004.77 : 621.39

Доц. д-р **Сашо ГЕЛЕВ, Александар СОКОЛОВСКИ**

МЕХАНИЗМИ ЗА ТРАНЗИЦИЈА ОД IPv4 во IPv6

Апстракт

Без сомнение информатичките технологии станаа значаен дел од нашиот живот. Инженерските иновации значително ги подобруваат мрежните технологии и ги следат во чекор со брза адаптација на компјутерските комуникации. Од друга страна, трендот за конвергирање на сите комуникации, податоци, видео и звук, во еден единствен мрежен протокол доведува до лимитирање на ресурсите за понатамошно посвојување од страна на компјутерско комуникациските базирани сервиси.

Адресниот простор на IPv4 не може да постигне да ја услужи се поголемата побарувачка од глобално достапни IP уреди. Со трошењето на IPv4 адресниот простор и со приватниот адресен простор кој се докажува дека е неадекватен за денешните мрежи, се бара еволуирање на Интернет Протоколот во IPv6 (Интернет Протокол верзија 6).

Клучот за успешна IPv6 транзиција е компатибилноста со распространета употреба на IPv4 хостовите и рутерите. Одржувањето на компатибилноста со IPv4 паралелно со имплементирање на IPv6 ќе ја олесни задачата за транзиционирање во IPv6. Во овој труд ке бидатат наведени множество од механизми кои IPv6 хостовите може да ги имплементираат за да бидат компатибилни со IPv4 хостови и рутери.

Клучни зборови: *IPv4, IPv6, Двоен IP Слој Dual IP Layer Dual Stack), Конфигурирано тунелирање, Автоматско тунелирање на IPv6 преку IPv4.*

1. Вовед

Интернет протоколот е неконекциски ориентиран, што значи дека патеката т.е. рутата од изворот до дестинацијата не треба да се воспостави пред пакетите (со податоците) да влезат во мрежата. Можно е секој пакет да си има своја различна независна рута од рутата на претходниот пакет кој има иста изворна и дестинациска IP адреса. IP не гарантира дека пакетите ќе пристигнат во оригиналната секвенца ниту пак дека воопшто ќе пристигнат до нивната дестинација.

Засега постојат две верзии на IP протоколот, и тоа: IP version 4 (IPv4), која е опишана во RFC 791, и IP version 6 (IPv6), опишана во RFC 1883-1887. Описот на IP ги содржи следниве многу значајни елементи:

- IP ги дефинира основните податочни единици кои можат да се испратат преку Интернет т.е. IP дефинира формат на податочни единици (датаграми) кои се испраќаат;
- IP софтверот ги извршува рутирачките функции врз основа на IP адресите;
- Фрагментација и составување на датаграмите со цел да се обезбеди пренос на податоци со различни должини;
- IP содржи множество правила за тоа како хостовите (крајните корисници) и рутерите да се справат со добиените датаграми, како и кога да се генерираат пораки за грешка и за тоа кога може датаграмите да се отстранат од мрежата.

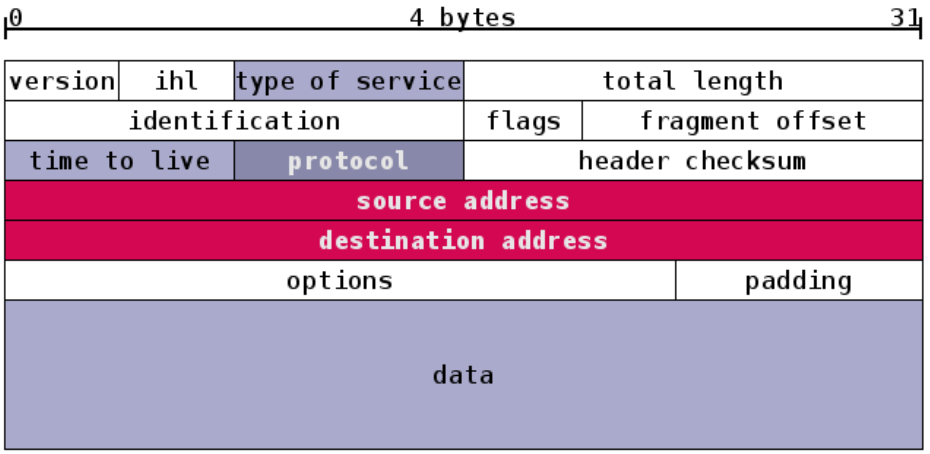
Интернет Протоколот (IP) е податочно ориентиран протокол кој се користи за пренос на податоци низ поврзани мрежи со користење на технологијата на комутација на пакети. IP е протокол на мрежно ниво во пакетот на интернет протоколи кој е енкапсулиран во протоколите на податочно ниво (како што е на пример Етернет). Како протокол на пониско ниво, IP обезбедува сервиси за комуникација помеѓу комјутерите со користење на единствени адреси.

1.1 Интернет протокол верзија 4 (IPv4)

Интернет протокол верзија 4 е четврта генерација на Интернет Протоколот (IP) и прва верзија на овој протокол која е пошироко прифатена и имплементирана.

Целта на IP е да обезбеди систем на адресирање на компјутерите во мрежата со доделување на единствен идентификациски број. IP датаграмот се состои од заглавие и информационо поле. Заглавието кај IPv4 е составено од фиксен дел со должина 20 бајти и опционен дел со променлива должина. Секој бајт од ваквата структура се праќа во мрежата во редослед од MSB (Most significant bit) кон LSB (Least significant bit) бит, па по тој редослед и се прима во дестинационата машина.

На следната слика е прикажано заглавјето на IP пакетот.



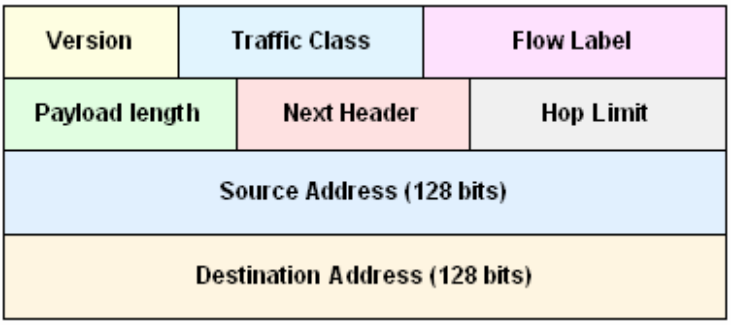
Слика 1. Заглавје на IP пакетот

1.2 Интернет протокол верзија 6 (IPv6)

Интернет Протокол верзија 6 (IPv6) е протокол на мрежно ниво (англиски network layer протокол) за пакет-комутирани вмрежувања. Дизајниран е како наследник на IPv4 - тековната верзија на Интернет Протокол за општа намена.

Главно подобрување кое го дава IPv6 (Интернет Протокол верзија 6) е зголемувањето на бројот на адреси на располање за вмрежените уреди. Тоа овозможува, на пример, секој мобилен телефон или било кој мобилен електронски уред да има сопствена адреса. IPv4 подржува 2^{32} (околу 4,3 милијарди) адреси, кои не се доволни согласно нараснатите потреби. IPv6 подржува 2^{128} адреси; тоа е околу $3{,}4\times10^{38}$ адреси или по околу 5×10^{28} адреси за секого од околу 6,5 милијарди денешни жители на земјата. На овој начин ќе се надмине проблемот со недостаток на јавни IP адреси и најверојатно нема да има потреба од NAT (network address translation).

IPv6 не е директно компатибилен со IPv4. Адресната шема на IPv6 е нова и е базирана да им служи на демографски и модерни мрежи. Адресниот простор на IPv6 е долг 128 бити со кој е овозможено постоење на огромен број адреси во споредба со 32 бити за адреси кај IPv4. Но, IPv6 не е развиена со цел да го разреши само проблемот со адресите, бидејќи истиот може да биде решен со користење на јавни и приватни IP адреси.



Слика 2. IPv6 хедер

2. Механизмите на транзиција

Механизмите се дизајнирани за да бидат употребени во IPv6 уреди кои треба да бидат назад-компатибилни со IPv4 уреди и да можат да употребуваат IPv4 рутирачки инфраструктури, но IPv6 може да се имплементира и во околина каде што IPv4 може да не се употребува.

Овие механизми вклучуваат:

- Двоен IP Слој (Dual IP Layer, Dual Stack): Техника за провајдирање на комплетна подршка за двата Интернет Протоколи - IPv4 и IPv6 – во хостови и рутери,
- Конфигурирано тунелурање за IPv6 преку IPv4: Точка до точка тунели направени со енкапсулирање на IPv6 преку IPv4 пакети во IPv4 хедери за да ги пренесуваат преку IPv4 рутирачки инфраструктури,
- IPv4-компатибилни IPv6 адреси: IPv6 адресен формат кој вклучува вградени IPv4 адреси,
- Автоматско тунелирање на IPv6 преку IPv4: механизам за употребување на IPv4-компатибилни адреси за автоматско тунелирање на IPv6 пакети преку IPv4 мрежи.

2.1. Двоен IP Слој (Dual IP Layer)

Наједноставниот начин за IPv6 уредите да останат компатибилни со IPv4 е да се провајдира комплетна IPv4 имплементација во нив. IPv6 уредите кои имплементираат целосна подршка за IPv4 ќе ги наречеме "IPv6/IPv4 уреди". IPv6/IPv4 уредите ја имаат сопособноста да праќаат и да примаат IPv6 и IPv4 пакети. Тие директно можат да соработуваат со IPv4 уреди користејќи IPv4 пакети и исто така да соработуваат со IPv6 уреди користејќи IPv6 пакети.

Иако еден уред може да биде опремен со подршка за двата протоколи една или друга подршка може да биде исклучена од операциски причини, т.е. IPv6/IPv4 уредите може да работат на некои од следниве 3 опции:

- Со нивната IPv4 подршка вклучена, додека IPv6 е исклучена.
- Со нивната IPv6 подршка вклучена, додека IPv4 е исклучена.
- Со двете поддршки вклучени.

2.2. Конфигурирање на адреси (во Dual IP layer)

Со тоа што IPv6/IPv4 уредите ги подржуваат двата протокола, IPv6/IPv4 уредите може да бидат конфигурирани со IPv6 и IPv4 адреси. IPv6/IPv4 уреди употребуваат IPv4 механизми (пример: DHCP) да добијат IPv4 адреси и IPv6 протоколи/механизми (пример: stateless address autoconfiguration) за да земат IPv6 адреси. Подоцна ќе објасниме како работи механизмот со кои IPv6/IPv4 уредите кои подржуваат автоматско тунелирање може да користат IPv4 протоколи/механизми да добијат IPv4 – компатибилна IPv6 адреса.

2.3. DNS

Domain Naming System (DNS) е употребуван во IPv4 и IPv6 за да се мапираат имињата на хостовите и IP адресите. Нов ресурс именуван "A6" е дефиниран за IPv6 адреси [1] кој го подржува претходникот "AAAA". Откако IPv6/IPv4 уредите мора да се способни да соработуваат директно со IPv4 и IPv6 уреди, тие мораат да провајдираат "resolver libraries" кои се способни со делење на IPv4 "A", "A6" и "AAAA" записи. DNS "resolver libraries" на IPv6/IPv4 уредите мора да се способни за управување со A6/AAAA и "A" записи. Но, кога има побарување кое лоцира A6/AAAA запис кој содржи IPv6 адреса, и

А запис кој содржи IPv4 адреса тогаш резолверот може да филтрира со цел резултатите кои се вратени на апликацијата да можат да влијаат на верзијата на IP пакети кои се користени за комуникација со тој уред, т.е. резолверот може да филтрира со следниве 3 алтернативи:

- Враќај само IPv6 адреса на апликацијата,
- Враќај само IPv4 адреса на апликацијата,
- Враќај ги двата типа на адреси.

Ако ги враќа само IPv6 адресите, тогаш апликацијата ќе комуницира со уредот користејќи IPv6. Ако ги враќа само IPv4 адресите, тогаш апликацијата ќе комуницира со уредот користејќи IPv6, ако ги враќа двете тогаш ќе има избор кој протокол да го користи, т.е. која адреса да ја користи.

Ако ги враќа двете тогаш резолверот може да одбере ред со кој ќе се избираат адресите, како на пример IPv6 или IPv4 прво.

Одлуката за филтрирањето или редот на DNS резултатите е специфична за имплементирањето. IPv6/IPv4 уредите може да дозволат полиса за конфигурацијата и контрола на филтрирањето, или редот на адреси кои се вратени од DNS резолверот, или да ја остават одлуката во рацете на апликацијата.

Имплементацијата мора да дозволи апликацијата да контролира или не како ќе се филтрираат резултатите.

3. Тунелирачки механизми

Додека IPv6 инфраструктурата е во развивање, веќепостоечката IPv4 инфраструктура може да остане функционална, и може да се искористи да пренесува IPv6 сообраќај. Тунелирањето претставува начин да се користи постоечката IPv4 мрежа за рутирање и пренесување на IPv6 сообраќај.

IPv6/IPv4 хостовите и рутерите може да тунелираат IPv6 датаграми преку региони со IPv4 топологија, со енкапсулирање (од IPv6 во IPv4 пакети).

Тунелирањето може да се имплементира на повеќе начини:

- **Рутер до Рутер**. IPv6/IPv4 рутери кои се меѓусебно поврзани со IPv4 мрежа можат да тунелираат IPv6 пакети помеѓу себе,
- **Хост до Рутер**. IPv6/IPv4 хостовите можат да тунелираат IPv6 пакети до IPv6/IPv4 рутер кој е достапен преку IPv4 инфраструктура,

- **Хост до Хост**. IPv6/IPv4 хостови кои се меѓусебно поврзани со IPv4 инфраструктура можат да тунелираат IPv6 пакети меѓусебно,
- **Рутер до Хост**. IPv6/IPv4 рутери можат да тунелираат IPv6 пакети до нивната финална дестинација IPv6/IPv4 хост.

Тунелирачки техники вообичаено се класифицираат според механизмот според кој енкапсулирачкиот уред ја детерминира адресата на уредот на крајот од тунелот. Во првите тунелирачки методи наведени погоре (рутер до рутер и Хост од рутер) IPv6 пакетот е тунелиран од страна на рутер. Крајната точка на ваков тунел е посредник рутер кој мора да го декапсулира IPv6 пакетот и препрати до неговата финална дестинација. Кога се тунелира до рутер, крајната точка на тунелот е различна од крајната дестинација на пакетот кој е тунелиран, т.е. адресата на IPv6 пакетот кој е тунелиран е различна од IPv4 адресата на пакетот.

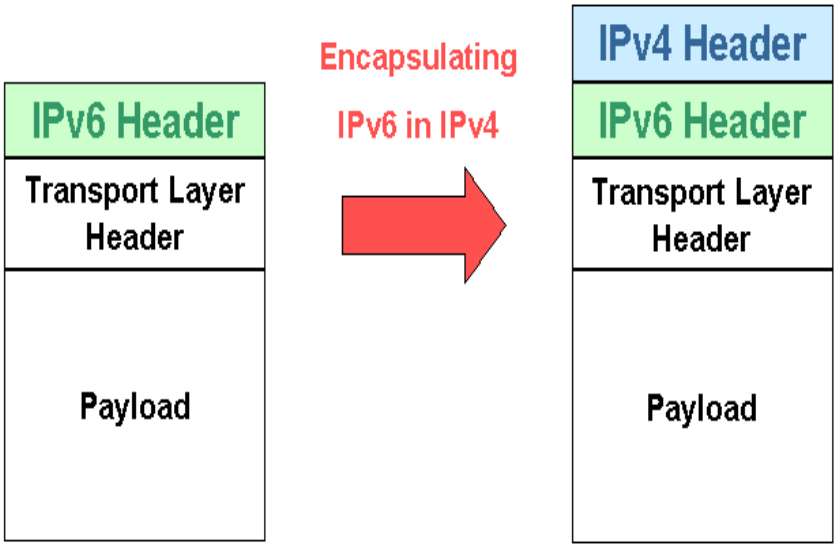
Во последните два тунелирачки методи (хост до хост и рутер до хост) IPv6 пакетот е тунелиран на целиот пат сé до неговата финална дестинација. Во овој случај, енкапсулираниот IPv6 пакет и IPv4 пакетот имаат иста дестинација. Овој факт може да биде злоупотребен со енкодирање на информации во IPv6 дестинацискатa адреса така што ќе дозволи енкапсулирачкиот уред да одреди која ке биде IPv4 дестинацискатa адреса автоматски. Автоматското тунелирање ја користи оваа техника, користејќи специјален IPv6 адресен формат со вградена IPv4 адреса кој дозволува тунелирачките уреди автоматски да ја изведат адресата на крајната цел на тунелот. Ова ја елиминира потребата за експлицитно да се конфигурира тунелот, т.е. олеснувајќи ја конфигурацијата.

Двете тунелирачки техники (автоматски и конфигурирано) се разликуваат главно во одлучувањето на крајната адреса на тунелот. Повеќето механизми се исти:

- Влезниот уред (тој кој енкапсулира) креира енкапсулирачки IPv4 хедер и го трансмитира енкапсулираниот пакет,
- Излезниот уред од тунелот (тој кој декапсулира) го прима енкапсулираниот пакет, го составува од повеќе пакети ако е потребно, го отстранува IPv4 хедерот, и го процесира IPv6 пакетот,
- Енкапсулирачкиот уред може да задржи некои информации за секој тунел како на пример MTU со цел да процесира IPv6 пакети кои треба да се препратат во тунелот. Бројот на вакви тунели кои ги употребува еден хост или рутер може да стане голем затоа тие се ставаат во кеш меморија која може да се ослободи ако не се користи.

3.1. Енкапсулација

Енкапсулацијата на IPv6 датаграмите во IPv4



Слика 3. Енкапсулација на IPv6 во IPv4

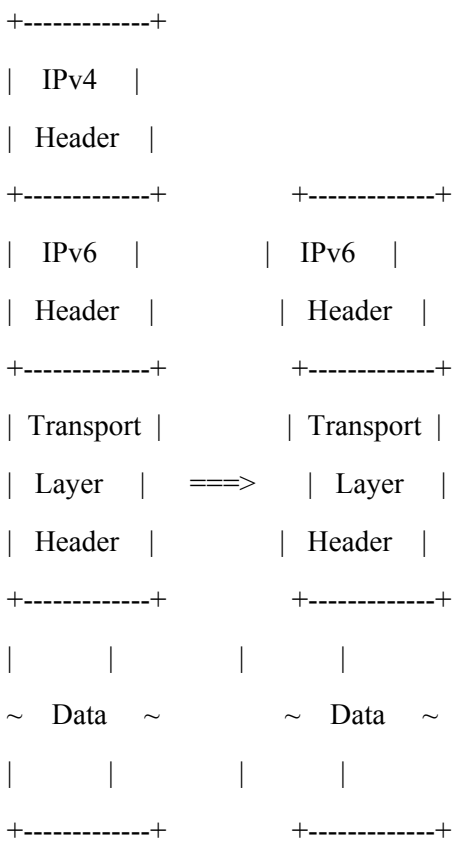
Покрај додавањето на IPv4 хедерот, енкапсулирачкиот хост/рутер исто така има неколку покомплексни проблеми:

- Да одлучи кога да го фрагментира пакетот и кога да прати ICMP "packet too big" порака назад до изворот,
- Како да рефлектира IPv4 ICMP грешки од рутери во тунелот назад до изворот како IPv6 ICMP грешки.

Декапсулација

Кога IPv6/IPv4 хост или рутер прима IPv4 датаграм кој е адресиран на една од неговите адреси и вредноста на протокол полето е 41, тој го реасемблира фрагментираниот пакет, потоа го отстранува IPv4 хедерот и го препраќа пакетот до неговата дестинација.

Декапсулирачкиот уред мора да биде способен за реасемблирање на IPv6 пакет кој е 1300 бајти (1280 бајти со IPv4 хедер).



Слика 4. Декапсулирање на IPv6 од IPv4

Кога имаме декапсулирање на пакетот, IPv6 хедерот останува не модифициран. Ако пакетот е препратен тогаш имаме декрементирање на хоп лимитот за еден.

Како дел од декапсулацијата, уредите треба да ги отфрлаат пакетите со инвалидни IPv4 изворни адреси како мултикаст адреси и броадкаст адреси (пример 0.0.0.0 и 127.0.0.1). Генерално треба да важат правилата за филтрирање во [5] и [6].

Декапсулирачкиот уред потоа извршува IPv4 реасемблирање пред декапсулирањето на IPv6 пакетот. Сите IPv6 опции се зачувани иако енкапсулираниот IPv4 пакет е фрагментиран.

Откога IPv6 пакетот е декапсулиран, тој е процесиран исто како некој примен IPv6 пакет (не тунелиран). Единствената разлика е тоа што пакетот не треба да е препратен ако тоа не е експлицитно конфигурирано да препраќа такви пакети да дадена IPv4 изворна адреса, оваа рестрикција е

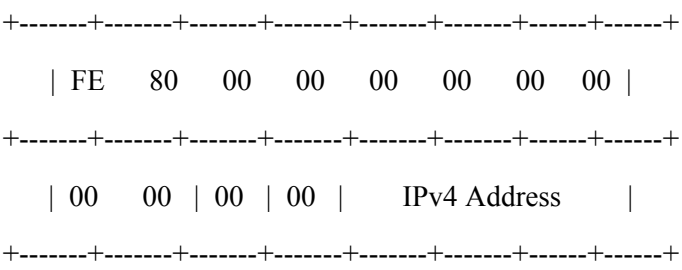
потребна за да се превентира тунелирањето да биде користено како алатка за “circumvent ingress filtering”[6].

3.2. Link-Local Адреси

Конфигурираните и автоматските тунели се IPv6 интерфејси (преку IPv4 “link layer”) и мораат да имаат link-local адреси. Link-local адресите се користени од рутирачките протоколи кои рутираат преку тунелите.

Interface Inentifier-от [7] за такви интерфејси треба да биде 32-битна IPv4 адреса на тој интерфејс, со ист ред на бајти како што се појавуваат во хедерот на IPv4 пакетот, со додадени нули на лево до 64 бита. Да забележиме дека “Universal/local” бит е нула, индицирајќи дека Interface Identifier-от не е глобално уникатен. Кога хост има една или повеќе IPv4 адреси во употреба на физичкиот интерфејс, се прави административен избор на една IPv4 адреса.

IPv6 Link-local адреса [7] за IPv4 виртуелен интерфејс е формирана со додавање на Interface Identifier-от, на префиксот FE80::/64.



Слика 5. Link-Local адреса

3.3. Nighbor Discovery преку Тунели

Автоматските и повеќенасочни конфигурирани тунели се сметаат за повеќенасочни. Со тоа единствените аспекти од Neighbor Discovery [8] и Stateless Address Autoconfiguration [9] кои се однесуваат на овие тунели е формацијата на link-local адресите.

Ако имплементацијата провајдира двонасочни конфигурирани тунели тогаш мора да прима и да одговара на “probe” пакетите користени од Neighbor Unreachability Detetion [8]. Вакви имплементации треба исто така да праќаат NUD probe пакети за да детектираат кога конфигурираниот тунел не работи, по кое време имплементацијата може да користи алтернативен пат по кој да достапи до дестинацијата. Да забележиме дека Neighbor Discovery дозволува

NUD probes да бидат изоставени во рутер до рутер врски ако рутирачкиот протокол следи двонасочна достапност.

За целите на Neighbor Discovery автоматските и конфигурираните тунели наведени во овој документ, се претпоставува дека немаат link-layer адреса, иако IPv4 link-layer-от има. Ова значи дека испраќач на Neighbor Discovery пакети:

- Не треба да вклучува опции за изворната Link-layer адреса во постоечката врска во тунелот,
- Треба без одговор да ги игнорира сите добиени SLLA или TLLA опции во врската во тунелот.

4. Конфигурирано тунелирање

Во конфигурирано тунелирање, адресата на крајот од тунелот се одредува од конфигурациските информации во енкапулирачкиот уред. За секој тунел, енкапсулирачкиот рутер/хост мора да ја зачува крајната адреса на тунелот. Кога IPv6 пакет е пратен преку тунел крајната адреса на е конфигурирана така што овој тунел е користен како дестинациска адреса за енкапсулирачкиот IPv4 хедер.

Одредувањето кои пакети треба да се тунелираат е вобичаено одредувано според рутирачките информацци во енкапсулирачкиот уред, според рутирачки табели, т.е. се насочуваат пакетите според нивната дестинациска адреса.

4.1. Стандардно конфигурирани Тунели

IPv6/IPv4 хостовите кои се поврзани за даталинкови без IPv6 рутери можат да користат конфигуриран тунел да стигнат до IPv6 рутер. Овој тунел дозволува хостот да комуницира со остатокот од IPv6 Интернетот (т.е. уреди кои основно се базирани на IPv6 адреси). Ако се знае IPv4 адреса од IPv6/IPv4 рутер кој се граничи со backbone, таа може да се користи како крајна дестинација за тунели. Овој тунел може да биде конфигуриран во рутирачка табела како IPv6 “default route”, т.е. сите пакети со IPv6 дестинациски адреси ќе можат потенцијално да поминуваат преку тунелот. Поради должината на ваква стандардна врска која е нула таа ќе биде употребувана само ако нема други врски со поголема должина кои се совпаѓаат со дестинацијата. Вака стандардно дефинираниот тунел може да биде користен заедно со автоматско тунелирање.

4.2. Стандардно конфигуриран тунел со користење на IPv4 “Anycast Address”

Крајната адреса на така конфигурираното тунел може да биде IPv4 адреса на IPv6/IPv4 рутер на границата со IPv6 backbone. Алтернативно крајната адреса може да биде IPv4 “anycast” адреса. Со овој начин, повеќе IPv6/IPv4 рутери на границата може да адвертизираат IPv4 достапност до истата IPv4 адреса. Сите од овие рутери прифаќаат пакети до таа адреса како нивни и ќе ги декапсулираат IPv6 пакетите кои се тунелирани до истата адреса. Кога IPv6/IPv4 уред праќа енкапулиран пакет до оваа адреса, пакетот ке биде прерутиран до еден до граничните рутери, но испраќачкиот уред нема да знае до кој. IPv4 рутирачкиот систем генерално ќе го пренесува сообраќајот до најблискиот рутер.

Употребувајќи стандардно конфигуриран тунел со IPv4 “anycast” адреса се провајдира робустност, бидејќи може да има повеќе гранични рутери, и со употреба на стандарди механизми за стабилност на IPv4 рутирањето, сообраќајот автоматски ќе биде пренасочен на друг рутер ако еден престане да работи.

Но, треба да се внимава додека се користи овој вид на тунелирање, како на пример да не се доведе до различни фрагменти да стигнуваат до различни рутери, ова може да биде избегнато со некористење на фрагментација т.е. MTU на пакетите да биде максимум 1300 бајти.

4.3. Ингресно Филтрирање

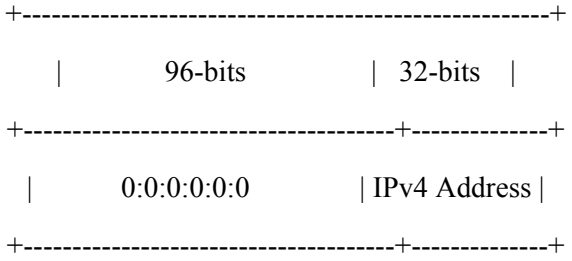
Декапсулирачкиот уред мора да верифицира дали почетната адреса на тунелот е прифатлива пред да препраќа декапсулирани пакети да избегне заобиколување на ингресно филтрирање [10]. Да забележиме дека пакетите кои се пренесени до транспортните протоколи на декапсулирачкиот уред не треба да се предмет на овие проверки. За двонасочни конфигурирани тунели ова е направено со верифицирање на изворните адреси (тие се IPv4 адреси од другата страна на тунелот). За еднонасочни конфигурирани тунели декапсулирачкиот уред мора да е конфигуриран со листа на изворни IPv4 адресни префикси кои се прифатливи.

5. Автоматско тунелирање

Во автоматското тунелирање, крајната адреса на тунелот е одредена од IPv4-компатибилната дестинациска адреса на IPv6 пакетот кој е пратен. Автоматското тунелирње дозволува IPv6/IPv4 уреди да комуницираат преку IPv4 рутирачки инфраструктури без претходно конфигурирани тунели.

5.1. IPv4-Компатибилен адресен формат

IPv6/IPv4 уредите кои извршуваат автоматско тунелирање се со предодредени IPv4 компатибилни адреси. IPv4компатибилна адреса е идентификувана според сите нули во 96-битниот префикс додека крајните 32 бита ја содржат IPv4 адресата. Тие се структуирани на следниов начин:



Слика 6. IPv4 компатибилен адресен формат

IPv4-компатибилните адреси се доделени ексклузивно на уреди кои подржуваат автоматско тунелирање.

IPv4-компатибилните адреси се глобално уникатни доколку не формираат адреса од IPv4 приватиот адресен простор [11]. Имплементацијата треба да се однесува како да нејзините IPv4-компатибилни адреси се зададени на интерфејсите на уредите за автоматско тунелирање. Исто така IPv4-компатибилните адреси не треба да бидат гледани како да се задатени на, пример, на етернет интерфејс т.е. не траба да се користат механизми кои користат Neighbor Discovery механизми како NUD [12], во етернет.

5.2. IPv4-Компатибилна автоматска конфигурација

IPv4/IPv6 компатибилен уред ја користи IPv4-компатибилната адреса како една од неговите IPv6 адреси, додека IPv4 адресата е впишана во последните 32 бита, користена на еден од неговите интерфејси.

IPv4/IPv6 уред може да ја добие својата адреса(IPv4-компатибилна) преку IPv4 конфигурациски протоколи, т.е. може да користи IPv4 конфигурациски механизам да ја добие, а потоа да ја “мапира” во IPv4-компатибилна со додавање на 96 битен префикс од нули. Алгоритмот е следниот:

1. IPv6/IPv4 уред употребува стандардни IPv4 механизми или протоколи да добие IPv4 адреса за еден од неговите интерфејси, т.е. следниве:
   - Dynamic Host Configuration Protocol (DHCP),

- Bootstrap Protocol (BOOTP),
- Reverse Address Resolution Protocol (RARP)[13],
- Мануална конфигурација.

2. Уредот ја употребува таа адреса како IPv4 адреса за тој интерфејс.
3. Уредот го додава 96 битниот префикс од 0:0:0:0:0:0 на 32 битната IPv4 адреса која ја има добиено од чекор 1. Резултатот е IPv4-компатибилна IPv6 адреса која содржи "вградена" IPv4 адреса во последните 32 бита. Уредот ја користи таа адреса како една од неговите IPv6 адреси.

5.3. Операции на автоматското тунелирање

Во автоматското тунелирање, крајната дестинација на адресата е детерминирана од пакетот кој е тунелиран. Ако IPv6 дестинацијата е IPv4 компатибилна тогаш пакетот може да се испрати со користење на автоматско тунелирање. Ако дестинацијата е IPv6 адреса тогаш пакетот не може да се испрати со автоматско тунелирање.

Рутирачки табели може да се користат да се директира автоматското тунелирање, имплементација може да има специјална статичка рутирачка табела за секој префикс 0:0:0:0:0:0:/96 (т.е рута со сите нули префикс со 96 битна маска). Пакети кои одговараат на овој префикс се праќаат на псевдо-интерфејс кој го изведува автоматското тунелирање. Бидејќи сите IPv4 компатибилни адреси ќе одговараат на овој префикс тие ќе бидат автоматски тунелирани.

Откога ќе бидат пренесени на модул за автоматско тунелирање, IPv6 пакетите ќе се енкапсулираат во IPv4 хедер. Изворните и дестинациските адреси за енкапсулираните пакети се доделуваат на следниов начин:

Дестинациска IPv4 адреса:

- Последните 32 бита од IPv6 дестинацискатa адреса

Изворна IPv4 адреса:

- IPv4 адреса од интерфејсот на пакетот од кој е пратен.

Модулот за автоматско тунелирање секогаш праќа пакети во оваа енкапсулирана форма, иако дестинацијата е прикачена на даталинк.

Модулот за автоматско тунелирање не смее да праќа до IPv4 броадкаст или мултикаст дестинации, исто така мора да ги игнорира сите IPv6 пакети кои се со дестинација до IPv4 компатибилна адреса кога таа е броадкаст,

мултикаст, неспецифицирана (0.0.0.0), или пак луп-бак (loopback 127.0.0.0) адреса.

5.4. Употреба на стандардно конфигурираните тунели

Автоматското тунелирање е често употребувано во комбнација со техниката за стандардно конфигурирање на тунели. "Изолирани" IPv6/IPv4 хостови (тие без врска со IPv6 рутери) се конфигурирани да употребуваат автоматско тунелирање и IPv4 компатибилни IPv6 адреси, и имаат најмалку еден предефиниран конфигуриран тунел до IPv6 рутер. Тој рутер е конфигуриран да извршува автоматско тунелирање исто така. Овие изолирани хостови праќаат пакети до IPv6 дестинации преку предефинираниот тунел со автоматското тунелирање и пакети за IPv6-нативни адреси преку автоматски конфигурираниот тунел. IPv4 компатибилни дестинации ќе го исполнуваат условот за 96 битниот префикс од сите нули (дискутиран претходно) додека IPv6 нативните дестинации ќе се совпаѓаат со конфигурираниот тунел. Повратни пакети од IPv6 дестинации се прерутирани назад до IPv6/IPv4 рутер кој ги пренесува нив до оригиналниот хост со автоматско тунелирање. Вакви примери може да се најдат дискутирани во [14].

5.5. Селекција на изворни адреси

Кога IPv6/IPv4 уред креира IPv6 пакет, тој мора да селектира изворна IPv6 адреса за употреба. IPv6/IPv4 уредите кои се конфигурирани да извршуваат автоматско тунелирање може да бидат конфигурирани со глобална IPv6 адреса и со IPv4 компатибилна адреса. Селекцијата за која адреса да се користи ќе се утврди од формата на враќање, т.е. од каде тој се препраќа назад. Ако е користена IPv4 компатибилната адреса повратниот сообраќај ќе биде автоматски тунелиран, но ако е употребувана IPv6 адресата тој нема да биде автоматски тунелиран. За да се направи сообраќајот да биде симетричен колку што е можно повеќе, за селекција на изворна адреса следнава референца е препорачлива:

Дестинацијата е IPv4 компатибилна:

- Употреба на IPv4 компатибилна изворната адреса која е врзана на излезниот интерфејс.

Дестинацијата е IPv6 адреса:

- Употреба на IPv6 адресата на излезниот интерфејс.

Ако IPv6/IPv4 уредот нема глобална IPv6 нативна адреса, но влезниот сообраќај доваѓа од IPv6 адреса тогаш може да се користи IPv4 компатибилната адреса како изворна.

5.6. Ингресно филтрирање

Декапсулирачкиот уред мора да верифицира дега енкапсулираните пакети се прифатливи пред да ги препраќа декапсулираните пакети за да избегне ингресно филтрирање [10]. Да ги забележиме дека пакетите кои се пренесени до транспортните протоколи на декапсулирачкиот уред не треба да бидат предмет на овие проверки. Бидејќи автоматските тунели секогаш енкапсулираат до дестинацијата и секој пакет добиен преку автоматско тунелирање не треба да биде препратен.

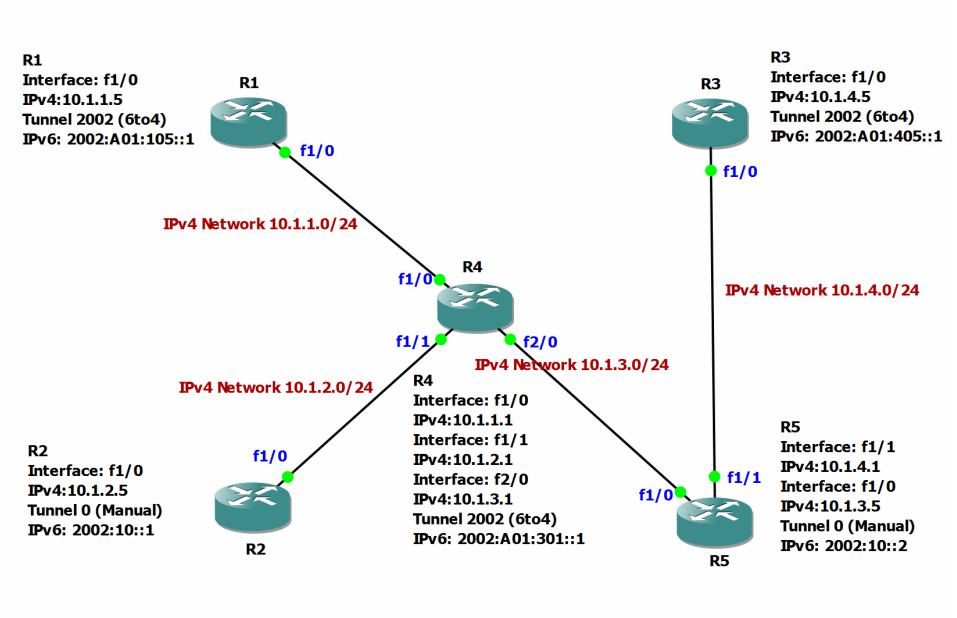
6. Експериментален дел

Како што можеме да видиме од конфигурациските фајлови имаме инплементирано два типа на тунели и тоа:

- Конфигуриран тунел помеѓу R2 и R5,
- Автоматски тунели помеѓу R1,R3 и R4

Конфигурираниот тунел (или Мануелен) тунелира IPv6 пакети преку R4 со тоа што ги енкапсулира пакетите во IPv4, тој има фиксни изворни и дестинациски интерфејси (на R2 - f1/0 е изворен, додека дестинацискиот интерфејс е на R5 - f1/0, исто така на R5 - f1/0 е извоен, додека дестинацискиот интерфејс е на R2 - f1/0). На двата интерфејси имаме Dual IP Layer со конфигурирани фиксни IPv4 и IPv6 адреси, за да го овозможиме рутирањето исто така имеме конфигурирано RIPv2 (Routing Information Protocol version 2) конфигурирано на посредникот т.е. на R4.

Со оваа имплментација имаме еден статичен тунел кој може да пренесува IPv6 пакети преку IPv4 инфраструктура, т.е. ако имавме IPv6 мрежи на двете страни од двата рутера тие ќе беа достапни помеѓу себе без да има никакви пречки во сообраќајот т.е. како да беа во нативна IPv6 околина, исто така рутерот R4 за двете мрежи ќе беше транспарентен со тоа што ќе изгледаше како да имаме еден хоп помеѓу R2 и R5.



Слика 7. Мапа на експериментот

Автоматските тунели тунелираат IPv6 пакети помеѓу R1,R3 и R4 со тоа што ја користат IPv4 инфраструктурата, тие за разлика од мануелниот тунел не е потребно да се конфигурираат со дестинациски адреси, туку се конфигурираат со префикс кој користат т.е. со 2002::/16 каде што форматот е 2002:border-router-IPv4-address::/48 (во нашиов случај користиме автоматско тунелирање 6to4, да користевме друг тип на автоматско тунелирање префиксите ке беа различни). Ова ги прави автоматските тунели да бидат многу пофлексибилни и поедноставни за поголема имплементација таму каде што е потребна исто така бараат помалку време во административното одржување.

Како што можеме да видиме и двата типа на тунели се многу практични и со различни намени но имаат негативни страни како што е користењето на поголеми ресурси таму каде што се имплементираат, нивните негативни страни се следниве:

- Поголема работна меморија во рутерите, поради користењето на Dual IP layer, т.е. треба да се чуваат рутирачките табели за двата протокола,
- Поголема процесирачка моќ на рутерите, за енкапулацијата и декапулацијата да може да се извршува покрај нормалната работа на руерот,
- Некои од тунелите исто така имаат посебни негативни ефекти.

Заклучок

Овие механизми се со намера да се употребуваат како дел од “Транзициските Алатки” – колекција од техники за имплементација, кои можат да се користат по потреба, зависно од имплементирачите и местата на кои треба да се имплементира, во зависност од специфичните и конкретни потреби. Во овој документ се наброени “главните” механизми но не се очекува да се употребуваат само овие туку и други алатки и механизми кои се достапни.

Литература

1. Crawford, M., Thomson, S., and C. Huitema. "DNS Extensions to Support IPv6 Address Allocation and Renumbering", RFC 2874, July 2000.
2. Kent, C. and J. Mogul, "Fragmentation Considered Harmful". In Proc. SIGCOMM '87 Workshop on Frontiers in Computer Communications Technology. August 1987.
3. Mogul, J. and S. Deering, "Path MTU Discovery", RFC 1191, November 1990.
4. Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
5. Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.
6. Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2267, January 1998.
7. Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.
8. Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.
9. Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC 2462, December 1998.
10. Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2267, January 1998.
11. Rechter, Y., Moskowitz, B., Karrenberg, D., de Groot, G.J. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.
12. Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.
13. Finlayson, R., Mann, T., Mogul, J. and M. Theimer, "Reverse Address Resolution Protocol", STD 38, RFC 903, June 1984.
14. Callon, R. and D. Haskin, "Routing Aspects of IPv6 Transition", RFC 2185, September 1997.