HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Dodjeljivanje IP adresa

CCERT-PUBDOC-2007-09-203

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.

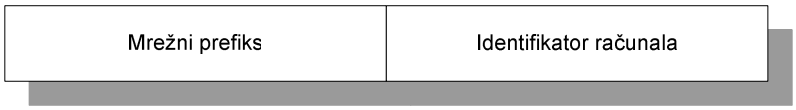
Sadržaj

1. Uvod

IP (eng. *Internet Protocol*) je osnovni protokol u radu Interneta. Temelj njegova rada je adresiranje računala, odnosno dodjela jedinstvene adrese svakom računalu priključenom na mrežu.
Korisnici računala ne mogu adrese dodjeljivati proizvoljno, već je dodjela adresa vrlo strogo kontrolirana. Razlog za ovu strogost je izvjesnost potpunog kolapsa mreže u slučaju istovremene pojave većeg broja računala s jednakim adresama.
Nemogućnost korištenja istih IP adresa, kombinirana s vrlo velikim i sve brže rastućim brojem priključenih računala te ograničenim brojem adresa dovodi do velikih problema u organizaciji njihove dodjele, ali i do novih rješenja. Jedno od njih je i dinamička dodjela adresa.
U ostatku dokumenta opisane su temeljne značajke IP adresiranja i njihov razvoj kroz povijest. Iako se na prvi pogled čini nepotrebnim, poznavanje povijesti Interneta je neophodno za razumijevanje njegovih današnjih trendova. Osim osnova IP adresiranja dokument nudi pregled češće korištenih protokola dinamičke dodjele adresa. Pritom je posebna pažnja posvećena trenutno najčešće korištenom među njima – protokolu DHCP, ali i sigurnosnim rizicima vezanim uz njegovu primjenu.

2. Općenito o IP adresama

Kada je 1981. godine IP (eng. *Internet Protocol*) protokol prvi puta standardiziran, specifikacija je zahtijevala da svako računalo spojeno na IP mrežu ima jedinstvenu 32-bitnu adresu. Računala koja su spojena na više mreža trebaju imati po jednu IP adresu za svako svoje mrežno sučelje. Prvi dio te adrese identificira mrežu na kojoj se računalo nalazi, dok drugi dio identificira računalo unutar mreže. Ovakav pristup definira dvorazinsku hijerarhiju adresiranja koja je ilustrirana slijedećom slikom.



Slika 1. Sastavnice adrese u dvorazinskoj hijerarhiji adresiranja

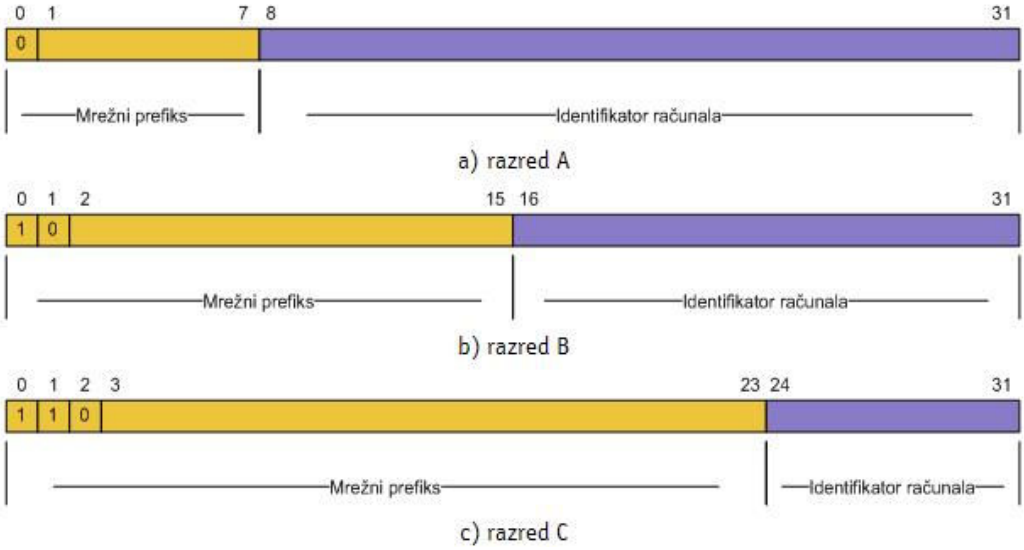
Posljednjih se godina identifikator mreže često naziva mrežnim prefiksom. Sva računala jedne mreže imaju jednak mrežni prefiks i različit identifikator računala u svojim IP adresama. Analogno tome, dva računala s dviju različitih mreža obvezatno moraju imati različite mrežne prefikse, ali mogu imati jednake identifikatore računala.

2.1. Primarni adresni razredi

Kako bi se postigla fleksibilnost potrebna za implementaciju mreža različite veličine, dizajneri IP protokola odlučili su da IP adrese treba podijeliti u tri razreda:

- razred A,
- razred B i
- razred C.

Razredi se međusobno razlikuju po točci u kojoj se dijeli dio adrese namijenjen identifikaciji mreže i dio adrese namijenjen identifikaciji računala. Formati primarnih adresnih razreda prikazani su slijedećom slikom.



Slika 2. Formati primarnih adresnih razreda

Jedno od temeljnih svojstava ovakve podjele u razrede je mogućnost izravnog utvrđivanja pripadnosti adrese nekom razredu samo na temelju njenih vodećih bitova i bez potrebe za dodatnim popisima. Primjerice, ako su prva dva bita adrese 10, odmah je moguće utvrditi da se točka dijeljenja nalazi između 15. i 16. bita. Ovo svojstvo uvelike je olakšalo usmjeravanje u ranim danima Interneta.

2.1.1. Adresni razred A

Svaka adresa ovog razreda ima 8-bitni mrežni prefiks kome je najvažniji bit postavljen na 0. Ostatak od 24 bita ispunjava identifikator računala. Opisana raspodjela omogućava adresiranje 126 različitih

mreža koje svaka mogu imati do 2^{24} -2, odnosno 16 777 214 računala. Izračun broja dostupnih adresa oduzima dva, jer su adrese koje sadrže sve nule i sve jedinice rezervirane za označavanje trenutne mreže odnosno tzv. "*broadcast*" adrese. Jednako tako, broj dostupnih mreža nije 128 jer su mreže koje započinju s početnim bajtom 0 ili završnim bajtom 127 rezervirane za posebne namjene.
Budući da ukupno ima 2^{31} adresa adresnog razreda A, one zauzimaju 50% od 2^{32}, odnosno broja svih dostupnih IP adresa.

2.1.2. Adresni razred B

Svaka adresa adresnog razreda B ima mrežni prefiks i identifikator računala jednake duljine od 16 bitova. U mrežnom prefiksu dva prva bita fiksirana su na vrijednost 10, tako da postoji ukupno 2^{14}, odnosno 16 384 mreža razreda B. Svaka od tih mreža može imati do 2^{16} -2, odnosno 65 534 računala. Budući da cijeli blok adresa adresnog razreda B sadržava 2^{30} adresa, on predstavlja 25% svih dostupnih IP adresa.

2.1.3. Adresni razred C

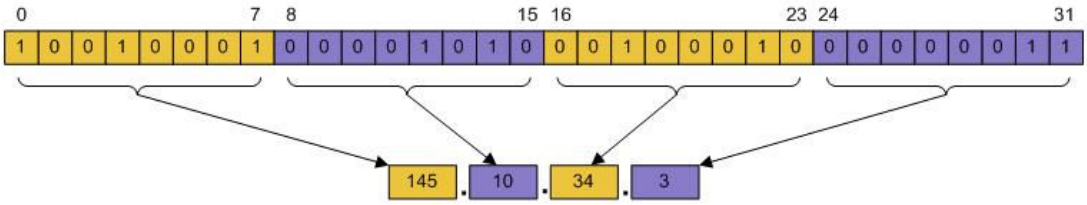
Svaka adresa ovog razreda ima 24-bitni mrežni prefiks i 8-bitni identifikator računala. Budući da su svakoj adresi adresnog razreda C prva tri bita fiksirana na vrijednost 110, ovim adresnim razredom može se pokriti ukupno 2^{21}, odnosno 2 097 152 različitih mreža. U svakoj od njih može biti do 2^8 -2, odnosno 254 računala.
Adresni prostor kojeg zauzimaju adrese razreda C sadržava ukupno 2^{29} adresa, što je 12.5% ukupnog IP adresnog prostora.

2.1.4. Ostali adresni razredi

Osim pobrojenih A, B i C razreda, postoje još i manje popularni razredi D i E. Adresa razreda D započinje sekvencom bitova 1110 i koristi se za podržavanje višeodredišne komunikacije (eng. *multicasting*). Adrese razreda E započinju sekvencom 1111 i rezervirane su za eksperimentalno korištenje.

2.1.5. Dekadski zapis s točkama (eng. *Dotted-Decimal Notation*)

Kako bi ljudi mogli lakše rukovati IP adresama izmišljen je njihov dekadski zapis s točkama. On 32-bitnu adresu dijeli u četiri 8-bitne sekvence od kojih se svaka zapisuje kao dekadski broj u rasponu od 0 do 255. Četiri broja se zapisuju međusobno odijeljeni točkama. Pretvorba 32-bitne binarne adrese u dekadski zapis s točkama prikazana je na slijedećoj slici.



Slika 3. Pretvorba binarne adrese u dekadski zapis s točkama

Slijedeća tablica prikazuje raspone adresa koji pripadaju određenim glavnim adresnim razredima.

Adresni razred	Raspon adresa u dekadskom zapisu s točkama
A	1.xxx.xxx.xxx – 126.xxx.xxx.xxx
B	128.0.xxx.xxx – 191.255.xxx.xxx
C	192.0.0.xxx – 223.255.255.xxx

Tablica 1. Rasponi adresa prema razredima

2.2. Nepredviđena ograničenja razrednog adresiranja

Izvorni dizajneri Interneta nikada nisu zamišljali da će on toliko brzo rasti i da će toliko brzo doseći svoju današnju veličinu. Mnogi danas prisutni problemi Interneta svoje korijene imaju upravo u njihovim prvim odlukama donesenim još u vrijeme samih početaka umrežavanja računala.

- Tijekom prvih godina Interneta, prividno bezgraničan adresni prostor dijelio se organizacijama i ljudima samo na temelju njihovih zahtjeva, bez razmatranja njihovih stvarnih potreba. Kao rezultat toga, većina adresa se besplatno razdijelila onima koji su ih tražili bez brige o eventualnom iscrpljivanju cijelog adresnog prostora.
- Odluka o standardizaciji 32-bitnog adresnog prostora ograničila je ukupan broj adresa na 2^{32}, odnosno 4 294 967 296. Odluka da se podrži adresni prostor sa samo malo većim brojem bita dovela bi do eksponencijalnog rasta broja dostupnih adresa, pri čemu bi se eliminirao problem njihova nestanka.
- Razredna organizacija adresa u razrede A, B i C bila je laka za razumijevanje i implementaciju, ali nije osiguravala efikasno korištenje ograničenog adresnog prostora. Ovaj problem je prvi puta došao do izražaja kada su se iscrpile adrese za mreže razreda B. Mreže B razreda izvorno su bile zamišljene kako bi osigurale infrastrukturu za organizacije srednje veličine. Budući da se na početku ove mrežne adrese dijelilo organizacijama koje su u stvari trebale samo nekoliko stotina adresa, umjesto da se njihov zahtjev rješavao dodjelom nekoliko mrežnih adresnih prostora razreda C.

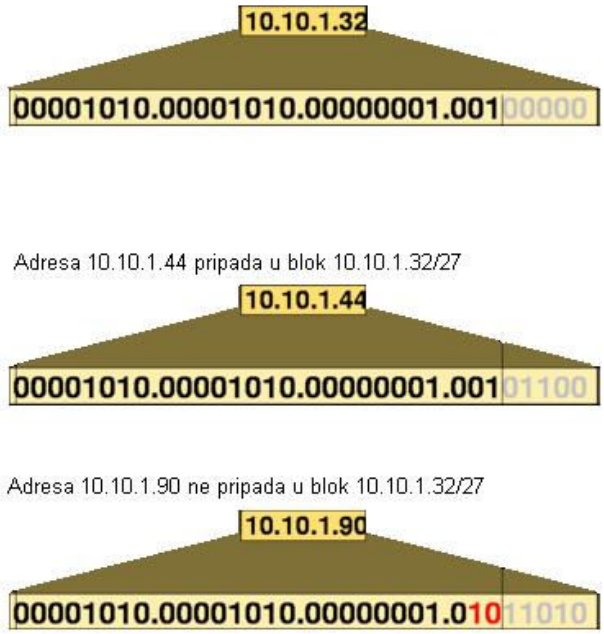
Postupnim razvojem događaja, povijest pokazuje, donošene su odluke koje su ublažile ili uklonile opisane probleme i omogućile brzo širenje Interneta.

2.3. CIDR (eng. *Classless Inter-Domain Routing*)

CIDR je sustav upravljanja IP adresnim prostorom koji je 1993. zamijenio klasično razredno adresiranje. Njegova glavna prednost je u mogućnosti podjele prijašnjih razreda u veće ili manje blokove adresa koji se mogu dodijeliti entitetima (poput pružatelja pristupa Internetu ili njihovih klijenata) ili lokalnim mrežama.

2.3.1. CIDR blokovi

Za razliku od razrednog adresiranja koje adresni prostor dijeli u razrede, CIDR sustav ga dijeli u blokove. Pri tome adresa opet ima dva dijela: dio koji označava blok i dio koji označava računalo unutar bloka. Ipak, točka razdvajanja između ta dva dijela nije unaprijed definirana, već ju opisuje dodatan broj između nula i trideset i dva koji označava koliko početnih bitova adrese identificira blok. U kontekstu CIDR adresiranja mreža se naziva CIDR blokom.
Primjer interpretacije bloka 10.10.1.32/27 prikazan je na slijedećoj slici.



Slika 4. Interpretacija CIDR bloka 10.10.1.32/27

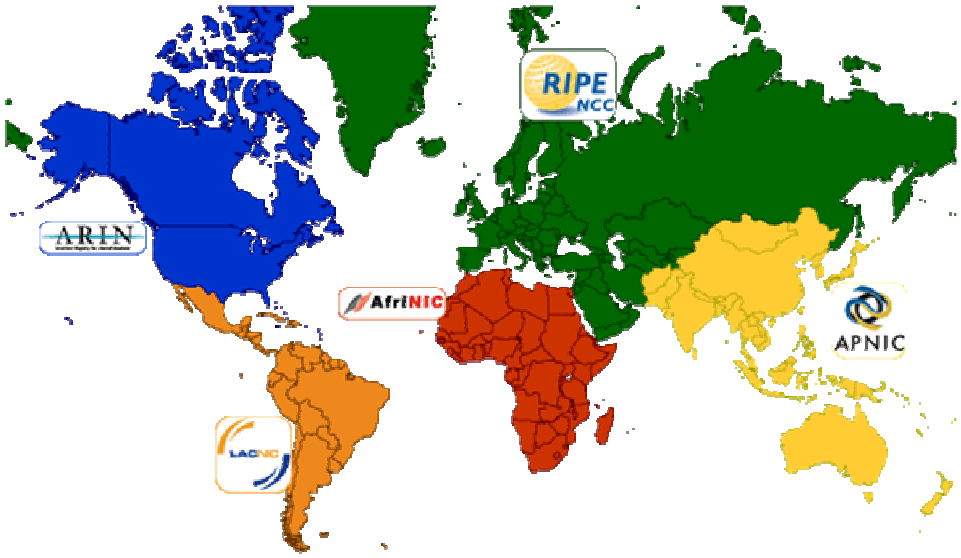
IP adresa je dio CIDR bloka X.Y.Z.W/N ukoliko joj je prvih N bitova jednako prvih N bitova bloka. Budući da je duljina adrese fiksna i iznosi 32 bita, N-bitni CDR prefiks ostavlja 32-N bitova za identificiranje pojedinih računala unutar bloka. Unutar bloka, dakle, može biti ukupno $2^{(32-N)}$ računala.

2.3.2. IANA

Dodjela CIDR blokova ni u kom slučaju nije slučajna. Obzirom da svaka adresa na Internetu mora biti jedinstvena, očita je potreba za organizacijom koja će nadzirati dodjelu i korištenje adresa. Ova je organizacija osnovana i zove se IANA (eng. *Internet Assigned Numbers Authority*). Njena RIR (eng. *Regional Internet Registries*) tijela upravljaju dodjelom adresa na cijelom Internetu. Ukupno ih je pet i ona su:

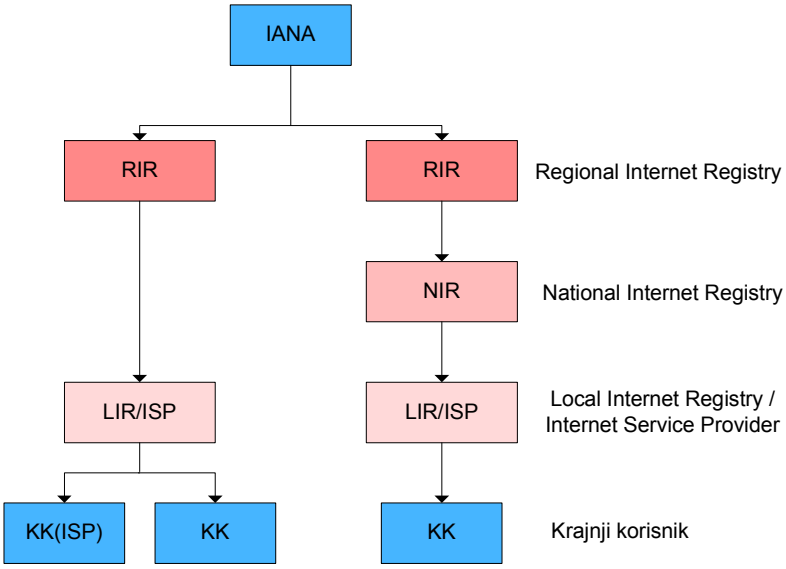
- *Réseaux IP Européens Network Coordination Centre* (RIPE NCC) sa sjedištem u Amsterdamu u Nizozemskoj. Obuhvaća područje Europe, Bliskog Istoka i Središnje Azije.
- *African Network Information Centre* (AfriNIC) sa sjedištem u Ebene City na otoku Mauricijusu. Obuhvaća Afričko područje.
- *Asia – Pacific Network Information Centre* (APNIC) sa sjedištem u Brisbaneu u Australiji. Obuhvaća područje jugoistočne Azije, Indiju, Pacifik i Australiju.
- *Latin American and Caribbean Internet Address Registry* (LACNIC) sa sjedištem u Montevideu u Urugvaju. Obuhvaća područje Latinske Amerike i Karipske regije.
- *American Registry for Internet Numbers* (ARIN) sa sjedištem u gradu Chantilly pokraj Washingtona u SAD-u. Obuhvaća područje Sjeverne Amerike.

Geografski raspored ovih pet tijela prikazan je na slijedećoj karti.



Slika 5. Geografski raspored pet RIR tijela

Hijerarhiju IANA organizacije u njenoj APNIC regiji nastavljaju tzv. NIR (eng. *National Internet Registry*) tijela koja su osnovana na državnoj razini i svaka država ima po jedno ovakvo tijelo. U svim ostalim regijama hijerarhija se nastavlja izravno LIR (eng. *Local Internet Registry*) tijelima, odnosno ISP (eng. *Internet Service Provider*) organizacijama. Shematski prikaz hijerarhije IANA organizacije prikazan je slijedećom slikom.



Slika 6. Hijerarhija tijela IANA organizacije

LIR tijela odnosno pružatelji Internet usluga u Hrvatskoj podijeljeni su u tri grupe:

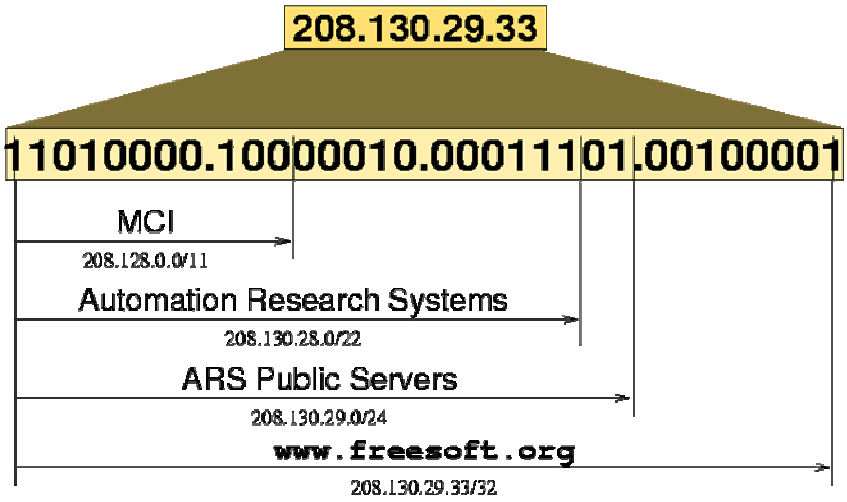
- U LARGE grupu s područja Hrvatske pripada samo HT.
- U MEDIUM grupu pripadaju Optima Telekom d.o.o., DCM , ISKON te neki pružatelji usluga koji nemaju sjedište u Hrvatskoj, ali svoje usluge nude i na našem području.
- U SMALL grupu spadaju CARNet, FINA, Global Net Grupa d.o.o., HEP d.d., Metronet telekomunikacije d.d., Optika Kabel TV d.o.o., Portus d.o.o., T-Mobile Hrvtska d.o.o., VIPnet d.o.o., Vodatel d.o.o., Vodatel telekomunikacije d.o.o. kao i neki pružatelji koji nemaju sjedište u Hrvatskoj, ali svoje usluge nude i na našem području.

Navedene grupe LARGE, MEDIUM i SMALL dobivaju se složenim izračunom korištenih IP adresa tijekom vremena.

2.3.3. Dodjela CIDR blokova

IANA svojim RIR tijelima dodjeljuje velike CIDR blokove. Primjerice, blok 62.0.0.0/8 koji sadrži preko šesnaest milijuna IP adresa dodijeljen je RIPE RIR tijelu. RIR tijelo dobiveni blok dijeli u manje podblokove te ih čini javno dostupnima. Podjela bloka na podblokove može se ponavljati nekoliko puta na različitim razinama. Veliki pružatelji pristupa Internetu (eng. *Internet Service Provider* - ISP) obično CIDR blokove dobivaju izravno od RIR tijela, te ih zatim dijele u manje blokove i dodjeljuju svojim pretplatnicima. Veličina bloka koji će biti dodijeljen pojedinom pretplatniku ovisi o veličini njegove mreže. Ovdje je potrebno primijetiti da IETF (eng. *Internet Engineering Task Force*), jedna od temeljnih standardizacijskih organizacija Interneta, korisnicima koji Internetu pristupaju putem samo jedne ISP organizacije preporuča traženje adresa od te organizacije, dok onima koji pristupaju putem više njih preporuča traženje adresa izravno od RIR tijela.

Kako bi se bolje razumjela hijerarhija u dodjeli CIDR blokova, može se promotriti primjer iz kasnih 1990-tih. U to vrijeme (od tada se situacija promijenila) stranica www.freesoft.org imala je IP adresu 208.130.29.33. Analiza te adrese otkriva tri CIDR prefiksa (slijedeća slika). Veliki CIDR blok 208.128.0.0/11 je ARIN RIR tijelo dodijelilo organizaciji MCI. Tvrtka *Automation Research System* (ARS) unajmila je vezu na Internet od tvrtke MCI i pritom dobila blok 208.130.28.0/22 kojim se može adresirati preko 1000 uređaja. Od tog bloka tvrtka ARS je jedan /24 blok namijenila svojim javnim poslužiteljima. Raspored CIDR prefiksa u adresi 208.130.29.33 prikazan je slijedećom slikom.



Slika 7. Raspored CIDR prefiksa u adresi 208.130.29.33

Pobrojani prefiksi adrese 208.130.29.33 koriste se na različitim mjestima u Internetu. Izvan MCI mreže koristi se prefiks 208.128.0.0./11 koji usmjerava sav promet prema cijeloj MCI mreži, te nijedan usmjernik izvan MCI mreže nije svjestan, primjerice bloka 208.130.28.0/22. S druge je strane, usmjernik koji se nalazi unutar MCI mreže svjestan 208.130.28.0/22 ali nije svjestan bloka 208.130.29.0/24. Ovakav princip hijerarhijskog uslojavanja omogućuje efikasno usmjeravanje prometa na Internetu.

2.3.4. Prednosti CIDR adresiranja

Glavna prednost CIDR adresiranja u odnosu na razredno adresiranje je mogućnost podjele adresnog prostora u finije dijelove. Ova mogućnost automatski vodi na bolje gospodarenje prostorom, odnosno na rjeđu pojavu neiskorištenih adresa.

Osim toga, grupiranje adresa u blokove omogućuje lakše i brže usmjeravanje paketa po mreži, jer ključni usmjernici ne moraju više poznavati smjerove za svaku od korištenih adresa, već im je dovoljno poznavati smjerove dodijeljenih blokova. Obzirom da je cijeli koncept rekurzivan, odnosno da se blokovi daju dijeliti u podblokove, problem usmjeravanja je dodatno olakšan.

CIDR adresiranje nudi još jednu prednost. Naime, moguće je više blokova ujediniti u jedan veći, što doprinosi fleksibilnosti mreže i također utječe na zaustavljanje rasta usmjerničkih tablica.

3. Protokoli automatskog dodjeljivanja IP adresa

3.1. RARP

RARP (eng. *Reverse Address Resolution Protocol*) je protokol koji se koristi za prevođenje fizičke adrese u IP adresu, a utemeljen je na mrežnom sloju OSI stoga. Naslijedili su ga protokoli BOOTP i DHCP koji podržavaju mnogo širi skup funkcionalnosti.
RARP protokol ima dva vrlo značajna ograničenja. Prvo se odnosi na obligatno konfiguriranje svake fizičke adrese izravno na središnjem RARP poslužitelju, dok je drugo povezano s nemogućnošću središnje konfiguracije podmreža, pristupnih poslužitelja (eng. *gateway*) i sl.

3.2. BOOTP

BOOTP (eng. *Bootstrap Protocol*) je UDP mrežni protokol kojeg klijenti koriste za automatsko određivanje svojih IP adresa. Sam proces određivanja adrese obično se pokreće prije inicijalizacije operativnog sustava, što je omogućilo primjenu ovog protokola u radnim stanicama bez tvrdih diskova (eng. *diskless workstation*).
Izvorno je protokol korišten na Unix utemeljenim radnim stanicama, gdje je pokretanje računala uključivalo i korištenje diskete za uspostavljanje inicijalne mrežne konekcije. Kasnije je implementacija ovog protokola uključena u neke mrežne kartice i većinu matičnih ploča koje otada podržavaju učitavanje operacijskog sustava izravno s mreže.
U novije vrijeme DHCP je istisnuo BOOTP protokol iz uporabe. Unatoč tome, većina današnjih DHCP poslužitelja također nudi i BOOTP podršku.

3.3. DHCP

DHCP (eng. *Dynamic Host Configuration Protocol*) je protokol koji komunikacijski uređaji poput računala, usmjernika ili mrežnog prilagodnika (eng. *network adapter*) koriste za dohvaćanje IP adrese, adrese preporučenog pristupnog poslužitelja (eng. *default gateway*), adrese DNS (eng. *Domain Name Server*) poslužitelja i sličnih podataka.
DHCP poslužitelj ima na raspolaganju skup IP adresa koje dodjeljuje svojim klijentima, pritom osiguravajući jedinstvenost IP adrese svakog od njih.

3.3.1. Pregled rada

Kada se računalo konfigurirano za korištenje DHCP usluge poveže na mrežu, DHCP klijentska aplikacija šalje DHCP poslužitelju zahtjev za potrebnim informacijama. Ovaj upit uobičajeno se šalje odmah nakon podizanja operacijskog sustava ili priključenja mrežnog kabela, a u vremenu do završetka njegove obrade klijent ne može pristupati ostalim računalima na mreži. DHCP poslužitelj upravlja skupom povjerenih mu IP adresa, a ima i informaciju o predodređenom pristupnom poslužitelju (eng. *default gateway*), nazivu domene, DNS poslužiteljima i sl. Klijentu na njegov zahtjev šalje odgovor koji sadrži dodijeljenu IP adresu, naziv domene, mrežnu masku, adresu pristupnog i DNS poslužitelja i slične informacije.
DHCP nudi tri tehnike upravljanja IP adresama. Najpoznatija među njima je dinamička (eng. *dynamic*) u kojoj se klijentu "iznajmljuje" određena IP adresa na određeni period vremena. Ovisno o stabilnosti mreže, ovaj period varira od nekoliko sati (primjerice u bežičnoj mreži zračne luke) do nekoliko dana (u žičnoj uredskoj mreži). U svakom trenutku prije isteka "najma" DHCP klijent može zahtijevati njegovo obnavljanje za trenutnu IP adresu. Odgovarajuće postavljen klijent koristi mehanizam obnove kako bi dodijeljenu adresu zadržavao cijelo vrijeme svoje povezanosti na dotičnu mrežu. Održavanje jednake IP adrese neophodno je za ispravan rad aplikacija koje se koriste višim slojevima OSI modela. Ako se dogodi istek "najma", klijent mora započeti novi proces pregovaranja za adresu, te u tom procesu može zatražiti dodjelu istekle adrese. Ipak, ne postoji nikakav oblik jamstva za njeno dobivanje.
Dvije preostale tehnike upravljanja IP adresama su automatska dodjela (eng. *automatic*) u kojoj je jedna adresa trajno povezana s jednim klijentom i ručna dodjela (eng. *manual*) u kojoj klijent sam odabire svoju IP adresu te potom, korištenjem DHCP protokola, obavještava poslužitelj o svom izboru.

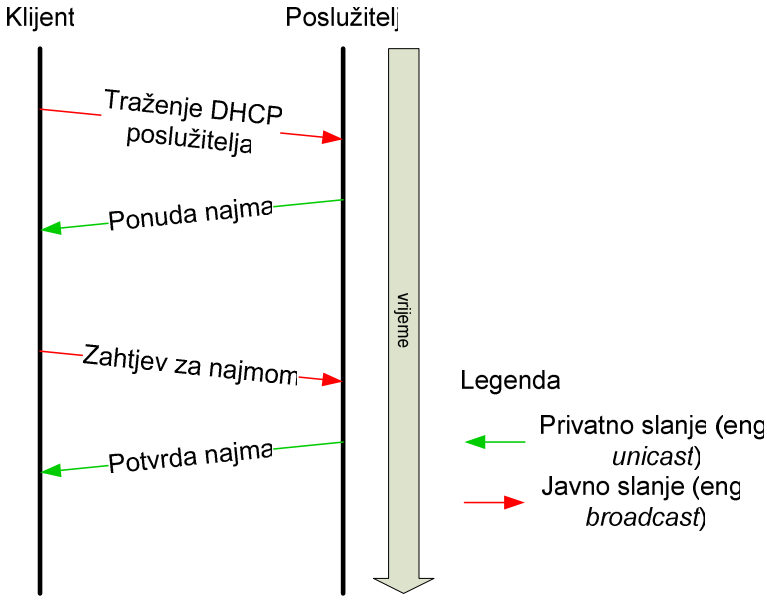
Dinamička dodjela IP adresa, iako na prvi pogled idealna, na probleme nailazi prilikom korištenja vatrozida (eng. *firewall*). Naime, zbog stalne promjene IP adresa vrlo je teško prilagoditi rad ove zaštitne aplikacije. U tim slučajevima obično se pribjegava primjeni neke od preostalih dviju tehnika upravljanja.
Pregovaranje za inicijalnu adresu započinje klijent slanjem javne (eng. *broadcast*) poruke. Ukoliko DHCP poslužitelj nije postavljen u lokalnoj mreži, a usmjernik (eng. *router*) nije prilagođen za kompenzaciju nastale situacije, DHCP poslužitelj neće primiti poslani zahtjev jer usmjernici po svom predodređenom ponašanju javne poruke prosljeđuju samo unutar lokalne mreže.

3.3.2. Tehnički detalji

DHCP koristi dva priključka (eng. *port*) koja je IANA (eng. *Internet Assigned Numbers Authority*) organizacija dodijelila protokolu BOOTP. Radi se o UDP priključcima 67 i 68, pri čemu prvog od njih koristi poslužitelj, a drugog klijenti.
Rad DHCP protokola može se podijeliti u četiri faze:

- zahtjev za "najmom" IP adrese,
- ponuda "najma",
- izbor "najma" i
- potvrda "najma".

Slijed pobrojanih faza u vremenu prikazan je na slijedećoj slici.



Slika 8. Komunikacija u DHCP protokolu

4. Sigurnosni problemi automatske dodjele IP adresa

4.1. Napadi na DHCP

Iako su DHCP poslužitelji kritični za rad većine poslovnih mreža, njihova sigurnost je jedno od najrjeđe razmatranih područja računalne sigurnosti. Razlog za to je vjerojatno posvemašnja jednostavnost ovog protokola.
Međutim, upravo se u toj jednostavnosti skriva i najveća ranjivost. Između DHCP klijenta i poslužitelja ne odvija se nikakav oblik autorizacije ni autentikacije, tako da poslužitelj ne može znati je li računalo koje zahtjeva adresu legitimni korisnik mreže, a klijent, s druge strane, ne može provjeriti legitimnost DHCP poslužitelja. Prisutnost ilegalnih DHCP klijenata i poslužitelja u nekoj računalnoj mreži može prouzročiti različite probleme.

Primjerice, ilegalni DHCP poslužitelj može legalnim klijentima dati krive informacije o njihovom TCP/IP okruženju, te tako spriječiti njihovo povezivanje na mrežu. Ovo predstavlja oblik tzv. DoS (eng. *Denial of Service*) napada, odnosno napada uskraćivanja usluge. Pri ovom razmatranju potrebno je u obzir uzeti i jednostavnost postupka postavljanja ilegalnog poslužitelja. Postupak je, naime, toliko jednostavan da zahtjeva samo malo socijalnog inženjeringa kojim se ostvaruje fizički pristup mrežnom priključku. Osim toga potrebno je i prijenosno računalo koje, spojeno na dobiveni priključak, može postati DHCP poslužitelj.
Drugi primjer napada može uključivati napadača koji je kompromitirao neko od računala računalne mreže i instalirao program koji stalno šalje zahtjeve za novim IP adresama koristeći krivotvorene MAC adrese u njihovom formiranju. Ovaj postupak radi sve dok ne iscrpi sve adrese koje su na raspolaganju DHCP poslužitelju. Nakon toga legitimni klijenti se više ne mogu spojiti na računalnu mrežu, što je ponovno oblik napada uskraćivanja usluge.
Mnogo ozbiljniji problem nastaje kada napadač uspije ovladati računalima koja su mrežni DHCP poslužitelji. U tom trenutku on može nastaviti s izmjenom koja će svim klijentima slati krive podatke o podmreži i tako opet dovesti do DoS stanja. Druga mogućnost je izmjena DNS (eng. *Domain Name System*) DHCP postavki. Ovako se legalna mrežna računala može usmjeriti na zlonamjerno oblikovane web stranice gdje klijenti, bez svijesti o tome što se događa, mogu kompromitirati svoje računalo. Treća mogućnost je izmjena DHCP poslužitelja na način da on klijentima kao adresu pristupnog poslužitelja šalje adresu napadačevog računala. Tada sav dolazni i odlazni promet prolazi preko tog računala, što napadaču otvara mogućnost za izvođenje tzv. *Man-In-the-Middle* napada, odnosno za razotkrivanje osjetljivih informacija.

4.2. Obrana DHCP sustava

Unatoč postojanju određenog broja zaštitnih rješenja koji omogućuju detekciju, pa čak i sprečavanje rada ilegalnih DHCP poslužitelja, pokazuje se da se sva ona, s više ili manje uloženog truda mogu zaobići.
Dosad se najboljom pokazala metoda zaštite koja napadaču onemogućuje pristup štićenoj mreži. Ova zaštita ima dva aspekta:

- zaštitu fizičkog pristupa i
- zaštitu od mrežnog pristupa.

Zaštita od fizičkog pristupa obuhvaća isključivanje nekorištenih mrežnih priključaka, zaključavanje vrata i edukaciju osoblja sa ciljem osposobljavanja za prepoznavanje socijalnog inženjeringa i borbu protiv njega.
Zaštita od mrežnog pristupa uključuje primjenu rigorozne vatrozidne zaštite zajedno sa sustavom za otkrivanje upada (eng. *Intrusion Detection System* - IDS).
Još od 2003. organizacija *Internet Engineering Task Force* (IETF) radi na problemu sigurnosti DHCP poslužitelja. Oni predlažu proširenje DHCP protokola dodatkom autentikacije temeljene na korištenju tokena ili na zaštiti simetričnim kriptiranjem. Ovakvo rješenje ipak uvodi potrebu za pretkonfiguracijom klijenata, koja se upravo htjela izbjeći uvođenjem DHCP protokola.
S druge strane, IPv6 može ponuditi jednostavnije rješenje ovog problema. Budući da je, za razliku od IPv4, dizajniran sa stalnim razmišljanjem o sigurnosti, on može ponuditi zaštitu DHCP prometa. Ako se u obzir uzme veliko zalaganje Ministarstva obrane Sjedinjenih Američkih Država spram uvođenja IPv6 protokola u sve njihove mreže, logična je posljedica i trenutno veliki interes proizvođača, kako sklopovlja, tako i programske potpore, koji svoje proizvode žele čim prije uskladiti s ovim standardom. Sve ovo vodi na brže prihvaćanje IPv6, nego što je to izvorno očekivano. Kad se to jednom dogodi, kada IPv6 konačno prevlada, na pitanje sigurnosti DHCP protokola i računalne sigurnosti općenito morat će se ionako tražiti novi odgovor.

5. Zaključak

IP je kao protokol osmišljen još 1980-tih godina. U tim danima rijetki su bili oni koji su mogili predvidjeti kasnije ostvarenu brzinu razvoja Interneta i njegovog uključivanja u sve sfere ljudskog života.

Upravo su ti rani trenuci Interneta, odnosno odluke koje su u njima donošene ocrtale njegovu današnju strukturu i njegove današnje probleme. Adresiranje, koje je jedan od temeljnih koncepata IP protokola, bilo je napravljeno u skladu s tadašnjim predodžbama razvoja. Međutim, kada se pokazalo da je taj razvoj u stvari daleko brži, došlo je do različitih problema.

Tu se u prvom redu misli na problem iscrpljivanja adresnog prostora, odnosno nestanka dostupnih IP adresa, ali i na problem brzo rastućih usmjerničkih tablica. Potonji od dva problema gotovo je u potpunosti riješen uvođenjem CIDR sustava raspolaganja adresama, ali problem uskog adresnog prostora aktualan je i danas.

U pokušaju njegova rješavanja uvedena su različita poboljšanja i nastali su različiti protokoli. Neki su od njih usmjereni prema dinamičkoj dodjeli adresa te su opisani u ovom dokumentu.

Ipak, pravo i potpuno rješenje problema malog adresnog prostora , a ujedno i rješenje koje će gotovo u potpunosti eliminirati potrebu za bilo kakvom dinamikom, može se ostvariti jedino potpunim prelaskom s IPv4 na IPv6 protokol.

6. Reference

[1] IP Adrese , http://en.wikipedia.org/wiki/IP_address, rujan 2007.

[2] Razumijevanje IP adresa: Sve što ste ikad htjeli znati http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf, rujan 2007.

[3] DHCP, http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol, rujan 2007.

[4] Sigurnost DHCP poslužitelja, http://www.windowsecurity.com/articles/DHCP-Security-Part1.html, rujan 2007.

[5] Sve o IP adresama, http://www.networkcomputing.com/netdesign/ip101.html , rujan 2007.

[6] RIPE NCC Billing Procedure and Fee Schedule 2004, http://www.ripe.net/docs/billing2004.html, rujan 2007.