HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Point-to-Point Protocol

CCERT-PUBDOC-2007-03-186

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

PPP (eng. *Point-to-Point Protocol*) koristi se za izravno povezivanje dvaju čvorova računalne mreže. Omogućuje povezivanje računala serijskim, telefonskim ili optičkim kabelom, pomoću mobilnih telefona te posebno oblikovanom radio ili satelitskom vezom. Većina ISP (eng. *Internet Service Provider*) poslužitelja koristi ovaj protokol za omogućavanje pristupa Internetu preko telefonskog priključka korištenjem modema (eng. *dial-up*). Ugrađena (eng. *encapsulated*) inačica PPP protokola, tzv. PPPoE (eng. *Point-to-Point over Ethernet*) protokol, se na sličan način koristi kod DSL (eng. *Digital Subscriber Line*) pristupa Internetu. Kod ovog protokola se PPP podatkovni paketi umeću u *Ethernet* pakete.

PPP protokol se koristi na drugom, podatkovnom, sloju OSI (eng. *Open System Interconnection*) mrežnog modela za povezivanje preko sinkronih i asinkronih veza. Ovaj je protokol u velikoj mjeri zamijenio starije protokole, kakav je npr. SLIP (eng. *Serial Line Internet Protocol*) protokol, i protokole telefonskih kompanija, kao što je LABP (eng. *Line Access Balanced Protocol*) protokol iz X.25 skupine protokola. PPP je građen tako da omogućuje rad s brojnim protokolima mrežnog sloja, uključujući IP (eng. *Internet Protocol*), IPX (eng. *Internetwork Packet Exchange*) i *AppleTalk* protokole.

U nastavku dokumenta objašnjeni su neki osnovni pojmovi vezani uz serijsku komunikaciju, navedene su funkcionalnosti PPP protokola, opisan je sadržaj PPP podatkovnih paketa i postupak ovijanja paketa različitih protokola. Također su opisani LCP i NCP upravljački protokoli te PAP i CHAP autorizacijski protokoli, a uspostavljanje, održavanje i prekidanje veze ilustrirano je dijagramom stanja PPP protokola.

2. Osnove serijske komunikacije

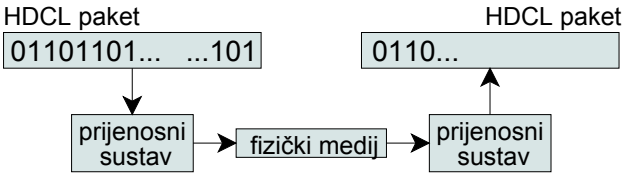
U kontekstu telekomunikacije i računalnih znanosti pod pojmom serijske komunikacije podrazumijeva se prijenos podataka slijednim slanjem pojedinačnih bitova komunikacijskim medijem. Oprečan pristup ovome je paralelna komunikacija kod koje se svi bitovi pojedinog simbola šalju istovremeno. Zbog skupoće kablova i poteškoća sa sinkronizacijom signala serijski prijenos podataka koristi se za komunikaciju preko većih udaljenosti (eng. *long-haul*) i kod većine računalnih mreža. Napredak tehnologije kojim se omogućuju veće brzine prijenosa kao i smanjenje broja priključaka, a samim time i cijene, razlog su sve češće primjene serijske komunikacije kod integriranih sklopova.

Kod računalnih mreža pojedini bitovi koji tvore paket podatkovnog sloja OSI modela, šalju se posredstvom prvog sloja prema fizičkom mediju, kao što je prikazano na slici Slika 1 (podatkovni sloj OSI modela je u primjeru na slici HDLC (eng. *High-Level Data Link Control*) protokol na osnovu kojeg je nastao PPP protokol). Podaci se fizičkim medijem prenose:

- NRZ-L (eng. *Nonreturn to Zero Level*),
- DHB3 (eng. *High Density Binary 3*) ili
- AMI (eng. *Alternate Mark Inversion*) prijenosnim kodom.

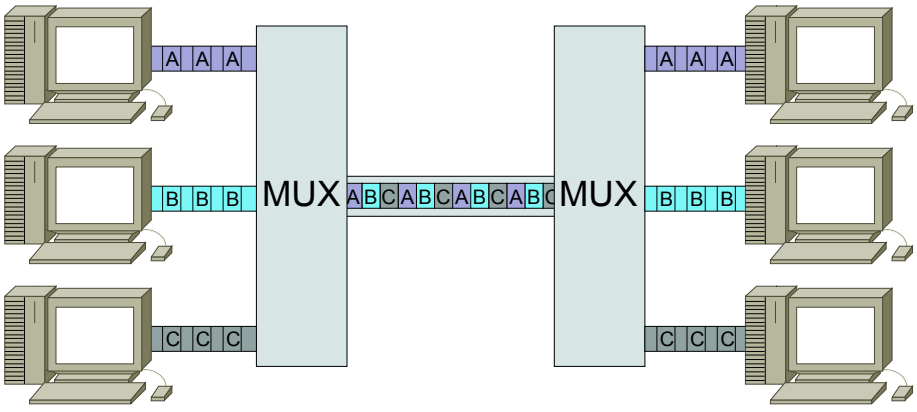
Primjeri standarda koji definiraju serijsku komunikaciju su:

- RS-232 (eng. *Recommended Standard 232*),
- V.35 i
- HSSI (eng. *High Speed Serial Interface*).



Slika 1: Serijski prijenos HDCL paketa

Serijski komunikacijski kanal moguće je dijeliti između više uređaja ispreplitanjem signala podjelom vremena (eng. *Time-Division Multiplexing - TDM*). TDM ispreplitanje omogućuje prijenos više signala, ili podataka iz više izvora, preko zajedničkog komunikacijskog kanala te rekonstrukciju izvornih podataka na odredištu. U primjeru na slici Slika 2 prikazano je ispreplitanje triju signala.



Slika 2: TDM ispreplitanje signala

Postupak ispreplitanja provodi se odabirom dijela ulaznih signala. To je najčešće jedan bit ili jedan oktet (eng. *byte*) svakog signala pa se TDM postupci dijele na:

- one koji isprepliću bitove (eng. *bit-interleaving*) i
- one koji isprepliću oktete (eng. *byte-interleaving*).

Vremenski intervali za prijenos dijelova signala iz svih izvora prisutni su neovisno o tome jesu li spremni novi podaci za slanje. U primjeru na slici Slika 2 šalju se isprepleteni podaci iz tri izvora, podaci iz prvog izvora označeni su s A, iz drugog slovom B, a iz trećeg izvora slovom C. Ako su na ulazu prisutni podaci sa sva tri izvora podaci se šalju redom: A, B, C. Ako u jednom trenutku nema novih podataka iz drugog izvora redoslijed slanja podataka je: A, „_“, C, gdje je oznakom „_“ naznačen vremenski period u kojem se ne šalju podaci.
TDM se provodi na fizičkom sloju, neovisno o tipu podataka koji se šalju ili protokolu koji se izvodi na podatkovnom sloju. Primjer ovakvog ispreplitanja je ISDN (eng. *Integrated Service Digital Network*) sustav s dva kanala B1 i B2 brzine prijenosa 64 kbps i jedan D kanal brzine prijenosa 16 kbps. Prijenos se provodi u devet intervala koji se ponavljaju, pa je slijed slanja: … B1, B2, B1, B2, B1, B2, B1, B2, D, …

3. Osnove funkcionalnosti PPP protokola

PPP protokol namijenjen je jednostavnom povezivanju dvaju ravnopravnih korisnika dvosmjernom (eng. *full-duplex*) vezom koja omogućuje simultano dvosmjerno dostavljanje paketa redoslijedom kojim su poslani. Ovaj protokol omogućuje povezivanje različitih računala, premosnika i usmjerivača, a njegove osnovne funkcionalnosti su:

- ovijanje (eng. *encapsulation*) protokola mrežnog sloja,
- upravljanje vezom,
- interakcija s mrežnim slojem i
- podesivost.

3.1. Ovijanje protokola mrežnog sloja

Ovijanje omogućuje istovremeni prijenos podatkovnih paketa različitih protokola preko iste veze. Postupak omatanja je osmišljen tako da podržava širok raspon arhitektura mrežnih uređaja. Ako se ovijanje izvodi korištenjem uobičajenog HDLC oblika podatkovnih paketa izvornim podacima dodaje se 8 okteta dodatnih informacija. U primjenama s ograničenom propusnošću komunikacijskog kanala ovijanje je moguće implementirati uz samo 2 ili 4 dodatna okteta. Veličina zaglavlja stvorenog ovijanjem ograničena je na 32 bita dok duljina podataka dodanih na kraju paketa nije ograničena.

3.2. Upravljanje vezom

Upravljanje vezom definirano je LCP (eng. *Link Control Protocol*) protokolom. Ovaj protokol provodi usuglašavanje postavki formata ovijanja i veličine podatkovnih paketa, uočava pogreške proizišle iz neispravnih postavki, prekida vezu te omogućuje autorizaciju korisnika i otkrivanje neispravnog funkcioniranja veze.

3.3. Interakcija s mrežnim slojem

PPP veze često imaju poteškoće u interakciji s protokolima mrežnog sloja. Na primjer, pridjeljivanje IP adresa i upravljanje njima složene su zadaće i u LAN (eng. *Local Area Network*) okruženjima, a kod PPP veza s prospajanjem krugova (eng. *circuit switched*) ovo je naročito težak problem. Za svaki protokol mrežnog sloja postoji poseban NCP (eng. *Network Control Protocol*) protokol koji rješava specifične poteškoće u interakciji s PPP vezama.

3.4. Podesivost

PPP veze su osmišljene kao vrlo podesive te su građene tako da prvotne postavke zadovoljavaju većinu uobičajenih konfiguracija. Prilikom implementacije moguće je unaprijediti izvorne postavke, a nove postavke se prilikom povezivanja automatski šalju drugoj strani. Također je moguće podesiti posebne postavke veze koje joj omogućuju rad u inače neprikladnim uvjetima.
Samopodešavanje PPP veza implementirano je opsežnim mehanizmom usuglašavanja postavki kod kojega svaka strana veze drugoj prenosi svoje mogućnosti i zahtjeve. Ovakvi mehanizmi ugrađeni su u LCP protokol, u skupinu NCP protokola i u druge kontrolne protokole.

4. Ovijanje PPP protokola i sadržaj paketa

PPP ovijanje koristi se za ujednačavanje podatkovnih paketa različitih protokola mrežnog sloja. Na taj način nastaju novi paketi s oznakama kraja i početka. Na slici Slika 3 prikazan je sadržaj PPP paketa, pri čemu se prikazana polja prenose s lijeva na desno.
PPP podatkovni paket sastoji se od sljedećih elemenata:

- oznaka protokola ,
- podaci i
- dopuna.

Slika 3: PPP ovitak mrežnog paketa

4.1. Polje s opisom protokola

Polje s opisom protokola dugo je jedan ili dva okteta, a njegov sadržaj određuje vrstu podatkovnog paketa koji se nalazi u polju s podacima. Brojevne oznake protokola sadržane u ovom polju građene su prema ISO 3309 standardu te trebaju zadovoljiti sljedeće uvjete:

- iznos oznake je neparna vrijednost,
- najmanje značajan bit najmanje značajnog okteta treba biti „1“,
- najmanje značajan bit najznačajnijeg okteta treba biti „0“.

Ako oznaka protokola ne zadovoljava jedan ili više navedenih uvjeta protokol kojem pripadaju podaci smatra se neprepoznatim.
Rasponi vrijednosti ovog polja pridijeljeni su pojedinim skupinama protokola na sljedeći način:

- od „0***“ do „3***“ – određuje protokol mrežnog sloja pripadnog podatkovnog paketa,
- od „4***“ do „7***“ – za protokole mrežnog sloja s niskim intenzitetom prometa i bez pridijeljenog NPC protokola,
- od „8***“ do „b***“ – određuje pripadnost danog paketa određenom NCP protokolu,
- od „c***“ do „f***“ – određuje pripadnost danog paketa određenom protokolu za upravljanje vezom (npr. LCP protokolu).

U tablici Tablica 1 navedeni su primjeri oznaka protokola.

Heksadecimalna vrijednost	Naziv protokola
0021	*Internet Protocol*
0023	*OSI Network Layer*
0029	*AppleTalk*
8021	*IP Control Protocol*
8023	*OSI Network Layer Control Protocol*
8029	*AppleTalk Control Protocol*
C021	*Link Control Protocol*
C023	*Password Authentication Protocol*
C029	*CallBack Controll Protocol*

Tablica 1: Primjeri oznaka protokola

4.2. Polje s podacima

Polje s podacima sadrži podatkovni paket protokola određenog oznakom u prethodno opisanom polju i dugo je nula ili više okteta. Maksimalna duljina ovog polja i polja s dopunom određena je iznosom MRU (eng. *Maximum Receive Unit*) parametra koji je izvorno postavljen na 1500 okteta. Drugačije podešene vrijednosti spomenutog parametra među klijentima se usklađuju u postupku usuglašivanja postavki.

4.3. Polje s dopunom

Tijekom prijenosa ovijeni mrežni paket moguće je dopuniti proizvoljnim brojem dodatnih okteta, ali tako je ukupna duljina manja od one podešene MRU parametrom. Najčešće su tu pohranjena dva FCS (eng. *Frame Check Sequence*) okteta u kojima je zapisana kontrolna suma korištena prilikom otkrivanja i uklanjanja pogrešaka.

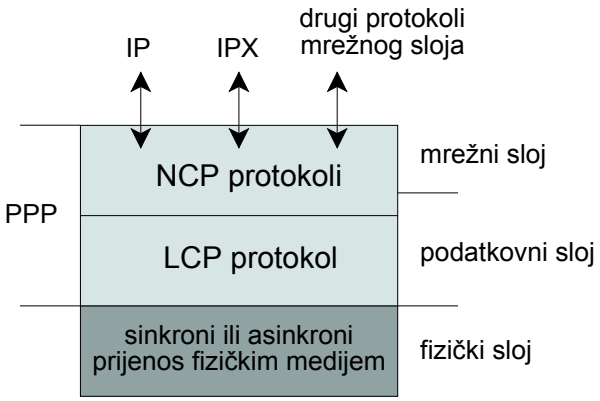
4.4. Ovijanje PPP paketa na nižem OSI sloju

PPP paketi opisani u prethodnim poglavljima ovijaju se ovojnicom protokola nižeg OSI sloja koji mogu osigurati dodatne funkcije kao što je npr. provjera integriteta poruke dodavanjem kontrolne sume. PPP paketi u serijskoj komunikaciji obično su ovijeni ovojnicom sličnom onoj koju daje HDLC protokol i koja sadrži sljedeće elemente:

- **zastavica** predstavlja binarni niz „01111110“ koji označuje početak i kraj paketa,
- **adresa** je binarni niz „11111111“, a predstavlja standardnu adresu emitiranja (eng. *broadcast address*) pri čemu PPP protokol ne pridjeljuje jedinstvene adrese pojedinim mrežnim čvorovima,
- **kontrolni oktet** sadrži binarni niz „00000011“ i predstavlja zahtjev za slanjem korisničkih podataka,
- **datagram** sadrži PPP paket,
- **FCS oktet** sadrži kontrolnu sumu za provjeru integriteta.

5. LCP i NCP upravljački protokoli

PPP protokol građen je slojevito. Na slici Slika 4 prikazani su slojevi ovog protokola, kao i njegov odnos prema slojevima OSI modela. PPP protokol je većim dijelom protokol drugog, podatkovnog, sloja OSI modela. Komunikaciju s fizičkim slojem provodi LCP protokol, a interakcijom s nadređenim protokolima mrežnog sloja upravlja odgovarajući NCP protokol, ovisno o korištenim protokolima mrežnog sloja.



Slika 4: Slojevita struktura PPP protokola

5.1. LCP protokol

LCP protokol se naslanja na fizički sloj OSI modela. Moguće ga je podesiti tako da koristi jedno od sljedećih sučelja:

- asinkrono serijsko,
- sinkrono serijsko,
- HSSI ili
- ISDN sučelje.

Pored oblikovanja komunikacije u skladu s korištenim fizičkim sučeljem ovaj protokol provodi sljedeće zadatke:

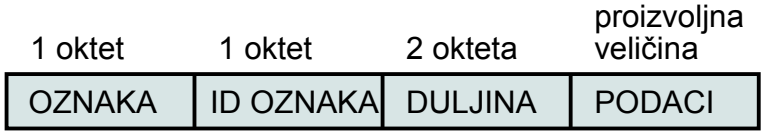
- **Autorizacija** – od pozivatelja, korisnika koji otvara vezu, se zahtijevaju identifikacijski podaci kako bi se utvrdilo ima li on dozvolu mrežnog administratora za uspostavljanje određene PPP veze. Autorizacijske poruke prenose se PAP ili CHAP protokolom.
- **Kompresija** – njome se postiže veća propusnost PPP veze smanjenjem količine podataka unutar pojedinog paketa. LCP protokol na odredištu vrši dekompresiju paketa. Moguće je korištenje različitih kompresijskih algoritama, npr. *Stacker* i *Predictor* algoritama.
- **Otkrivanje pogrešaka** – omogućuje stvaranje pouzdanih PPP veza bez petlji (eng. *loop-free*).
- **Upravljanje višestrukim vezama** – uspostavljanjem višestrukih PPP veza (eng. *multilink*) između dva mrežna čvora postiže se veća propusnost. Na ovaj način moguće je iskoristiti propusnost dvaju ili više fizičkih komunikacijskih kanala, kakvi su npr. analogni ili ISDN modemi.
- **Ostvarivanje povratnih poziva** – povratni pozivi (eng. *callback*) implementiraju se u slučaju potrebe za povišenom razinom sigurnosti. Klijent u tom slučaju poziva poslužitelja, predaje zahtjev za uspostavom veze i prekida poziv. Na temelju klijentova zahtjeva i vlastitih postavki poslužitelj tada otvara ili ne otvara vezu prema klijentu, odnosno ostvaruje povratni poziv.

5.1.1. LCP paketi

Podatkovni paketi LCP protokola dijele se u tri skupine:

- paketi za podešavanje postavki veze (eng. *Link Configuration*):
  - *Configure-Request* paket predstavlja zahtjev za otvaranjem veze i njime se prenose eventualne izmjene izvornih postavki PPP protokola,
  - *Configure-Ack* paket šalje se kao odgovor na zahtjev za uspostavljanje veze ako su prihvaćene sve izmjene izvornih postavki PPP protokola,
  - *Configure-Nak* paket šalje se u slučaju ne prihvaćanja izmjena postavki,
  - *Configure-Reject* paket se šalje ako postavke koje se pokušava izmijeniti nisu prepoznate ili ih nije dozvoljeno mijenjati;
- paketi za prekidanje veze (eng. *Link Termination*):
  - *Terminate-Request* paket predstavlja zahtjev za prekidanjem veze,
  - *Terminate-Ack* je odgovor na zahtjev za prekidom veze;
- paketi za održavanje veze (eng. *Link Maintenance*):
  - *Code-Reject* paket šalje se u slučaju primitka LCP paketa s nepoznatom oznakom do čega može doći u slučaju korištenja različitih inačica LCP protokola,
  - *Protocol-Reject* paket šalje se u slučaju primitka PPP paketa s nepoznatom oznakom protokola,
  - *Echo-Request* i *Echo-Reply* paketi koriste se kod otkrivanja pogrešaka, određivanja kvalitete veze, ispitivanja performansi i brojnih drugih primjena,
  - *Discard-Request* paket ima sličnu primjenu kao i prethodna dva.

Unutar PPP paketa moguće je oviti jedan LCP paket. Oznaka u polju s opisom protokola tada je „c021“ čime se naznačuje da polje PPP paketa s podacima sadrži LCP paket. Svaki LCP paket sastoji se od polja s oznakom paketa, s ID oznakom, polja u kojem je upisana duljina paketa i polja s podacima, kao što je prikazano na slici Slika 5.

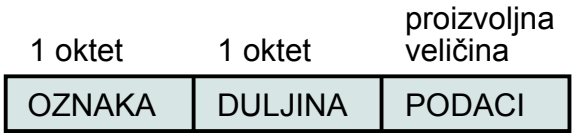


Slika 6: LCP podatkovni paket

Polje s oznakom paketa dugo je jedan oktet i nosi oznaku vrste LCP paketa. Na pakete koji imaju nepoznatu oznaku odgovara se *Code-Reject* paketom. ID oznaka paketa koristi se za povezivanje pojedinih odgovora s pripadnim zahtjevima. Paketi s neispravnom ID oznakom se zanemaruju.

5.1.2. LCP postavke

LCP postavke (eng. *Configuration Options*) omogućuju izmjenu postavki PPP veze. Ako se *Configure-Request* paketom ne zatraži izmjena pojedine postavke, koristi se njezino izvorno podešenje. LCP postavke, strukture kao na slici Slika 7, prenose se u polju s podacima LCP paketa. Sastoje se od oznake postavke koja se podešava, polja u kojem je zapisana duljina strukture i polja s podacima čiji sadržaj ovisi o podešavanoj postavci.



Slika 7: LCP postavka

Neke od oznaka postavki koje je moguće odabrati su:

0 oznaka rezervirana za buduću uporabu
1 *Maximum-Received-Unit* postavka određuje veličinu PPP paketa. Izvorno je podešena na 1500 okteta.
3 *Authentication-Protocol* postavkom odabire se autorizacijski protokol.
4 *Quality-Protocol* postavka se koristi za odabir protokola kojim se nadzire kvaliteta veze.
5 *Magic-Number* postavka omogućuje uočavanje pogrešaka karakterističnih za podatkovni sloj OSI mrežnog modela.
7 *Protocol-Field-Com* postavka omogućuje kompresiju polja PPP paketa s oznakom protokola.
8 *Address-And-Control-Field-Compression* je također postavka koja omogućuje kompresiju pojedinih polja PPP paketa.

5.2. NCP protokoli

Osnovne prednosti PPP protokola su njegova prilagodljivost i nadogradivost. Iako je prvotno osmišljen za prenošenje IP podatkovnih paketa ostavljena je mogućnost proširenja funkcionalnosti i na prenošenje paketa drugih protokola mrežnog sloja te na istovremeno prenošenje paketa različitih protokola.

Podržavanje višestrukih protokola 3. sloja jedinstvenim i kompaktnim PPP protokolom zahtijevalo bi poznavanje specifičnih karakteristika svakog podržanog protokola. Osim toga, u opisanom slučaju bila bi potrebna neprestana nadogradnja takvog PPP protokola kako bi se podržali novi protokoli mrežnog sloja i kako bi se održala kompatibilnost s postojećim protokolima za koje su definirani novi parametri.

Umjesto opisanog neprilagodljivog modela, PPP protokol je građen modularno tako da je za svaki podržani protokol mrežnog sloja definiran poseban NCP protokol. Pojedini NCP protokol upravlja interakcijom s pridruženim mu protokolom mrežnog sloja rješavajući pri tom specifične poteškoće vezane uz njega.

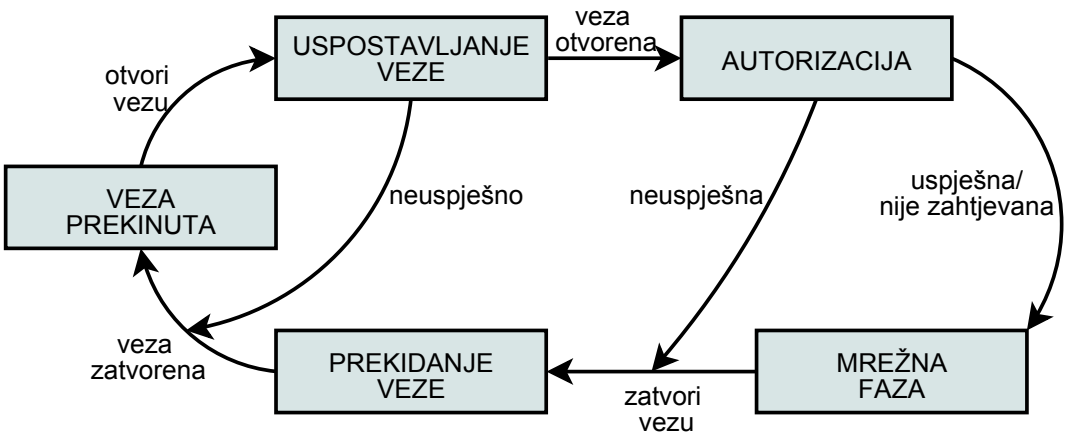
Primjeri NCP protokola su: IPCP (eng. *Internet Protocol Control Protocol*), IPXCP (eng. *Internetwork Packet Exchange Control Protocol*) i ATCP (eng. *AppleTalk Control Protocol*) protokoli koji su redom namijenjeni uspostavljanju, podešavanju i prekidanju komunikacije prema IP, IPX, odnosno *AppleTalk* protokolu preko PPP veze. Navedeni protokoli, kao i ostali NCP protokoli, koriste mehanizam razmjene podatkovnih paketa jednak onom LCP protokola, a prihvaćaju se samo paketi pristigli nakon početka mrežne faze PPP protokola prikazanoj na slici Slika 8.

6. Dijagram stanja PPP protokola

Postupak uspostavljanja, podešavanja, održavanja i prekidanja PPP veze provodi se u pet faza:

1. veza prekinuta,
2. uspostavljanje veze,
3. autorizacija,
4. mrežna faza i
5. prekidanje veze.

Navedene faze prikazane su na slici Slika 8.



Slika 8: Dijagram stanja PPP protokola

6.1. Faza prekinutosti veze

Svaka PPP veza nužno započinje i završava ovom fazom. Faza prekinutosti veze (eng. *link dead*) završava obaviješću o spremnosti fizičkog sloja na uspostavljanje veze. Takva obavijest može na primjer potjecati od algoritma uočavanja nosioca signala ili može nastati uslijed djelovanja administratora. Završetak ova faze znači prelazak PPP algoritma u fazu uspostavljanja veze.

6.2. Faza uspostavljanja veze

Tijekom faze uspostavljanja veze (eng. *link establishment phase*) LCP protokol se koristi za razmjenu *Configure* podatkovnih paketa kojima se prenose postavke veze. Razmjena takvih paketa je završena kada su obje strane poslale i primile *Configure-Ack* pakete. Pretpostavljeni su izvorni iznosi svih postavki veze koje nisu izmijenjene *Configure* paketima.

Tijekom ove faze podešavaju se samo postavke neovisne o pojedinim protokolima mrežnog sloja. Podešavanje postavki vezanih uz protokole trećeg sloja provodi se tijekom mrežne faze od strane odgovarajućih NCP protokola.

U ovu fazu moguće je, osim iz faze prekinutosti veze, ući i iz mrežne faze te iz faze autorizacije u slučaju primitka *Configure-Request* paketa koji predstavlja zahtjev za ponovnim podešavanjem postavki PPP veze.

6.3. Faza autorizacije

Izvorne postavke PPP protokola ne zahtijevaju autorizaciju mrežnih čvorova koji uspostavljaju PPP vezu. U pojedinim primjenama moguće ju je zahtijevati prije razmjene paketa protokola mrežnog sloja. Tada je tijekom faze uspostavljanja veze potrebno odrediti korišteni autorizacijski protokol.

Autorizaciju je poželjno provesti čim prije nakon završetka faze uspostave veze. U isto vrijeme moguć je početak postupka utvrđivanja kvalitete uspostavljene veze. Zbog toga je unutar pojedine implementacije PPP protokola potrebno spriječiti onemogućavanje autorizacije uslijed razmjene paketa za određivanje kvalitete veze.

Prelazak u mrežnu fazu nije dozvoljen do uspješnog okončanja autorizacije. U slučaju neuspjele autorizacije iz ove faze prelazi se u fazu prekidanja veze. Tijekom autorizacije dozvoljena ja razmjena isključivo LCP paketa, autorizacijskih paketa i paketa kojima se nadzire kvaliteta veze. Svi ostali paketi primljeni tijekom ove faze zanemaruju se.

Autorizaciju je preporučeno implementirati tako da se izostanak odgovora na zahtjev ne interpretira kao neuspjela autorizacija već da se u takvom slučaju provodi neki od mehanizama ponovnog slanja zahtjeva. Kod takvih implementacija autorizacija se smatra neuspjelom tek nakon određenog broja pokušaja.

6.4. Mrežna faza

Nakon završetka prethodno opisanih faza potrebno je posebno podesiti sve korištene protokole mrežnog sloja. Ovu zadaću rješavaju NCP protokoli, čije djelovanje je moguće pokrenuti i prekinuti u bilo kojem trenutku unutar ove faze.
Nakon završetka podešavanja potrebnih NCP protokola PPP protokol prenosi podatkovne pakete odgovarajućih protokola mrežnog sloja. Primljeni paketi podržanog protokola mrežnog sloja za kojega odgovarajući NCP protokol nije podešen se zanemaruju, a paketi nepodržanih protokola vraćaju se unutar *Protocol-Reject* paketa.
Tijekom ove faze preko uspostavljene veze prenose se LCP, NCP i paketi protokola mrežnog sloja.

6.5. Faza prekidanja veze

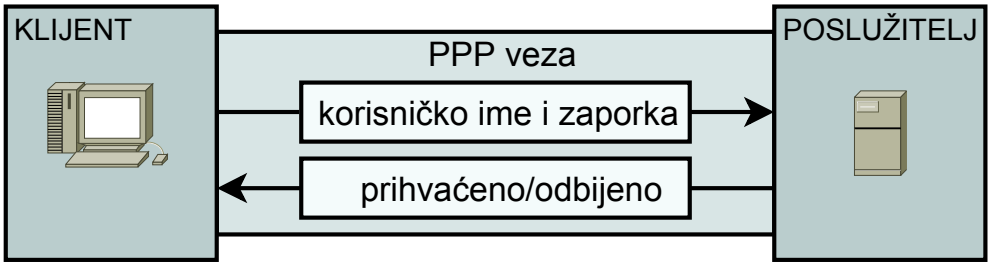
PPP protokol može prekinuti vezu u bilo kojem trenutku. Prekid može biti uzrokovan gubitkom signala nosioca, neuspjelom autorizacijom, degradacijom kvalitete veze ili njenom neaktivnošću, a moguće je i zatvaranje PPP veze od strane administratora. PPP protokol aktivne protokole mrežnog sloja obavještava o prekidanju veze kako bi mogli izvršiti potrebne postupke prije konačnog zatvaranja veze.
Prekidanje veze provodi LCP protokol razmjenom *Terminate* paketa. Nakon razmjene ovih paketa fizičkom sloju šalje se zahtjev za isključivanjem kako bi se osiguralo prekidanje PPP veze. Ovo je naročito bitno u slučaju zatvaranja veze uslijed neuspjele autorizacije. Pošiljatelj *Terminate-Request* paketa, kojim se zahtjeva gašenje veze, isključuje se nakon primitka *Terminate-Ack* paketa, kojim druga strana potvrđuje primitak zahtjeva, ili nakon isteka određenog vremena (određenog *Restart* parametrom) od slanja spomenutog zahtjeva. Primatelj *Termonate-Request* paketa čeka isključenje druge strane i istjecanje najmanje jednog *Restart* vremenskog perioda prije vlastitog isključivanja.
Svi paketi primljeni tijekom ove faze koji ne pripadaju LCP protokolu zanemaruju se.

7. Protokoli za autorizaciju: PAP i CHAP

Izvorne postavke PPP protokola ne zahtijevaju autorizaciju korisnika prilikom povezivanja, ali u primjenama gdje je to potrebno moguće ju je implementirati. Autorizacija se tada provodi nakon uspostavljanja PPP veze i odabira autorizacijskog protokola, a prije početka mrežne faze. U ovom postupku pozivač, strana koja zahtjeva uspostavljanje PPP veze, šalje svoje autorizacijske podatke kako bi druga strana mogla odrediti ima li pozivač dozvolu mrežnog administratora za uspostavljanje zatražene veze. U slučaju povezivanja dvaju ravnopravnih mrežnih čvorova oni međusobno razmjenjuju autorizacijske poruke. U postupku podešavanja postavki PPP protokola moguće je odabrati PAP ili CHAP protokol za autorizaciju.

7.1. PAP autorizacija

Autorizacija PAP (eng. *Password Authentication Protocol*) protokolom provodi se u dva koraka, i prikazana je na slici Slika 9. Nakon završetka faze uspostavljanja veze mrežni čvor koji se autorizira opetovano šalje korisničko ime i zaporku dok ne dobije potvrdu o uspješnoj autorizaciji ili do prekida veze.



Slika 9: Autorizacija u dva koraka PAP protokolom

U tablici Tablica 2 prikazan je sadržaj PAP podatkovnih paketa. Tri su vrste PAP paketa:

- zahtjev za autorizacijom,

- paket koji potvrđuje uspješnu autorizaciju i
- paket s obaviješću o neuspješnoj autorizaciji.

Svi paketi započinju oznakom, koja određuje kojoj vrsti pojedini paket pripada, nakon koje slijedi identifikacijska ID oznaka koja povezuje pakete jednog pokušaja autorizacije, zatim oznaka duljine korisničkog imena ili cijelog paketa, ovisno o vrsti paketa, te polje s korisničkim imenom. Paket sa zahtjevom za autorizacijom sadrži još i oznaku duljine korisničke zaporke i samu zaporku.

Opis paketa	Duljina polja u oktetima						
	1	1	2	1	promjenjiva	1	promjenjiva
zahtjev	oznaka = 1	ID	duljina	duljina imena	korisničko ime	duljina zaporke	zaporka
autorizacija uspješna	oznaka = 2	ID	duljina	duljina poruke	korisničko ime	–	
autorizacija neuspješna	oznaka = 3	ID	duljina	duljina poruke	korisničko ime		

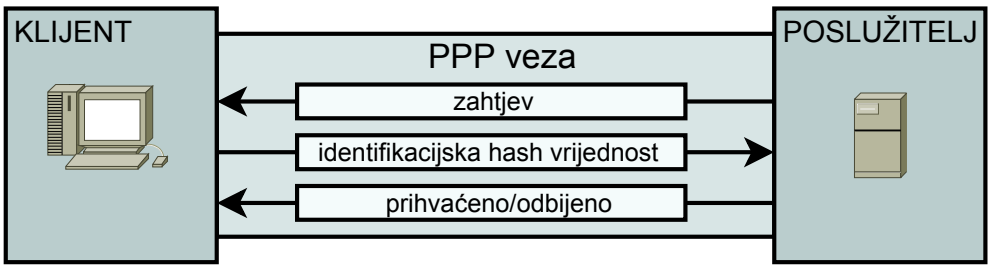
Tablica 2: Sadržaj PAP podatkovnih paketa

PAP se smatra nesigurnim autorizacijskim protokolom jer se korisnički podaci prenose zapisani ASCII (eng. *American Standard Code for Information Interchange*) kodom te zbog toga što ne postoje mehanizmi zaštite od napada krađom korisničke zaporke (eng. *replay attack*) i napada nagađanjem korisničkih podataka (eng. *trial-and-error attack*). Dio nedostataka ovog protokola proizlazi iz činjenice da udaljeni mrežni čvor započinje postupak autorizacije i kontrolira učestalost pokušaja.

7.2. CHAP autorizacija

Autorizacija CHAP (eng. *Challenge-Handshake Authentication Protocol*) protokolom provodi se neposredno nakon završetka faze uspostavljanja veze te se može ponoviti u bilo kojem trenutku tijekom trajanja veze. Postupak se temelji na dijeljenoj tajni, a provodi se u tri koraka:

1. Autorizator, mrežni čvor na kojega se druga strana povezuje, šalje zahtjev za autorizacijom.
2. Čvor koji se autorizira na zahtjev odgovara proračunatom vrijednošću jednosmjerne funkcije (eng. *hash*). Na primjer, ovaj odgovor može sadržavati MD5 (eng. *Message Digest algorithm 5*) kontrolnu sumu korisničke zaporke i vrijednosti zahtjeva.
3. Autorizator provjerava primljenu vrijednost jednosmjerne funkcije uspoređivanjem s vlastitim izračunom iste veličine. Ako su njihovi iznosi jednaki autorizacija je uspješno provedena, a u suprotnom veza se prekida.



Slika 10: Autorizacija u tri koraka CHAP protokolom

CHAP protokol definira četiri vrste podatkovnih paketa:

- zahtjev za autorizacijom,
- odgovor na zahtjeva za autorizacijom,
- paket koji potvrđuje uspješnu autorizaciju i
- paket s obaviješću o neuspješnoj autorizaciji.

Paketi započinju oznakom tipa, slijedi ID identifikacijska oznaka pokušaja autorizacije i duljina paketa. Paketi sa zahtjevom i odgovorom sadrže polja s oznakama duljine vrijednosti zahtjeva, odnosno odgovora, te polja sa samim vrijednostima zahtjeva i odgovora. Vrijednost zahtjeva (eng. *challenge value*) jedinstvena je za svaki pokušaj autorizacije, a vrijednost odgovora (eng. *response*

value) dobiva se izračunom jednosmjerne funkcije nad iznosom dobivenim ulančavanjem ID oznake, dijeljene tajne (npr. korisnička zaporka) i vrijednosti zahtjeva. Ime predstavlja oznaku računalnog sustava, pošiljatelja paketa. Paketi s obaviješću o uspješnosti ili neuspjehu autorizacije sadrže polje s porukom. Ova poruka prikazuje se korisniku koji se pokušava prijaviti i najčešće je zapisana ASCII kodom.

	Duljina polja u oktetima					
Paket	1	1	2	1	promjenjiva	promjenjiva
zahtjev	oznaka = 1	ID	duljina	duljina vrijednosti zahtjeva	vrijednost zahtjeva	ime
odgovor	oznaka = 2	ID	duljina	duljina vrijednosti odgovora	vrijednost odgovora	ime
autorizacija uspješna	oznaka = 3	ID	duljina	–	poruka	–
autorizacija neuspješna	oznaka = 4	ID	duljina	–	poruka	–

Tablica 3: Sadržaj CHAP podatkovnih paketa

CHAP protokol zaštićen je od napada krađom korisničke zaporke korištenjem jedinstvene i nasumične vrijednosti zahtjeva kod svake autorizacije što rezultira jedinstvenim iznosom jednosmjerne funkcije. Ponovljenim zahtjevima za autorizacijom tijekom trajanja veze skraćuje se vrijeme koje napadač ima za zlonamjerno djelovanje u slučaju uspješne krađe PPP veze. Mrežni čvor na kojega se drugi povezuju započinje autorizaciju i kontrolira učestalost pokušaja.

8. Zaključak

PPP (eng. *Point-to-Point Protocol*) je protokol podatkovnog sloja OSI modela koji se koristi za izravno povezivanje dvaju računala serijskim, telefonskim ili optičkim kabelom, pomoću mobilnih telefona te posebno oblikovanom radio ili satelitskom vezom. Ovaj protokol omogućuje povezivanje različitih računala, premosnika i usmjerivača te simultano dvosmjerno dostavljanje podatkovnih paketa redoslijedom kojim su poslani.

PPP protokol je građen modularno iz čega proizlaze njegove glavne prednosti: prilagodljivost i nadogradivost. Sastoji se od dva sloja, nižeg na kojem djeluje LCP protokol i višeg unutar kojega je moguć istovremen rad većeg broja NCP protokola. LCP (eng. *Link Control Protocol*) protokol provodi usuglašavanje postavki formata ovijanja i veličine podatkovnih paketa, uočava pogreške proizišle iz neispravnih postavki, prekida vezu te omogućuje autorizaciju korisnika i otkrivanje neispravnog funkcioniranja veze.

Za svaki protokol mrežnog sloja nadređen PPP protokolu definiran je poseban NCP (eng. *Network Control Protocol*) protokol. Ovime je omogućeno jednostavno proširivanje PPP protokola kako bi se podržali novi protokoli mrežnog sloja i kako bi se osigurala kompatibilnost s novim inačicama postojećih protokola.

Visoka razina podesivosti prisutna je i kod mehanizma autorizacije unutar PPP protokola. Uspostavljanje veze moguće je provesti bez autorizacije ili uz autorizaciju PAP (eng. *Password Authentication Protocol*) ili CHAP (eng. *Challenge-Handshake Authentication Protocol*) protokolom. Osnovna prednost PAP protokola je njegova široka rasprostranjenost dok CHAP protokol pruža daleko veću razinu sigurnosti.

9. Reference

[1] Point-to-Point Protocol, http://en.wikipedia.org/wiki/Point_to_Point_Protocol, ožujak 2007.

[2] Serial communications, http://en.wikipedia.org/wiki/Serial_communications, ožujak 2007.

[3] W. Simpson: The Point-to-Point Protocol (PPP), http://tools.ietf.org/html/rfc1661, ožujak 2007.

[4] Point-to-Point Protocol Field Assignments, http://www.zvon.org/tmRFC/RFC1700/Output/chapter54.html, ožujak 2007.

[5] Cisco Certified Network Associate 4: WAN Technologies v3.1.1, Module 3: PPP

[6] Link Control Protocol, http://en.wikipedia.org/wiki/Link_Control_Protocol, ožujak 2007.

[7] PPP Network Control Protocols (IPCP, IPXCP, NBFCP and others), http://www.tcpipguide.com/free/t_PPPNetworkControlProtocolsIPCPIPXCPNBFCPandothers.htm ,ožujak 2007.

[8] Password authrntication protocol, http://en.wikipedia.org/wiki/Password_authentication_protocol, ožujak 2007.

[9] Challenge-handshake authentication protocol, http://en.wikipedia.org/wiki/Challenge-handshake_authentication_protocol, ožujak 2007.