/s. Rata erorilor, obţinută cu o astfel de legătură, este în jur de 10^{-9} (1 bit eronat la 10^9 biţi transmişi).

Grupează trei variante, cu diferenţe foarte mici între ele (în general, echipamentele corespunzătoare pot fi interconectate fără probleme):

- 10 Base FP, destinat utilizării în configuraţii cu stea pasivă, ca atare funcţionând în mod semi-duplex.
- 10 Base FB, destinat utilizării în conjuncţie cu multe repetoare în cascadă şi funcţionând în mod semi-duplex.
- 10 Base FL, funcţionând în mod duplex.

Se utilizează o fibră optică cu diametrul miezului de 62,5 μm (şi diametrul exterior, al învelişului, de 125 μm), având o viteză de propagare de minim $0{,}67c$, o atenuare de 3,75 dB/km (dacă atenuarea fibrei utilizate este mai mare, lungimea maximă a unei legături trebuie micşorată corespunzător) şi o bandă de 160 MHzkm. Lungimea unui tronson de cablu este maxim 2 km (pentru 10 Base FP, lungimea fiecărei conexiuni dintre placa de reţea şi steaua pasivă este de cel mult 1 km).

Conectarea cablului la echipamente se face cu ajutorul a două conectoare (câte unul pentru fiecare fibră; reamintim că se utilizează o fibră pentru fiecare sens). Conectoarele sunt descrise de standardul IEC 60874-10:1992 sub numele BFOC/2.5. Atenuarea introdusă de conector nu trebuie să depăşească 1 dB, iar puterea undei reflectate nu trebuie să depăşească -25 dB din puterea undei incidente.

Pentru semnalizare se folosesc unde infraroşii cu lungimea de undă cuprinsă între 800 nm şi 910 nm. Nivelul semnalului emiţătorului este între -15 dBm şi -11 dBm pentru 10 Base FP şi între -12 dBm şi -11 dBm pentru 10 Base FB şi 10 Base FL. Nivelul acceptabil pentru semnalul recepţionat este între -41 dBm şi -27 dBm pentru 10 Base FP şi între $-32{,}5$ dBm şi -12 dBm pentru 10 Base FB şi 10 Base FL.

Semnalizarea utilizează codificarea Manchester, întocmai ca în cazul lui 10 Base T.

Spre deosebire de 10 Base T, nu se utilizează pulsuri de testare a legăturii care să permită negocierea modului semiduplex sau duplex sau a vitezei de transmisie; ca urmare, aceşti parametri trebuie configuraţi manual.

100 Base FX: oferă o viteză de transfer de 100 Mbit/s. Pe lângă viteza mai mare, 100 Base FX aduce câteva modificări faţă de 10 Base F, şi anume utilizarea unor conectoare duble (conectând ambele fibre simultan) şi un mecanism de negociere a vitezei de transfer.

1000 Base SX şi 1000 Base LX. Aceste standarde oferă viteză de transfer de 1 Gbit/s.

Varianta 1000 Base SX transmite pe lungimea de undă de 850 nm, prin fibre cu diametrul miezului de 62,5 μm sau de 50 μm. Lungimea maximă de cablu între două echipamente este cuprinsă între 220 m pentru fibră cu dispersie intermodală de 160 MHzkm şi 550 m pentru fibră cu dispersie intermodală de 500 MHzkm.

Varianta 1000 Base LX transmite pe lungimea de undă de 1310 nm, prin fibre multimod de 62,5 μm sau de 50 μm sau monomod de 10 μm. Lungimea maximă de cablu între două echipamente este de 550 m pentru fibra multimod şi 5 km pentru fibra monomod.

9.1.3. Legături prin cablu magistrală

Există două variante de legături prin cablu magistrală standardizate prin IEEE 802.3; ambele variante realizează o viteză de transmisie de 10 Mbit/s.

Cele două variante sunt foarte asemănătoare, motiv pentru care le vom studia împreună.

Mediul de comunicaţie este un cablu format dintr-o pereche de conductoare coaxiale. Impedanţa caractersitică a cablului este de 50 Ω (este deci incompatibil cu cablul utilizat pentru televiziune, care are impedanţa de 75 Ω). Cablul nu are voie să aibă ramificaţii şi trebuie încheiat la ambele capete prin terminatoare. Ramificaţiile sau lipsa terminatoarelor duc la reflexia semnalului la ramificaţie sau la capătul fără terminator, rezultând bruierea semnalului de către reflexia lui.

Pe cablu se leagă, în paralel, interfeţele de reţea şi eventual repetoarele. Derivaţia pentru legătura la interfaţa de reţea este construită special pentru a reduce la minim reflexiile produse (impedanţa emiţătorului şi receptorului este mult mai mare decât impedanţa cablului, anume de cel puţin 100 kΩ); din acest motiv circuitele emiţătorului şi receptorului trebuie plasate la cel mult câţiva centimetri de cablu.

Semnalul este produs în codificare Manchester, cu durata unui bit de 100 ns; de aici viteza brută de transmisie de 10 Mbit/s.

Ca modificare faţă de codificarea Manchester clasică, peste semnal este suprapusă o componentă continuă, în scopul simplificării detectării coliziunilor. Pe cablul în repaus, tensiunea între conductoare este 0 V. Dacă o interfaţă emite date, apare o tensiune continuă între conductorul central şi tresă. Dacă două sau mai multe interfeţe emit simultan, tensiunea continuă creşte peste un anumit prag la care se declară coliziune. La detectarea unei coliziuni, interfeţele de reţea conectate la cablu opresc transmisia, conform metodei CSMA/CD (§ 4.2.2).

Există două sub-standarde privitoare la caracteristicile mecanice şi electrice ale cablului de conectare: *10 Base 5* şi *10 Base 2*.

10 Base 5, numit şi *cablu galben* sau *cablu gros*, prevede utilizarea unui cablu coaxial având aproximativ 10 mm grosime totală, preferabil colorat în galben pentru o mai bună vizibilitate. Lungimea totală maximă a unui cablu este de 500 m. Standardul este gândit pentru cablare prin exteriorul clădirilor.

Denumirea sub-standardului vine de la viteza (10Mbit/s), codificarea (în banda de bază — *Base*) şi lungimea maximă a cablului, în sute de metri.

Cu titlu informativ, dăm câteva detalii, specificate prin standard, cu privire la caracteristicile cablului:

- impedanţa caracteristică: $50\ \Omega \pm 2\ \Omega$;
- viteza de propagare a semnalului: minim $0{,}77 \cdot c$;
- atenuarea: maxim 17 dB/km (8,5 dB pe tot tronsonul de cablu) la 10 MHz şi maxim 12 dB/km (6 dB pe tot cablul) la 5 MHz;
- se acceptă maxim 100 interfeţe de reţea pe un tronson de cablu.

Cablul trebuie conectat la pământ (la instalaţia de pământare a clădirii) *într-un singur punct*. Se specifică explicit prin standard că atât cablul cât şi elementele legate de el trebuie să fie izolate faţă de pământ sau faţă de alte conductoare (cu excepţia sus-menţionatei unice legături de pământare). De asemenea, interfeţele de reţea trebuie să realizeze o izolare electrică între cablul de reţea şi circuitele calculatorului care să reziste la o tensiune de 1500 V. La efectuarea lucrărilor asupra reţelei, persoanele care lucrează trebuie să aibă grijă să nu atingă simultan cablul de reţea şi un conductor legat la pământ, iar în cazul în care conectează sau deconectează două tronsoane de reţea să aibă grijă să nu închidă contactul electric între cele două tronsoane prin corpul lor. Toate aceste măsuri sunt luate deoarece este posibil să apară tensiuni electrice între legăturile de pământarea ale instalaţiilor electrice în clădiri diferite. De

asemenea, este posibil ca într-un cablu, în special dacă este dus prin exterior, să se inducă, inductiv sau capacitiv, tensiuni parazite importante din cauza reţelelor de alimentare electrică din apropiere sau din cauza fulgerelor.

Circuitele electronice ale interfeţelor de reţea sunt împărţite în două module: un modul, conţinând emiţătorul şi receptorul propriu-zise, se ataşează direct pe cablu; al doilea modul cuprinde logică de comandă şi este construit sub forma unei plăci ce se introduce în calculator.

Ataşarea modulului de semnal la cablul de reţea se poate realiza în două moduri:

- prin conectarea celor două segmente de cablu de-o parte şi de alta prin conectoare standardizate (conectoare coaxiale, numite *conectoare N*, cu prindere cu filet);
- prin realizara unei *prize vampir*: se dă o gaură în cablu fără a-i intrerupe conductoarele, prin gaură se introduce o clemă ce va face contact cu firul central, iar legătura cu tresa se face printr-o altă clemă ce se strânge pe o zonă de pe care s-a îndepărtat mantaua exterioară a cablului.

Legătura dintre modulul emiţător-receptor (engl. *transceiver*) şi modulul de logică al plăcii de reţea sau al repetorului este de asemenea standardizată, sub numele de interfaţă AUI. Cablul de legătură dintre cele două module constă din 5 perechi de conductoare torsadate şi ecranate individual, utilizează conectoare trapezoidale cu 15 pini şi poate avea lungime maximă de aproximativ 50m.

10 Base 2 se mai numeşte *cablu subţire*, *cablu negru* sau *cablu BNC* (oarecum incorect, BNC fiind numele conectoarelor prevăzute a fi utilizate pentru acest tip de legătură). Este foarte asemănător cu 10 Base 5, însă foloseşte un cablu mai potrivit pentru cablaje în interior. Lungimea maximă a unui tronson este de 185 m.

Cablul este tot coaxial, dar este mai subţire (≈ 5 mm) pentru a putea fi îndoit mai uşor (standardul cere să poată fi îndoit la raza de 5 cm), în schimb este admis să aibă atenuare mai mare şi, ca urmare, tronsoanele sunt limitate la lungime mai mică.

Dăm din nou câteva caracteristici ale cablului:

- viteza de propagare: $0{,}65 \cdot c$;
- atenuarea, pentru 185 m: maxim 8,5 dB la 10 MHz şi maxim 6 dB la 5 MHz;
- maxim 30 interfeţe ataşate pe un tronson.

Conectarea interfeţelor de reţea şi a terminatoarelor se face prin conectori standardizaţi sub numele *BNC*(conectorii BNC sunt standardizaţi pentru aparatură electronică în general, nu se folosesc doar la reţele Ethernet), astfel (fig. 9.5): Fiecare bucată de cablu trebuie să aibă montate pe capete conectoare BNC mamă. Există elemente numite *joncţiuni T* care conţin o ramificaţie şi sunt prevăzute cu un conector BNC mamă (pe mijlocul T-ului) şi două conectoare BNC tată. La conectoarele tată se ataşează bucăţile de cablu de-o parte şi de alta, iar la conectorul mamă al T-ului se ataşează conectorul tată de pe placa de reţea. Terminatoarele sunt prevăzute cu conector BNC mamă şi se ataşează pe T-urile de la plăcile de reţea extreme.

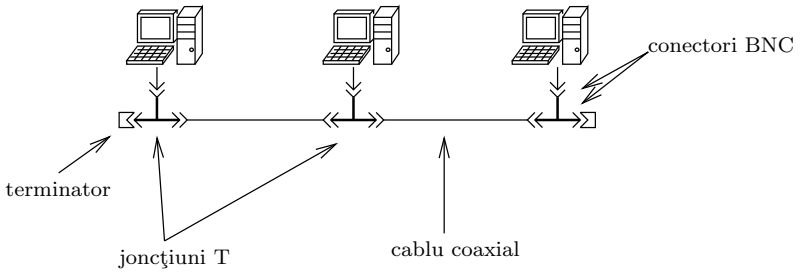


Figura 9.5: Conectarea unei reţele 10 Base 2

Pana cea mai frecventă ce apare la o reţea, afectând conexiunile directe, este întreruperea unui fir (de obicei o pană de contact între sârmă şi conector sau între contactele unui conector). O întrerupere a cablului magistrală duce de regulă la oprirea funcţionării întregii reţele, nu doar „ruperea“ în două a reţelei. Aceasta se întâmplă deoarece capătul de cablu unde s-a produs întreruperea reflectă semnalul (este ca un cablu fără terminator) şi, ca urmare, orice pachet emis pe acel cablu se ciocneşte cu reflexia lui. Soluţia cea mai eficientă de găsire a penei este o căutare binară prin izolarea — neapărat cu terminatoare — a unor porţiuni din ce în ce mai lungi din cablul reţelei.

9.1.4. Repetoarele şi comutatoarele

Ca funcţie în cadrul unei reţele, atât repetorul cât şi comutatorul este un dispozitiv la care sunt conectate mai multe cabluri de reţea şi care, la primirea unui pachet pe un cablu, retransmite pachetul pe toate *celelalte* cabluri conectate. Interfaţa repetorului sau comutatorului către fiecare dintre cabluri se numeşte *port*.

Excepţie făcând cazul comutatoarelor mai evoluate (vezi § 9.1.6.4), o reţea construită cu repetoare sau comutatoare trebuie să aibă o *topologie*

arborescentă, adică între orice două interfeţe de reţea trebuie să existe *un drum şi numai unul* format din cabluri directe şi repetoare sau comutatoare.

Într-o reţea construită corect, arborescent, un pachet emis de o placă de reţea se propagă prin cabluri şi repetoare sau comutatoare din ce în ce mai departe de interfaţa de origine, sfârşind prin a ajunge la toate plăcile din reţea.

În cazul în care reţeaua, în loc să fie arborescentă, conţine circuite, se va întâmpla ca două copii ale aceluiaşi pachet să ajungă pe două căi distincte la un anumit repetor sau comutator. Dacă este un repetor, cele două copii, ajungând aproximativ simultan, vor produce o coliziune. Cum acest lucru se întâmplă cu orice pachet trimis în reţea, fiecare pachet va suferi o coliziune cu el însuşi şi va fi repetat la infinit cu acelaşi insucces, rezultând astfel trafic util nul. În cazul comutatoarelor, dacă două copii ale unui pachet ajung pe două căi diferite la un comutator, acesta le va considera ca fiind pachete distincte. În consecinţă, le va memora şi retransmite, fiecare copie fiind retransmisă inclusiv pe calea prin care a intrat cealaltă copie. În acest fel, copiile ciclează la infinit prin reţea, rezultând o „furtună de pachete“, adică o multiplicare incontrolabilă a pachetelor.

În cazul utilizării repetoarelor, pe lângă topologia în arbore mai trebuie respectate nişte condiţii, şi anume:

- toate componentele legate la repetoare trebuie să lucreze la aceeaşi viteză (fie 10 Mbit/s, fie 100 Mbit/s, fie 1 Gbit/s). Aceasta deoarece un repetor nu memorează pachetul de retransmis şi, ca urmare, nu-l poate retransmite la altă cadenţă a biţilor decât cea cu care îl recepţionează.
- să nu existe mai mult de 4 repetoare de-a lungul nici unui drum între două interfeţe de reţea. Această restricţie este impusă pentru ca diferenţele de viteză de transmisie a repetoarelor şi variaţia întârzierii introduse de repetoare să nu ducă la micşorarea sub o anumită limită a timpului dintre două pachete consecutive.
- întârzierea cea mai mare a transmisiei între două interfeţe de reţea (întârzierea pe cablu plus întârzierea introdusă de repetoare) să nu fie mai mare decât jumătate din durata necesară emiterii unui pachet. Pentru o reţea de 10 Mbit/s, aceasta înseamnă o lungime maximă totală de 2500 m între oricare două interfeţe de reţea.

În cazul switch-urilor, nu apare nici una din limitările expuse mai sus, cu excepţia faptului că pe eventualele legături semi-duplex întârzierea trebuie să fie de cel mult jumătate din durata minimă a pachatului.

La reţele ce utilizează atât switch-uri cât şi repetoare, restricţiile de la repetoare se aplică, separat, pe fiecare subreţea formată din repetoare

interconectate şi legăturile acestora spre interfeţele de reţea şi switch-uri.

9.1.5. Dirijarea efectuată de comutatoare (switch-uri)

Comutatoarele (switch-urile) sunt capabile să realizeze o dirijare primitivă a pachetelor primite. Anume, un comutator ţine o tabelă cu asocierea între adresa fizică (adresa MAC) a unei interfeţe de reţea şi *portul* (conectorul) la care este conectată, direct sau indirect, acea interfaţă.

Dacă un comutator primeşte un pachet cu o anumită adresă MAC sursă, comutatorul va asocia acea adresă cu portul prin care a intrat pachetul. Ulterior, dacă comutatorul primeşte un pachet având ca destinaţie acea adresă MAC, îl va trimite doar prin portul asociat acelei adrese.

Asocierea între adresa MAC şi port este menţinută doar un timp scurt (de ordinul secundei) pentru ca să se asigure actualizarea asocierii în cazul mutării interfeţei de reţea de la un port la altul (prin mutarea fizică a cablului).

Mai multe adrese MAC pot avea asociat acelaşi port; această situaţie apare dacă la acel port este conectat un repetor sau un alt comutator. Unei adrese îi poate fi asociat cel mult un port.

La primirea unui pachet, comutatorul caută portul asociat adresei. Dacă există, va trimite pachetul doar prin acel port. Dacă nu există asociere, pachetul este trimis prin toate porturile cu excepţia celui prin care a intrat. Evident, pachetele de broadcast se încadrează în această din urmă categorie.

9.1.6. Facilităţi avansate ale switch-urilor

9.1.6.1. Switch-uri configurabile

În mod obişnuit, switch-urile nu au parametri configurabili şi nu au adresă; ele sunt transparente faţă de traficul ce trece prin ele.

Switch-urile mai avansate au parametri configurabili. Pentru configurare, este necesar să poată fi accesate de pe un calculator. Accesul se poate realiza în următoarele moduri:

- *Prin intermediul unui cablu serial:* La switch se conectează, prin intermediul unui cablu serial, un teleterminal (sau un calculator care execută un simulator de terminal, de genul *HyperTerm*). Switch-ul oferă o interfaţă text — oferă câteva comenzi de configurare. De cele mai multe ori, există o comandă *help* sau *?* care listează comenzile disponibile.
- *Prin telnet:* Switch-ul se prezintă ca şi cum ar mai avea intern o interfaţă de reţea conectată la el însuşi. Această interfaţă de reţea are o adresă MAC (adesea scrisă pe eticheta aplicată pe carcasă) şi o adresă IP

configurabilă (adresa IP iniţială se configurează prin intermediul conexiunii seriale descrise mai sus). Conectarea prin *telnet* la adresa IP a switch-ului (pe portul standard al protocolului telnet, anume 23) oferă acces la interfaţa de configurare prezentată mai sus. Evident, pentru împiedicarea configurării switch-ului de către persoane neautorizate, switch-ul permite configurarea unei parole, care este cerută la conectare.

- *Prin interfaţă web:* Ca şi la conectarea prin telnet, switch-ul prezintă o adresă IP. Administratorul se poate conecta cu orice navigator web la această adresă şi va primi pagini ce conţin parametrii actuali şi formulare pentru modificarea parametrilor. Ca şi în cazul configurării prin telnet, accesul poate şi este recomandabil să fie restricţionat prin parolă.

Pentru cazul uitării parolei, există o procedură de revenire la configurarea implicită. Aceasta constă de obicei în apăsarea unui buton de reset timp de 10–15 secunde sau punerea sub tensiune a switch-ului în timp ce se ţine apăsat butonul de reset.

9.1.6.2. Filtrare pe bază de adrese MAC

Unele switch-uri pot fi configurate să nu accepte, pe un anumit port, decât pachete ce provin de la o anumită adresă MAC sau de la o adresă dintr-o anumită listă. De asemenea, un pachet destinat unei adrese MAC dintr-o astfel de listă nu va fi trimis decât prin portul pe a cărui listă se găseşte adresa.

Această facilitate este introdusă pentru a împiedica eventuali intruşi să intre în reţea racordându-se pur şi simplu la prizele de reţea accesibile.

Deşi îmbunătăţeşte securitatea unei reţele, soluţia are câteva limitări:

- lista adreselor asociabile unui port este limitată (de multe ori la 8 sau 16 adrese);
- multe plăci de reţea permit schimbarea (prin soft) a adresei MAC.

9.1.6.3. Trunking

Prin *trunking* se înţelege utilizarea mai multor cabluri în paralel ca legătură între două switch-uri. În acest fel, traficul ce se poate stabili între acele două switch-uri este suma capacităţilor legăturilor configurate în trunking.

Porturile utilizate în regim trunking trebuie configurate pe ambele switch-uri. Este de asemenea posibil ca legarea în trunking să utilizeze o extensie a protocolului IEEE 802.3 care este proprietatea firmei producătoare a switch-ului; în acest caz este posibil ca două swithc-uri realizate de firme diferite să nu se poată lega în trunking.

9.1.6.4. Legături redundante

IEEE 802.1D [IEEE 802.1D, 2004] prevede un protocol pentru descoperirea şi dezactivarea ciclurilor (în sensul teoriei grafelor) formate de legăturile dintre switch-uri.

Majoritatea switch-urilor nu implementează însă acest algoritm şi, ca urmare, în majoritatea cazurilor existenţa ciclurilor duce la „furtuni de pachete“ (multiplicarea incontrolabilă a pachetelor în reţea).

Dacă toate swicth-urile de pe traseul unui ciclu implementează protocolul de descoperire a ciclurilor, ele colaborează automat pentru dezactivarea uneia dintre legături şi utilizarea doar a unui arbore parţial al grafului iniţial al legăturilor. La căderea unei legături, switch-urile vor colabora pentru reactivarea unei legături dezactivate, în vederea păstrării conexităţii reţelei.

Menţionăm că, în cazul existenţei unui ciclu, nu este posibilă împărţirea traficului între drumurile alternative. Unul din drumuri va fi obligatoriu dezactivat complet, cât timp celălalt este funcţional.

9.1.6.5. Reţele virtuale (VLAN)

Mecanismul de *reţele virtuale* (*Virtual Local Area Network*) constă în împărţirea unei reţele fizice în mai multe reţele virtuale disjuncte. Fiecare reţea virtuală se comportă exact ca o reţea IEEE 802.3 independentă. Constructiv, reţelele virtuale partajează aceleaşi echipamente (comutatoare, cabluri sau chiar plăci de reţea).

A nu se confunda VLAN cu *VPN* (*Virtual Private Network — reţea privată virtuală* — descrisă în § 10.7.4).

Partiţionarea în VLAN-uri poate fi dezirabilă din mai multe motive, cum ar fi: limitarea traficului de broadcast sau separarea traficului din motive de securitate.

Există două posibilităţi de construcţie a VLAN-urilor.

O primă posibilitate constă în partiţionarea porturilor unui switch. În acest fel, un switch se comportă ca mai multe switch-uri (virtuale) independente, fiecare având doar o parte a porturilor switch-ului fizic. Un port al unui switch poate să aparţină doar unui singur VLAN.

O a doua posibilitate este cea definită în [IEEE 802.1Q, 2003]. Fiecare VLAN constă dintr-o parte din echipamentele (interfeţe de reţea, cabluri şi switch-uri) reţelei fizice; VLAN-uri distincte pot partaja în voie echipamente fizice. Astfel, fiecare interfaţă de reţea aparţine unuia sau mai multor VLAN-uri, fiecare cablu aparţine unuia sau mai multor VLAN-uri şi fiecare port al fiecărui switch aparţine unuia sau mai multor VLAN-uri. Fiecare switch, la primirea unui pachet de broadcast sau pentru a cărui destinaţie nu are asociere,

va trimite pachetul prin toate porturile aparţinând VLAN-ului pachetului, cu excepţia portului prin care a intrat pachetul.

Pentru ca mecanismul descris mai sus să poată funcţiona, este necesar ca, pe cablurile ce aparţin mai multor VLAN-uri, pentru fiecare pachet să se poată deduce cărui VLAN aparţine. Pentru aceasta, fiecare pachet este etichetat cu un *identificator de VLAN* (*VLAN-ID*); acest VLAN-ID este un număr reprezentabil pe 12 biţi.

Pentru păstrarea compatibilităţii cu echipamentele ce nu suportă VLAN-uri 802.1Q, un segment de reţea care aparţine doar unui singur VLAN poate fi configurat să utilizeze pachete neetichetate; switch-ul ce realizează legătura dintre un astfel de segment şi restul reţelei fizice realizează adăugarea şi eliminarea etichetei de VLAN pe pachetele ce tranzitează spre, respectiv dinspre, restul reţelei. Echipamentele incompatibile 802.1Q pot fi montate doar pe cabluri prin care trac pachete neetichetate.

O placă de reţea compatibilă 802.1Q poate fi configurată să facă parte din mai multe VLAN-uri. Pentru aceasta, ea se montează pe un cablu prin care trec pachete etichetate. Placa de reţea se comportă ca şi când ar fi de fapt mai multe plăci de reţea, virtuale, câte una în fiecare VLAN. Fiecare placă virtuală are asociat un VLAN-ID, primeşte doar pachetele ce poartă acel VLAN-ID şi marchează cu VLAN-ID-ul său toate pachetele emise.

Pe fiecare switch trebuie configurate porturile care aparţin fiecărui VLAN. De asemenea, pentru fiecare port trebuie stabilit dacă utilizează pachete etichetate (cu VLAN ID-ul) sau pachete neetichetate. Un port ce utilizează pachete neetichetate poate aparţine unui singur VLAN.

9.1.7. Considerente privind proiectarea unei reţele

Proiectarea şi construcţia unei reţele Ethernet este în general extrem de uşoară; acesta este şi unul din motivele popularităţii Ethernet-ului.

De obicei este necesar să se construiască o reţea în care toate calculatoarele să se „vadă“ între ele (la nivel de reţea Ethernet; controlul accesului la diversele resurse oferite de sisteme se face prin soft, la nivel superior). Tot ce este necesar în acest caz este să se amplaseze un număr de switch-uri şi cabluri astfel încât fiecare calculator să fie legat la un switch şi switch-urile să fie legate între ele într-o reţa conexă şi fără „bucle“.

Se utilizează de obicei o structurare ierarhică a legăturilor (aşa-numita *cablare structurată*): de la calculatoarele dintr-o încăpere sau eventual 2–3 încăperi vecine se adună cablurile într-un switch, iar de la aceste switch-uri se adună cabluri către un switch central. Pentru reţelele mai mari, între switch-ul central şi switch-urile asociate încăperilor se mai adaugă un nivel.

În instalaţiile mici şi fără pretenţii, cablurile se duc aparent şi se fixează de pereţi sau pe mobilă numai acolo unde este strict necesar. Uşurinţa realizării şi reconfigurării este plătită prin faptul că apar dificultăţi la curăţenie, cablurile se degradează uşor dacă se calcă pe ele şi, în sfârşit, se mai întâmplă ca cineva să se împiedice de un cablu, rezultând echipamente trase pe jos sau cabluri smulse din conectoare.

Pentru evitatarea neajunsurilor expuse mai sus, se preferă să se tragă cablurile prin paturi de cablu, tuburi îngropate (ca la instalaţiile electrice) sau prin tavane false. Deoarece astfel de cablaje se modifică mai dificil, este bine să se aibă în vedere posibilele modificări ce ar putea fi de dorit în viitor. Asta înseamnă:

- Să se prevadă mai multe cabluri de la posibile amplasamente de calculatoare la amplasamentul switch-ului asociat încăperii. Cablurile neutilizate nu e necesar să aibă toate loc în switch; se vor conecta sau deconecta după necesităţi.
- Să se prevadă 2–3 cabluri de la switch-urile corespunzătoare unei încăperi la switch-ul central. Astfel, dacă va fi nevoie să se construiască două reţele distincte, o parte din calculatoarele din încăpere conectându-se la o reţea şi altele la altă reţea, se vor pune două switch-uri în încăpere, fiecare conectat prin câte un cablu la switch-ul central.

9.2. Reţele IEEE 802.11 (Wireless)

9.2.1. Arhitectura reţelei

Elementul de bază într-o reţea wireless [IEEE 802.11, 1999] este *celula wireless* (termenul original conform standardului este *Basic Service Set* — BSS). O celulă wireless este formată din mai multe staţii (STA) situate într-o zonă geografică destul de restrânsă (de ordinul câtorva zeci de metri) pentru ca semnalul emis de fiecare staţie să fie recepţionat de toate staţiile din celulă.

Fiecare celulă are asociat un identificator de 48 de biţi, unic, numit *Basic Service Set ID* — BSSID. Acest identificator este înscris în fiecare pachet de date vehiculat în reţea, astfel încât pentru orice pachet de date recepţionat prin antenă se poate determina celula wireless căreia îi aparţine. Mai multe celule wireless pot coexista în aceeaşi zonă, traficul din cadrul fiecărei celule putând fi distins pe baza BSSID-ului de traficul celorlalte celule.

Fiecare staţie aparţine (este asociată) la un anumit moment cel mult unei celule. Asocierile sunt dinamice — o staţie poate să intre sau să iasă

oricând dintr-o celulă. Fiecare staţie se identifică printr-o *adresă* unică de 48 de biţi, numită în mod curent *adresa MAC* a staţiei.

Accesul la mediu este controlat în principal prin metode bazate pe urmărirea traficului pe mediu, detectarea coliziunilor şi, într-o anumită măsură, metode de rezervare în prealabil a accesului la mediu. Acestea vor fi descrise în detaliu în § 9.2.2.

Prezenţa unei celule wireless organizate într-o anumită zonă este manifestată prin emiterea periodică de către una dintre staţii a unui pachet special, numit *beacon*. Pe lângă BSSID-ul celulei, pachetele *beacon* mai conţin un şir de caractere numit SSID sau uneori *numele reţelei* (engl. *network name*). Acest şir este fixat de administratorul reţelei şi serveşte la identificarea reţelei pentru utilizatorii umani.

O staţie poate obţine lista celulelor active în zona sa ascultând pachetele *beacon*. Lista afişată utilizatorului va conţine SSID-urile reţelelor.

Există două moduri de lucru în care poate funcţiona o reţea 802.11:

- Reţea formată dintr-o singură celulă independentă, neconectată prin mijloace IEEE 802 de alte echipamente. În terminologia standardului, o astfel de celulă se numeşte *Independent BSS* — IBSS; în mod curent reţeaua astfel formată se numeşte *ad-hoc*.
- Reţea formată din una sau mai multe celule, operând împreună şi posibil conectate la o infrastructură IEEE 802 (de exemplu la o reţea Ethernet — 802.3). Un astfel de mod de lucru se numeşte *mod infrastructură* sau *managed*.

În mod infrastructură, în cadrul fiecărei celule există o staţie care are rolul legării celulei la infrastructură (altfel spus, la restul reţelei IEEE 802.11). O astfel de staţie poartă denumirea de *Access Point* — AP. Un AP este o staţie, şi ca atare are o adresă MAC. Într-o celulă a unei reţele de tip infrastructură, o staţie ce intră sau iese dintr-o celulă trebuie să anunţe AP-ul responsabil de celula respectivă.

AP-ul este responsabil de generarea pachetelor *beacon* şi BSSID-ul celulei este adresa MAC a AP-ului.

AP-urile unei aceleiaşi reţele 802.11 trebuie să fie interconectate, formând aşa-numitul *Distribution System* (DS). DS-ul poate fi conectat la alte reţele din familia IEEE 802 prin intermediul unor dispozitive numite *portal*-uri. Celulele din aceeaşi reţea vor avea acelaşi SSID.

Standardul original nu prevede nimic în legătură cu modul de conectare a AP-urilor şi deci de realizare a DS-ului. Ca urmare, fiecare fabricant de AP-uri şi-a construit propriul protocol de comunicare inter-AP. Ulterior IEEE a

emis un standard, [IEEE 802.11F, 2003], care fixează un protocol de comunicare între AP-uri.

De obicei un dispozitiv vândut sub numele de *access point* conţine un AP şi un portal către reţele Ethernet. Un astfel de dispozitiv prezintă un modul radio prin intermediul căruia se comportă ca o staţie cu rol de AP şi un conector Ethernet. Într-o primă aproximaţie, un astfel de dispozitiv poate fi privit ca un *switch* conectat pe de o parte la fiecare dintre staţiile membre ale celulei şi pe de altă parte la un dispozitiv Ethernet.

Unele *access point*-uri ce se găsesc în comerţ oferă funcţionalităţi suplimentare faţă de un AP combinat cu un portal. Aceste funcţii sunt oferite prin extensii ale protocolului şi ca urmare pot fi utilizate de regulă doar împreună cu echipamente produse de aceeaşi firmă. Funcţionalităţile sunt:

- funcţie de *switch* (punte) între o reţea Ethernet (fixă) şi o celulă *wireless*, acţionând însă ca şi staţie oarecare (nu AP). Această funcţie se numeşte *wireless bridge* sau *AP client* (uneori există funcţii cu ambele nume, cu diferenţe minore între ele);
- funcţie de AP, dar utilizând tot reţeaua *wireless* pentru partea de infrastructură. În acest mod, dispozitivul este în acelaşi timp AP pentru o celulă şi staţie oarecare în altă celulă, iar a două legătură este utilizată pentru dirijarea spre reţeaua fixă a datelor din celula în care dispozitivul este AP.

9.2.2. Accesul la mediu

Deoarece într-o reţea 802.11 avem un mediu partajat între mai mulţi emiţători, este necesar să avem un mecanism de control al accesului la mediu. Metoda de control al accesului la mediu în IEEE 802.11 se numeşte *Carrier-Sense Multiple Access with Collision Avoidance* (CSMA/CA; rom: acces multiplu cu detectarea semnalului purtător şi evitarea coliziunilor).

În principal, strategia de control al accesului la mediu se bazează pe detectarea coliziunilor şi repetarea pachetelor ce au suferit coliziuni, adică aceeaşi strategie ca şi pentru *Ethernet*-ul pe cablu coaxial.

Datorită condiţiilor specifice reţelelor fără fir, sunt aduse câteva modificări. În principal, la transmisia radio nu există o delimitare comună între zonele de acţiune pentru diverse staţii din aceeaşi celulă: este posibil ca o staţie B să recepţioneze bine transmisia staţiei A, staţia C să recepţioneze transmisia lui B, dar staţia C să nu recepţioneze transmisia lui A. Într-un astfel de caz, dacă A şi C transmit simultan, pachetele emise se ciocnesc la B, dar deoarece nici

una din staţiile A şi C nu recepţionează transmisia celeilalte ele nu au cum să detecteze coliziunea.

În reţelele IEEE 802.11, o staţie care doreşte să trimită un pachet va trimite întâi un pachet de control, numit *Request To Send* (RTS; rom: *cerere de transmisie*), în care specifică destinatarul şi durata de timp necesară transmiterii pachetului. Dacă destinatarul a primit pachetul RTS şi este liber, va trimite înapoi un pachet de control *Clear To Send* (CTS; rom: *accept transmisia*). La primirea pachetului CTS, emiţătorul trimite pachetul de date.

O staţie care recepţionează un pachet CTS destinat altei staţii nu are voie să trimită nimic pe durata rezervată de pachetul CTS, pentru a nu interfera cu transmisia acceptată prin acel CTS. Această restricţie trebuie respectată şi în cazul recepţiei unui pachet CTS destinat altei reţele din aceeaşi zonă (adică purtând un BSS-ID diferit).

Utilizarea pachetelor RTS şi CTS nu este obligatorie. Pentru pachetele mici este preferabilă trimiterea direct a pachetului de date şi repetarea acestuia în cazul unei coliziuni. Pentru pachetele de *broadcast*, utilizarea RTS şi CTS este imposibilă; ca urmare un pachet de broadcast este trimis direct.

9.2.3. Generarea pachetelor *beacon*

În modul infrastructură, pachetele *beacon* ale unei celule sunt generate exclusiv de către AP-ul celulei.

În modul ad-hoc, generarea pachetelor *beacon* este făcută distribuit, de către toate staţiile membre ale celulei IBSS. Simplificat, o staţie care nu recepţionează un *beacon* într-un anumit interval de timp predefinit generează ea însăşi pachetul *beacon*.

9.2.4. Securitatea reţelelor 802.11

Deoarece la reţelele 802.11 comunicaţia este prin unde radio, a căror domeniu de acţiune nu poate fi net limitat, utilizarea unor metode care să asigure confidenţialitatea şi integritatea datelor transportate este esenţială.

Există mai multe mecanisme de securitate ce pot fi utilizate. În cadrul unei celule se poate utiliza, la alegere, unul singur dintre acestea:

- *Open system*: înseamnă, de fapt, lipsa oricărui mecanism de securitate. Se utilizează acolo unde se doreşte să se ofere acces public la Internet. De remarcat însă că, datorită lipsei oricărui mecanism de confidenţialitate sau asigurarea integrităţii mesajelor, oricine poate asculta sau modifica comunicaţia oricui în cadrul celulei.
- *Wired Equivalent Privacy — WEP* (rom. *securitate echivalentă cu reţeaua cablată*): oferă confidenţialitate şi autentificarea şi verificarea integrităţii

mesajelor. În acest scop, toţi membrii celulei trebuie să cunoască o anumită cheie de lungă durată, numită *pre-shared key* (rom. *cheie partajată în prealabil*); această cheie trebuie dată de utilizator la iniţierea celulei sau, după caz, la introducerea staţiei în celulă. Criptarea se face utilizând cifrul RC4, cu o cheie construită din secretul partajat şi dintr-un *vector de iniţializare* ales aleator, pentru fiecare pachet, de către emiţător şi transmis în antetul pachetului. Controlul integrităţii pachetului este făcut tot pe baza secretului partajat. WEP are două slăbiciuni: pe de o parte, datorită existenţei unei slăbiciuni a cifrului RC4 (există câteva chei slabe, foarte uşor de spart), WEP poate fi spart destul de uşor; pe de altă parte, modelul de securitate oferit este destul de neflexibil.

- *WiFi Protected Access — WPA*: corectează problemele WEP, păstrând compatibilitatea cu plăcile de reţea existente. În privinţa criptării, WPA păstrează cifrul RC4 din motive de compatibilitate, dar vine cu o schemă diferită de gestiune a cheilor de criptare, capabilă să evite cheile slabe.

  În privinţa obţinerii unui model de securitate mai flexibil, WPA are două moduri de lucru:

  - *WPA-Personal*, numit şi *WPA-PSK* (de la *Pre-Shared Key*), în care se utilizează un secret partajat între toţi membrii celulei, fiind similar cu WEP (dar mult mai sigur).
  - *WPA-Entreprise*, în care cheile se obţin pe baza unor chei individuale ale utilizatorilor. Controlul accesului şi obţinerea cheilor se face printr-un mecanism numit *Extensible Authentication Protocol* (*EAP*), descris mai jos.

- *IEEE 802.11i* [IEEE 802.11i, 2004], numit şi *WPA2*, extinde *WPA* adăugând, între altele, posibilitatea utilizării cifrului AES. Ca şi în cazul *WPA*, există două moduri de lucru, cu cheie partajată în prealabil sau utilizând *EAP*.

Protocolul de autentificare extensibil, *EAP* [RFC 3748, 2004], este un protocol generic, ce permite utilizarea mai multor scheme de autentificare. *EAP* este utilizat şi de alte protocoale în afară de *WPA* şi *WPA2*, şi anume poate fi utilizat în cadrul legăturilor *PPP* [RFC 1661, 1994], precum şi pentru autentificarea conectărilor la o reţea cablată IEEE 802.3, conform [IEEE 802.1X, 2001].

Arhitectura *EAP* conţine următoarele componente:

- *clientul* ce trebuie să-şi dovedească identitatea în scopul obţinerii accesului

la reţea. Rolul clientului îl are placa de reţea 802.11 (sau placa de reţea 802.3 sau clientul PPP). În terminologia *EAP*, acesta este numit *supplicant*.

- *punctul de acces* este entitatea care trebuie să autentifice clientul pentru a-i oferi acces la serviciile reţelei. Rolul de punct de acces îl are AP-ul 802.11 (sau switch-ul 802.3 sau serverul PPP). În terminologia *EAP*, acesta se numeşte *authenticator*.
- *serverul de autentificare* este entitatea care deţine baza de date cu cheile clienţilor şi realizează efectiv autentificarea.

Protocolul *EAP* prevede un schimb de mesaje între client şi serverul de autentificare. Dacă serverul de autentificare este distinct faţă de punctul de acces, comunicaţia dintre client şi serverul de autentificare trece prin punctul de acces, iar porţiunea din calea de comunicaţie dintre punctul de acces şi serverul de autentificare este protejată criptografic pe baza unui secret partajat între punctul de acces şi serverul de autentificare. Serverul de autentificare este de obicei un server RADIUS.

Unele dintre mecanismele efective de autentificare utilizabile în cadrul *EAP* sunt:

- *EAP-MD5* prevede că serverul de autentificare trimite clientului un număr aleator, iar clientul răspunde cu dispersia MD5 a concatenării numărului aleator cu parola clientului. Funcţionarea mecanismului necesită ca serverul să aibă în baza de date, în clar, parola clientului. *EAP-MD5* permite doar autentificarea clientului, nu şi stabilirea unor chei pentru criptarea sau autentificarea mesajelor.
- *EAP-TLS* necesită ca atât clientul cât şi serverul de autentificare să aibă prestabilite chei secrete SSL/TLS, iar fiecare dintre ei să aibă certificatul TLS al celuilalt (vezi şi § 11.3.2.5). Se stabileşte o conexiune TLS între client şi serverul de autentificare, utilizând certificatele acestora, iar în cadrul acestei conexiuni stabilesc cheile pentru comunicaţia ulterioară între client şi punctul de acces.
- *PEAP* (de la *Protected EAP*) prevede utilizarea TLS pentru deschiderea unei conexiuni securizate între client şi serverul de autentificare, însă doar serverul are o cheie TLS, clientul autentificând serverul pe baza certificatului corespunzător. După deschiderea conexiunii TLS, urmează autentificarea clientului de către server, iar în caz de succes are loc negocierea cheilor pentru securizarea comunicaţiei între client şi punctul de acces. În terminologia *PEAP*, conexiunea *TLS* se numeşte *mecanismul exterior de autentificare*, iar mecanismul de autentificare a clientului

se numeşte *mecanismul interior*. Mecanismul interior cel mai răspândit este *MSCHAP*, care este un mecanism similar cu *EAP-MD5*.