УДК 004.724.4

Лазебний В.С., к.т.н,
Зубець А.М.

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ТУНЕЛЮВАННЯ ПАКЕТІВ IPV6 У МЕРЕЖНІЙ ІНФРАСТРУКТУРІ IPV4

Національний технічний університет України «Київський політехнічний інститут»

smartvs@mail.ru
azubets@mail.ru

Розглянуто способи передавання інформаційних потоків, сформованих згідно протоколу IPv6, засобами мережної архітектури IPv4. Проаналізовано особливості застосування технології 6to4 для мережних станцій під керуванням Windows XP та технології Teredo для станцій під керуванням Windows 7 та старших версій. Сформовано рекомендації щодо можливості й особливостей застосування зазначених технологій для передавання IPv6 трафіку

Ключові слова: *протокол IPv4, IPv6, тунелювання, операційні системи, маршрутизація, мережний рівень*

Вступ

З 5 лютого 2008 року організація ICANN, що наглядає за використанням інтернет-протоколів, почала додавати в DNS-сервери записи, що містять адреси у форматі протоколу IPv6. Це поклало початок переходу від протоколу IPv4 до сучаснішого IPv6. На тепер співіснують мережі, що функціонують за обома зазначеними протоколами і, як прогнозують фахівці таке співіснування буде тривати невизначено тривалий час [1].

Логіка роботи і формати даних двох протоколів істотно відрізняються, тому їх сумісність можна забезпечити зовнішніми по відношенню до них засобами.

Для того, щоб можна було використовувати інфраструктуру мереж IPv4 для передавання пакетів сформованих за протоколом IPv6 запропоновано кілька механізмів:

- механізм подвійного стеку;
- механізм тунелювання;
- механізм транслювання.

Головною перевагою механізму тунелювання є відсутність необхідності купувати і встановлювати додаткове програмне забезпечення на кожному вузлі. Тунелювання – метод передавання IPv6 пакету через IPv4-мережу, коли пакет IPv6 розміщують (інкапсулюють) в пакеті IPv4, як певний блок даних.

Механізм тунелювання використовують для часткового вирішення проблеми сумісності між протоколами IPv6 та IPv4. Його не можна застосовувати для зв'язку IPv6-вузлів з IPv4-хостами. Тунелювання призначено для організації зв'язку між IPv6-вузлами або мережами із застосуванням мережного середовища, що функціонує за протоколом IPv4 [2].

Користувачі сучасних телекомунікаційних мереж використовують у своїх комп'ютерах (мережних вузлах) операційні системи різних поколінь, що мають різні можливості щодо адаптації до мережного протоколу IPv6. У зв'язку з цим існує проблема адаптації наявних мереж, що функціонують за протоколом IPv4, для передавання інформаційних пакетів, створених мережними ресурсами за протоколом IPv6.

Метою дослідження є з'ясувати особливості реалізації і застосування тунелів для передавання пакетів IPv6 засобами інфраструктури IPv4.

Налаштування тунелю 6to4

Використання такого тунелю можливе у випадку, якщо комп'ютер має глобальну IP-адресу. Цей момент є принциповим, оскільки даною технологією пе-

редбачено формування унікальної глобальної IPv6 адреси саме за глобальною IPv4 адресою [3]. Оскільки з різних причин операційна система Windows XP залишається й натепер популярною у багатьох користувачів проаналізуємо можливість та особливості налаштування тунелю 6to4 в середовищі цієї ОС. Такий механізм може бути реалізовано і в разі використання ОС Windows старших версій.

Спочатку переконаємось, що досліджуваний комп'ютер не має доступу до ресурсів IPv6. Застосуємо для цього онлайн перевірку на доступність і звернемось на сайт http://test-ipv6.com/.

Результат тестування наведено на рис.1. Як випливає з наведеної екранної інформації, можливість обміну пакетами з IPv6-ресурсами у мережного IPv4 вузла відсутня.

Для налаштування тунелю необхідно у командному режимі прописати й виконати команду:

```
>netsh int ipv6 6to4 set relay 192.88.99.1 enabled 1440.
```

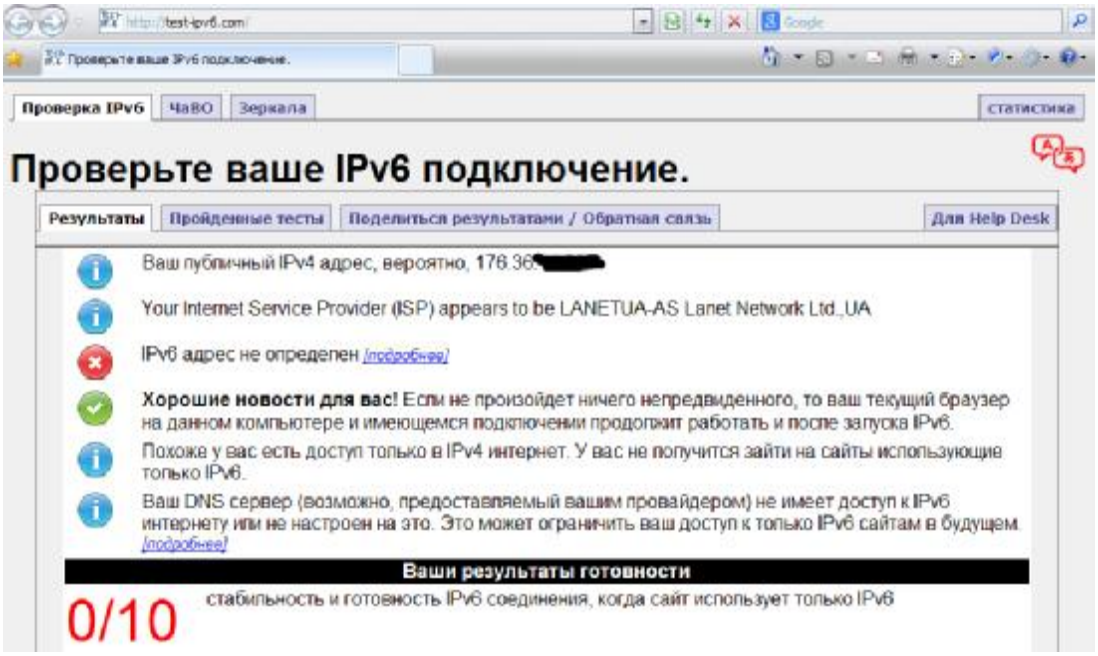

Рис.1. Результати перевірки на доступність IPv6-з'єднань для мережної станції

Адреса 192.88.99.1 є спеціальною широкомовною (anycast) адресою, завдяки якій відбувається пошук шлюзів 6to4. Один з них, на який потрапить наш запит, незалежно від свого територіального розташування, буде брати участь у реалізації механізму 6to4 для нашої станції, і на нього буде маршрутизовано 6to4-трафік. Внаслідок такої організації з'єднання у процесі передавання інформаційних потоків можливі певні проблеми з продуктивністю роботи [3]. Після виконання наведеної вище команди знову перевіряємо доступність IPv6-ресурсів для досліджуваного мережного вузла, рис.2.

Рис.2. Результати повторної перевірки щодо доступності IPv6-з'єднань

З наведених результатів тестування випливає, що досліджуваному комп'ютеру було надано IPv6-адресу, і тепер він може здійснювати обмін пакетами з IPv6-ресурсами. Для більш детального аналізу результатів здійснених налаштувань перевіримо з'єднання з довільним IPv6-ресурсом і проаналізуємо прокладений маршрут до цього ресурсу. Спочатку робимо ICMPv6 запит до ресурсу www.xbox.com.

На запит отримано стандартну відповідь, що підтверджує коректність налаштування 6to4-з'єднання. Екранна інформація командного режиму має такий вигляд:

```
Microsoft Windows XP [Версия 5.1.2600]
<C> Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Admin>ping -6 wwu.xbox.com

Обмен пакетами с e2820.dspb.akanaiedge.net  [2a02:26f0:f:184::b041 no 32
байт:

Ответ   от   2a02:26f0:f:184::b04:    время=59мс
Ответ   от   2a02:26f0:f:184::b04:    время=57мс
Ответ   от   2a02:26f0:f:184::b04     время=57мс
Ответ   от   2a02:26f0:f:184::b04:    время=57мс

Статистика   Ping  для   2a02:26f0:f:184::b04:

      Пакетов:отправлено = 4, получено = 4, потеряно = 0 <0% потерь),
Приблизительное  время  приема-передачи  в  мс:
      Минимальное = 57мсек, Максимальное = 59 мсек. Среднее = 57 мсек

C:\Documents and Settings\Admin>_
```

Для подальшого дослідження проаналізовано маршрут до ресурсу www.xbox.com, щоб визначити шлях проходження пакетів і з'ясувати який сервер забезпечує тунелювання 6to4:

```
C:\Documents and Settings\Admin>tracert –6 www.xbox.com

Трассировка маршрута к e2820.dspb.akamaiedge.net [2a02:26f0:f:186::b04]
      с максимальным числом прыжков 30:
```

```
  1  31 ms     31 ms     34 ms     GW-NetAssist.retn.net
f2a02:2d8:0:2801:232a::1]
  2  32 ms     31 ms 31 ms ae2-299.RT.NTL.KIV.UA.retn.net
[2a02:2d8:0:2801:232a::]
  3  38 ms     41 ms 29 ms RT.IRX.FKT.DE.retn.net  [2a02:2d8::57f5:e0a1]
  4  47 ms     29 ms 87 ms     if-ae25.0.tcorel.FR0-Frankfurt.ipv6.as6453.net
[ 2a01:3e0:ff20::69]
  5  66 ms     50 ms  50 ms   if-ae7.832.tharl.WIT-Uarsaw.ipu6.as6453.net
[2a01:3e0:ff20::3e]
  6  60 ms     58 ms 59 ms 2001:5a0:900:100::2a
  7  58 ms     57 ms 57 ms     2a02:26f0:f:186::b04

Трассировка завершена.

C:\Docunents   and   Settings\Admin>_
```

За результатами трасування можна зробити висновок, що створений тунель проходить через сервер компанії "NetAssist". У даному випадку він і є 6to4-шлюзом, що забезпечує з'єднання за протоколом IPv6.

Для перевірки процесу функціонування створеного тунелю було застосовано мережний аналізатор пакетів Wireshark і розглянуто процес передавання IPv6-пакетів від мережного IPv4-вузла (176.36.14.95) до IPv6-вузла (ресурс www.xbox.com з адресою 2a02:26f0:f:186::b04).

Аналізатор надає можливість розглянути процес проходження пакетів згідно моделі стеку TCP/IP. З отриманих результатів випливає, що на канальному рівні відбувається передавання пакетів за MAC-адресами від комп'ютера до шлюзу, а на мережному рівні – передавання пакету від джерела (Source) з адресою 176.36.14.95 до 6to4-шлюзу з адресою 192.88.99.1 (Destination). А слідом за ним, над IPv4, вже надходить інкапсульований пакет IPv6.

Подальше проходження IPv6-пакетів відбувається за схемою, рис. 3: від джерела (шлюз) з адресою 2002:b024:e5f::b024:e5f, до пункту призначення з адресою 2a02:26f0:f:186::b04 (www.xbox. com). Шлюз здійснює деінкапсуляцію пакету, відкидає заголовки IPv4, відновлює і передає IPv6-пакети в мережу IPv6. У разі передавання в зворотному напрямку пакет IPv6 потрапляє на шлюз, який його інкапсулює в пакети IPv4 і передає далі до ПК клієнта згідно його IPv4-адреси.

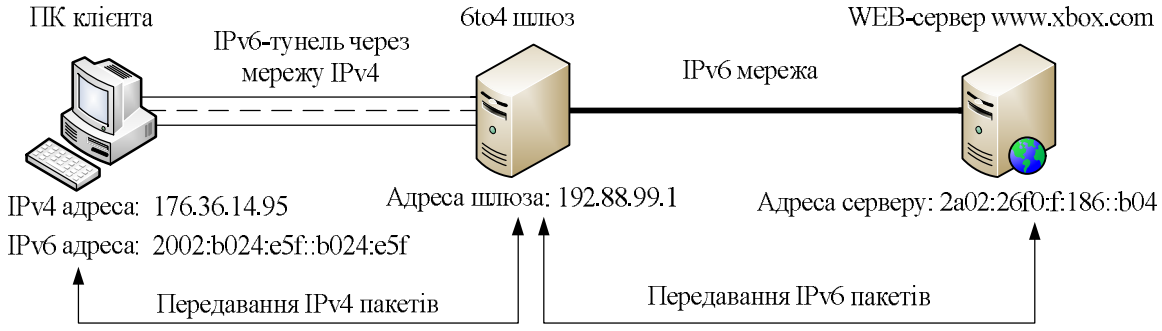

Рис. 3. Схема процесу передавання пакетів через тунель на шлюз і далі в мережу IPv6

До позитивних властивостей наведеного методу тунелювання слід віднести простоту налаштування, яке можна здійснити швидко і забезпечити доступ до ресурсів IPv6. Серед недоліків даного методу можна відзначити такі:

- вимога обов'язкової наявності глобальної IPv4-адреси;
- призначення лише однієї IPv6-адреси, тому можна з'єднати лише один пристрій;
- неможливість роботи через NAT.

Налаштування тунелю Teredo

Тунель Teredo запропоновано для випадку, коли станція знаходиться у внутрішній мережі по відношенню до маршрутизатора NAT, тобто не має глобальної IP адреси [4]. Тунель Teredo аналогічний до реалізованого в Linux та Mac OS X тунелю Miredo. Тунель Teredo більш універсальний порівняно з розглянутим вище 6to4 тунелем, але вимагає і додаткового налаштування.

Зазначимо, що в ОС Windows 7 і старших версіях операційної системи Windows програмне забезпечення для налаштування Teredo є в наявності, але застосування такого тунелю передбачено в основному для обслуговування різних мережних програм у фоновому режимі. Тому, зокрема, за відсутності IPv6-трафика ОС швидко деактивує тимчасово налаштований тунель Teredo. Для запобігання цьому треба виконати низку налаштувань, що дозволить за необхідності безперебійно користуватись зазначеною технологією.

Щоб з'ясувати особливості налаштування, розглянемо всю процедуру налаштування тунелю Teredo для Windows 7. Для операційних систем Windows більш нових версій процес є аналогічним. Спочатку треба увімкнути службу "Допоміжна служба IP" ("IP Helper"), якщо її не було активовано: "Мій комп'ютер" (контекстне меню) → "Управління" → "Служби". Шукаємо "Допоміжна служба IP", викликаємо "Властивості", ставимо тип запуску "Автоматично".

Наступним кроком є редагування реєстру. За адресою "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Dnscache\Parameters" необхідно створити ключ "DWORD – AddrConfigControl" і призначити йому значення "нуль".

Оскільки без налаштування DNSv6 нема можливості відкривати сайти у браузері за їх доменним ім'ям, ініціюємо призначення DNSv6. З цією метою використовуємо публічні DNS IPv6 компанії "Google". Вони мають такі адреси:

2001:4860:4860::8888,
2001:4860:4860::8844.

Тепер здійснюємо безпосереднє налаштування Teredo. Для цього потрібно змінити кілька параметрів у редакторі групових політик (gpedit.msc): знайти в розділі "Конфігурація комп'ютера" ("Computer Configuration") → "Адміністративні шаблони" ("Administrative Templates") → "Мережа" ("Network") → "Параметри TCP/IP" ("TCPIP Settings") → "Технології тунелювання IPv6" ("IPv6 Transition Technologies").

Необхідно зробити низку налаштувань:

– Класифікація Teredo за початковим призначенням → Увімкнути → Активований стан;
– Частота оновлення Teredo → Увімкнути → 10;
– Стан Teredo → Увімкнути → Корпоративний клієнт;
– Порт клієнта Teredo → Не задано;
– Ім'я сервера Teredo → Увімкнути → Вибираємо зі списку:
  – teredo.remlab.net (France);
  – teredo.trex.fi (Finland);
  – teredo.ipv6.microsoft.com (United Kingdom / USA) default for windows;
  – teredo.ngix.ne.kr (South Korea);
  – teredo.managemydedi.com (USA, Chicago);
  – teredo.autotrans.consulintel.com (Spain).

Перевірити доступність кожного із зазначених серверів можна шляхом перевірки наявності з'єднання командою "ping". Для подальших досліджень було обрано сервер "teredo.remlab.net".

Сервери керовані Microsoft розташовані й функціонують у різних регіонах планети, тому наперед невідомо, з яким саме буде встановлено зв'язок.

Для більш продуктивної роботи IPv6 слід деактивувати інші технології тунелювання:

– Ім'я ретранслятора 6to4 → Відімкнути;

– Інтервал дозволу імен ретранслятора 6to4 → Відімкнути;
– Стан 6to4 → ВИМКНУТИ → Відімкнутий стан;
– Стан IP - HTTPS → Відімкнути;
– Ім'я маршрутизатора ISATAP → Відімкнути;
– Стан ISATAP → ВИМКНУТИ → Відімкнутий стан.

Усі зроблені налаштування буде відображено у вікні налаштувань групових політик.

Подальшим кроком є налаштування інтерфейсу/маршрутів. Для здійснення цього налаштування треба виконати дві команди:

```
netsh int ipv6 delete route ::/0 Teredo ,
netsh int ipv6 add route ::/0 Teredo .
```

Після усіх зроблених налаштувань перевіряємо працездатність тунелю Teredo і для цього надсилаємо запити на IPv6-ресурси nnm-club.me та ipv6.google.com. Результати перевірки наведено нижче:

```
C:\Users\Andrew>ping ipv6.nnm-club.me

Pinging ipu6-nnm-club.me [2001:470:26:482::2] with 32 bytes of data:
Reply from 2001:470:26:482::2:  time=85ms
Reply from 2001:470:26:482::2:  time=40ms
Reply from 2001:470:26:482::2:  time=41ms
Reply from 2001:470:26:482::2:  time=39ms

Ping statistics for 2001:470:26:482::2:
      Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
Approxinate round trip times in milli-seconds:
      Mininun = 39ms, Maxinun = 85ms, Average = 51ms

C::\Users\Andrew>ping  -6 ipv6.google.com

Pinging ipv6.1.google.con [2a00:1450:4010:c02::65] with 32 bytes of data
Request timed out.
Reply from 2a00:1450:4010:c02::65:  time =37ns
Request timed out.
Reply from 2a00:1450:4010:c02::65:  time =35ms

Ping statistics for 2a00:1450:4010:c02::65:
      Packets: Sent = 4, Received =  2 ,  Lost = 2 <50% loss>,
Approxinate round trip times in milli-seconds:
      Mininun = 35ms, Maxinun = 37ms, Average = 36ms

C:\Users\Andrew>
```

Як випливає з результатів перевірки, зв'язок з ресурсами ipv6.nnm-club.me та ipv6.google.com присутній, тунель працює правильно. Також зробимо загальну он-лайн перевірку щодо доступності ресурсів IPv6 через сайт http://test-ipv6.com/, рис.4.

Особливо слід звернути увагу на такий результат:

```
"Ваш публичный IPv6 адрес, вероятно,  2001:0:53aa:64c:28db:19d5:4fdb:f11d
Вероятно, ваш IPv6 провайдер: Teredo"
```

Тобто, перевірка підтвердила, що тунель працює саме за технологією Teredo.

Слід зробити важливе зауваження, що виконані операції можуть не забезпечити 100% гарантії працездатності Teredo, що може бути пов'язано з використанням симетричного NAT (дуже малоймовірний і окремий випадок). З'ясовано також, що під час зміни адреси IPv4, з'єднання IPv6 може перерватись. У такому разі необхідно зачекати – тунель Teredo буде автоматично відновлено протягом 1-5 хвилин.

Крім того, Teredo дозволяє використати тільки одну IPv6-адресу, тобто роздати з його допомогою IPv6-адреси в локальній мережі не вдасться.

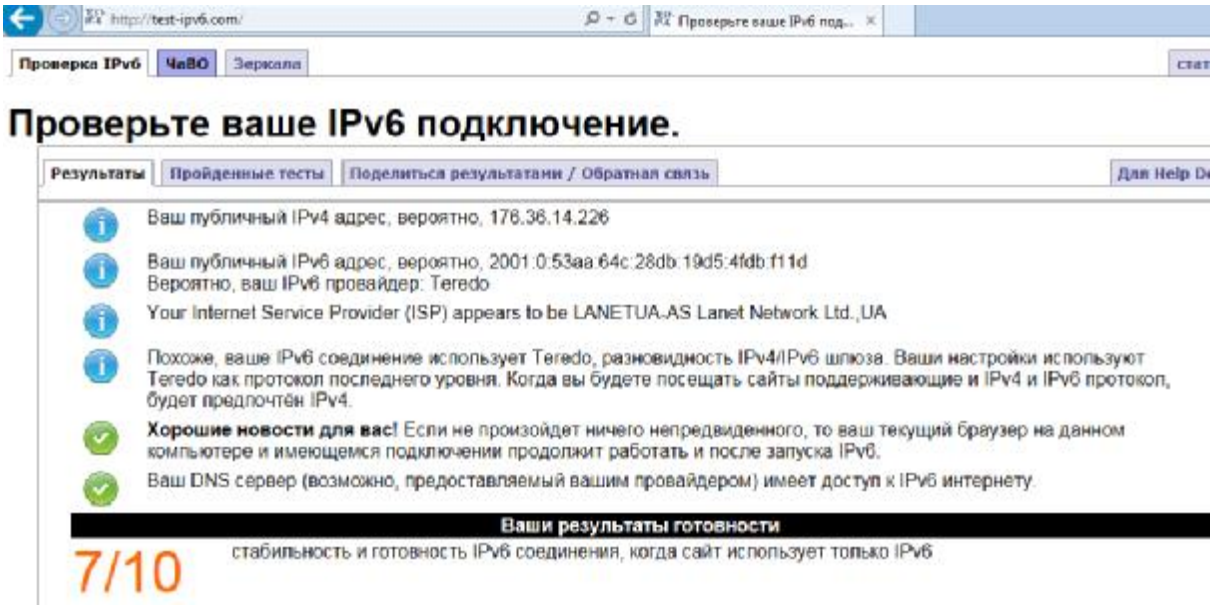

Рис. 4. Web-сторінка з інформацією стосовно IPv6-з'єднання

За умови правильного налаштування Teredo/IPv6, не потрібно подальшої участі користувача, все буде працювати автоматично [4].

Teredo має кілька особливостей, про які слід знати.

По-перше, його підтримку формують два типи серверів: допоміжні, які потрібні тільки на етапі конфігурації (один з них розгорнутий самою Microsoft), і шлюзи, що забезпечують звернення до реальних IPv6-адрес шляхом розшифровки адрес інкапсульованого трафіка (взаємодія між Teredo-адресами відбувається безпосередньо). Відповідно, пропускна здатність тунелю може залежати від завантаження згаданих мережних вузлів.

По-друге, потрібно зважати на те, що Teredo дозволяє приймати вхідні з'єднання, що створює потенційну загрозу безпеці. На даний момент це навряд чи є великою загрозою, оскільки сканувати IPv6-адреси (а Teredo навіть складніше, ніж реальні) занадто складно. Але під час практичного застосування варто передбачити додатковий захист, наприклад, за допомогою брандмауера Windows Firewall [5].

До переваг даного методу слід віднести:

– можливість роботи через NAT;
– кожен пристрій може отримати доступ до IPv6-інтернету;
– налаштування не є дуже складним, проте вимагає певних знань і навичок в адмініструванні Windows чи Linux системи.

Недоліком даного методу є необхідність налаштовувати кожен пристрій окремо.

Висновки

Розроблені механізми тунелювання пакетів IPv6 через інфраструктуру IPv4 дозволяють реалізовувати їх на комп'ютерах (мережних вузлах), що функціонують під керуванням операційних систем різних поколінь. Зокрема тунель 6to4 може бути реалізовано для будь-якого користувацького комп'ютера з операційною системою Windows XP і вище, що коректно функціонує в IPv4 мережі і має реальну адресу.

У найпростішому випадку IPv6 вузол просто додає IPv4 заголовок до пакетів і передає їх. Вузол відновлення відділяє IPv4 заголовок і далі продовжує опрацьовувати пакет, як звичайний пакет IPv6. Тунелювання має підтримувати кілька спеціальних процедур:

– забезпечувати фрагментування, якщо оригінальний IPv6 пакет занадто довгий і перевищує припустимий розмір області даних IPv4 пакету. Для мінімізації подібних явищ потрібно використовувати механізм PMTU (Path MTU), тобто застосовувати найменші MTU серед MTU (пакетів максимально допустимої довжини) каналів даних, що знаходяться між джерелом і приймачем;

– правильно обмежувати кількість переходів (TTL). За домовленістю, тунель IPv6-в-IPv4, незалежно від того якої він довжини, вважають одним переходом. Значення TTL в IPv4 пакеті має бути встановлено відповідно до запровадженого механізму;

– оброблення IPv4 ICMP помилок. Оскільки під час проходження тунелю можуть виникати ICMP помилки, має бути передбачено спеціальний механізм для того, щоб повідомити про них відправника пакетів.

До недоліків тунелюваннння слід віднести те, що:

- користувачі створеної нової структури не можуть використовувати ресурси інфраструктури нижчого рівня (тобто мережі, через яку прокладено тунель);
- тунелювання не дозволяє користувачам нового протоколу обмінюватись даними з користувачами старого протоколу (IPv4) без застосування технології подвійного стека [6].

Під час автоматичного тунелювання адреса кінцевої точки тунелю визначається IPv4-адресою, за якою надіслано IPv6 пакет. Автоматичне тунелювання дозволяє IPv6/IPv4 вузлам використовувати маршрутну інфраструктуру IPv4 без попередньо сконфігурованих тунелів.

Список використаних джерел

1. Сергей Орлов. Один день из жизни IPv6. [Електронний ресурс]. – Режим доступу: http://www.osp.ru/telecom/2011/06/13009351/

2. Gilligan R., Nordmark E., "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005. [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc4213.

3. 6to4. From Wikipedia, the free encyclopedia. [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/6to4.

4. Настройка IPv6/Teredo в Windows 7,8. [Електронний ресурс]. – Режим доступу: http://blog.cherepovets.ru/serovds/2011/11/15/teredo-win7/.

5. IPv6, не дожидаясь провайдера. [Електронний ресурс]. – Режим доступу: http://www.ixbt.com/soft/ipv6.shtml.

6. Enterprise IPv6 Solution. NAT64 Technology: Connecting IPv6 and IPv4 Networks. [Електронний ресурс]. – Режим доступу: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html.

Статтю подано до редакції 24.03.2016