УДК 004.72,004.738.5:005.936.3

Черкасов Д. І.

ПІДХОДИ ДО СУМІСНОГО ВИКОРИСТАННЯ ПРОТОКОЛІВ IPV4 ТА IPV6 У МЕРЕЖІ ПІДПРИЄМСТВА

Розробку протоколу IPv6 здійснено внаслідок непереборних обмежень протоколу IPv4, які постали на шляху розвитку всесвітньої мережі Інтернет. Утім, оскільки одночасно замінити широко використовуваний IPv4 на IPv6 виявилося неможливим, поширеною практикою на сьогодні є співіснування обох протоколів. Оскільки IPv4 та IPv6 призначені для вирішення одних і тих самих завдань, одночасна їх підтримка означає надлишковість витрачених ресурсів. У статті розглянуто підходи до оптимізації використання обох протоколів 3-го рівня OSI в мережі сучасного підприємства з урахуванням тенденції до переважного розвитку мереж на основі протоколу IPv6.

Ключові слова: IP, IPv6, Інтернет, корпоративна мережа, підприємство, адресація, співіснування, міграція, накладені мережі.

Вступ

Головними завданнями протоколів 3-го рівня моделі OSI (протоколів L3) є адресація пристроїв у мережах та визначення шляху пересування – маршрутизація, пакетів між ними.

Адресація полягає в призначенні унікального ідентифікатора – адреси, кожному з пристроїв мережі, кількість яких може сягати від десятків для малих офісів, сотень та тисяч для середніх підприємств до мільярдів, якщо мова йде про всесвітню мережу Інтернет [2].

Маршрутизація здійснюється шляхом покрокової передачі пакетів між проміжними пристроями – маршрутизаторами, для наближення до кінцевого пункту – пристрою призначення.

Оскільки загальна кількість пристроїв, під'єднаних до Інтернету, має чітку тенденцію до зростання [5], до протоколів L3 ставиться вимога забезпечення можливості адресації та маршрутизації в мережах дедалі більшого обсягу. Обмежені можливості адресації протоколу IPv4, які стали очевидними вже в 1994 р., призвели до початку розробки нового протоколу L3 – IPv6 [6; 18], характеристики якого вважаються цілком достатніми для забезпечення потреб адресації на сьогодні і в найближчому майбутньому.

У статті розглянуто підходи до вирішення завдань, що постають перед протоколами L3, із забезпеченням вищої ефективності використання засобів адресації та маршрутизації, а також спрощення алгоритмів функціонування і зменшення використовуваних ресурсів задіяних пристроїв.

Головна проблема – обмеження адресного простору

Протокол IPv6 своєю появою завдячує істотним обмеженням, з якими зіткнувся його попередник IPv4. Найчастіше серед цих обмежень зазначають такі [1]:

- нестача адрес для глобальної адресації;
- складність заголовка пакетів, яка підвищує складність його аналізу в пристроях;
- відсутність інтегрованих засобів для забезпечення якості обслуговування – Quality-of-Service (QoS);
- відсутність інтегрованих засобів для захисту даних, які передаються, застосування технології IPSec [15] є опціональним;
- використання фрагментації на шляху передачі пакетів у разі, коли їхній розмір перевищує максимум, підтримуваний транзитним пристроєм.

Усунення зазначених вище обмежень вважають ключовими перевагами протоколу IPv6. Утім, лише нестача унікальних IP-адрес виявилася проблемою, яка мала непереборний характер. Апаратна реалізація обробки пакетів та використання багатопротокольної комутації по позначках – Multiprotocol Label Switching (MPLS) знизили вплив складності заголовків на навантаження центральних процесорів пристроїв. Сумісне використання з IPv4 додаткових технологій захисту даних, як-от IPSec, та забезпечення QoS, особливо з апаратною підтримкою, знизило критичність відсутності відповідних інтегрованих засобів в IPv4. Технологія автоматичного визначення максимального розміру пакету на повному шляху передачі – Path MTU

Discovery [11], дозволила позбуватися фрагментації пакетів.

Як захід для уповільнення швидкості вичерпання адрес IPv4 значного поширення набула технологія підміни мережевих адрес – Network Address Translation (NAT). Утім, відсутність NAT в IPv6 і забезпечення прозорої двобічної передачі пакетів між пристроями, що взаємодіють, не варто вважати самостійною перевагою IPv6 перед IPv4, оскільки поява NAT була зумовлена обмеженими можливостями адресації в IPv4.

Додатковими перевагами IPv6 також вважають зокрема:

- автоматичне самоналаштування адрес пристроїв без використання додаткових процесів типу DHCP – Stateless Address Autoconfiguration (SLAAC);
- спрощення глобального розподілу адресного простору IPv6 за рахунок використання фіксованої довжини мінімального префікса мережі 48 бітів замість гнучкого вибору довжини префікса згідно з методом Classless Interdomain Routing (CIDR) в IPv4;
- спрощення планування внутрішнього розподілу адресного простору локальних мереж за рахунок використання для всіх її сегментів єдиної довжини префікса 64 біти (/64) замість змінної довжини маски згідно з методом Variable Length Subnet Mask (VLSM) в IPv4;
- активне використання локальних канальних (link local) адрес;
- нечітка – anycast, адресація для взаємодії з будь-яким пристроєм групи (на відміну від групової адресації – multicast, яка передбачає взаємодію з усіма пристроями групи).

Зазначені переваги, одначе, не можна визнати такими, що роблять впровадження IPv6 критично необхідним. Отже, можна дійти висновку, що саме нестача адрес в IPv4 стала ключовим фактором, який прискорив початок реального використання IPv6 в Інтернеті.

За рахунок використання 128-бітових адрес IPv6 забезпечує загальну кількість адрес на багато порядків більшу, ніж IPv4. Утім, можливості адресації в IPv6 не безкінечні, а особливості розподілу адрес IPv6 для глобальної адресації (global unicast) ще більше обмежують загальну кількість пристроїв, яка може бути під'єднана до мережі [14]. До таких особливостей слід віднести такі:

- стандартна довжина адресного префікса для кожного сегмента локальної мережі становить 64 біти (/64);
- максимальна довжина адресного префікса для блоку адрес, який призначається локальній мережі, що має множину сегментів, становить 48 бітів (/48);
- адреси для глобальної адресації виділяються з діапазону 2000::/3.

Зважаючи на зазначене, охарактеризувати наявний обсяг адрес глобальної маршрутизації можна як 2^{45} локальних мереж (а не 2^{128} пристроїв, які можна під'єднати до мережі).

Зростання обсягу використаних адрес IPv6 наразі має лінійний характер [19], при цьому здебільшого IPv6 впроваджується у вже існуючих мережах, які використовують IPv4. Створення мереж із виключним використанням IPv6 має дослідницький характер [17], але з початком їх масового використання (що є неминучим, оскільки адресний простір IPv4 уже вичерпано) темпи використання адрес IPv6 зростатимуть.

Зокрема, суттєве прискорення використання адрес IPv6 відбудеться з початком надання доступу до Інтернету по IPv6 для дрібних (retail) клієнтів – приватних помешкань та малих офісів. Окрім великої кількості користувачів зазначеної категорії, кожному з них, окрім адреси для під'єднання до провайдера Інтернету – Internet Service Providers (ISP), необхідно делегувати один чи декілька префіксів /64 для пристроїв локальної мережі цього користувача [13].

Значну додаткову кількість адрес потребуватиме впровадження архітектури мікросервісів, яка набуває дедалі більшої популярності [9]. Використання контейнерів для кожного з мікросервісів вимагатиме виділення одного чи декількох префіксів /64 для кожного кластеру.

Певна втрата ефективності розподілу адрес IPv6 може статися внаслідок виділення великих адресних блоків континентальним (регіональним) інтернет-реєстрам – Regional Internet Registries (RIR).

Надлишкова витрата адрес IPv6 матиме місце внаслідок неоптимального їх використання підприємствами. Наприклад, у разі під'єднання локальної мережі підприємства до декількох ISP, оптимальним є використання власного мережевого префікса /48, який не залежить від конкретного ISP. Утім, для спрощення конфігурації (усунення налаштування протоколу BGP з кожним ISP) підприємство може обрати сумісне використання префіксів /48 від кожного з провайдерів [10], що очевидно є надлишковістю.

Прискоренню зростання обсягу використаного адресного простору IPv6 сприятимуть новітні тренди, як-от Internet of Things (IoT) [7]. У майбутньому можлива поява нових технологій, які також потребуватимуть великих обсягів адрес.

Одночасно з наданням значного за обсягом адресного простору впровадження IPv6 призведе до збільшення обсягів оперативної пам'яті пристроїв, відведених для таблиць маршрутизації та інших пов'язаних із ними структур даних, підвищення обчислювального навантаження для підтримки протоколів динамічної маршрутизації [BGP]. Збільшення адресного простору призведе до розширення можливого фронту здійснення атак і ускладнення протидії їм.

Оскільки протокол IPv6 справді суттєво розширює можливості адресації порівняно з IPv4, зазначені фактори дають підстави для обережних оцінок щодо можливого терміну вичерпання адрес IPv6, а отже, обґрунтовують необхідність системного їх розподілу.

Стратегії впровадження IPv6

Несумісність протоколів IPv4 та IPv6 визначила неможливість поступового еволюційного переходу від одного до іншого. Оскільки революційний перехід шляхом одночасної заміни IPv4 на IPv6 також не є реальним, обидва протоколи вимушені співіснувати принаймні протягом певного перехідного періоду. Упродовж зазначеного перехідного періоду IPv6, як вважається, має поступово замістити IPv4. Серед стратегій міграції від IPv4 до IPv6 протягом перехідного періоду найчастіше розглядають такі [22]:

- тунелювання – передача пакетів між мережами IPv6 через тунелі, які створюються в мережах IPv4;
- перетворення (трансляція) пакетів між протоколами – Network Address Translation (NAT);
- подвійний стек – одночасна підтримка пристроями обох протоколів із переважним використанням IPv6.

Тунелювання забезпечує транспортування пакетів між мережами IPv6 у випадку, якщо між цими мережами не існує з'єднання з підтримкою IPv6. Цей захист не забезпечує можливості взаємодії між пристроями, що підтримують різні протоколи.

Технологія NAT має декілька різновидів [8] і призначена для забезпечення взаємодії пристроїв з підтримкою різних протоколів, але така взаємодія має обмежену функціональність [16].

Повну функціональність забезпечує лише взаємодія в межах одного протоколу, таким чином, лише підтримка пристроями подвійного стеку – IPv4 та IPv6, єдина забезпечує повноцінну взаємодію з будь-якими пристроями, які підтримують лише один із протоколів.

Класи об'єктів в Інтернеті – потреби в підтримці IPv4 та IPv6

Інтернет – глобальна мережа обміну інформацією. Для аналізу особливостей використання в Інтернеті протоколів IPv4 та IPv6 (які за визначенням є базовими протоколами Інтернету) застосуємо поняття інтернет-об'єктів (далі – об'єкти), які беруть участь в інформаційному обміні. Серед об'єктів в Інтернеті можна виділити такі класи:

- інформаційні ресурси (далі – ресурси), які надають інформацію в різних форматах за запитом;
- запитувачі, які звертаються із запитами до ресурсів;
- партнери за симетричною (peer-to-peer) взаємодією (далі – партнери);
- компоненти транспортної інфраструктури, які здійснюють транзитну передачу інформації.

Як будь-яка мережа, Інтернет утворена пристроями і каналами зв'язку між ними. Пристрої можуть мати апаратну або програмну (зокрема віртуальну) реалізацію. Об'єкт є ширшим поняттям, ніж пристрій. Приклади об'єктів наведено нижче.

Ресурс

- сайт, який може мати у своєму складі низку серверів, організованих у вигляді кластеру, або територіально рознесених для балансування навантаження та забезпечення високої доступності, а також мережа доставки вмісту – Content Delivery Network (CDN);
- група серверів доменної системи імен – Domain Name System (DNS), які здійснюють підтримку певних доменів або тимчасове проміжне збереження інформації DNS – кешування (caching).

Запитувач

- мережа офісу або житлового будинку, яка об'єднує в собі множину кінцевих користувачів, що здійснюють запити до ресурсів;
- сервери-посередники (proxy), які здійснюють запити до ресурсів за дорученням користувачів.

Партнери

- сукупності прикордонних маршрутизаторів мереж підприємств, які обмінюються інформацією про маршрутизацію за протоколом Border Gateway Protocol (BGP);
- сервери електронної пошти, які передають між собою електронні листи;
- вузли керування телефонними викликами в IP-телефонії.

Компоненти транспортної інфраструктури

- транспортні мережі провайдерів, створені за технологією MPLS;

● магістральні транспортні мережі Інтернет, які утворюються сукупністю транспортних мереж низки провайдерів;

● мережа глобального зв'язку – World Area Network (WAN), яка поєднує в корпоративну мережу територіально рознесені компоненти підприємства.

Для створення об'єкта використовуються один чи декілька пристроїв. Кожен пристрій може входити до складу одного чи декількох об'єктів (наприклад, у разі створення декількох інформаційних ресурсів на одному сервері).

Кожен обмін інформацією в Інтернеті передбачає участь об'єктів двох типів:

● кінцеві об'єкти – ті, що, власне, обмінюються інформацією між собою;

● проміжні об'єкти – ті, що здійснюють підтримку передачі інформації між кінцевими об'єктами.

Як кінцеві об'єкти виступають ресурси, запитувачі, партнери. Проміжні об'єкти є компонентами транспортної інфраструктури.

Очевидно, що обов'язковою умовою для можливості взаємодії кінцевих пристроїв є підтримка єдиного спільного протоколу – IPv4 або IPv6. У разі, якщо підтримуються обидва протоколи, використовується один з них. Згідно з рекомендаціями Ради з архітектури Інтернету (Internet Architecture Board (IAB)), на сьогодні IPv6 є пріоритетним протоколом [4], отже, у разі підтримки обох протоколів перевагу слід віддати IPv4.

Так само очевидно, що протокол, обраний для взаємодії кінцевих об'єктів, має підтримуватися проміжними об'єктами, які безпосередньо контактують із зазначеними кінцевими об'єктами. Для інших проміжних об'єктів підтримка протоколу взаємодії кінцевих об'єктів не є обов'язковою. У разі, якщо такої підтримки немає, передача інформації можлива, наприклад, через тунель, кінці якого розташовані на проміжних об'єктах, які контактують із кінцевими об'єктами.

Проміжні об'єкти, через які передається інформація між кінцевими об'єктами, мають задовольняти вимогу: проміжні об'єкти, які безпосередньо контактують між собою, повинні підтримувати єдиний спільний протокол. Відповідно, у разі, якщо частина проміжних об'єктів, що здійснюють передачу інформації між кінцевими об'єктами, не підтримує протокол, що використовується кінцевими об'єктами, на шляху передачі інформації повинні бути об'єкти, які підтримують обидва протоколи. Ці об'єкти мають здійснювати тунелювання протоколу, що використовується кінцевими об'єктами, використовуючи як зовнішній протокол, що підтримується проміжними об'єктами.

Ці тези ілюструють застосування стратегії впровадження IPv6 на основі тунелювання (див. вище «Стратегії впровадження IPv6»). Складність її використання визначається додатковими вимогами до проміжних об'єктів – підтримка протоколів і створення тунелів. Оскільки проміжні об'єкти в загальному випадку не перебувають під технічним контролем власників кінцевих об'єктів, ця стратегія є ненадійною.

Мережа підприємства – оптимальне співіснування IPv4 та IPv6

Згідно з поширеною моделлю архітектури підприємства воно містить у собі територіально рознесені регіональні відділення, обмін інформацією між якими здійснюється через WAN [21]. Окремі відділення виконують роль головного офісу та дата-центру (можуть бути поєднані). Реалізація WAN здійснюється у вигляді проміжного об'єкта рівня L2 або L3 у разі, якщо всі відділення під'єднані до єдиного провайдера передачі даних, або у вигляді захищених тунелів – Virtual Private Network (VPN), через Інтернет. Технологія VPN також використовується для доступу до ресурсів мережі підприємства працівників, що перебувають поза її межами (вдома, у відрядженні і т. п.).

На відміну від Інтернету, корпоративні мережі підприємств, які не спеціалізуються на наданні послуг широкому загалу інтернет-користувачів, мають такі особливості:

● єдине адміністративно-технічне керування;

● однорідний і контрольований спектр використовуваного обладнання та програмного забезпечення;

● обмежений і контрольований перелік використовуваних застосувань всередині підприємства;

● переважна частка передачі інформації між кінцевими об'єктами, які належать мережі підприємства;

● обмежений і контрольований перелік зовнішніх ресурсів, з якими здійснюють обмін інформацією кінцеві об'єкти;

● прихованість кінцевих об'єктів від доступу з боку Інтернету (за винятком об'єктів, які призначені для використання як ресурси в Інтернеті);

● обмежена загальна кількість кінцевих пристроїв.

У корпоративній мережі наявні можливості для забезпечення підтримки всіма кінцевими та проміжними об'єктами єдиного базового протоколу – IPv4 або IPv6. Відсутність тунелювань, перетворень пакетів між протоколами і надлишкової підтримки обох протоколів у межах

кожного регіонального відділення сприятиме вищій надійності, функціональності та оптимальному використанню ресурсів.

Щодо зв'язку між відділеннями, у разі використання єдиного провайдера для WAN цей провайдер надає транспорт L2 або L3 з підтримкою потрібного протоколу (на сьогодні підтримка обох протоколів – IPv4 та IPv6, є нормою для провайдерів [19]). У разі зв'язку через Інтернет використання тунелів із кінцями на прикордонних маршрутизаторах відділень є неминучим. У цьому разі будь-яке співвідношення внутрішніх та зовнішніх протоколів для тунелів характеризується однаковим рівнем складності, функціональності та обсягом витрачених ресурсів.

Для зв'язку із зовнішніми ресурсами в разі, якщо підтримуваний ресурсом протокол не збігається з базовим протоколом корпоративної мережі, можливе вжиття таких заходів:

- для доступу до HTTP/HTTPS ресурсів із базовою функціональністю – використання серверів-посередників (proxy), які підтримують IPv4 та IPv6;
- для зв'язку з ресурсами партнера – використання тунелю до мережі партнера;
- для окремих випадків, які вимагають нетипової функціональності і для яких недостатньо зазначених вище методів – використання NAT із перетворенням протоколів або спеціалізованих рішень.

Для адресації в корпоративних мережах у разі базового протоколу IPv4 стандартом є використання так званих «приватних» адрес [12]. Один з блоків приватних адрес – 10.0.0.0/8, забезпечує можливість надання унікальних адрес $16x10^6$ пристроям, що на сьогодні є достатнім для переважної більшості підприємств. Оскільки найкритичніше обмеження IPv4 – нестача адрес, в цьому випадку неактуальне, протокол IPv6 як базовий для корпоративної мережі не має суттєвих переваг.

Стандартним технічним заходом у разі застосування приватних адрес для внутрішньої адресації в корпоративній мережі є використання NAT для зв'язку із зовнішніми ресурсами. Важливим побічним ефектом від використання NAT є захист об'єктів корпоративної мережі від контактів з боку Інтернету. Відсутність подібного захисту в IPv6 створює додаткові виклики щодо безпеки. Цей фактор, а також використання застарілого апаратного та програмного забезпечення, що склалося історично, можуть стати аргументами на користь обрання IPv4 як базового протоколу в корпоративній мережі.

Утім, для щойно створюваних нових мереж доцільно розглядати можливість їх базування на протоколі IPv6. Розвиток мереж – як Інтернету, так і корпоративних мереж, невпинно здійснюється в бік збільшення кількості об'єктів у їхньому складі, а отже, використання більшої кількості адрес. Це призводитиме до переважного використання IPv6 у нових мережах і поступового зростання загальної частки мереж із цим протоколом як базовим.

На певному етапі ключовим фактором на користь IPv6 стане вже не кількість доступних адрес, а потреба в сумісності з переважаючою кількістю існуючих об'єктів у мережах (на сьогодні цей фактор працює на користь IPv4). Після цього частка мереж IPv4 почне стрімко скорочуватися, зокрема за рахунок міграції старих мереж з IPv4 до IPv6. Одним із підходів для міграції корпоративної мережі з базовим протоколом IPv4 до IPv6 є використання технології так званих «накладених» (overlay) мереж [20], яка дає змогу створити і розвивати мережеву інфраструктуру, базовану на IPv6, незалежно і не порушуючи існуючої інфраструктури на IPv4.

Висновки

Розвиток мереж усіх різновидів здійснюється в бік зростання кількості об'єктів у них, а отже, важливість фактора більшої кількості адрес в IPv6 порівняно з IPv4 зростатиме. Карколомне зростання кількості об'єктів в Інтернеті, зокрема, під впливом новітніх трендів, як-от IoT, призводитиме до активного впровадження IPv6 у найближчі роки.

Натомість у корпоративних мережах підприємств унаслідок їх більшої консервативності і контрольованості (що дає змогу зменшити вплив фактора нестачі адрес за рахунок ефективності централізованого адміністративного керування) використання IPv4 як базового протоколу збережеться протягом довшого часу. Передовсім це стосується вже існуючих мереж із розвинутою інфраструктурою на базі IPv4. Наявність технологій для взаємодії із зовнішніми ресурсами IPv6 також сприятиме тривалості використання підприємствами IPv4.

Проте, оскільки зростання загальної частки IPv6 у мережах є невпинним, міграція мереж корпоративного сегмента з IPv4 до IPv6 є неминучою. Для щойно створюваних мереж доцільно розглядати як базовий протокол IPv6, а міграцію існуючих IPv4 мереж до IPv6 планувати з використанням підходів, які не порушують працездатності існуючої інфраструктури, наприклад, шляхом впровадження накладених мереж.

Список літератури

1. [BGP] 2017 BGP Table Size Prediction and Potential Impact on Stability of Global Internet Infrastructure [Electronic resource]. – Mode of access: http://bgphelp.com/2017/01/01/bgpsize/. – Title from the screen.
2. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016 : Press Release [Electronic resource]. – Egham, U. K., February 7, 2017. – Mode of access: https://www.gartner.com/newsroom/id/3598917. – Title from the screen.
3. Goralski W. Learn About: Differences in Addressing between IPv4 and IPv6 [Electronic resource] / W. Goralski. – Juniper Networks, 2014. – Mode of access: https://www.juniper.net/documentation/en_US/learn-about/ipv4-ipv6-differences.pdf. – Title from the screen.
4. IAB Statement on IPv6 [Electronic resource]. – Mode of access: https://www.iab.org/documents/correspondence-reports-documents/2016-2/iab-statement-on-ipv6/. – Title from the screen.
5. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) [Electronic resource]. – Mode of access: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. – Title from the screen.
6. IPv6 – The History and Timeline [Electronic resource]. – Mode of access: https://www.ipv6.com/general/ipv6-the-history-and-timeline/. – Title from the screen.
7. Meola A. What is the Internet of Things (IoT)? [Electronic resource] / A. Meola. – Dec. 19, 2016. – Mode of access: http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8. – Title from the screen.
8. NAT64–Stateless versus Stateful [Electronic resource]. – Mode of access: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676277.html. – Title from the screen.
9. Pattern: Microservice Architecture [Electronic resource]. – Mode of access: http://microservices.io/patterns/microservices.html. – Title from the screen.
10. Pepelnjak I. IPv6 multihoming without NAT: the problem [Electronic resource] / I. Pepelnjak. – Mode of access: http://blog.ipspace.net/2011/12/ipv6-multihoming-without-nat-problem.html. – Title from the screen.
11. Request for Comments: 1191. Path MTU Discovery [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc1191. – Title from the screen.
12. Request for Comments: 1918. Address Allocation for Private Internets [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc1918. – Title from the screen.
13. Request for Comments: 3769. Requirements for IPv6 Prefix Delegation [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc3769. – Title from the screen.
14. Request for Comments: 4291. IP Version 6 Addressing Architecture [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc4291. – Title from the screen.
15. Request for Comments: 4301. Security Architecture for the Internet Protocol [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc4301. – Title from the screen.
16. Request for Comments: 4966. Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc4966. – Title from the screen.
17. Request for Comments: 6586. Experiences from an IPv6-Only Network [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc6586. – Title from the screen.
18. Request for Comments: 8200. Internet Standard STD: 86. Internet Protocol, Version 6 (IPv6) Specification [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc8200. – Title from the screen.
19. State of IPv6 Deployment 2017 [Electronic resource]. – Internet Society, 25 May 2017. – Mode of access: https://www.internetsociety.org/resources/doc/2017/state-of-ipv6-deployment-2017/. – Title from the screen.
20. Tarkoma S. Overlay Networks: Toward Information Networking / S. Tarkoma. – Auerbach Publications, 2010. – ISBN 9781439813713 – CAT# K10708.
21. Tiso J. Designing Cisco Network Service Architectures (ARCH). Foundation Learning Guide / John Tiso. – Third Edition. – Cisco Press, 2012. – 698 p.
22. Wilkins S. IPv6 Translation and Tunneling Technologies [Electronic resource] / S. Wilkins. – Cisco Press, Jun 26, 2013. – Mode of access: http://www.ciscopress.com/articles/article.asp?p=2104947. – Title from the screen.

D. Cherkasov

APPROACHES FOR COEXISTENCE OF IPV4 AND IPV6 PROTOCOLS IN THE ENTERPRISE NETWORK

The most critical restriction of IPv4 – a lack of available addresses – caused IPv6 to be introduced in the production networks. As neither of the protocols is compatible, they are going to coexist during the transition period which is supposed to last quite a long time. Several strategies are considered to provide interoperation between IPv4 and IPv6 capable objects, with dual-stack being the most functional yet requiring most of resources and complicacy of configuration.

While coexistence of IPv4 and IPv6 is inevitable in the Internet with frequent function duplication and dual-stack used widely, enterprise networks have features that provide for better efficiency of using both protocols. Centralized management, controlled hardware and software diversity as well as the used set of applications enable using a single L3 protocol as the basic with the other protocol used only to communicate with external resources if needed.

Newly created enterprise networks should be based on IPv6, which will be beneficial in the future, as the overall part of IPv6 capable objects is growing rapidly. Legacy IPv4 based enterprise networks can still be used for quite a long time, as the amount of currently used private addresses is quite sufficient and the means of communication with external IPv6 resources provide satisfactory functionality. Yet migration to IPv6 is inevitable for these networks too, and introducing IPv6 in the form of overlay networks that do not break existing IPv4 infrastructure looks like an optimal solution.

Keywords: IP, IPv6, Internet, enterprise network, addressing, coexistence, migration, overlay networks.

Матеріал надійшов 12.09.2017