HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

IPv6 protokol

CCERT-PUBDOC-2006-11-173

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

Trenutna inačica IP-a (eng. *Internet Protocol*), IPv4, nije značajnije izmijenjena od 1981. godine, odnosno izdavanja RFC norme pod rednim brojem 791. Glavni razlozi tome su jednostavnost njegovih implementacija i dokazana robusnost na skaliranje u globalnoj računalnoj mreži. Ipak, prilikom oblikovanja IPv4 protokola nisu mogle predvidjeti sljedeće činjenice:

- Eksponencijalni rast globalne računalne mreže koji je doveo do potrošnje cjelokupnog adresnog prostora IPv4 protokola.
- Potrebu za jednostavnijim postupkom postavljanja adresa. Većina IPv4 implementacija zahtjeva ručno postavljanje IP adrese ili korištenje dodatnog protokola, kao što je, primjerice, DHCP (eng. *Dynamic Host Configuration Protocol*). Povećanje broja uređaja koji pristupaju Internetu zahtjeva jednostavnije (automatsko) postavljanje adrese koja ne ovisi o DHCP infrastrukturi.
- Potrebu za sigurnosnom zaštitom na razini samog IP-a. Komunikacija putem javne mreže kao što je Internet zahtjeva kriptografske servise koji osiguravaju tajnost i integritet podataka. Iako standard koji pruža sigurnost IPv4 paketima postoji (IPsec), on je opcionalan i nedovoljno prihvaćen.
- Potrebu za većom kvalitetom usluge, odnosno osiguranjem dostave podataka u stvarnom vremenu (eng. *Quality of Service*). Kod IPv4 protokola ona se ostvaruje poljem „Vrsta usluge“ odnosno identifikacijom sadržaja paketa, što je pokazalo ograničenu funkcionalnost. To ograničenje je posebice izraženo u slučajevima u kojima sadržaj samog mrežnog paketa nije moguće odrediti, primjerice zbog korištenja enkripcije.

Za rješavanje navedenih, ali i velikog broja dodatnih problema, međunarodna radna skupina IETF (eng. *Internet Engineering Task Force*) oblikovala je skupinu protokola i normi (RFC 1752, 1883, 1886, 1971, 1993) pod zajedničkim imenom IPv6 (IP inačice 6). Pri njezinom oblikovanju nastojalo se osigurati neophodnu nadogradnju uz što manji utjecaj na ostale slojeve mrežne arhitekture.

U nastavku dokumenta opisane su glavne funkcionalnosti IPv6 protokola te raspoloživi načini adresiranja.

2. Značajke IPv6 protokola

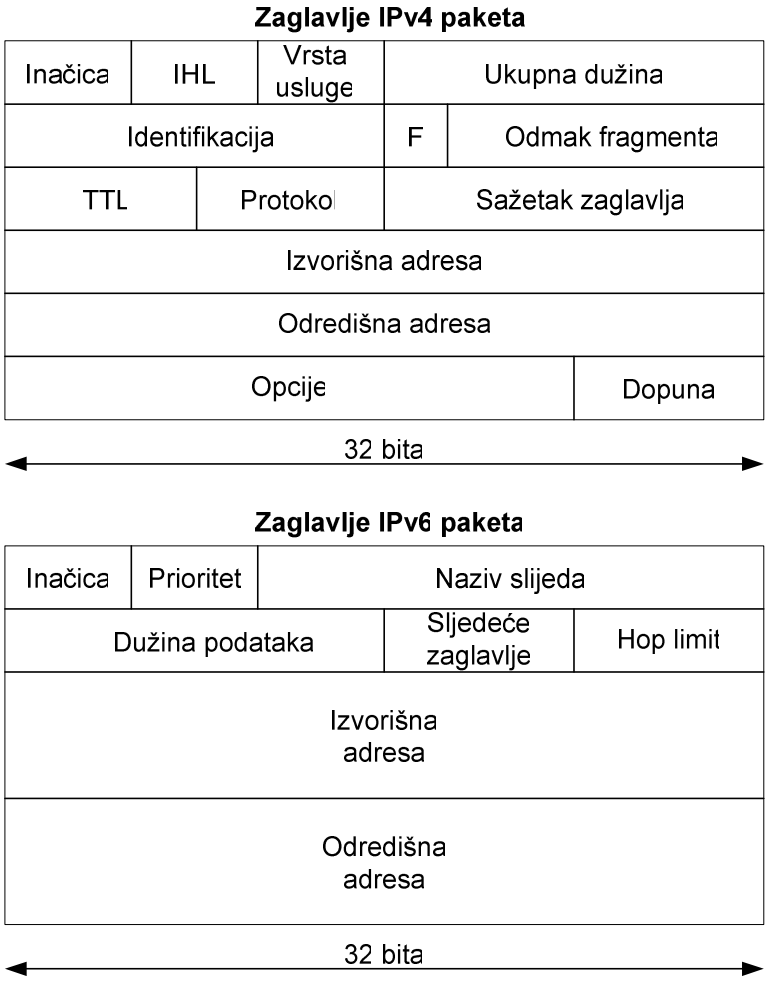
Najvažnije značajke IPv6 protokola su sljedeće:

- novi format zaglavlja,
- veličina adresnog prostora,
- ugrađeni sigurnosni mehanizmi,
- poboljšana podrška za kvalitetu usluge (QoS) i
- proširivost.

U slijedećim poglavljima pregledno je objašnjena svaka od navedenih značajki.

2.1. Novi format zaglavlja

Usporedbom zaglavlja IPv6 paketa sa zaglavljem IPv4 paketa (slika 1) moguće je primijetiti kako određena polja nedostaju. Riječ je o poljima IHL (ukupna veličina zaglavlja IP paketa), vrsta usluge, odmak fragmenta, identifikacija, F (zastavica), sažetak zaglavlja i opcije.



Slika 1: Usporedba zaglavlja IPv4 i IPv6 paketa

Najznačajnija promjena odnosi se na polje „Opcije“. Kod IPv4 protokola polje „Opcije“ koristi se za dodavanje dodatnih informacija o raznim opcionalnim uslugama (primjerice enkripciji sadržaja paketa). Zbog navedene činjenice dužina zaglavlja IPv4 paketa nije ujednačena, već ovisi o broju korištenih opcija što znatno otežava i usporava postupak obrade i usmjeravanja paketa te nameće veće zahtjeve na sklopovlje usmjerivača. S druge strane, IPv6 protokol informacije o dodatnim uslugama pomiče u dio paketa koji se naziva ekstenzija zaglavlja (na slici 1 prikazan je samo osnovni

dio zaglavlja IPv6 paketa). Na taj način, veličina zaglavlja „običnih“ IP paketa fiksirana je na 40 okteta, što znatno olakšava njihovu obradu.
Druga značajna razlika IPv4 i IPv6 zaglavlja jest polje „Sažetak zaglavlja“. To je polje koje se kod IPv4 protokola koristi kod kontrole integriteta sadržaja zaglavlja, a prilikom čijeg se izračuna koriste vrijednosti svih polja zaglavlja. Budući da „TTL“ polje u zaglavlju paketa sadrži vrijednost koja se mijenja svakim prolazom kroz usmjerivač, polje „Sažetak zaglavlja“ treba se ponovno računati na svakom koraku prolaza kroz mrežu. Uklanjanjem tog polja, IPv6 protokol znatno umanjuje količinu posla kojeg obavljaju usmjerivači te na taj način smanjuje kašnjenje koje unose u računalnu mrežu. Integritet prenesenih podataka pritom nije ugrožen, budući da TCP sloj, koji se nalazi „iznad“ IP sloja, između ostalog provjerava integritet adresa izvorišta odnosno odredišta pa to nije potrebno izvoditi i u IP sloju.
Polje „Vrsta usluge“ kod IPv4 protokola koristi se za označavanje prioriteta paketa, pri čemu se razina prioriteta prikazuje cjelobrojnom vrijednošću od 0 do 7. IPv6 protokol pruža istu funkcionalnost kroz polje koje se zove „Prioritet“.
Polje „Naziv slijeda“ uvedeno je u zaglavlje IPv6 paketa radi određivanja slijeda paketa određene vrste usluge (primjerice VoIP). Ta funkcionalnost postoji i kod IPv4 protokola, iako zahtjeva veći broj zasebnih operacija (provjera broja mrežnog priključka, odredišnih i izvorišnih adresa). Budući da se određivanje slijeda paketa pokazalo kao iznimno korisna funkcionalnost, prilikom specifikacije IPv6 protokola za tu je svrhu rezervirano posebno polje.
Prilikom oblikovanja zaglavlja IPv6 paketa nastojalo se višak informacija preseliti u ekstenziju zaglavlja. Na taj je način postignuta učinkovitija obrada paketa na usmjerivačima, pogotovo u slučaju posrednih usmjerivača koji paket samo prosljeđuju. Važno je također primijetiti kako ne postoji kompatibilnost IPv4 i IPv6 zaglavlja, tako da usmjerivači koji rade u miješanim okruženjima moraju implementirati oba protokola.
IPv6 paket može imati nula ili više ekstenzija zaglavlja pri čemu polje „Sljedeće zaglavlje“ definira sljedeću ekstenziju zaglavlja, s tim da posljednja ekstenzija zaglavlja na tom mjestu ukazuje na protokol višeg mrežnog sloja (npr. TCP ili UDP).

2.2. Veličina adresnog prostora

IPv4 adresa je duga 32 bita, čime se ostvaruje približno 4,3 milijarde jedinstvenih adresa. Uzimajući u obzir porast broja mobilnih uređaja koji se spajaju na Internet, poput prijenosnih računala, dlanovnika ili mobitela i tehnološki razvoj određenih zemalja (Indija, Kina), jasno je da IPv4 protokol polako iscrpljuje svoje resurse. Kao posljedica javila se potreba za uvođenjem NAT (eng. *Network Address Translation*) usluge koja višestruke privatne IP adrese preslikava u jednu javnu IP adresu. Iako NAT usluga rješava većinu problema oko ograničenosti javnog adresnog prostora, ona uvodi kašnjenje u računalne mreže te onemogućava izravno adresiranje koje je sukladno ideji IP protokola.
Kod IPv6 protokola IP adresa računala je veličine 128 bita čime se ostvaruje približno 3.4×10^{38} (340282366920938463463374607431768211456) jedinstvenih adresa. Veličina adresnog prostora IPv6 protokola omogućuje definiranje podmreža višestrukih razina te zauzimanje ogromnog broja javnih adresa. Na taj način moguće je ostvariti izravno adresiranje te nestaje potreba za tehnikama očuvanja javno dostupnih adresa.

2.3. Zapis IPv6 adrese

IPv6 adresa se obično zapisuje kao osam grupa od četiri heksadekadske znamenke odijeljene dvotočkom. Kao primjer može se prikazati sljedeća IPv6 adresa:

```
0010000111011010000000001101001100000000000000000010111100111011
0000001010101010000000001111111111111111000101000100111000101101O
```

Adresa se može podijeliti u 8 grupa od po 16 bitova:

```
0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010
```

Svaki 16-bitni blok pretvara se u heksadekadske znamenke i odvaja dvotočkom:

```
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
```

Prikaz IPv6 adrese dodatno se može pojednostaviti uklanjanjem početnih nula svakog 16-bitnog bloka:

```
21DA:D3:0:2F3B:2AA:FF:FE28:9C5A
```

Dodatno pojednostavljivanje IPv6 adresa moguće je izvesti i za slučaj adresa koje sadrže slijedne 16-bitne blokove isključivo sačinjene od nula. Na taj se način adrese:

```
FE80:0:0:0:2AA:FF:FE9A:4CA2, odnosno
FF02:0:0:0:0:0:0:2
```

mogu prikazati kao:

```
FE80::2AA:FF:FE9A:4CA2, odnosno
FF02::2
```

Kod pojednostavljivanja adresa korištenjem dvostruke dvotočke skraćivanje je moguće izvesti samo jednom za pojedinu adresu, budući da u protivnom nije moguće odrediti broj bitova postavljenih na nulu za pojedinu „::“ sekvencu.

2.4. Prefiksi IPv6 adresa

Dio IPv6 adrese koji sadrži bitove čija je vrijednost fiksna ili određena prefiksom podmreže naziva se prefiks IPv6 adrese. Prefiksi se za IPv6 adrese označavaju analogno CIDR (eng. *Classless Inter-Domain Routing*) zapisu IPv4 protokola, koristeći notaciju *adresa/dužina prefiksa*. Kao primjer može poslužiti sljedeći prefiks podmreže:

```
21DA:D3:0:2F3B::/64
```

Valja napomenuti kako se kod IPv4 protokola koristila notacija prefiksa mreže poznatija kao mrežna maska. Pojam mrežne maske ne koristi se kod IPv6 protokola, već isključivo notacija s dužinom prefiksa.

2.5. Sigurnosni aspekt ekstenzija zaglavlja IPv6 paketa

Norma RFC 2460 definira sljedeće ekstenzije zaglavlja IPv6 paketa, koje moraju biti podržane od strane svakog mrežnog čvora:

- zaglavlje za svaki skok (eng. *hop*),
- zaglavlje odredišnih opcija,
- usmjerivačko zaglavlje,
- zaglavlje fragmenta,
- autentikacijsko zaglavlje i
- zaglavlje enkapsuliranih sigurnosnih podataka (eng. *Encapsulating Security Payload*).

Sa stajališta sigurnosti, zanimljiva su posljednja dva zaglavlja pa će ona biti i detaljnije opisana.

2.5.1. Autentikacijsko zaglavlje

Sigurnosna arhitektura IP protokola, definirana normom RFC 2401, uključuje i autentikacijsko zaglavlje paketa. To je zaglavlje definirano posebnom normom - RFC 2402, a koristi se za autentikaciju

izvora podataka (potvrdu mrežnog čvora koji je poslao paket), očuvanje integriteta podataka (osiguranje od izmijene podataka u prijenosu) te zaštitu od napada presretanjem i ponovnim slanjem paketa.
Autentikacijsko zaglavlje identificira se vrijednošću 51 u polju „Sljedeće zaglavlje“ prethodnog zaglavlja. Zaglavlje sadrži sljedeće elemente:

- polje „Sljedeće zaglavlje“ (ukazuje na postojanje dodatnog zaglavlja),
- indeks sigurnosnih parametara (identifikator IPSec sigurnosne asocijacije),
- broj sekvence (omogućava zaštitu od napada presretanjem i ponovnim slanjem paketa) i
- autentikacijski podaci (omogućavaju provjeru integriteta i autentičnosti poruke).

Potrebno je primijetiti kako autentikacijsko zaglavlje ne ostvaruje tajnost podataka. Ukoliko postoji potreba i za tom uslugom, ovo je zaglavlje moguće koristiti u sprezi sa zaglavljem enkapsuliranih sigurnosnih podataka (eng. *Encapsulating Security Payload*).

2.5.2. Zaglavlje enkapsuliranih sigurnosnih podataka

Norma RFC 2406 definira zaglavlje enkapsuliranih sigurnosnih podataka, koje putem kriptografskih mehanizama ostvaruje tajnost podataka uključenih u IP paket. Osim tajnosti, ovo zaglavlje osigurava autentičnost i integritet podataka. Zaglavlje enkapsuliranih sigurnosnih podataka identificira se vrijednošću 50 u polju „Sljedeće zaglavlje“ prethodnog zaglavlja.
Ono sadrži sljedeće elemente:

- indeks sigurnosnih parametara (identifikator IPSec sigurnosne asocijacije),
- broj sekvence (omogućava zaštitu od napada presretanjem i ponovnim slanjem paketa),
- polje „Sljedeće zaglavlje“ (ukazuje na postojanje dodatnog zaglavlja) i
- autentikacijski podaci (omogućavaju provjeru integriteta i autentičnosti podataka).

Osim navedenih elemenata, zaglavlje sadrži i polje dopune (eng. *padding*). Ono se koristi kada korišteni kriptografski algoritam zahtjeva blokove podataka čija je veličina višekratnik nekog broja.

3. Načini IPv6 adresiranja

Postoje 3 osnovna načina IPv6 adresiranja:

1. **Jednoodredišno adresiranje (eng. *unicast*)**
   Adresiranje jednog mrežnog sučelja, unutar dosega odgovarajućeg tipa jedinične adrese, naziva se jednoodredišno adresiranje. Takvi adresirani paketi isporučuju se jednom mrežnom sučelju pa se ovaj tip adresiranja koristi kod 1:1 komunikacije.
2. **Višeodredišno adresiranje (eng. *multicast*)**
   Istovremeno adresiranje većeg broja mrežnih sučelja ostvaruje se višeodredišnim adresiranjem. Takvo se adresiranje koristi kod 1:N komunikacije, gdje se isti paket dostavlja svim adresiranim mrežnim sučeljima.
3. **Adresiranje „najbliže“ adrese (eng. *anycast*)**
   Ovaj tip adrese adresira jedinstveno mrežno sučelje, pri čemu se paket dostavlja sučelju koje je „najbliže“ odredišnoj adresi. Pojam „najbliže“ određen je usmjerivačkom metrikom. Ovaj se tip adresiranja koristi kod komunikacije 1:(1 od N).

Valja primijetiti kako, neovisno o načinu adresiranja, IPv6 adrese označuju sučelja, a ne mrežne čvorove (računala). Mrežni čvor je određen bilo kojom jednoodredišnom (eng. *unicast*) adresom dodijeljenoj jednom od njegovih mrežnih sučelja. Dodatno, arhitektura adresiranja IPv6 protokola, definirana RFC normom 3513, ne zahtjeva univerzalnu (eng. *broadcast*) adresu kao što je to slučaj kod IPv4 protokola.

3.1. Jednoodredišno adresiranje (eng. *unicast*)

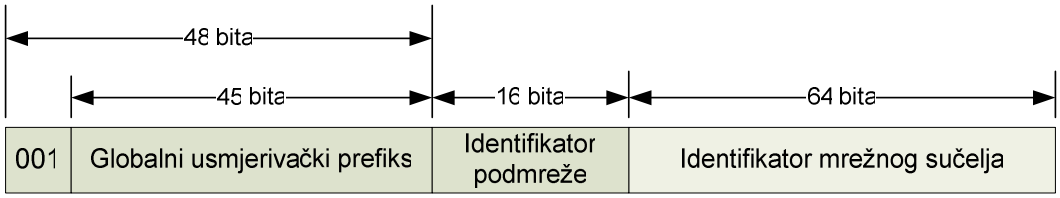
Sljedeće vrste adresa pripadaju skupini jednoodredišnih IPv6 adresa:

- globalne jednoodredišne adrese,
- adrese lokalne poveznice (eng. *link-local*),
- adrese administrativne domene (eng. *site-local*),
- jedinstvene lokalne IPv6 jednoodredišne adrese i

- posebne adrese.

3.1.1. Globalne jednoodredišne adrese

Globalne jednoodredišne adrese istovjetne su javnim IPv4 adresama. To su adrese koje su dostupne na globalnoj razini. Za razliku od IPv4 adresne arhitekture koja sadrži elemente „plošnog" i hijerarhijskog usmjeravanja, IPv6 arhitektura oblikovana je tako da podržava efikasno hijerarhijsko adresiranje i usmjeravanje. Doseg adrese – sekcija IPv6 mreže nad kojom je određena adresa jedinstvena, za slučaj globalne jednoodredišne adrese jest cjelokupna IPv6 mreža (Internet).
Na slici 2 prikazana je struktura globalne jednoodredišne adrese, definirane normom RFC 3587:



Slika 2: Struktura globalne jednoodredišne adrese

Može se uočiti da je struktura globalne jednoodredišne adrese podijeljena u sljedeće kategorije:

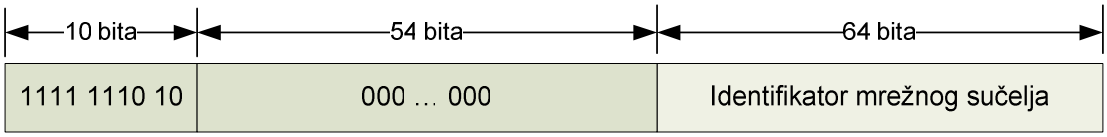
- Fiksni dio postavljen na vrijednost 001 - tri najznačajnija bita postavljena su na 001 pa je prefiks za globalne adrese 2000::/3.
- Globalni usmjerivački prefiks - označava globalni usmjerivački prefiks za administrativnu domenu određene organizacije. U kombinaciji s 3-bitnim fiksnim dijelom čini 48-bitni prefiks administrativne domene. Nakon dodjele ovakve adrese, usmjerivači na IPv6 Internetu prosljeđuju sav promet čijih se prvih 48 bita adrese poklapa s navedenim prema usmjerivačima dotične organizacije.
- Identifikator podmreže - koristi se unutar organizacije za identifikaciju podmreže kojoj je IPv6 paket namijenjen. Veličina ovog polja je 16 bita, što omogućava ostvarivanje 65.536 podmreža ili višestruke razine hijerarhije.
- Identifikator mrežnog sučelja - 64 bitni identifikator koji određuje mrežno sučelje odgovarajuće podmreže unutar administrativne domene organizacije kojemu je IPv6 paket namijenjen.

3.1.2. Jednoodredišne adrese za lokalno korištenje

Postoje dvije vrste jednoodredišnih adresa namijenjenih lokalnom korištenju:

1. adresa lokalne poveznice (eng. *link-local*) koje se koriste između dva računala na istoj lokalnoj mreži u procesu otkrivanja susjeda (eng. *Neighbor Discovery*) i
2. adresa administrativne domene (eng. *site-local*) koje se koriste za komunikaciju između dva čvora koji se nalaze unutar iste administrativne domene.

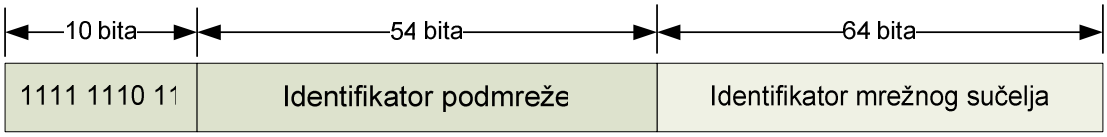
Komunikacija dvaju susjednih čvorova koji se nalaze na istoj poveznici odvija se pomoću adresa lokalne poveznice (eng. *link-local address*). Te adrese odgovaraju automatskim privatnim IP adresama (eng. APIPA - *Automatic Private IP Addressing*) korištenim kod IPv4 protokola.
Adresa lokalne poveznice potrebna je za proces otkrivanja susjeda (eng. *Neighbor Discovery*) i uvijek se postavlja automatski, čak i u slučaju kada jednoodredišna adresa ne postoji.
Na slici 3 prikazana je struktura adrese lokalne poveznice, definirane normom RFC 3587:



Slika 3: Struktura adrese lokalne poveznice

Adresa lokalne poveznice uvijek započinje sa sekvencom FE80, uz prefiks FE80::/64 (identifikator mrežnog sučelja veličine je 64 bita). Promet IPv6 paketa koji sadrže adresu lokalne poveznice nikad se od strane usmjerivača ne prosljeđuje izvan lokalne poveznice.

Adrese administrativne domene odgovaraju adresnom prostoru privatnih IPv4 adresa (10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16). Te se adrese koriste u privatnim lokalnim mrežama koje nisu izravno spojene na IPv6 Internet, bez opasnosti od konflikta s globalnim jednoodredišnim adresama. Adrese administrativne domene nisu dostupne izvan domene u kojoj su definirane te se promet IPv6 paketa koji sadrže takve adrese ne prosljeđuje izvan domene iz koje je potekao.
Na slici 4 prikazana je struktura adrese administrativne domene, definirane normom RFC 3587:

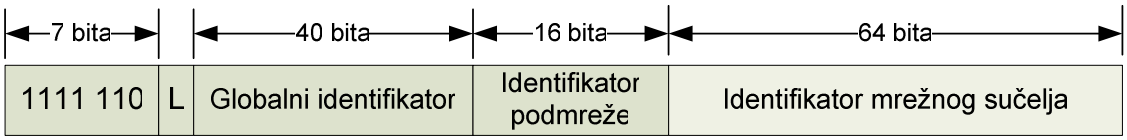


Slika 4: Struktura adrese administrativne domene

Prvih 10 bitova ovakvog tipa adrese uvijek su fiksirani na vrijednost 1111 1110 11 pa je prefiks ovakve adrese FEC0::/10. Identifikator podmreže je veličine 54, a mrežnog sučelja 64 bita.

3.1.3. Jedinstvene lokalne IPv6 jednoodredišne adrese

Adrese lokalne poveznice omogućuju privatno adresiranje. Budući da prefiks takve adrese može adresirati višestruke domene određene organizacije, isti se može duplicirati. Na taj način može doći do nejednoznačnosti adresa lokalne poveznice što uvodi dodatne poteškoće za aplikacije, usmjerivače i mrežne administratore. Iz tog se razloga adrese lokalne poveznice zamjenjuju adresama koje su u okvirima dotične organizacije privatne, ali opet jedinstvene. Norma RFC 4193 definira jedinstvene lokalne IPv6 jednoodredišne adrese, koje se jednostavnije nazivaju lokalnim adresama.
Na slici 5 prikazana je struktura lokalne adrese, definirane normom RFC 4193:



Slika 5: Struktura jedinstvene lokalne IPv6 jednoodredišne adrese

Prvih sedam bitova ove vrste adrese fiksirano je na vrijednost 1111 110, uz zastavicu L postavljenu na 1 pa je prefiks takvih adresa FD00::/7. Globalnim identifikatorom određuje se administrativna domena unutar organizacije.
Iako je doseg lokalne adrese globalni, dostupnost takve adrese određena je topologijom usmjeravanja. Organizacije neće oglašavati prefikse lokalnih adresa kao DNS AAAA zapise, čineći na taj način takve adrese globalno nedostupnim.

3.1.4. Posebne IPv6 adrese

U ovu kategoriju pripadaju sljedeće vrste adresa:

- Neodređene adrese (0:0:0:0:0:0:0:0 odnosno ::) koriste se za ukazivanje na nedostatak adrese. Ekvivalentna je neodređenoj IPv4 adresi (0.0.0.0). Takva se adresa nikada ne dodjeljuje mrežnom sučelju niti koristi kao odredišna adresa IPv6 paketa.
- Adresa povratne petlje (eng. *loopback address*), čija je vrijednost 0:0:0:0:0:0:0:1 odnosno ::1, koristi se za identifikaciju povratnog mrežnog sučelja, koje mrežnim čvorovima omogućava da šalju pakete sami sebi. Takve se adrese nikada ne šalju na mrežnu poveznicu niti prosljeđuju IPv6 usmjerivačima.

3.1.5. Kompatibilnost IPv4 i IPv6 adresa

Zbog pomoći prilikom prelaska s IPv4 na IPv6 mrežnu arhitekturu, odnosno istovremenog postojanja čvorova obje vrste, definirane su sljedeće adrese:

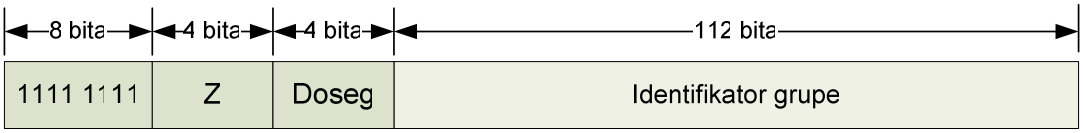
- IPv4-kompatibilna adresa - 0:0:0:0:0:0:*w.x.y.z* odnosno ::*w.x.y.z* (gdje je *w.x.y.z* uobičajeni prikaz IPv4 adrese) koristi se na IPv4/IPv6 čvorovima koji komuniciraju pomoću IPv6 protokola. IPv4/IPv6 čvorovi su čvorovi koji podržavaju oba protokola. Kada se u mrežnom

paketu koristi IPv4-kompatibilna adresa kao IPv6 odredišna adresa, paket se automatski preoblikuje u IPv4 paket i šalje putem IPv4 infrastrukture.

- IPv4-mapirana adresa - 0:0:0:0:0:FFFF:*w.x.y.z* odnosno ::FFFF:*w.x.y.z*, koristi se za interno predstavljanje čvora koji podržava isključivo IPv4 protokol. Takva se adresa nikada ne koristi kao izvorišna ili odredišna adresa IPv6 paketa.
- 6na4 adresa - koristi se za komunikaciju dva čvora koji podržavaju IPv4 i IPv6 protokol, i to preko IPv6 arhitekture. Adresa tipa 6na4 formira se kombiniranjem prefiksa 2002::/16 i 32-bitne javne IPv4 adrese, što rezultira 48-bitnim prefiksom. Na taj se način ova vrsta adresiranja može opisati kao tehnika tuneliranja, što je opisano normom RFC 3056.

3.2. Višeodredišno adresiranje (eng. *multicast*)

Višeodredišno adresiranje IPv6 protokola funkcionira kao i kod IPv4 protokola. Proizvoljan IPv6 čvor može osluškivati mrežni promet na proizvoljnoj IPv6 višeodredišnoj adresi, ili čak na više njih istovremeno. Čvorovi mogu pristupiti višeodredišnoj grupi ili ju napustiti u bilo kojem trenutku. Višeodredišna se adresa ne smije koristiti kao izvorišna.
IPv6 višeodredišne adrese imaju prvih osam bitova postavljenih u 1111 1111 pa je takve adrese jednostavno klasificirati.
Na slici 6 prikazana je struktura IPv6 višeodredišne adrese:



Slika 6: Struktura IPv6 višeodredišne adrese

Razvidna je podijeljenost globalne jednoodredišne na sljedeće dijelove:

- Polje Z - zastavica koje se sastoji od 4 bita. Prema normi RFC 3513, zasad je definirana samo zastavica T (koja se nalazi na najnižem od 4 bita). Ukoliko je zastavica T postavljena u 0, to označava da je navedenu višeodredišnu adresu permanentno dodijelila organizacija IANA (eng. *Internet Assigned Numbers Authority*). Ukoliko je postavljena u 1, riječ je o privremenoj višeodredišnoj adresi.
- Doseg - polje koje označava doseg IPv6 mreže za koji je navedeni višeodredišni paket namijenjen. Polje je veličine 4 bita. Osim informacija dobivenih od višeodredišnog usmjerivačkog protokola, usmjerivači koriste ovo polje prilikom određivanja je li određeni paket potrebno dalje prosljeđivati. Najčešće vrijednosti ovog polja jesu 1 (doseg lokalnog mrežnog sučelja), 2 (doseg lokalne poveznice) te 5 (doseg lokalne administrativne domene). Kao primjer korištenja ovog polja može se iskoristiti adresa FF02::2, čiji je doseg lokalna poveznica pa takav paket IPv6 usmjerivači neće nikada proslijediti izvan lokalne poveznice.
- Identifikator grupe - vrijednost ovog polja određuje višeodredišnu grupu, i jedinstvena je unutar dosega adrese. Veličina ovog polja je 112 bitova. Permanentno dodijeljeni identifikatori grupa neovisni su o adresnom dosegu.

Za identifikaciju čvorova na lokalnom mrežnom sučelju ili lokalnoj poveznici definirane su sljedeće višeodredišne adrese:

- FF01::1 (svi čvorovi unutar dosega lokalnog mrežnog sučelja) i
- FF02::1 (svi čvorovi unutar dosega lokalne poveznice).

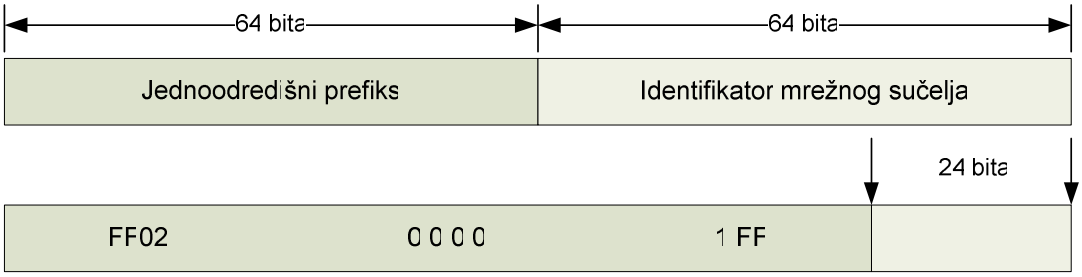
Za identifikaciju svih usmjerivača na lokalnom mrežnom sučelju, lokalnoj poveznici ili lokalnoj administrativnoj domeni definirane su sljedeće višeodredišne adrese:

- FF01::2 (svi usmjerivači unutar dosega lokalnog mrežnog sučelja),
- FF02::2 (svi usmjerivači unutar dosega lokalne poveznice) i
- FF05::2 (svi usmjerivači unutar dosega lokalne administrativne domene).

3.2.1. Višeodredišna adresa na zahtjev čvora (eng. *Solicited-Node Address*)

Ovaj je tip adrese definiran zbog jednostavnijeg upita mrežnih čvorova prilikom razlučivanja adresa (eng. *address resolution*). Kod IPv4 protokola, ARP (eng. *Address Resolution Protocol*) zahtjev za

razlučivanjem adrese šalje se na difuznu adresu MAC (eng. *Media Access Control*) razine, što utječe na sve čvorove mreže, čak i one koji ne podržavaju IPv4 protokol. IPv6, s druge strane, prilikom razlučivanja adresa koristi tzv. poruke za otkrivanje susjeda (eng. *Neighbor Solicitation Message*). Ova metoda, umjesto korištenja višeodredišne adrese s dosegom lokalne poveznice, kao odredišnu adresu takvih poruka koristi adrese na zahtjev čvora. One se sastoje od prefiksa FF02::1:FF00/104 i niža 24 bita IPv6 adrese koja se razlučuje (slika 7).



Slika 7: Struktura višeodredišne adrese na zahtjev čvora

Za prikaz postupka može se pretpostaviti slijedeće: Čvoru A je dodijeljena adresa lokalne poveznice FE80::2AA:FF:FE28:9C5A, pri čemu taj čvor dodatno osluškuje promet višeodredišne adrese na zahtjev čvora FF02::1:FF28:9C5A. Ukoliko čvor B, koji se nalazi na lokalnoj poveznici, mora razlučiti fizičku (MAC) adresu čvora A, poslat će poruku za otkrivanje susjeda na višeodredišnu adresu FF02::1:FF28:9C5A. Budući da čvor A osluškuje na toj adresi, obradit će dobivenu poruku za otkrivanje susjeda te čvoru B poslati jednoodredišnu poruku za oglašavanje susjeda (eng. *Neighbor Advertisement*).
Uzimajući u obzir učestalost zahtjeva za rezolucijom adrese, rezultat korištenja ovog mehanizma jest mnogo manja opterećenost mreže i pojedinih čvorova.

3.3. Adresiranje „najbližeg“ čvora (eng. *anycast*)

IPv6 „najbliža“ adresa dodjeljuje se višestrukim mrežnim sučeljima. Paketi koji su poslani na takvu adresu prosljeđuju se usmjerivačkom infrastrukturom do najbližeg mrežnog sučelja kojemu ja dotična „najbliža“ adresa dodijeljena, pri čemu je pojam „najbližeg“ određen usmjerivačkom metrikom. Trenutno se takve adrese koriste isključivo kao odredišne adrese, a dodijeljene su IPv6 usmjerivačima. „Najbliže“ adrese dodjeljuju se iz adresnog prostora jednoodredišnih adresa pa je njihov doseg određen dosegom odgovarajuće jednoodredišne adrese.
Svaki usmjerivač unutar određene podmreže mora imati „najbližu“ adresu, koja je predefinirana i određena prefiksom podmreže za dotično mrežno sučelje. „Najbliža“ adresa usmjerivača podmreže stvara se tako da se bitovi prefiksa mreže fiksiraju a ostali bitovi adrese postave u 0. Svim mrežnim sučeljima spojenim na dotičnu podmrežu dodjeljuju se takve adrese, koje se potom koriste u komunikaciji s jednim od usmjerivača neke udaljene podmreže.

3.4. Rekapitulacija IPv6 adresne arhitekture

3.4.1. IPv6 adrese računala

Uobičajen IPv4 mrežni čvor, koji posjeduje jedno mrežno sučelje, ima dodijeljenu jednu IPv4 adresu. S druge strane, IPv6 mrežni čvor koristi višestruke IPv6 adrese, čak i u slučaju da posjeduje jedno mrežno sučelje. Tipičnom IPv6 mrežnom čvoru dodijeljene su sljedeće jednoodredišne adrese:

- adresa lokalne poveznice za svako mrežno sučelje,
- jednoodredišna adresa za svako mrežno sučelje (može biti adresa lokalne administrativne domene ili jedna od globalnih jednoodredišnih adresa) i
- adresa povratne petlje (::1) za mrežno sučelje.

Upravo zbog činjenice da IPv6 čvor posjeduje veći broj IPv6 adresa, on može istovremeno primati pakete kako lokalnog tako i globalnog karaktera pa se takvi čvorovi često nazivaju višedomnim (eng. *multihomed*).

Osim navedenih jednoodredišnih adresa, svaki IPv6 mrežni čvor dodatno osluškuje mrežni promet na sljedećim višeodredišnim adresama:

- FF01::1 (adresa svih čvorova unutar dosega lokalnog mrežnog sučelja),
- FF02::1 (adresa svih čvorova unutar dosega lokalne poveznice),
- višeodredišna adresa na zahtjev čvora za svaku jednoodredišnu adresu svakog mrežnog sučelja i
- višeodredišna adresa svake grupe kojoj je čvor pristupio.

3.4.2. IPv6 adrese usmjerivača

Svakom IPv6 usmjerivaču dodijeljene su sljedeće jednoodredišne adrese:

- adresa lokalne poveznice za svako mrežno sučelje,
- jednoodredišna adresa za svako sučelje (može biti adresa lokalne administrativne domene ili jedna od globalnih jednoodredišnih adresa),
- „najbliža“ adresa usmjerivača podmreže,
- dodatne „najbliže“ adrese (opcionalno) i
- adresa povratne petlje (::1).

Dodatno, svaki IPv6 usmjerivač osluškuje mrežni promet i na sljedećim višeodredišnim adresama:

- FF01::1 (adresa svih čvorova unutar dosega lokalnog mrežnog sučelja),
- FF01::2 (adresa svih usmjerivača unutar dosega lokalnog mrežnog sučelja),
- FF02::1 (adresa svih čvorova unutar dosega lokalne poveznice),
- FF02::2 (adresa svih usmjerivača unutar dosega lokalne poveznice),
- FF05::2 (adresa svih usmjerivača unutar dosega lokalne administrativne domene),
- višeodredišna adresa na zahtjev čvora za svaku jednoodredišnu adresu svakog mrežnog sučelja i
- višeodredišna adresa svake grupe kojem je usmjerivač pristupio.

3.5. IPv6 i DNS

Norma RFC 1886 propisuje određene nadogradnje koje DNS (eng. *Domain Name System*) poslužitelji moraju implementirati za podržavanje IPv6 protokola. Nadogradnje se odnose na dva nova DNS elementa:

- „AAAA“ zapis - IPv6 adresa računala
- IP6.ARPA domena za reverzne upite

3.5.1. „AAAA zapis“

Nova vrsta DNS zapisa, pod nazivom „AAAA“ zapis, koristi se za razlučivanje IPv6 adrese računala za zadano simboličko ime. Naziv je nastao proširenjem naziva „A“, zapisa koji se koristi za razlučivanje IPv4 adrese, i to četiri puta budući da je IPv6 adresa 4 puta veća od IPv4 adrese. Primjer „AAAA“ zapisa:

```
računalo.domena.hr      IN    AAAA        FEC0:2AAA:FF:FE4F:2B1C
```

3.5.2. IP6.ARPA domena

Za reverzne IPv6 DNS zahtjeve koristi se IP6.ARPA domena. Reverzni zahtjevi koriste se za određivanje simboličkog imena računala na temelju njegove IP adrese. Prostor naziva za reverzne DNS upite ostvaruje se odvajanjem svakog heksadekadskog broja, koji postaje zasebna razina u hijerarhiji domena. Kao primjer može se uzeti adresa FEC0::2AA:FF:FE3F:2A1C, za koji bi odgovarajući zapis izgledao na sljedeći način:

```
C.1.A.2.F.3.E.F.F.F.0.0.A.A.2.0.0.0.
0.0.0.0.0.0.0.0.0.0.C.E.F.IP6.ARPA
```

4. Zaključak

U okviru ovog dokumenta razmotrene su osnovne značajke IPv6 protokola, uz usporedbu sa sličnim funkcionalnostima i konceptima koji trenutno postoje u IPv4 protokolu. Iako se IPv4 pokazao iznimno robusnim i skalabilnim, razvoj tehnologije i drugih protokola koji u vrijeme stvaranja IPv4 protokola (početak 1980-ih) nisu postojali njegovu je nadogradnju učinio nezaobilaznom.

Oblikovanje IPv6 zasnovano je na rješavanju nedostataka koji su tijekom godina primijećeni u radu IPv4 protokola. Unatoč tome, IPv6 donosi i određen broj novih funkcionalnosti. Jedna od njih je ugrađena podrška za osnovne elemente sigurnosne zaštite.

Na kraju, uzimajući u obzir sve prednosti opisanog IPv6 i nedostatke zastarjelog IPv4 protokola, lako je predvidjeti njihovu buduću zamjenu na mjestu najzastupljenijeg protokola globalne računalne mreže - Interneta.

5. Reference

[1] RFC 791, Internet Protocol, http://www.faqs.org/rfcs/rfc791.html, listopad 2006.
[2] RFC 4291, IP Version 6 Addressing Architecture, http://rfc.net/rfc4291.html, listopad 2006.
[3] RFC 2401, Security Architecture for the Internet Protocol, http://www.ietf.org/rfc/rfc2401.txt, listopad 2006.
[4] RFC 2402, IP Authentication Header, http://www.ietf.org/rfc/rfc2402.txt, listopad 2006.
[5] RFC 2406, IP Encapsulating Security Payload, http://www.ietf.org/rfc/rfc2406.txt, listopad 2006.
[6] RIPE NCC, IPv6 Home, http://www.ripe.net/rs/ipv6/index.html, listopad 2006.