LATVIJAS UNIVERSITĀTE

MAĢISTRA DARBS

RĪGA 2010

Latvijas Universitāte

Datorikas fakultāte

IPv6 praktiskas ieviešanas problēmu izpēte

Maģistra darbs

Autors: **Andris Segliņš**

Stud. apl. DatZ010078

Darba vadītājs: profesors Dr.sc.comp. Guntis Bārzdiņš

Rīga 2010

Anotācija

Maģistra darbā veikta teorētiska un praktiska izpēte par šībrīža reālajām IPv6 protokola izmantošanas iespējām pastāvošajā IPv4 Interneta vidē. Apskatītas iespējas izveidot apakštīklu balstītu tikai uz IPv6, no kura būtu pieejami IPv4 Interneta resursi un kurš būtu pieejams no IPv4 Interneta. Aplūkota praktiska uz IPv6 balstīta lokālā tīkla izveide ar reāli lietojamiem resursiem, piemēram, E-pasts, Tīkla lapas (WEB), failu apmaiņa, kā arī pieejamības nodrošināšana šiem resursiem no IPv4 Interneta vides. Apskatīts šobrīd pieejamo operētājsistēmu atbalstu IPv6 protokolam. Izpētīta šobrīd pieejamās programmatūras tādas kā Interneta pārlūki, e-pasta, failu apmaiņas, drošības un citas programmas, un aparatūras, SOHO tipa maršrutētāju un komutatoru atbalsts IPv6 protokolam un ar to saistītās problēmas, negācijas.

Abstract

Research of practical and theoretical implementation of IPv6 protocol in real life IPv4 Internet environment. Considered possibility of creating an IPv6 only network island within IPv4 network, with web resources accessible from IPv4 towards IPv6. Practical implementation of IPv6 only network with working resources such as e-mail, web pages and file sharing. Providing access to all of these resources from IPv4 only network. Survey of IPv6 support in contemporary operating systems. Theoretical research of IPv6 support in popular software such as web browsers, e-mail, file sharing, security and other, and SOHO class hardware such as routers and switches. Problem identification relevant to usage of these products.

Autoreferāts

Maģistra darba praktiskās daļas ietvaros autors ir iepazinies ar Cisco Systems maršrutētāja konfigurāciju NAT-PT protokola ieviešanai. Izmēģinot vairākus konfigurācijas parametrus un veidus, ir izveidots reālas dzīves piemērs IPv6 translēšanai uz IPv4 un pretējā virzienā. Konfigurācijas darboties spēja ir notestēta laboratorijas apstākļos un implementēta reālas dzīves slēgumā, padarot iespējamu Interneta resursu piekļuvi no izveidotā slēguma.

Izveidotajā slēgumā tika izvietotas Web, FTP un E-pasta serveris – testbed.mc.net.lv. E-pasta darbības pārbaudei tika izveidots testa e-pasta konts andriss@testbed.mc.net.lv, no kura tiek sūtītas automātiskas atbildes vēstules. Izejot no iespējām, autors ir veicis divu operētājsistēmu darboties spēju izveidotajā slēgumā. Testa nolūkos ir pārbaudīta Microsoft Windows 7 operētājsistēmas un Linux distribūcijas Ubuntu 10.10 darbība tikai IPv6 tīkla vidē. Autors ir veicis savus tiešos darba pienākumus vienas darba nedēļas laikā, ar īsiem pārtraukumiem, darbojoties tikai caur tikai IPv6 tīklu un NAT-PT vārteju. Darbojoties caur izveidoto slēgumu autors ir veicis ikdienā lietotās programmatūras atbalstu un spēju darboties tikai IPv6 tīkla vidē. Autors ir veicis īslaicīgu testu pieslēdzot savu darba staciju tikai IPv6 Interneta videi, bez pieejas IPv4 tīkla resursiem, tādējādi novērtējot lietotāja pirmo pieredzi IPv6 tīklā.

Darbā apskatīta situācija Latvijas Interneta vidē no IPv6 gatavības un ieviešanas ātrumu viedokļa. Autors ir konsultējies ar IT organizāciju tehniskajiem darbiniekiem ar mērķi saprast IPv6 ieviešanas stadijas reālo situāciju un nākotnes plānus, kā arī ar atbildīgo valsts institūciju speciālistiem ar mērķi saprast valsts nostāju šai jautājumā.

Izmantojot Internetā pieejamo informāciju, autors ir veicis populārāko un nepieciešamāko aplikāciju un aparatūras atbalstu IPv6 protokolam. Autors savā darbā apskata IPv4 un IPv6 protokolu izplatību un tendences globālajā tīmeklī. Ir apskatīti reģionālo un globālo Interneta resursu izdalītāju ziņojumi par IPv4 brīvo adrešu pieejamību, par prognozēm un paredzamajiem darbības plāniem.

Izstrādātais maģistra darbs kopumā sniedz ieskatu iespējās pāriet uz IPv6 protokola vidi jau šodien, turpinot lietot IPv4 Interneta vides resursus, un raksturo problēmas, kas saistītas ar šo pāreju.

Satura rādītājs

Apzīmējumi

NAT-PT – Network Address Translation, Protocol Translation. Protokols, kas ļauj pārtranslēt IPv6 pieprasījumus uz IPv4 pieprasījumiem un otrādi.

IPv6 – Internet Protocol version 6, jaunākās paaudzes Interneta protokols versija 6.

IPv4 – Internet Protocol version 4, šobrīd izmantotais Interneta protokols, versija 4.

ALG – Application Layer Gateway, aplikāciju līmeņa vārteja. Funkcija, kas veic konkrētu IPv6 protokolu pieprasījumu un atbilžu pārtranslēšanu uz IPv4 un otrādi.

Ievads

Interneta vide, tāda kāda tā pastāv šobrīd, tika izgudrota un sākta veidot jau 1970-tajos gados. Tas nebija laks, kam būtu pielīdzināma mūsdienu situācija, ka gandrīz katrā mājsaimniecībā un katrai darba vietai būtu pieejams personālais dators, kam nepieciešams lietot resursus Interneta vidē. IPv4 protokols paredzēja maksimāli teorētisko iespējamo IP adrešu apgabalu ar 2^{32} = 4’294’967’296 IP adresēm, kas ir gana daudz un tika uzskatīts par pietiekamu. Šobrīd 2009. gada ziņojumā, Eiropas IP adrešu reģistrs ir paziņojis, ka brīvās IP adreses visticamāk beigsies starp 2011. un 2012. gadu. Precīzu datumu, objektīvu iemeslu dēļ, nav iespējams noteikt, bet vēstījums ir skaidrs – nepieciešamība lietot cita veida adresāciju ir neizbēgama. Jau kopš 2002. gada eksistē IPv6 protokols, kas dod iespēju izmantot IP apgabalu, kas ir līdzvērtīgs 2^{128} = 340’282’366’920’938’463’463’374’607’431’768’211’456 jeb aptuveni $3{,}4 * 10^{38}$. Praktiskā IPv6 ieviešana notiek ļoti gausi un pieejamais Interneta resursu apjoms IPv6 tīklā, salīdzinot ar IPv4 tīklā esošajiem resursiem, ir minimāls. Tāpat, lai arī pēc Eiropas Savienības rezolūcijas, kas pieņemta 2008.gadā, Interneta pakalpojumu sniedzēji tiek iedrošināti un mudināti sniegt saviem klientiem IPv6 tīkla pakalpojumus, liela daļa pakalpojumu sniedzēju to vēl nav gatavi darīt, tāpat lielākā daļa klientu nav šajā pakalpojumā ieinteresēti. Uz šo brīdi Latvijā nepastāv neviens likums, vai normatīvais akts, kas noteiktu IPv6 obligātu ieviešanu vai šāda pakalpojuma piedāvāšanu pēc klienta pieprasījuma. Pēc autora domām, ir tikai laika jautājums, kad šie mudinājumi kļūs par obligātu noteikumu, ko apstiprina darba ietvaros īstenotās sarunas ar atbilstošo institūciju darbiniekiem. ko arī apstiprina neformāla saruna ar atbilstošo institūciju darbiniekiem.

Viens no darba uzdevumiem bija pierādīt, ka, ja izdotos atrisināt šīs divas augstāk minētās problēmas un padarīt iespējamu abu tīklu resursu piekļuvi uz pārejas laiku, iespējams IPv6 ieviešanas tempi palielinātos. Darba gaitā tiek izskatīta iespēja izveidot lokālo apakštīklu, kas darbojas uz tīra IPv6 tīkla un, izmantojot specializētu maršrutētāju, no šāda apakštīkla būtu pieejami IPv4 tīkla resursi, kā arī no IPv4 tīkla, būtu pieejami apakštīklā izvietotie resursi. Veiksmīgas implementācijas gadījumā autors pieļauj domu, ka būtu iespējams ieviest šādus apakštīklus klientiem, kas vēlas izmantot IPv6 tīkla iespējas. Ikdienas darbā autors, nodarbojoties

ar viena no lielākajiem Latvijas Interneta pakalpojumu sniedzēja tīklu uzturēšanu, ir praktiski pārliecinājies par iespējām un ieguvumiem šāda slēguma esamībai.

Šobrīd ir pieejami vairāki IPv6 tunelēšanas pakalpojumi, sākot no publiski pieejamiem tuneļu servisa sniedzējiem līdz operētājsistēmās iebūvētiem, jau standartizētiem tuneļu veidiem. Visas šīs sistēmas sniedz iespēju lietot IPv6 starp darba stacijām un apakštīkliem, izmantojot IPv4 tīklu kā datu nesēju, bet nav iespējama tieša pieeja IPv4 tīkla resursiem. Izpētes rezultātā autors uzgāja protokolu NAT-PT, kas nodrošina translāciju starp IPv6 un IPv4 tīkliem lokālā tīkla infrastruktūrā. Izmantojot NAT-PT protokolu uz Interneta vārtejas lokālajam tīklam ar tīru IPv6 tīklu, iespējama pieprasījumu un atbilžu translēšana, līdz ar to iespējama IPv4 tīkla resursu pieejamība.

Darba pirmajā daļā autors veic laboratorijas slēgumus, testējot pieejamo protokolu, lai pārliecinātos par tā teorētisko dzīvotspēju. Tāpat nepieciešams pārliecināties par vairāku priekšnoteikumu izpildīšanos kontrolētā slēgumā laboratorijas apstākļos, pirms būtu pamatoti mēģinājumi ieviest šādu slēgumu reālās dzīves situācijā. Darba otrajā daļā autors veic populārāko tīkla protokolu un aplikāciju darboties spēju, izmantojot izveidoto slēgumu, kur viena darba stacija atrodas IPv6 tīklā un tiek mēģināts piekļūt resursiem IPv4 tīklā. Tāpat tiek veikti testi par iespējām piekļūt IPv6 tīklā izvietotam serverim ar pieejami vienkāršotu Interneta vietni, e-pasta un FTP serveri. Testi tiek veikti gan darboties spējas, gan veiktspējas šķērsgriezumā.

Esošās situācijas novērtējums

Pēc pēdējiem datiem – 25.11.2010, kuri pieejami Interneta vietnē [12] Latvijas teritorijā reģistrētiem Interneta pakalpojumu sniedzējiem vai organizācijām, ir izdalīti 13 IPv6 prefiksi, tai skaitā Latvijas Banka un Matemātikas un Informātikas institūts, kuri nenodarbojas ar aktīvu Interneta pakalpojumu sniegšanu. No Interneta pakalpojumu sniedzējiem, kas ir izveidojuši Latvijas Interneta apmaiņas punktu LIX [13], IPv6 adrešu apgabalus ir saņēmuši visi, bet klientiem IPv6 pakalpojumus spēj piedāvāt tikai SIA Latnet Serviss, un arī tikai centrālajos pieslēguma punktos, bet ne reģionos. Konsultācijās ar konkrēto organizāciju atbildīgajiem speciālistiem tika noskaidrots, ka Sia Lattelecom nav veicis nekādus pasākumus IPv6 ieviešanas virzienā un Telia Latvija lieto IPv6 tīkla adreses sava ofisa ietvaros, bet savienojums ar globālo IPv6 tīklu ir caur tuneli uz mātes uzņēmumu. Aptaujājot lielākos Interneta pakalpojumu

sniedzējus, atklājās, ka tikai viens no tiem aktīvi ir ieviesis IPv6 un to piedāvā klientiem, papildus ir jau eksistējoši divi klienti, kas lieto šo pakalpojumu. Šis Interneta pakalpojumu sniedzējs ir Baltcom, toties Sia Latnet Serviss vienīgais IPv6 klients ir autora darba vieta, Sia Monitoringa centrs, kura testa režīmā ieviesa šo nākošās paaudzes IP protokolu.

No nekomerciālām organizācijām darba gaitā tika noskaidrots, ka Latvijas Matemātikas un Informātikas Universitātes ēkā ir pieejams IPv6 tīkls un arīdzan Latvijas pirmā līmeņa domēna uzturētājs NIC [14] ir ieviesis IPv6 savā tīklā un uztur Interneta vārdu serveri (NS zone server) IPv6 tīklā.

No augstāk minētā var spriest, ka šobrīd Latvijā iespējas pievienoties IPv6 lietotāju pulkam ir ļoti ierobežotas, tāpēc ir nepieciešams meklēt citus veidus, kā lietot šo pakalpojumu. Reālākais risinājums, kāds šobrīd ir pieejams Latvijas Interneta lietotājiem, ir IPv6 adrešu apgabala iegūšana no sava Interneta Pakalpojumu sniedzēja, jo vairums šādus apgabalus ir pieprasījuši un saņēmuši, un veicot IPv6 ieviešanu savā lokālajā tīklā, lieto globālos resursus, izmantojot kaut kāda veida tuneli caur IPv4 Internetu uz IPv6 tīklu.

Uz šo brīdi Latvijā nepastāv neviens likums vai normatīvais akts, kas regulētu IPv6 ieviešanas tempus vai Interneta pakalpojumu sniedzēju pienākumu sniegt šādu pakalpojumu. Pēc neoficiāliem datiem no nu jau likvidētā īpašo uzdevumu ministrijas elektroniskās pārvaldes lietu sekretariāta IT pārvaldes vadītāja, Latvija plāno piedalīties kopējā IPv6 ieviešanas plānu izstrādē ar Vācijas atbildīgajām pārvaldes iestādēm. Āzijas reģions ir norādījis uz faktu, ka būtu gatavs pāriet uz IPv6 līdz 2012. gada beigām, diemžēl Latvijas prognozes nav tik cerīgas.

Darbā apskatīto problēmu apkopojums

IPv6 adrešu apgabala pieejamība ir viens no svarīgākajiem nosacījumiem šī protokola lietošanā, bet, kā jau redzams iepriekšējā apakšnodaļā, šāda apgabala esamība nenozīmē automātisku šī protokola lietošanu. Nākamais solis ir IPv6 protokola atbalstošu tīkla iekārtu pieejamība un lietotājiem pats galvenais – darba staciju savietojamība ar šo protokolu. Darba izstrādes gaitā apskatīti visi soļi, sākot no tīkla iekārtu konfigurēšanas un IPv6 slēguma izveides, līdz konkrētu aplikāciju, rīku un Interneta vidē pieejamu resursu sasniedzamības no IPv6 tīklā esošas darba stacijas. Viena no problēmām, kas tiek risināta, ir tikai IPv6 apgabala darboties spēja IPv4 tīkla iekšienē, kā arī sasniedzamības gan no IPv6 uz IPv4, gan no IPv4 uz IPv6 tīklā

izvietotiem resursiem. Darba rezultātā autors ir izveidojis darbojošos tīkla slēgumu, kura ietvaros ir pieejams tikai IPv6 protokols un no kura ar dažādu tehnoloģiju palīdzību iespējams sasniegt gan IPv4 tīklā esošus resursus, gan IPv6 Internets. Tāpat autors ir apskatījis populārākās tīkla aplikācijas un to saderību vai gatavību darboties IPv6 tīklā. Autora daba pamatā tiek lietotas salīdzinoši dārgas, Interneta pakalpojumu sniedzēju klases tīkla iekārtas, lai pārliecinātos par mazākas klases iekārtu iespējām IPv6 protokola ieviešanā ir veikts teorētisks pētījums par tā saucamās SOHO klases iekārtu atbalstu IPv6 protokolam.

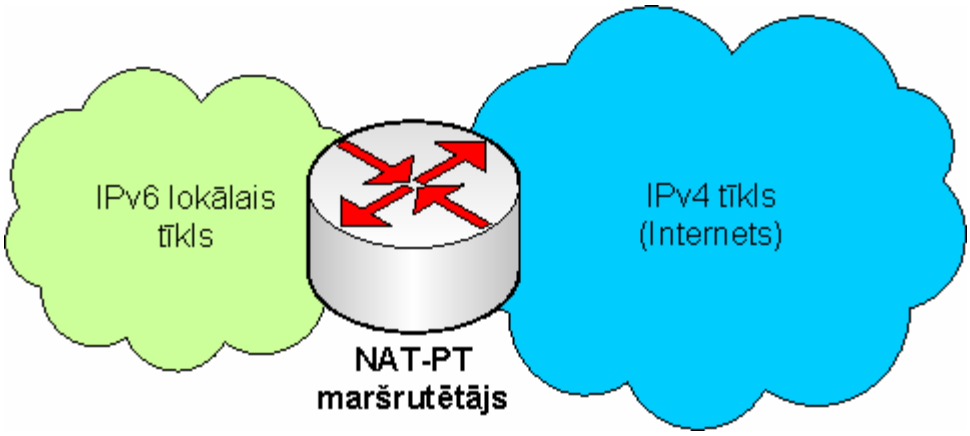
1 AUTONOMS IPV6 APGABALS IPV4 TĪKLĀ.

Mērķis: Izveidot uz IPv6 balstīta lokālā tīkla infrastruktūru, kas būtu sasniedzama no IPv4 Interneta vides un kurai būtu pieejami IPv4 Interneta resursi.

Risinājums: Izmantot NAT funkciju, kas veic IP protokola datu pakešu translēšanu no IPv4 uz IPv6 un otrādi NAT-PT (RFC2766).

Teorētiskais pamatojums: IPv4 adrešu apgabals ir galīgs un teorētiski pieejamo IPv4 adrešu skaits ir ierobežots ar lielāko iespējamo skaitli, kas pierakstāms izmantojot 32 bitus. Kas dod rezultāts 2^{32} = 4’294’967’296 IPv4 adreses, no kurām daļa ir rezervētas īpašiem tīkla resursiem, vai privātai lietošanai, tādējādi vēl vairāk samazinot kopējo publiski lietojamo IP adrešu skaitu [1]. IPv6 adrešu apgabals izmanto 128 bitus, kas jau ir tieši 4 reizes vairāk teorētiski pieejamo IP adrešu skaits [2]. Teorētiski ir iespējams „paslēpt” visu IPv4 adrešu apgabalu zem viena IPv6 apakštīkla, kura tīkla maska būtu /96, tādējādi izveidojot katrai IPv4 adresei atbilstošu IPv6 adresi.

Praktisks piemērs: Par pamatu tīkla adresācijas translēšanai tiek ņemts Cisco Systems maršrutētājs c2821, izmantojot programmnodrošinājumu C2800NM-ADVENTERPRISEK9-M Version 12.4(25d) un ražotājā interneta vietnē pieejamais konfigurācijas apraksts [3]. Slēguma shēma redzama attēlā 1.1.



1.1. att. **Vispārīga slēguma shēma**

NAT-PT protokols paredz, ka katrai IPv4 adresei tiks izveidota IPv6 adrese ar noteiktu prefiksu izmērā /96 un 32 bitu daļu, kas burtiski attēlo IPv4 adresi heksadecimālajā numerācijā. Tādējādi jebkura iekārta, kas atrodas IPv6 tīklā, var vērsties pie noteiktas IPv6 adreses, tādējādi zinot, ka šo adresi NAT-PT vārteja pārtranslēs šo IPv6 tīkla paketi uz IPv4 tīkla paketi ar noteikto IPv4 mērķadresi. Tīkla pakešu pārtranslēšana no IPv6 uz IPv4 un pretējā virzienā tiek veikta pateicoties ALG (*aplication level gateway*) funkcijai. Neizmantojot šo funkciju būtu iespējama tikai ļoti vienkāršotu TCP savienojumu translēšana, jo sarežģītākām IPv4 tīkla paketēm un protokoliem ir īpašas iezīmes, kuras nav iespējams bez papildus inteliģences pārnest uz IPv6 tīkla paketi.

1.1 Praktiska darba vides sagatavošana.

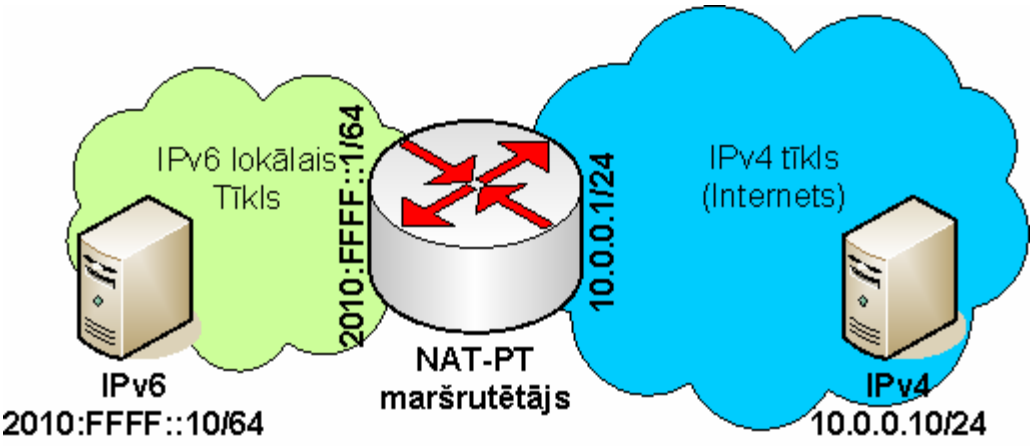
Tiecoties uz mērķi iegūt tīru IPv6 iekšējo tīklu, no kura būtu sasniedzami IPv4 tīkla resursi un kurā būtu resursi, kas ir sasniedzami no IPv4 tīkla, tiek veidoti vairāki dažādi konfigurāciju slēgumi, pārbaudot un testējot konkrētu funkcionalitāti:

1. Statiska, konkrētu IPv6 un IPv4 adrešu translācija;
2. Dinamiska IPv6 -> IPv4 adrešu translēšana neizmantojot DNS-ALG;
3. dinamiska IPv6 -> IPv4 adrešu translēšana izmantojot DNS-ALG;
4. galējais risinājums, visu gadījumu objektīvs apvienojums.

Lai pilnīgāk izprastu NAT-PT protokola darbību un saprastu tā iespējas, turpmāk darbā apskatīts katrs gadījums atsevišķi, sākot no relatīvi vienkāršākā līdz sarežģītākajam.

1.1.1. Statiska, konkrētu IPv6 un IPv4 adrešu translācija.

Šajā piemērā tiek veidots slēgums, kur definē konkrētu iekārtu IPv6 un IPv4 tīklā, starp kurām tiek veidota statiska adrešu translācija. Tādējādi tiek izveidots slēgums, kur visa datu plūsma starp šīm divām iekārtām tiek pārtranslēta un padota attiecīgajā IP protokola versijā, izmainot IP paketes galveni. Slēguma shēma redzama attēlā 1.2.



1.2. att. **Statiska IP translēšana**

Attēlā redzams, ka viena identificēta tīkla iekārta katrā no tīkliem, attiecīgi tīkla iekārta ar IPv6 adresi 2010:FFFF::10/64 un iekārta ar adresi 10.0.0.10/24. Mērķis ir panākt savienojumu izveidošanos no vienas iekārtas uz otru un pretējā virzienā. Šim nolūkam tiek veidota konfigurācija NAT-PT maršrutētājā. Konkrētajā slēgumā maršrutētājam ir divi tīkla interfeisi, no kuriem viens GigabitEthernet0/0 ir pievienots IPv4 tīklam un otrs GigabitEthernet0/1 attiecīgi IPv6 tīklam. Uz katra no interfeisiem tiek nokonfigurētas 2. attēlā redzamās adreses, papildus pievienojot komandu „*ipv6 nat*" tādējādi ieslēdzot NAT-PT funkcionalitāti. Rezultātā tīkla interfeisu konfigurācija ir sekojoša:

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 nat
end

interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:FFFF::1/64
```

```
 ipv6 nat
end
```

Ar šo konfigurāciju ir izveidota pamata tīkla konfigurācija, kuru iespējams pārbaudīt veicot ping pieprasījumu no katras tīkla iekārtas virzienā uz NAT-PT maršrutētāju.

```
Ipv4#ping ip 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

ipv6#ping ipv6 2010:ffff::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:FFFF::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Lai no IPv6 tīkla iekārtas sasniegtu IPv4 tīkla iekārtu nepieciešams to norādīt kā mērķi ping pieprasījumam vai citam tīkla IP protokolam, bet šobrīd tas nav iespējams, jo IPv6 iekārtai nav nokonfigurēts IPv4 protokola interfeiss, attiecīgi pieprasījumu, izmantojot IPv4 tīkla interfeisu kā mērķi, šī iekārta nesaprot:

```
ipv6#ping 10.0.0.1
% Unrecognized host or address, or protocol not running.
```

Tāpēc, nepieciešams nokonfigurēt konkrētu IPv6 adresi, uz kuru veicot pieprasījumus tie tiktu pārtranslēti uz IPv4 tīkla konkrēto adresi. Lai maršrutētājs NAT-PT veiktu jebkādas translēšanas darbības starp dažādajām IP protokolu versijām, nepieciešams definēt prefiksu, kurš viennozīmīgi norādītu, ka pieprasījumi uz šādu IPv6 adresi ir paredzēti pārtranslēšanai uz IPv4 protokolu. Konfigurācijas rindiņa

```
ipv6 nat prefix 2010::/96
```

norāda maršrutētājam, ka visi pieprasījumi uz adresēm 2010::/96 tiks apstrādāti kā potenciāli pārtranslējami. Maršrutētājā NAT-PT, konfigurācijas failā ierakstam rindiņu:

```
Ipv6 nat v4v6 source 10.0.0.10 2010::10
```

Attiecīgi ar to „pasakot" maršrutētājam, ka visi pieprasījumi, kas nākuši no IPv6 tīkla un adresēti IP adresei 2010::10 ir jāpārtranslē uz IPv4 tīkla adresi 10.0.0.10, kā arī jāveic attiecīgās darbības pretējā virzienā. Šobrīd visi pieprasījumi no IPv6 tīkla virzienā uz IP 2010::10 tiks pārtranslēti uz mērķa adresi, bet, lai maršrutētājs spētu pārtranslēt pieprasījumus, ir nepieciešams norādīt uz kādu izejas adresi pārtranslēt pieprasījumu, jo IP galvenē ir gan izejas, gan mērķa adreses. Konkrētajā gadījumā nepieciešams nokonfigurēt uz kādu IPv4 adresi tiks pārtranslēti pieprasījumi, kas nākuši no tīkla iekārtas ar adresi 2010:FFFF::10. Lai to panāktu nepieciešams papildināt konfigurācijas failu ar rindiņu:

```
ipv6 nat v6v4 source 2010:FFFF::10 192.168.0.10
```

norādām, ka visi pieprasījumi, kas nākuši no adreses 2010:ffff::10 ir jāpārtranslē uz IP 192.168.0.10 tāpat rīkojoties pretējā gadījumā. Ar šo statiska konfigurācija starp divām tīkla iekārtām ir pabeigta, lai pārliecinātos par konfigurācijas esamību varam veikt vairākas pārbaudes. Sākotnēji pārliecinoties, ka NAT-PT maršrutētājs ir sapratis ievadītās komandas un gatavs veikt translāciju nepieciešamības gadījumā:

```
NAT-PT#show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      10.0.0.10                2010::10
```

```
---   192.168.0.10            2010:FFFF::10
      ---                     ---
```

Komandas izvadā ir redzams, ka ir izveidoti ieraksti translēšanas tabulā, kas apraksta nokonfigurētās rindiņas, šobrīd nav redzamas nekādi aktīvi translācijas ieraksti, ko var spriest pēc tā, ka nav viena pāra gan IPv4 izejas, gan mērķa adreses un atbilstošās IPv6 adreses. Nākamā pārbaude ir reāli mēģinot sasniegt IPv4 tīkla iekārtu no IPv6 tīkla iekārtas, kā mērķa adresi izmantojot nokonfigurēto IPv6 adresi:

```
ipv6#ping 2010::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Ping rezultāts uzrāda pozitīvu atbildi, par translācijas notikuma esamību iespējams pārliecināties uz NAT-PT maršrutētāja:

```
NAT-PT#show ipv6 nat translations
Prot  IPv4 source             IPv6 source
      IPv4 destination        IPv6 destination
---   ---                     ---
      10.0.0.10               2010::10
---   192.168.0.10            2010:FFFF::10
      10.0.0.10               2010::10
---   192.168.0.10            2010:FFFF::10
      ---                     ---
```

Redzams, ka papildus jau bijušajām rindiņām ir redzams viens aktīvs translācijas notikums, jo ir ieraksts ar pilnu pāri – gan izejas, gan mērķa IP adresēm. Papildus ieraksti log failā norāda uz translētiem pieprasījumiem:

```
NAT-PT#
*May  6 14:55:45.986: IPv6 NAT: icmp src (2010:FFFF::10) -> (192.168.0.10), dst (2010::10) -> (10.0.0.10)
*May  6 14:55:45.990: IPv6 NAT: icmp src (10.0.0.10) -> (2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
*May  6 14:55:45.990: IPv6 NAT: icmp src (2010:FFFF::10) -> (192.168.0.10), dst (2010::10) -> (10.0.0.10)
*May  6 14:55:45.990: IPv6 NAT: icmp src (10.0.0.10) -> (2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
*May  6 14:55:45.994: IPv6 NAT: icmp src (2010:FFFF::10) -> (192.168.0.10), dst (2010::10) -> (10.0.0.10)
*May  6 14:55:45.994: IPv6 NAT: icmp src (10.0.0.10) -> (2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
*May  6 14:55:45.995: IPv6 NAT: icmp src (2010:FFFF::10) -> (192.168.0.10), dst (2010::10) -> (10.0.0.10)
*May  6 14:55:45.995: IPv6 NAT: icmp src (10.0.0.10) -> (2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
*May  6 14:55:45.997: IPv6 NAT: icmp src (2010:FFFF::10) -> (192.168.0.10), dst (2010::10) -> (10.0.0.10)
*May  6 14:55:45.998: IPv6 NAT: icmp src (10.0.0.10) -> (2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
```

Lai pārliecinātos par abpusēju protokola darbību iespējams veikt līdzīgu testu pretējā virzienā:

```
Ipv4#ping 192.168.0.10
Type escape sequence to abort.
```

```
    Sending 5, 100-byte ICMP Echos to 192.168.0.10, timeout is 2
seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max =
1/2/8 ms
```

Novērojams pozitīvs rezultāts, tāpat savienojumu aprakstošie ieraksti NAT-PT log failā, savukārt bez izmaiņām, translācijas tabulā, jo jau bija eksistējošs ieraksts, kas atbilda nepieciešamai translācijai:

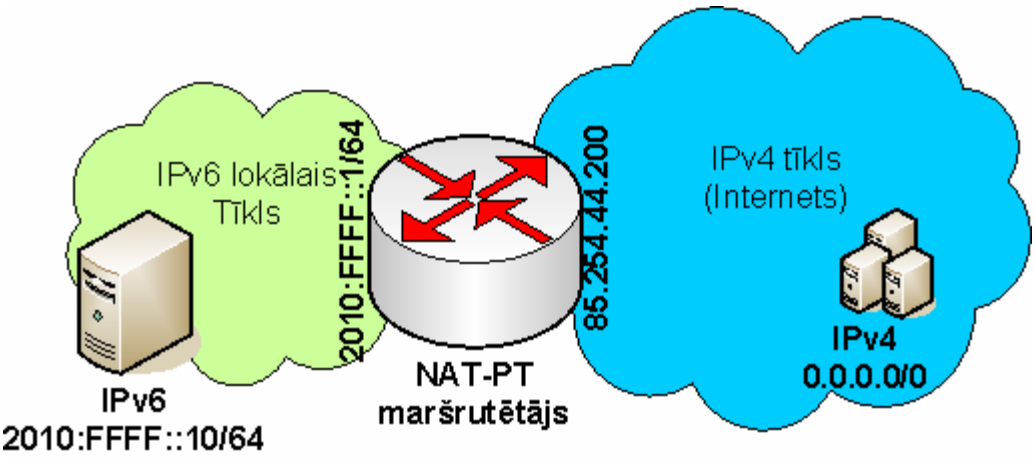
```
    *May   6 15:30:03.911: IPv6 NAT: icmp src (10.0.0.10) ->
(2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
    *May  6 15:30:03.911: IPv6 NAT: icmp src (2010:FFFF::10) ->
(192.168.0.10), dst (2010::10) -> (10.0.0.10)
    *May   6 15:30:04.915: IPv6 NAT: icmp src (10.0.0.10) ->
(2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
    *May  6 15:30:04.915: IPv6 NAT: icmp src (2010:FFFF::10) ->
(192.168.0.10), dst (2010::10) -> (10.0.0.10)
    *May   6 15:30:05.915: IPv6 NAT: icmp src (10.0.0.10) ->
(2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
    *May  6 15:30:05.919: IPv6 NAT: icmp src (2010:FFFF::10) ->
(192.168.0.10), dst (2010::10) -> (10.0.0.10)
    *May   6 15:30:06.919: IPv6 NAT: icmp src (10.0.0.10) ->
(2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
    *May  6 15:30:06.919: IPv6 NAT: icmp src (2010:FFFF::10) ->
(192.168.0.10), dst (2010::10) -> (10.0.0.10)
    *May   6 15:30:06.921: IPv6 NAT: icmp src (10.0.0.10) ->
(2010::10), dst (192.168.0.10) -> (2010:FFFF::10)
    *May  6 15:30:06.921: IPv6 NAT: icmp src (2010:FFFF::10) ->
(192.168.0.10), dst (2010::10) -> (10.0.0.10)
    NAT-PT#show ipv6 nat translations
```

```
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      10.0.0.10                2010::10
---   192.168.0.10             2010:FFFF::10
      10.0.0.10                2010::10
---   192.168.0.10             2010:FFFF::10
      ---                      ---
```

Ar šo konfigurācija un darbības pārbaude statiskai divu iekārtu translēšanai ir pabeigta. Pilns konfigurācijas fails pievienots 1. Pielikumā.

1.1.2. Dinamiska IPv6 -> IPv4 adrešu translēšana neizmantojot DNS-ALG

Statiska iekārtu definēšana un translācijas likumu aprakstīšana ir iespējama, bet diemžēl nav praktiska, jo aprakstīti visu IPv4 segmentu ir praktiski neefektīvi un nelietderīgi. Turpretim konfigurācija, kura dinamiski piekārtotu visas IPv4 adreses pie attiecīgajām IPv6 adresēm, būtu daudz parocīgāka. Slēguma shēma redzama attēlā 1.3.



1.3. att. **Dinamiska IPv6 translēšana bez ALG**

Šī slēguma mērķis ir aprakstīt likumu, pēc kura jebkura IPv4 tīkla iekārta būtu sasniedzama no IPv6 tīkla, izmantojot konkrētu mērķa adresi. Lai sagatavotu šo konfigurāciju, tika izmantota jau iepriekš nokonfigurēta IPv6 tīkla daļa, bet pārkonfigurēta IPv4 tīkla sadaļa, padarot tai pieejamu Interneta vidi, kā arī padarot to pieejamu no tās. Attiecīgi konfigurācija tīkla interfeisiem ir sekojoša:

```
interface GigabitEthernet0/0
 ip address 85.254.44.200 255.255.255.0
 duplex auto
 speed auto
 ipv6 nat
end

interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:FFFF::1/64
 ipv6 nat
end
```

Lai atlasītu interesējošo datu plūsmu, kurai ir nepieciešama izveidot IP pieejas sarakstu, kurā nodefinējam datu plūsmas, kuras paredzētas translēšanai:

```
ipv6 access-list ipv6_nat
 permit ipv6 any 2010::/96
```

tāpat kā iepriekš, nepieciešams aprakstīt IPv6 prefiksu, kas būs paredzēts translēšanai uz IPv4, tikai šoreiz pievienojot papildus iezīmi, kas norāda NAT-PT maršrutētājam, ka visas IPv6 adreses, kas sākas ar prefiksu 2010::/96 ir pārtranslējamas uz IPv4 adresēm, kuras veido pēdējie 32 biti no IPv6 adreses:

```
ipv6 nat prefix 2010::/96 v4-mapped ipv6_nat
```

tā kā šoreiz nebūs statiska konkrētu iekārtu aprakstīšana, nepieciešams definēt izejas IPv4 adrešu apgabalu, kuru NAT-PT izmantos IPv6 izejas adrešu translēšanai. Un attiecīgā konfigurācijas rinda adrešu pārtranslēšanai:

```
ipv6 nat v6v4 source list ipv6_nat pool v4pool
ipv6 nat v6v4 pool v4pool 85.254.52.0 85.254.52.255 prefix-length 24
```

Attiecīgi visa datu plūsma, kura būs paredzēta IPv6 adrešu apgabalam 2010::/96, tiks translēta, norādot kā izejas adreses IPv4 adreses no apgabala 85.254.52.0/24. Ja tiek skatīta translēšanas tabula, tur nav redzams neviens ieraksts, jo pagaidām neviens ieraksts vēl nav izveidojies, jo nav datu plūsmas, bet statiskās translācijas netika definētas. „*show ipv6 nat translations*” komandas rezultāts:

```
NAT-PT#show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
```

Lai pārbaudītu konfigurācijas pareizību un darboties spēju, nepieciešams izvēlēties IPv4 tīkla resursu, uzzināt tā IPv4 adresi un pārveidot to heksadecimālajā numerācijā. Par piemēru ņemot tīkla resursu www.lu.lv, kura IP adrese ir 195.13.129.210. Savukārt šī adrese heksadecimālā pierakstā būs: C30D:81D2. Tādējādi, lai sasniegtu šo IP no IPv6 lokālā tīkla, nepieciešams veikt *ping* pārbaudi uz IPv6 adresi 2010::C30D:81D2.

```
ipv6#ping 2010::C30D:81d2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::C30D:81D2, timeout is 2 seconds:
!!!!!
```

```
    Success rate is 100 percent (5/5), round-trip min/avg/max =
0/2/4 ms
```

Apskatam pieejamo informāciju no NAT-PT maršrutētāja, translācijas tabula un log faila ieraksti:

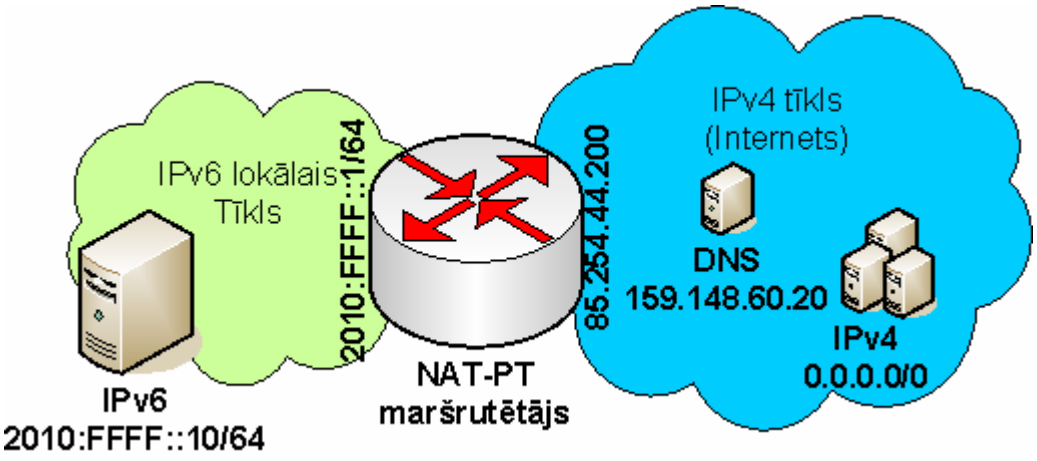
```
    NAT-PT#show ipv6 nat translations
    Prot  IPv4 source              IPv6 source
          IPv4 destination         IPv6 destination
    icmp  85.254.52.2,1281         2010:FFFF::10,1281
          195.13.129.210,1281      2010::C30D:81D2,1281


    *May  6 17:51:37.963: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.2), dst (2010::C30D:81D2) -> (195.13.129.210)
    *May  6 17:51:37.967: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.2) -> (2010:FFFF::10)
    *May  6 17:51:37.967: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.2), dst (2010::C30D:81D2) -> (195.13.129.210)
    *May  6 17:51:37.971: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.2) -> (2010:FFFF::10)
    *May  6 17:51:37.971: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.2), dst (2010::C30D:81D2) -> (195.13.129.210)
    *May  6 17:51:37.971: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.2) -> (2010:FFFF::10)
    *May  6 17:51:37.971: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.2), dst (2010::C30D:81D2) -> (195.13.129.210)
    *May  6 17:51:37.975: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.2) -> (2010:FFFF::10)
    *May  6 17:51:37.975: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.2), dst (2010::C30D:81D2) -> (195.13.129.210)
```

```
*May  6 17:51:37.975: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.2) -> (2010:FFFF::10)
```

Translēšanas tabulas un log faila ierakstos ir redzams, ka par izejas adresi maršrutētājs NAT-PT izvēlējies adresi 85.254.52.2 un izveidojis ierakstu translēšanas tabulā, norādot gan protokolu ICMP, gan izejas un mērķa IP adreses un portus. Šāds, daudz pilnīgāks, ieraksts translēšanas tabulā izveidots, jo tas ir dinamiski izveidojies no esošas datu plūsmas. Statiski izveidotiem ierakstiem neparādās protokola iezīme, jo ieraksts ir derīgs jebkuram protokolam attiecīgo tīkla iekārtu saziņā. Piemērs uzskatāmi pierāda, ka iespējama dinamiska IP adrešu translēšana, kaut gan šāds risinājums nav gana elastīgs. Salīdzinājumam šāda tipa risinājums būtu līdzvērtīgs šobrīd pielietotajam IPv4 protokolam, bez DNS sistēmas, kas nozīmē, ka jebkuru mērķa adresi lietotājs ir spiests sastādīt pats un nav iespējama translācija no domēna vārdiem uz numeriskām adresēm. Pilns konfigurācijas fails pieejams 2. Pielikumā.

1.1.3. Dinamiska IPv6 -> IPv4 adrešu translēšana izmantojot DNS-ALG

Lai arī iepriekš aprakstītais piemērs pierāda, ka iespējama dinamiska adrešu translēšana, tomēr tas pēc autora gūtās pieredzes slēguma izveidē, šāds risinājums nav ērts ikdienas lietošanai. Lai pilnībā izmantotu piedāvātas IPv4 Interneta vides iespējas, nepieciešamas pamata funkcijas - DNS sistēmas, risinājums. Šādu risinājumu piedāvā *Domain Name Server-Application Level Gateway*. DNS-ALG funkcionalitāte nodrošina IPv6 AAAA ieraksta pieprasījuma pārveidošanu uz IPv4 A ieraksta pieprasījumu, tādējādi IPv6 tīkla iekārtām iespējams veikt IPv4 tīklā esošo



1.4. att. **Dinamiska IPv6 translēšana izmantojot**

tīkla resursu DNS ierakstu atšifrēšana. Slēguma shēma redzama attēlā 1.4.

Šī slēguma mērķis ir panākt, lai lietotājs, atrodoties IPv6 tīklā, spētu pilnvērtīgi lietot IPv4 Interneta resursus, neaizdomājoties kas atrodas zem DNS vārdiem un nepārrēķinot IP adreses no decimālās uz heksadecimālo skaitīšanas sistēmu. Tīkla interfeisu konfigurācija šim mērķim paliek nemainīga no iepriekšējā slēguma:

```
interface GigabitEthernet0/0
 ip address 85.254.44.200 255.255.255.0
 duplex auto
 speed auto
 ipv6 nat
end

interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:FFFF::1/64
 ipv6 nat
end
```

līdzīgi kā iepriekšējā slēgumā arī šoreiz nepieciešamo datu plūsmu atlasīšanai, translēšanas nolūkiem, šim nolūkam ir nepieciešams izveidot IP pieejas sarakstu.

```
ipv6 access-list ipv6_nat
 permit ipv6 any 2010::/96
```

aprakstot IPv6 prefiksu, netiek izmantota iezīme, kas liek NAT-PT maršrutētājam translēt visus pieprasījumus ar mērķa adresi no apgabala 2010::/96, pārveidojot mērķa adresi izmantojot

IPv6 pēdējos 32 bitus. Tādējādi tiek atvieglots konfigurācijas darbs, jo nav nepieciešams atsevišķi definēt statisko translāciju.

```
ipv6 nat prefix 2010::/96
```

translēšanas likumi netiek mainīti un paliek tādi paši, kā iepriekš, izmantojot IP pieejas sarakstu un nodefinējot IPv4 adrešu apgabalu izejas adrešu translēšanai:

```
ipv6 nat v6v4 source list ipv6_nat pool v4pool
ipv6 nat v6v4 pool v4pool 85.254.52.0 85.254.52.255 prefix-length 24
```

papildus esošajai konfigurācijai, kas neiedziļinoties pieprasījumā pārveidot IP paketes galveni, nepieciešams ievadīt komandu, kas veic inteliģentāku pieprasījumu apstrādi. DNS-ALG veic IPv6 AAAA pieprasījumu atpazīšanu un veic šādu pieprasījumu pārveidi uz IPv4 A pieprasījumu. Ar sekojošu komandu iespējams ieslēgt šo funkciju:

```
ipv6 nat service DNS
```

Ieslēdzot šo funkciju, jebkurš IPv6 DNS pieprasījums, kas iet caur NAT-PT maršrutētāju, tiks korekti pārveidots par IPv4 pieprasījumu un atbilde tiks korekti implementēta, kā mērķa adresi norādot IPv6 adresi, ar sākuma prefiksu, kas norādīts konfigurācijas failā un beigu 32 bitiem, kas ir IPv4 decimālā pieraksta IP adreses pārveidots pieraksts heksadecimālajā skaitīšanas sistēmā. Papildus nepieciešams definēt DNS serveri, uz kuru pārsūtīt šos pieprasījumus.

```
ipv6 nat v4v6 source 159.148.60.20 2010::20
```

izmantojot šo konfigurāciju visi, IPv6 tīklā kā DNS serveri norādot IP 2010::20 tiks panākta situācija, ka lietotāji spēs piekļūt IPv4 Interneta resursiem norādot attiecīgos Domēnu vārdus. Lai pārliecinātos par konfigurācijas darbību nepieciešams veikt atkārtotu sasniedzamības testu:

```
ipv6#ping www.lu.lv
Translating "www.lu.lv"...domain server (2010::20) [OK]
Type escape sequence to abort.
```

```
    Sending 5, 100-byte ICMP Echos to 2010::C30D:81D2, timeout is
2 seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max =
1/9/32 ms
```

Un attiecīgas izmaiņas ir novērojamas NAT-PT maršrutētājā – gan ieraksti translēšanas tabulā, gan ieraksti log failā:

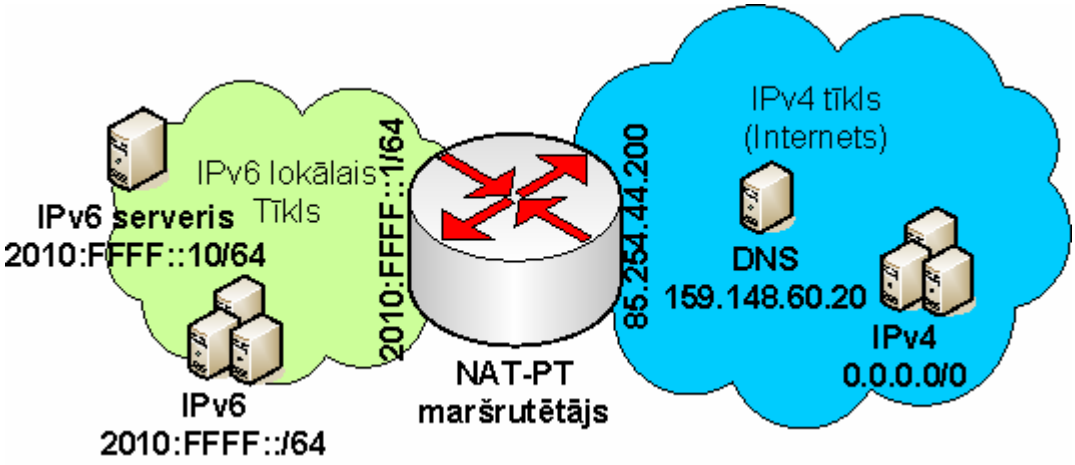
```
    show ipv6 nat translations
    Prot  IPv4 source              IPv6 source
          IPv4 destination         IPv6 destination
    udp   85.254.52.5,54649        2010:FFFF::10,54649
          159.148.60.20,53         2010::20,53

    icmp  85.254.52.5,1983         2010:FFFF::10,1983
          195.13.129.210,1983      2010::C30D:81D2,1983


    *May   6 21:47:50.270: IPv6 NAT: udp src (2010:FFFF::10) ->
(85.254.52.5), dst (2010::20) -> (159.148.60.20)
    *May   6 21:47:50.270: IPv6 NAT: udp src (159.148.60.20) ->
(2010::20), dst (85.254.52.5) -> (2010:FFFF::10)
    *May   6 21:47:50.282: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.5), dst (2010::C30D:81D2) -> (195.13.129.210)
    *May   6 21:47:50.286: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.5) -> (2010:FFFF::10)
    *May   6 21:47:50.286: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.5), dst (2010::C30D:81D2) -> (195.13.129.210)
    *May   6 21:47:50.290: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.5) -> (2010:FFFF::10)
```

```
    *May  6 21:47:50.290: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.5), dst (2010::C30D:81D2) -> (195.13.129.210)
    *May  6 21:47:50.290: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.5) -> (2010:FFFF::10)
    *May  6 21:47:50.294: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.5), dst (2010::C30D:81D2) -> (195.13.129.210)
    *May  6 21:47:50.294: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.5) -> (2010:FFFF::10)
    *May  6 21:47:50.298: IPv6 NAT: icmp src (2010:FFFF::10) ->
(85.254.52.5), dst (2010::C30D:81D2) -> (195.13.129.210)
    *May  6 21:47:50.298: IPv6 NAT: icmp src (195.13.129.210) ->
(2010::C30D:81D2), dst (85.254.52.5) -> (2010:FFFF::10)
```

Apskatot maršrutētāja log faila un translēšanas ierakstus, var redzēt, ka translēšanas tabulā izveidoti divi ieraksti, kur viens UDP protokola ieraksts vērsts uz portu 53, kas ir DNS pieprasījums, un otrs ping pieprasījums uz nupat resolvēto IPv4 DNS ierakstu. Šādā slēgumā iespējama ierasta darbība, kas līdzinās IPv4 slēgumam ar privāto tīklu un NAT konfigurāciju. Pilns konfigurācijas fails pieejams 3.Pielikumā. Pilnīgam slēgumam nepieciešams panākt noteikta resursa IPv6 tīkla iekšienē sasniedzamību no IPv4 tīkla.

1.1.4. Galējais risinājums, visu gadījumu objektīvs apvienojums

Ierasta situācija, kad lokālais tīkls organizācijā tiek veidots no privātām adresēm un uz Interneta vidi tiek veikts NATs, kas „paslēpj” visu lokālo tīklu zem vienas vai vairākām publiskām IPv4 adresēm. Tāpat, ja organizācijas iekšienē atrodas kāds serviss, kuram nepieciešama pieeja no publiskās Interneta vides, tad tiek veikta statiska konkrētu portu vai visas adreses retranslācija no publiskās IPv4 adreses uz privāto. 1.5. Attēlā redzama shēma, kuru nepieciešams realizēt, lai panāktu ierastu lokālā tīkla darbību neskatoties uz to, ka iekšējā tīklā tiek izmantotas tikai IPv6 tīkla adreses.



1.5. att. **Reālistiska slēguma shēma**

Šī slēguma mērķis ir panākt, lai lietotāji, kas atrodas IPv6 tīklā ar adresēm 2010:ffff::/64 spētu lietot IPv4 Interneta resursus, kā arī, lai no IPv4 tīkla būtu pieejams publiskais serveris IPv6 tīklā ar adresi 2010:ffff::10. Lai panāktu šādu funkcionalitāti, nepieciešams apvieno visus iepriekš iegūtos rezultātus vienā kopīgā konfigurācijā, tādējādi panākot vēlamo rezultātu. Tīkla interfeisu konfigurācija paliek nemainīga no iepriekšējā slēguma:

```
interface GigabitEthernet0/0
 ip address 85.254.44.200 255.255.255.0
 duplex auto
 speed auto
 ipv6 nat
end

interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:FFFF::1/64
 ipv6 nat
end
```

Lai varētu izmantot dinamisko translēšanu, nepieciešams definēt IPv6 pieejas sarakstu:

```
ipv6 access-list ipv6_nat
 permit ipv6 any 2010::/96
```

Lai panāktu IPv4 tīkla iekārtu sasniedzamību no IPv6 tīkla, nepieciešams definēt translēšanas likumus, kā arī norādīt IPv4 izejas adrešu apgabalu, kuru izmantos NAT-PT maršrutētājs nepieciešamības gadījumā, lai notranslētu izejošos savienojumus.

```
ipv6 nat v6v4 source list ipv6_nat pool v4pool overload
ipv6 nat v6v4 pool v4pool 85.254.52.0 85.254.52.255 prefix-length 24
```

Papildus jau iepriekš izmantotai komandai, kas norāda kurus pieprasījumus translēt un kādu izejas IPv4 adrešu apgabalu izmantot, ir pievienota iezīme „*overload*”, kas norāda, ka vienai IPv4 adresei varētu būt vairākas, vienlaicīgas translācijas uz dažādām IPv6 adresēm. Šāda iezīme ir nepieciešama, jo norādītajā IPv4 adrešu apgabalā ir tikai 256 IP adreses, toties IPv6 lokālajā tīklā ar masku /64 ir iespējams pieslēgt līdz 35565 tīkla iekārtas. Lai norādītu NAT-PT maršrutētājam kādi pieprasījumi paredzēti translēšanai, nepieciešams norādīt IPv6 prefiksu:

```
ipv6 nat prefix 2010::/96 v4-mapped ipv6_nat
```

lai saglabātu iespēju lietotājiem no IPv6 tīkla pašiem veikt tiešus savienojumus ar IPv4 tīklā esošām tīkla iekārtām, nepapildinot konfigurāciju NAT-PT maršrutētājā. Ar šo ir pabeigta dinamiskā konfigurācija, kas padara iespējamu IPv4 tīkla resursu sasniedzamību no IPv6 tīkla. Papildus nepieciešams nodefinēt translācijas likumus, lai IPv6 iekārta ar IP 2010:ffff::10 būtu pieejama no IPv4 tīkla. Tas iespējams ar sekojošu konfigurācijas rindiņu:

```
ipv6 nat v6v4 source 2010:FFFF::10 159.148.19.4
```

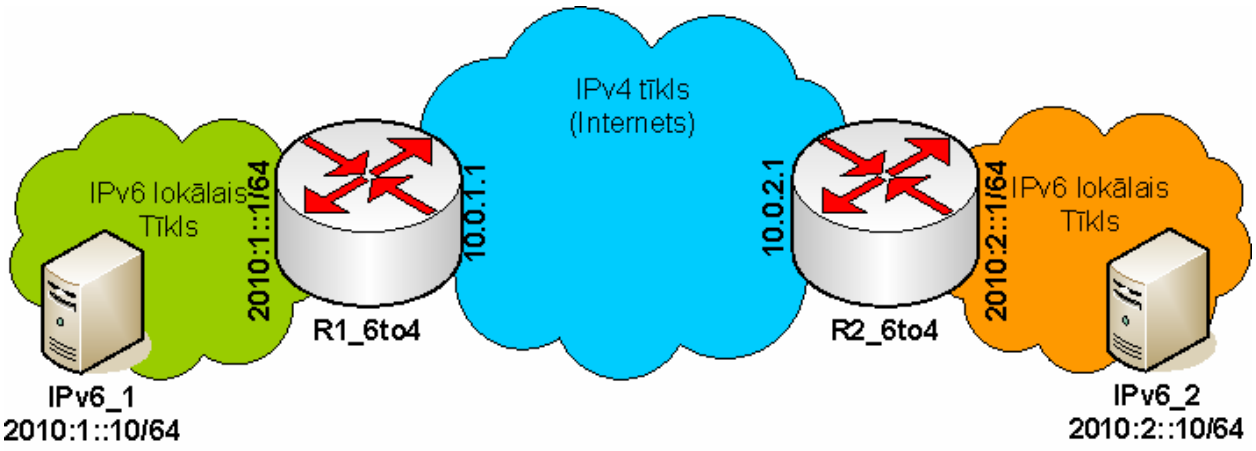
pateicoties šai rindiņai visi pieprasījumi, kas no IPv4 tīkla tiks adresēti uz adresi 159.148.19.4 tiks pārtranslēti uz 2010:ffff::10. Ar šādu konfigurāciju visas IPv6 tīkla iekārtas tiks

translētas uz IPv4 adrešu apgabalu 85.254.52.0 – 85.254.52.255, bet pieprasījumi no 2010:ffff::10 tiks translēti uz IP 159.148.19.4. Pilns konfigurācijas fails pieejams 4. Pielikumā.

1.2 Neatkarīgu IPv6 lokālo tīklu savstarpēji savienoju caur IPv4 tīkla.

Iepriekšējā nodāļā veicot laboratorijas slēgumus, autors pārliecinājās par iespējamību izveidot autonomu IPv6 apgabalu, kas ir pieslēgts tikai IPv4 tīklam un spēj efektīvi funkcionēt un lietot pieejamos IPv4 Interneta resursus. Veicot pārbaudes ar dažādiem slēgumiem tika izveidots slēgums, kas padara pieejamu IPv6 apgabalā izvietotu servisu no IPv4 tīkla. Pieņemot, ka šādu scenāriju varētu izmantot organizācijas vai lietotāji, kuri vēlas izmantot un pāriet uz IPv6 tīklu, bet kuru Interneta pakalpojuma sniedzējs nav spējīgs piegādāt šādu servisu, rodas jautājums vai ir iespēja panākt savienojumu ar citiem šādiem apgabaliem un IPv6 Internet resursiem kopumā. Risinājums ir IPv6 tunelēšana pār IPv4 tīklu. Ir pieejami vairāki risinājumi, kas piedāvā šādu funkcionalitāti, šī darba ietvaros par piemēru tika izvēlēts risinājums „6to4”, jo tas ir elastīgs, dinamisks risinājums, tam nav nepieciešama konkrētu divu punktu tuneļu izveidei, tāpat eksistē publiski servisi, kas piedāvā izmantot šo risinājumu, lai sasniegtu citus neatkarīgus IPv6 apgabalus, un arī IPv6 Internet servisus. Papildus teorijai, viens no Francijas vadošajiem Interneta pakalpojumu sniedzējiem Free [4] kā pakalpojumu klientiem sniedz nedaudz uzlabotu šīs tunelēšanas versiju „6rd”. Tādējādi paralēli izmantojot Dual-Stack risinājumu sniedz IPv6 Interneta resursu pieejamību gala lietotājiem nenodrošinot pilnīgu IPv6 atbalstu tīkla maģistrālēs. Diemžēl šī uzlabotā versija ir gana jauna un vēl nav plaši pieejama, šis konkrētais pakalpojumu sniedzējs ir viens no pirmajiem, kas plaši ieviesis šo pakalpojumu, pamatā balstoties uz pašu izstrādātas aparatūras, kura veidota sadarbībā ar 6rd līdzautoru Rémi Després.

Lai pārbaudītu praksē 6to4 darboties spēju autors veidoja laboratorijas slēgumu, kurā izveidosim tīru IPv4 tīkla simulāciju un divus neatkarīgus IPv6 tīkla apgabalus. Slēguma shēma redzama attēlā 2.1.



2.1. att. **6to4 tunelēšanas slēguma shēma**

Tīkla slēgums tiek veidots izmantojot tīkla iekārtu simulāciju programmu GNS3 (GNS3.net). Simulācijā tiek izmantoti Cisco 7200 sērijas maršrutētāji ar programmnodrošinājumu: c7200-advipservicesk9-mz.124-22.T4.bin un ražotāja dokumentācija par slēguma pamat konfigurāciju [5]. Pamata konfigurācijai nepieciešams izveidot pareizu tīkla interfeisu konfigurāciju, ar attiecīgi nodefinētām IPv4 un IPv6 adresēm:

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:1::1/64

interface FastEthernet0/1
 ip address 10.0.1.1 255.255.255.0
 duplex auto
 speed auto
```

Papildus, tā kā IPv4 ir strādājošais tīkls šai slēgumā, pilnvērtīgai konfigurācijai maršrutētājam ir jānokonfigurē pamata maršrutēšanas informācija, attiecīgi noklusētais maršruts, uz kuru sūtīt visus pieprasījumus, kuriem nav zināms konkrēts maršruts pieprasījumus:

```
ip route 0.0.0.0 0.0.0.0 10.0.1.254
```

lai veiktu tunelēšanas darbus, nepieciešams izveidot tunnel interfeisu maršrutētājā, kā izejas adresi norādot paša maršrutētāja interfeisa adresi virzienā uz IPv4 tīklu. Protams, ir iespējams izmantot jebkuru maršrutētājam piederošu, maršrutējamu IPv4 adresi, bet testa vienkāršības labad autors izmanto esošo pieslēgumu IPv4 tīklam. Tāpat nepieciešams norādīt tuneļa tipu 6to4 un IPv6 izejas adresi, kuru veido izmantojot prefiksu 2002::/16, kuram sākuma galā tiek pievienota IPv4 izejas adresi heksadecimālā pierakstā:

```
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2002:A00:101::/128
 tunnel source 10.0.1.1
 tunnel mode ipv6ip 6to4
```

IPv6 adrešu apgabals 2002::/16 ir rezervēts apgabals 6to4 tuneļu veidošanai (RFC3068), kas norāda, ka jebkurš pieprasījums, kura sākuma prefikss ir 2002, ir paredzēts tunelēšanai izmantojot 6to4 mehānismu. Kā jau tika minēts, IPv6 adrese veidojas no prefiksa 2002 un IPv4 izejas adreses heksadecimālajā pierakstā, kas savukārt norāda maršrutētājam uz kādu IPv4 adresi pārsūtīt pieprasījumus, kas tiek tunelēti. Attiecīgi nepieciešams maršrutētājam norādīt, ka visi 6to4 tuneļi sāksies no Tunnel0 interfeisa:

```
ipv6 route 2002::/16 Tunnel0
```

Lai panāktu tīkla 2010:2::/64 sasniedzamību no 2010:1::/64 tīkla, nepieciešams maršrutētājam R1_6to4 norādīt, ka attiecīgais tīkls ir sasniedzams caur 6to4 tuneli un atrodas aiz maršrutētāja ar IPv4 adresi 10.0.2.1, ko var panākt ar sekojošu konfigurācijas rindu:

```
ipv6 route 2010:2::/64 2002:A00:201::
```

kas norāda maršrutētājam, ka tīkls 2010:2::/64 ir sasniedzams caur IPv6 adresi 2002:A00:201::. Tā kā maršrutētājam nav konkrētu maršrutu uz šādu tīkla resursu, tad nostrādā maršruts 2002::/16, kas liek maršrutētājam uzsākt 6to4 tuneli. Atšifrējot IPv6 mērķa adresi, iespējams saprast, ka IPv4 adrese, aiz kuras ir atrodams interesējošais IPv6 tīkls ir a00:201, jeb pilnā pierakstā 0A00:0201, kas savukārt pārvēršot uz decimālo pierakstu ir 10.0.2.1. Attiecīgi uz šādu adresi arī maršrutētājs pārsūtīs IPv6 paketi, kas ievietota IPv4 paketes datu apgabalā. Izveidojot simetriski līdzvērtīgu konfigurāciju uz maršrutētāja R2_6to4, tiek iegūts strādājošs tunelis, caur kuru iespējams pārsūtīt IPv6 pieprasījuma paketes caur IPv4 tīklu, kurā nav nevienas IPv6 atbalstošas iekārtas. Veicot pārbaudi:

```
IPv6_1#ping 2010:2::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:2::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 800/1097/1344 ms
```

Redzams, ka no tīkla iekārtas IPv6_1 ir iespējams sasniegt tīkla segmentu 2010:2::/64, un konkrēti iekārtu 2010:2::10. Par tunelēšanas darbību iespējams pārliecināties R1_6to4 maršrutētāja log ierakstos:

```
*May  8 10:28:13.599: Tunnel0: IPv6/IP adjacency fixup, 10.0.1.1->10.0.2.1, tos set to 0x0
*May  8 10:28:14.143: Tunnel0: IPv6/IP to classify 10.0.2.1->10.0.1.1 (tbl=0,"IPv4:Default" len=120 ttl=253 tos=0x0) ok, oce_rc=0x0
*May  8 10:28:14.399: Tunnel0: IPv6/IP adjacency fixup, 10.0.1.1->10.0.2.1, tos set to 0x0
*May  8 10:28:15.319: Tunnel0: IPv6/IP to classify 10.0.2.1->10.0.1.1 (tbl=0,"IPv4:Default" len=120 ttl=253 tos=0x0) ok, oce_rc=0x0
```

```
    *May    8  10:28:15.707:  Tunnel0:  IPv6/IP  adjacency  fixup,
10.0.1.1->10.0.2.1, tos set to 0x0
    *May  8 10:28:16.339: Tunnel0: IPv6/IP to classify 10.0.2.1-
>10.0.1.1  (tbl=0,"IPv4:Default"  len=120  ttl=253  tos=0x0)  ok,
oce_rc=0x0
    *May    8  10:28:16.527:  Tunnel0:  IPv6/IP  adjacency  fixup,
10.0.1.1->10.0.2.1, tos set to 0x0
    *May  8 10:28:17.339: Tunnel0: IPv6/IP to classify 10.0.2.1-
>10.0.1.1  (tbl=0,"IPv4:Default"  len=120  ttl=253  tos=0x0)  ok,
oce_rc=0x0
    *May    8  10:28:17.619:  Tunnel0:  IPv6/IP  adjacency  fixup,
10.0.1.1->10.0.2.1, tos set to 0x0
    *May  8 10:28:18.583: Tunnel0: IPv6/IP to classify 10.0.2.1-
>10.0.1.1  (tbl=0,"IPv4:Default"  len=120  ttl=253  tos=0x0)  ok,
oce_rc=0x0
```

Redzams, ka maršrutētājs ir atpazinis nepieciešamību veikt tunelēšanu un pārveidot pieprasījumu to iekļaujot jaunas IPv4 paketes datu segmentā un pārsūtot uz pareizo maršrutētāju, kuram ir tālāka informācija par IPv6 segmentu. Pilni konfigurācijas faili pieejami 5. Un 6. Pielikumos.

Aprakstītais piemērs ir darboties spējīgs tikai laboratorijas apstākļos, jo, lai arī nav nepieciešams veidot statiskus tuneļus, nepieciešams aprakstīt visus, vai daļu IPv6 tīkla segmentus un to maršrutējošos IPv4 maršrutētājus. IPv4 adrešu segmentā starp vairākām rezervētām IP adresēm eksistē adrešu apgabals 192.88.99.0 – 192.88.99.255, kas tieši paredzēts 6to4 tunelēšanas mērķiem. Attiecīgi, ja kāds Interneta pakalpojumu sniedzējs vēlas veikt šādu pakalpojumu saviem klientiem un paziņot pārējiem pakalpojumus sniedzējiem, ka viņam ir pieejami IPv6 resursi caur 6to4 tuneli un atrodas aiz IPv4 tīkla iekārtām, tad atliek tikai izziņot par savā tīklā pieejamu adresi no tīkla 192.88.99.0/24. Reālās dzīves konfigurācijā, izmantojot BGP protokolu Interneta servisa sniedzēji apmainās ar informāciju par pieejamiem IPv6 un IPv4 resursiem, attiecīgi 2002::/16 un 192.88.99.0/24. Pamatojoties uz šo informāciju jebkurš cits

Interneta servisa sniedzējs spēj novirzīt IPv6 pieprasījumus uz nepieciešamajām IPv4 adresēm. Kā noklusētā vērtība visiem IPv6 tīkla maršrutēšanas ierakstiem tiek norādīts maršrutēšanas ieraksts uz adresi 2002:C058:6301:: kas ir 192.88.99.1 jeb tuvākais pieejamais 6to4 atbalstošais maršrutētājs apstrādās šo saņemto pieprasījumu un nosūtīs tālāk nepieciešamajā virzienā.

2 PRAKTISKAIS TĪRA IPV6 APAKŠTĪKLA IEVIEŠANAS MĒĢINĀJUMS

Teorētiska izpēte ar laboratorijas slēgumu sniedz pārliecību, ka ir iespējama IPv4 Interneta vides resursu pieejamība no tīra IPv6 tīkla, izmantojot NAT-PT, bet, lai gūtu pilnīgu pārliecību par esošā slēguma dzīvotspēju, tiek veidots reāls, strādājošs slēgums, kurā izvietoti publiski pieejami resursi un no kura būtu pieejami ārējie Interneta resursi. Papildus reālākiem testiem autors pārslēdzās pilnībā uz šo risinājumu un savā ikdienas darbā lietoja šādu pieeju.

Atrodoties aiz IPv6 translējoša maršrutētāja, autors izmantoja publisku IPv6 apakštīklu 2a02:610:2010/64, kurš ir maršrutējams IPv6 tīklā, līdz ar to tika radīta teorētiska iespēja pilnvērtīgi lietot IPv6 Interneta resursus. Lokālajā tīklā tika izvietots e-pasta serveris, kurš nodarbojās ar e-pasta saņemšanu un izsūtīšanu, tika reģistrēts domēns testbed.mc.net.lv, kas norāda uz šo e-pasta serveri. Kā arī autora darba stacija tika pieslēgta paralēli lokālajā tīklā izvietotajam serverim. Slēguma shēma redzama attēlā 3.1.

Autora ikdienas darbs ir saistīts ar tīkla iekārtu konfigurāciju un konkrētu Interneta vietņu apskati, kas nodrošināja tīkla iekārtu uzraudzību, papildus ikdienas saziņai ar kolēģiem un klientiem tiek lietots e-pasts un Skype [6] saziņas rīks. Paralēli tiešajiem darba pienākumiem autors ir veicis vairākus iespējamo scenāriju testus un apskatījis dažādu populāru resursu un protokolu darbību izveidotajā slēgumā.

2.1 Ikdienas darba iespējamība IPv6 NAT-PT slēgumā

Pirmā pamanītā nepilnība no ikdienas darbā izmantojamām aplikācijām bija IPv6 neatbalstīšana populārajā saziņas līdzeklī Skype. Domājot par nākotnes perspektīvām un attīstot savu risinājumu, izstrādātāji ir atstājuši novārtā tādu svarīgu punktu attīstības ceļā kā atbalstu IPv6 protokolam. Spriežot pēc izstrādātāja Interneta vietnē [7] pieejamās informācijas, tuvākajā laikā netiks nodrošināts atbalsts IPv6 protokolam.

Vienīgais autoram pilnvērtīgi pieejamais elektroniskais saziņas līdzeklis, lietojot IPv6, bija e-pasts. Šeit situācija ir daudz labvēlīgāka. Attiecīgos pieprasījumus uz IPv4 tīklā esoša e-pasta

servera ir iespējams veikt, līdz ar to pilnvērtīgi lietot gan IMAP gan POP3 protokolus. Tāpat iespējams izsūtīt e-pasta vēstules, lietojot SMPT serveri, kas arīdzan ir izvietots IPv4 tīklā un uz kuru pieeja tiek nodrošināta izmantojot DNS vārdu un DNS-ALG funkcionalitāti. E-pasta lietošana izmantojot e-pasta programmas ir kritiski nepieciešams mūsdienu instruments, ar kuru darbojas lielākā daļa Interneta lietotāju, tāpēc šī resursa pieejamība ir labs arguments pāriet uz IPv6 lokālo tīklu, pat ja e-pasta serviss tiek lietots no kāda koplietošanas servisa vai Interneta pakalpojuma sniedzēja servera, kas viennozīmīgi sākotnēji paliks IPv4 tīklā.

Interneta resursu pieejamība tika testēta jau laboratorijas slēgumā, veicot ping pieprasījumus uz Interneta vietni www.lu.lv. Atrodoties IPv6 tīklā autoram bija iespēja pārliecināties, ka darbojas ne tikai ping pieprasījumu nosūtīšana un saņemšana, bet arī pilnvērtīga HTTP un HTTPS protokolu lietošana. Darba gaitā autoram neradās problēmas piekļūt kādai no IPv4 tīklā esošai Interneta vietnei, kā arī bija iespējama pilnvērtīga darbība ar to. Tāpat pēc profesionālās darba specifikas, autoram, bieži nākas veikt tīkla iekārtu konfigurācijas izmaiņas lietojot Web bāzētu pieejas portālu. Arī šādos gadījumos darbs bija iespējams un rezultāts nebija atšķirams no IPv4 tīklā pieredzētā.

Autora darba dienas ietvaros konfigurācijas faili tiek mainīti arī uz iekārtām, kurām drošības vai funkcionalitātes dēļ nav pieejami Web bāzēti pieejas portāli, tāpēc nepieciešams izmantot SSH vai TELNET savienojumus. Ņemot vērā, ka šie protokoli ir vēsturiski veidoti vienkāršu savienojumu izveidošanai, to sarežģītība ir neliela, kas padara tos vieglus ALG vārtejai pārtranslēšanai no vienas IP protokola versijas uz otru. Attiecīgi darbā ar šiem protokoliem autors nesastapa problēmas.

2.2 Specializētu protokolu un savienojumu darbība NAT-PT slēgumā.

Papildus ikdienā lietojamiem protokoliem un savienojumiem, autors pārbaudīja dažādu IPv4 tīklā lietotu protokolu darbību izveidotajā slēgumā. Kā vienu no pirmajiem autors izmēģināja peer-to-peer datu apmaiņas protokolu BitTorrent. Pamatojoties uz viena no lielākajiem tīkla iekārtu ražotājiem, kas nodrošina datu pārraides tīklu uzraudzību, ierobežošanu un analīzi, Ipoque, tieši peer-to-peer datu plūsmas ir dominējošās mūsdienu Interneta vidē, un kā

viens no populārākajiem ir tieši BitTorrent protokols. Izmantojot šo protokolu ir iespējams operatīvi pārsūtīt lielus datu apjomus maksimāli utilizējot pieejamo tīklu un samazinot neoptimālu datu pārraidi. Kā šī protokola testa piemēru autors veica uTorrent aplikācijas instalāciju savā datorā un testa lejupielādi jaunākajai Linux distributīva Ubuntu, servera instalācijai. Pateicoties tam, ka lielākā daļa Interneta servisa sniedzēju veic automātisko DNS ierakstu izveidošanu savām IP adresēm, uTorrent programma spēj sazināties ar visām iesaistītajām pusēm, kurām ir pieejami korekti DNS vārdi. DNS-ALG funkcionalitāte veic pilnvērtīgu IPv4 adrešu pārtranslēšanu uz adresēm ar nokonfigurēto IPv6 prefiksu un decimālā pieraksta translāciju uz heksadecimālo. Lejupielādes laikā bija brīdis, kad lejupielāde notika ar ātrumu virs 700KiloBaitiem/sekundē, kas ir līdzvērtīgi 4,8Megabitiem/sekundē. NAT-PT iekārtas noslodze šī procesora vidū bija zem 10%, kas norāda, ka šāda ātruma daudz mazu savienojumu pārtranslēšana nesagādā problēmas izvēlētajai iekārtai un ir iespējami krietni lielāki datu apjomi. Kā otru populārāko datu pārsūtīšanas veidu augstāk minētā organizācija min uz HTTP protokolu bāzēta failu apmaiņa. Praktiski šāda veida failu apmaiņa ir BitTorrent adaptācija, padarot to pieejamāku lietotājiem, kuriem drošības vai citu ierobežojošu iemeslu dēļ nav pieejami citi resursu Interneta vidē. Protokola darbība ir likumsakarīga, jo pēc savas būtības simulē Interneta vietnes apskati, kas ir iespējama no izveidotā slēguma.

Par vienu no vecākajiem peer-to-peer datu pārsūtīšanas protokoliem var minēt FTP protokolu. Datu apmaiņa, izmantojot FTP protokolu, ilgu laiku bija vienīgais veids lielu datņu pārsūtīšanai, kuras nebija iespējams nosūtīt izmantojot e-pastu. Atšķirībā no iepriekš aprakstītā protokola, kur tika veidoti daudz dinamiski savienojumi, FTP ir stingri peer-to-peer savienojuma protokols, kurā iesaistītās puses tiek definētas kā serveris un klients. Pieslēgums tiek veikts no klienta uz serveri un datu nosūtīšana vai saņemšana arī tiek inicializēta vienā virzienā. Ir iespējami paralēli savienojumi, bet nav iespējams šādi lejupielādēt vienu datni. Testa nolūkos autors izvietoja Web resursu IPv6 tīkla vidē, kuram bija pieeja no IPv4 Interneta vides, izmantojot DNS adresi testbed.mc.net.lv. Nokonfigurējot FTP servera aplikāciju uz izvietotā resursa, tika izveidots IPv4 tīklam pieejams FTP serveris, kas atrodas tikai IPv6 tīklā. Tādējādi, izmantojot tīkla pārlūka programmu un izvēloties par mērķa adresi ftp://testbed.mc.net.lv, iespējams sasniegt izvietoto serveri, izmantojot FTP protokolu, un lejupielādēt tur esošo teksta

datni. Drošības nolūku dēļ nav iespējama datņu augšupielādēšana neizmantojot autorizāciju, bet darba autors ir pārliecinājies, ka šāda veida datu pārraide arī ir iespējama.

Papildus, lai izvietotais tīkla resurss būtu pilnīgs, autors ir izvietojis tajā e-pasta serveri un nelielu Web resursu. Apskatot tīkla adresi http://testbed.mc.net.lv, iespējams ielogoties izvietotajā e-pasta servera Web grafiskajā lietotāja saskarnē. Tāpat, apskatot resursu http://testbed.mc.net.lv:8080, iespējams apskatīt izvietoto nelielo, vienkāršo Interneta vietni ar īsu informāciju par to un sīkrīku, kas norāda uz brīvo IPv4 adrešu skaita samazinājumu ARIN[1] datu bāzē, kas ir atbildīga par IPv4 resursu sadalījumu Ziemeļamerikas reģionā. Pēc kopējām aplēsēm šis reģions ir vien no pirmajiem, kurš izjutīs IPv4 adrešu trūkumu. Lai arī konkrētu datumu nav iespējams noteikt, tomēr kā visticamākais datums tiek minēts 2011.gada 11.martu. Pie tam, ja IPv4 adrešu izdalīšana turpinātos šādos apmēros, tad kopējā IPv4 brīvo adrešu datu bāze tiks iztukšota līdz 2011.gada 16.septembrim. Lai arī nav iespējams noteikt konkrētu datumu, kad tiks izsniegta pēdējā brīvā IPv4 adrese, tomēr šāds piemērs liek pievērsties domai, ka esošais brīvi pieejamais daudzums var un visticamāk izbeigsies tuvāko dažu gadu laikā. Lai papildus nodrošinātu objektīvu testu, autors izveidoja e-pasta lietotāju esošajā e-pasta serverī ar automātisko atbildētāju. Attiecīgi sūtot e-pasta vēstuli uz adresi andriss@testbed.mc.net.lv no jebkura IPv4 tīklā esoša e-pasta resursa, iespējams saņemt atbildi, kas tiek automātiski ģenerēta un nosūtīta no IPv6 tīklā izvietotā servera. Tādējādi iespējams pārliecināties, ka ir pieejami ne tikai e-pasta servisi virzienā no IPv6 uz IPv4, bet arī pretēji.

Autora ikdienas darba ietvaros ir nepieciešams administrēt dažādus serverus vai attālināti darboties ar citām darba stacijām. Attālinātai Windows Operētājsistēmas serveru administrācijai tiek lietos Attālinātās pieejas rīks, jeb Remote desktop tool. Izmantojot šo rīku iespējams caur IP tīklu pārraidīt no servera monitora izskatu un izmaiņas tajā, kā arī nosūtīt ziņas par peles un klaviatūras aktivitātēm. Lai arī protokols izmanto standarta TCP savienojumu, tas ir īpašs ar savu pieeju veicot datu pārraidi, attiecīgā servera monitora attēlojums un izmaiņas tajā netiek sūtīts kā bilde, bet gan kā vektorgramma. Izmantojot šādu pieeju tiek uzlabota ātrdarbība un samazināts minimāli nepieciešamā datu plūsmas caurlaides spēja, tādējādi padarot iespējamu protokola lietošanu pat uz iezvana interneta pieslēguma. Protokola būtība ir peer-to-peer savienojums starp

[1] ARIN – American Registry for Internet Numbers

serveri un klienta aplikāciju, starp kuriem tiek nodibināta saite un pārsūtītas ekrāna izmaiņas klienta virzienā, kā arī peles un klaviatūras darbības servera virzienā. Testējot Remote Desktop rīku virzienā no IPv6 tīkla uz IPv4, autors sastapās ar IP adrešu pierakstīšanas specifiku. IPv4 adreses pierakstā decimālie cipari tiek atdalīti ar punktiem un ar kolu tiek atdalīts pieslēguma ports, ja nepieciešams norādīt citu, ne noklusēto, bet IPv6 adrese tiek pierakstīta izmantojot kolus. Iepazīstoties ar attiecīgā rīka dokumentāciju noskaidrots, ka pareizs IPv6 pieraksts šādā situācijā ir pierakstot IP adresi iekļaujot to kvadrātiekavās, un nepieciešamības gadījumā tās galā norādot pieslēgumportu, izmantojot kolu. Atrisinot šo problēmu autors veiksmīgi veica pieslēgšanos IPv4 tīklā esošam serverim. Pretējā virzienā pieslēgums problēmas nesagādāja, jo pieslēgšanās tiek veikta uz konkrētu IPv4 adresi. Remote desktop rīks ir fleksibls no iespēju viedokļa, jo iespējama gan darba virsmas pārņemšana, gan dalīšana, lai lokālais lietotājs redz administratora veiktās darbības. Bet diemžēl šis rīks nav pielietojams, ja nav iespējama tieša saziņa starp gala iekārtām. Ja servera pusē ir ugunsmūra iekārta, kurai ir aizliegti Remote desktop pieejas porti, tad pieeja, izmantojot Remote Desktop rīku, ir neiespējama. Alternatīva šim rīkam, kas arī spēj darboties aiz ugunsmūra esoša servera situācijā un atbalsta gan Windows, gan Mac gan dažādas Linux platformas, ir TeamViewer aplikācija [8]. Diemžēl, līdzīgi kā ar Skype rīku, arī šī rīka izstrādātāji nav pielikuši pūles, lai tas darboties Ipv6 tīklā. Bezmaksas alternatīva Windows attālinātās pieejas rīkam ir uz AT&T izstrādātā VNC rīka bāzes izveidots RealVNC attālinātas pieejas rīks[9] un tam līdzīgie[10]. Taču, lai arī pats VNC rīks atbalsta Ipv6 savienojumus, ne visi atvasinātie, specializētie varianti saglabā šo atbalstu. Ieguvums ir dažādu platformu atbalstā, bet tās tomēr saglabā ierobežojumu uz tiešo savienojumu servera virzienā, tādējādi bez izmaiņām ugunsmūra noteikumos nav iespējams pieslēgties datoram aiz tā.

2.3 Tīkla slēguma ātrdarbība.

Kā jau minēts 1. sadaļas sākumā, par pamatu slēgumam tika lietots Cisco Systems 2821 sērijas maršrutētājs, kura oficiālie veiktspējas dati sola maršrutēšanas spēju līdz 100Mbps lielai datu plūsmai. Veicot pārbaudi un testus 2. sadaļas pirmajos divos apakšpunktos aprakstītajiem protokoliem un aplikācijām, autors veica maršrutētāja jaudas novērtējumu. Kā vienu no konkrētā slēguma galvenajiem trūkumiem var minēt Cisco Systems maršrutētāja nepilnīgu atbalstu NAT-

PT protokolam aparatūras līmenī. Jebkura uz kādas no Unix distribūcijas bāzēta maršrutētāja galvenais trūkums ir visu darbību veikšana uz centrālā procesora, IPv4 gadījumā Cisco maršrutētāji ir pārāki, jo viņiem, tāpat kā daudziem citiem augstāka līmeņa maršrutētajiem, liela daļa darbību tiek veiktas izmantojot šiem nolūkiem paredzētus specializētus procesorus. Liela daļa IPv4 datu plūsmu apstrāde nenonāk līdz maršrutētāja procesoram, jo tiek apstrādāta tīkla interfeisu līmenī un nosūtīta tālāk. Toties IPv6 NAT-PT risinājums nespēj izmantot šīs iespējas, tādējādi visas darbības ar šāda veida datu plūsmām tika veiktas izmantojot centrālo procesoru, kas būtiski samazina veiktspējas rādītājus.

2.3.1. Datu pārsūtīšanas ātrdarbība.

Sākotnējai infrastruktūras novērtēšanai autors veica caurlaidības stresa testu, maksimāli noslogojot maršrutētāju, lai pārliecinātos par praktiski iespējamo maksimālo veiktspēju. Izmantojot liela apjoma datni un jau nokonfigurēto FTP servera funkcionalitāti IPv6 tīklā izvietotajam serverim, autors veica vairākkārtēju datu pārsūtīšanu. Veicot šo testu tika mērīta maršrutētāja centrālā procesora noslodze un tīkla interfeisu noslodze, kā arī datnes sūtošā un datnes saņemošā servera rādītājus, lai pārliecinātos par vājāko ķēdes punktu. Turpinot testus tika veikti izmēģinājumi ar citiem protokolu veidiem. Veikto testu apkopojums redzams tabulā 2.3.1.1.

Nr.p.k.	Izmantotais Protokols/Rīks	Vidējais datu pārsūtīšanas ātrums	NAT-PT maršrutētāja noslodze	Komentāri.
1.	FTP	5,9MB/s ~ 47Mb/s	99%	
2.	SCP (SSH)	5,8MB/s ~ 46Mb/s	99%	Droša datu pārsūtīšana izmantojot SSH protokolu

3.	BitTorrent	1,5MB/s ~ 12Mb/s	35%	Iedarbojās Interneta pakalpojumu sniedzēja ierobežojums.

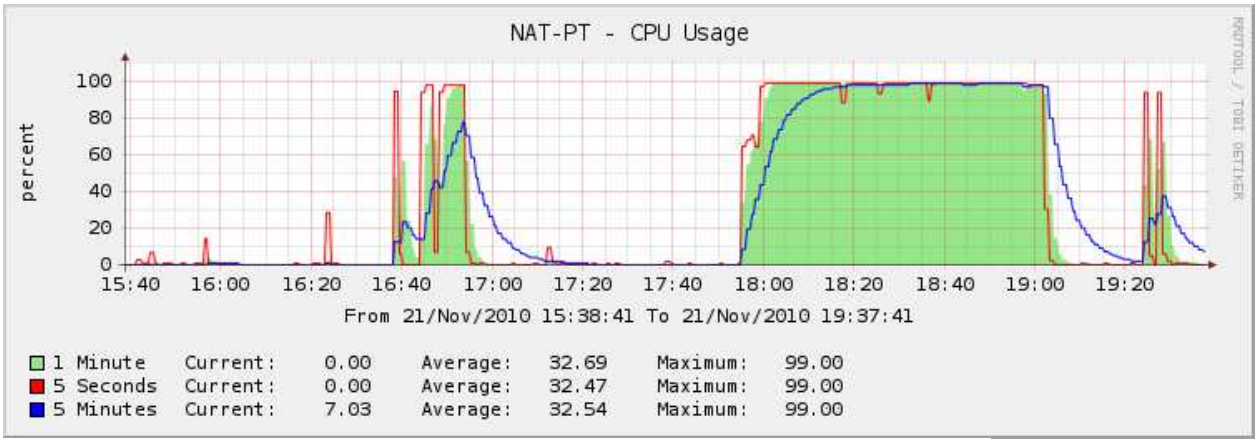
2.3.1.1. tabula. **Datu pārsūtīšanas protokolu ietekme uz maršrutētāju**.

Kā redzams pēc testu rezultātiem visos maršrutētāja noslodze ir praktiski 100%, kas norāda uz to, ka tas kļūst par ierobežojošo faktoru. Salīdzinājumam tiek veikti testi IPv6 tīkla iekšienē, sk. Tabula 2.3.1.2., lai pārliecinātos par maršrutētāja faktoru.

Nr.p.k.	Izmantotais Protokols/Rīks	Vidējais datu pārsūtīšanas ātrums	Gala iekārtu CPU noslodzes (klients, serveris)
1.	FTP	9,8MB/s ~ 78,4Mbps	55%, 10%
2.	SCP (SSH)	6,2MB/s ~ 50Mb/s	80%, 40%

2.3.1.2. tabula. **Datu pārsūtīšanas protokolu darbība IPv6 tīklā**.

Testu rezultāti uzrādīja, ka FTP gadījumā ievērojami palielinājies datu pārsūtīšanas ātrums. Nedaudz mazāk, bet tomēr redzams pieaugums arī SCP protokola gadījumā, kas norāda uz to, ka vājais ķēdes posms ir tieši maršrutētājs. Līdz ar to, iespējams secināt, ka maršrutētājs, kas paredzēts IPv4 tīkla ietvaros maršrutēt līdz 100Mbps, tomēr nespēj nodrošināt šāda veida funkcionalitāti gadījumā, ja nepieciešama translēšana uz IPv6 protokolu. Apskatot grafikus brīžos, kad notikuši testi ir skaidri redzams, ka maršrutētājs tiek maksimāli noslogots vienlaicīgi



2.3.1.1.att. **Maršrutētāja noslodze pastiprinātas slodzes apstākļos**

ar datu plūsmas sākumu. Attēlā 2.3.1.1 ir skaidri redzams, ka procesora noslodze ir izdalāmi divi lielumi – normāla darbība zem 10%, un darbība maksimāli noslogotos apstākļos – 100%.

Papildus informāciju var iegūt skatoties noslodzes tabulā uz paša maršrutētāja:

```
     NAT-PT#show processes cpu sorted 5min
     CPU utilization for five seconds: 99%/27%; one minute: 99%;
five minutes: 98%
      PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min
TTY Process
      107     1579496    917415       1721 60.09% 60.05% 60.54%
0 IPv6 Input
       78      863952   4321941        199 10.81% 10.96% 10.89%
0 IP Input
        5      335484     38744       8658  0.00%  0.12%  0.11%
0 Check heaps
      132        1176   3796308          0  0.08%  0.04%  0.02%
0 RBSCP Background
      227       16016     26825        597  0.00%  0.03%  0.02%
0 SNMP ENGINE
```

Attiecīgā komanda uzrāda visus procesus, kas izmanto centrālā procesora laiku, sakārtotus pēc vidējā rādītāja pēdējo 5 minūšu laikā. Uzskatāmības labad ir uzrādīti tikai pirmie 5 procesi, jo tālākie ļoti minimāli noslogo procesoru. Var pamanīt, ka vairāk kā 60% no procesora laika aizņem process ar nosaukumu *IPv6 Input*, kas norāda uz maršrutētāja grūtībām apstrādāt tieši ar IPv6 saistītās datu plūsmas. Nākamais process ir *IPInput*, kas ir IPv4 datu plūsmas apstrāde. Kā jau minēju nodaļas sākumā, IPv6 atbalsts vēl nav iestrādāts aparatūras līmenī, tāpēc varam novērot, ka vienādas datu plūsmas apstrāde IPv4 un IPv6 protokolos, aizņem dažādu centrālā procesora laiku.

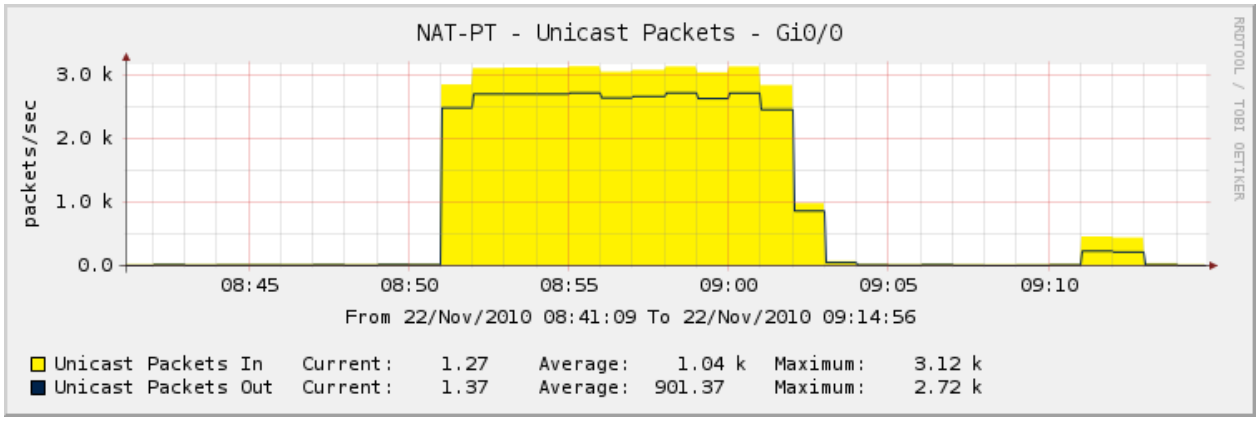
2.3.2. Vairāku vienlaicīgu pieprasījumu apstrādes ātrdarbība.

IPv4 tīkla maršrutētājiem ierasts ir norādīt divus veiktspējas rādītājus – datu caurlaidības spēju un pakešu apstrādes spēju. Pēc IPv4 protokola uzbūves, katra maršrutējošā iekārta ir spiesta veikt vairākas darbības ar IP paketi, pirms tā var to nosūtīt tālāk – pirmkārt pakete ir jāsaliek kopā, ja tā ir bijusi par lielu un pārsūtīta vairākos freimos. Otrkārt nepieciešams aprēķināt

kontrolsummu, kuras kļūdas gadījumā jāignorē šī pakete un atkarībā no protokola ir vai nav jāpieprasa atkārtots sūtījums. Treškārt saņemot, saliekot un pārbaudot paketi, tā ir jāpārbauda pret visiem likumiem, kas paredzēti maršrutētājā un tikai tad, kad ir zināms, kur sūtīt paketi to iespējams sūtīt tālāk, protams, sadalot mazākos gabalos, jeb freimos, ja tas nepieciešams. Visas šīs darbības sarežģī vienas IP paketes apstrādi, tāpēc gadījumā, ja datu plūsmā ir daudz mazu IP pakešu, tad kopējais maksimāli iespējamais datu pārsūtīšanas apjoms sarūk, salīdzinot ar situāciju, kad pieejamas lielas IP paketes. Interneta vietņu pārlūkošana ierasti neveido lielu datu apjomu, bet gan daudz mazu IP pakešu īslaicīgu aktivitāšu pīķus. Lai pārbaudītu šādu savienojumu apstrādi, autors veica testu, kura laikā uz izveidoto Interneta vietni, tika veikti vairāki vienlaicīgi pieprasījumi, tādējādi veidojot sava veida pārslodzi tīklā. Šis tests tika veikts ar mērķi pārbaudīt cik liels ir teorētiski iespējamais vienlaicīgo apmeklētāju skaits uz vienu izvietoto serveri IPv6 tīklā, kas darbojas caur NAT-PT vārteju. Testa laikā, izmantojot bezmaksas atvērtā pirmkoda utilīti *httperf*[11] tika veikti 100’000 pieprasījumi uz Interneta vietni tā, ka vienlaicīgo pieprasījumu skaits bija 300. Attiecīgi testa dators veica 300 vienlaicīgus pieprasījumus uz Interneta vietni ar uzdevumu atgriezt pirmo dokumentu, un saņemot to aizvēra savienojumu un veica nākamo tādējādi uzturot vienlaicīgas 300 sesijas. Ar pilnu testa rezultātu iespējams iepazīties 7. pielikumā, bet īsumā iegūtie rezultāti ir sekojoši – veiksmīgi veiktie pieprasījumi ir vidēji līdz 60% gadījumu, kur vienlaicīgo savienojumu skaits, kas reāli darbojās ir vidēji 292 savienojumi sekundē. Testa ilgums vidēji 5 minūtes un 4 sekundes. Testa datora noslodze vidēji 99%, testa servera noslodze vidēji līdz 40%, toties NAT-PT maršrutētāja noslodze 99%. Šis tests viennozīmīgi nenorāda uz to, ka tieši maršrutētājs bija vājākais ķēdes posms, bet ir redzams, ka tas bija viens no vājākajiem. Secinājums no šāda testa ir, ka iespējams izvietot Interneta vietni šādā slēgumā, ja tai paredzēto vienlaicīgo apmeklētāju skaits būs zem 200 vienlaicīgiem apmeklētājiem sekundē. Skaitlim tuvojoties 300, daļa apmeklētāju varētu izjust nekorektu mājas lapas darbību vai pat pārtraukumus saziņai ar to. Attēlā 2.3.2.1 redzams IP pakešu daudzums sekundē, kad Httperf tests tikai veiks ar dubultu pieslēgumu skaitu – 20000. kā redzams testa ilgums ir nedaudz pāri 10 minūtēm un vidējais pakešu skaits sekundē ir nedaudz virs 3 tūkstoš paketēm sekundē, kas nozīmē, ka viena savienojuma izveidei un Interneta vietnes lapas lejupielādēšanai ir nepieciešamas vismaz 10 IP paketes.

2.4 Plašāk pazīstamo aplikāciju un iekārtu atbalsts IPv6 protokolam

Maģistra darba praktiskās daļas izstrādes procesā vairakkārt bija situācija, kad daļa aplikāciju vai tīkla iekārtu ne tikai nespēja darboties IPv6 tīkla vidē, bet tai arī nav paredzētas. Tādēļ veicot nelielu aptauju savu darba kolēģu un sadarbības partneru ietvaros, tika noskaidrotas plašāk un biežāk izmantotās aplikācijas un rīki, kā arī fiziskās iekārtas, kurām būtu vēlams IPv6 atbalsts.



2.3.2.1. att. **Httperf testa laikā noslodze uz tīkla interfeisu (paketes sekundē)**

2.4.1. Operētājsitēmas ar IPv6 atbalstu.

Neapšaubāmi viena no visvairāk izmantotām operētājsistēmām vēl joprojām ir Microsoft Windows XP. No aktuālām sistēmām darba stacijām ir Vista, 7, kā arī serveru sistēmas attiecīgi 2000., 2003. un 2008. Vecākajās operētājsistēmās no ražotāja Microsoft nav iestrādāts IPv6 atbalsts, jo to izstrāde notika pirms IPv6 protokola apstiprināšanas, līdz ar to, lai lietotu IPv6, piemēram, darba stacijā ar Windows XP operētājsistēmu, ir nepieciešams spraudnis. Jaunākajos atjauninājumos tas jau ir iekļauts, atliek tikai iespējot šo funkciju. Līdzīgi ir ar servera instalācijām – 2000. un 2003. servera instalācijām nepieciešamas papildus darbības – spraudņu instalēšana un iespējošana, lai iegūtu atbalstu IPv6 protokolam. Toties darba staciju versijām Vista un 7, tāpat kā 2008. serverim IPv6 ir ieslēgts pēc noklusējuma un nav nepieciešamas nekādas papildus darbības tā lietošanai paralēli IPv4 tīklam. Lai izmantoto tunelēšanas

pakalpojumus ir nepieciešama papildus tuneļu iespējošana, bet tas nepieciešams, lai iegūtu tiešu pieslēgumu IPv6 tīklam no konkrētas darba stacijas vai servera, apejot lokālo tīklu.

Kā otru lielu sadaļu operētājsistēmu sarakstā var minēt Unix viedīgās sistēmas, kuras sevī ietver gan pēdējā laikā popularitāti ieguvušās Linux sistēmas, gan BSD sistēmas un arīdzan Mac OS. Linux sistēmām, kas uzmanto linux kerneli ar versijas numuru 2.6.x ir atbalsts IPv6 protokolam jau kerneļa līmenī. Atkarībā no konkrētās Linux distribūcijas šis atbalsts var būt pieejams pēc noklusējuma, vai arī nepieciešamas papildus darbības – spraudņu instalācija un iespējošana. Jebkurā gadījumā jaunākajām Linux distribūcijām ir pieejams IPv6 protokola atbalsts. BSD sistēmas ir zināmas kā daudz konservatīvākas, līdz ar to jaunākās tehnoloģijas šajās sistēmās parādās daudz vēlāk, bet arī šajās sistēmās ir pieejams IPv6 protokola atbalsts. Mac OS operētājsistēma ir vēsturiski izveidota no BSD sistēmas, vēlāk papildināta ar daļām no NetBSD un FreeBSD sistēmām, bet tik un tā veidota slēgta atšķirībā no pārējām BSD sistēmām. Arī Mac OS pēdējās versijās Mac OS X 10.5 un Mac OS X 10.6 atbalsta IPv6 protokolu.

Mūsdienu tehnoloģiju vidē par operētājsistēmām var runāt ne tikai personālo datoru vai serveru ietvaros, lielai daļai pasaulē strādājošo telefonu ir savas operētājsistēmas, kas pēc darbspējas un parametriem atbilst personālo datoru sistēmām pirms 10 – 15 gadiem. Tieši viena no telefonu vai mobilo ierīču operētājsistēmu izveidotājām kompānija Google ar savu produktu Android OS apgalvo, ka tuvāko divu gadu laikā eksistēs vairāk kā miljards Android OS mobilās ierīces. Tieši šī iemesla dēļ Google attīsta IPv6 servisus gan datoru lietotājiem, gan mobilo ierīču lietotājiem. Tāpat Google veic IPv6 atbalsta iestrādi savā darba stacijām paredzētajā operētājsistēmā ChromiumOS. Apple produkts IPhone arī ir pieskaitāms pie jaunākās paaudzes sakaru ierīcēm, tas darbojas uz iPhoneOS, kas teorētiski ir lielās operētājsistēmas MacOS limitēta versija. Jaunākajā iPhoneOS, sākot no 4.0 versijas, ir pieejams IPv6 atbalsts. IPv6 protokola atbalsts tiek iestrādāts arī jaunākajās Symbian operētājsistēmas versijās, arī limitētā versijā pieejams Microsoft Windows Mobile sakaru ierīcēm.

Apkopojums par populārāko operētājsistēmu atbalstu un gatavību darboties IPv6 tīklā ir redzams tabulā 2.4.1.1.

Nr. p.k.	Operētājsistēmas nosaukums	IPv6 gatavība	IPv6 tunelēšanas iespējas

Populārākās Darba staciju un Serveru sistēmas.			
1.	BSD sistēmas (OpenBSD, FreeBSD un NetBSD)	Pilnībā atbalsta IPv6	OpenBSD neatbalsta 6to4 tunelēšanas iespēju.
2.	Apple Mac OS X	Nav pieejams DHCPv6	Pieejamas visas tunelēšanas iespējas.
3.	Linux kernel 2.6.x	Pilnībā atbalsta IPv6	Pieejams visas tunelēšanas iespējas
4.	Microsoft Windows XP, Vista un 7	Atbalsta IPv6 (nav datu par Windows 7 ugunsmūra atbalstu)	Visas tunelēšanas iespējams pieejamas Windows Vista, XP neatbalsta PPPoE, PPPo6, nav ziņu par atbalstu no Windows7
5.	Solaris/Open Solaris	Pilnībā atbalsta IPv6	Pieejamas visas tunelēšanas iespējas.
Populārākās sakaru un mobilo ierīču operētājsistēmas.			
1.	Android OS	Atbalsta IPv6 sākot ar versiu 2.1	
2.	BlackBerry OS	Nav IPv6 atbalsts	
3.	iPhone OS	Atbalsta IPv6 sākot ar versiju 4.0	
4.	Symbian	Atbalsta IPv6 sākot ar versiju 7.0	
5.	Windows Mobile	Atbalsta IPv6 sākot ar versiju 5.0	

2.4.1.1. tabula. **Populārāko operētājsistēmu IPv6 protokola atbalsts.**

2.4.2. Tīkla iekārtu atbalsts IPv6

Izvēloties tīkla iekārtu mazos birojos vai mājas vajadzībām, lietotāja galvenās intereses ir samērīga cena un maksimāli pieejams plašs iespēju spektrs. Bezvadu tīkls 802.11n standartā jau

ir ierasta lieta. No augstāka līmeņa ražotājiem pieejamie risinājumi maziem birojiem vai mājas birojiem cenas ziņā tomēr vairākkārtīgi pārsniedz šim spektram specializējošos tīkla iekārtu ražotājus. Cisco Systems piedāvā zemā gala maršrutētājus ar bezvadu tīkla interfeisiem, kas ir 800 sērijas iekārtas. Funkcionalitātes ziņā tās gandrīz neatšķiras no lielajām Cisco iekārtām, tikai bez servisu sniedzēju funkcionalitātēm maršrutētājos. Alternatīva ir specializēti SPHP tipa maršrutētāji, kas paredzēti šim klientu segmentam. Populārākie ražotāji ir Linksys, kurš šobrīd jau ir Cisco paspārnē, Bufffalo, Netgear, D-Link, Asus, Zyxel un TP-Link. Katram no šiem ražotājiem ir dažādi produkti, no kuriem ir daļa, kas kaut kādā ziņā atbalsta IPv6. Papildus jau esošai ražotāja programmatūrai, daļā no minētajiem maršrutētājiem iespējams instalēt uz Linux kerneli bāzētu operētājsistēmu DD-WRT [15]. Izmantojot šo operētājsistēmu tiek iegūtas papildus konfigurēšanas iespējas, kas noklusētajā versijā ir nepieejamas. Tāpat izmantojot parastu darba staciju var veidot maršrutētāju no Unix operētājsistēmas, vai jau iepriekš pieejamām sagatavēm, kas bāzētas uz kādu no Unix sistēmām. Kā vienu no šādām izstrādnēm var minēt MoNoWall [16], kas veidots uz FreeBSD operētājsistēmas, izveidojot tam web bāzētu, intuitīvu lietotāja saskarni. Kā savdabīgu risinājumu var minēt Latvijā veidotu maršrutētāju operētājsistēmu Mikrotik RputerOS [17], kas pieejama kopā jau ar aparatūras risinājumiem vai iespējama tās instalācija uz darba stacijas vai servera iekārtas. Tabulā 2.4.2.1. ir redzams apkopojums par autoram zināmiem maršrutētājiem un to atbalstu IPv6 protokolam.

Nr.p.k	Ražotājs, modelis	IPv6 atbalsts	IPv6 tunelēšanas atbalsts	NAT-PT atbalsts
1.	Asus	Nav pieejams ar oriģinālo programmatūru	N/A	N/A
2.	Buffalo	Bezvadu maršrutētājs WZR-AG300NH	Nav pieejams ar oriģinālo programmatūru	N/A
3.	Cisco	Sākot ar IOS versiju 12.2.x	Sākot ar IOS versiju 12.2.x	Sākot ar IOS versiju 12.2.x
4.	D-Link	Pieejams atbalsts jaunākajos maršrutētājos: DI-784	Pieejams atbalsts jaunākajos maršrutētājos: DI-784	Nav pieejams

		abg, DI-524 bg, DI-624 bg u.c.	abg, DI-524 bg, DI-624 bg u.c.	
5.	DD-WRT maršrutētāju programmatūra	Sākot ar versiju 24 sp1.	Sākot ar versiju 24 sp1.	Nav pieejams
6.	Linksys	Pieejams ar ražotāja programmatūru modelī WRT610N	6to4 tunelis darbojas pēc noklusējuma, un nav iespējams to izslēgt	Nav pieejams
7.	Mikrotik RouterOS	Sākot ar versiju 3.28	Sākot ar versiju 3.28	Nav pieejams
8.	MoNoWall	Atbalsts sākot ar 1.3b12 versiju	Atbalsts sākot ar 1.3b12 versiju	Nav pieejams
9.	Netgear	Nav pieejams	Tikai tuneļu padošanas (forwarding) funkcija	Nav pieejams
10.	ZyXel	Sākot ar ZyWall USG sērijas iekārtām, paredzēts visām iekārtām sākot ar 2011. gadu		

2.4.2.1 tabula. **SOHO klases aparatūras IPv6 protokola atbalsts.**

2.4.3. Programmatūras atbalsts IPv6

Maģistra darbā iepriekš tika aprakstīta dažādu programmatūru gatavību darboties IPv6 tīklā, šajā nodāļā papildus tiek aprakstītas vēl neminētās, pēc autora domām, populārākās programmas un to gatavība darboties IPv6 tīklā. Programmatūru apkopojums, sadalot pa funkcijām, ir redzams tabulā 2.4.3.1.

Nr.p.k.	Programmas nosaukums	IPv6 atbalsts
Interneta pārlūkprogrammas		

1.	Google Chrome, Internet Explorer, Mozilla Firefox, Opera, Safari	Atbalsta IPv6
Tiešsaistes saziņas rīki		
2.	MSN Messenger	Atbalsts kopš versijas 7.x
3.	ICQ	Nav atbalsts
4.	IRC chat	Ir atbalsts un pieejami IPv6 serveri
5.	Google talk	Nav atbalsta
6.	Skype	Nav atbalsta
7.	http://imo.im	Ir atbalsts – darbojas izmantojot Interneta pārlūku, atbalsta lielāko daļu saziņas rīku.
Vadības un pārvaldības rīki.		
8.	Microsoft Windows Remote Desktop	Ir atbalsts
9.	VNC Remote desktop tool.	Ir atbalsts
10.	TeamViewer remote management tool.	Nav atbalsts
Failu apmaiņas rīki		
11.	DC++	Šobrīd nav atbalsta, bet ir iestrādnes
12.	BitTorrent programmatūra	Ir atbalsts
Antivīrusu programmatūra		
13.	Kaspersky Internt Security	Ir atbalsts sākot ar 7.0 versiju
14.	AVG	Ir atbalsts
15.	Avasts Antivirus	Šobrīd nav, bet ir paredzēts nākotnē.

Secinājumi

Mūsdienās Interneta vide sniedz gan izklaidi, gan komunikācijas, gan darba iespējas. Arvien vairāk un vairāk iekārtu tiek pieslēgtas globālajam tīmeklim gan lai sazinātos ar noteiktiem resursiem tajā, gan lai būtu sasniedzamas no tā. Tehnoloģijai attīstoties šādas iekārtas ir panākušas sākotnējās prognozes par nepieciešamo adresācijas daudzumu IPv4 Interneta vidē. Nākotnes plāni paredz vēl vairāk Interneta videi pieslēgtu iekārtu online režīmā, kas ir novedis pie nepieciešamības pēc jaunas adresācijas izstrādes. 1996. gadā iesāktas IPv6 protokola izstrādes risina adresācijas problēmu, piedāvājot šobrīd paredzamai nākotnei pietiekamu skaitu unikālu IP adrešu. Lai arī ziņas par IPv4 brīvo IP adrešu skaita sarukšanu un IPv6 ieviešanas nepieciešamību ir apritē jau vairākus gadus, organizācijas un Interneta pakalpojumu sniedzēji nesteidzas ar šī protokola ieviešanu. Pēdējos gados gan šis process ir paātrinājies, bet salīdzinot ar IPv4 globālas tabulas izmēriem, tas pārsniedz 300 tūkstoš ierakstu. IPv6 tabula 2009.gadā saturēja ap 2000 ierakstu, uz šo brīdi ir redzami jau 3770 vidējais pieaugums vidēji ir aptuveni 50% teorētiski šiem tempiem vajadzētu augt ģeometriskā progresijā. Pesimistiskākās prognozes paredz brīvo IPv4 IP adrešu izbeigšanos, Ziemeļamerikas reģionā, jau 2011.gada martā, Eiropā 2012. gada vidū. Ja globālā Interneta adrešu izsniedzēj organizācija optimizēs IP sadali pa reģioniem, tad ar esošajiem tempiem brīvo IPv4 adrešu skaits var izbeigties līdz 2011.gada beigām. IP adresācijas izmaiņas ir neizbēgamas, jo iekārtu skaits, kas pieslēgtas kopējam tīklam, tikai palielināsies.

Darba gaitā autors izveidoja tikai IPv6 slēgumu iekšējā tīklā, kuram ir izeja uz IPv4 Interneta vidi izmantojot specializētu vārteju. Izmantojot slēgumu autors testēja reālo slēguma darboties spēju. Veiksmīgs izrādījās tests ar web servera izvietošanu IPv6 tīklā un piekļuves nodrošināšanu no IPv4 Interneta vides. Darbojas ne tikai HTTP pieprasījumu, bet arī e-pasts, gan izsūtīšanas, gan saņemšanas režīmos. Izvietotais serveris darbojas slēgumā vairāk kā mēnesis bez problēmām ir vēl joprojām pieejams, kā arī iespējams nosūtīt un saņemt e-pasta vēstules. Paralēli izvietotajam serverim autors pieslēdza savu darba staciju un mēģināja veikt savus ikdienas pienākumus caur šo specializēto slēgumu. Pamata darbības bija iespējamas, pieejama bija lielākā daļa IPv4 Interneta vietņu, nedarbojas tikai specializēti protokoli vai aplikācijas, kas izmanto šāda veida protokolus. Kā viens no lielākajiem pārsteigumiem bija Skype nespēja darboties IPv6 tīklā. Pamata testu veikšanai tika izmantota darba stacija ar Microsoft Windows 7

operētājsistēmu. Autors ikdienas darbos izmanto arī Linux, konkrētu Ubuntu 10.04 versijas operētājsistēmu, bet diemžēl darbs izmantojot šo sistēmu bija apgrūtināts. Pēc autora novērojumiem problēmas radīja esošais IPv4 protokols un tā neesamība uz citām tīkla iekārtām lokālajā tīklā, dēļ DNS pieprasījumu aiztures, visas darbības, kas veiktas no tikai IPv6 tīklā pieslēgtas Ubuntu darba stacijas bija ar 5 sekunžu aizturi. Bet visumā pieejamais resursu daudzums sakrita ar Windows darba stacijas iespējām. Diemžēl autoram nebija iespējas reālajā dzīvē notestēt Mac OS operētājsistēmas darbību šādā slēgumā, bet pamatojoties uz teorētisko izpēti var apgalvot, ka šai sistēmai arī būtu jāstrādā šāda tipa slēgumā.

Jau praktiskajā daļā pieskaroties un teorētiskajā daļā turpinot autors veica dažādu, pēc viņa domām, populārāko aplikāciju atbalstu IPv6 videi. Kā jau minēts darba gaitā, autors bija spējīgs gandrīz pilnvērtīgi darboties, neievērojot starpību starp IPv4 un IPv6 protokolu darbībām lokālajā tīklā. Autora ikdienas darbs saistīts ar tīkla iekārtu administrēšanu, uzraudzību un konfigurēšanu, attiecīgās aplikācijas un protokoli tādi kā FTP, SSH un Telnet pilnvērtīgi spēj darboties NAT-PT režīmā. Tāpat autors bija spējīgs, izmantojot pasta programmu, saņemt un sūtīti e-pasta ziņojumus uz serveriem, kas izvietoti IPv4 Interneta vidē. Vienīgā no autora ikdienā lietojamām aplikācijām, kas neatbalstīja jauno slēgumu bija Skype tiešsaistes sazināšanās rīks. Autors kā vienīgo alternatīvu izmantoja tiešsaistes rīku izmantošanu caur Interneta vietni https://imo.im/, kura sniedz iespēju izmantot tiešsaistes saziņas rīkus caur HTTP protokolu.

Apskatot SOHO līmeņa aparatūras atbalstu IPv6 protokolam autoram pavērsās neiepriecinošs skats. Daudzi ražotāji vēl joprojām nav veikuši nepieciešamos soļus, lai ražotu IPv6 atbalstošas iekārtas, kas samazina pieejamo iekārtu, ar attiecīgo atbalstu, loka samazināšanos. Kā alternatīvu šiem ierobežojumiem autors uzskata atvērtā pirmkoda maršrutētāju programmatūru, kuru iespējams uzinstalēt uz vairums SOHO maršrutētajiem. Izmantojot DD-WRT programmatūru ir pieejamas pamata IPv6 iespējas, tādās kā IPv6 maršrutēšana un tunelēšana. Diemžēl NAT-PT protokola atbalsts nav pieejamas uz šādas klases iekārtām. Autora slēgumā izmantotā ražotāja Cisco Systems maršrutētāju klāstā ir arī salīdzinoši mazjaudīgākas iekārtas ar līdzvērtīgu funkcionalitāti, bet cenu ziņā tās nav samērojamas ar mazu biroju vai mājas pieslēgumiem paredzētiem maršrutētājiem.

Aplikāciju vidū ir novērojamas pozitīvākas iezīmes, lielākoties ir atrodamas aplikācijas konkrētu darbību veikšanai, tiešā vai savādākā veidā atbalsta IPv6 tīklu. Diemžēl eksistē arī aplikācijas, kurām nav alternatīvu, un kurās nav iestrādātas IPv6 atbalsts. Pēc autora pieredzes, ir iespējams, atsakoties no zināmiem principiem un vēlmēm, veiksmīgi darboties Interneta vidē arī izmantojot IPv6 protokolu. Diemžēl liela daļa specializēto protokolu nedarbojas IPv6 tīklā vai ari tiem nav atbalsta NAT-PT translējošajā iekārtā. Bet populārākās datu apmaiņas vai datu straumēšanas funkcijas, tādas kā video un audio, jeb Interneta televīzija un Interna radio – ir pieejamas. Tāpat ir pieejams šobrīd populārākais un Interneta datu plūsmu visvairāk noslogojošais protokols BitTorrent, konkrēti ar klientu uTorrent autors spēja lejupielādēt izvēlētās datnes un spēja ar tām arī dalīties.

Izveidojot 6to4 tuneli līdz sava Interneta pakalpojumu sniedzēja tuvākajam IPv6 uzturošam maršrutētājam, autors bija veicis visus priekšnoteikumus tikai IPv6 Interneta vides lietošanai. Nomainot DNS servera konfigurāciju no IPv4 tīkla vidē esoša servera uz IPv6 DNS serveri un neizmantojot DNS-ALG funkcionalitāti uz Interneta vārtejas, autors veica praktisku IPv6 Interneta vides eksperimentu. Diemžēl, maz pieejamās informācijas dēļ par esošajām IPv6 atbalstošām Interneta vietnēm, šī Interneta pieredze bija skopa. Autors veiksmīgi atvēra meklētāja Google mājas lapu ipv6.google.com, tāpat veiksmīgi tika atvērta Cisco Systems Interneta vietne IPv6 tīklam – www.ipv6.cisco.com. Kā arī Eiropas Interneta reģistra specializēto Interneta vietni www.ipv6actnow.com. Pretēji pieejamai informācijai, populārās sociālās vietnes facebook IPv6 Interneta vietnes lapa www.ipv6.facebook.com , nebija pieejama. Autoram nebija pieejama informācija par vēl kāda populāras IPv4 Interneta vietnes atbalstu vai kopiju IPv6 Internetā. Kompānija Google, jau piedāvā savus produktus IPv6 tīklam, un šobrīd nodarbojas ar video straumēšanas vietnes Youtube.com pielāgošanu. Secinājums par IPv6 Internetu pēc autora domām ir, ka neskatoties uz visiem priekšnoteikumiem, kam vajadzētu mudināt cilvēkus pārriet uz šo protokolu un veikt jaunās izstrādes šai virzienā, tomēr IPv6 tīkls ir salīdzinoši tukšs. Pēc loģikas un personīgās pieredzes spriežot, kamēr IPv6 tīklā nebūs pieejams vērā ņemams resursu daudzums, tikmēr pāreja uz to būs gausa. Autors redz divus risinājumus šai problēmai, kur pirmais ir, ja kāds populārs un plaši izmantots resurss spertu izšķirošu soli un piedāvātu savus pakalpojumus tikai IPv6 tīklā, vai minimizētu tos IPv4 tīklam, tad tas būtu kā pirmais grūdiens lavīnveidīgai pārejai uz IPv6, otrais variants būtu vecmodīga cilvēku piespiedu pārvietošana uz

jauno Interneta vidi. Cilvēki rakstura ziņā ir konservatīvi un vienmēr atradīsies daļa, kura neuzskatīs par vajadzīgu mainīties, ja iespējams izdzīvot esošajā situācijā, uz šo brīdi IPv4 Interneta vide vēl attīstās straujiem tempiem un vienīgais, kas iet negatīvā virzienā ir brīvo IPv4 IP adrešu skaits. Neskatoties uz to Interneta pakalpojumu sniedzējiem vēl ir pietiekoši brīvo adrešu, lai kādu brīdi spētu apmierināt pieaugošo nepieciešamību pēc IPv4 adresēm. Situācija krasi varētu mainīties, kad plašāk būtu pieejamas sakaru ierīces ar IPv6 atbalstu un mobilo telefonu sakaru sniedzēji pārietu no šobrīd pielietotās IPv4 adrešu translācijas uz publisku IPv6 adresi katram Interneta lietotājam. Šobrīd, piemēram, visi LMT klienti lieto 3 IPv4 C klašu apakštīklus, kas summāri ir nedaudz virs 750 IP adresēm, turpretim ar vienu /112 IPv6 prefiksu šo skaitli varētu palielināt gandrīz 100 reizes. Pēc šobrīd pieņemtās politikas Interneta pakalpojumu sniedzējiem un citām telekomunikāciju organizācijām tiek piešķirti /32 prefiksi, kas ir gana liels skaitlis, lai izdalītu pa IPv6 adresei katrai tīkla iekārtai Latvijas teritorijā.

Kā visaptverošu secinājumu var minēt, ka šobrīd pieejamais IPv6 Internets un protokola atbalsts ir salīdzinoši niecīgs, konkrētos skaitļos – tikai 0.2% no pieprasījumiem meklētāja Google ir veikti no IPv6 atbalstošas darba stacijas un tikai 40% no tiem ir veikti no tikai IPv6 tīkla, neizmantojot papildus tunelēšanas pakalpojumus. Attiecīgi cilvēki kā lietotāji, tīkla uzturētāji un servisu piegādātāji vēl nav gatavi pilnībā atteikties no IPv4, bet ir novērojamas pozitīvas tendences pieejamo IPv6 tīklu skaita ziņā, kas ir audzis par 50% kopš 2009. gada, un nav redzamu iemeslu, lai tas tā neturpinātu augt. Pēc autora domām ir nepieciešams tikai viens sākotnējais solis, lai pārnestu kritisko masu uz jaunā protokola vidi un pārējais ir laika jautājums, jo visi priekšnosacījumi ir izpildīti.

Pateicība

Autors izsaka pateicību Sia Latnet Serviss un Sia Monitoringa centrs, par iespēju savā darba praktiskajā daļā izmantot tīkla infrastruktūru un iekārtas, kā arī IPv4 un IPv6 resursus.

Izmantotā literatūra

1. Elektroniskie informācijas avoti.

1. Wikipedia [tiešsaiste] –IP 4. Versijas protokola apraksts un galvenie raksturlielumi [atsauce 13.11.2010]. Pieejams: http://en.wikipedia.org/wiki/IPv4

2. Wikipedia [tiešsaiste] – IP 6. Versijas protokola apraksts un galvenie raksturlielumi [atsauce 13.11.2010]. Pieejams: http://en.wikipedia.org/wiki/IPv6

3. Wikipedia [tiešsaiste] – Informācija par Interneta pakalpojumu sniedzēju Free [atsauce 13.11.2010]. Pieejams: http://en.wikipedia.org/wiki/Free_%28ISP%29

4. Cisco Systems inc [tiešsaiste] – Ražotāja apraksts un pamatvirzieni NAT-PT konfigurācijas izveidei [atsauce 01.11.2010]. Pieejams: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-nat_trnsln_ps6350_TSD_Products_Configuration_Guide_Chapter.html

5. Cisco Systems inc [tiešsaiste] – Ražotāja apraksts un pamatvirzieni 6to4 tuneļa konfigurācijas izveidei [atsauce 01.11.2010]. Pieejams: http://www.cisco.com/en/US/tech/tk872/technologies_configuration_example09186a00801f3b4f.shtml

6. Skype instant messaging tool [tiešsaiste] – Izstrādātāja mājas lapa [atsauce 01.11.2010]. Pieejams: http://www.skype.com/intl/en/home

7. Skype oficiālais forums [tiešsaiste] – Izstrādātāja Interneta vietnē pieejamā informācija par IPv6 atbalstu [atsauce 01.11.2010]. Pieejams: http://forum.skype.com/index.php?showtopic=632023&st=

8. Teamviewer free remote access and remote desktop sharing over the Internet [tiešsaiste] – Izstrādātāja mājas lapa [atsauce 20.11.2010]. Pieejams: http://www.teamviewer.com/index.aspx

9. RealVNC – Cros-platform remote control solution [tiešsaiste] – Izstrādātāja mājas lapa [atsauce 20.11.2010]. Pieejams: http://www.realvnc.com/vnc/index.html

10. The VNC family of Remote Control Applications [tiešsaiste] – uz VNC bāzētie attālinātas vadības rīki [atsauce 20.11.2010]. Pieejams: http://ipinfo.info/html/vnc_remote_control.php

11. Httperf – web testing tool [tiešsaiste] – Rīka aprakstam un lejupielādes saitēm, izveidotā mājas lapa [atsauce 20.11.2010]. Pieejams: http://www.hpl.hp.com/research/linux/httperf/

12. RIR Delegations & RIPE NCC Allocations [tiešsaiste] – statisktika par izdalītajiem Interneta resursiem (IPv4, IPv6 un AS numuriem) sadalījumā pa valstīm un reģioniem [atsauce 25.11.2010]. Pieejams http://www-public.int-evry.fr/~maigron/RIR_Stats/RIR_Delegations/Delegations/IPv6/LV.html#RIPENCC

13. Latvian Internet Exchange [tiešsaiste] – LIX Interneta vietne [atsauce 25.11.2010]. Pieejams: http://lix.lv/site/members

14. NIC [tiešsaiste] – paziņojums par atbalstu IPv6 NIC Interneta vietnē [atsauce 25.11.2010]. Pieejams: http://www.nic.lv/resource/show/116

15. DD-WRT [tiešsaiste] – DD-WRT Interneta vietne [atsauce 30.11.2010]. Pieejams: http://www.dd-wrt.com/site/index

16. Monowall [tiešsaiste] – MoNoWall Interneta vietne [atsauce 30.11.2010]. Pieejams: http://m0n0.ch/wall/

17. Mikrotik routers and wireless [tiešsaiste] – Mikrotik Interneta vietne, Router OS un citas Mikrotik aplikācijas [atsauce 30.11.2010]. Pieejams: http://www.mikrotik.com

Pielikumi

1. pielikums

NAT-PT maršrutētāja konfigurācija, statiska translēšana.

```
Building configuration...
Current configuration : 1419 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname NAT-PT
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ip cef
!
ip domain name test.org
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 nat
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:FFFF::1/64
 ipv6 nat
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ipv6 nat v4v6 source 10.0.0.10 2010::10
ipv6 nat v6v4 source 2010:FFFF::10 192.168.0.10
```

```
ipv6 nat prefix 2010::/96
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

2. pielikums

NAT-PT maršrutētāja konfigurācija, dinamiska translācija bez DNS-ALG.

```
Building configuration...
Current configuration : 1419 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname NAT-PT
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ip cef
!
ip domain name test.org
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface GigabitEthernet0/0
 ip address 85.254.44.200 255.255.255.192
 duplex auto
 speed auto
 ipv6 nat
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:FFFF::1/64
 ipv6 nat
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 85.254.44.254
!
ip http server
no ip http secure-server
!
ipv6 nat v6v4 source list ipv6_nat pool v4pool
```

```
ipv6 nat v6v4 pool v4pool 85.254.52.0 85.254.52.255 prefix-length 24
ipv6 nat prefix 2010::/96 v4-mapped ipv6_nat
!
ipv6 access-list ipv6_nat
 permit ipv6 any 2010::/96
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
End
```

3. pielikums

NAT-PT maršrutētāja konfigurācija, dinamiska translācija ar DNS-ALG.

```
Building configuration...
Current configuration : 1419 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname NAT-PT
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!

no ip cef
!
ip domain name test.org
ip name-server 85.254.44.1
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface GigabitEthernet0/0
 ip address 85.254.44.200 255.255.255.192
 duplex auto
 speed auto
 ipv6 nat
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:FFFF::1/64
 ipv6 nat
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 85.254.44.254
!
ip http server
no ip http secure-server
```

```
!
ipv6 nat service DNS
ipv6 nat v4v6 source 159.148.60.20 2010::20
ipv6 nat v6v4 source list ipv6_nat pool v4pool
ipv6 nat v6v4 pool v4pool 85.254.52.0 85.254.52.255 prefix-length 24
ipv6 nat prefix 2010::/96
!
ipv6 access-list ipv6_nat
 permit ipv6 any 2010::/96
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

4. pielikums

NAT-PT maršrutētāja konfigurācija, reālistiska konfigruācija.

```
Building configuration...
Current configuration : 1419 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname NAT-PT
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ip cef
!
ip domain name test.org
ip name-server 85.254.44.1
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface GigabitEthernet0/0
 ip address 85.254.44.200 255.255.255.192
 duplex auto
 speed auto
 ipv6 nat
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:FFFF::1/64
 ipv6 nat
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 85.254.44.254
!
ip http server
no ip http secure-server
!
```

```
ipv6 nat service DNS
ipv6 nat v6v4 source list ipv6_nat pool v4pool
ipv6 nat v6v4 source 2010:FFFF::10 159.148.19.4
ipv6 nat v6v4 pool v4pool 85.254.52.0 85.254.52.255 prefix-length 24
ipv6 nat prefix 2010::/96 v4-mapped ipv6_nat
!
ipv6 access-list ipv6_nat
 permit ipv6 any 2010::/96
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
End
```

6to4 tuneļa konfigurācija maršrutētājs R1.

```
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IPv6_1_border
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2002:A00:101::/128
 tunnel source 10.0.1.1
 tunnel mode ipv6ip 6to4
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:1::1/64
!
interface FastEthernet0/1
 ip address 10.0.1.1 255.255.255.0
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.0.1.254
```

```
no ip http server
no ip http secure-server
!
logging alarm informational
ipv6 route 2002::/16 Tunnel0
ipv6 route 2010:2::/64 2002:A00:201::
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

6to4 tuneļa konfigurācija maršrutētājs R2.

```
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IPv6_2_border
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2002:A00:201::/128
 tunnel source 10.0.2.1
 tunnel mode ipv6ip 6to4
!
interface FastEthernet0/0
 ip address 10.0.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:2::1/64
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.0.2.254
no ip http server
```

```
no ip http secure-server
!
logging alarm informational
ipv6 route 2010:1::/64 2002:A00:101::
!
control-plane
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
End
```

Httperf, noslodzes testu rezultātu izvads.

```
andriss@vafele:~$ httperf --server testbed.mc.net.lv --port 8080 --rate 300 --
num-conn 100000 --num-call 1 --timeout 5
httperf --timeout=5 --client=0/1 --server=testbed.mc.net.lv --port=8080 --
uri=/ --rate=300 --send-buffer=4096 --recv-buffer=16384 --num-conns=100000 --
num-calls=1
Maximum connect burst length: 5

Total: connections 99266 requests 56887 replies 56626 test-duration 338.246 s

Connection rate: 293.5 conn/s (3.4 ms/conn, <=1022 concurrent connections)
Connection time [ms]: min 9.0 avg 1962.3 max 9272.3 median 1307.5 stddev
1699.5
Connection time [ms]: connect 1264.3
Connection length [replies/conn]: 1.000

Request rate: 168.2 req/s (5.9 ms/req)
Request size [B]: 70.0

Reply rate [replies/s]: min 154.4 avg 168.1 max 180.8 stddev 4.6 (67 samples)
Reply time [ms]: response 113.8 transfer 584.4
Reply size [B]: header 241.0 content 21812.0 footer 0.0 (total 22053.0)
Reply status: 1xx=0 2xx=56626 3xx=0 4xx=0 5xx=0

CPU time [s]: user 3.05 system 331.80 (user 0.9% system 98.1% total 99.0%)
Net I/O: 3616.9 KB/s (29.6*10^6 bps)

Errors: total 43374 client-timo 42640 socket-timo 0 connrefused 0 connreset 0
Errors: fd-unavail 734 addrunavail 0 ftab-full 0 other 0

andriss@vafele:~$ httperf --server testbed.mc.net.lv --port 8080 --rate 300 --
num-conn 100000 --num-call 1 --timeout 5
httperf --timeout=5 --client=0/1 --server=testbed.mc.net.lv --port=8080 --
uri=/ --rate=300 --send-buffer=4096 --recv-buffer=16384 --num-conns=100000 --
num-calls=1
Maximum connect burst length: 3

Total: connections 99099 requests 54948 replies 54619 test-duration 338.330 s

Connection rate: 292.9 conn/s (3.4 ms/conn, <=1022 concurrent connections)
Connection time [ms]: min 8.4 avg 1894.3 max 8882.0 median 1115.5 stddev
1698.7
Connection time [ms]: connect 1201.7
Connection length [replies/conn]: 1.000

Request rate: 162.4 req/s (6.2 ms/req)
```

```
Request size [B]: 70.0

Reply rate [replies/s]: min 148.6 avg 162.1 max 173.6 stddev 5.4 (67 samples)
Reply time [ms]: response 114.6 transfer 577.7
Reply size [B]: header 241.0 content 21812.0 footer 0.0 (total 22053.0)
Reply status: 1xx=0 2xx=54619 3xx=0 4xx=0 5xx=0

CPU time [s]: user 2.56 system 333.20 (user 0.8% system 98.5% total 99.2%)
Net I/O: 3487.8 KB/s (28.6*10^6 bps)

Errors: total 45381 client-timo 44480 socket-timo 0 connrefused 0 connreset 0
Errors: fd-unavail 901 addrunavail 0 ftab-full 0 other 0
```

Maģistra darbs „IPv6 praktiskas ieviešanas problēmu izpēte” izstrādāts Latvijas Universitātes Datorikas nodaļā

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai. Piekrītu sava darba publicēšanai Internetā.

Autors: Andris Segliņš _____

Ar savu parakstu apliecinu, ka esmu lasījis augstāk minēto maģistra darbu un atzīstu to par **p i e m ē r o t u / n e p i e m ē r o t u** (nevajadzīgo svītrot) aizstāvēšanai Latvijas Universitātes datorzinātņu maģistrantūrā.

Darba vadītājs: Dr.sc.comp. Guntis Bārzdiņš _____

Darbs iesniegts **maģistratūras sekretariātā** _____.

Ar šo apliecinu, ka darba elektroniskā versija ir augšupielādēta LU informatīvajā sistēmā.

Studiju metodiķe: _____

Recenzents: _____

Darbs aizstāvēts maģistra gala pārbaudījuma komisijas sēdē

_____ prot.Nr. _____, vērtējums _____

Komisijas sekretārs(e): _____