РЕАЛИЗАЦИЯ НА ПРОТОКОЛ IPv6 В УНИВЕРСИТЕТСКА МРЕЖА

Веселин Колев[1], Стефан Димитров[2], Николай Николов[3], Георги Найденов[4]

[1]Hebrew University, Jerusalem, Israel, e-mail: vlk@lcpe.uni-sofia.bg
[2]Софийски университет "Св. Кл. Охридски", 1164-София, e-mail: stefan@ucc.uni-sofia.bg
[3]Софийски университет "Св. Кл. Охридски", 1164-София, e-mail: nikolay.nikolov@ucc.uni-sofia.bg
[4]Софийски университет "Св. Кл. Охридски", 1164-София, e-mail: georgi@ucc.uni-sofia.bg

РЕЗЮМЕ. В доклада е предложена методика за приложение на протокол IPv6, който да работи паралелно със съществуващия протокол IPv4 в рамките на университетска мрежа. Реализирани са рефлекторна схема за маршрутизация по протокол BGP, услугите DNS, електронна поща и уеб.

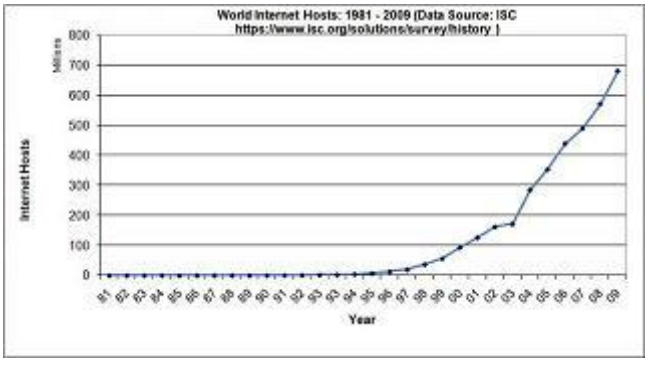
IMPLEMENTATION OF IPv6 PROTOCOL IN A UNIVERSITY NETWORK

Vesselin Kolev[1], Stefan Dimitrov[2], Nikolay Nikolov[3], Georgi Naydenov[4]
[1]Hebrew University, Jerusalem, Israel, e-mail: vlk@lcpe.uni-sofia.bg
[2]Софийски университет "Св. Кл. Охридски", 1164-София, e-mail: stefan@ucc.uni-sofia.bg
[3]Софийски университет "Св. Кл. Охридски", 1164-София, e-mail: nikolay.nikolov@ucc.uni-sofia.bg
[4]Софийски университет "Св. Кл. Охридски", 1164-София, e-mail: georgi@ucc.uni-sofia.bg

ABSTRACT. In the paper presented methodology is proposed for the application of IPv6 protocol working in parallel with the existing IPv4 protocol. This is the dual-stack scheme. Route reflector scheme for BGP routing within the network and the DNS, email and web services are implemented

Въведение

Протоколът IPv4 (RFC 791), по който се осъществява маршрутизацията и адресацията на мрежови устройства в съвременните компютърни мрежи, е разработен през 1970-те години. Той е с дължина 32 бита, което ограничава адресното пространство до 2^{32}. Стръмно експоненциалният растеж на броя на възлите (хостовете) в Интернет от средата на 1990-те (фиг. 1) доведе до тяхото изчерпване. В момента се раздават последните блокове с IPv4 адреси.



Фиг. 1 **Растеж на Интернет хостовете през годините**

Очаква се в следващите години броят на хостовете да расте още по-интензивно. Предпоставка за това твърдение са развитието на мобилните комуникации от четвърто поколение, интелигентните електрически уреди (smart grid) и др. Всичко това предполага огромно търсене на IP адреси, което прави неотложен прехода към новата версия на протокола - IPv6.

IPv6 дефинира адреси с дължина 128 бита (RFC 4291), които са с шестнадесетична нотация за разлика от IPv4 адресите, които са с десетична (например, fe80:43e3:9095:02e5:0216:cbff:feb2:7474). Предлагат огромно, на практика неизчерпаемо, адресно пространство – 2^{128}.

Протоколът IPv6 има и други предимства:

- Автоконфигуриране (RFC 4862) - автоматично (plug-and-play) присвояване на адрес без помощта на DHCP сървър като в Ipv4.
- Заглавната част в IPv6 (header) е по-опростена спрямо IPv4, с фиксирана дължина 40 байта, като допуска до шест допълнителни „заглавия" (extension headers) (RFC 2460).
- IP security (IPSec) е част от IPv6, а не допълнителен протокол, както е в IPv4. Достатъчно е да включим две от допълнителните заглавия: Encapsulating Security Payload (ESP) и Authentication Header (AH). IPSec е задължителен атрибут в мобилната версия Mobile IPv6 и протоколите за маршрутизация;
- Mobile IPv6 (MIPv6) поддържа мобилност на мрежовите възли (роуминг), придвижване от една мрежа в друга, без да губят IP свързаност (RFC 3775). Поддържане на мобилност в IPv4 (RFC 3344) е ограничено от протокола ARP, който в IPv6 е заменен с Neighbor Discovery (RFC 4861).

◆ IPv6 по-подробно дефинира качеството на услугите (QoS) и приоритетизиране на трафика чрез полетата Traffic Class и Flow Label в заглавната част, което е особено полезно за приложения в реално време като IP телефония (VoIP), видеоконфернеции и др.

IPv6 не е обратно съвместим с IPv4, което налага промени в мрежовата инфраструктура и системи.

Механизми за преход от IPv4 към IPv6

Преходът от IPv4 към IPv6 ще отнеме значително време. Затова се налага да се прилагат механизми, осигуряващи съвместното съществуване на чисто-IPv4 възли, чисто-IPv6 и двустекови (dual stack) IPv4/IPv6 възли.

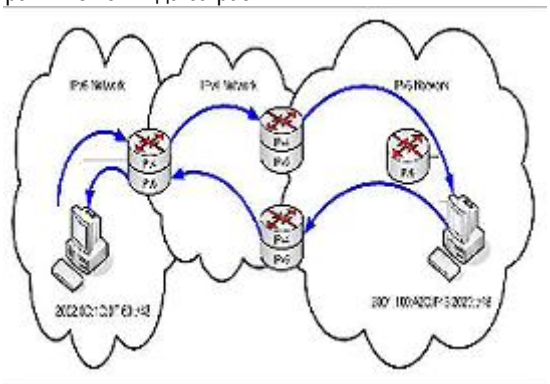
Механизмите за преход (RFC 4213) трябва да поддържат взаимодействието между IPv4 и IPv6 възлите. Те попадат в три категории:

- тунелиране;
- транслация;
- поддържане на двоен стек (dual stack).

Тунелиране

Тунелирането представлява опаковане на един протокол в друг. Тунелиращият протокол носи тунелирания протокол, за когото тунела, както и възлите, през които преминава, са прозрачни. Тунелите могат да бъдат IPv6-върху-IPv4 (вмъкване на IPv6 пакети в IPv4) или IPv4-върху-IPv6 (вмъкване на IPv4 пакети в IPv6).

На Фиг. 2 е показан общ случай на тунел. Два хоста от IPv6 мрежи могат да комуникират помежду си само през IPv4 мрежа. Всеки хост има достъп до двустеков IPv4/IPv6 маршрутизатор. Този маршрутизатор има път до друг IPv4/IPv6 маршрутизатор през IPv4 мрежа. Тези два маршрутизатора са крайните точки на тунела, където IPv6 пакета се опакова в IPv4 пакет, който се предава до другата крайна точка. Тунелът не е задължително да бъде симетричен. Възможно е във всяка от двете посоки крайните точки да са различни.



Фиг.2 **Пример на тунелиране на** IPv6 **върху** IPv4 **мрежа**.

Транслация

Транслацията предполага преобразуване на IPv4 или IPv6 пакети в друг протокол, по който те се пренасят през мрежата. Network Address Translation—Protocol Translation (NAT-PT) позволява на IPv6 и IPv4 устройства да комуникират чрез посредничеството на транслиращо устройство. Transport Relay Translator (TRT) е друг механизъм, който позволява на IPv6 хостове да комуникират с IPv4 такива чрез посредник. Но методите на транслация (IPv4 в IPv6 и IPv6 в IPv4) въвеждат нови методи за конструиране на мрежи и системи, с което внасят и нови възможности за атаки срещу мрежите и системите.

Траанслацията на протоколи не се препоръчва като дългосрочно решение по ред причини. Транслирането на IPv6 в IPv4 на първо място прави излишен прехода към IPv6. Всичките изброени по-горе предимства и нововъведения при IPv6 се губят при транслирането му в IPv4. Не се решава и проблема с изчерпването на адресното пространство в IPv4. Този механизъм е полезен до тогава, докато се налага да се комуникира с чисто-IPv4 системи.

Поддържане на двоен стек

Механизмът за преход с поддържане на двоен стек (dual stack) предполага всеки възел или хост в мрежата да има едновременно и IPv4, и IPv6 свързаност, да им бъдат присвоени и IPv4 адреси, и IPv6 адреси. Организациите използват двойния стек, когато основната част от оборудването е с dual stack възможности и се изисква бърза реализация на IPv6 свързаността. При реализация на dual stack среда трябва да се имат предвид следните моменти: споделената инфраструктура, необходимост от повече ресурси и спецификата на приложните протоколи.

IPv4 и IPv6 имат различни инфраструктури. Маршрутизацията (на мрежовия слой) и комутирането (на каналния) трябва да разпознават съответния протокол. Двойностековите среди използват повече ресурси от еднопротоколните — процесорна мощност и време, оперативна памет.

Маршрутизаторите трябва да поддържат и IPv4, и IPv6 таблици с маршрутите, както и съответните протоколи за маршрутизация. Някои от тях като RIP (RFC 2080) и OSPF (RFC 2740) изискват стартиране на отделни процеси за IPv4 и IPv6, докато BGP с въведените разширения позволява в един процес да се поддържат едновременно IPv4 и IPv6 (RFC 4760). Това предполага наложените в IPv4 схеми за филтриране и контролиране на трафика да се приложат и в IPv6.

Някои приложения са чисто-IPv4, други са чисто-IPv6, а трети - IPv4/IPv6. Хостът трябва да бъде настроен да използва точния протокол. Подреждането на записите в системата за съответствие между имена и адреси в Интернет (DNS - Domain Name System) има решаващо значение при избора на точния протокол. Приложенията са писани да запитват само A (IPv4), само AAAA (IPv6) или и A, и AAAA записи (RFC 3596).

Не трябва да се пренебрегват и средствата за обучение и квалификация на техническия персонал. На този етап хората, които имат задълбочени познания по темата са в дефицит.

Реализация на двустекова инфраструктура и услуги в университетска мрежа

От анализа в предишния абзац може да се направят следните изводи:

◆ Тунелирането внася закъснения.

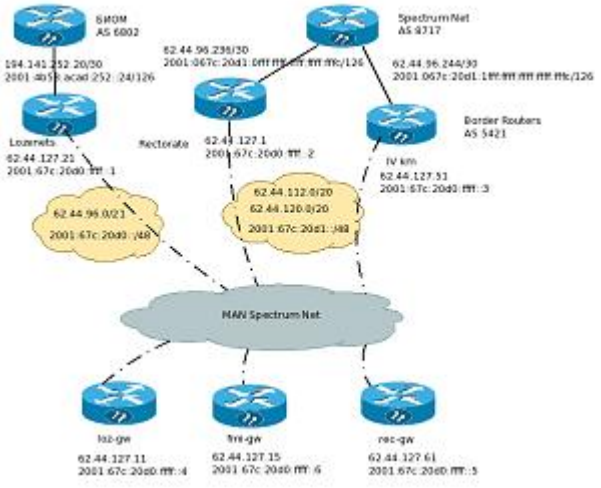
◆ При транслирането на IPv6 в IPv4 се губят предимствата на нововъведенията в IPv6.

Въпреки ресурсоемкостта си механизма с двоен стек

се явява най-подходящ при реализация на преход от IPv4 към IPv6. Можем да посочим следните предпоставки в подкрепа на това твърдение:

- Наличие на софтуер с отворен код, който реализира основните мрежови услуги (маршрутизация, DNS, електронна поща, Web) едновременно и в IPv4, и в IPv6.
- Операционните системи за потребителски станции с отворен код и последните версии на Microsoft Windows (Vista и Windows7) поддържат по подразбиране IPv6.
- Услугите се реализират прозрачно за потребителите, на тях не им трябва да знаят дали ползват IPv4 или IPv6; тук трябва да се посочи едно от подобренията в IPv6 — автоматичното раздаване на адреси.

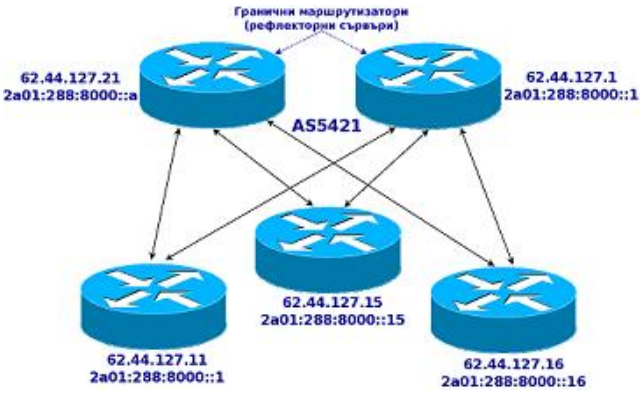
За да се реализира двустекова инфраструктура е необходимо на първо място наличието на адресно пространство в обхват, зависещ от мащабите на мрежите. IPv6 адресно пространство се получава от Интернет доставчиците (Provider Assigned — PA) или директно от регионалния регистратор, за Европа това е RIPE (Provider Independent — PI) (ripe-509). На крайни клиенти, какъвто е и даден университет, се раздават един или повече адресни блокове с префикс /48 (ripe-512). След това полученото адресно пространство се разпределя между отделните звена, като възприетата практика е блоковете да са с префикс /64. Възможно е префиксите да са по-къси, т.е блоковете да са с по-голям обхват, например /60. Префикси с по-големи дължини се присвояват на опорните мрежи и устройствата, които реализират основните мрежови услуги. Връзките от тип «точка-точка» са с префикс /126 (Фиг. 3).



Фиг. 3. **Двустекова инфраструктура в университетска мрежа**.

Динамична маршрутизация по BGP

В разглежданата университетска мрежа се прилага динамична маршрутизация по протокол BGP с въведена рефлекторна схема (RFC 4456). С помощта на рефлекторна схема се редуцира броя на сесиите между iBGP съседи и от там натоварването на процесори и комуникационни канали. Един маршрутизатор (или два за резервираност) става рефлекторен сървър, а другите – рефлекторни клиенти. Всички участници в рефлекторната схема имат IP адрес от единен адресен сегмент (напр. 62.44.127.0/25, респ. 2001:67c:20d0:ffff::/64). Всеки клиент изгражда BGP4/4+ сесия до сървъра и излъчва мрежите достижими през него и получава индиректно (през сървъра) маршрутите, излъчвани от останалите клиенти, с директно достижим следващ възел (Фиг. 4).



Фиг.4 BGP **рефлекторна схема**.

Електронна поща

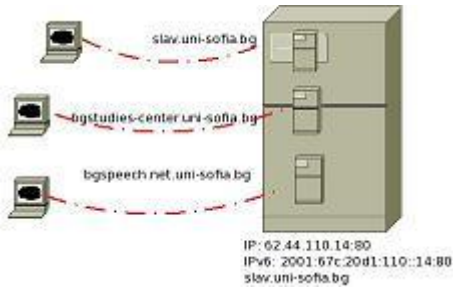
Пощенските сървъри в университетската мрежа осигуряват двупротоколна SMTP услуга, в духа на пълна IPv6 интеграция. Пакетът sendmail е компилиран с поддръжка на IPv6, което свежда IPv6 интеграцията на SMTP услугата само до въвеждане на съответните конфигурационни опции (Колев, 2008). Конфигурационният файл sendmail.cf, който демонът sendmail чете при стартирането си, се генерира от m4 макросен прототип, който по подразбиране се съхранява във файла sendmail.mc.

За да може sendmail демона да обслужва SMTP сесии, които се транспортират по протокол IPv6, е добра практика да се декларира на кой точно локален IPv6 адрес слуша демона (по подразбиране на порт 25/tcp). За да се настои sendmail демона да слуша на точно определени локални за стека IPv6 адреси, се използва опцията DAEMON_OPTIONS:

```
DAEMON_OPTIONS(`Port=smtp,Addr=62.44.109.37, Name=MTA')dnl
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
DAEMON_OPTIONS(`Port=smtp,Addr=2001:67c:20d0:10::37, Name=MTA6,
Family=inet6')dnl
DAEMON_OPTIONS(`Port=smtp,Addr=::1, Name=MTA6, Family=inet6')dnl
```

Уеб услуги

Използването на продукта с отворен код Apache (Apache, 2011) позволява да се създават уеб сървъри, чиито httpd процеси да “слушат” едновременно на IPv4 и IPv6 адрес. В зависимост от това как DNS сървъра на потребителя (клиента) «решава» (resolve) адреса на сървъра, по IPv4 или по IPv6, браузърът отваря съответната страница. И всичко това е «прозрачно» за потребителя. На Фиг. 5 е даден пример на една физическа машина, на която са инсталирани три виртуални уеб сървъри, достъпни и по IPv4 и по IPv6.



Фиг. 5 **Компютър**, **на който са инсталирани три виртуални уеб сървъра**.

Директивите, с които е показано на процеса httpd на кои портове и адреси да «слуша», са следните:

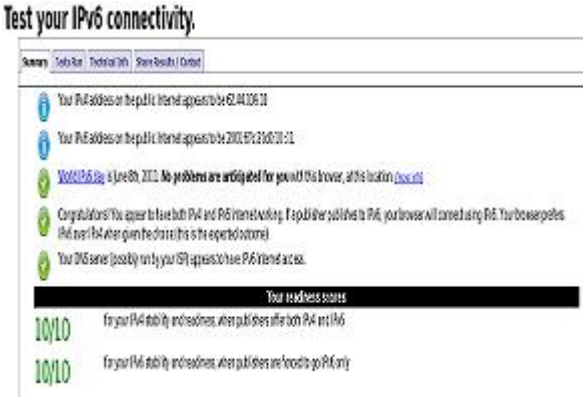
```
Listen 62.44.110.14:80
Listen [2001:67c:20d1:110::14]:80
NameVirtualHost 62.44.110.14:80
NameVirtualHost [2001:67c:20d1:110::14]:80
```

Заключение

Описаната по-горе двустекова инфраструктура е реализирана на универсални машини (често и втора употреба), работещи под управлението на операционната система с отворен код Linux, дистрибуция CentOS release 5.6 (CentOS, 2011). Пакетът за маршрутизация е Quagga Routing Software Suite (Quagga, 2011), а DNS софтуерът е BIND 9.X - Berkeley Internet Name Daemon (BIND, 2011).

Така предложеното решение осигурява напълно прозрачни по отношение на адресацията услуги с висока производителност и на ниска цена. Проведените тестове (Фиг. 6) във връзка със «Световния IPv6 Ден» на 8 юни 2011 г. (World IPv6 Day) сочат 100% подготвеност на мрежата за обслужване на потребителите и по двата протокола - IPv4 и IPv6 (test-ipv6).

Препоръчана за публикуване от
Редакционен съвет



Фиг. 6 **Проведените тестове сочат** 100% **подготвеност на мрежата**.

Литература

Колев, 2008, Настройки на пощенските концентратори на мрежата на СУ "Св. Климент Охридски" за работа с IPv6, *http://www.vesselin.org/papers/xhtml/sendmail-ipv6.html*

Apache, 2011, *http://httpd.apache.org/docs/trunk/*

BIND, 2011, *http://www.isc.org/software/bind*

CentOS, 2011, *http://www.centos.org/*

Quagga, 2011, *http://www.quagga.net/*

RFC 791, *HTTP://TOOLS.IETF.ORG/HTML/RFC791*

RFC 4291, *http://tools.ietf.org/html/rfc4291*

RFC 4862, *http://www.ietf.org/rfc/rfc4862.txt*

RFC 2460, *http://www.ietf.org/rfc/rfc2460.txt*

RFC 3775, *http://www.ietf.org/rfc/rfc3775.txt*

RFC 3344, *http://www.ietf.org/rfc/rfc3344.txt*

RFC 4861, *http://tools.ietf.org/html/rfc4861*

RFC 4213, *http://tools.ietf.org/html/rfc4213*

RFC 2080, *http://tools.ietf.org/html/rfc2080*

RFC 2740, *http://www.ietf.org/rfc/rfc2740.txt*

RFC 4760, *http://tools.ietf.org/html/rfc4760*

RFC 3596, *http://www.ietf.org/rfc/rfc3596.txt*

RFC 4456, *http://tools.ietf.org/html/rfc4456*

ripe-509, *http://www.ripe.net/ripe/docs/ripe-509*

ripe-512, *http://www.ripe.net/ripe/docs/ripe-512#assignment_multiple*

test-ipv6, *http://test-ipv6.com/*

World IPv6 Day, *http://www.worldipv6day.org/*