CARNet srce

CAR6Net

Podprojekt Giga CARNet projekta,
zajedničkog projekta Hrvatske akademske i istraživačke mreže i
Sveučilišnog računskog centra Sveučilišta u Zagrebu

Testiranje IPv6 okruženja: Bind9 DNS poslužitelj

Izradio	Dinko Korunić
Autor(i):	Dinko Korunić
Datum:	13. travnja 2004.
Oznaka dokumenta	
Status dokumenta	javni

Testiranje IPv6 okruženja: Bind9 DNS poslužitelj

Dinko Korunić, kreator@srce.hr

Ključne riječi:

DNS, A6, AAAA, reverse, forward, resolving, nameserver

Sažetak:

U slijedećem dokumentu pokazat ćemo pripremu i konfiguriranje Bind9 DNS poslužitelja. To obuhvaća od same osnovne konfiguracije softvera, do pripadnim IPv6 DNS zona koje se poslužuju klijentima, ali i samu provjeru podataka odgovarajućim postupcima.

SADRŽAJ

1. UVOD

Bind9 je jedan od rijetkih DNS softvera koji se ističe po svojoj kvaliteti i složenosti. Od podrške za dinamički DNS, IPv6, DNS SEC ekstenzija, itd. Sam Bind9 paket iz Debian distribucije navodno u potpunosti podržava IPv6, stoga ćemo u daljnjem članku prikazati testove i njihove rezultate.

Ne ulazeći u osnove funkcioniranja DNS sustava ili zapise IPv6 adresa za koje se prepostavlja da je čitatelj već proučio, spomenimo kakve zahtjeve podržava prema dokumentaciji:

- za *forward* zahtjeve (iz poznatog imena se traži adresa) u vidu A6 i AAAA zapisa, pri čemu AAAA zapisi služe zbog kompatibilnosti sa starim načinom rada i većinom dosadašnjih *resolvera* i klijenata koji poznaju samo AAAA zapise,

- za *reverse* zahtjeve (iz poznate adrese se traži simboličko ime) su podržani novi *bitstring* zapisi koristeći ip6.arpa domenu, ali i stariji *nibble* zapisi koristeći ip6.int domenu.

U nastavku ćemo ukratko pokriti teoriju IPv6 adresa, a kasnije i pripadnu Bind9 konfiguraciju i alate za testiranje.

2. TEORIJSKA PODLOGA I METODOLOGIJA RADA

Budući da je DNS problematika daleko presložena za kratko opisivanje u ovom dokumentu, a i tematski izlazi van zadanih okvira, opisat ćemo samo ukratko oblik IPv6 A6 adresa radi boljeg razumijevanja kasnijih konfiguracija:

Općenito, IPv6 adrese su 128-bitni opisnici za sučelja ili grupe sučelja. Postoje osnovna 3 tipa adresa, o čemu možete detaljnije pročitati u RFC2374: Unicast (identifikator za samo jedno sučelje), Anycast (identifikator za set sučelja) i Multicast (također identifikator za set sučelja).

3	***13***	***8***	***24***	***16***	***64 bita***
FP	TLA ID	RES	NLA ID	SLA ID	ID sučelja
javna topologija				lokalna topologija	identifikator sučelja

FP je Format Prefix (001 za globalnu Unicast adresu), TLA ID je Top-Level Aggregation Identifier (formira ga prefiks TLD backbonea), RES je rezervirano polje (iako se trenutno ne koristi), NLA ID je Next-Level Aggregation Identifier (organizacije i sami klijenti ga koriste za dodatno razdjeljivanje vlastitog IP prostora), a SLA ID je Site-Level Aggregation Identifier (jedinstven za mrežu, na ethernet mrežama formira se od prva 3 bajta hardverske adrese što slijedi FFFE i zadnja 3 bajta hardverske adrese).

IPv6 adrese obično sadrže duge nizove nula, pa se dvostruka dvotočka (::) koristi da specificira najduži mogući niz znakova koji se može ubaciti i koristi se samo jednom u adresi.

AAAA zapis je tipični primjer zapisa analognog običnom IPv4 A zapisu, te specificira cijelu adresu u jednom zapisu. Kao što je već rečeno, dana služi za podršku starijim IPv6 aplikacijama:

```
$ORIGIN primjer.hr.
racunalo 3600 IN AAAA 3ffe:8050:201:1860:42::1
```

A6 zapis je nešto fleksibilniji od starog AAAA zapisa, ali i kompliciraniji. A6 zapis se može iskoristiti za formiranje cijelih nizova A6 zapisa, ali tako da se zapisuje samo dio IPv6 adrese. Iako je, naravno, moguće napisati i cjelokupnu adresu:

```
$ORIGIN primjer.hr.
racunalo 3600 IN A6 0 3ffe:8050:201:1860:42::1
```

A idući primjer pokazuje kako jedna organizacija može imati IPv6 prostor pružan od strane čak dva različita ISP-a koji kontroliraju vlastiti IPv6 prefiks, a A6 zapis će poslužiti da se specificira samo dio adresnog prostora koji kontrolira vlasnik domene. Jasno, kad se takav zapis bude pogledao preko DNS resolvera, resolver će dobiti dvija djelomična A6 zapisa i korištenjem dodatnih simboličkih imena će pronaći ostatak zapisa:

Organizacija će imati:

```
$ORIGIN primjer.hr.
racunalo 3600 IN A6 64 0:0:0:0:42::1 organizacija.primjer1.hr.
racunalo 3600 IN A6 64 0:0:0:0:42::1 organizacija.primjer2.hr.
```

ISP1 će imati:

```
$ORIGIN primjer1.hr.
organizacija 3600 IN A6 0 3ffe:8050:201:1860::
```

ISP2 će imati:

```
$ORIGIN primjer2.hr.
organizacija 3600 IN A6 0 1234:5678:90ab:fffa::
```

Idući primjer pokazuje A6 i A zapis koji specificira IPv6 i IPv4 adresu DNS poslužitelja, koji je preporučljivo pisati cijelom adresom (a ne parcijalno). Preporučuje se i izbjegavati IPv4-u-IPv6 pakiranje adresa u A6 zapisu (npr. ::ffff:192.168.42.1), već koristiti čisti A zapis kao što je u primjeru:

```
ORIGIN primjer.hr.
@ 14400 IN NS ns0
  14400 IN NS ns1
ns0 14400 IN A6 0 3ffe:8050:201:1860:42::1
ns1 14400 IN A 192.168.42.1
```

Pokažimo sada i povezivanje adrese sa imenom, odnosno *nibble* format zapisa za reverse zapise koji služi za stare IPv6 aplikacije. Jasno, komponente adrese su napisane od kraja prema početku (kao što se radi sa IPv4 adresama) i dodan je ip6.int sufiks. Na primjer, reverzna adresa za 3ffe:8050:201:1860:42::1 je:

```
$ORIGIN 0.6.8.1.1.0.2.0.0.5.0.8.e.f.f.3.ip6.int.
1.0.0.0.0.0.0.0.0.0.0.0.2.4.0.0 14400 IN PTR stroj.domena.hr.
```

Ista adresa (3ffe:8050:201:1860:42::1) se može zapisati koristeći i bitstring zapis, pri čemu zapis može početi i završiti na bilo kojem bitu (umjesto na grupama po 4 bita kao u gornjem primjeru). Koristi se ip6.arpa sufiks:

```
$ORIGIN \[x3ffe805002011860/64].ip6.arpa.
\[x0042000000000001/64] 14400 IN PTR stroj.domena.hr.
```

Kao što smo već rekli, kod IPv6 adresiranja jedno računalo može imati nekoliko adresa i to kod nekoliko različitih ISP-jeva. Kako krajnji dio IPv6 adrese (zadnjih 64 bita) ostaje isti, može se korištenjem DNAME-a smanjiti broj zona potrebnih za reverse mapiranje. U našem primjeru, računalo ima dva svoj adresni prostor pružan od strane dva ISP-a (organizacija1.hr i organizacija2.hr), pa ima i dvije IPv6 adrese:

```
$ORIGIN primjer.hr.
racunalo IN A6 64 ::1234:5678:1212:5675 cust1.example.net.
 IN A6 64 ::1234:5678:1212:5675 subnet5.example2.net.

$ORIGIN organizacija1.hr.
korisnik1 IN A6 48 0:0:0:dddd:: ipv6net.organizacija.hr.
ipv6net IN A6 0 aa:bb:cccc::

$ORIGIN organizacija2.hr.
korisnik2 IN A6 48 0:0:0:1:: ipv6net2.organizacija2.hr.
ipv6net2 IN A6 0 6666:5555:4::
```

Da bi reverzno povezivanje radilo, ISP organizacija1.hr treba samo:

```
$ORIGIN \[x00aa00bbcccc/48].ip6.arpa.
\[xdddd/16] IN DNAME ipv6-rev.primjer.hr.
```

Dok ISP organizacija2.hr treba:

```
$ORIGIN \[x666655550004/48].ip6.arpa.
\[x0001/16] IN DNAME ipv6-rev.primjer.hr.
```

Jasno, korisnik primjer.hr treba imati samo jednu zonu:

```
$ORIGIN ipv6-rev.primjer.hr.
\[x1234567812125675/64] IN PTR racunalo.primjer.hr.
```

No, vratimo se na sam Bind9 softver. Standardno, on sluša na svim IPv4 i IPv6 dostupnim adresama ako je izgrađen sa --enable-ipv6 postavkom pri inicijalnoj izgradnji. Alternativno, moguće je u named.conf konfiguracijskoj datoteci specificirati IPv6 adrese na kojima će Bind] slušati nadolazeći promet:

```
options
{
 ...
 listen-on-v6 { any; };
};
```

Da bi pružili usluge IPv6 adresiranja, postavit ćemo 3 zone:

- lokalnu reverznu zonu "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa",
- forward zonu "ip6",
- reverse zonu "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.a.a.4.0.2.e.8.6.b.0.1.0.0.2.ip6.arpa".

Prikažimo ih redom prvo u konfiguraciji u named.conf:

```
zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
.ip6.arpa"
```

```
{
 type master;
 notify no;
 file "/etc/bind/ip6-local.rev";
};



zone "ip6" {
  type master;
  file "/etc/bind/ip6.db";
};



zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.a.a.4.0.2.e.8.6.b.0.1.0.0.2
.ip6.arpa" {
  type master;
  notify no;
  file "/etc/bind/ip6.rev";
};
```

Pojednostavljena zona za 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa izgleda ovako (omogućiti će resolving ::1 u ip6-localhost):

```
$TTL 1D
@ SOA ip6. postmaster.ns.ip6 (
 1 604800 86400 2419200 604800 )
 NS ns.ip6.
1 PTR ip6-localhost.
```

Pojednostavljena zona za ip6 izgleda ovako:

```
$TTL 1D
@ SOA ns.ip6. postmaster.ns.ip6. (
 200404226 28800 7200 604800 86400 )
 NS ns
 NS ns2
 MX 5 mail
 AAAA 2001:b68:e204:aa11::2
 A6 0 2001:b68:e204:aa11::2
 A    161.53.2.207

ns AAAA 2001:b68:e204:aa11::4
    A6 0 2001:b68:e204:aa11::4
    A    161.53.2.208
zatocnica CNAME ns

ns2 AAAA 2001:b68:e204:aa11::3
    A6 0 2001:b68:e204:aa11::3
```

```
    A    161.53.2.209
kosjenka CNAME ns2

localhost AAAA ::1
          A6 0 ::1
          A    127.0.0.1
```

Naposljetku, reverzna zona za
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.a.a.4.0.2.e.8.6.b.0.1.0.0.2.ip6.arpa izgleda ovako:

```
$TTL 1D
@ SOA ip6. postmaster.ns.ip6 (
 200404226 28800 7200 604800 86400 )
 NS ns.ip6.
3 PTR ns.ip6.
4 PTR ns2.ip6.
```

3. PRIKAZ I TUMAČENJE REZULTATA

Prvo, provjerit ćemo da li Bind9 poslužitelj uopće sluša na IPv6 sučelju:

```
zatocnica:/etc/bind# grep listening /var/log/daemon.log
Apr 27 12:40:43 zatocnica named[7320]: listening on IPv6
interfaces, port 53
Apr 27 12:34:23 zatocnica named[7230]: listening on IPv4
interface lo, 127.0.0.1#53
Apr 27 12:34:23 zatocnica named[7230]: listening on IPv4
interface eth0, 161.53.2.208#53
Apr 27 12:34:23 zatocnica named[7230]: command channel
listening on 127.0.0.1#953
Apr 27 12:34:23 zatocnica named[7230]: command channel
listening on ::1#953
```

Zatim, provjerimo to isto korištenjem lsof programa listajući samo IPv6 domain listenere:

```
zatocnica:/etc/bind# lsof -i6:53
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
named   7318 bind   20u  IPv6 307511       UDP *:domain
named  7318 bind   21u  IPv6 307512       TCP *:domain
(LISTEN)
itd.
```

A sad ćemo korištenjem programa host (ili bind9-host, oba podržavaju IPv6 lookupove) provjeriti DNS zapise:

Provjerimo 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa zonu:

```
zatocnica:/etc/bind# host ::1
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.ip6.arpa domain name pointer ip6-localhost.

zatocnica:/etc/bind# host -t SOA
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
ip6.arpa
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
ip6.arpa SOA ip6.
postmaster.ns.ip6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.0.0.0.0.0.0.0.ip6.arpa. 1 604800 86400 2419200 604800
```

Eto i detalji ip6 domene:

```
zatocnica:/etc/bind# host -t SOA ip6
ip6 SOA ns.ip6. postmaster.ns.ip6. 200404226 28800 7200 604800
86400
```

```
zatocnica:/etc/bind# host -t a ns.ip6
ns.ip6 has address 161.53.2.208

zatocnica:/etc/bind# host -t aaaa ns.ip6
ns.ip6 has AAAA address 2001:b68:e204:aa11::4

zatocnica:/etc/bind# host -t a6 ns.ip6
ns.ip6 has v6 address 0 2001:b68:e204:aa11::4

zatocnica:/etc/bind# host zatocnica.ip6
zatocnica.ip6 is an alias for ns.ip6.
ns.ip6 has address 161.53.2.208

zatocnica:/etc/bind# host -t a6 zatocnica.ip6
zatocnica.ip6 is an alias for ns.ip6.
ns.ip6 has v6 address 0 2001:b68:e204:aa11::4

zatocnica:/etc/bind# host -t aaaa zatocnica.ip6
zatocnica.ip6 is an alias for ns.ip6.
ns.ip6 has AAAA address 2001:b68:e204:aa11::4

zatocnica:/etc/bind# host -t aaaa ip6
ip6 has AAAA address 2001:b68:e204:aa11::2
```

Preostaje nam pogledati podatke o reverznoj zoni

```
host -t ns
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.a.a.4.0.2.e.8.6.b.0.1.0.0.2.
ip6.arpa
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.a.a.4.0.2.e.8.6.b.0.1.0.0.2.
ip6.arpa name server ns.ip6.

host -t ptr
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.a.a.4.0.2.e.8.6.b.0.1.0.0.
2.ip6.arpa
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.a.a.4.0.2.e.8.6.b.0.1.0.0.
2.ip6.arpa domain name pointer ns.ip6.
```

Isprobali smo u gornjim primjerima kako IPv4 tako i IPv6 sučelje koristeći slijedeće postavke u resolv.conf:

```
search ip6 srce.hr
nameserver ::1
nameserver 161.53.2.208
```

Jasno, to smo i ručno provjerili:

```
zatocnica:/etc/bind# host -t ptr
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.a.a.4.0.2.e.8.6.b.0.1.0.0.
2.ip6.arpa ::1
```

```
Using domain server:
Name: ::1
Address: ::1#53
Aliases:
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.a.a.4.0.2.e.8.6.b.0.1.0.0.
2.ip6.arpa domain name pointer ns.ip6.
```

I time smo završili naše testiranje i provjeru IPv6 mogućnosti i kompatilnosti Bind9 DNS softvera.

4. PREPORUKE

Po našem izboru, Bind9 (http://www.isc.org/) predstavlja dobar i ugodan izbor za DNS softver. U testiranju se pokazao jednostavnim za korištenje i administiranje, te potpuno podržava sve nužne IPv6 funkcionalnosti. Nažalost, njegova povijest nije bez sigurnosnih propusta, pa se čitatelj upućuje na dodatne sigurnosne mjere prilikom implementacije DNS poslužitelja u vidu chroot okoline i otpuštanja nepotrebnih root privilegija.

Jasno, postoje i alternative ovom DNS poslužitelju. Jedna od zanimljivijih je definitivno djbdns (http://cr.yp.to/djbdns.html) koji spada u najsigurniji DNS softver koji postoji. Uz odlične performanse, softver standardno podržava IPv6 adrese kao oktetni zapis, s mogućnošću nadogradnje (http://www.fefe.de/dns/) na "ljudski" format koji je nešto lakši za održavanje.

5. ZAKLJUČAK

Ovime zaključujemo da je IPv6 podrška u Bind9 softveru potpuna. No, nameće se i zaključak da je nužno koristiti i A6 i AAAA adrese zbog standarda koji se promijenio i zbog toga što ne podržavaju svi klijenti nove A6 adrese. Uz te, kao i mnoge ostale probleme, direktan prijelaz na IPv6 adrese (A6 i AAAA) i zanemarivanje starih IPv4 adresa se nikako ne preporuča, zbog nepoznate situacije sa klijentima koji mogu, ali ne moraju razumjeti niti A6, niti AAAA zapise.

Više o cijeloj problematičnoj A6 i AAAA implementaciji iz pera DJBDNS autora je moguće vidjeti i na adresi http://cr.yp.to/djbdns/ipv6mess.html.

LITERATURA I BIBLIOGRAFIJA

- BIND 9 Administrator Reference Manual
- D. J. Bernstein: The IPv6 mess
- Bertrand Buclin: IPv6 DNS Setup
- David C. Lee: IPv6 DNS Examples

ipv6@carnet.hr

http://ipv6.carnet.hr/

Hrvatska akademska i istraživačka mreža - CARNet
Josipa Marohnića bb
10000 ZAGREB
01/6165616

Sveučilište u Zagrebu
Sveučilišni računski centar
Josipa Marohnića bb
10000 ZAGREB
01/6165555