УДК 004.8

М.Р. Обертюх
Я.І. Мельник

ВИКОРИСТАННЯ ПРОТОКОЛУ IPV6 В КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

Вінницький національний технічний університет

Анотація

У роботі розглянуто особливості використання протоколу IPv6 у корпоративній комп'ютерній мережі. Проаналізовано проблеми сумісності з наявною IPv4-інфраструктурою та шляхам їх вирішення. Досліджено технологію Dual Stack як основний підхід до поетапної міграції корпоративної мережі на IPv6. Розглянуто принципи її роботи, переваги та обмеження.

Ключові слова: IPv6, корпоративна комп'ютерна мережа, Dual Stack, мережева інфраструктура, інформаційна безпека..

Abstract

The paper examines the features of using the IPv6 protocol in a corporate computer network. The issues of compatibility with the existing IPv4 infrastructure and the ways to address them are analyzed. The Dual Stack technology is investigated as the main approach for the phased migration of a corporate network to IPv6. Its operating principles, advantages, and limitations are discussed.

Keywords: IPv6, corporate computer network, Dual Stack, network infrastructure, information security..

Вступ

Сучасні корпоративні комп'ютерні мережі функціонують в умовах стрімкого зростання кількості мережевих пристроїв, розвитку хмарних технологій та підвищених вимог до масштабованості й безпеки. У цьому контексті використання протоколу IPv6 стає важливим етапом модернізації мережевої інфраструктури та забезпечення її довгострокової ефективності.

Протокол IPv6 надає значно більший адресний простір порівняно з IPv4, що дозволяє реалізувати ієрархічну адресацію та спростити управління корпоративною мережею. Завдяки вбудованій підтримці автоконфігурації адрес (SLAAC, DHCPv6) зменшується складність налаштування кінцевих пристроїв, а також підвищується гнучкість при масштабуванні мережі. Крім того, IPv6 забезпечує більш ефективну маршрутизацію за рахунок спрощеного заголовка пакета та зменшення навантаження на мережеве обладнання [1].

Результати дослідження

Використання протоколу IPv6 у корпоративному середовищі суттєво сприяє підвищенню рівня інформаційної безпеки мережевої інфраструктури. Однією з ключових переваг IPv6 є вбудована на рівні стандарту підтримка криптографічних механізмів IPsec, що дозволяє забезпечити автентифікацію, цілісність та конфіденційність переданих даних між мережевими вузлами. Завдяки цьому можливе створення захищених каналів зв'язку як між окремими сегментами корпоративної мережі, так і при організації віддаленого доступу співробітників до внутрішніх ресурсів [2].

Відмова від обов'язкового використання механізмів трансляції мережевих адрес (NAT), характерних для IPv4-мереж, значно спрощує реалізацію та адміністрування політик безпеки. Кожен пристрій у мережі IPv6 може мати унікальну глобальну адресу, що підвищує прозорість мережевого трафіку та полегшує ідентифікацію джерел і приймачів даних. Це, у свою чергу, дозволяє більш точно застосовувати правила міжмережевих екранів, систем виявлення вторгнень та засобів моніторингу безпеки.

Крім того, прозора адресація IPv6 спрощує інтеграцію корпоративних сервісів, зокрема вебзастосунків, поштових серверів та систем віддаленого адміністрування, без необхідності складних

схем пробросу портів і додаткових налаштувань. Це зменшує кількість потенційних помилок конфігурації, які можуть бути використані зловмисниками для здійснення атак. У контексті віддаленого доступу IPv6 забезпечує більш надійне та безпечне підключення користувачів до корпоративної мережі, що є особливо актуальним в умовах поширення дистанційної роботи [3].

Застосування протоколу IPv6 у корпоративній комп'ютерній мережі створює більш структуроване, кероване та безпечне мережеве середовище, що відповідає сучасним вимогам інформаційної безпеки та корпоративних стандартів захисту даних.

Важливим аспектом впровадження протоколу IPv6 у корпоративній комп'ютерній мережі є забезпечення його сумісності з уже наявною інфраструктурою, побудованою на основі IPv4. Оскільки більшість корпоративних сервісів, мережевого обладнання та прикладного програмного забезпечення продовжують функціонувати з використанням IPv4, повна відмова від цього протоколу на початковому етапі міграції є недоцільною та пов'язана з високими ризиками порушення стабільності роботи мережі [4].

На практиці для поетапного переходу до IPv6 найчастіше застосовується модель Dual Stack, яка передбачає одночасну підтримку протоколів IPv4 та IPv6 на мережевих пристроях, серверах і кінцевих вузлах. Такий підхід дозволяє поступово впроваджувати IPv6, тестувати його роботу в реальних умовах та забезпечувати взаємодію як із новими, так і з уже існуючими сервісами без необхідності їх негайної модернізації. При цьому вибір протоколу для передавання даних здійснюється автоматично, залежно від можливостей клієнта та доступності відповідних мережевих ресурсів.

Використання Dual Stack сприяє зниженню ризиків, пов'язаних із міграцією мережевої інфраструктури, оскільки у разі виникнення проблем з IPv6 зберігається можливість використання перевірених механізмів IPv4. Це забезпечує безперервність бізнес-процесів, стабільну роботу корпоративних інформаційних систем та мінімізує простої, які можуть негативно вплинути на діяльність організації. Крім того, поетапне впровадження дозволяє адміністраторам мережі накопичувати практичний досвід роботи з IPv6, адаптувати політики безпеки та оптимізувати мережеві налаштування.

Модель Dual Stack є ефективним та безпечним підходом до інтеграції IPv6 у корпоративну комп'ютерну мережу, що дозволяє забезпечити сумісність з наявною IPv4-інфраструктурою, знизити технічні та організаційні ризики та створити умови для поступового і контрольованого переходу до сучасних мережевих технологій.

Dual Stack — це підхід до побудови мережевої інфраструктури, за якого мережеві пристрої, сервери та кінцеві вузли одночасно підтримують протоколи IPv4 та IPv6. Кожен вузол у такій мережі має щонайменше одну IPv4-адресу та одну IPv6-адресу, що дозволяє забезпечити сумісність із наявною інфраструктурою та поступово впроваджувати IPv6 без відмови від IPv4.

У корпоративному середовищі Dual Stack є найбільш поширеною та безпечною моделлю міграції, оскільки не потребує кардинальної перебудови мережі та дозволяє зберегти працездатність усіх бізнес-критичних сервісів [4].

Принцип роботи Dual Stack полягає у тому, що в такій мережі кожен пристрій одночасно функціонує у двох стеків мережевих протоколів. Вибір протоколу для встановлення з'єднання здійснюється автоматично операційною системою або прикладним програмним забезпеченням на основі доступності сервісу та налаштувань DNS. Якщо сервер має як IPv4-, так і IPv6-адресу, клієнт віддає перевагу IPv6, а у разі його недоступності використовується IPv4.

Такий механізм забезпечує прозору для користувачів роботу мережі та дозволяє поступово переводити сервіси на IPv6 без переривання доступу.

У корпоративних мережах Dual Stack застосовується на різних рівнях інфраструктури:

- мережеве обладнання (маршрутизатори, комутатори рівня L3) підтримує маршрутизацію IPv4 та IPv6;
- сервери корпоративних сервісів (поштові, файлові, веб-сервери, сервери баз даних) налаштовуються для роботи з обома протоколами;
- кінцеві пристрої користувачів автоматично отримують IPv4- та IPv6-адреси за допомогою DHCP, DHCPv6 або SLAAC.

Це дозволяє організувати єдиний адресний простір та забезпечити стабільну взаємодію між усіма компонентами корпоративної мережі.

Основними перевагами використання Dual Stack у корпоративній комп'ютерній мережі є:

- поетапний і контрольований перехід від IPv4 до IPv6;
- мінімізація ризиків збоїв у роботі корпоративних сервісів;

- збереження сумісності з застарілими застосунками та обладнанням;
- можливість тестування IPv6 в реальному робочому середовищі;
- забезпечення безперервності бізнес-процесів.

Попри свої переваги, Dual Stack має низку недоліків:
- збільшення складності адміністрування мережі через необхідність підтримки двох протоколів;
- підвищені вимоги до кваліфікації мережевих адміністраторів;
- необхідність подвійного налаштування політик безпеки, маршрутизації та моніторингу;
- зростання навантаження на мережеве обладнання.

Ці фактори вимагають ретельного планування та документування мережевих налаштувань.

У середовищі Dual Stack важливо враховувати, що IPv6-трафік повинен бути так само захищений, як і IPv4. Часто зустрічається ситуація, коли політики безпеки налаштовані лише для IPv4, тоді як IPv6 залишається недостатньо захищеним. Тому необхідно забезпечити повну підтримку IPv6 на міжмережевих екранах, системах виявлення вторгнень та засобах моніторингу.

Dual Stack є проміжним, але надзвичайно важливим етапом переходу корпоративної мережі до повноцінного використання IPv6. Він дозволяє організації поступово адаптувати інфраструктуру, оновити обладнання, навчити персонал і підготуватися до майбутньої відмови від IPv4 без негативного впливу на стабільність роботи мережі.

Висновки

В результаті дослідження особливостей використання протоколу IPv6 у корпоративній комп'ютерній мережі встановлено, що його впровадження є важливим кроком у розвитку сучасної мережевої інфраструктури. IPv6 забезпечує значно більший адресний простір, спрощує процес адресації та створює умови для ефективного масштабування корпоративної мережі відповідно до зростаючих потреб організації.

Особливу роль у процесі міграції відіграє технологія Dual Stack, яка дозволяє одночасно використовувати IPv4 та IPv6 без порушення роботи існуючих корпоративних сервісів. Застосування цього підходу забезпечує сумісність з наявною інфраструктурою, мінімізує ризики виникнення збоїв і гарантує безперервність бізнес-процесів. Dual Stack дає можливість поступово адаптувати мережеве обладнання, програмне забезпечення та політики безпеки до вимог IPv6. Перехід до використання протоколу IPv6 з застосуванням моделі Dual Stack є доцільним і обґрунтованим рішенням для корпоративних комп'ютерних мереж, яке забезпечує стабільну роботу мережі в перехідний період та створює надійну основу для її подальшого розвитку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вишневський В. М., Ляхов А. А. Комп'ютерні мережі та телекомунікації: Навчальний посібник. — К.: Техніка, 2010. — 560 с.

2. Кучерявий Є. А. Сучасні мережеві технології: Навчальний посібник. — Харків: ХНУРЕ, 2016. — 312 с.

3. Олійник А. О., Ковальчук Л. В. Інформаційна безпека комп'ютерних мереж: Навчальний посібник. — Львів: Видавництво Львівської політехніки, 2018. — 284 с.

4. Баглай В. І. Організація комп'ютерних мереж і телекомунікаційних систем. — Вінниця: ТОВ "Нілан-ЛТД", 2017. — 432 с.

Обертюх Максим Романович — PhD., доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця

Мельник Ярослав Іванович — студент групи 2КІ-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Obertiukh Maksym — PhD, Associate Professor of the Department of Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Melnyk Yaroslav — student of Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.