Engineer

DHCP

протокол, що видає пристроям IP-адреси й мережеві параметри

Що це таке

DHCP (Dynamic Host Configuration Protocol) — це спосіб, у який пристрій, що щойно під'єднався до мережі, дізнається, яке місце він у ній займає. Ноутбук, що під'єднується до мережі Wi-Fi, знає власну апаратну адресу і майже нічого більше. DHCP дає йому IP-адресу, маску підмережі, маршрутизатор, через який слід надсилати трафік, і DNS-сервери, до яких слід звертатися, і нікому не треба нічого вводити вручну. Протокол визначено в RFC 2131, опублікованому в березні 1997 року; його анотація описує DHCP як основу для передавання конфігураційної інформації хостам у мережі TCP/IP. Він виріс зі старішого Bootstrap Protocol, BOOTP, і головним, що він додав, став автоматичний розподіл адрес, які можна використовувати повторно.

RFC 2131 називає три способи видати адресу. За автоматичного розподілу клієнт отримує постійну адресу. За динамічного він отримує адресу на обмежений час або доки сам її не поверне. За ручного адресу вибирає мережевий адміністратор, а DHCP лише доставляє її. Динамічний розподіл — єдиний із трьох, за якого адреса сама повертається до пулу, щойно її власникові вона більше не потрібна, і саме про цей механізм ідеться в решті статті.

Таке тимчасове надання адреси називають орендою (lease). Клієнт може продовжити оренду, повернути адресу достроково і навіть попросити безстрокову оренду; RFC зауважує, що сервер однаково може віддавати перевагу довгим, але скінченним термінам, щоб рано чи пізно помітити клієнта, якого вивели з експлуатації. Сервер спирається на те, що RFC називає постійним сховищем: по одному запису на кожного клієнта, з ідентифікатором як ключем і параметрами, які цей клієнт отримав.

DHCP працює поверх UDP. Клієнти надсилають запити на порт 67 сервера, а сервери відповідають на порт 68 клієнта. Опції, які може надіслати сервер, від маски підмережі до терміну оренди, специфіковано окремо, в RFC 2132. Для IPv6 існує власний протокол, DHCPv6, який тепер описано в RFC 9915 — інтернет-стандарті від січня 2026 року, що замінив RFC 8415. Він використовує інші порти: 546 для клієнтів і 547 для серверів та агентів ретрансляції, і може працювати замість автоконфігурації адрес без збереження стану (SLAAC) або поряд із нею. Сам RFC 9915 називає протокол для IPv4 DHCPv4, коли треба розрізнити ці два, і фіксує консенсус IETF про те, що конфігурацію IPv4 слід передавати через DHCPv4, а не через DHCPv6.

Застосуйте поняття до рішення

Застосуйте «Що таке DHCP?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Wi-Fi, фаєрволи і віддалений доступ налаштовані так, щоб працювати можна було звідусіль, а заходити — лише своїм.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Керувала 30 інстансами Ubuntu Linux VPS — 30 серверів Linux під управлінням, із планом відновлення

Керувала 30 інстансами Ubuntu Linux VPS Зв'язатися з нами →

Чому це важливо

Кожному пристрою в мережі потрібні ті самі кілька налаштувань, і одного хибного значення досить, щоб відрізати його від мережі: маска, що не відповідає підмережі, адреса маршрутизатора, яка належить комусь іншому, DNS-сервер, який вимкнули ще минулого року. Без DHCP кожне з цих значень треба ввести на кожному пристрої і підтримувати правильним щоразу, коли щось змінюється. З DHCP вони живуть в одному місці, і заміна DNS-сервера для цілого офісу стає зміною в конфігурації сервера, а не обходом усієї будівлі.

Саме оренда дає протоколу змогу масштабуватися. Оскільки за динамічного розподілу адреси видаються на певний час, пул може за тиждень обслужити більше пристроїв, ніж має адрес, якщо вони не присутні в мережі всі водночас. RFC 2131 пише, що динамічний розподіл особливо корисний для клієнтів, під'єднаних лише тимчасово, і для спільного використання обмеженого пулу клієнтами, яким не потрібні постійні адреси. А оскільки клієнт може просто зникнути, протокол не покладається на прощання: RFC стверджує, що коректна робота не залежить від того, чи надішле клієнт повідомлення про звільнення адреси. Адреса повертається, коли спливає термін оренди, незалежно від того, чи повідомив про це її власник.

Тому термін оренди — справжнє проєктне рішення, а не значення за замовчуванням, яке можна не чіпати. Довга оренда довше тримає заблокованими адреси пристроїв, які давно пішли. Коротка означає більше трафіку на продовження і менше часу, щоб полагодити сервер, який перестав відповідати, бо клієнт, чия оренда спливла раніше, ніж він достукався до сервера, мусить припинити користуватися своєю адресою.

DHCP — це також питання довіри. Перша відповідь, яку приймає пристрій, каже йому, через який маршрутизатор піде весь його трафік і який DNS-сервер перекладатиме кожне ім'я, яке він шукає, тож той, хто контролює цю відповідь, контролює, куди потрапить пристрій. RFC 2131 каже про це прямо: розділ про безпеку називає протокол у його нинішньому вигляді доволі незахищеним, бо він побудований безпосередньо на UDP та IP, а машини, для яких його створено, важко забезпечити паролями чи ключами. У тому самому розділі зазначено, що несанкціоновані сервери легко розгорнути і що вони можуть роздавати хибні чи дубльовані адреси, підроблені маршрутизатори й підроблені сервери імен. Захист має йти від мережі навколо протоколу, а не від самого протоколу.

Як це виглядає на практиці

Візьмімо ноутбук з апаратною адресою 00-00-5E-00-53-2A, що під'єднується до офісної підмережі 192.0.2.0/24, де одна машина за адресою 192.0.2.1 є водночас маршрутизатором і DHCP-сервером. Ноутбук починає роботу без адреси, тож його перше повідомлення виходить з адресою відправника 0.0.0.0 і розсилається широкомовно всім у локальному сегменті. Через чотири повідомлення ноутбук уже налаштований:

```
ноутбук 00-00-5E-00-53-2A                       сервер 192.0.2.1

1  DHCPDISCOVER  0.0.0.0 -> 255.255.255.255, порт сервера 67
                 чи є тут сервер?
2  DHCPOFFER     пропонує 192.0.2.50 на 86400 с, id сервера 192.0.2.1
3  DHCPREQUEST   широкомовно: id сервера 192.0.2.1, просить 192.0.2.50
4  DHCPACK       192.0.2.50 належить ноутбуку на 86400 с
```

На DHCPDISCOVER може відповісти будь-яка кількість серверів, і клієнт може зачекати, щоб зібрати більше ніж одну пропозицію. Потім він вибирає одну і широкомовно надсилає запит, у якому називає вибраний сервер в опції server identifier і просить саме ту адресу, яку запропонував цей сервер.

Кожен інший сервер, що бачить цю розсилку, сприймає її як відмову від своєї пропозиції. Вибраний сервер записує прив'язку у своє сховище і підтверджує її повідомленням DHCPACK.

Підтвердження несе налаштування, кожне з яких є нумерованою опцією, визначеною в RFC 2132. Для цього ноутбука воно могло б містити:

```
option 53  тип повідомлення   5 (DHCPACK)
option 54  id сервера         192.0.2.1
option 51  термін оренди      86400 (секунд, одна доба)
option 1   маска підмережі    255.255.255.0
option 3   маршрутизатор      192.0.2.1
option 6   DNS-сервери        192.0.2.53
```

RFC 2132 вимагає, щоб маска підмережі йшла перед опцією маршрутизатора, коли присутні обидві, і дозволяє серверу перелічити кілька маршрутизаторів і кілька серверів імен у порядку пріоритету. Термін оренди та ідентифікатор сервера не є необов'язковими: RFC 2131 робить обидва обов'язковими в DHCPACK у відповідь на DHCPREQUEST.

Перш ніж використовувати 192.0.2.50, клієнт має перевірити, що цю адресу ще ніхто не використовує, наприклад за допомогою ARP. Якщо адреса виявиться зайнятою, клієнт мусить надіслати DHCPDECLINE і почати спочатку. Інакше запускаються таймери. Якщо сервер не надсилає власних значень, T1 дорівнює половині терміну оренди, а T2 — семи восьмим, тож за оренди на одну добу це виглядає так:

```
t = 0 с        отримано DHCPACK, оренда починається
t = 43200 с    T1: RENEWING, DHCPREQUEST напряму (unicast) до 192.0.2.1
t = 75600 с    T2: REBINDING, широкомовний DHCPREQUEST до будь-якого сервера
t = 86400 с    оренда спливає: припинити використання 192.0.2.50, почати знову
```

RFC радить додавати до обох таймерів певну випадкову варіацію, щоб кімната, повна ноутбуків, увімкнених одночасно, не продовжувала оренду вся разом. Якщо запит лишається без відповіді, клієнт чекає половину часу, що лишився, перш ніж спробувати знову, але не менше 60 секунд. Справний клієнт продовжує оренду на половині терміну і ніколи не наближається до його кінця.

Сервер не мусить бути в тій самій підмережі, що й ноутбук. Маршрутизатор може працювати як агент ретрансляції (relay agent): він перехоплює широкомовне повідомлення й пересилає його серверу деінде, а його власна адреса, записана в полі giaddr повідомлення, підказує серверу, куди надіслати відповідь. RFC 2131 розраховує на це і зазначає, що агенти ретрансляції усувають потребу в DHCP-сервері на кожному сегменті мережі. Наша сторінка налаштування мереж та VPN згадує налаштування та встановлення 1 000 Wi-Fi-роутерів і адміністрування мережевої інфраструктури для понад 1 000 серверів. У такому масштабі вводити адреси вручну не вийде, і розміщення пулів, оренд і агентів ретрансляції стає частиною проєкту мережі.

Де виникають проблеми

Першим відповідає чужий сервер. Домашній роутер, увімкнений не тим боком, тестова машина, з’єднана мостом з офісною мережею, або зловмисник — будь-хто з них може відповісти на DHCPDISCOVER, і ніщо в протоколі не підкаже клієнтові, який сервер справжній. RFC 2131 перелічує, що може зробити такий сервер: роздавати хибні чи дубльовані адреси й спрямовувати клієнтів на підроблений маршрутизатор або підроблені сервери імен. Комутатори вміють це фільтрувати, і RFC 7610 зазначає, що аналогічний механізм для IPv4, DHCP snooping, широко розгорнуто. Дозвольте серверні повідомлення DHCP лише на тих портах комутатора, що ведуть до ваших справжніх серверів або агентів ретрансляції, і відкидайте їх на всіх інших.

Пул вичерпується. Пул містить фіксовану кількість адрес, а динамічний розподіл повертає їх лише тоді, коли спливає оренда. У гостьовій мережі, через яку телефони проходять сотнями, оренда на тиждень означає, що кожен відвідувач за останній тиждень досі тримає адресу. RFC 2131 також попереджає, що зловмисний клієнт може зайняти всі адреси пулу й залишити інших клієнтів без адрес. Розраховуйте розмір пулу на кількість пристроїв, присутніх у мережі протягом одного терміну оренди, і скорочуйте оренду всюди, де пристрої приходять і йдуть.

Нова підмережа без агента ретрансляції. DHCPDISCOVER розсилається широкомовно, а широкомовні повідомлення зупиняються на маршрутизаторі. Новий VLAN або новий поверх офісу без налаштованого агента ретрансляції не отримує жодної відповіді. Хост, що реалізує RFC 3927, тоді може призначити собі локальну адресу каналу (link-local) з діапазону 169.254/16, яка працює лише в цьому одному сегменті, бо маршрутизатори

не повинні пересилати пакети до таких адрес чи від них. Налаштуйте агент ретрансляції на маршрутизаторі кожної підмережі, де є клієнти DHCP, і сприймайте адресу 169.254 на клієнті як ознаку того, що жоден сервер не відповів.

Два сервери, що суперечать один одному. Запускати два сервери заради відмовостійкості розумно, але RFC 2131 каже, що всі сервери мають повертати ті самі параметри, крім самої адреси, щоб клієнт поводився однаково, хоч би яку пропозицію він прийняв, і покладає на адміністратора відповідальність за їхню узгодженість. Два сервери з діапазонами, що перекриваються, можуть до того ж видати ту саму адресу двом клієнтам. Дайте кожному серверу власний діапазон, тримайте опції однаковими і порівнюйте обидва сервери після кожної зміни.

Фіксовані адреси всередині пулу. Принтер, якому вручну призначили статичну адресу з діапазону, який роздає DHCP, рано чи пізно зіткнеться з орендою. Протокол намагається це вловити: сервер має перевірити адресу, яку збирається видати повторно, наприклад запитом ICMP echo, а клієнт, який виявив, що його нова адреса зайнята, мусить відхилити її, після чого сервер позначає адресу як недоступну і має повідомити адміністратора. Це страховка, а не проєктне рішення. Тримайте вручну налаштовані адреси поза пулом або використовуйте ручний розподіл, щоб резервування тримав сам сервер.

Про IPv6 забули. Фільтрація DHCPv4 нічого не дає проти DHCPv6, який працює на інших портах і який клієнт може запустити, коли оголошення маршрутизатора (Router Advertisement) повідомляє, що DHCPv6 доступний. RFC 9915 відсилає до RFC 7610, DHCPv6-Shield, щоб стримувати несанкціоновані сервери DHCPv6, а RFC 7610 зазначає, що підроблені оголошення маршрутизатора лежать поза його межами; ними опікується Router Advertisement Guard. Фільтруйте серверні повідомлення DHCPv6 на портах доступу так само, як фільтруєте повідомлення DHCPv4, і вмикайте RA-Guard поряд.

Що почитати далі

- RFC 2131: Dynamic Host Configuration Protocol — сам протокол: способи розподілу адрес, оренда, обмін повідомленнями, таймери T1 і T2 і розділ про безпеку.

- RFC 2132: DHCP Options and BOOTP Vendor Extensions — усі нумеровані опції, від маски підмережі й списку маршрутизаторів до терміну оренди й типу повідомлення.
- RFC 9915: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) — протокол для IPv6, його порти й повідомлення та взаємодія зі SLAAC; він замінює RFC 8415.
- RFC 7610: DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers — фільтрація серверних повідомлень на комутаторі, DHCP snooping як прецедент з IPv4 і те, що лишається для RA-Guard.
- RFC 3927: Dynamic Configuration of IPv4 Link-Local Addresses — адреси 169.254/16, які хост може призначити собі сам, коли сервери мовчать, і чому маршрутизатори ніколи їх не пересилають.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке DHCP?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/dhcp/