UNIVERSITATEA TEHNICĂ CLUJ-NAPOCA

DEPARTAMENTUL ELECTROTEHNICĂ ŞI MĂSURĂRI

Cursul 8 PROTOCOLUL PUNCT LA PUNCT

Introducere curs	În acest curs este prezentat protocolul punct la punct.
Obiective curs	• Introducere: prezentare, modul de operare, cerinţe impuse nivelului fizic. • Componentele PPP: componente de bază; nivelul legăturii de date PPP; protocolul de control al legăturii - LCP; autentificarea părţilor; protocolul de control al pachetelor de reţea - NCP; compresia datelor; criptarea datelor; conexiunile multiple; lista protocoalelor care compun PPP;componente asociate la PPP; • Utilizarea şi configurarea PPP: Configurarea unui client PPP (*Dial Out*)**;** Procedura de conectare şi autentificare *(sign in)***;** Obţinerea informaţiilor despre serviciu şi echipamente.
Durată medie de studiu individual	Durata medie de studiu individual: 100 minute. Acest interval de timp presupune parcurgerea continutului cursului şi rezolvarea testelor de autoevaluare

Cuprins:

8.1. Introducere.

8.1.1. Prezentare.

Iniţial, protocolul **PPP** *(Point-to-Point* - punct la punct) a apărut ca o metodă de încapsulare folosită pentru a transfera **pachete IP** de-a lungul unor **conexiuni seriale** (punct la punct), ca o alternativă îmbunătăţită a protocoalelor **SLIP** şi **CSLIP** *(Serial Line Internet Protocol - Compressed SLIP)*. Spre deosebire de acestea, **PPP** a fost conceput pentru transferul, printr-un mecanism de **multiplexare,** a **protocoalelor de reţea**, care pot fi transmise simultan pe aceea şi legătură.

Pentru multiplexare se pot folosi două metode, prima de tip **asincron,** foloseşte pentru **delimitarea** unităţilor de date de protocol încapsulate indicatori de **start** şi **stop,** iar cea de a doua de tip **sincron** utilizează în plus **bit de sincronizare** a canalelor multiplexate. Pentru **creşterea eficienţei** transmisiei şi a **secretizării** informaţiei, **PPP** este dotat cu componente de **compresie** şi **criptare** a datelor.

PPP are în componenţa sa **mecanisme** specifice pentru **configurarea** şi **testarea** calităţii **legăturii fizice**, detectarea erorilor, **negocierea dinamică** a adresei de reţea şi a metodelor de compresie şi criptare [1, 4].

8.1.2. Modul de operare.

Pentru a **stabili** o **legătură** de **comunicaţie**, de-a lungul unei conexiuni "punct la punct", **componenta PPP**, de la capătul care **cere iniţierea** legăturii, **transmite** mai întâi **cadre LCP** pentru a **configura** şi **testa** (opţional) **legătura** de date.

După ce legătura a fost **stabilită** şi eventualii **parametri** au fost **negociaţi**, în funcţie de necesităţile impuse de scopul legăturii, **se trimit** în continuare **cadre NCP** pentru a alege şi **configura unul** sau **mai multe protocoale** de nivel superior, nivel **OSI 3 reţea**.

În următoarea etapă, dacă este cazul, **CCP negociază** metoda de **compresie** şi **criptare** a datelor încapsulate în cadrele **PPP**. Când toate aceste protocoale au configurat parametrii conexiunii, **se pot trimite** pe această **legătură în ambele sensuri** pachete provenind de la **oricare** dintre **protocoalele de reţea** folosite.

Legătura îşi **păstrează configuraţia**, până când se **trimite** în mod **explicit** un cadru **LCP** sau **NCP** care să **închidă linia**. În cazul în care apare o problemă externă (întreruperea accidentală sau voită a legăturii seriale), sau după **expirarea** unei **perioade de inactivitate** negociată anterior, **legătura se închide**.

8.1.3. Cerinţe impuse nivelului fizic.

PPP poate să opereze **de-a lungul** oricărei legături între concepute pentru conectarea echipamentelor **DTE** şi **DCE**. Sunt incluse aici interfaţa **EIA/TIA 232-C** (cunoscută şi ca RS 232-C) **EIA/TIA 422** (cunoscută şi ca RS 422), sau **V 35 (**standard ITU-T *International Telecommunication Union Telecommunication Standardization Sector)*.

Singura condiţie impusă de **PPP** este ca **circuitul să permită** comunicaţie ***full duplex,*** pe linie **dedicată** sau **comutată**, care poate să opereze serial, atât asincron cât şi sincron. **PPP nu impune** nici o **restricţie** referitoare la **rata de transfer**, restricţii impuse eventual doar de echipamentele (DTE sau DCE) folosite [1, 4].

8.2. Componentele PPP.

8.2.1. Componente de bază.

Pentru a putea transmite datagrame de-a lungul unor linii seriale "punct la punct" este nevoie de patru componente principale.

- Un protocol sincron, specific subnivelului **LLC** (OSI 2 legătură), numit **HDLC** (*High-Level Data Link Control)* utilizat pentru încapsularea datagramelor şi controlul transmisiei;
- O familie de protocoale complexe **LCP** (*Link Control Protocol*), concepute special pentru PPP, folosite pentru **stabilirea**, **configurarea** şi **testarea** conexiunii. Acestea operează la nivelul fizic şi al legăturii de date, a nivelelor **OSI 1** şi **2 MAC**. **LCP** este responsabil cu asigurarea unei **conexiuni** robuste la **nivelul fizic** şi al **legăturii de date**;
- O familie de protocoale **NCP** (*Network Control Protocol*), folosite pentru **negocierea** utilizării şi configurarea protocoalelor de reţea, de la nivelul **OSI 3**. În afară de **IP**, pentru care a fost conceput iniţial, **PPP** permite încapsularea şi transferul simultan a unor protocoale ca **Novell IPX** (*Internetwork Packet Exchange*), **DECnet** şi uneori **NetBEUI** *(NetBIOS Extended User Interface* - protocol de transport dezvoltat de firma Microsoft, bazat pe funcţii ale protocolului NetBIOS, dezvoltat de IBM);
- Un protocol **CCP** *(Compression Control Protocol)* care permite negocierea şi utilizarea unor metode de **compresie** a **datelor încapsulate** în cadrele **PPP**.
- Un protocol **ECP** *(Encryption Control Protocol)* care permite negocierea şi utilizarea unor algoritmi de criptare a datelor.

Lista tuturor protocoalelor care compun **PPP** este prezentată la punctul 8.2.9.

8.2.2. Nivelul legăturii de date PPP.

PPP foloseşte principiile, terminologia şi structura cadrelor impuse de **ISO** *(Organizaţia Internaţională pentru Standardizare)*, în conformitate cu standardul **ISO 3309-79** modificat prin ISO 3309-84/PDAD1 *(Addendum 1)*. Standardul **ISO 3309-79** specifică **structura cadrului HDLC** folosit la transmisiile în medii sincrone, iar ISO 3309-84/PDAD1, propune modificări ale celui dintâi pentru a permite utilizarea în medii asincrone.

Procedurile de control PPP utilizează definiţiile şi semnificaţia câmpurilor conform standardului ISO 4335-79, Addendum 1. **Formatul** cadrelor **PPP** arată ca în **figura 8.1**.

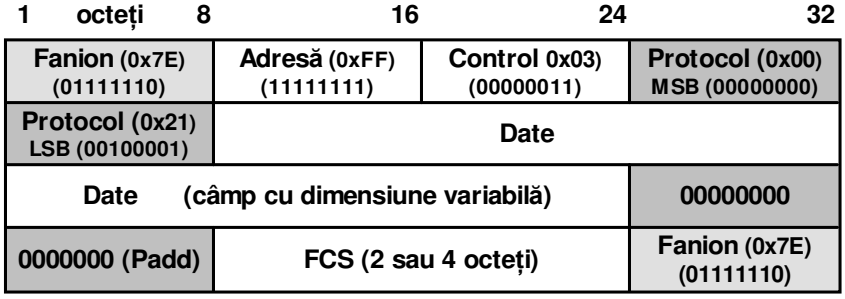

Fig. 8.1. Formatul cadrului PPP.

Semnificaţia câmpurilor prezentate în **figura 8.1** este următoarea:

- **Fanion** (*Start Flag*) **- Indicator** de **start** şi de **stop**, format dintr-un octet care marchează începutul şi sfârşitul unui cadru. Acesta este compus din succesiunea binară **01111110.**

- **Adresă,** un octet care conţine secvenţa binară **11111111,** care reprezintă **adresa** standard de ***broadcast***. PPP **nu alocă** adresă **individuală** (de nivel OSI 2) pentru **nodurile** implicate în stabilirea legăturii.
- **Control,** un octet care conţine secvenţa binară **00000011** care **precede** transmisia **datelor utile**, într-un cadru izolat (care nu face parte dintr-o succesiune de cadre). Pentru **controlul legăturii** este folosit un **serviciu fără conexiune**, similar cu **LLC** de tipul **1**.
- **Protocol,** câmp format din **doi octeţi** care identifică **protocolul încapsulat** în câmpul de **date** (informaţii utile) ale cadrului.
- **Date**, un câmp cu **dimensiune variabilă** între **zero** şi **1500** (uzual, se poate modifica această valoare prin consens între părţile care se conectează).
- **FCS** (*Frame Check Sequence*), un câmp format de obicei din **doi octeţi**, dar pentru a creşte performanţele de detecţie a erorilor, în urma unui consens între părţi, se pot folosi 4 octeţi (32 biţi).
- **Sfârşitul** câmpului de date se marchează cu ajutorul **fanionului** (indicatorului) de **sfârşit**.

8.2.3. Protocolul de control al legăturii PPP - LCP.

LCP (al cărui cod este `c021`) face parte dintr-o familie de protocoale care furnizează suportul necesar pentru stabilirea, configurarea, întreţinerea şi închiderea unei conexiuni, operând în cinci faze distincte:

- În prima fază se stabileşte legătura şi se negociază configuraţia. Înainte ca să se poată trimite datagrame ale unui protocol de nivel superior, **LCP** trebuie să deschidă legătura şi să negocieze parametrii de configurare. Această fază este terminată atunci când sunt trimise şi recepţionate, de către ambele capete ale legăturii, cadre cu mesaje de confirmare.
- În a doua fază se determină calitatea legăturii. **LCP** permite determinarea opţională a calităţii legăturii, după ce aceasta a fost stabilită şi configurată. În această fază legătura este testată pentru a determina dacă condiţiile de calitate sunt suficiente pentru a suporta un protocol de reţea (în general de nivel superior). Există situaţii în care o viteză prea mică a liniei nu permite transmiterea datagramelor cu o rată suficient de mare, care să le permită să ajungă la destinaţie înainte de expirarea timpului de viaţă al acestora. Această fază este opţională, iar în cazul în care se foloseşte, **LCP** poate întârzia transmisia datelor utile până la încheierea acesteia.
- În faza a treia are loc autentificarea legăturii, după o metodă negociată în faza întâi. Această fază este opţională, prezenţa sau absenţa ei nu influenţează desfăşurarea fazelor următoare.
- În faza a patra are loc negocierea şi configurarea protocoalelor de nivel superior. După ce **LCP** încheie faza de verificare a calităţii legăturii, iar faza de autentificare este trecută cu succes, fiecare protocol de nivel superior poate fi configurat separat prin utilizarea unei componente **NCP** corespunzătoare. **NCP** poate activa, sau dezactiva în orice moment, protocoalele de nivel superior. Dacă **LCP** închide legătura, va informa protocoalele de nivel superior pentru ca acestea să poată lua măsurile care se impun.
- Ultima fază este aceea în care **LCP** încheie legătura. **LCP** poate face acest lucru în orice moment. În mod normal, acest lucru se întâmplă în urma unei cereri din partea unei părţi, dar legătura se poate închide şi în cazul unui eveniment datorat nivelului fizic, cum ar fi pierderea purtătoarei, sau expirarea unei perioade de inactivitate stabilite anterior. Inactivitatea este caracterizată prin absenţa unui trafic prin legătură (nu se transmit nici un fel de cadre).

Deoarece **PPP nu este** conceput cu o **structură** de tip **client/server**, fiecare partener care doreşte stabilirea unei conexiuni, trebuie să trimită o **cerere** de configurare a conexiunii(**CONFREQ** *(Configuration Request)*, pe care celălalt partener **trebuie** să o **accepte**. În aceste cereri **pot fi incluse opţiuni** care **nu** sunt **definite implicit** cum sunt: **protocolul de autentificare**, **MRU** *(Maximum Receive Unit* - numărul maxim de octeţi care pot fi recepţionaţi), convenţia caracterelor de control etc.

Tot în această etapă, partenerii **negociază** metoda de **autentificare** şi dacă partenerii suportă conexiuni fizice multiple, *multilink*. În urma unei astfel de cereri, sunt posibile **trei tipuri** de **răspunsuri**:

1. **CONFACK** *(Configure Acknoledgement)* este un răspuns de **confirmare** a configuraţiei pe care un partener trebuie să-l trimită celuilalt care a făcut cererea, în cazul în care **acceptă opţiunile** formulate în **CONFREQ**.

2. **CONFREJ** *(Configure Reject)* este un răspuns care trebuie trimis partenerului care a făcut cererea (CONFREQ), în cazul în care **unele** dintre **opţiuni nu** sunt **recunoscute** (din motive de incompatibilitate, sau pentru că sunt inactivate).

3. **CONFNAK** *(Configure Negative Acknoledgement)* este un răspuns care trebuie trimis partenerului care a făcut cererea în cazul în care **opţiunile sunt recunoscute**, dar **valorile nu** sunt **acceptate**.

Partenerii continuă să schimbe astfel de mesaje până când fiecare transmite **CONFACK**, până la întreruperea conexiunii, sau până când unul dintre parteneri (sau ambii) anunţă că negocierea nu poate fi încheiată.

LCP foloseşte **trei categorii** distincte de cadre, diferite în funcţie de faza de operare şi de scop. Cadrele folosite la stabilirea şi configurarea legăturii sunt diferite de cele folosite la închiderea acesteia, sau pentru întreţinerea şi depanarea unei legături.

LCP poate să **negocieze modificarea** structurii standard a **cadrului PPP**. **Cadrele modificate** vor trebui **marcate** pentru a putea fi **deosebite** de cele standard.

8.2.4. Autentificarea părţilor.

8.2.4.1. Principiul autentificării PPP.

În cazul conectării unui terminal aflat la distanţă, la un server de acces, terminalul sau operatorul acestuia trebuie să se autentifice pe baza unui nume de acces şi a unei parole. În funcţie de nivelul de securitate impus de scopul conectării, există mai multe metode de autentificare.

Autentificarea partenerilor este o **fază opţională**, dar **recomandată** în toate cazurile de conectare de la distanţă. În anumite situaţii, autentificarea este **impusă explicit** din motive de **securitate**.

Există **două metode** de bază folosite pentru autentificare în cazul **PPP**. Acestea sunt **PAP** *(Password Authentication Protocol)* şi **CHAP** *(Challenge Handshake Authentication Protocol)*, **definite** de **RFC 1334** şi actualizate **RFC 1994**. Atunci când se discută despre autentificare trebuie să se definească doi termeni **pereche** care participă la aceasta:

Solicitantul (*requester*) este dispozitivul care **iniţiază cererea** de acces la reţea şi care trebuie să **furnizeze informaţiile** de **autentificare.**

Autentificatorul (*authenticator*) este cel care verifică valabilitatea informaţiilor de autentificare şi să permită sau nu stabilirea conexiunii.

Particularitatea autentificării **PPP** este aceea că **ambii parteneri** pot să fie în aceiaşi măsură **solicitant** şi **autentificator**, cererea de autentificare putând fi formulată de **oricare** dintre **parteneri**, autentificarea făcându-se de celălalt partener.

Autentificarea are loc doar între **faza de configurare** a legăturii de către LCP şi **înaintea** fazei de **negociere** a **protocolului de reţea** de către **NCP**. În prima fază se transmit pachete scurte (fără câmp de date) prin care se negociază protocolul utilizat pentru autentificare, iar după aceea mesajele de autentificare propriu-zise.

8.2.4.2. Autentificarea prin PAP.

Autentificarea prin **PAP** *(Password Authentication Protocol)* se face simplu, de către o componentă a familiei de protocoale de control a legăturii, prin **trimiterea repetată**, **„în clar”** de

către **solicitant**, a perechii **nume/parolă** (*username/password*), până când **autentificatorul,** care **verifică** într-o bază de date **valabilitatea** acesteia, trimite un răspuns de **confirmare**. În caz contrar, **autentificatorul închide** forţat conexiunea.

Autentificarea prin **PAP** se **negociază** de către **LCP** şi este caracterizată prin **codul** `0xC023`. Mesajele sunt apoi încapsulate în cadre specifice nivelului OSI 2 şi transferate între părţi. Formatul acestor pachete, care conţin mesajele de autentificare, se poate vedea în **figura 8.2.**

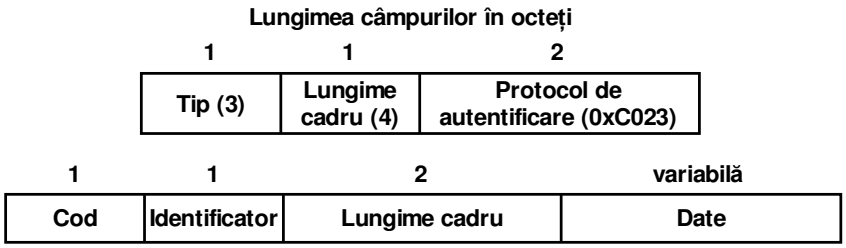

Fig. 8.2. Formatul pachetelor de autentificare **PAP**.

Pentru negocierea autentificării se folosesc trei tipuri de mesaje, în conformitate cu **RFC 1334**, a căror câmpuri au semnificaţia prezentată în **tabelul 8.1**.

Tabelul 8.1.

Cod	Denumire mesaj	Semnificaţie
1	Authenticate-Request	Cerere de autentificare
2	Authenticate-Ack	Confirmarea autentificării
3	Authenticate-Nak	Respingerea autentificării

Identificator – câmp de un octet care identifică sesiunea la care se referă mesajul.

Lungime – câmp de doi octeţi care indică lungimea pachetului care conţine mesajul PAP, incluzând câmpurile **Cod**, **Identificator**, **Lungime** şi **Date**. Informaţiile care se transmit în afara acestei dimensiuni, sunt tratate ca „umplutură” *(padding)* şi sunt ignorate.

Date – câmp cu dimensiune nulă sau variabilă, în funcţie de valoarea înscrisă în câmpul **cod** (rolul cadrului)

Etapele metodei de autentificare prin **PAP** sunt prezentate în **figura 8.3**.

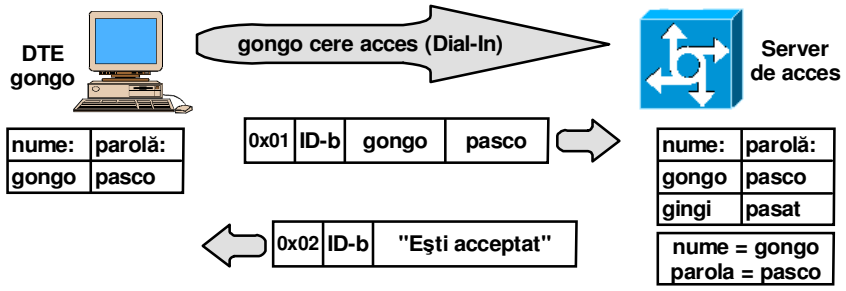

Fig. 8.3. Principiul metodei de autentificare **PAP**.

8.2.4.3. Autentificarea prin CHAP.

Autentificarea prin **CHAP** (*Challenge-Handshake Authentication Protocol*) este o metodă de autentificare folosită atunci când se doreşte un grad sporit de securitate, care se poate aplica atât în faza de iniţiere a unei conexiuni PPP cât şi periodic pe parcursul utilizării ei.

Metoda de autentificare prin **CHAP** se negociază de către **LCP** şi are codul `0xC223`.

Protocolul foloseşte o metodă de verificare în trei etape (*3-way handshake*), după încheierea de către **LCP** a fazei de configurare a legăturii, şi poate fi repetată în orice moment după stabilirea conexiunii **PPP**. Astfel, autentificatorul trimite un mesaj de "somaţie" (*challenge message*) solicitantului, care conţine informaţii de identificare unică a sesiunii curente.

Solicitantul va răspunde printr-un mesaj-cod, calculat din informaţiile primite de la autentificator, pe baza unei funcţii de criptare **MD5** *(Message Digest 5)* care se poate aplica într-un singur sens *(one-way hash)* şi a unei chei, numită "codul secret", cunoscute de ambele părţi. Răspunsul va fi recepţionat şi recalculat de autentificator, care va verifica informaţiile criptate şi va accepta, sau nu, continuarea autentificării. Verificarea repetată prin transmitere periodică a mesajului de somaţie (*challenge*) are rolul de a limita efectele unor interceptări nedorite ale comunicaţiei.

Metoda foloseşte un cod secret, cunoscut doar de către partenerii implicaţi în conexiunea **PPP**. Acest cod nu se transmite de-a lungul liniei, ci trebuie stocat pe fiecare dintre cele două echipamente, fiind folosit pentru interpretare mesajului de somaţie şi a răspunsului. Pentru stocarea informaţiilor necesare autentificării se poate folosi un server central.

Schimbul de mesaje se face prin pachete încapsulate în câmpul de date al cadrelor PPP de nivel **OSI 2**. Formatul acestor pachete se poate vedea în **figura 8.4**, codul de identificare a mesajelor fiind prezentate în **tabelul 8.2**.

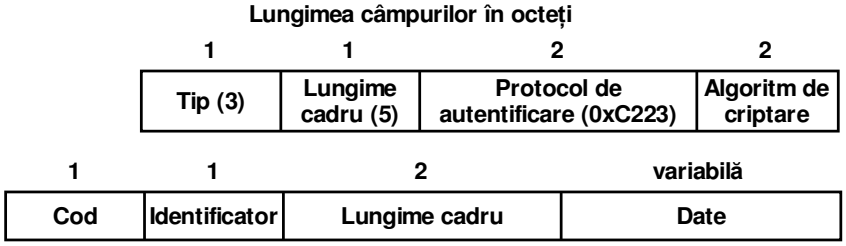

Fig. 8.4. Formatul pachetelor de autentificare CHAP.

Semnificaţia câmpurilor, în conformitate cu **RFC 1994**, este următoarea:

Tip – un câmp de un octet care are valoarea **3**;

Lungime cadru - un câmp de un octet care are valoarea 5;

Protocol de autentificare - un câmp de doi octeţi care are valoarea `0xC223`;

Algoritm de criptare – câmp de un octet care specifică algoritmul de criptare folosit. În cazul utilizării CHAP cu MD5, cest câmp are valoarea **5**.

Tabelul 8.2.

Cod	Denumire mesaj	Semnificaţie
1	Challange	Somaţie
2	Response	Răspuns
3	Success	Confirmarea autentificării
4	Failure	Eroare (Respingerea autentificării)

Celelalte câmpuri au semnificaţia prezentată în paragraful anterior.

Etapele metodei de autentificare prin **CHAP** sunt reprezentate în **figura 8.5**.

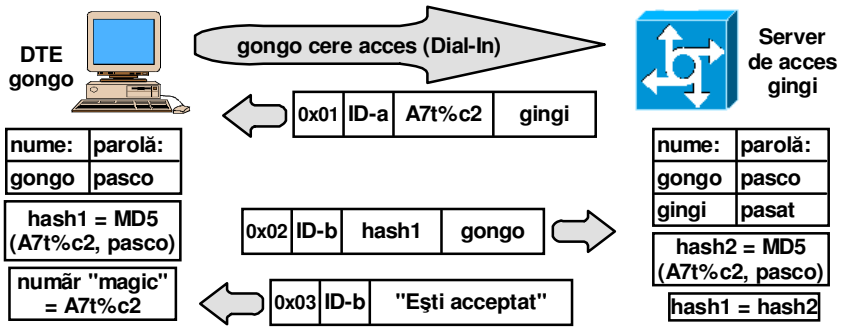

Fig. 8.5. Principiul metodei de autentificare prin **CHAP**.

În prima fază după primirea unei cereri de conectare, autentificatorul trimite mesajul de somaţie (cu codul egal cu 1) în care include identificatorul sesiunii curente "id" împreună cu un cuvânt generat aleator (numărul "magic").

În faza a doua, solicitantul va răspunde cu un mesaj (care are codul egal cu 2) şi care include identificatorul sesiunii şi numărul de control criptate după algoritmul **MD5**.

Deoarece parola, sau codul secret, nu se transmite explicit prin reţea, acesta trebuie stocat pe ambele echipamente pentru a putea fi folosit în faza de criptare şi decriptare. Autentificatorul va recalcula numărul de control, după acelaşi procedeu, iar dacă rezultatul se potriveşte, va transmite în faza a doua un răspuns de acceptare. Răspunsul de acceptare are codul 3 şi permite trecerea la etapa următoare de negociere a configuraţiei protocoalelor de reţea. În cazul în care se întrunesc condiţii prin care se poate refuza conexiunea, autentificatorul va transmite un mesaj de refuz (care are codul 4), sau de eroare.

Microsoft a conceput două variante a metodei **MS-CHAP** şi **MS-CHAPv2**, pe care le utilizează pentru conectarea terminalelor pe care operează sisteme din familia Windows. **MS-CHAPv2** permite autentificarea reciprocă, în acelaşi schimb de mesaje, a părţilor implicate în transferul datelor. Aceste metode sunt utilizate şi în cazul tunelării **VPN**.

8.2.4.4. Autentificarea prin EAP.

EAP *(Extensible Authentication Protocol)* este o componentă suplimentară concepută pentru a permite diferite metode de autentificare, prin schimb repetat de chei publice de criptare bazate pe algoritmi speciali ca **DES** şi **MD5**, *smartcard*, sau certificate de autenticitate, care pot fi configurate în funcţie de cerinţele echipamentelor de acces *(servere de Dial-In)*.

EAP, configurat cu opţiuni severe de securitate, poate fi utilizat pentru transferul datelor confidenţiale care necesită conexiuni sigure, rezistente la tentative de interceptare. Se foloseşte pentru conectarea reţelelor private, prin medii de transmisie publice, realizate prin tunelare **VPN** *Virtual Private Nerwork)*. Datorită mecanismelor suplimentare de autentificare şi criptare, metoda **EAP** are performanţe superioare chiar şi faţă de metoda **CHAP**.

EAP permite utilizarea **TLS** *(Transport Layer Security)* un protocol de transport, constituit ca un nivel suplimentar, care transferă datele prin criptare, în baza unor algoritmi de criptare complecşi, bazat pe schimb de chei şi certificate de autenticitate. Aceasta permite atât autentificarea clientului, care face cererea, cât şi a server-ului de acces.

8.2.4.5. Certificatele de autenticitate şi *Smart card.*

Un certificat de autenticitate este un set de informaţii de acreditare criptate, care include o semnătură digitală emisă şi garantată de un for care are autoritate în acest domeniu.

În cazul proceselor de autentificare bazate pe certificate, terminalul care intenţionează să se conecteze la un server de acces, împreună cu acesta din urmă, îşi prezintă reciproc informaţii de acreditare criptate, care sunt verificate cu ajutorul unei chei publice. Cheia publică se transferă o

singură dată, în condiţii de securitate sporite şi este păstrată local într-o bază de date numită *Trusted Authority Root Certificate*, instalată şi gestionată de către administratorul sistemului.

În această bază de date se pot adăuga, sau şterge, certificate provenite de la diferite resurse, în funcţie de încrederea acordată acestora. Aceste certificate pot fi materializate prin fişiere text conţinând informaţiile de acreditare criptate, sau sub formă de ***smart card***. Acesta este un dispozitiv electronic, ca o cartelă magnetică sau de telefon, care se introduce într-un echipament de citire conectat la terminal. Utilizarea uneia dintre aceste variante (certificate de autenticitate sau smart card) este opţională şi se alege în funcţie de strategia de securitate folosită [3].

8.2.5. Protocolul de control al pachetelor de reţea - NCP.

NCP *(Network Control Protocol)* este componenta care se ocupă, în **faza** care **urmează autentificării**, de **negocierea variabilelor** specifice **protocolului de reţea**, folosind **mesaje CONFREQ**, **CONFREJ**, **CONFNAK** şi **CONFACK**, asemănătoare cu cele folosite de **LCP**.

Codul protocolului de negociere depinde de protocolul de reţea care urmează să fie încapsulat în PPP.

Trebuie remarcat că **se pot încapsula mai multe protocoale** de reţea în cursul **aceleiaşi sesiuni**, toate acestea fiind **negociate în aceeaşi fază** de către un protocol din familia **NCP**, specific.

De exemplu, pentru **IP** (protocolul de Internet) protocolul de negociere corespunzător este **IPCP** *(Internet Protocol Control Protocol)*, al cărui cod este `8021` şi este reglementat în RFC 1332, fiecare dintre aceste protocoale făcând obiectul unor astfel de norme specifice.

8.2.6. Compresia datelor.

PPP oferă suportul necesar compresiei datelor transferate. De această problemă este responsabilă componenta **CCP** *(Compression Control Protocol)*, în conformitate cu documentul RFC 1962, care negociază şi decide metoda de compresie şi, dacă este cazul, de criptare.

Negocierea compresiei se face după încheierea fazei de negociere şi configurare a protocoalelor de reţea de către familia de protocoale **NCP**, prin transmiterea de către **CCP** a unor mesaje, asemănătoare cu cele folosite de **LCP** pentru configurarea conexiunii. Se pot negocia mai multe metode de compresie, dar nu se poate folosi decât una singură, pentru ambele sensuri, într-o sesiune de conectare.

Fiecare platformă pe care operează acest protocol, a dezvoltat propriile soluţii de compresie şi criptare, ceea ce conduce la apariţia unor situaţii de incompatibilitate, în faza de negociere.

Microsoft a dezvoltat propriile protocoale de compresie, create pentru transferul datelor prin **PPP**. Componenta care permite negocierea, configurarea şi compresia datelor, pentru transferul acestora prin conexiuni punct la punct, este **MPPC**, protocol folosit la această oră şi de către comunitatea de utilizatori ai sistemelor de operare din familia **UNIX** şi **Linux**.

8.2.7. Criptarea datelor.

PPP oferă suport pentru criptarea datelor transferate de-a lungul unei legături. De această problemă este responsabilă componenta **ECP** *(Encryption Control Protocol)* , în conformitate cu documentul RFC 1968, care permite negocierea între părţi, după faza de configurare a protocoalelor de reţea, a metodei de criptare. Algoritmii de criptare utilizaţi sunt **DES** *(Data Encryption Standard)* (RFC 1969), **3DES** *(Triple-DES Encryption Protocol)* [RFC 2420] şi variante ale acestora.

Microsoft a dezvoltat propriile protocoale de criptare, utilizate pentru transferul datelor prin **PPP**. Componenta care permite negocierea, configurarea şi transferul criptat al datelor, prin conexiuni punct la punct, este **MPPE**, folosit la această oră şi de către comunitatea de utilizatori ai sistemelor de operare din familia **UNIX** şi **Linux**.

8.2.8. Conexiunile multiple.

Modul în care a fost conceput PPP permite transferul datelor între două sisteme, prin „despicarea” pachetelor de reţea, transmiterea pe linii diferite şi reasamblarea lor ulterioară.

Astfel, protocolul **MLP** *(Multilink Point-to-Point Protocol)*, definit prin RFC 1990, permit transferul datelor canale, ca şi când ar fi o singură conexiune, dar cu o rată de transfer mai mare. Împărţirea pe canale se face diferit în funcţie de rata de transfer a fiecărui canal în parte, iniţierea legăturilor se poate face simultan, sau pe rând, în funcţie de fluxul de date necesar.

Fragmentarea pachetelor şi controlul secvenţelor prin marcarea acestora, împreună cu modul de echilibrare a încărcării canalelor, fac obiectul aceluiaşi document. **MLP** poate să opereze atât pe linii analogice, conectate şa interfeţe seriale asincrone (EIA/TIA 232), cât şi pe linii digitale ISDN BRI sau PRI.

8.2.9. Lista protocoalelor care compun PPP.

Protocoale de control a conexiunilor multiple.
Coduri între 0x0000 şi 0x3FFF.
- **MP** - Multi-link Protocol.
- **MP+** - Ascend's Multilink Protocol Plus.
- **SDTP** - Serial Data Transport Protocol.

Protocoale de control a legăturii.
Coduri între 0xC000 to 0xFFFF.
- **BACP** - Bandwidth Allocation Control Protocol.
- **BAP** - Bandwidth Allocation Protocol.
- **CHAP** - Challenge Handshake Authentication Protocol.
- **EAP** - Extensible Authentication Protocol.
- **LCP** - Link Control Protocol.
- **LQR** - Link Quality Report Protocol.
- **PAP** - Password Authentication Protocol.

Protocoale de control a nivelului de reţea.
Coduri între 0x8000 to 0xBFFF.
- **ATCP** - AppleTalk Control Protocol.
- **BCP** - Bridging Control Protocol.
- **BVCP** - Banyan Vines Control Protocol.
- **CCP** - Compression Control Protocol.
- **DNCP** - DECnet Phase IV Control Protocol.
- **ECP** - Encryption Control Protocol.
- **IPCP** - Internet Protocol Control Protocol.
- **IPv6CP** - IPv6 Control Protocol.
- **IPXCP** - IPX Control Protocol.
- **NBFCP** - NetBIOS Frames Control Protocol.
- **OSINLCP** - OSI Network Layer Control Protocol.
- **PPP-LEX** - LAN Extension Protocol.
- **SDCP** - Serial Data Control Protocol.
- **SNACP** - SNA Control Protocol.
- **XNSCP** - XNS IDP Control Protocol.

Protocoale de control a compresiei.
Coduri definite de opţiuni ale CCP.
- **BSD** - BSD UNIX Compression Protocol.
- **Deflate** - PKZIP Deflate Protocol.
- **DCE** - for Data Compression in Data Circuit-Terminating Equipment.
- **FZA** - Gandalf FZA Compression Protocol.
- **LZS** - Stac LZS Compression Protocol.

- **LZS-DCP** - LZS-DCP Compression Protocol.
- **MPPC** - Microsoft Point-To-Point Compression Protocol.
- **MVRCA** - Magnalink Variable Resource Compression Algorithm.

Protocoale de criptare.
Coduri definite de opțiuni ale ECP.

- **3DESE** - Triple-DES Encryption Protocol.
- **DESE** - DES Encryption Protocol.
- **DESE-bis** - DES Data Encryption Standard Protocol, Versiunea 2.

8.2.10. Componente asociate la PPP.

8.2.10.1. AAA.

AAA *(Authentication, Authorization, and Accounting)* este tehnologie de conectare care include operațiile cele mai importante asociate conectării de la distanță.

Protocoalele utilizate pentru rezolvarea acestei probleme sunt **TACACS** şi **RADIUS**, care au fost dezvoltate pentru a avea o metodă centralizată de autentificarea şi control al accesului, unui utilizator la resurse de rețea [4].

Pentru a face posibile aceste funcții, sistemul utilizează o **bază de date** care conține **informații** despre **fiecare utilizator**, operatori, terminale sau grupuri de terminale.

Exemple de informații care pot fi administrate centralizat sunt: perechea **numele de acces / parolă**, drepturi de acces la resurse (sau de utilizare a unor protocoale) şi **restricții de viteză** sau de **trafic**, priorități sau motive pentru deconectare. **AAA** este **soluția ideală** pentru orice **furnizor de servicii** de rețea.

8.2.10.2. DDR.

DDR *(Dial on Demand Routing)* este o opțiune de conectare automată la un server de acces, în cazul în care o anumită aplicație, sau terminale dintr-o rețea conectată prin **PPP** necesită acest lucru. **PPP** dispune de mecanisme care interpretează cererile de comunicație şi declanşează automat procedura de conectare. Această opțiune poate opera atât pe terminale, de sine stătătoare, cât şi pe echipamente de interconectare între rețele, cum sunt ruterele sau porțile de acces.

În această situație, trebuie actualizate şi tabelele de rutare şi configurate opțiuni speciale de filtrare a mesajelor inutile transmise, de cele mai multe ori cu adrese de *broadcast*. Această tehnică se foloseşte alături de cea a utilizării conexiunilor multiple, prin linii telefonice analogice sau digitale (**ISDN**).

8.3. Utilizarea şi configurarea PPP.

8.3.1. Configurarea unui client PPP (*Dial Out*).

Utilizatorii de calculatoare folosesc **PPP** pentru a se conecta prin linie telefonică, la un furnizor de servicii de Internet, sau pentru a extinde accesul la o rețea privată. Relația dintre utilizatori şi rețeaua la care doresc să se conecteze, se poate vedea în **figura 8.6**.

În această relație, poziția calculatorului izolat este aceea de "client". Pe parcursul acestui paragraf se va folosi termenul "client" în acest context (terminalul care cere accesul la un serviciu de conectare). **PPP** asigură conectarea pe linie serială şi reprezintă suportul pentru nivelele **OSI 1** şi **2**.

De obicei, conectarea „în afară” prin linie comutată *(Dial Out)* se foloseşte pentru a conecta un calculator izolat, la un server de acces (D*ial In Server*), sau un ruter care are „în spate” o reţea locală, căreia trebuie să-i asigure accesul la resurse de reţea.

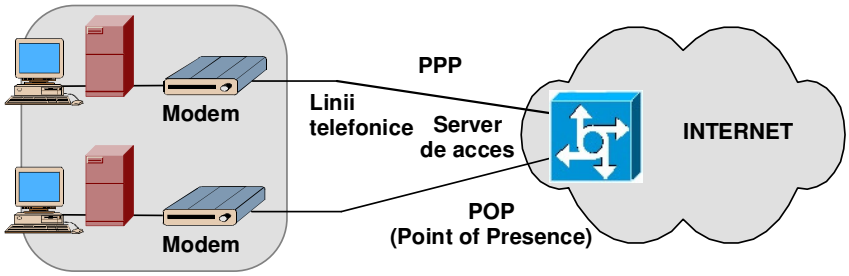

Fig. 8.6. Conectarea prin PPP la un server de acces.

Scopul acestui paragraf este de a prezenta modul în care trebuie configurate componentele *software*, folosite pentru conectarea prin **PPP**.

Majoritatea furnizorilor de servicii de conectare distribuie gratuit componentele necesare. Acesta este motivul pentru care se găsesc pe piaţă multe variante de produse care pot să asigure acest tip de serviciu. Sistemele de operare, utilizate pe scară mare (Microsoft Windows, Linux etc.,) conţin în pachetul de bază astfel de componente.

Din păcate nu toţi utilizatorii sunt suficient de bine pregătiţi pentru a configura optim aceste resurse. Unele sisteme de operare asigură, pentru configurare, un ghid interactiv care pe baza unor întrebări puse utilizatorului, îl conduc spre o configuraţie potrivită. Deşi **PPP** este standardizat, există un număr mare de variante de utilizare, ceea ce face necesară prezentarea în detaliu a unor etape, de configurare manuală, mai importante.

8.3.2. Procedura de conectare şi autentificare *(Sign In)*.

Pentru a configura componenta **PPP,** care să permită conectarea la un serviciu de comunicaţie, Internet sau reţea privată, este nevoie de un cont de acces la acesta şi de câteva informaţii despre echipamentele care vor fi folosite (interfaţa serială, modem, server de acces).

8.3.3. Obţinerea informaţiilor despre serviciu şi echipamente.

Pentru accesul la o reţea care utilizează **TCP/IP**, administratorul de reţea trebuie să furnizeze următoarele elemente:

- Numărul de telefon de acces la serviciul de conectare,
- Un nume de utilizator şi o parolă pentru autentificare,
- Procedura interactivă pentru selectarea protocolului (dacă este cazul) şi a parametrilor de comunicaţie (compresie, dimensiunea maximă a câmpului de date etc.),
- Metoda şi procedurile de autentificare (unele sisteme solicită autentificare înainte de lansarea componentei **PPP**, iar altele în cadrul acestuia),
- Modul de atribuire a adresei **IP** (fixă sau dinamică) pentru capetele conexiunii **PPP** (maşina locală şi de la distanţă),
- Adresa **IP** a serverului de nume (**DNS**) necesar pentru conversia (rezolvarea) numelui simbolic în adresă **IP** [1, 2].

În general, sistemele de operare cu utilizare largă conţin componentele *software* necesare pentru o gamă largă de tipuri de servicii de acces, permiţând atât autentificarea prin **PAP** (*Password Authentication Protocol*) cât şi prin **CHAP** (*Chalenge Handshake Authentication Protocol*). Pot exista şi situaţii când furnizorul serviciului solicită condiţii speciale de conectarem dar acestea sunt destul de rare.

8.3.4. Etapele configurării PPP.

Configurarea componentelor de conectare în exterior prin **PPP** începe cu componentele *hardware, software* şi sistemul de operare, instalate în calculatorul utilizatorului.

După instalarea componentelor *software* suplimentare (dacă este cazul), trebuie configurate componentele, pentru fiecare nivel în parte, aşa cum se poate vedea mai jos:

1. Configurarea interfeţei seriale,
2. Stabilirea configuraţiei optime şi a comenzilor pentru modem. Dacă un calculator client nu are deja un profil configurat cu modem, acesta trebuie creat şi modemul instalat (trebuie definit şirul de iniţializare).
3. Se construieşte scenariul de lansare (*chat script* - scenariu de conversaţie). Acesta trebuie să conţină, mai întâi, secvenţele necesare pentru iniţializarea modemului, iar apoi pentru a comanda serverului de comunicare să iniţializeze sesiunea PPP. Această "conversaţie poate include şi autentificarea utilizatorului, dacă se cere acest lucru.
4. Configurarea componentei **PPP** poate include autentificarea proprie a protocolului.
5. Configurarea **TCP/IP** include modul în care se atribuie adresa **IP**, configurarea severului de nume (**DNS**) şi a porţii de acces. Acestea sunt, în cele mai dese cazuri, alocate dinamic de către serverul de comunicaţie.
6. Stabilirea şi utilizarea conexiunii.

Aceste etape se derulează de obicei pe parcursul aceluiaşi proces de configurare şi uneori în cadrul aceleiaşi componente software. Cu toate astea, interfaţa serială, modemul, componentele **TCP/IP** şi **PPP** sunt "articole" distincte! [1, 2]

TESTE DE AUTOEVALUARE

I. Alege□i varianta de răspuns corectă:

1. Componentele de bază ale protocolului PPP sunt:
   a) MAC, LLC, NCP, CCP şi ECP;
   b) HDLC, LCP, NCP, CCP şi ECP;
   c) HDLC, IP, NCP, CCP şi ECP;
   d) HDLC, LCP, NCP, CCP şi DECnet;
   e) NetBEUI, LCP, NCP, IP şi ECP
2. Autentificarea partenerilor utilizează următoarele metode de bază:
   a) LCP şi RFC;
   b) LCP şi NCP;
   c) PAP şi ECP;
   d) PAP şi CHAP;
   e) PAP şi MD5
3. PPP oferă suport pentru compresie şi criptare a datelor. Această fază se desfăşoară:
   a) După negocierea LCP;
   b) După negocierea NCP;
   c) Înainte de autentificare;
   d) Înainte de negocierea NCP;
   e) După negocierea LCP;

II. Alege□i răspunsul corect:

1. NCP este componenta care se ocupă de controlul logic al legăturii.
   □ adevărat □ fals

2. ECP este o componentă suplimentară concepută pentru a permite diferite metode de autentificare, prin schimb repetat de chei publice de criptare, bazate pe algoritmi speciali ca DES şi MD5, smartcard, sau certificate de autenticitate.
   □ adevărat □ fals

3. MPPC şi MPPE sunt componente ale protocolului PPP, dezvoltate de Microsoft, care se pot utiliza si pe sistemele de operare UNIX şi Linux.
   □ adevărat □ fals

RĂSPUNSURI

I. Varianta de răspuns corectă:

1. b
2. d
3. b

II. Alege□i răspunsul corect:
1. fals
2. fals
3. adevărat

Bibliografie

1. **Sun, A.**, *Using & Managing PPP,* O'Reilly 1999, ISBN 10: 1-56592-321-9
2. **Light-Williams, C., Drake, J.**, „*Linux PPP HOWTO*", Distribuție Linux, CommandPromp Inc. 2000
3. * * * Manuale Lab Microsoft Windows 2000 Resource Kit, Cap. 9, Virtual Private Networking VIEW
4. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ppp.htm