https://doi.org/10.31891/2307-5732-2026-361-67
УДК 004.056.5

ПЕТКОВ ЄВГЕН
Міжнародний університет, м.Одеса, Україна
https://orcid.org/0009-0000-8248-5408
e-mail: yepetkov@gmail.com
СТРЕЛКОВСЬКА ЮЛІЯ
Ворзінг коледж, Ворзінг, Велика Британія
http://orcid.org/0000-0002-9835-0222
e-mail: 4800632s@gmail.com

АНАЛІЗ ТИПІВ СПУФІНГ АТАК ТА ЗАСОБІВ ЗАХИСТУ НА МЕРЕЖІ РІВНЯ ДОСТУПУ

Дослідження включає аналіз типів Spoofing-атак та засобів боротьби з ними в мережі рівня доступу. Розглядаються чотири поширені типи спуфінг атак: MAC Spoofing, DHCP Spoofing, ARP Spoofing та IP Spoofing, детально описуються їхні механізми, потенційний вплив та стратегії захисту.

Ключові слова: *атаки типу спуфінг (spoofing), MAC-адреса, MAC Spoofing атаки, DHCP Spoofing атаки, ARP Spoofing атаки, IP Spoofing атаки.*

PETKOV YEVGEN
International University, Odesa, Ukraine
STRELKOVSKA JULIYA
Worthing college, Worthing, United Kingdom

ANALYSIS OF TYPES OF SPOOFING ATTACKS AND PROTECTION MEANS AT THE ACCESS NETWORK LAYER

In the article, the authors delve into the critical area of network security, focusing on spoofing attacks that exploit vulnerabilities in computer networks, starting with the access layer network. Spoofing attacks involve impersonating legitimate individuals or devices to gain unauthorized access, intercept data, or disrupt services, creating significant threats to network integrity, confidentiality, and availability. This paper systematically examines four prevalent types of spoofing attacks: MAC spoofing, DHCP spoofing, ARP spoofing, and IP spoofing, detailing their mechanisms, potential impacts, and corresponding defensive strategies. MAC spoofing is one of the main attacks discussed. With this technique, an attacker changes the MAC address of their network interface card (NIC) to mimic the MAC address of an authorized device. Moving to DHCP spoofing, the paper explores how attackers impersonate legitimate Dynamic Host Configuration Protocol (DHCP) servers to distribute malicious IP configurations. In a typical network, DHCP servers automatically assign IP addresses, subnet masks, gateways, and DNS servers to clients. A rogue DHCP server can respond faster to client requests or provide false information, redirecting traffic to attacker-controlled gateways for man-in-the-middle (MITM) interception. ARP spoofing, or Address Resolution Protocol spoofing, is another key focus, where attackers poison the ARP cache of devices to associate their MAC-address with the IP-address of a legitimate host, such as a gateway. By sending gratuitous ARP replies, attackers can redirect traffic intended for the victim through their machine. Finally, IP-spoofing is analyzed as a technique where attackers forge the source IP address in packet headers to disguise their origin. This occurs at the network layer (Layer 3) and is commonly used in DDoS attacks, where spoofed packets amplify traffic to overwhelm targets. The study evaluates effective countermeasures, including port security, 802.1X authentication protocols, DHCP snooping, dynamic ARP inspection, IP Source Guard on switches, ingress/egress filtering and Unicast Reverse Path Forwarding (uRPF)verification on routers, advocating for a layered defense approach. This comprehensive analysis serves as a valuable resource for network engineers, security professionals, and researchers aiming to fortify access networks against evolving spoofing threats, emphasizing proactive measures to safeguard digital infrastructures in an increasingly hostile cyber landscape.

Keywords: *spoofing attacks, MAC-address, MAC Spoofing attacks, DHCP Spoofing attacks, ARP Spoofing attacks, IP Spoofing attacks*

Стаття надійшла до редакції / Received 22.11.2025
Прийнята до друку / Accepted 11.01.2026
Опубліковано / Published 29.01.2026

Формулювання цілей статті

Метою роботи є проаналізувати типи спуфінг атак, принципи їх дії та можливі засоби боротьби безпосередньо в мережі рівня доступу.

Виклад основного матеріалу

Атаки типу спуфінг (spoofing) — це категорія кібератак, де зловмисник підробляє ідентичність (наприклад, свою MAC-адресу, IP-адресу тощо), щоб виглядати як довірена особа чи пристрій. Основні цілі таких атак включають:

- Несанкціонований доступ до систем або мереж.
- Перехоплення конфіденційних даних, таких як паролі, фінансові дані чи особиста інформація.
- Введення в оману, наприклад, для фішингу чи розсилки шкідливого ПЗ.

MAC Spoofing атаки. Зазвичай мережевий комутатор рівня L2 (switch) за замовчуванням автоматично вивчає MAC-адреси пристроїв, підключених до його портів, не обмежуючи кількість MAC-адрес, які можуть бути вивчені для одного порту, і не блокує записи в CAM-таблиці. Зловмисник може скористатися цими слабкими місцями кількома методами.

- По-перше, підробити (продублювати) MAC-адресу іншого легітимного хоста в локальній мережі. Хакер відправляє Ethernet кадр з такою ж самою MAC-адресою відправника, і комутатор оновить в своїй CAM-

таблиці запис, що посилається на викрадену MAC-адресу вже за портом підключення зловмисника, а не легітимного пристроя. Приклад атаки зображено на рис.1.

- По-друге, зловмисник може швидко заповнити CAM таблицю комутатора, надсилаючи велику кількість Ethernet кадрів, з різними підробленими MAC-адресами відправника. Після переповнення CAM-таблиці комутатор більше не може вивчати нові записи та не знає, куди пересилати кадри хостам яких немає в таблиці. Коли в CAM-таблиці немає відповідного запису для MAC-адреси призначення кадру, комутатор відправляє кадри широкомовним способом на всі свої порти, фактично діючи як хаб. Зловмисник таким чином може отримувати трафік, який йому не відправлявся джерелом. Це є MAC flooding, різновид атаки типу MAC Spoofing.

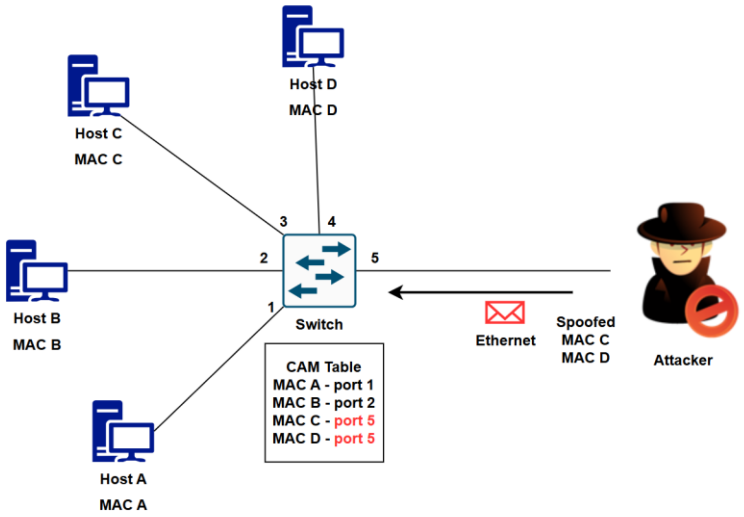

Рис. 1. Приклад атаки типу MAC Spoofing

Для боротьби з MAC Spoofing атаками можна використовувати такий функціонал комутаторів доступу як Port security [2-3]. Активація його дозволяє: по-перше, обмежити кількість MAC-адрес вивчаємих на порту комутатора, по-друге, прив'язати певні MAC-адреси до певних портів комутатора в CAM-таблиці після їх першого вивчення.

Іншим засобом боротьби з MAC Spoofing може використовуватись протокол 802.1x для аутентифікації підключених пристроїв та запобіганню їх несанкціонованому доступу до мережі. Пристрій при початковому підключенні до порта комутатора залишається заблокованим для всього типу трафіка окрім 802.1x. Комутатор надсилає клієнту запит на аутентифікацію, і пристрій з підримкою 802.1x надає свої облікові дані, які комутатор (аутентифікатор) відправляє серверу аутентифікації, і якщо вони правильні – пристрою розблоковується порт з повним доступом до мережі. Також при будь-якому засобі боротьби важливо здійснювати моніторинг мережевої інфраструктури, та виявляти тимчасові або постійні зміни MAC-адрес за допомогою систем аналізу логів подій.

DHCP Spoofing атаки. В основі такої атаки лежить імітація зловмисником DHCP-сервера в локальній мережі. Пристрої, налаштовані на отримання мережевих параметрів через протокол DHCP, надсилають запит у локальну мережу (зазвичай перший пакет DHCP Discover є широкомовним і розсилається всім хостам у мережі). На цьому етапі зловмисник може перехопити запит клієнта і від імені фальшивого DHCP-сервера надіслати пропозицію DHCP Offer із підробленими параметрами конфігурації (такими як IP-адреса, шлюз за замовчуванням або DNS-сервери). У результаті клієнт може прийняти цю пропозицію від нелегітимного сервера швидше, ніж від легітимного. Приклад атаки зображено на рис.2. Таким чином, зловмисний DHCP сервер може організувати більш складну атаку "людина посередині" (man-in-the-middle), наприклад, надавши клієнту свою IP адресу як шлюз за замовчуванням. Тоді кінцевий хост з отриманим неправильним налаштуванням буде пересилати свій трафік через пристрій зловмисника. Або з іншого боку, зловмисник може просто перевантажити чи зробити локальну мережу непрацездатною, надсилаючи надмірну кількість підроблених відповідей DHCP сервера.

Можливий засіб боротьби з даним типом атак – це активація на комутаторах рівня доступу функції DHCP snooping. Цей функціонал в першу чергу дозволяє розділити всі порти комутатора на довірені та недовірені (trusted, untrusted). За замовчуванням після активації функціоналу DHCP snooping всі порти стають недовіреними (untrusted) – до них підключаються клієнти. З недовірених портів комутатор дозволяє приймати DHCP запити, але забороняє приймати відповіді DHCP сервера. При спробі пристроєм підключеним до недовіреного порта відправити пакет серверної DHCP відповіді – він буде видалений комутатором. Тільки окремі порти спеціально налаштовуються адміністратором як довірені (trusted), і тільки до таких портів може бути підключений легітимний DHCP сервер, DHCP відповіді якого будуть передаватись комутатором на інші порти. Крім цього, комутатор з функціоналом DHCP snooping аналізує інформацію в DHCP пакетах (запити від клієнтів та відповіді сервера), на основі якої будує базу прив'язки DHCP snooping binding table, яка містить по кожному клієнту: MAC адресу, порт підключення, IP адресу отриману від сервера в оренду, час оренди IP-адреси,

клієнтський VLAN, тощо. Ця база прив'язки DHCP параметрів відіграє важливу роль і для функціонування інших фунціоналів безпеки на комутаторах доступа, таких як Dynamic ARP Inspection, та IP Source Guard.

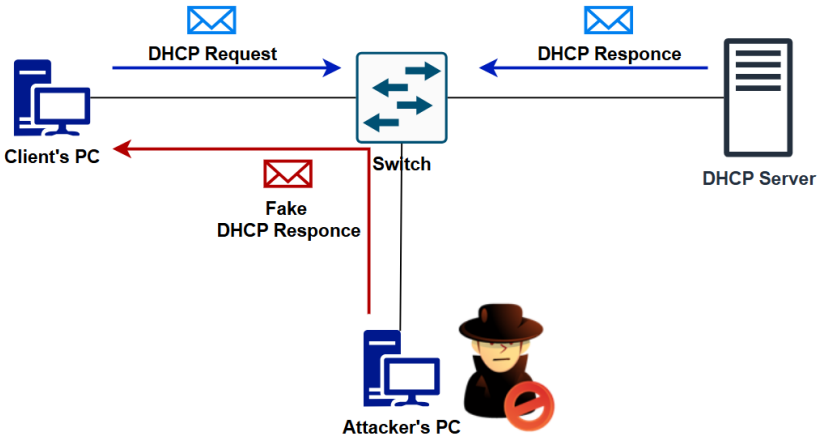

Рис. 2. Приклад атаки типу DHCP Spoofing

Слід зазначити, що для критично важливих пристроїв у локальній мережі, таких як сервери чи маршрутизатори, зазвичай налаштовують статичні IP-адреси та фіксовані параметри підключення, замість використання динамічного отримання IP-параметрів.

ARP Spoofing атаки. Для здійснення цієї атаки зловмисник відправляє жертві фальшиві ARP-пакети, пов'язуючи свою MAC-адресу з IP-адресою іншого пристрою в локальній мережі. Особливість протоколу ARP полягає в тому, що зловмисник може надсилати ARP-відповіді навіть без отримання попереднього ARP-запиту від клієнта, тим самим отруюючи ARP-кеш жертви [4].

Розглянемо ситуацію на рисунку 3. Клієнт потребуючи взаємодії зі «шлюзом за замовчуванням» своєї мережі знає IP адресу шлюза (192.168.0.1), але не знає його MAC адреси. Для динамічного визначення MAC-адреси пристрою за відомою IP-адресою у локальній мережі використовується протокол ARP (Address Resolution Protocol). Також кожен пристрій підтримує свою локальну ARP-таблицю (кеш), де зберігається відповідність IP-адрес до MAC-адрес інших пристроїв мережі. Але зловмисник в цій же локальній мережі може відправляти підроблені ARP відповіді, наприклад:

- Клієнту-жертві: «IP-адреса шлюзу 192.168.0.1 має MAC-адресу C (зловмисника)»;
- Шлюзу: «IP-адреса клієнта 192.168.0.11 має MAC-адресу C (зловмисника)».

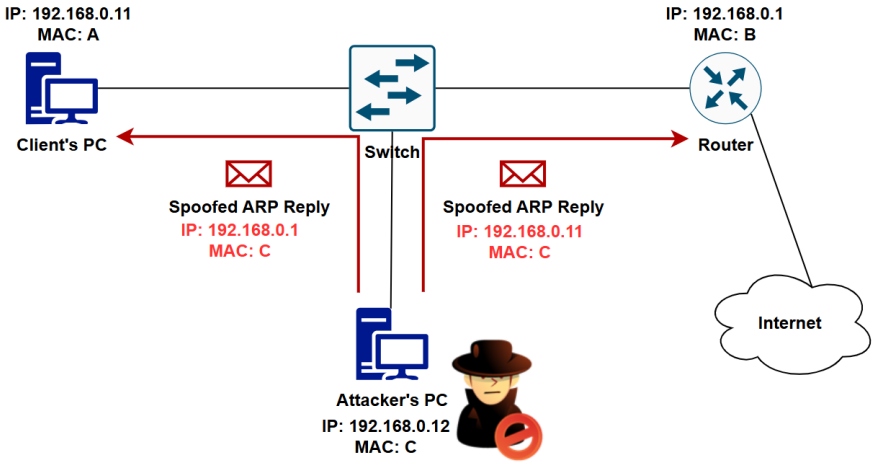

Рис. 3. Приклад атаки типу ARP Spoofing

Таким чином жертви ARP Spoofing атаки в локальній мережі будуть відправляти Ethernet пакети неправильному хосту (зловмиснику). Зловмисник в свою чергу, може отримувати чужий трафік з важливою інформацією, персональними даними, а також займатися підміною даних. Перенаправляючи пакети між скомпрометованими жертвами атаки, як в розглянутому випадку між клієнтом та шлюзом, зловмисник здійснює атаку "людина посередині" (man-in-the-middle).

Для боротьби з ARP Spoofing атаками можна використовувати статичні ARP записи на окремих пристроях, але це не зовсім ефективна процедура в мережах з великою кількістю пристроїв та ускладнює адміністрування. Більш зручною є активація на комутаторах доступу функції Dynamic ARP Inspection (DAI), яка працює разом із функціоналом DHCP snooping. Комутатор з функцією DAI інспектує клієнтські ARP пакети

та перевіряє на відповідність IP-адрес до MAC-адрес у ARP відповідях з власною базою прив'язки DHCP snooping binding table. Якщо у клієнському ARP пакеті невірна інформація – він буде відкинутий. Подібно до DHCP snooping, в конфігурації DAI також визначаються довірені та недовірені порти (trusted, untrusted). DAI перевіряє усі ARP-пакети, отримані на недовірених портах, які можна налаштовувати для великої кількості портів клієнського обладнання. Пакети, що надходять на довірені інтерфейси, які можна налаштовувати для серверного обладнання, обходять усі перевірки DAI.

IP Spoofing атаки. В цьому типу атаки зловмисник змінює свою вихідну IP-адресу в заголовку IP пакетів, щоб приховати свою ідентичність або видати себе за інший пристрій, наприклад, довірений сервер чи користувача [5]. Цей тип атаки може бути використаний як частина DoS/DDoS атаки. Наприклад, якщо зловмисник відправить велику кількість підроблених запитів на сервер від різних «відправників», а віддалений сервер буде намагатись відповідати на кожен такий запит, відкриваючи велику кількість TCP сессій і витрачаючи свої ресурси. Або з іншого боку, якщо на одну легітимну IP-адресу клієнта прийдуть відповіді від серверів, які він не замовляв – це також буде прикладом атаки на відмову ресусів жертви. Приклад атаки зображено на рис.4.

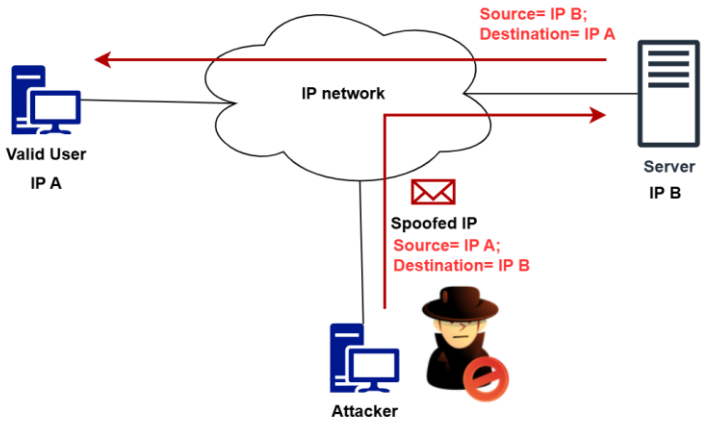

Рис. 4. Приклад атаки типу IP Spoofing

Для протидії IP Spoofing атакам можна застосувати безпосередньо на комутаторі рівня доступу функціонал IP Source Guard, який перевіряє достовірність вхідної IP-адреси пакетів, що надходять на порт комутатора. IP Source Guard може використовувати таблицю прив'язки DHCP snooping binding table (якщо такий активовано та клієнт використовує протокол DHCP для мережевого налаштування) або статичні прив'язки IP-адрес до портів підключення недовірених пристроїв. Таким чином, будь-який вхідний IP пакет з вихідною IP-адресою, відмінною від тієї, що призначена по DHCP або статичної конфігурації, буде видалено. Також на маршрутизаторах це може бути Anti-spoofing функціонал, який фільтрує вхідні пакети з використанням списків контролю доступу (ACL), або перевіряє на присутність в таблиці маршрутизації зворотнього маршрута до підмережі від якої прийшов вхідний IP пакет через той самий інтерфейс маршрутизатора на який був прийнятий цей пакет.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Таким чином, функції безпеки комутаторів рівня доступу, такі як Port security, DHCP snooping, Dynamic ARP Inspection та IP Source Guard дозволяють блокувати більшість спуфінг-атак безпосередньо в локальній мережі та максимально близько до потенційного джерела загрози. Однак варто враховувати, що підтримка цих функцій безпеки залежить від моделі та виробника комутаторів, що необхідно врахувати під час проєктування надійної, відмовостійкої та безпечної мережі. Також протоколи аутентифікації та ідентифікації пристроїв відіграють ключову роль, так само як професійне адміністрування, правильна конфігурація та попередній вибір дизайну мережі, своєчасне оновлення обладнання та програмного забеспечення, постійний моніторинг і своєчасне виявлення підозрілих активностей. Впровадження мереж SDN з централізованим керуванням мережевими пристроями, автоматизованими засобами моніторингу та шаблонами реагування, зможуть зменшити вплив атак, які дедалі будуть ставати складніше. Безумовно, для мінімізації впливу атак типу "людина посередині" (man-in-the-middle) необхідно застосовувати протоколи шифрування мережевого трафіку.

Література

1. Петков Є. І. Типи спуфінг атак та засобів захисту в локальних мережах / Є. І. Петков // Передові технології в інформаційно-комунікаційній інженерії (ATICE'2025) : матеріали Міжнародної конференції / за заг ред. С. В. Ківалова ; Міжнародний гуманітарний університет. Одеса : Видавничий дім «Гельветика», 2025. С. 85-90. URL: https://hdl.handle.net/11300/30133; DOI: 10.32837/11300.30133

2. The Cisco Learning Network. Layer 2 Security Features. URL: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKLCEA4/members-choice-layer-2-security-features.

3. Wikipedia. MAC spoofing. URL: https://en.wikipedia.org/wiki/MAC_spoofing.
4. Wikipedia. ARP spoofing. URL: https://en.wikipedia.org/wiki/ARP_spoofing.
5. Wikipedia. IP address spoofing. URL: https://en.wikipedia.org/wiki/IP_address_spoofing.
6. Best Practices for Securing Cisco Switches in Enterprise Environments. URL: https://community.cisco.com/t5/cisco-cafe-blogs/best-practices-for-securing-cisco-switches-in-enterprise/ba-p/5243372.
7. Cisco. Port Security. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/port_security.pdf.
8. ManageEngine. DHCP snooping. URL: https://www.manageengine.com/products/oputils/tech-topics/dhcp-snooping.html.
9. Cisco. Configuring Dynamic ARP Inspection. URL: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/security/503_u2_2/Cisco_n3k_security_cg_503_u2_2_chapter11.html?dtid=osscdc000283&linkclickid=srch.
10. Cisco. Configuring IP Source Guard. URL: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0110110.html.

References

1. Petkov Y. I. Typy spufinh atak ta zasobiv zakhystu v lokalnykh merezhakh / Y. I. Petkov // Perodovi tekhnolohii v informatsiino-komunikatsiyniy inzhenerii (ATICE'2025) : materialy Mizhnarodnoi konferentsii / za zah red. S. V. Kivalova ; Mizhnarodnyi humanitarnyi universytet. Odesa : Vydavnychyi dim «Helvetyka», 2025. S. 85-90. URL: https://hdl.handle.net/11300/30133; DOI: 10.32837/11300.30133
2. The Cisco Learning Network. Layer 2 Security Features. URL: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKLCEA4/members-choice-layer-2-security-features.
3. Wikipedia. MAC spoofing. URL: https://en.wikipedia.org/wiki/MAC_spoofing.
4. Wikipedia. ARP spoofing. URL: https://en.wikipedia.org/wiki/ARP_spoofing.
5. Wikipedia. IP address spoofing. URL: https://en.wikipedia.org/wiki/IP_address_spoofing.
6. Best Practices for Securing Cisco Switches in Enterprise Environments. URL: https://community.cisco.com/t5/cisco-cafe-blogs/best-practices-for-securing-cisco-switches-in-enterprise/ba-p/5243372.
7. Cisco. Port Security. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/port_security.pdf.
8. ManageEngine. DHCP snooping. URL: https://www.manageengine.com/products/oputils/tech-topics/dhcp-snooping.html.
9. Cisco. Configuring Dynamic ARP Inspection. URL: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/security/503_u2_2/Cisco_n3k_security_cg_503_u2_2_chapter11.html?dtid=osscdc000283&linkclickid=srch.
10. Cisco. Configuring IP Source Guard. URL: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0110110.html.