УДК 004.7

Ліщинський В.В., здобувач,
Романець О. А., здобувач,
Марчук Я. В., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

РОЛЬ DHCPv6 У АВТОМАТИЧНІЙ КОНФІГУРАЦІЇ IPv6-АДРЕС У КОРПОРАТИВНИХ МЕРЕЖАХ

Швидке зростання кількості мережевих пристроїв у корпоративних інфраструктурах та перехід до IPv6 створили потребу у гнучких та керованих механізмах автоматичної конфігурації мережевих параметрів. Одним з ключових інструментів, який забезпечує централізоване та масштабоване налаштування хостів в IPv6-середовищі, є протокол DHCPv6.

На відміну від IPv4-версії, DHCPv6 тісно взаємодіє з протоколами SLAAC та Neighbor Discovery, що дозволяє створювати комбіновані методи конфігурації. DHCPv6 підтримує як stateful, так і stateless режими роботи. У stateful-режимі сервер повністю керує видачею IPv6-адрес і зберігає записи про клієнтів, що важливо для аудиту, журналювання та доступності. Stateless-режим дозволяє надавати додаткову інформацію (DNS, доменні параметри), залишаючи призначення адрес механізмам SLAAC. Такий підхід робить DHCPv6 гнучким інструментом, який може бути адаптований під різні корпоративні сценарії.

Використання DHCPv6 дозволяє легко масштабувати мережу: великі IPv6-префікси можуть ефективно розподілятися між тисячами хостів без додаткових ускладнень, що є критично важливим для швидкозростаючих корпоративних середовищ. У динамічних середовищах, де постійно додаються IoT-пристрої, робочі станції або сервери, DHCPv6 забезпечує автоматичне надання необхідних параметрів, роблячи такі зміни прозорими та керованими.

DHCPv6 має важливе значення у підвищенні рівня безпеки корпоративної інфраструктури. По-перше, кожен клієнт ідентифікується унікальним DUID, що унеможливлює конфлікт адрес та дозволяє відстежувати активність конкретних пристроїв. По-друге, централізована конфігурація DNS-серверів допомагає впроваджувати політики фільтрації, моніторингу та захисту від фішингу. По-третє, у поєднанні з Relay-агентами DHCPv6 дозволяє контролювати видачу параметрів між сегментами мережі, що знижує ризик підробки конфігураційних повідомлень.

Додатково DHCPv6 сприяє побудові сегментованих і керованих мереж відповідно до концепцій Zero Trust та Network Access Control, забезпечуючи співпрацю з механізмами 802.1X, firewall-політиками та ACL.

У великих мережах DHCPv6 часто поєднується з системами керування (Cisco Prime, SolarWinds, Zabbix), забезпечуючи повний контроль над адресним простором.

Попри численні переваги, використання DHCPv6 має деякі обмеження:

- потребує додаткової інфраструктури (сервери, relay-агенти);
- складніша конфігурація, особливо при комбінуванні зі SLAAC; затримки у видачі параметрів у великих мережах, якщо сервери перевантажені;
- залежність від довіреної взаємодії з Router Advertisements, оскільки саме вони визначають, чи використовуватиметься DHCPv6;
- повільніше відновлення після збоїв, якщо сервер DHCPv6 є єдиною точкою конфігурації без резервування.

Однак ці недоліки можуть бути мінімізовані за рахунок використання кластерів DHCPv6, резервування та коректної сегментації мереж.

DHCPv6 відіграє ключову роль у побудові сучасних корпоративних мереж на базі IPv6, забезпечуючи централізовану, гнучку та безпечну автоматичну конфігурацію мережевих параметрів. Його інтеграція з іншими компонентами IPv6 дозволяє ефективно масштабувати інфраструктуру, підвищувати рівень безпеки та покращувати мережеве управління.

Список використаних джерел:

1. John RFC 8415: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). *IETF Datatracker*. URL: https://datatracker.ietf.org/doc/html/rfc8415
2. What is an IPv6 Address?. *Bright Data*. URL: https://surl.lu/hpehxx
3. DHCPv6 Server | Junos OS | Juniper Networks. *Juniper Networks, Now Part of HPE – Leading the Convergence of AI & Networking*. URL: https://www.juniper.net/documentation/us/en/software/junos/dhcp/topics/topic-map/dhcpv6-server.html