Mrežni protokoli - I deo

Kako je u prethodnom poglavlju opisano, komunikacija na računarskim mrežama definisana je modelima, OSI i TCP/IP, koji imaju sedam, odnosno četiri nivoa. Na svakom nivou odvija se komunikacija po unapred sefinisanim pravilima – po protokolu određenog nivoa. Protokoli svih nivoa su standardizovani od strane međunarodnih organizacija za standardizaciju (IETF, IEEE, ISO, ITU-T, i dr.). U ovom poglavlju biće opisani prookoli TCP/IP mrežnog modela, počev od fizičkog, zaključno sa aplikativnim nivoom.

3.1. Paketne mreže

Generalno, postoje dva tipa mreža:

- komutacija kanala, i

- komutacija paketa, ili paketne mreže.

Istorijski gledano, prvi vidovi telekomunikacija bili su bazirani na komutaciji kanala. Na početku razvoja, u centrali postojalo je radno mesto operatera, pa je telefonski poziv uspostavljan tako što se prvo uspostavljala veza sa operaterom. Operateru se davao nalog da pozove određeni broj, a operater je u bukvalnom smislu prespajao dva odgovarajuća priključka na tabli sa onoliko priključaka koliko telefonskih brojeva u gradu ima.

|  |  |
| --- | --- |
|  |  |
| **Sika 3.2.** Primer mreže sa komutacijom kanala | |

Velika mana ovakvog načina komunikacije je ta da je ceo komunikacioni kanal bio „zauzet“ u toku komunikacije. U slučaju međumesnih veza, gde je postojalo samo par kanala između gradova bilo je izuzetno skupo zauzeti kanala. Drugim rečima, ako jedan korisnik koristi jedan od dva kanala, koliko ih operater poseduje, korisnik zauzima 50% kapaciteta telekomunikacione kompanije, pa shodno tome iznosi i njegov račun.

Vremenom kapaciteti su povećani, a operatere sa slike zamenile su automatske centrale, tako da su troškovi u tom pogledu smanjeni. Međutim, i automatske centrale imale su istu ulogu kao i operateri sa slike.

Drugi koncept mreža, koji je u mnogome oborio cenu komunikacija, pa samim tim i doveo do ekspanzije mreža kakvu danas poznajemo u vidu Inteneta, jesu paketne mreže. Ideja paketnih mreža je da korisnik prenosi malu količinu informacija za veoma kratko vreme, nakon čega oslobađa kanal kako ga mogu koristiti drugi korisnici. Veći broj korisnika – manja cena prenosa podataka.

Paketne mreže su mnogostruko komplikovanije od mreža sa komutacijom kanala, pa sam prstup u razmatranju ovakvih mreža je zbog jednostavnosti izučavanja podeljen u slojeve, kako je to u prethodnom poglavlju objašnjeno. U ovom poglavlju biće reči o slojevima TCP/IP modela, kako modela na kome se zasniva Internet.

3.2. Sloj pristupa mreži

Sloj pristupa mreži, po TCP/IP specifikaciji, praktično se sastoji od dva podsloja. To su **fizički** i **nivo linka** (eng. *Data Link Layer*), po OSI specifikaciji. Fizički nivo predstavlja sam medijum, odnosno komunikacioni kanal kroz koji se prenose informacije i može biti žičani, optički ili bežični. Kod žičanog informacije se prenose u vidu električnog napona, kod optičkog putem svetlosnih zraka, dok se kod bežičnog informacije prenose elektromagnetnim talasima. Posmatrano sa fizičkog nivoa, slično kao u prethodnom primeru sa dispečerom i patrolama, prenose se električni impulsi bez ulaženja u detalje šta ti impulsi zapravo znače. Na ovom nivou definišu se električne (odnosno elektromagnetne, ili optičke) karakteristike komunikacionog kanala, kao što su: nivo napona, jačina struje, dozoljeno slabljenje, predajna snaga antene, ili jačina i talasna dužina svetlosnog snopa ako je optika u pitanju, kao i konektori koji se koriste za povezivanje, s jedne strane, i način na koji se predstavljaju informacije (binarne cifre 0 i 1, ili dr) sa druge strane.

Na nivou linka protokolom je definisano kako se kroz medijum, električni, optički ili elektromagnetni prenose cele poruke u vidu grupa binarnih nila i jedinica iz jedne tačke u drugu. Na ovom nivou poruke koje se razmenjuju zovu se **frejmovi** (eng. *frame* – *okvir, ram, uramljeni*). U bukvalnom prevodu frejm znači okvir, tj. uovireni ili uramljeni podaci. Na sledećoj slici je prikazan izgled jednog okvira:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Start | Odredište | Izvor | Tip | **Podaci** | CRC |

**Slika 3.3.** Tipičan izgled okvira

Na ovom nivou, pre slanja samih podataka, izvorna strana mora poslati signal za start, mora navesti kome su podaci namenjeni (odredište), mora navesti svoju identifikaciju (izvor) kako bi odredište znalo kome treba da odgovori, mora navesti tip poruke, pa tek tada može početi sa prenosom podataka. Nakon prenosa podataka izvor dodaje specijalnu informaciju koja se korsti na idredišnoj strani za proveru da li je došlo do greške prilikom prenosa. Ovo se naziva **format poruke**. Pored formata protokol definiše i redosled slanja poruka.

Na nivou linka najpoznatiji su **Ethernet** i **PPP** protokol. Pored ova dva protokola, tu su i TokenRing, AppleTalk, SLIP, i dr.

Za raliku od OSI modela, TCP/IP model objedinjuje fizički i nivo linka u jedan nivo i naziva ih jedinstvenim imenom **sloj pristupa mreži**. Ovo je uglavnom zbog toga što se obično ova dva nivoa implementiraju hardverski na jednoj kartici. Da bi računar pristupio nekoj mreži mora biti opremljen odgovarajućom karticu za tu mrežu. U zavisnosti od tipa računara u koji se kartica ugrađuje razlikujemo **PCI** (za desktop) i **PCMCIA** kartice za laptop računare, a u zavisnosti od tipa mreže kojoj želimo da pristupimo razlikujemo:

- Ethernet kartice – za pristup lokalnim mrežama;

- Wireless kartice – za pristup bežičnim mrežama;

- Modeme i ISDN uređaje – za pristup mreži preko telefonskog priključka;

- ADSL – za pristup mreži preko ADSL-a;

- Kablovske – za pristup kablovskoj mreži.

Na sledećoj slici su prikazane dve varijante kartica: PCI i PCMCIA i način ugradnje u računar.

|  |  |
| --- | --- |
|  |  |

**Slika 3.4.** PCI i PCMCIA kartice

Na sledećoj slici prikazane su Ethernet i Wireless kartice u obe varijante.

|  |  |
| --- | --- |
|  |  |
|  |  |

**Slika 3.5.** Ethernet i Wireless kartice u PCI i PCMCIA varijanti

Većina proizvođača danas Ethernet mrežne kartice ugrađuje u matične ploče računara.

3.2.1. Ethernet

Od tipa mreže na koju se računar povezuje zavisi koji će se **data link** protokol (protokol druog nivoa OSI modela) koristiti. Lokalne mreže, ili skraćeno LAN, u današnje vreme skoro bez izizetka koriste Ethernet kao protokol za pristup mreži. Drugi protokol ovog nivoa, takođe široko rasprostranjen za pristup WAN mrežama i Internetu preko modema, ISDN-a i sličnih uređaja je PPP, i o njemu će biti reči kasnije.

Ethernet je protokol koji je razvijen za lokalne mreže sa dva ili više od dva računara kod kojih računari prisutpaju deljivom medijumu za prenos informacija. Ethernet lokalne mreže imaju zajednički deljvi medijum preko koga uređaji komuniciraju.

Ethernet sloj za pristup mreži, u TCP/IP terminologiji, čini skup gradivnih elemenata koji omogućavaju računaru pristup lokalnoj mreži. Gradivni elementi etherneta su specifikacija tipa kalbova i konektora koji se koriste, ograničenja po pogledu kabliranja u vidu maksimalne moguće dužine kablova, način na koji računari međusobno komuniciraju, i sl.

Bez obzira što danas Ethernet dominira na lokalnim mrežama, pre deceniju - dve na lokalnim mrežama je bilo moguće naći i protokole kao što su **TokenRing** i **ARCNet**. TokenRing je IBM-ov standard koji se danas uglavnom koristi u velikim organizacijama kod kojih postoji IBM-ov „glavni računar“ (eng. *mainframe*) sa više terminala koji mu pristupaju. ARCNet danas nalazi primenu u industrijskim mrežama, kao što je na primer mreža na koju su povezani industrijski roboti na proizvodnoj traci. Danas, kako je već rečeno, dominira Ethernet. Ethernet kartice je veoma lako nabaviti u bilo kojoj specijalizovanoj radnji, po veoma niskim cenama.

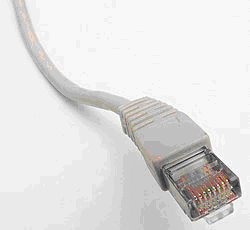
Kada se govori o Ethernetu, prvenstveno se misli na skup standarda koji definišu lokalnu mrežu sa Ethernet protokolom na drugom nivou OSI modela. Svi poznati operativni sistemi (Windows, NetWare, Linux, Unix, MacOS, Symbian, i dr) imaju podršku za Ethernet i moguće je preko ovog tipa mreže povezati različite operativne sisteme u jednu mrežu.

3.2.1.1. Ethernet standardi

Ethernet je originalno razvila kompanija **Xerox PARC** 1973-1975. godine.Godine 1975. Xerox je objavio patente navodeći imena Roberta Metcalfea, Davida Bouggsa, Chuck Thackera i Butler Lampsona kao pronalazače **sistema za komunikaciju sa više pristupnih tačaka sa detekcijom kolizije**. Eksperimentalni Ethernet je radio na brzini od 3 Mbps i mogao da podrži do 255 računara na mreži. Metcalfe je napustio Xerox 1979. godine i osnovao firmu 3Com, koja je u kooperaciji sa firmom DEC, Intelom i Xeroxom 1980. godine standardizovala 10 Mbps Ethernet. Međunarodno udruženje IEEE standardizovalo je Ethernet i po IEEE oznaci Ethernet nosi naziv 802.3 (osamstodva-tačka-tri standard). Ethernet je od 1980. godine pretrpeo mnoga unapređenja tako da današnji Ethernet podržava 1 Gbps i 10 Gbps lokalne mreže. U sledećoj tabeli navedeni su neki od Ethernet standarda koji su razvijeni počev od 80-tih do donašnjih dana.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Standard** | **Brzina** | **Medijum** | **Maksimalna dužina segmenta** | **Topologija** | **Konektor** |
| 10BASE2 | 10 Mbps | 50ohm koaksijalni (tanki) | 185m | Magistrala | BNC |
| 10BASE5 | 10 Mbps | 50ohm koaksijalni (debeli) | 500m | Magistrala | AUI |
| 10BASE-T | 10 Mbps | UTP kategorije 3, 4 ili 5, osmožilni, koriste se dve parice | 100m | Zvezda | RJ-45 |
| 100BASE-TX | 100 Mbps | UTP kategorije 3, 4 ili 5, osmožilni, koriste se dve parice | 100m | Zvezda | RJ-45 |
| 100BASE-FX | 100 Mbps | Optičko flakno 62.5/50 | 400m | Zvezda | ST ili SC |
| 1000BASE-CX | 1000 Mbps | Oklopljeni UTP – STP kabl | 25m | Zvezda | RJ-45 |
| 1000BASE-T | 1000 Mbps | UTP kategorije 5, osmožilni, koriste se četiri parice | 100m | Zvezda | RJ-45 |

Danas najzastupljeniji Ethernet konektor je RJ-45, koji je prikazan na slici.

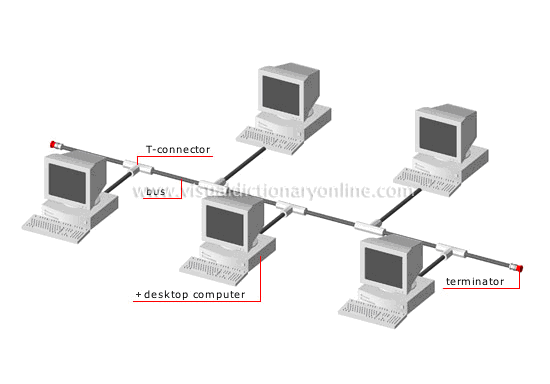


Ethernet je originalno projektovan za komunikaciju više računara preko koalksijalnog kabla (10BASE2 i 10BASE5). Mrežna kartica 10BASE2 Etherneta i koaksijalni kabl sa BNC konektorima su prikazani na slici.

|  |  |
| --- | --- |
|  |  |

**Slika 3.6.** BNC kartica i kabl

Koaksijalni vod ima slične osobine kao i radio sistemi. Zajednički kabl na koji su povezani svi računari (slika) ima ulogu etra za komunikaciju (eng. *ether*, odakle se izvodi reč *Ethernet*).



Od ovog jednostavnog koncepta, Ethernet je evoluirao u veoma složen sitem koji uključuje linkove od računara do centra ožičavanja, hub-a, ili switch-a i podržava i 1.000 puta veće brzine od originalnih. Koaksijalni kabl je zamenjen UTP kablom, kablom sa upredenim paricama, koji ima bolje karakteristike od koaksijalnog kabla u pogledu osetljivosti na smetnje i pouzdanosti. Takođe, kabl sa upredenim paricama, UTP (eng. *unshilded twisted pair*) je jefitiniji i jednostavniji za ugradnju od koaksijalnog kabla. Pored navedenih prednosti UTP kabla, potrebno je istaći i jednostavnije održavanje UTP mreža. Naime, kod 10BASE2 mreža otkaz dela mreže prouzrokuje otkaz cele mreže, pa je teško lokalizovati kvar, dok kod UTP-a otkaz dela na kome je računar je lokalizovan i lako ga je pronaći jednostavnim praćenjem LED dioda na hub-u ili switch-u.

Bitno je istaći to da svaki računar na Ethernet mreži ima **jedinstvenu adresu** koja se naziva **MAC** adresa (eng. ***M****edia* ***A****ccess* ***C****ontrol – upravljanje pristupom medijumu*). Ova adresa je 48-bitna, tako da je, teoretski, na jednoj lokalnoj mreži moguće adresirati 248 uređaja.

MAC adresa se predstavlja sa 12 heksadekadnih cifara (cifre su: 0,1,2,3,...,9,A,B,C,D,E i F), gde se jednom heksa cifrom zamenjuju 4 bita.

Primer MAC adrese: **00-1C-AA-05-11-FA**.

MAC adresa se nalazi u samom Ethernet kontroleru na mrežnoj kartici i (uglavnom) je nije moguće menjati. Jedinstvenost adrese se postiže na taj način da svaki proizvođač ima svoj kod koji upisuje u prvu polovinu MAC adrese, dok druga polovina predstavlja serijski broj kartice.

Napomena: MAC adresa Ethernet kontrolera se može saznati iz command prompta Windowsa naredbom **ipconfig /all**. Na osnovu MAC adrese moguće je odrediti proizvođača kartice (<http://www.techzoom.net/lookup/check-mac.en>).

Bez obzira na značajnu promenu fizičkog nivoa Etherneta od koaksijalnog do 1 Gbps i bržih UTP mreža, format Ethernet frejma je ostao nepromenjen:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Start | MAC odredišta | MAC izvora | Tip | **Podaci** | CRC |

**Slika 3.7.** Ethernet frejm

Nakon start signala računar koji šalje frejm šalje MAC adresu odredišta kome je frejm namenjen, nakon čega šalje i svoju MAC adresu, kako bi odredište znalo kome da vrati odgovor. Za poljem koje označava tip šalju se podaci. Polje za podatke ne sme biti duže od 1.500B (1.5kB), kako je definisano standardom. Razlog za ograničenje maksimalne dužine frejma je uvođenje ravnopravnosti prilikom slanja, inače bi kada jedan računar počne prenos velike količine podataka svaka druga komunikacija na mreži bila nemoguća.

Napomena: Ukoliko računar prenosi više od 1.5kB podataka, te podatke deli u delove od po 1.5kB i šalje jedan po jedan deo (frejm). Npr. 150 kB podataka mora biti podeljeno u 100 frejmova.

3.2.1.2. Ethernet kablovi

Međunarodna organizacija za standardizaciju, EIA-TIA, standardizovala je izgled ethernet kabla na sledeći način:

- za konektor ethernet kabla koristi se RJ-45 konektor sa **8 pinova** (konektor za telefon je sa 4 pina i oznaka je RJ-11);

- Ethernet kabl sastoji se od četiri parice (4x2=8 žica), koje su upredene na određeni način tako da je nivo šuma minimalan;

- parice su različitih boja, a svaka parica ima jednu vezu u boji, a druga veza je kombinacija osnovne boje i bele; parice su: zelena + zeleno-bela, narandžasta + narandžasto-bela, plava + plavo-bela i braon + braon-bela;

- postoje dve mogućnosti povezivanja parica u konektoru i obe su prikazane u tabeli (T568A i T568B);

Za povezivanje uređaja Ethernet kablom koriste se tri tipa kabla:

1. *Straight through*

2. *Crossover*

3. *Rollover*

Kako ime *straight through* bukvalno prevedeno sa engleskog znači direktno povezani, tako se ovaj tip kabla pravi direknom vezom odgovarajućih parica. To znači da raspored pinova u RJ-45 konektoru ovakvog kabla je ili na obe strane T568A, ili na obe strane T568B. Ovakav tip kabla se koristi prilikom povezivanja uređaja različitog tipa:

- računara na switch ili hub, i

- hub-a ili switcha na ruter.

*Crossover*, ili u prevodu upredeni ethernet kabl se dobija menjanjem mesta zelenoj i narandžastoj parici sa kraja na kraj kabla. Tako, ovakav tip kabla se dobija kada se na jednoj strani primeni T568A raspored, a na drugoj T568B. Ovakav tip kabla koristi se kada se povezuju uređaji istog tipa:

- PC na PC,

- Hub ili switch na hub ili switch, i

- Ruter na ruter.

Takođe, ova veza se koristi i prilikom direktnog vezivanja PC-ja na ruter.

tab. 1.1 asdasd

|  |  |  |  |
| --- | --- | --- | --- |
| **Pin** | **T568A** | **T568B** | **Raspored pinova na konektoru** |
| 1 | belo/zelena | belo / narandžasta |  |
| 2 | zelena | narandžasta |
| 3 | belo /narandžasta | belo / zelena |
| 4 | plava | plava |
| 5 | belo / plava | belo / plava |
| 6 | narandžasta | zelena |
| 7 | belo/braon | belo/ braon |
| 8 | braon | braon |

Veliki broj današnjih mrežnih kartica i uređaja su takozvane *auto-sense* (eng. *automatski-detektuj,* odnosno *oseti* u bukvalnom prevodu). Ovo znači da kartica sama može da prepozna ako je pogrešan tip kabla korišćen i da automatski prekonfiguriše sebe tako da zameni mesta odgovarajućim paricama. Tako, dve dva računara sa *auto-sense* karticama mogu se povezati bilo kojim tipom kabla.

Napomena: ukoliko se koristi pogrešan tip kabla, povezani uređaji neće moći da komuniciraju. Ovo ne može dovesti do oštećena i pregorevanja kartica! Korišćenje pogrešnog tipa kabla može se prepoznati po tome što LED diode na kartici uređaja ne svetle.

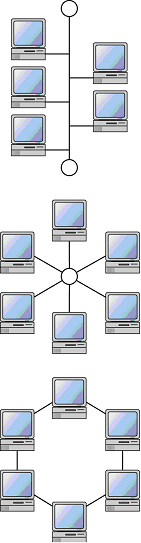
3.2.1.3. Topologije

Kada se govori o lokalnim mrežama i Ethernetu neophodno je reći i koje su topologije ovakvih mreža moguće. Generalno, postoje tri tipa topologija:

         Magistrala (eng. *Bus*)

         Prsten (eng. *Ring*)

         Zvezda (eng. *Star*)



Kod Etherneta se sreću topologije magistrale i topologija zvezde. Topologija prstena karakteristična je za TokenRing mreže. U tabeli gde su navedeni Ethernet standardi navedene su i topologije koje standard koristi. Tako, 10BASE2 i 10BASE5 Ethernet na koaksijalnim  vodovima koristi toplogiju magistrale, dok Ethernet standardi koji koriste UTP kablove imaju topologiju zvezde. U centru zvezde nalazi se **hub** ili **switch**. Koji imaju ulogu sabirnice/razdelnika i o njima će biti više reči kasnije.

3.2.1.4. CSMA/CD procedura

Sistem za komunikaciju sa više pristupnih tačaka sa detekcijom kolizije koji je patentirao Metcalfe (eng. ***C****arrier* ***S****ense* ***M****ultiple* ***A****ccess with* ***C****ollision* ***D****etect*), skraćeno CSMA/CD procedura, predstavlja srž Etherneta. Procedura za slanje frejma preko Etherneta je sledeća:

1.      kreira se frejm, u odgovarajuća polja se upisuje MAC adresa odredišta i MAC adresa računara koji šalje frejm;

2.      osluškuje se kanal i proverava se da li  je medijum slobodan za slanje ili ne; ukoliko je na medijumu neki prenos u toku čeka se na završetak prenosa;

3.      kada je medijum slobodan počinje se sa prenosom frejma;

4.      bez prekida se u toku slanja proverava da li je došlo do kolizije (istovremeno slanje od strane dva računara); ukoliko se detektuje kolizija prelazi se na proceduru za otklanjanje kolizije;

5.      kraj prenosa.

Procedura za otklanjanje kolizije je sledeća:

1.      nastavi sa slanjem paketa kako bi se mreža zagušila i svi računari na mreži mogli da detektuju da je došlo do kolizije;

2.      povećati pbojač kolizija za jedan;

3.      da li je brojač kolizija jednak dozvoljenom maksimumu (16), ako jeste prekini sa pokušajima da se frejm pošalje i javi višim nivoima da je slanje neuspešno;

4.      uzmi slučajan broj i čekaj toliko milisekundi do sledećeg prenosa;

5.      pređi na stavku 2 u glavnoj proceduri.

Glavna prednost ovog algoritma je otpornost na „sudare“ frejmova na medijumu do kojih dolazi, uprošćeno rečeno, ukoliko dva računara istovremeno počnu sa slanjem frejma. Ova otpornost na kolizije dobijena je tačkom 4 procedure za otklanjanje kolizije. Pretpostavka je da dva računara koja su prouzrokovala koliziju neće imati isto izabrano vreme čekanja pa će jedan početi retransmisiju pre drugog. Tako će drugi, koji kasnije počinje retransmisiju imati prilike da osluškujući kanal sazna da neko već šalje, i samim tim sačeka dok se ne završi slanje.

CSMA/CD algoritam može se predstaviti i na analogiji skupa ljudi gde svi prisutni ne govore istovremeno (kroz zajednički medijum - vazduh) i ne upadaju u reč jedni drugima. Ukoliko dva čoveka počnu da govore istovremeno, oba prestaju sa pričom i čekaju kratko (svako od učesnika proizvoljno, slučajno trajanje pauze). Uz pretpostavku da se izabrana slučajna vremena razlikuju, oba čoveka neće krenuti da govore u isto vreme, već će jedan od njih sa govorom krenuti ranije, tkao da je ovim izbegnuta kolizija. Svi prisutni čekaju završetak govora (koji je ograničenog trajanja), i tek tada mogu da krenu da govore, ali po istim pravilima.

3.2.1.5. ARP

Što se adresiranja tiče, svaki računar na lokalnoj mreži može komunicirati sa drugim računarom, pod uslovom da zna njegovu MAC adresu. Inicijalno, računar ne zna koji su sve računari prisutni na mreži. Preciznije, ne zna ni za jedan.

U oviru Etherneta razvijen je mehanizam koji se naziva ARP (*eng. Address Resolution Protocol – protokol za razrešavanje adresa*) koji rešava navedeni problem. Standardom je predviđeno da se svaki računar „odaziva“ na svoju MAC adresu, ali takođe i na „zajedničku“ (eng. *broadcast*) adresu. Ova adresa je MAC adresa kod koje su svih četrdesetiosam bitova binarne jedinice.

Ukoliko računar želi da sazna ko je sve **na lokalnoj mreži** prisutan, pripremiće frejm sa broadcast adresom u polju odredišne MAC adrese. Ovaj frejm, takozvani **ARP zahtev**, će primiti svi računari, a odazvaće se onaj koji prepozna svoju adresu slanjem **ARP ogovora**.

Napomena: Svaki računar čuva ARP tabelu u kojoj se nalaze MAC adrese računara sa kojima je komunicirao u poslednjih nekoliko minuta, zavisno od operativnog sistema. Na Windows računarima ova tabela se može izlistati iz komandne linije naredbom **arp –a**.

3.3. Mrežni nivo

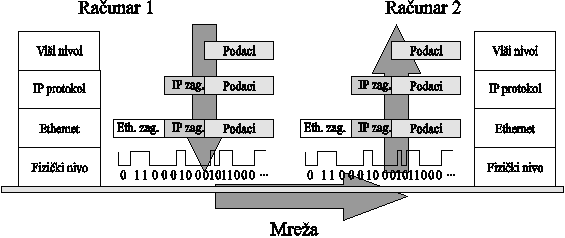
Intenet nivo u TCP/IP terminologiji, odnosno mrežni nivo kod OSI modela je ključni nivo koji omogućava međusobno povezivanje lokalnih mreža u jednu mrežu, pa može se u krajnjoj instanci reći i čini Internet mogućim. Primarna uloga ovog nivoa je definisanje adresne šeme računara.

Na ovom nivou nalaze se protokoli za komunikaciju na paketnim mrežama, kao što su IP, IPX, AppleTalk, X.25, i sl. U ovom poglavlju biće više reči o IP protokolu kao najznačajnijem protokolu na Internetu danas.

IP je skaćenica od **Internet Protokol**, a prva značajnija verzija ovog protokola je IPv4 (IP verzija 4). U današnje vreme postoji velika inicijativa za prelazak na novu verziju 6 ovog protokola, IPv6. Prednosti koje verzija 6 donosi u odnosu na verziju 4 biće diskutovane na kraju poglavlja.

3.3.1. IP enkapsulacija

Podaci protokola viših nivoa, u cilju slanja kroz mrežu, predaju se IP modulu koji realizuje IP protokol na Internet nivou. Ovaj nivo deli podatke koje treba poslati u pakete. Svaki paket sadrži zaglavlje paketa (eng. *header*) i, naravno, podatke dobijene od viših nivoa. Heder paketa sadrži, pored ostalog, mrežnu adresu odredišta i mrežnu adresu računara koji šalje paket. Ovako pripremljen paket predaje se nivou ispod koji dalje vrši enkapsulaciju na svom nivou i dodaje MAC adrese kao što je prethodno opisano.



**Slika 3.8.** Enkapsulacija

3.3.2. IP adresna šema

Kao što je već rečeno, primarna funkcija IP nivoa jeste adresiranje računara na mreži, uz napomenu da se mreža može sastojati od većeg broja lokalnih mreža. Po IP adresnoj šemi, svaki računar mora imati jedinstvenu adresu na mreži, **IP adresu**, kako se naziva na ovom nivou.

Logično pitanje koje se nameće jeste:

„Zašto uopšte uvoditi novi sloj, Internet sloj sa IP protokolom na njemu, i kratko rečeno komplikovati stvari, ako već na Ethernet mreži postoji nešto što se zove MAC adresa, i jedinstvena je na svakom računaru na svetu (!) ?“

Naime, Ethernet protokol (CSMA/CD) omogućio je implementaciju mreža po izizetno niskoj ceni sa relativno velikim brojem računara koji je moguće povezati na jednu lokalnu mrežu (teoretski ogromnim, 248 koliko kombinacija nula i jedinica u MAC adresi ima). Kako se broj računara sa mogućnošću povezivanja na mrežu povećavao, javio se problem sa adresiranjem velikog broja računara.

Da podsetimo: MAC adresa se sastoji od 48 binarnih cifara, od kojih su prve 24 binarne cifre oznaka proizvođača, dok su preostale 24 cifre serijski broj kartice. Iz razloga nepostojanja nikakve hierarhijske šeme u kreiranju MAC adresa, ARP tabela koju smo ranije pominjali, u kojoj se pamte MAC adrese računara na mreži bila bi prevelika!

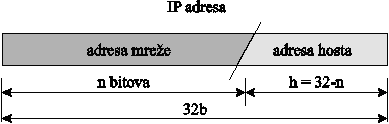
Kod Etherneta svaki računar mora da zna MAC adresu računara na svojoj mreži. Kada bi Internet bio jedna velika lokalna mreža, uz pretpostavku da je na Internet povezano 1.000.000.000 računara i uređaja, svaki od računara morao bi da ima MAC aresu svakog računara u ARP tabeli. MAC adresa je 48b = 6B, što ukupno za veličinu ARP tabele svakog računara iznosi 1GB!!! Čak i većina današnjih računara nema 1 GB RAM memorije koji bi odvojio samo za čuvanje ARP tabele, pored ostalih potreba koje nameće operativni sistem i korisnički programi, da ne govorimo o računarima osamdesetih i devedestih. S druge strane, i da računar i ima 2GB RAM-a, što bi bio neki minimum za normalni rad uz istovremenu povezanost na Internet, javlja se problem po pogledu brzine pretrage takve tabele. Svaka pretraga trajala bi dosta sporo. Nešto je bilo neophodno preduzeti. Tako je uveden novi sloj – Internet sloj.

MAC adrese i dalje ostaju aktuelne i jedinstvene, ali smisla adresirati računare MAC adresama ima samo na lokalnoj mreži. Lokalne mreže čine par desetina, pa i stotina računara, što je relativno mali broj. Da bi bilo moguće povezati više lokalnih mreža u jedinstvenu mrežu svaki od računara mora dobiti još jednu adresu - IP adresu. Zbog ovoga se IP protokol u žargonu naziva i „lepak koji drži Internet da se ne raspadne“.

IP adresu podešava korisnik (ili se automatski dodeljuje), i ona se čuva se u sistemskim fajlovima operativnog sistema na hard-disku, za razliku od MAC adrese, koja je „utisnuta“ u hardver mrežne kartice. IP adresa je 32-bitni broj, tj. sastoji se od 32 binarne nule i jedinice. Ukupno postoje 232= 4.294.967.296 različitih IP adresa. Da bi IP adrese bile bliže i razumljivije ljudima, za predstavljanje IP adrese adresa se deli u 4 grupe od po 8 bitova. Ove grupe predstavljaju se jednim brojem u opsegu 0-255. Gornja granica od 255 postavlja se zato što sa 8 binarnih cifara moguće je predstaviti najviše 28=256 brojeva. Grupe brojeva se odvajaju tačkom.

Primer IP adrese: **132.10.15.128**

U dosadašnjoj priči nema velike razlike, sem u dužini, između MAC i IP adrese. Međutim, glavna razlika je u značenju cifara. Naime, kod MAC adrese prvi deo adrese je oznaka proizvođača, dok je kod IP adrese prvi deo adrese **oznaka mreže**, odnosno broj mreže (*network* deo IP adrese). Drugi deo MAC adrese rezervisan je za serijski broj kartice, dok je drugi deo IP adrese rezervisan za redni broj **računara na mreži** (*host* deo IP adrese).



**Slika 3.9.** Deljenje adrese na adresu mreže i adresu uređaja

Pitanje je na kom mestu podeliti IP adresu? Ukoliko je host deo veći, moguće je više računara povezati na takvu lokalnu mrežu, ali takvih mreža ima manje, jer je deo za adresiranje mreža manji. Važi i obrnuto.

Na osnovu veličine dela za adresiranje mreža razlikujemo 3 klase IP adresa: klasu A, klasu B i klasu C.

Klasa A IP adresa ima 8-bitnu oznaku mreže. Deo za adresiranje hostova na mreži je 24 bita. Ovakvih mreža je 127. Na svakoj mreži može se naći 224= 16.777.216 različitih IP adresa.

Klasa B IP adresa ima podjednak broj mreža i hostova: po 16b za predstavljanje. Tako da su ovo druge po veličini mreže, ali ih ima značajno više nego mreža klase A. Ukupan broj IP adresa po mreži klase B je 216=65.536.

Klasa C IP adresa predviđa 8 bitova za adresiranje računara i 24 bita za adresiranje mreže. Ovo su najmanje mreže, ali istovremeno su i najzastupljenije. Ukupan broj različitih IP adresa po mreži klase C je 28=256.

Da bi se znalo koji deo IP adrese se odnosi na adresu mreže, a koji deo se odnosi na adresu računara, uz IP adresu navodi se još i **subnet maska**. Subnet maska je 32-bitni broj koji ima binarnu nulu na mestu koje odgovara hostu, a binarnu jedinicu na mestu koje odgovara mreži. Radi lakšeg predstavljanja koristi se označavanje kao kod IP adrese, tako da se osam binarnih jedinica predstavlja brojem 255.

Primer podrazumevane subnet maske za IP adrese klase C: **255.255.255.0**

Informacija koju je na uređaju potrebno postaviti je, na primer:

IP :             **132.10.15.128**

Subnet:       **255.255.255.0**

Uređaj (računar) iz primera nalazi se na mreži broj 132.10.15, a njegov broj je 128 na mreži. Uobičajeni kraći zapis IP adrese mreže u kome se navodi i subnet maska je **132.10.15.0/24**, gde 24 znači broj binarnih cifara sa leve strane IP adrese koji se koriste za predstavljanje mreže. Konkretno, u navedenom primeru 24 je ekvivalentno subnet masci 255.255.255.0 (tri puta po 8 binarnih cifara).

IP adresiranje je hierarhisko adresiranje u dva nivoa. Analogija se može uspostaviti sa telefonskim sistemom adresiranja, koji je takođe u dva nivoa, ako se ima u vidu komunikacija u okviru jedne zemlje. Naime, da bi se uspostavila veza potrebno je pozvati broj 010399999, gde je 010 pozvni za grad, a ostatak je broj telefona.

Još jedan primer adresiranja je poštanski sistem adresiranja, sa kojim se može uspostaviti analogija. Poštansko adresiranje je u 5 nivoa: zemlja, grad, ulica, broj, ime i prezime. Prilikom slanja pisma na koverti se navode pomenuti podaci. Scenario je sledeći:

1.      lokalna pošta preuzima pismo;

2.      proverava se odredišna zemlja;

3.      ukoliko je odredišna zemlja druga država, jedino što lokalna pošta treba da zna jeste koji avion leti za odredišnu zemlju;

Ovo je ključni momenat kod hierarhijskog adresiranja. Jednostavno, u lokalnoj pošti nije bitno znati po imenu i prezimenu koji čovek u kući koje boje stanuje! Za to su zaduženi lokalni poštari, i to samo za svoj reon.

4.      kada pismo stigne u odredišnu državu, centralna pošta proverava odredišni grad i šalje pismo lokalnim vozilom;

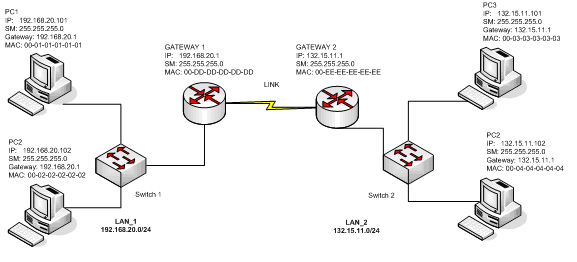
5.      u odredišnom gradu, na osnovu ulice pismo se daje poštaru;

6.      poštar zna broj kuće i odneće pismo na odredište.

Postavljanjem IP sloja kao sloja sa hierarhijskim adresama, lokalni računar pored MAC adrese dobija i IP adresu. Računar zna i može saznati preko ARP-a MAC adrese računara na lokalnoj mreži. Ukoliko odredište nije na lokalnoj mreži na mreži mora postojati uređaj koji zna kako da paket dostavi odredištu. Ovo se naziva **rutiranje paketa**, i u većini slučajeva ovu funkciju obavlja specijalizovani uređaj koji se naziva **router**, mada je moguće i jednom PC računaru na mreži poveriti ovu ulogu. Ovakav uređaj naziva se i **gateway** lokalne mreže, kako samo  ime govori „kapija za izlazak van“.

3.3.3. Primer IP komunikacije

Na sledećoj slici dat je primer mreže na kome će biti ilustrovana komunikacija dva računara u okviru lokalne mreže, i dva računara koja su na različitim mrežama.



**Slika 3.10.** Primer komunikacije računara na mreži

Na slici su prikazane dve lokalne mreže: mreža 192.168.20.0/24 i mreža 132.15.11.0/24. Obe mreže su Ethernet mreže formirane oko switheva kao centra ožičavanja (switch1 i switch2).

Napomena: više reči o principu rada i konfiguraciji samih mrežnih uređaja kao što su ruteri u svičevi biće u narednim poglacljima.

Na lokalnoj mreži 1 povezani su računari PC1 i PC2, kao i gateway te mreže. Preko gateway-a i „link-a“ mreža 1 je povezana sa mrežom 2 koja ima sličnu topologiju. Naime, mreža 2 ima takođe topologiju zvezde sa svičem u centru. Tri uređaja čine mrežu 2: PC3, PC4 i gateway mreže 2. Svaki uređaj ima podešenu IP adresu i subnet masku, a računarima je podešena i IP adresa gateway-a. MAC adrese su „fabričke“.

Scenario koumnikacije dva računara na istoj lokalnoj mreži je sledeći:

1.      PC1 ima spremne podatke sa viših nivoa koje želi poslati do PC2.

2.      Bilo koja komunikacija na IP mreži se obavlja isključivo preko IP adresa, tako da PC1 zna IP adresu računara kome treba dostaviti podatke. To je adresa 192.168.20.102.

3.      Ovaj korak je veoma važan i u okviru njega PC1 odlučuje da li paket treba poslati gateway-u ili ne: pre pakovanja u pakete na IP nivou PC1 proverava da li je odredišna IP adresa na istoj mreži. Za ovo je potrebna subnet maska, pa PC1 određuje: na osnovu svoje IP adrese 192.168.20.101 i subnet maske 255.255.255.0, mrežna adresa lokalne mreže je 192.168.20, što je isto sa adresom mreže odredišne IP adrese. Sledi, paket ne treba slati gateway-u jer je odredište na istoj mreži.

4.      Podaci se na IP nivou dele u pakete. Podaci se pakuju u prvi paket tako što se dodaje IP zaglavlje u vidu izvorne IP adrese i odredišne IP adrese: 192.168.20.101 je izvor, 192.168.20.102 je odredište.

5.      Spreman paket se predaje Ethernet nivou.

6.      Da bi se paket „upakovao“ u ethernet frejm, potrebno je saznati MAC adresu odredišta. MAC adresa izvora je poznata jer je na samoj kartici: 00-01-01-01-01-01.

7.      Kako je, recimo, PC1 tek uključen, njegova ARP tabela je prazna, odnosno on ne zna MAC adresu PC2.

8.      Da bi saznao MAC adresu odredišta PC1 sprema ARP zahtev koji bukvalno glasi: „ko ima IP adresu 192.168.20.102?“, i šalje ga na lokalnu mrežu sa broadcast odredišnom MAC adresom kako bi svi uređaji na lokalnoj mreži „čuli“ zahtev.

9.      Svi uređaji na lokalnoj mreži primaju ARP zahtev, ali jedino PC2 odgovara jer je prepoznao svoju IP adresu. On kaže: „Ja imam IP adresu 192.168.20.102, a moja MAC adresa je 00-02-02-02-02-02-02“. Ovaj ARP odgovor PC2 šalje direktno na 00-01-01-01-01-01 jer zna od koga je zahtev primio.

10.  Kada PC1 dobije ARP odgovor, on u svoju ARP tabelu upisuje par IP adresa – MAC adresa. Napomena: kao što je ranije rečeno, informacija ostaje u ARP tabeli 5min nakon poslednjeg korišćenja IP adrese, a može se na Windows računarima izlistati naredbom arp –a.

11.  Sada PC1 zna MAC adresu odredišta i vraća se gde je stao (korak 6). PC1 pakuje IP paket u frejm tako što dodaje svoju MAC adresu i MAC adresu odredišta: 00-01-01-01-01-01 i 00-02-02-02-02-02.

12.  PC1 šalje frejm na lokalnu mrežu.

13.  Kako svi uređaji na lokalnoj mreži mogu da vide frejm, svi proveravaju da li su oni zapravo odredište frejma na osnovu MAC adrese. Jedino PC2 prepoznaje svoju MAC adresu, uklanja heder frejma i CRC, nakon čega mu ostaje IP paket koji predaje IP nivou. Na IP nivou se proverava da li je odredišna adresa u paketu zapravo 192.168.20.102, adresa PC2, i kako jeste, podaci se raspakuju iz paketa i prosleđuju višim nivoima.

14.  Naredni paket koji PC1 šalje PC-ju 2 neće prolaziti kroz ARP proceduru, tj. neće imati korake 8 – 10, već će u koraku 7 pročitati odredišnu MAC adresu na osnovu odredišne IP adrese iz lokalne RAM memorije (ARP tabele).

Komunikacija računara sa različitih lokalnih mreža je nešto složenija i odvija se podsredstvom gateway uređaja. Komunikacija u slučaju kada PC1 šalje paket PC-ju 3 odvija se po sledećem scenariju:

1.      PC1 ima spremne podatke sa viših nivoa koje želi poslati do PC3.

2.      Bilo koja komunikacija na IP mreži se obavlja isključivo preko IP adresa, tako da PC1 u startu zna IP adresu računara kome treba dostaviti podatke. To je adresa 132.15.11.101.

3.      PC1 odlučuje da li paket treba poslati gateway-u ili ne: pre pakovanja u pakete na IP nivou PC1 proverava da li je odredišna IP adresa na istoj mreži. Za proveru je potrebna subnet maska, tako da PC1 na osnovu svoje IP adrese 192.168.20.101 i subnet maske 255.255.255.0 određuje da je adresa lokalne mreže 192.168.20. Adresa mreže odredišta je određena na sličan način u ona je 132.15.11, što je različito od adrese lokalne mreže. PC1 zaključuje da paket treba proslediti gateway lokalne mreže.

4.      Podaci se na IP nivou dele u pakete. Podaci se pakuju u prvi paket tako što se dodaje IP zaglavlje u vidu izvorne IP adrese i odredišne IP adrese: 192.168.20.101 je izvor, 132.15.11.101 je odredište, bez obzira što je odredište na različitoj mreži.

5.      Na PC-ju 1 je već podešena adresa gateway računara prilikom instalacije na mrežu, i ona je 192.168.20.1.

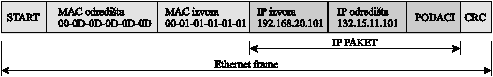
6.      PC1 treba da prosledi paket gateway koji je na lokalnoj mreži – preko etherneta. PC1 treba da sazna MAC adresu gateway-a.

7.      Bilo čitanjem iz lokalne ARP tabele, ukoliko je u prethodnih 5 min bilo komunikacije sa gateway-om, ili ARP zahtevom, kako je pokazano u prethodnom scenariju, PC1 saznaje da je MAC adresa računara sa IP adresom 192.168.20.1 jednaka 00-0D-0D-0D-0D-0D-0D.

Napomena: Ukoliko se radi o ARP upitu PC1 šalje upit „ko ima IP adresu 192.168.20.1?“, jer u ovom trenutku njega interesuje jedino gateway.

8.      Paket spremljen u koraku 4 se predaje Ethernet nivou.

9.      Na ethernet nivou se dodaje zaglavlje u vidu izvorne i odredišne MAC adrese. MAC adresa izvora je 00-01-01-01-01-01. Ključni momenat ovog scenarija je da je MAC adresa odredišta zapravo MAC adresa gateway-a: 00-0D-0D-0D-0D-0D, tako da ethernet frejm koji PC1 šalje ima sledeći izgled:



10.  PC1 šalje pripremljeni frejm na lokalnu mrežu.

11.  S obzirom na prirodu etherneta, kako je ranije naglašeno, na zajedničkom medijumu svi uređaji sa lokalne mreže primaju frejm, ali jedino gateway prepoznaje svoju MAC adresu. Kada prepozna svoju MAC adresu, gateway raspakuje paket iz frejma i predaje ga svom višem nivou: IP nivou. Podaci koje ethernet modul gateway-a predaje IP modulu su:



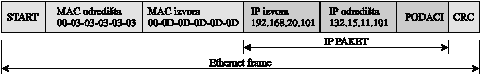
12.  Gateway na svom IP nivou proverava IP adresu odredišta i odlučuje preko kog linka treba poslati paket. Ovaj proces se naziva **rutiranje** i biće detaljnije objašnjen kasnije. Dakle, na osnovu odredišne IP adrese, gateway odlučuje da paket treba poslati gateway 2.

Napomena: slanje paketa od gateway-a 1 do gateway-a 2 obavlja se takođe enkapsulacijom i adresiranjem na 2 nivou OSI modela i deenkapsulacijom na odredištu.

13.  Kada gateway 2 primi paket, on proverava da li je odredišna IP adresa na lokalnol mreži 132.15.11 ili ne. Naravno, na osnovu svoje subnet maske i svoje IP adrese on zaključuje da odredište jeste na istoj lokalnoj mreži, i jedino što preostaje je da gateway2 „sazna“ MAC adresu odredišta kako bi preko etherneta dostavio podatke.

14.  Proveravanjem lokalne ARP tabele, ili postavljanjem ARP upita „ko ima IP adresu 132.15.11.101?“, gateway 2 saznaje da je MAC adresa računara sa IP adresom 132.15.11.101 jednaka 00-03-03-03-03-03.

15.  Paket se predaje ethernet modulu koji kreira frejm sledećeg izgleda:



16.  Svi računari na lokalnoj mreži 132.15.11.0/24 dobijaju frejm, s tim da jedino PC3 prepoznaje svoju MAC adresu u odredišnom polju, raspakuje frejm i IP paket prosleđuje svom IP modulu.

Napomena: naglašavamo da se IP adresa odredišta i IP adresa izvora **ne menjaju** bez obzira koliko prelazaka sa jedne lokalne mreže na drugu postoje na putu paketa od izvora do odredišta.

3.3.4. Karakteristike IP protokola

Sami dizajn pricipi mreža koje se zasnivaju na IP protokolu podrazumevaju da je mrežna infrastruktura nepouzdana, odnosno da može doći do otkaza svakog čvora u mreži, ili prekida bilo koje veze u bilo kom trenutku. Kao što je u uvodnom poglavlju napomenuto, ovakve zahteve za dizajnom IP mreže postavilo je američko Ministarstvo odbrane. Mrežna infrastruktura je prilikom projektovanja protokola posmatrana kao dinamička kategorija koja je podložna pormeni, namernoj, zbog intervencije administratora na mreži, ili nenamerno, u slučaju otkaza uređaja. Ovakav pogled na mrežu doveo  je do takvog razvoja da se o prenosu vodi računa jedino od strane krajnjih tačaka u komunikaciji (eng. *end-to-end* princip). Ruteri na koje paket nailazi jednostavno na onovu odredišne IP adrese prosleđuju paket na jedan od svojih linkova, bez ikakvih dodatnih razmatranja (npr. da li je to prvi u nizu paketa, ukoliko se prenosi velika količina podataka, i sl).

Kao posledica ovakvog pristupa, Internet Protokol (IP) je razvijen po principu **najefikasnije dostave** (eng. *best effort delivery*) i njegovi servisi se karakterišu kao **nepouzdani**. IP protokol se ubraja u *connection-less* protokole, za razliku od *connection-oriented* modova za prenos. *Connection-less* protokoli su protokoli koji ne zahtevaju **prethodno uspostavljanje veze** između učesnika u komunikaciji. Kod *ocnnection-oriented* protokola veza se pre prenosa bilo kakve informacije mora uspostaviti. Analogija sa ovakvim vidom komunikacije je telefonski poziv. Osoba koja zove bira broj, što uzrokuje zvonjavu telefona na drugom kraju komunikacionog kanala. Pre no što se osoba sa druge strane ne javi, nema smisla počinjati razgovor.

Bez obzira na način uspostavljanja veze, i bez prethodno uspostavljene veze je moguće komunicirati i razmenjivati više od jedne poruke u nizu. Primer sa kojim se može uspostaviti analogija su pošta i prijem i slanje pisama. Naime, kao i kod IP protokola, pošiljalac šalje pismo navodeći adresu primaoca i svoju (povratnu) adresu. Primalac prima pismo i odgovara na njega, itd. U međuvremenu pošta je ta koja prenosi (rutira) pisma iz mesta u mesto.

Otsustvo pouzdanosti omogućava:

-          oštećenje delova paketa,

-          gubitak celih paketa,

-          duplirani dolazak paketa na odredište,

-          vanredosledni prijem paketa.

Paketi se mogu oštetiti usled prolaska kroz linkove lošeg kvaliteta na kojima postoji veliki uticaj šumova, dok se paketi mogu izgubiti usled, na primer, nestanka napajanja, ili kvara usputnih uređaja. Duplirani dolazak može se javiti zbog raznih softverskih grežaka i protokolarnih nedostataka na usputnoj infrastrukturi. Do vanredoslednog prijema paketa može doći ako paketi ne putuju istom putanjom.

Razmotrićemo jedan scenario vanredoslednog prijema paketa. Računar A šalje paket a1, a za njim i a2, a3, ..., itd. Paket a1 putuje kroz spori, modemski link, u trenutku kada se aktivira još jedan brzi, satelitski link. Preko satelitskog linka kreće slanje paketa a2, a3, ... Odredište će primiti pakete u sledećem redosledu: a2, a3, a4, a1, a5, ...

Jedinu zaštitu koju IP protokol pruža je zaštita od oštećenja delova paketa. Ovo je postignuto time što izvor u heder IP paketa, pored IP adresa, umeće i CRC čeksum za dati paket. Na odredištu se ponovo računa čeksum primljenog paketa i ako se ček-sume slažu, paket je prenet bez grešaka. Međutim, ako paket sadrži greške, odredište ga odbacuje bez obaveštavanja izvora da je paket odbačen!

Potrebno je napomenuti da ovakve probleme može da reči pomoćni, ICMP protokol mrežnog nivoa, mada se IP protokol ne oslanja na usluge ovakve vrste. Rešenje svih navedenih problema leži u protokolima viših nivoa: transpornom protokolu, o kome će biti više reči nešto kasnije.

3.3.5. Adresna kriza i IPv6

Prva vertija IP protokola koja je javno korišćena jeste verzija 4 (IPv4). Ova verzija IP protokola ima kapacitet adresni kapacitet od 232 adresa, što je nešto preko 4 milijarde adresa. Po prvim vizijama Interneta, u vreme pre eksplozivnog širenja Interneta, ovo je bilo više nego dovoljno.

U toku prve dekade eksploatacije TCP/IP baziranog Interneta, do kasnih 80-tih, postalo je očigledno da je nešto potrebno preduzeti kako bi se sačuvao adresni prostor. Naime, kada bi neka organizacija od IANA-e (međunarodne agencije za dodelu jedinstvenih Internet IP adresa, takođe poznatih i pod imenom javne IP adrese) tražila dodelu IP mreže, ta organizacija dobijala je u najmanju ruku mrežu klase C kao najmanju mrežu. Mreža klase C ima 256 IP adresa. Većini organizacija je bilo potrebno mnogo manje od toga, tako da je za par računara zauzimano par stotina adresa.

Početkom 90-tih počelo se upotrebom takozvanih *classless* IP adresa (prev. *ne pripadaju ni jednoj klasi*, misli se na klasu mreža A, B, ili C). *Classless* IP adrese su adrese koje kojih deo koji predstavlja mrežu ne mora biti celobrojni umnožak 8 bitova – 8, 16, 24 (klasa A, B ili C). Tako na primer, IP mreža 150.15.15.0/30 ima samo 4 IP adrese na mreži, jer je mreža predstavljena sa 30 bitova, dok su za hostove na mreži ostavljena 2 bita (22=4).

Godine 1992. zvanično se počelo sa radim na IP protokolu sledeće generacije (eng. *IP Next Generation*), što je objavljeno u dokumentu RFC-1550. Međunarodno telo za razvoj Interneta (eng. *Internet Engineering Task Force -* IETF) je od 1994. do 1996. usvojilo seriju dokumenata i standarda (počev od RFC-2460) koji definišu novi IP protokol – IPv6.

Napomena: nakon verzije 4 IETF nije koristio oznaku IPv5 zato što je ova oznaka u međuvremenu dodeljena *Internet Streaming Protocol-*u (ISP).

Prognoze o trajanju IPv4 (sve dok postoji bar i jedna slobodna IP adresa) su različite. Godine 2003. Paul Wilson (direktor APNIC-a) izjavio je po njihovim istraživanjima baziranim na prognozu razvoja i sl., IPv4 će trajati do 2023. godine. Na sajtu IANA godine 2007. objavljeno je da bi do krize moglo doći već između maja 2010. i aprila 2011. godine.

Cilj IPv6 je da postepeno zameni IPv4. Što se PC računara tiče, svaki računar pored IP adrese verzije 4 može imati još jednu IP adresu verzije 6 jednostavnim instaliranjem „drajvera“ IPv6. Problem nastaje kod same infrastrukture, koja treba da prenosi pakete, i to samo zato što se formati adresa IPv4 i IPv6 razlikuju.

Glavne odlike IPv6 su:

-          **Veći adresni prostor** – ovo je ključna razlika. IPv6, za razliku od 32 bita sa koliko se predstavlja adresa kod IPv4, koristi 128 bitova za predstavljanje adrese. Ovo je broj koji u dekadnom zapisu čine 33 cifre!!! Iako su ove brojke impresivne, namera dizajnera nije bila da „zasiti“ tržište narednih 1.000 godina, kako kažu, već je do upotrebe dužih adresa došlo kako ib se omogućila bolja sistematičnost i bolje postizanje  kvalitetnije hierarhije adresa. IP adresa se i dalje po istom principu deli na mrežni deo i deo hosta. IP adrese verzije 6 predstavljaju se sa po 32 heksadekadne cifre (svaka cifra po 4 binarne cifre) gde su po četiri heksa cifre odvojene dvotačkama. Primer IP adrese IPv6: **003F:D2FF:A115:0000:0000:8A2E:0307:7334**

-          **Automatska konfiguracija IP adresa** – IPv6 host može sam sebi konfigurisati IP adresu ako je povezan na mrežu koja rutira IPv6 paketa korišćenjem ICMPv6 protokola.

-          **Milticast** – mogućnost da se jedan paket sa izvora pošalje ka više od jednog odredišta. Ovo se koristi u slučaju IP televizije ili radio prenosa. Specifikacija multicast paketa uvedena je u sam IPv6 standard, dok je kod IPv4 ovakva mogućnost opciona.

-          **Pojednostavljena obrada na ruterima** – heder IPv6 paketa je pojednostavljen, tako da ruteri mogu efikasnije da obrađuju veći broj paketa.

-          **Veliki paketi** – IPv6 može upakovati do 64kB u jedan paket, dok je kod IPv4 ova cifra znatno skromnija i iznosi 1.5kB.

3.3.6. Tipovi IP adresa

Postoji nekoliko podela IP adresa zavisno od aspekta u kome se posmatra određena IP adresa. Podela IP adresa se vrši:

1.      **po klasama**, na osnovu subnet maske,

2.      **po nameni** na upotrebljive i na specijalne IP adrese,

3.      **po vidljivosti** na privatne i javne IP adrese.

Po klasama koje su definisane standardom i označene subnet maskama /8, /16 I /24, IP adrese se dele na IP adrese:

-          klase A – u ovu klasu spadaju adrese od 1.0.0.0/8 do 127.255.255.255/8;

-          klase B – u ovu klasu spadaju adrese od 128.0.0.0/16 do 191.255.255.255/16;

-          klase C – u ovu klasu spadaju adrese od 192.0.0.0/24 do 239.255.255.255/24;

-          klase D – u ovu klasu spadaju adrese od 240.0.0.0 do 247.255.255.255, i koriste se za milticast na IPv4 mreži;

-          klase E – sve ostale (od 248.0.0.0 do 255.255.255.255), i koriste se u cilju testiranja od strane IANA-e.

Postoje specijalne IP adrese kojim se označavaju mreže i IP adrese kojima se označavaju svi hostovi na mreži (broadcast adrese mreža). Za adresu same mreže se uzima ona odresa koja u host delu ima sve nule.

Primer: mreža klase B 192.168.1.0/24, mreža klase B 172.16.0.0/16, mreža klase A 10.0.0.0/8.

Za broadcast adrežu mreže uzima se IP adresa koja u delu za host ima sve binarne jedinice (255 dekadno). Za primer gore: broadcast adresa mreže klase B 192.168.1.0/24 je 192.168.1.255, mreže klase B 172.16.0.0/16 je 172.16.255.255, dok je broadcast adresa mreže klase A 10.0.0.0/8 jednaka 10.255.255.255.

Po vidljivosti IP adrese se dele na privatne i javne IP adrese. Javne IP adrese su one adrese koje dodeljuje IANA. Privatne IP adrese je mehanizam razvijen kako bi se sačuvale adrese i što duže očuvao adresni prostor IPv4. Naime, standardom je definisano da su IP adrese:

-          klase A 10.0.0.0/8 (jedna mreža),

-          klase B od 172.16.0.0/16 do 172.31.0.0/16 (ukupno 16 mreža), i

-          klase C 192.168.0.0/24 do 192.168.255.0/24 (ukupno 256 mreža)

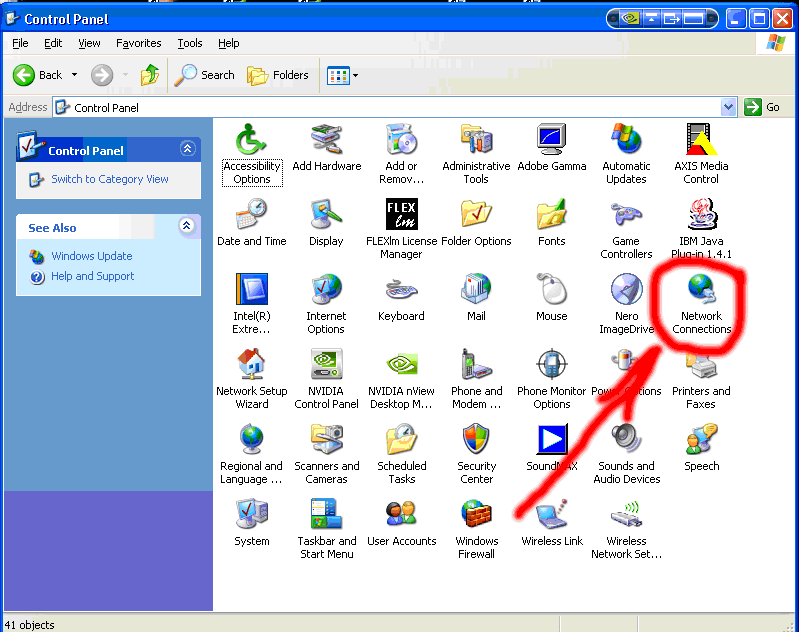
privatne adrese i da se ne smeju koristiti na Internetu. Ove adrese se mogu koristiti na provatnim lokalnim mrežama, i nisu jedinstvene jer ih mnogi koriste.

Da bi mreža sa privatnim IP adresama imala pristup Internetu, gateway ruter mora imati instaliran poseban softver, **NAT** (eng. *Network* *Address Translation*), koji privatne adrese prevodi u javne prilikom rutiranja (ili javnu, pošto uglavnom cele mreže imaju samo jednu javnu adresu).

NAT se može posmatrati i na analogiji telefonske centrale u firmi, gde svaki zaposleni ima svoj **lokal**. Centala ima ulogu NAT-a. Mnoge firme mogu imati lokal 101, ali se veza sa lokalom uspostavlja tek nakon uspostavljanja veze sa centralom (koja ima javni broj).

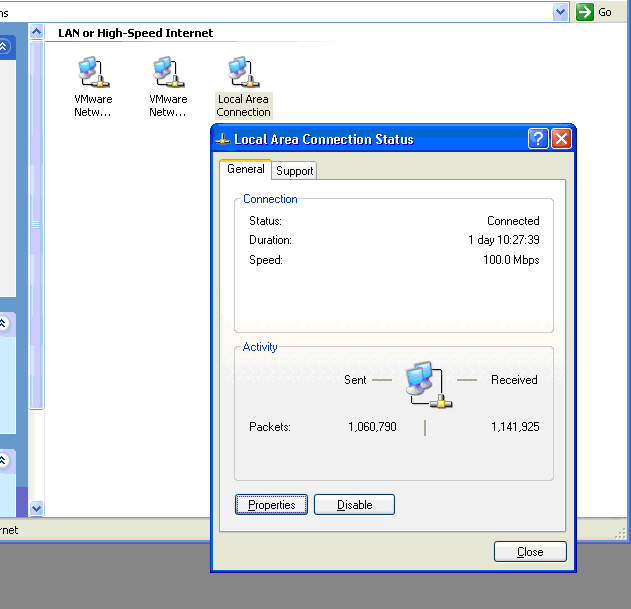
3.3.7. Mrežni nivo i IP protokol na Windows računarima

IP protokol mrežnog nivoa implementiran je kao softverska komponenta operativnog sistema, bez obzira o kom se operativnom sistemu radi. Do podešavanja ove komponente na Wondows računarima moguće je doći kroz *Control Pannel* Windows-a na način prikazan na slici.



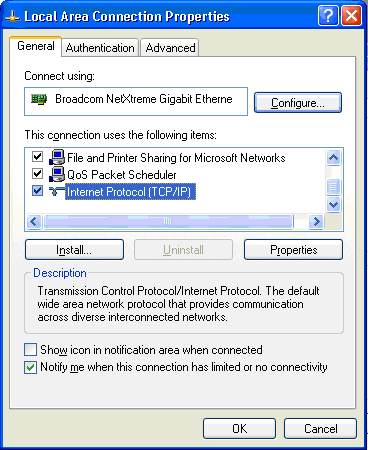
**Slika 3.11.** Lokacija komponente za podešavanje mrežne konekcije

Pod mrežne konekcije (eng. *Network Connections*) u *control panel-u* wondows-a spadaju svi uređaji koji mogu komunicirati preko mreže: modemi i ISDN, ADSL i kablovski modemi, Ethernet kartice, i sl. Svaki uređaj koji ima *Network Access* sloj nudi mogućnost podešavanja IP nivoa.



**Slika 3.12.** Mrežna konekcija

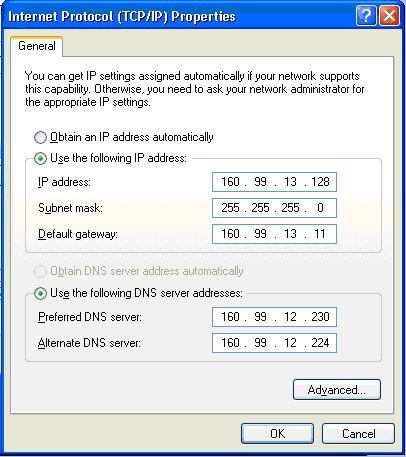
Na sledećoj slici prikazana je IP softwerska komponenta koja implementira IP protokol na Windows-u XP. Do ovoga se može doći klikom na *Properties* dijalog asa prethodne slike.



sl. 1.3. **Slika 3.13.** Softverska komponenta koja realizuje IP protokol

Potrebno je naglasiti da neke od ranijih verzija Windows operativnog sistema prilikom instalacije operativnog sistema ne instaliraju automatski ovu komponentu. Ukoliko komponenta ne posoji moguće je instalirati (*Install* taster). Takođe je moguće instalirati i druge protokole na ovom nivou, koji se ne instaliraju automatski sa operativnim sistemom (IPX, AppliTalk, i sl).

Podešavanja IP adresa i subnet maske prikazana su na sledećoj slici (*properties* na dialogu sa prethodne slike).



**Slika 3.14.** Podešavanje IP protokola

Napomena: zaključak koji je potrebno izvući iz prethodnih poglavlja je da računari na lokalnoj mreži mogu komunicirati ukoliko se nalaze na istoj IP mreži. Da li su na istoj IP mreži vidi se kombinovanjem IP adrese i subnet maske. Tako, računar sa primera sa slike može komunicirati sa računarima sa lokalne mreže **i ako na mreži ne postoji ruter**, odnosno gateway ukoliko su IP adrese računara u opsegu 160.99.13.1 do 160.99.13.255. Kako na mreži postoji gateway (160.99.13.11), računar sa primera može komunicirati i sa računarima koji nisu na lokalnoj mreži.

Računar sa primera ima javnu IP adresu sa mreže koja po standarnoj podeli mreža pripada mreži klase B (vidi se na osnovu IP-a), ali je ta mreža dalje podeljena u klasu C, što se vidi iz subnetmaske. Ukoliko se postavlja lokalna mreža na kojoj računarima nisu dodeljene javne IP adrese, potrebno je podesiti IP adrese sa neke od privatnih mreža navedenih ranije.

Postoji i automaska konfiguracija IP adrese hosta preko DHCP protokola. Ovaj protokol je protokol aplikativnog nivoa i biće obrađen u delu koji se bavi protokolima aplikativnog nivoa. DNS takođe.