Лекція
Основи адресування

При роботі з комп'ютерними мережами чітке розуміння основ IP-адресації є надзвичайно важливим і позбавляє від безлічі можливих і помилок при налаштуванні мережевого обладнання.

Для ідентифікації абонентів і знаходження місця їх розташування в мережі кожному з них привласнюється ознака – адреса.

Під адресою розуміється умовний номер, знання якого є достатнім для доставки повідомлення необхідному абонентові.

Сукупність правил присвоєння адрес абонентів, з обліком місць їх розташування й структури мережі називається *способом адресування*.

Ім'я й адреса бувають двох типів: плоскі (неструктуровані) та ієрархічні (структуровані).

Існуючий стек протоколів пакетних мереж використовує три типи адрес:

— локальні (називаємі апаратними фізичними адресами);
— мережні (IP-адреси);
— символьні (доменні імена).

Неструктуровані плоскі адреси мають рівноправні частини і не мають жодних структурних елементів, що ідентифікують їх належність до будь-яких груп. Тому для пошуку плоскої адреси треба переглянути майже їх усі, що потребує значного часу. В комп'ютерних мережах для пошуку плоскої адреси використовується широкомовний запит, тобто одночасне звернення до всіх адресатів. Такі запити додатково завантажують мережу і тому плоскі адреси мають обмежене застосування: їх використовують для адресації всередині обмежених за розмірами локальних мереж (побудованих лише на комутаторах чи концентраторах).

У комп'ютерних мережах використовуються різні плоскі адреси. Найбільш відомі MAC-адреси. **MAC-адреса - це унікальний 6-ти байтовий код, який використовується на канальному рівні для розпізнавання мережевих інтерфейсів вузлів.**

Ці адреси призначаються при виробництві всім мережевим інтерфейсам: мережевим адаптерам і портам маршрутизаторів. MAC-адресу ще називають **апаратною (чи фізичною**) тому, що вона пов'язана з апаратним (фізичним) рівнем. Іноді її ще називають **локальною**, адже вона працює в межах локальної мережі. **Фізична локальна адреса** – це адреса, що використовується для доставки даних в локальних межах (підмережах), які є елементами складної мережі. Фізична локальна адреса – це **MAC-адреса** (***Media Access Control***), яка призначається мережним адаптерам і мережним інтерфейсам маршрутизаторів, інтерфейсам ПК і усім інтерфейсам елементів мережі. MAC-адреса назначається виробником обладнання і є унікальною, так як управляється централізовано.

Для усіх відомих технологій ЛОМ MAC-адреса (рис.1) має формат 48 біт (6 октетів), наприклад: 11-A0-17-3D-BC-01.

MAC-адресу можна розділити на дві частини (рис.1). У першій частині

вказується *унікальний ідентифікатор виробника устаткування* (Organizationally Unique Identifier, OUI). Цей унікальний ідентифікатор привласнюється виробникові інститутом IEEE.

Останні 24 біта MAC-адреси призначаються безпосередньо виробником устаткування. Перший біт MAC-адреси (I/G) указує, чи є адреса індивідуальною або груповою:

— 0 (індивідуальна) – адреса, асоційована з певним мережним пристроєм;

— 1 (групова) – адреса, асоційована з кількома або всіма вузлами даної мережі.

Рисунок 1 – Формат MAC-адреси

Існує два види групових адрес:

– *багатоадресна* або *групова* (*multicast*) – адреса, асоційована із групою вузлів мережі;

– *широкомовна* (*broadcast*) – адреса, асоційована з усіма вузлами мережі. Її значення – (0x11)F-FF-FF-FF-FF-FF.

Другий біт MAC-адреси (U/L) указує, чи є MAC-адреса глобально або локально адмініструєма:

— 0 (глобально адмініструєма MAC-адреса пристрою) – вона глобально унікальна (адмініструється IEEE) і звичайно “зашита” в апаратуру;

— 1 (локально адмініструєма MAC-адреса) – вона вибирається довільно й може не містити інформації про виробника даного встаткування (OUI). Деякі виробники мережних адаптерів підтримують можливість змінювати MAC-адреси пристрою.

Якщо локальна мережа з'єднується з іншими мережами, то адресування на основі плоских адрес буде занадто складним. Потрібна більш гнучка й універсальна **високорівнева система, яка не залежить від адресування в локальних мережах** (тобто від канального та фізичного рівнів) і дозволяє об'єднувати локальні мережі різного фізичного складу та технологій. **Ця загальна система має універсальним і однозначним чином ідентифікувати будь-який інтерфейс складної мережі**. Такою системою є **ієрархічне адресування**. **Ієрархічні адреси мають частини, які ідентифікують групи та рівні ієрархії, до яких належать адресовані об'єкти (мережі, підмережі, комп'ютери).** Посилання на ці групи спрощує керування такими адресами, дозволяє простіше та швидше сортувати і знаходити об'єкти.

Приміром, такою універсальною системою **є IP-адресація**, яка працює на **мережевому рівні OSI**. Вона не **залежить від типу локальних адрес і забезпечує переміщення пакетів через будь-які локальні та глобальні мережі**.

IP-адреса логічно поділяється на адресу (код, ідентифікатор) мережі (підмережі) й адресу комп'ютера (хоста, вузла). При цьому внутрішня технологія кожної локальної мережі потребує використання також свого локального адресування. Так, в мережах Ethernet для доставки пакетів використовується MAC-адреса. Тому кожному пакету при потраплянні до відповідного локального сегмента мережі призначається ще і локальна (MAC) адреса одержувача пакету (кінцевого вузла одержувача інформації, або вузла посередника – чергового маршрутизатора для спрямування пакета в іншу локальну мережу).

IP-адреса одержувача пакета залишається незмінною при просуванні пакета по мережі від однієї локальної мережі до іншої. MAC-адреса одержувача кожного пакета використовуються тільки в локальних мережах і постійно змінюється при передачі через кожен новий сегмент мережі. Крім того, IP-адреса застосовується також і для ідентифікації інтерфейсів у межах локальної мережі. Таким чином, всі типи адрес виконують свої функції й використовуються одночасно в залежності від потреби. При цьому між ними весь час встановлюється однозначна відповідність.

Для визначення чергової локальної MAC-адреси за IP-адресою вузла використовується протокол перетворення адрес (Adress Resolution Protocol, ARP). Протокол ARP підтримує на кожному інтерфейсі мережевого адаптера та маршрутизатора таблицю, в якій записані відповідні IP і MAC адреси усіх активних інтерфейсів мережі. Спочатку, при вмиканні обладнання, ці таблиці порожні, а при функціонуванні мережі в них накопичується інформація. Для цього протокол ARP постійно розсилає широкомовні запити по локальній мережі та поновлює свої таблиці.

Широкомовні запити розповсюджуються тільки в межах «плоскої» мережі (на основі концентраторів і комутаторів), яка обмежена маршрутизаторами. Тому ARP протокол має інформацію тільки про цю мережу. Подивитись ARP-таблицю дозволяє команда ARP, яку можна виконати в командному рядку.

При потраплянні до чергової локальної мережі, коли пакет має підтримати нову MAC-адресу вузла призначення, необхідно її з'ясувати за IP адресою вузла призначення. Для цього протокол IP створює запит до протоколу ARP. Той знаходить у себе потрібну інформацію та відповідає. Якщо такої інформації немає, то в мережу посилається широкомовний запит з питанням: «Яку MAC-адресу має інтерфейс з потрібною IP- адресою?». Кожен комп'ютер, який отримав цей запит, направляє запит своєму ARP-протоколу. Таким чином, коли потрібну інформацію нарешті буде знайдено, її буде відправлено в ARP-відповіді, отримано на тому комп'ютері, який здійснив запит, і записано в таблицю ARP. А пакет отримає відповідну MAC-адресу вузла призначення, з якою він прямуватиме локальною мережею.

Якщо інформації про MAC-адресу немає, то це означає, що адресата не існує і пакет буде знищено.

Спостерігати за тим, як протокол ARP постійно створює широкомовні запити в локальній мережі можна, приміром, за допомогою програми WireShark. Вибором фільтру можна налаштувати WireShark для спостереження різних типів пакетів (зокрема ARP-запитів).

IP- і MAC- адреси є цифровими кодами, з якими зручно працювати комп'ютеру. Оскільки людині зручніше працювати з символьними адресами, то на прикладному рівні TCP/IP також використовується ієрархічна доменна (символьна) система іменування з довільною кількістю частин. Кожна частина – це ім'я домену (об'єднання комп'ютерів) різного рівня, яке надається відповідною установою. Ієрархічна структура дозволяє розподіляти відповідальність установ за унікальність адрес у межах свого рівня ієрархії в своєму домені. Домени вказуються в порядку зростання ієрархічного рівня зліва направо.

Пошук інформації про відповідність між символьними іменами та IP-адресами може здійснюватися засобами локального хоста (файл hosts.txt), але переважно це здійснюється централізованою службою DNS (Domain Name System система доменних імен). Ця служба використовує DNS сервери, на яких зберігається розподілена база даних доменних імен та IP-адрес. Клієнти DNS звертаються до серверів DNS для перетворення доменного імені в IP-адресу. За кожний домен відповідає певний сервер DNS, який зберігає імена свого рівня.

Мережні адреси (IPv4)

IP-адреса або **адреса третього рівня** – це логічна адреса, яка не прив’язується до конкретної апаратури (мережній карті, інтерфейсу і т.д.) і призначається адміністратором мережі:

— протокол IP версії 4 (IPv4) – використовує 32-бітні адреси;

Класова адресація IPv4

Споконвічно розмір IPv 4-адреси був обраний довжиною в 32 біта (при цьому можна адресувати $2^{32} \approx 4{,}3$ млрд. пристроїв).

Хронологічно першим методом поділу IP-адрес є так звана класова модель IP-адресації, яка частково розв’язала проблему нераціонального використання адресного простору. Згідно із цією моделлю, увесь простір IP- адрес ділиться на 5 класів залежно від значення перших чотирьох біт IPv4- адреси. Класам привласнені імена від A до E (таблиця 1). Перші 3 класи A, B и C використовуються для індивідуальної (unicast) адресації мереж і вузлів, клас D – для багатоадресного або групового (multicast) розсилання, клас E зарезервований для експериментів. Класи A, B и C мають різну довжину мережної частини адреси.

Таблиця 1 – Класи IP-адрес

Клас	Перші біти	Найменший номер мережі	Найбільший номер мережі	Максимальне число вузлів у мережі
A	0	1.0.0.0	126.0.0.0	2^{24} (поле 3 байти)
B	10	128.0. 0.0	191. 255.0.0	2^{16} (поле 2 байти)
C	110	192.0. 0.0	223. 255.255.0	2^{8} (поле 1 байт)
D	1110	224.0. 0.0	239. 255.255.255	Групові адреси
E	11110	240.0. 0.0	247. 255.255.255	Зарезервований

Клас мережі	Початкова адреса пулу	Кінцева адреса пулу	Кількість мереж	Кількість вузлів у мережі
A	1.0.0.0	126.255.255.255	126	16 777 214
Резерв	127.0.0.0	127.255.255.255		
B	128.0.0.0	191.255.255.255	16 384	65 534
C	192.0.0.0	223.255.255.255	2 097 152	254
D	224.0.0.0	239.255.255.255		
E	240.0.0.0	254.255.255.255		

У кожному із класів IP-мереж визначено так званий "приватний, простір IP-адрес" (таблиця 2). IP-адреси, що належать до цього "приватного простору" призначені для використання в локальних комп'ютерних мережах і не маршрутизуються (не сприймаються) в глобальних мережах (в Інтернеті).

Таблиця 2

Клас мережі	Початкова адреса	Кінцева адреса	Кількість мереж	Кількість вузлів у мережі
A	10.0.0.0	10.255.255.255	1	16 777 214
B	172.16.0.0	172.31.255.255	16	65 534
C	192.168.0.0	192.168.255.255	256	254

Крім того, визначено IP-адреси, що мають спеціальні значення ("спеціальні адреси"), які перелічені у таблиці 7.

Таблиця 7

Адреса мережі	**Адреса вузла**	
Усі "0"	Усі "0"	(Усі 0) — адреса вузла, що згенерував пакет
Усі "0"	Адреса вузла	Вузол призначення належить до тієї ж IP-мережі, що і вузол відправлення
Адреса мережі	Усі "0"	Адреса IP-мережі
Адреса мережі	Усі "1"	Обмежена широкомовна адреса (в межах даної IP-мережі)
Усі "1"	Усі "1"	(Усі 1) — "глобальна" широкомовна адреса
127.0.0.1		Адреса зворотного зв'язку (loopback), призначена для тестування обладнання без реального вісилання пакету

Певна частина IP-адреси адресує IP-мережу, а частина, що залишилась, - окремий вузол у цій IP-мережі. Так, у класі А адреса IP мережі міститься и першому октеті, а адреса вузла – у 2-му, 3-му та 4-му октетах (рис. 2). У класі В адреса IP мережі міститься в 1 -му та 2-му октетах, а адреса Вузла - у 3-му та 4-му октетах. У класі С адреса IP мережі - 1-й, 2-й та \ її октети, а адреса вузла — 4-й октет.

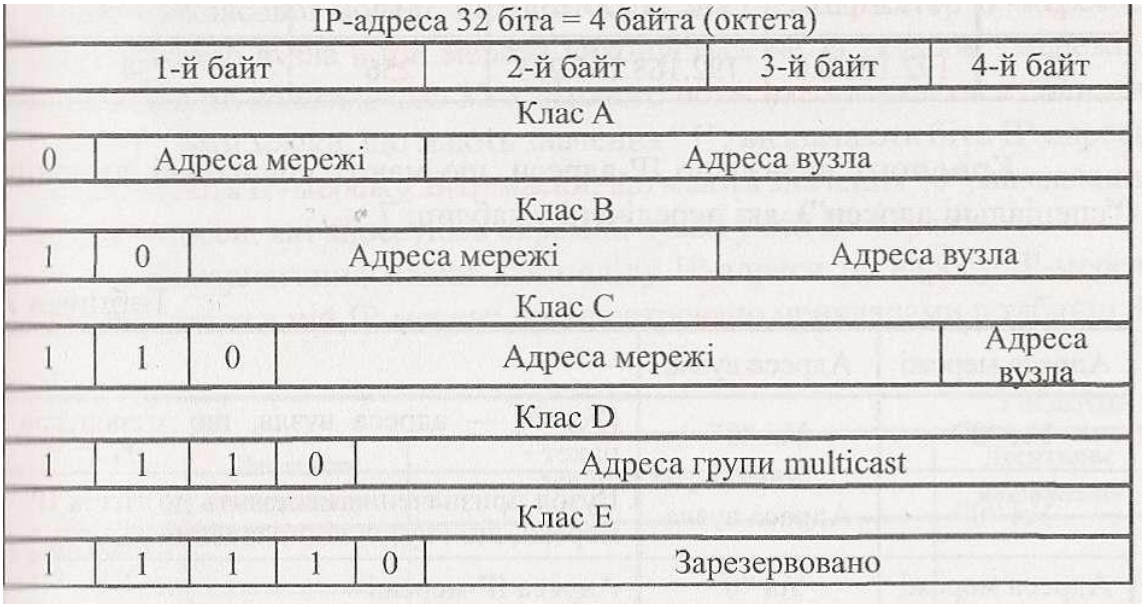

Рисунок 2 – Класи IP-мереж

Для мереж класу А (рис.3) під ідентифікатор мережі приділяється 1 байт (перший октет), 3 байти (3 октети), що залишилися використовуються для ідентифікатора вузла, причому старший (лівий) біт ідентифікатора мережі завжди рівний 0.

Оскільки перший біт ідентифікатора мережі завжди дорівнює нулю, то 7 біт, що залишилися дозволяють адресувати 128 (2) різних мереж. Однак через те, що адреси 0.0.0.0 і 127.0.0.0 є спеціальними IPv4-адресами, кількість доступних мереж класу А рівно 126 (2^7-2). У кожній мережі класу А можна адресувати до 16 777 214 (2^{24}-2) вузлів. Дві адреси віднімаються внаслідок того, що вони використовуються в спеціальних цілях і не можуть бути призначені пристрою (перший – адреса мережі, останній – широкомовна адреса).

Рисунок 3 – Формат IPv 4-адреси класу А

Мережі класу В (рис. 4) визначаються значеннями 10 у двох старших бітах адреси. Перші 2 байта в адресі використовуються для ідентифікатора мережі, 2 байта, що залишилися – для ідентифікатора вузла. У результаті кількість доступних мереж класу В становить 16 384 (2^{14}) з кількістю вузлів у кожній мережі рівним 65 534 (2^{16}-2).

Рисунок 4 – Формат IPv 4-адреси класу B

Для мереж класу 3 (рис.5) під ідентифікатор мережі приділяється 3 байта в той час як під ідентифікатор вузла тільки 1 байт. Три старші біти першого октету завжди рівні 110, дозволяючи визначити, що адреса ставиться саме до класу C. Таким чином, одержуємо 2 097 152 (2^{21}) мереж, у кожній з яких перебуває 254 (2-2) вузла.

Рисунок 5 – Формат IPv 4-адреси класу 3

Мережі класу D (рисунок 6) визначаються значеннями 1110 у перших чотирьох бітах адреси, інші біти використовуються для адресації багатоадресної групи. Адресний простір класу D зарезервоване для групового розсилання й використовується для адресації групи вузлів. Ідентифікаторів мереж і вузлів в IPv4-адресі класу D не виділяють.

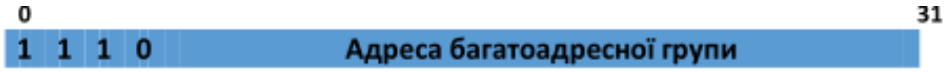

Рисунок 6 – Формат IPv4-адреси класу D

Мережі класу E (рис. 7) є експериментальними й у цей час не використовуються. Адреси в цьому класі визначаються значеннями 1111 у перших чотирьох бітах.

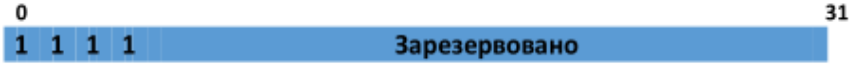

Рисунок 7 – Формат IPv4-адреси класу E

Застосування IP- адресації на основі класового розподілу обмежує можливості раціонального використання всього переліку (пула) адрес в кожній мережі, тому в подальшому стали використовувати два додаткових варіанти IPv4: на основі підмереж та основі безкласового адресування.

Велика кількість пристроїв, що використовують IP-адреси, а також нераціональне використання наявних адрес призвели до того, що виник дефіцит IP-адрес. Тимчасовим виходом з цього становища було більш економне використання IP-адрес за безкласовою технологією (CIDR) та залучення додаткових приватних адрес з перетворенням за технологією NAT. Наразі впроваджується нова система адресування - IPv6, головною метою якої є кардинальне вирішення проблеми дефіциту IP-адрес. Адреса IPv6 має 128 розрядів, що потенційно дозволяє адресувати близько $3{,}4*10^{38}$ хостів (для порівняння: адреса IPv4, що має 32 розряди, дозволяє адресувати лише близько $4{,}3*10^{9}$ хостів).

Бінарне та десяткове зображення IP-адрес

У бінарному («машинному») виді IP-адреса версії v4 є єдиним 32-х бітовим полем. Для зручності сприйняття людиною ця адреса зазвичай записується у виді чотирьох десяткових чисел, розділених крапками

Перетворення IP-адреси з бінарного зображення в десяткове проілюструємо на такому прикладі.

10100000010100010000010110000011 (бінарне зображення)
10100000.01010001.00000101.10000011 {розділено крапками на октети по 8 біт)
160.81.5.131 {десяткове зображення)

Таблиця 3 пояснює перетворення з бінарного в десяткове зображення числових значень окремих октетів цього прикладу (користуємося правилами переводу десяткових чисел у двійкові та навпаки).

Таблиця 3

	Бінарне зображення								**Десяткове зображення**			
1-й октет	1	0	1	0	0	0	0	0				
Десяткові значення розрядів	128	64	32	16	8	4	2	1	=	128+32	=	160
2-й октет	0	1	0	1	0	0	0	1				
Десяткові значення розрядів	128	64	32	16	8	4	2	1	=	64+16+1	=	81
3-й октет	0	0	0	0	0	1	0	1				
Десяткові значення розрядів	128	64	32	16	8	4	2	1	=	4+1	=	5
4-й октет	1	0	0	0	0	0	1	1				
Десяткові значення розрядів	128	64	32	16	8	4	2	1	=	128+2+1	=	131

Безкласова модель IP-адресації, маска змінної довжини

Класова модель IP-адресації виявилась дуже нераціональною з і очки зору ефективності використання обмеженого простору IP-адрес. Приміром, для мережі з 1000 комп'ютерів призначається пул адрес класу II, у якому біля 60 тис. адрес. При цьому 1000 адрес використовуються, а 50 тис. не використовуються.

З часом було прийнято "безкласову модель" IP-адресації з використанням маски змінної довжини і технологію безкласової міждоменної маршрутизації (Classless Inter Domain Routing, CIDR). Згідно безкласової моделі, поділ IP-адрес на ідентифікатор IP-мережі й ідентифікатор вузла в цій мережі виконується не за "класом" мережі, а відповідно до додаткового 32-х бітового поля, яке називається "Маскою мережі". Біти маски, що мають значення "1", визначають біти IP-адреси, і адресують IP-мережу. Біти маски, що мають значення "0", визначають біти IP-адреси, які адресують окремий вузол у цій IP-мережі.

Використання маски для поділу IP-адреси на адресу IP-мережі і адресу вузла в цій IP-мережі проілюстровано прикладами в таблиці 4 та рис. 8.

Таблиця 4

	Десяткове зображення	Бінарне зображення	Десяткове зображення
Приклад №1			
IP-адреса	20537.193.134	11001101.00100101.11000001.10000110	
Маска	255.255.255.192	11111111.11111111.11111111.11000000	
		звідси випливає:	
IP-адреса мережі		11001101.00100101.11000001.10000000	205.37.193.128
IP-адреса широкомовна		11001101.00100101.11000001.10111111	205.37.193.191
Приклад №2			
IP-адреса	205.37.193.204	11001101.00100101.11000001.11001100	
Маска	255.255.255.192	11111111.11111111.11111111.11000000	
		звідси випливає:	
IP-адреса мережі		11001101.00100101.11000001.11000000	205.37.193.192
IP адреса широкомовна		11001101.00100101.11000001.11111111	205.37.193.255

Рисунок 8 – Формування маски підмережі

Щоб одержати адресу мережі, знаючи IPv4-адресу й маску підмережі, необхідно застосувати до них операцію *логічне "І"* (рис. 9). Інакше кажучи, у тих позиціях IPv4-адреси, у яких в масці підмережі є двійкові 1, перебуває ідентифікатор мережі, а де двійкові 0 – ідентифікатор вузла.

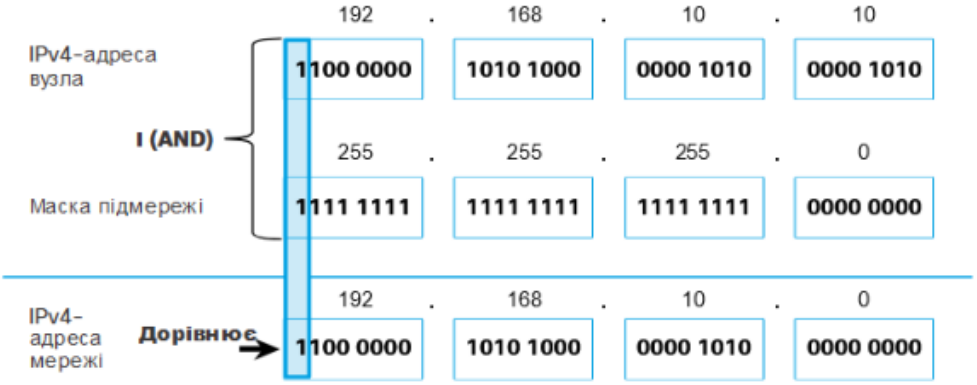

Рисунок 9 – Отримання адреси мережі

Для мереж класу A, B и C визначені фіксовані маски підмережі, які жорстко визначають кількість можливих IPv4-адрес. Технологія поділу мережі дає можливість створювати більше число мереж з меншою кількістю вузлів у них, що дозволяє ефективно використовувати адресний простір.

Для обчислення кількості підмереж використовується формула 2^s, де s – кількість біт, зайнятих під ідентифікатор мережі із частини, відведеної під ідентифікатор вузла. Кількість вузлів у кожної підмережі обчислюється по формулі $2^n–2$, де n – кількість біт, що залишилися в частини, що ідентифікує вузол, а дві адреси – адреса підмережі й широкомовна адреса – у кожної отриманої підмережі зарезервовані.

IP-адресу і маску можна записати коротше (дивись таблицю 5).

Таблиця 5

IP-адреса	205.37.193.134	205.37.193.134/26
Маска	255.255.255.192	
IP-адреса	205.37.193.204	205.37.193.204/26
Маска	255.255.255.192	

При такій формі запису значення префікса, що вказується через косу після IP-адреси, означає число старших бітів IP-адреси, які адресують IP-мережу.

Наприклад, розбиття мережі класу "С" за допомогою маски на підмережі можна зробити таким чином, як показано в таблиці 6. Таке розбиття дуже часто використовується в невеликих мережах.

Таблиця 6

Маска				Число хостів	Число підмереж	Префікс
1-й октет	2-й октет	3-й октет	4-й октет			
255	255	255	**252**	4(-2)	64	**/30**
255	255	255	**248**	8(-2)	32	**/29**
255	255	255	**240**	16(-2)	16	**/28**
255	255	255	**224**	32(-2)	8	**/27**
255	255	255	**192**	64(-2)	4	**/26**
255	255	255	**128**	128(-2)	2	**/25**
255	255	255	**0**	256(-2)	1	**/24**

Мережні адреси (IPv6)

- Протокол IP версії 6 (IPv6) – використовує 128-бітні адреси.

Протокол IPv6 – це нова версія протоколу IP, яка розроблена в якості спадкоємця IPv4 і покликана розв'язати проблему вичерпання адресного простору. На відміну від адреси IPv4, яка має довжину 32 біта, розмір адреси IPv6 становить 128 біт, що дозволяє адресувати приблизно $3{,}4 \times 10^{38}$ інтерфейсів пристроїв. Адреса IPv6 відображається як вісім груп по чотири шістнадцяткові цифри, розділені двокрапкою Наприклад (рис.к 10), 2001:0DB8:AC10:FE01:0018:8BFF:FED8:E3E0.

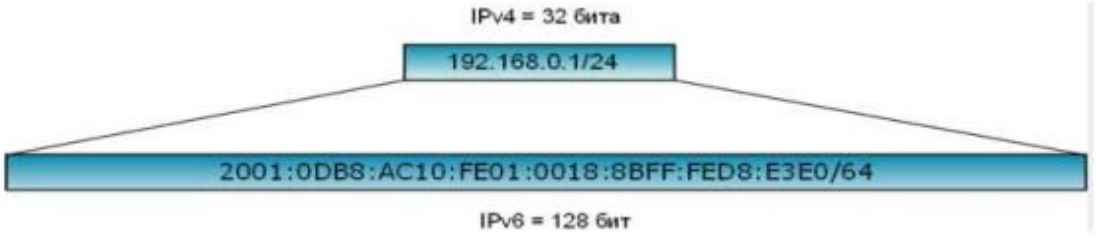

Рисунок 10 – Адреси IPv4 і IPv6

Існує кілька способів, які дозволяють скоротити запис IPv6-адреси:

- нулі на початку групи можна замінити одним;
- одна або кілька послідовних груп, що складаються з нулів, можуть бути замінені позначкою "**::**", але тільки один раз;
- кінцеві нулі в групі повинні бути присутнім.

Для наведеної нижче адреси цифри, виділені жирним шрифтом, представляють позиції, у яких адреса може бути скорочена:

2001:1000:**0000**:**0000**:**0000**:ABCD:**0000**:**0001**

Варіанти можливих скорочень:

- 2001:1000::ABCD:0:0001;
- 2001:1000::ABCD:0:1.

IPv6-адреса складається із двох логічних частин – *префікса* (Prefix) і *ідентифікатора інтерфейсу* (Interface ID) (рис. 11).

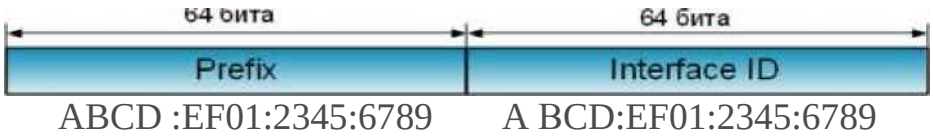

Рисунок 11 – Структура IPv6-адреси

***Префікс* (Prefix)** – перші 64 біти адреси, частина адреси, відведена під ідентифікатор мережі/підмережі (аналог ідентифікатора мережі в IPv4). Префікс адреси IPv6 записується у вигляді *адреса IPv6/довжина префікса*. Якщо довжина префіксу має значення 64, значить розбивка на підмережі не передбачена, якщо менше наприклад 48, то 48 біт відведені під номер мережі, а інша частина префіксу (64-48=16 біт) для номера підмережі:

Розглянемо для прикладу IPv6-адресу:
2001:0f68:0000:0000:0000:0000:1986:69af/48. Оскільки префікс (/48) указує на перші 48 біт, то 2001:0f68:0000 є номером мережі (Global Routing Prefix), а наступне поле, 0000, указує на ідентифікатор під мережі (Subnet ID).

***Ідентифікатор інтерфейсу* (Interface ID)** – останні 64 біта IPv6- адреси використовуються для ідентифікації інтерфейсу в сегменті мережі (аналог ідентифікатора вузла в IPv4). Він повинен бути унікальним усередині мережі/підмережі.

Адресний простір протоколу IPv6 розділений на три типи адрес:

- індивідуальні (unicast) адреси
- багатоадресні (multicast) адреси;
- альтернативні (anycast) адреси.

Індивідуальні адреси ідентифікують один інтерфейс пристрою. Пакети, відправлені на цю адресу, доставляються тільки на цей інтерфейс.

Типи Unicast адрес:

- *Глобальні*

Відповідають публічним IPv4 адресам. Можуть перебувати в будь- якому не зайнятому діапазоні. У цей час регіональні Інтернет-регістратори розподіляють блок адрес 2000::/3 (з 2000:: по 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF).

- *Link-Local*

Адреси мережі, які призначені тільки для комунікацій в межах одного сегмента

місцевої мережі або магістральної лінії. Вони дозволяють звертатися до хостів, не використовуючи загальний префікс адреси. Маршрутизатори не відправлятимуть пакети з адресами link-local.

Адреси link-local часто використовуються для автоматичного конфігурування мережної адреси, у випадках, коли зовнішні джерела інформації про адресу мережі недоступні.

- *Unique-Local*

RFC 4193, відповідають частковим IP-адресам, якими у версії IPv4 були 10.0.0.0/8, 172.16.0.0/12 і 192.168.0.0/16. Починаються із цифр FC00 і FD00.

- *Групові адреси* IPv6, подібно однойменним адресам IPv4, визначають групу інтерфейсів. Пакети, що посилають на цю адресу, доставляються всім інтерфейсам – учасникам групи розсилання.

- *Альтернативні адреси* дозволяють адресувати групу інтерфейсів (звичайно приналежних різним вузлам). Однак на відміну від багатоадресних адрес, пакети, передані на альтернативну адресу, доставляються на один з інтерфейсів (звичайно "найближчий", згідно з метрикою маршрутизації), обумовлених цією адресою.

- *Широкомовні адреси (Broadcast)*, які використовуються в IPv4, в IPv6 відсутні, що сприяє зменшенню мережного трафіка й зниженню навантаження на більшість систем. Широкомовні адреси замінені багатоадресними.

Серед IPv6-адрес також передбачені зарезервовані адреси (таблиця 5), які мають спеціальне призначення (спеціальні адреси).

Таблиця 5 – Зарезервовані адреси IPv6

IPv6 адреса	**Довжина префіксу (бітів)**	**Опис**	**Примітки**
::	128	Невизначена адреса	див. 0.0.0.0 в IPv4
::1	128	loopback адреса	див. 127.0.0.1 в IPv4
::ffff: xx.xx.xx.xx	96	Адреса IPv4, що відображена на IPv6	Нижні 32 біти – це адреса IPv4. Для хостів, що не підтримують IPv6.
2001:db8::	32	Документування	Зарезервовано для прикладів в документації в rfc3849
fe80:: – febf::	10	link-local	Аналог 169.254.0.0/16 в IPv4
fec0:: — feff::	10	site-local	Відмічений як застарілий в
			rfc3879
fc00::	7	Unique Local Unicast	Аналог 169.254.0.0/16 в IPv4
ffxx::	8	multicast	Мультімовлення для всіх маршрутизаторів ff02 :: 2 Мультімовлення для всіх вузлів ff02 :: 1

Символьні адреси

Символьні адреси, які в *Internet* називають доменними іменами застосовують для зручності роботи користувача у клієнтських програмах перегляду web-сторінок. Символьні адреси зазвичай несуть якесь смислове навантаження, їх набагато легше запам'ятовувати і вони формуються за ієрархічною ознакою. Складові повної символьної адреси в мережі розділяються крапкою і перераховуються в наступному порядку:

– спочатку ім’я кінцевого вузла, наприклад ***home***;

– потім ім’я групи вузлів, наприклад ***managers***;

– потім ім’я більшої групи, наприклад ***company***;

– і так до самого вищого рівня, наприклад ***ua***.

Символьні адреси зазвичай несуть якесь смислове навантаження і їх набагато легше запам'ятовувати, але реальна взаємодія вузлів все одно відбувається за IP-адресами. Тобто кожній символьній адресі співставляється певна IP-адреса. Проте між символьною адресою (доменним іменем) і IP- адресою вузла нема ніякої алгоритмічної відповідності, тому необхідні додаткові таблиці або служби, щоб вузол однозначно визначався, як по доменному імені, так і по IP-адресі.

В мережах на основі стеку TCP/IP використовується спеціальна служба ***Domain Name System*** (**DNS**), яка установлює цю відповідність на основі створюємих адміністраторами мережі *таблиць відповідності*. Тому доменні імена також називають DNS-імена.

Система DNS є ієрархічної й розподіленою. Не існує єдиної бази даних, що зберігає інформацію про всі імена та відповідні їм IP-адреси і інші записи. DNS – це мільйони баз даних, кожна з яких містить інформацію про конкретний домен. Ієрархію DNS можна побачити в доменному імені, наприклад, в імені веб-сайту. Візьмемо, наприклад, сайт – **www.cip.gov.ua**. Це ім’я складається із трьох частин, розділених крапками. Точніше чотирьох, оскільки, формально говорячи, повне доменне ім’я завжди закінчується крапкою, що позначає так званий кореневий домен, або кореневу зону DNS. Отже:

Коренева зона	Містить інформацію про всі піддомени: net, com, org, ru, su, і т.д. Точніше, інформацію про сервери, що обслуговують ці домени.
ua	Домен **ua**, що містить інформацію про всі піддомени, зареєстровані у ньому, наприклад, **gov**. Знову ж, цей домен містить адреси серверів, у яких можна одержати додаткову інформацію про вміст піддоменів.
gov	Домен **gov**, що містить інформацію про всі піддомени наступного, зареєстровані у ньому, зокрема **cip**. Знову ж, цей домен містить адреси серверів, у яких можна одержати додаткову інформацію про вміст піддоменів.
cip	Домен **cip**, що містить інформацію про всі служби або файли, а також імена серверів, зареєстрованих безпосередньо в цьому домені, зокрема **www.cip.gov.ua**
www	Послуга веб-сервера і відповідна йому IP-адреса.

Таким чином, трансляція імені www.cip.gov.ua у відповідну йому IP- адресу буде відбуватися в кілька етапів (рисунок 12). Спочатку будуть запитані сервери, що обслуговують кореневу зону. Ці сервери нічого не знають про існування доменів gov чи cip і тим більш адреси www.cip.gov.ua. Але вони повідомлять, як можна зв'язатися із серверами, що обслуговують домен наступного рівня ua (операції 2 та 3). Від них можна довідатися адреси серверів домену gov (операції 4 та 5). Від наступних – домену cip, які, у свою чергу, дадуть відповідь на запит про IP-адресу сервера www.cip.gov.ua.

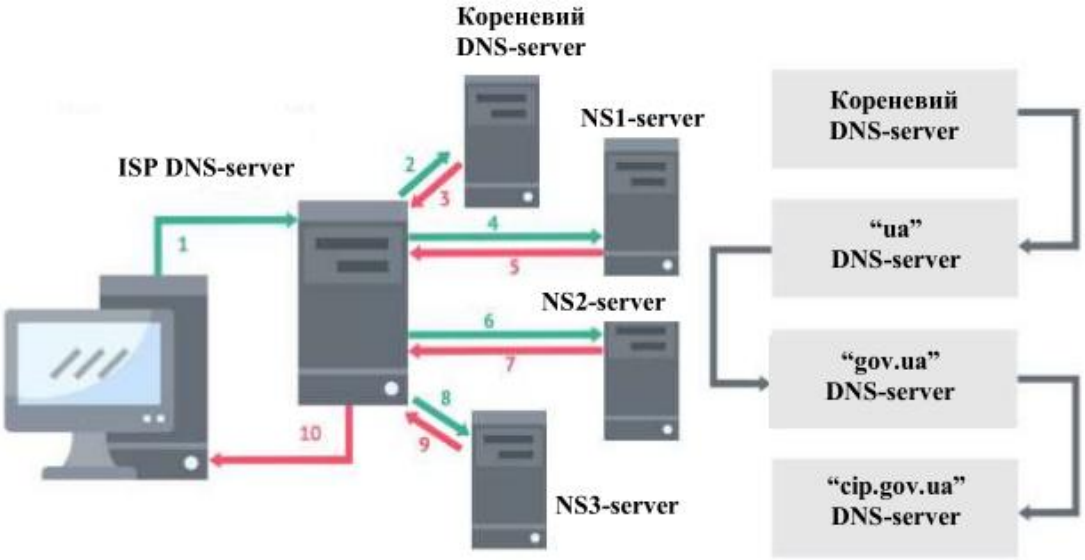

Рисунок 12 – Процес трансляції імен в DNS

Така архітектура DNS дозволяє розподілити навантаження й відповідальність за роботу системи між адміністраторами окремих доменів. До їхніх завдань входить забезпечення нормальної продуктивності при відповіді на запити до певної зони, підтримка унікальності імен у рамках зони, а також повідомлення адміністраторові батьківської зони про зміни в складі серверів, що обслуговують зону.

Порядок роботи протоколу DHCP

DHCP (англ. *Dynamic Host Configuration Protocol* – протокол динамічної конфігурації вузла) – це стандартний протокол прикладного рівня, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі. Для цього комп'ютер звертається до DHCP-сервера. Мережний адміністратор може задати діапазон адрес, які будуть розподілені між комп'ютерами. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості великих мереж TCP/IP.

Крім IP-адреси, DHCP також може повідомляти клієнтові додаткові параметри, необхідні для нормальної роботи в мережі. Ці параметри називаються опціями DHCP. Список стандартних опцій можна знайти в RFC 2132. Деякими з найбільш часто

використовуваних опцій є:

1. IP-адреса маршрутизатора за замовчуванням;
2. маска підмережі;
3. адреси серверів DNS;
4. ім’я домену DNS.

Деякі постачальники програмного забезпечення можуть визначати власні, додаткові опції DHCP.

Протокол DHCP працює за схемою клієнт-сервер. Під час запуску системи комп’ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення- відповідь, яка містить IP-адресу і деякі інші конфігураційні параметри. При цьому сервер DHCP може працювати в різних режимах, включаючи:

1. **Динамічний розподіл** - адміністратор присвоює IP-діапазон адрес на сервері DHCP. Кожен клієнтський комп’ютер в мережі повинен запросити IP-адресу від DHCP-сервера, коли мережа ініціалізується за концепцією "оренди". Коли закінчується термін оренди, якщо вона не буде продовжена, DHCP-сервер має право повернути адресу і призначити її на інші комп’ютери.
2. **Автоматичне виділення** - сервер DHCP буде постійно призначати вільний IP-адрес з діапазону, встановленого адміністратором, запитуючому комп’ютеру. Основна відмінність з динамічним розподілом в тому, що сервер зберігає записи минулих завдань IP і намагається привласнити ту ж адресу тому ж комп’ютеру для майбутніх мережних підключень.
3. **Статичний розподіл** - сервер DHCP робить призначення IP-адрес виключно на основі таблиці MAC-адрес, які зазвичай заповнені вручну адміністратором мережі. Якщо MAC-адреса комп’ютера не зазначена в таблиці, йому не буде призначена мережна адреса.

Протокол DHCP побудований так, що клієнт може звертатися із запитом відразу до декількох серверів.

Клієнт DHCP, що потребує адресу, посилає широкомовний пакет *DHCPDISCOVER* в пошуках сервера. Пакет містить апаратну адресу запитувача клієнта. Потім один або кілька серверів DHCP розглядають запит і посилають у відповідь пакет *DHCPOFFER*, що містить пропоновану IP- адресу і "час оренди".

Клієнт вибирає адресу з отриманих пакетів DHCPOFFER. Вибір клієнта залежить від його призначення - наприклад, він може вибрати адресу з найбільшим часом оренди. Слідом за тим клієнт посилає пакет *DHCPREQUEST* з адресою вибраного сервера.

Обраний сервер посилає підтвердження (*DHCPACK*) і процес узгодження завершується. Пакет DHCPACK містить обумовлені адресу та час оренди. Сервер позначає виділену адресу як зайняту - до закінчення терміну оренди цю адресу не можна буде присвоїти іншому клієнту. Клієнту залишилося тільки сконфігурувати

себе відповідно до надісланих даних і можна приступати до роботи в мережі.

Отже, на запит DHCPDISCOVER може відповісти кілька серверів. Клієнт повинен вибрати одну з пропозицій і послати у відповідь пакет DHCPREQUEST з ідентифікатором вибраного сервера. Інші сервери переглядають пакет DHCPREQUEST і укладають на основі ідентифікатора сервера, що їх пропозиція була відкинута. Таким чином, вони знають, що запропоновані ними IP-адреси вільні для призначення іншим клієнтам.

У разі якщо сервер не може прийняти конфігурацію, він посилає пакет DHCPNAK (відмова в підтвердженні), що змушує клієнта почати процес узгодження заново. Виходячи з цього, якщо в мережі два DHCP-сервера з різними конфігураціями, немає ніякої гарантії, що клієнт вибере саме ваш сервер.

Якщо DHCP-сервер, розташований на віддаленому маршрутизаторі (R3), в іншій мережі і централізовано видає адреси в усі локальні мережі (LAN_1 і LAN_2), то необхідна конфігурація агентів DHCP-relay на маршрутизаторах, до яких підключені ці локальні мережі (R1 і R2) (рис. 13). Сутність DHCP-relay полягає в пересиланні широкомовного пакету від клієнта одноадресним пакетом до DHCP-сервера.

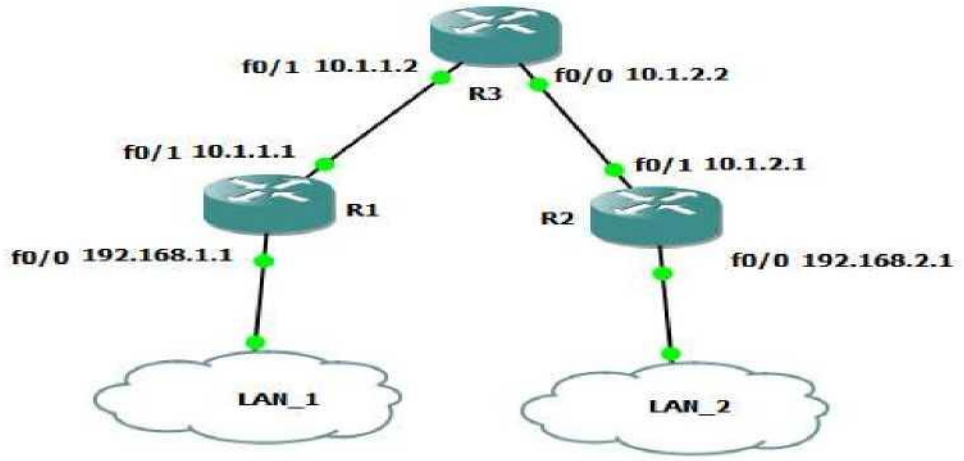

Рисунок 13 – DHCP-сервер, розташований на віддаленому маршрутизаторі

DHCPV6

SLAAC – це спосіб, який дозволяє пристрою отримати свій префікс, довжину префікса і адреса шлюзу від маршрутизатора IPv6 без допомоги DHCPv6-сервера. При використанні SLAAC для отримання необхідної інформації пристрої покладаються на повідомлення “Оголошення маршрутизатора ICMPv6”.

IPv6-маршрутизатори періодично відправляють повідомлення “Оголошення маршрутизатора ICMPv6” всіх пристроїв в мережі під управлінням IPv6. За замовчуванням маршрутизатори Cisco відправляють такі повідомлення кожні 200 секунд на адресу груповий передачі всім IPv6- вузлів. IPv6-пристрою, що знаходиться в мережі, не потрібно чекати цих періодичних повідомлень. Пристрій може відправити повідомлення “Запит маршрутизатора ICMPv6”, який використовує адресу груповий передачі всім IPv6-вузлів. Коли маршрутизатор IPv6 отримує таке

повідомлення, він відразу ж відправляє у відповідь оголошення маршрутизатора.

IPv6-маршрутизація не включена за замовчуванням. Щоб маршрутизатор працював як IPv6-маршрутизатор, необхідно використовувати команду глобальної конфігурації ipv6 ***unicast-routing.***

Повідомлення "Оголошення маршрутизатора ICMPv6" містить префікс, довжину префікса і інші відомості IPv6-пристрої. Крім того, таке повідомлення вказує IPv6-пристрою, як йому отримати інформацію по адресації. повідомлення "Оголошення маршрутизатора" може виглядати в одному з наступних 3 варіантів:

– **Варіант 1:** ***тільки SLAAC***. Пристрій повинен використовувати префікс, довжину префікса і шлюз за замовчуванням, які містяться в повідомленні «Оголошення маршрутизатора». Інша інформація недоступна з DHCPv6-сервера.

– **Варіант 2:** ***SLAAC і DHCPv6***. Пристрій повинен використовувати префікс, довжину префікса і шлюз за замовчуванням, які містяться в повідомленні "Оголошення маршрутизатора". На DHCPv6-сервері доступна і інша інформація, наприклад адресу DNS-сервера. Пристрій отримає цю додаткову інформацію в процесі пошуків і запитів до DHCPv6-сервера. Цей процес називається "DHCPv6 без запам'ятовування станів", оскільки DHCPv6-сервери не виділяють і не відстежують будь-які призначення IPv6- адрес, а надають додаткову інформацію, наприклад про адресу DNS-сервера.

– **Варіант 3:** ***тільки DHCPv6*.** Пристрій не має використовувати інформацію з повідомлення "Оголошення маршрутизатора" для поповнення своєї інформації про адресації. Замість цього пристрій буде використовувати звичайні процеси пошуків і запитів до DHCPv6-серверів для отримання всієї своєї інформації про адресації. Така інформація включає в себе індивідуальну адресу IPv6, довжину префікса, адреса шлюзу та адреси DNS-серверів. В цьому випадку DHCPv6-сервер працює як DHCP-сервер, який фіксує дані аналогічно DHCP-сервера для IPv4. DHCPv6-сервер виділяє і відстежує IPv6- адреси, щоб не призначати один і той же IPv6-адреса на декількох пристроях.