УКРАЇНА

(19) UA (11) 161742 (13) U

(51) МПК (2025.01)
H04L 12/00

НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНА ОРГАНІЗАЦІЯ "УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ОФІС ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ІННОВАЦІЙ"

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2024 05451**

(22) Дата подання заявки: **18.11.2024**

(24) Дата, з якої є чинними права інтелектуальної власності: **01.01.2026**

(46) Публікація відомостей про державну реєстрацію: **31.12.2025, Бюл.№ 53**

(72) Винахідник(и):
Гурко Олександр Геннадійович (UA),
Кудінов Євген Олександрович (UA)

(73) Володілець (володільці):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АВТОМОБІЛЬНО-ДОРОЖНІЙ УНІВЕРСИТЕТ,
вул. Ярослава Мудрого, 25, м. Харків, 61002 (UA)

(74) Представник:
Азарова Алла Володимирівна

(54) СПОСІБ ПЕРЕДАЧІ ДОДАТКОВИХ МАРШРУТІВ VPN-КЛІЄНТУ ПО ПРОТОКОЛУ ТИПУ POINT-TO-POINT В ОПЕРАЦІЙНІЙ СИСТЕМІ МАРШРУТИЗАТОРА

(57) Реферат:

Спосіб передачі додаткових маршрутів VPN-клієнту через протокол типу point-to-point в операційній системі маршрутизатора включає дії, в ході яких підключають клієнтський пристрій до серверного обладнання через PPP-з'єднання. Обмін сигналами йде через протокол LCP, налаштовують мережевий рівень через IPCP, передають пакети даних DHCPINFORM від клієнтського пристрою та надсилають у відповідь пакети даних DHCPACK з додатковою маршрутною інформацією. Пакети даних DHCPINFORM, що надходять від клієнтського пристрою, перенаправляють за допомогою програмно-апаратного блока трансляції пакетів DHCP до внутрішнього DHCP-сервера, що функціонує на тому ж самому серверному обладнанні. Пакети даних DHCPACK надсилають від вказаного внутрішнього DHCP-сервера до клієнтського пристрою.

UA 161742 U

Дана корисна модель належить до галузі телекомунікаційних технологій та комп'ютерних мереж, зокрема способів керування фізичним обладнанням для обробки та маршрутизації пакетів даних у системах зв'язку при з'єднанні за протоколом VPN (Virtual Private Network) типу "точка - точка" (point-to-point protocol, PPP) між клієнтським пристроєм та серверним обладнанням.

VPN є технологією, що дозволяє створювати безпечні мережеві з'єднання поверх публічної мережі (наприклад інтернет). Вона широко використовується для надання віддаленим користувачам доступу до корпоративних мереж, які функціонують на базі фізичного серверного обладнання (сервера VPN).

Для забезпечення безпечного доступу використовують протоколи тунелювання, такі як L2TP та SSTP. При встановленні VPN-з'єднання виникає технічна проблема передачі клієнтському пристрою інформації про статичні маршрути до внутрішніх мережевих ресурсів. Без автоматизації цього процесу адміністратор змушений вручну налаштовувати таблиці маршрутизації на кожному клієнтському пристрої, що є трудомістким та неефективним.

Відомий спосіб передачі інформації про маршрути до мережевих адрес (https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd469790(v=ws.11)?redirectedfrom=MSDN), реалізований компанією Microsoft у сервісі "Маршрутизація та віддалений доступ (RRAS)», що працює на серверній операційній системі Windows. Цей спосіб вимагає взаємодії фізичного серверного обладнання з операційною системою Windows з окремим сервісом DHCP. Недоліками способу є високі вимоги до апаратних ресурсів серверного обладнання, вартість ліцензійного програмного забезпечення та обмежена підтримка протоколів.

Відоме також програмне рішення SoftEther (https://www.softether.org), яке є кросплатформним, однак воно також має обмежений набір підтримуваних протоколів VPN.

Найбільш близьким аналогом є спосіб, реалізований в операційній системі RouterOS (https://mikrotik.com/download), встановленій на спеціалізованому серверному обладнанні (маршрутизаторі). Цей спосіб полягає у підключенні клієнтського пристрою за допомогою протоколів PPP. Після встановлення з'єднання, клієнтський пристрій надсилає широкомовні пакети DHCPINFORM для отримання додаткової інформації, зокрема маршрутів. Недоліком цього способу є те, що вбудований у RouterOS DHCP-сервер технічно не може обробляти ці запити від VPN-клієнтів. Тому для реалізації способу необхідно використовувати окремий, зовнішній фізичний сервер з операційною системою (Windows, Linux тощо), на якому запущено DHCP-сервер. Це призводить до ускладнення фізичної архітектури системи, вимагає додаткового апаратного забезпечення з відповідними матеріальними витратами, збільшує енергоспоживання всієї системи та знижує її надійність через наявність додаткової точки відмови (зовнішнього сервера). Крім цього, використання окремого DHCP-сервера ускладнює адміністрування та налаштування системи й призводить до неоптимального використання обчислювальних ресурсів маршрутизатора.

В основу корисної моделі поставлено задачу удосконалення способу взаємодії апаратних і програмних компонентів серверного обладнання, що працює під управлінням операційної системи маршрутизатора, для передачі маршрутної інформації клієнтському пристрою VPN.

Поставлена задача вирішується тим, що в способі передачі додаткових маршрутів VPN-клієнту через протокол типу point-to-point на операційній системі маршрутизатора, що включає дії, в ході яких підключають клієнтський пристрій до серверного обладнання через PPP-з'єднання, де обмін сигналами йде через протокол LCP, налаштовують мережевий рівень через IPCP, передають пакети даних DHCPINFORM від клієнтського пристрою та надсилають у відповідь пакети даних DHCPACK з додатковою маршрутною інформацією, згідно з корисною моделлю, пакети даних DHCPINFORM, що надходять від клієнтського пристрою, перенаправляють за допомогою програмно-апаратного блока трансляції пакетів DHCP до внутрішнього DHCP-сервера, що функціонує на тому ж самому серверному обладнанні, а пакети даних DHCPACK надсилають від вказаного внутрішнього DHCP-сервера до клієнтського пристрою.

Технічним результатом, на вирішення якого спрямована корисна модель, є підвищення енергоефективності та надійності системи зв'язку в цілому, а також оптимізація використання обчислювальних ресурсів серверного обладнання. Цей результат вирішують за рахунок усунення необхідності в окремому фізичному сервері для DHCP-служб, що, в свою чергу, знижує загальне енергоспоживання системи, усуває зовнішню апаратну точку відмови та дозволяє виконувати всі операції в межах одного фізичного пристрою під час обробки мережевих сигналів.

На кресленні зображена функціональна схема взаємодії апаратних та програмних компонентів при реалізації запропонованого способу, де: 1 - клієнтський пристрій; 2 - сервер VPN, реалізований на серверному обладнанні під управлінням операційної системи маршрутизатора; 3 - блок трансляції пакетів DHCP, реалізований як програмно-апаратний модуль у складі маршрутизатора; 4 - внутрішній сервер DHCP, що функціонує на тому ж серверному обладнанні, що і сервер VPN.

Відомості, що підтверджують можливість здійснення корисної моделі

Спосіб реалізують за допомогою серверного обладнання (наприклад маршрутизатора MikroTik), на якому встановлена операційна система маршрутизатора, та віддаленого клієнтського пристрою.

Послідовності дій над матеріальними об'єктами, згідно із запропонованим способом:

1. Клієнтський пристрій (1) встановлює фізичне з'єднання та тунель з серверним обладнанням, на якому працює сервер VPN (2).

2. Між клієнтським пристроєм (1) та сервером (2) відбувається обмін сигналами LCP для налаштування канального рівня, після чого виконують автентифікацію.

3. Сервер VPN (2) за допомогою протоколу IPCP надає IP-адресу клієнтському пристрою (1).

4. Клієнтський пристрій (1) генерує та надсилає через тунель широкомовні пакети даних DHCPINFORM для запиту додаткової маршрутної інформації.

5. Ці пакети даних надходять на сервер VPN (2) і перенаправляють до блока трансляції пакетів DHCP (3), реалізованого на тому ж апаратному забезпеченні.

6. Блок (3) модифікує пакети та направляє їх до внутрішнього DHCP-сервера (4), що функціонує на тому ж фізичному пристрої.

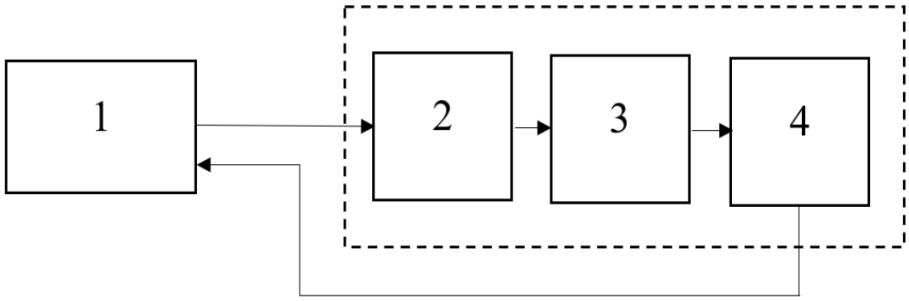
7. Внутрішній DHCP-сервер (4), отримавши запит, генерує пакети даних DHCPACK, що містять необхідну маршрутну інформацію, та відправляє їх через тунель до клієнтського пристрою (1).

Таким чином, запропонований спосіб змінює архітектуру обробки та маршрутизації пакетів даних всередині одного фізичного пристрою. Це дозволяє відмовитися від використання окремого зовнішнього сервера, що безпосередньо призводить до зниження споживання електроенергії, підвищення надійності системи зв'язку (за рахунок усунення зовнішньої точки відмови) та більш ефективного використання ресурсів існуючого серверного обладнання.

Запропонований спосіб може бути багаторазово реалізований у галузі телекомунікацій та інформаційних технологій, зокрема, при налаштуванні корпоративних та приватних мереж інтернет-провайдерами, системними адміністраторами та IT-спеціалістами. Для його здійснення використовують стандартне, широко розповсюджене та комерційно доступне серверне обладнання (маршрутизатори), що працює під управлінням операційної системи, наприклад RouterOS, та стандартні клієнтські пристрої. Таким чином, спосіб не потребує створення спеціальних спеціальних технічних засобів і може бути застосований у галузі телекомунікаційних технологій та комп'ютерних мереж безпосередньо на основі інформації, наведеної в матеріалах заявки.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб передачі додаткових маршрутів VPN-клієнту через протокол типу point-to-point в операційній системі маршрутизатора, що включає дії, в ході яких підключають клієнтський пристрій до серверного обладнання через PPP-з'єднання, де обмін сигналами йде через протокол LCP, налаштовують мережевий рівень через IPCP, передають пакети даних DHCPINFORM від клієнтського пристрою та надсилають у відповідь пакети даних DHCPACK з додатковою маршрутною інформацією, який **відрізняється** тим, що пакети даних DHCPINFORM, що надходять від клієнтського пристрою, перенаправляють за допомогою програмно-апаратного блока трансляції пакетів DHCP до внутрішнього DHCP-сервера, що функціонує на тому ж самому серверному обладнанні, а пакети даних DHCPACK надсилають від вказаного внутрішнього DHCP-сервера до клієнтського пристрою.



Комп'ютерна верстка С. Чулій

ДО "Український національний офіс інтелектуальної власності та інновацій", вул. Дмитра Годзенка, 1, м. Київ – 42, 01601