НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут комп’ютерних інформаційних технологій

Кафедра комп'ютерних систем та мереж

# Лабораторна робота № 1

з дисципліни «Комп’ютерні мережі»

Виконав: Клокун В. Д. Роботу захищено:

Група: СП-425

Перевірив: Зіньков Ю.Г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Київ 2019

**Мережі TCP/IP**

**Адресація в мережах TCP/IP**

Головним елементом, що відрізняє TCP / IP від інших стеків протоколів, що забезпечують сервіси Мережевого і Транспортного рівнів, є власна унікальна система адресації. Кожному пристрою мережі TCP / IP присвоюється IP-адреса (іноді більше, ніж один), однозначно ідентифікує цей пристрій для інших систем. Більшість персональних комп'ютерів, задіяних в мережі, використовують в даний час мережеві адаптери типу Ethernet і TokenRing з заздалегідь присвоєними вбудованими унікальними ідентифікаторами (МАС-адресами), які роблять IP-адреси надлишковими. Багато інших типів комп'ютерів мають всілякі адреси, які призначаються мережевими адміністраторами, причому немає ніякої впевненості в тому, що в іншого комп'ютера в мережі масштабу Інтернету не буде точно такого ж адреси.

Так як IP-адреси реєструються централізовано, можна бути впевненим, що ніякі два (правильно сконфігуровані) комп'ютера в Інтернеті не матимуть однакових IP-адрес. Завдяки своїй системі адресації, протоколи TCP / IP здатні підтримувати практично будь-апаратне забезпечення або програмну платформу з нині існуючих.

**Стек TCP/IP**

Стек протоколів TCP / IP передбачає чотири рівні, кожен з яких обробляє свій набір протоколів:

*прикладний рівень*: Створено для забезпечення роботи користувача з мережею На цьому рівні обробляється все те, що бачить і робить користувач. Рівень дозволяє користувачеві отримати доступ до різних мережних служб, наприклад: доступ до баз даних, можливість прочитати список файлів і відкрити їх, відправити повідомлення електронної пошти або відкрити веб-сторінку. Разом з одними даними і діям, на цьому рівні передається службова інформація.

*транспортний рівень:* це механізм передачі пакетів в чистому вигляді. На цьому рівні абсолютно не має значення ні вміст пакету, ні його приналежність до якого б то ні було дії. На цьому рівні має значення тільки адреса вузла відправки пакета і адреса вузла, на який пакет повинен бути доставлений. Як правило, розмір фрагментів, що передаються з використанням різних протоколів, може змінюватися, тому на цьому рівні блоки інформації можуть дробитися на виході і збиратися в єдине ціле в точці призначення. Цим обумовлена можлива втрата даних, якщо в момент передачі чергового фрагмента відбудеться короткочасний розрив з`єднання.

Транспортний рівень включає в себе багато протоколів, які діляться на класи, від найпростіших, які просто передають дані, до складних, які оснащені функціоналом підтвердження прийому, або повторного запиту недоотриманого блоку даних.

Даний рівень, надає вищестоящому (прикладному) два типи сервісу:

* Здійснює гарантовану доставку, за допомогою протоколу ТСР.
* Здійснює доставку по можливості по протоколу UDP*.*

Щоб забезпечити гарантовану доставку, згідно з протоколом TCP встановлюється з`єднання, яке дозволяє виставляти на пакетах нумерацію на виході і підтверджувати їх прийом на вході. Нумерація пакетів і підтвердження прийому - це так звана службова інформація. Цей протокол підтримує передачу в режимі "Дуплекс". Крім того, завдяки продуманому регламенту протоколу, він вважається дуже надійним.

Протокол UDP призначений для моментів, коли неможливо налаштувати передачу по протоколу TCP, або доводиться економити на сегменті мережевий [передачі даних.](http://poradi.ru/tehnika-ta-tehnologii/32005-peredacha-danih-pristroju-sistemi-programi.html) Також протокол UDP може взаємодіяти з протоколами більш високого рівня, для підвищення надійності передачі пакетів.

*Мережевий рівень або "рівень інтернету":*базовий рівень для всієї моделі TCP / IP. Основний функціонал цього рівня ідентичний однойменним рівню моделі OSI і описує переміщення пакетів в складовою мережі, що складається з декількох, більш дрібних підмереж. Він пов`язує сусідні рівні протоколу TCP / IP.

Мережевий рівень є сполучною між вищим транспортним рівнем і нижчестоящим рівнем мережевих інтерфейсів. Мережевий рівень використовує протоколи, які отримують запит від транспортного рівня, і за допомогою регламентованої адресації передають оброблений запит на протокол мережевих інтерфейсів, вказуючи, за якою адресою направити дані.

На цьому рівні використовуються наступні мережеві протоколи TCP / IP: ICMP, IP, RIP, OSPF. Основним, і найбільш популярним на мережевому рівні, звичайно ж є протокол IP (Internet Protocol). Основним його завданням є передача пакетів від одного роутера до іншого до тих пір, поки одиниця даних не потрапить на мережевий інтерфейс вузла призначення. Протокол IP розгортається не тільки на хостах, але і на мережевому обладнанні: маршрутизаторах і керованих комутаторах. Протокол IP працює за принципом негарантованої доставки з максимальними зусиллями. Т. е., Для відправки пакета немає необхідності заздалегідь встановлювати з`єднання. Такий варіант призводить до низького споживання каналу і часу на русі зайвих службових пакетів. Пакет направляється в сторону призначення, і цілком можливо, що вузол залишиться недоступним. В такому випадку повертається повідомлення про помилку.

*Рівень мережевих інтерфейсів:*відповідає за те, щоб підмережі з різними технологіями могли взаємодіяти один з одним і передавати інформацію в тому ж режимі. Реалізовано це двома простими кроками:

* Кодування пакета в одиницю даних проміжної мережі.
* Перетворення інформацію щодо кінцевого пункту в стандарти необхідної підмережі і відправка одиниці даних.

Цей підхід дозволяє постійно розширювати кількість підтримуваних технологій побудови мереж. Як тільки з`являється нова технологія, вона відразу потрапляє в стек проколів TCP / IP і дозволяє мережам зі старими технологіями передавати дані в мережі, побудовані із застосуванням більш сучасних стандартів і способів.

**Типи адрес стеку TCP/IP**

У стеці TCP/IP використовуються три типи адрес: локальні (які також називаються апаратними), [IP-адреси](https://uk.wikipedia.org/wiki/IP-адреса) й символьні доменні імена.

У термінології TCP/IP під локальною адресою розуміється такий тип адреси, що використовується засобами базової технології для доставки даних у межах підмережі, що є елементом складеної інтермережі. У різних підмережах припустимі різні мережеві технології, різні стеки протоколів, тому при створенні стека TCP/IP передбачалася наявність різних типів локальних адрес. Якщо підмережею інтермережі є локальна мережа, то локальна адреса - це **Мас-адреса**. Мас-адреса призначається мережевим адаптерам і мережевим інтерфейсам маршрутизаторів. Мас-адреси призначаються виробниками обладнання і є унікальними, тому що управляються централізовано. Для всіх існуючих технологій локальних мереж Мас-адреса має формат 6 байт, наприклад 11-A0-17-3D-BC-01. Однак протокол IP може працювати й над протоколами більш високого рівня, наприклад над протоколом IPX або Х.25. У цьому випадку локальними адресами для протоколу IP відповідно будуть адреси IPX і Х.25. Варто врахувати, що комп'ютер у локальній мережі може мати кілька локальних адрес навіть при одному мережевому адаптері. Деякі мережеві пристрої не мають локальних адрес. Наприклад, до таких пристроїв відносяться глобальні порти маршрутизаторів, призначені для з'єднань типу «точка-точка».

***IP-адреси*** являють собою основний тип адрес, на підставі яких мережевий рівень передає пакети між мережами. Ці адреси складаються з 4 байт, наприклад 109.26.17.100. IP-адреса призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. IP-адреса складається із двох частин: номера мережі й номера вузла. Номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу Internet (Internet Network Information Center, InterNIC), якщо мережа повинна працювати як складова частина Internet. Звичайно постачальники послуг Internet одержують діапазони адрес у підрозділів InterNIC, а потім розподіляють їх між своїми абонентами. Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор по визначенню входить відразу в кілька мереж. Тому кожен порт маршрутизатора має власну IP-адресу. Кінцевий вузол також може входити в кілька IP-мереж. У цьому випадку комп'ютер повинен мати кілька IP-адрес, по числу мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

***Символьні доменні імена****.* Символьні імена в IP-мережах називаються доменними й будуються по ієрархічній ознаці. Складові повного символьного імені в IP-мережах розділяються крапкою й перераховуються в наступному порядку: спочатку просте ім'я кінцевого вузла, потім ім'я групи вузлів (наприклад, ім'я організації), потім ім'я більшої групи (піддомена) і так до імені домена найвищого рівня (наприклад, домена об'єднуючої організації за географічним принципом: UA - Україна, US - США). Прикладом доменного імені може служити ім'я base2.sales.zil.ua. Між доменним ім'ям й IP-адресою вузла немає ніякої алгоритмічної відповідності, тому необхідно використовувати якісь додаткові таблиці або служби, щоб вузол мережі однозначно визначався як по доменному імені, так і по IP-адресі. У мережах TCP/IP використовується спеціальна розподілена служба Domain Name System (DNS), що встановлює цю відповідність на підставі створюваних адміністраторами мережі таблиць відповідності. Тому доменні імена називають також DNS-іменами.

**Формат IP-адреси**

Адреса IP складається з двох частин: номера мережі та номеру вузла. У разі ізольованої мережі її адреса може бути обрана адміністратором з навмисно зарезервованих для таких мереж блоків адрес (10.0.0.0/8, 172.16.0.0/12 або 192.168.0.0/16). Якщо ж мережа повинна працювати як складова частина [Інтернету](https://uk.wikipedia.org/wiki/Інтернет), то адреса мережі видається провайдером або регіональним інтернет-реєстратором (Regional Internet Registry, [RIR](https://uk.wikipedia.org/wiki/RIR)). Згідно з даними на сайті IANA існує п'ять RIR: [ARIN](https://uk.wikipedia.org/w/index.php?title=ARIN&action=edit&redlink=1), який обслуговує [Північну Америку](https://uk.wikipedia.org/wiki/Північна_Америка); APNIC, який обслуговує країни [Південно-Східної Азії](https://uk.wikipedia.org/wiki/Південно-Східна_Азія); [AfriNIC](https://uk.wikipedia.org/w/index.php?title=AfriNIC&action=edit&redlink=1), який обслуговує країни [Африки](https://uk.wikipedia.org/wiki/Африка); [LACNIC](https://uk.wikipedia.org/w/index.php?title=LACNIC&action=edit&redlink=1), обслуговує країни [Південної Америки](https://uk.wikipedia.org/wiki/Південна_Америка) й басейну Карибського моря; та [RIPE NCC](https://uk.wikipedia.org/wiki/RIPE_NCC), який обслуговує [Європу](https://uk.wikipedia.org/wiki/Європа), [Центральну Азію](https://uk.wikipedia.org/wiki/Центральна_Азія), [Близький Схід](https://uk.wikipedia.org/wiki/Близький_Схід). Регіональні реєстратори отримують номери автономних систем та великі блоки адрес у [IANA](https://uk.wikipedia.org/wiki/IANA), а потім видають номери автономних систем та блоки адрес меншого розміру локальним інтернет-реєстраторам (Local Internet Registries, [LIR](https://uk.wikipedia.org/wiki/LIR)), зазвичай є великими провайдерами.

Номер вузла в [протоколі IP](https://uk.wikipedia.org/wiki/IP) призначається незалежно від локальної адреси вузла. Маршрутизатор входить відразу до кількох мереж. Тому кожен порт маршрутизатора має власну адресу ІР. Кінцевий вузол також може входити до кількох мереж IP. У цьому випадку комп'ютер повинен мати кілька адрес IP, за числом мережних зв'язків. Таким чином, адреса IP характеризує не окремий комп'ютер чи маршрутизатор, а одне мережне з'єднання.

IP адреса - 32-бітове число, яке в традиційному уявленні записується у вигляді чисел, від 1 до 255, розділених між собою крапками.

Вид IP адреси в різних форматах запису:

* Десятковий вид IP адреси: 192.168.0.10.
* Двійковий вид того ж IP адреси: 11000000.10101000.00000000.00001010.
* Запис адреси в шістнадцятковій системі числення: C0.A8.00.0A.

Між ID мережі і номером точки в запису немає розділового знака, але комп`ютер здатний їх розділяти. Для цього існує три способи:

1. *Фіксована межа.* При цьому способі весь адреса умовно ділиться на дві частини фіксованої довжини побайтно. Таким чином, якщо під номер мережі віддати один байт, тоді ми отримаємо 28 мереж по 224 вузлів. Якщо кордон зрушити ще на байт вправо, на той час мереж стане більше - 216, а вузлів стане менше - 216. На сьогоднішній день підхід вважається застарілим і не використовується.
2. *Маска підмережі.* Маска йде в парі з IP адресою. Маска має послідовність значень "1" в тих розрядах, які відведені під номер мережі, і певну кількість нулів у тих місцях IP адреси, які відведені на номер вузла. Кордон між одиницями і нулями в масці - це межа між ідентифікатором мережі і ID вузла в IP-адресу.
3. *Метод класів адрес.* Компромісний метод. При його використанні розміри мереж не можуть бути обрані користувачем, однак є п`ять класів - А, В, С, D, Е. Три класи - А, В і С - призначені для різних мереж, а D і Е - зарезервовані для мереж спеціального призначення . У класової системі кожен клас має свою межу номера мережі і ID вузла.

**Класи IP-адрес**

До *класу А* відносяться мережі, в яких мережа ідентифікується по першому байту, а три залишилися є номером вузла. Всі IP адреси, які мають в своєму діапазоні значення першого байта від 1 до 126 - це мережі класу А. Кількісно мереж класу А виходить зовсім мало, зате в кожній з них може бути до 224 точок.

*клас В* - мережі, в яких дві вищі біти рівні 10. У них під номер мережі і ідентифікатор точки відводиться по 16 біт. В результаті виходить, що кількість мереж класу В у велику сторону відрізняється від кількості мереж класу А кількісно, але вони мають меншу кількість вузлів - до 65 536 (216) Шт.

У мережах *класу С* - зовсім мало вузлів - 28 в кожній, але кількість мереж величезна, завдяки тому, що ідентифікатор мережі в таких структурах займає цілих три байта.

мережі *класу D* - вже відносяться до особливих мереж. Він починається з послідовності 1110 і називається груповою адресою (Multicast adress). Інтерфейси, мають адреси класу А, В і С, можуть входити в групу і отримувати додатково до індивідуального ще й груповий адресу.

адреси *класу Е* - в резерві на майбутнє. Такі адреси починаються з послідовності 11110. Швидше за все, ці адреси будуть застосовуватися в якості групових, коли настане брак IP адрес в глобальній мережі.

У протоколі IP існує кілька угод про особливу інтерпретацію IP-адрес.

* Якщо вся IP-адреса складається тільки із двійкових нулів, то вона позначає адресу того вузла, що згенерував цей пакет; цей режим використовується тільки в деяких повідомленнях ICMP.
* Якщо в полі номера мережі стоять тільки нулі, то за замовчуванням вважається, що вузол призначення належить тій же самій мережі, що й вузол, що відправив пакет.
* Якщо всі двійкові розряди IP-адреси рівні 1, то пакет з такою адресою призначення повинен розсилатися всім вузлам, що перебувають у тій же мережі, що й джерело цього пакета. Таке розсилання називається **обмеженим широкомовним повідомленням (limited broadcast).**
* Якщо в поле номера вузла призначення стоять тільки одиниці, то пакет, що має таку адреса, розсилається всім вузлам мережі із заданим номером мережі. Наприклад, пакет з адресою 192.190.21.255 доставляється всім вузлам мережі 192.190.21. 0. Таке розсилання називається широкомовним повідомленням(broadcast).

При адресації необхідно враховувати ті обмеження, які вносяться особливим призначенням деяких IP-адрес. Так, ні номер мережі, ні номер вузла не може складатися тільки з одних двійкових одиниць або тільки з одних двійкових нулів. Звідси треба, що максимальна кількість вузлів, наведена в таблиці для мереж кожного класу, на практиці повинна бути зменшена на 2. Наприклад, у мережах класу С під номер вузла відводиться 8 біт, які дозволяють задавати 256 номерів: від 0 до 255. Однак на практиці максимальне число вузлів у мережі класу С не може перевищувати 254, тому що адреси 0 й 255 мають спеціальне призначення. Із цих же міркувань слідує, що кінцевий вузол не може мати адресу типу 98.255.255.255, оскільки номер вузла в цій адресі класу А складається з одних двійкових одиниць.

Особливе значення має IP-адреса, перший октет якої дорівнює 127. Вона використовується для тестування програм і взаємодії процесів у межах одної машини. Коли програма посилає дані по IP-адресі 127.0.0. 1, то утвориться «петля». Дані не передаються по мережі, а повертаються модулям верхнього рівня, як тільки що прийняті. Тому в IP-мережі забороняється привласнювати машинам IP-адреси, що починаються з 127. Ця адреса має назву **loopback.** Можна віднести адресу 127.0.0.0 до внутрішньої мережі модуля маршрутизації вузла, а адресу 127.0.0.1 - до адреси цього модуля на внутрішній мережі. Насправді будь-яка адреса мережі 127.0.0.0 служить для позначення свого модуля маршрутизації, а не тільки 127.0.0.1, наприклад 127.0.0.3.

У протоколі IP немає поняття широкомовності в тому розумінні, у якому воно використовується в протоколах канального рівня локальних мереж, коли дані повинні бути доставлені абсолютно всім вузлам. Як обмежена широкомовна IP-адреса, так і широкомовна IP-адреса мають межі розповсюдження в інтермережі - вони обмежені або мережею, до якої належить вузол-джерело пакета, або мережею, номер якої зазначений в адресі призначення. Тому ділення мережі за допомогою маршрутизаторів на частини, локалізує широкомовний шторм межами, однієї зі складових частин загальної мережі, просто тому, що немає способу адресувати пакет одночасно всім вузлам всіх мереж складеної мережі.

Уже згадувана форма групової IP-адреси — **multicast** — означає, що даний пакет повинен бути доставлений відразу декільком вузлам, які утворять групу з номером, зазначеним у полі адреси. Вузли самі ідентифікують себе, тобто визначають, до якій із груп вони належать. Той самий вузол може входити в кілька груп. Члени якої-небудь групи multicast не обов'язково повинні належати одній мережі. У загальному випадку вони можуть розподілятися по зовсім різних мережах, що перебувають один від одної на довільній кількості хопів. Групова адреса не ділиться на поля номера мережі й вузла й обробляється маршрутизатором особливим чином.

Основне призначення **multicast** -адрес - розповсюдження інформації зі схеми «один-до-багатьох». Хост, що хоче передавати ту саму інформацію багатьом абонентам, за допомогою спеціального протоколу IGMP (Internet Group Management Protocol) повідомляє про створення в мережі нової мультимовної групи з певною адресою. Машрутизатори, що підтримують мультимовність, поширюють інформацію про створення нової групи в мережах, підключених до портів цього маршрутизатора. Хости, які хочуть приєднатися до знов створеною мультимовної групи, сповіщають про це своїм локальним маршрутизаторам і ті передають цю інформацію хосту, ініціаторові створення нової групи.

Щоб маршрутизатори могли автоматично поширювати пакети з адресою **multicast** по складеній мережі, необхідно використовувати в кінцевих маршрутизаторах модифіковані протоколи обміну маршрутною інформацією, такі як, наприклад, MOSPF (Multicast OSPF, аналог OSPF).

Групова адресація призначена для економічного поширення в Internet або великої корпоративної мережі аудіо- або відеопрограм, призначених відразу великій аудиторії слухачів або глядачів. Якщо такі засоби знайдуть широке застосування (зараз вони представляють в основному невеликі експериментальні острівці в загальному Internet), то Internet зможе створити серйозну конкуренцію радіо й телебаченню.

**Поняття маски підмережі. Маски змінної довжини**

**Маска** — це число, що використовується в парі з IP-адресою; двійковий запис маски містить одиниці в тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Оскільки номер мережі є цільною частиною адреси, одиниці в масці також повинні становити безперервну послідовність. Для стандартних класів мереж маски мають наступні значення:

* клас А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
* клас В - 11111111. 11111111. 00000000. 00000000 (255.255.0.0);
* клас С- 11111111.11111111.11111111.00000000(255.255.255.0).

Для запису масок використовуються й інші формати, наприклад, зручно інтерпретувати значення маски, записаної в шістнадцятковому коді: FF.FF.00.00 - маска для адрес класу В. Часто зустрічається й таке позначення 185.23.44.206/16 - цей запис говорить про те, що маска для цієї адреси містить 16 одиниць або, що в указаній IP-адресі під номер мережі відведено 16 двійкових розрядів.

Позначаючи кожну IP-адресу маскою, можна відмовитися від понять класів адрес і зробити гнучкішою систему адресації. Наприклад, якщо розглянуту вище адресу 185.23.44.206 асоціювати з маскою 255.255.255.0, то номером мережі буде 185.23.44.0, а не 185.23.0.0, як це визначено системою класів.

У масках кількість одиниць у послідовності, що визначає границю номера мережі, не обов'язково повинне бути кратним 8, щоб повторювати розподіл адреси на байти. Нехай, наприклад, для IP-адреси 129.64.134.5 зазначено маску 255.255.128.0, тобто у двійковому виді: IP-адреса 129.64.134.5 - 10000001. 01000000.10000110. 00000101 Маска 255.255.128.0- 11111111.11111111.10000000.00000000

Якщо ігнорувати маску, то відповідно до системи класів адреса 129.64.134.5 відноситься до класу В, а виходить, номером мережі є перші 2 байти - 129.64.0.0, а номером вузла - 0.0.134.5.

Якщо ж використовувати для визначення границі номера мережі маску, то 17 послідовних одиниць у масці, «накладені» на IP-адресу, визначають як номер мережі у двійковому представленні число:

10000001. 01000000. 10000000. 00000000 або в десятковій формі запису - номер мережі 129.64.128.0, а номер вузла 0.0.6.5.

Механізм масок широко розповсюджений в IP-маршрутизації, причому маски можуть використовуватися для різних цілей. З їхньою допомогою адміністратор може структурувати свою мережу, не жадаючи від постачальника послуг додаткових номерів мереж. На основі цього ж механізму постачальники послуг можуть поєднувати адресні простори декількох мереж шляхом введення так званих «префіксів» з метою зменшення обсягу таблиць маршрутизації й підвищення за рахунок цього продуктивності маршрутизаторів.

**Порядок призначення IP-адрес**

Номери мереж призначаються або централізовано, якщо мережа є частиною Internet, або довільно, якщо мережа працює автономно. Номери вузлів і в тому і в іншому випадку адміністратор вільний призначати на свій розсуд, не виходячи, зрозуміло, з дозволеного для цього класу мережі діапазону.

Координуючу роль в централізованому розподілі IP-адрес до деякого часу грала організація InterNIC, однак з ростом мережі завдання розподілу адрес стала занадто складною, і InterNIC делегувала частину своїх функцій іншим організаціям і великим постачальникам послуг Internet.

Вже порівняно давно спостерігається дефіцит IP-адрес. Дуже важко отримати адреса класу В і практично неможливо стати володарем адреси класу А. При цьому треба зазначити, що дефіцит обумовлений не тільки зростанням мереж, але і тим, що наявне безліч IP-адрес використовується нераціонально. Дуже часто власники мережі класу С витрачають лише невелику частину з наявних у них 254 адрес. Розглянемо приклад, коли дві мережі необхідно з'єднати глобальним зв'язком. У таких випадках в якості каналу зв'язку використовують два маршрутизатора, з'єднаних за схемою «точка-точка» (рис. 5.10). Для вироджених мережі, утвореної каналом, що зв'язує порти двох суміжних маршрутизаторів, доводиться виділяти окремий номер мережі, хоча в цій мережі є всього 2 вузли.

Якщо ж деяка IP-мережа створена для роботи в «автономному режимі», без зв'язку з Internet, тоді адміністратор цієї мережі вільний призначити їй довільно обраний номер. Але і в цій ситуації для того, щоб уникнути будь-яких колізій, в стандартах Internet визначено кілька діапазонів адрес, рекомендованих для локального використання. Ці адреси не обробляються маршрутизаторами Internet ні за яких умов. Адреси, зарезервовані для локальних цілей, обрані з різних класів: в класі А - це мережа 10.0.0.0, в класі В - це діапазон з 16 номерів мереж 172.16.0.0-172.31.0.0, в класі С - це діапазон з 255 мереж - 192.168.0.0-192.168.255.0.

Для пом'якшення проблеми дефіциту адрес розробники стека TCP / IP пропонують різні підходи. Принциповим рішенням є перехід на нову версію IPv6, в якій різко розширюється адресний простір за рахунок використання 16-байтних адрес. Однак і поточна версія IPv4 підтримує деякі технології, спрямовані на більш економне витрачання IP-адрес. Однією з таких технологій є технологія масок і її розвиток - технологія безкласової междоменной маршрутизації (Classless Inter-Domain Routing, CIDR). Технологія CIDR відмовляється від традиційної концепції поділу адрес протоколу IP на класи, що дозволяє отримувати в користування стільки адрес, скільки реально необхідно. Завдяки CIDR постачальник послуг одержує можливість «нарізати» блоки з виділеного йому адресного простору в точній відповідності з вимогами кожного клієнта, при цьому у нього залишається простір для маневру на випадок його майбутнього зростання.

Інша технологія, яка може бути використана для зняття дефіциту адрес, це трансляція адрес (Network Address Translator, NAT). Вузлів внутрішньої мережі адреси призначаються довільно (природно, відповідно до загальних правил, визначених в стандарті), так, як ніби ця мережа працює автономно. Внутрішня мережа з'єднується з Internet через деякий проміжний пристрій (маршрутизатор, міжмережевий екран). Це проміжний пристрій отримує в своє розпорядження кілька зовнішніх «нормальних» IP-адрес, погоджених з постачальником послуг або іншою організацією, що розподіляє IP-адреси. Проміжне пристрій здатний перетворювати внутрішні адреси в зовнішні, використовуючи для цього якісь таблиці відповідності. Для зовнішніх користувачів всі численні вузли внутрішньої мережі виступають під декількома зовнішніми IP-адресами. При отриманні зовнішнього запиту цей пристрій аналізує його вміст і при необхідності пересилає його у внутрішню мережу, замінюючи IP-адреса на внутрішній адресу цього вузла. Процедура трансляції адрес визначена в RFC 1 631.

**Автоматизація процесу призначення IP-адрес**

Призначення IP-адрес вузлам мережі навіть при не дуже великому розмірі мережі може представляти для адміністратора тяжку процедуру. протокол Dynamic Host Configuration Protocol (DHCP) звільняє адміністратора від цих проблем, автоматизуючи процес призначення IP-адрес.

DHCP може підтримувати спосіб автоматичного динамічного розподілу адрес, а також більш прості способи ручного і автоматичного статичного призначення адрес. Протокол DHCP працює відповідно до моделі клієнт-сервер. Під час старту системи комп'ютер, що є DHCP-клієнтом, посилає в мережу широкомовний запит на отримання IP-адреси. DHCP-cepвер відгукується і посилає повідомлення-відповідь, що містить IP-адресу. Передбачається, що DHCP-клієнт і DHCP-сервер знаходяться в одній IP-мережі.

При динамічному розподілі адрес DHCP-сервер видає адреса клієнту на обмежений час, зване часом оренди (lease duration), що дає можливість згодом повторно використовувати цей IP-адреса для призначення іншого комп'ютера. Основна перевага DHCP - автоматизація рутинної роботи адміністратора по конфігурації стека TCP / IP на кожному комп'ютері. Іноді динамічне поділ адрес дозволяє будувати IP-мережу, кількість вузлів в якій перевищує кількість наявних у розпорядженні адміністратора IP-адрес.

У ручній процедуру призначення статичних адрес активну участь приймає адміністратор, який надає DHCP-серверу інформацію про відповідність IP-адрес фізичним адресами або іншим ідентифікаторів клієнтів. DHCP-сервер, користуючись цією інформацією, завжди видає певному клієнту призначений адміністратором адресу.

При автоматичному статичному способі DHCP-сервер привласнює IP-адреса з пула готівкових IP-адрес без втручання оператора. Межі пулу призначаються адрес задає адміністратор при конфігуруванні DHCP-сервера. Адреса дається клієнту з пулу в постійне користування, тобто з необмеженим терміном оренди. Міжідентифікатором клієнта і його IP-адресою, як і раніше, як і при ручному призначення, існує постійну відповідність. Воно встановлюється в момент першого призначення DHCP-сервером IP-адреси клієнта. При всіх наступних запитах сервер повертає той же самий IP-адресу.

DHCP забезпечує надійний і простий спосіб конфігурації мережі TCP / IP, гарантуючи відсутність дублювання адрес за рахунок централізованого управління їх розподілом. Адміністратор управляє процесом призначення адрес за допомогою параметра «тривалість оренди», яка визначає, як довго комп'ютер може використовувати призначений IP-адреса, перед тим як знову запросити його від DHCP-сервера в оренду.

Прикладом роботи протоколу DHCP може служити ситуація, коли комп'ютер, що є DHCP-клієнтом, видаляється з підмережі. При цьому призначений йому IP-адреса автоматично звільняється. Коли комп'ютер підключається до іншої підмережі, то йому автоматично призначається нову адресу. Ні користувач, ні мережевий адміністратор не втручаються в цей процес. Це властивість дуже важливо для мобільних користувачів.

DHCP-сервер може призначити клієнту не тільки IP-адресу клієнта, але і інші параметри стека TCP / IP, необхідні для його ефективної роботи, наприклад, маску, IP-адреса маршрутизатора за замовчуванням, IP-адреса сервера DNS, доменне ім'я комп'ютера і т . п.

**Відображення IP адрес на локальні адреси**

Однією з головних завдань, яке ставилося при створенні протоколу IP, було забезпечення спільної узгодженої роботи в мережі, що складається з підмереж,

в загальному випадку використовують різні мережеві технології. Безпосередньо з вирішенням цього завдання пов'язаний рівень міжмережевих інтерфейсів стека TCP / IP. На цьому рівні визначаються вже розглянуті вище специфікації упаковки (інкапсуляції) IP-пакетів в кадри локальних технологій. Крім цього, рівень міжмережевих інтерфейсів повинен займатися також украй важливим завданням відображення IP-адрес в локальні адреси.

Для визначення локального адреси по IP-адресою використовується протокол разреше-ня адреси (Address Resolution Protocol, ARP). Протокол ARP працює по-різному залежно від того, який протокол канального рівня працює в даній мережі - протокол локальної мережі (Ethernet, Token Ring, FDDI) з можливістю широкомовного доступу одночасно до всіх вузлів мережі або ж протокол глобальної мережі (Х.25, frame relay), як правило не підтримуючий широкомовний доступ. Існує також протокол, що вирішує зворотну задачу - знаходження IP-адреси за відомим локальному адресою. Він називається реверсивним ARP (Reverse Address Resolution Protocol, RARP) і використовується при старті бездискових станцій, хто знає в початковий момент свого IP-адреси, але знають адресу свого мережевого адаптера.

Необхідність у зверненні до протоколу ARP виникає кожен раз, коли модуль IP передає пакет на рівень мережевих інтерфейсів, наприклад драйверу Ethernet. IP-адреса вузла призначення відомий модулю IP. Потрібно на його основі знайти МАС-адресу вузла призначення.

Робота протоколу ARP починається з перегляду так званої ARP-таблиці .Кожен рядок таблиці встановлює відповідність між IP-адресою і МАС-адресою. Для кожної мережі, підключеної до мережевого адаптера комп'ютера або до порту маршрутизатора, будується окрема ARP-таблиця.

**Система DNS**

**Доменна система імен** ([англ.](https://uk.wikipedia.org/wiki/Англійська_мова) *Domain Name System*, DNS) — ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в [IP-адресу](https://uk.wikipedia.org/wiki/IP-адреса).

Кожен [комп'ютер](https://uk.wikipedia.org/wiki/Комп'ютер) в [Інтернеті](https://uk.wikipedia.org/wiki/Інтернет) має свою власну унікальну адресу — число, яке складається з чотирьох (у протоколі [IPv4](https://uk.wikipedia.org/wiki/IPv4)) або шістнадцяти (у протоколі [IPv6](https://uk.wikipedia.org/wiki/IPv6)) [байтів](https://uk.wikipedia.org/wiki/Байт). Оскільки запам'ятовування десятків чи навіть сотень номерів — не надто приємна процедура, то всі (чи майже всі) машини мають імена, запам'ятати які (особливо якщо знати правила утворення імен) значно легше.

Уся система імен в Інтернеті — [ієрархічна](https://uk.wikipedia.org/wiki/Ієрархічна_структура). Це зроблено для того, щоб не підтримувати одне централізоване джерело, а *роздати владу на місця*.

Повне доменне (від [англ.](https://uk.wikipedia.org/wiki/Англійська_мова) *domain*) ім'я машини (FQDN, Fully Qualified Domain Name) можна розбити на дві частини — ім'я області-домена та власне ім'я машини. Наприклад, *m30.ziet.zhitomir.ua* — повне доменне ім'я машини *m30*, яка перебуває у домені *ziet.zhitomir.ua*.

За порядок у доменах, як правило, відповідає певний комп'ютер, користувачі-адміністратори якого слідкують за тим, щоб не було, наприклад, різних машин з однаковими ІР-адресами. Наприклад, відповідальність за область-домен *ziet.zhitomir.ua* покладається на машину *alpha.ziet.zhitomir.ua* Ця влада делегується зверху вниз від машини *ns.lucky.net*, яка відповідає за домен *zhitomir.ua*. В свою чергу, відповідальність за область ua делегована машині зверху від так званих кореневих серверів (*root server*).

Всю цю систему можна уявити у вигляді перевернутого дерева. Список імен доменів верхнього рівня на сайті [IANA](https://uk.wikipedia.org/wiki/IANA)(<https://www.iana.org/domains/root/db>). Повний список географічних областей, в основному, відповідає [двохбуквеним ISO-кодам країн](https://uk.wikipedia.org/w/index.php?title=Двохбуквені_ISO-коди_країн&action=edit&redlink=1) і його можна знайти, наприклад, на WWW-сервері [ISOC](https://uk.wikipedia.org/wiki/ISOC) ([http://www.isoc.org](http://www.isoc.org/)).

Необхідно розрізняти доменне ім'я, та поштову адресу. В поштовій адресі повинен бути знак [«@»](https://uk.wikipedia.org/wiki/@), який в економіці має назву «комерційне *at*», а в електронній пошті — «равлик». Знак [«@»](https://uk.wikipedia.org/wiki/@) у поштовій адресі відокремлює ім'я поштової скриньки від [доменного ім'я](https://uk.wikipedia.org/wiki/Доменне_ім'я). Знак [«@»](https://uk.wikipedia.org/wiki/@) вперше у 1971 році використав [Рей Томлінсон](https://uk.wikipedia.org/wiki/Рей_Томлінсон), щоб відокремити імена користувача і комп'ютера, коли він відправив повідомлення з одного ДЕК-10 (*Digital Equipment Corporation*) комп'ютера на інший ДЕК-10. Обидва комп'ютери були розміщені поруч один з одним.

Коли мережа [Інтернет](https://uk.wikipedia.org/wiki/Інтернет) була молода та невелика, таблиці відповідності імен та адрес зберігалися у звичайному [текстовому файлі](https://uk.wikipedia.org/wiki/Текстовий_файл), який періодично просто розсилався всім учасникам електронною поштою. Після того, які кількість машин значно збільшилася, така схема перестала ефективно працювати і програмісти [університету штату Каліфорнія в Берклі](https://uk.wikipedia.org/wiki/Університет_Каліфорнії,_Берклі) спроектували і написали програму BIND (Berkeley Internet Name Domain), яка відповідає на запити машин користувачів, які стосувалися імен та ІР-адресу.

Служба імен DNS (Domain Name System) — це [розподілена база даних](https://uk.wikipedia.org/wiki/Розподілена_база_даних) доволі простої структури. Для початкового знайомства можна вважати, що це кілька таблиць, у яких записано:

* яку ІР-адресу має машина з певним іменем;
* яке ім'я має машина з визначеною адресою;
* що це за комп'ютер і яка операційна система встановлена на ньому;
* куди потрібно направляти електронну пошту для користувачів цієї машини;
* які псевдоніми є у даної машини.

Для прикладу розглянемо випадок, коли користувач посилає пошту з машини *polesye.zhitomir.ua* користувачу за адресою *rozhik@ziet.zhitomir.ua*. При встановленні на машину протоколів [TCP/IP](https://uk.wikipedia.org/wiki/TCP/IP) системний адміністратор вказує ІР-адресу комп'ютера — найближчого серверу імен. Поштова програма подає цьому найближчому серверу запит: «Куди посилати пошту для ziet.zhitomir.ua» Якщо найближчий сервер не може відповісти, то він, в свою чергу, посилає запит до більш «старшого» серверу. Нарешті, стає зрозумілим, що всю пошту для області *ziet.zhitomir.ua* необхідно відправляти на машину *alpha.ziet.zhitomir.ua*або *relay2.lucky.net*. Разом з цим відповіді містять ще адресу цієї машини. Поштова програма зв'язується з цим комп'ютером (використовуючи не ім'я, а адресу) та передає йому пошту. Всі ці переговори та відправка пошти, як правило, відбувається протягом кількох секунд і користувач не помічає цього. Якщо машина *ziet.zhitomir.ua* недоступна то тоді пошта на час, в якій неможливо зв'язатися з машиною *ziet.zhitomir.ua* (наприклад під час профілактики каналу зв'язку) чекає своєї черги на пересилку на машині *relay2.lucky.net*.

Це характерна для Internet-програм поведінка. Як правило, поштові програми подають доволі багато запитів службі [DNS](https://uk.wikipedia.org/wiki/DNS), і ці питання доволі складні. У більшості випадків у програмах користувачів намагаються дізнатися лише одне — яка [ІР-адреса](https://uk.wikipedia.org/wiki/ІР-адреса) у машини з відповідним іменем. Зрозуміло, що всередині цієї системи імен існує маса нюансів, правил та хитрощів. Докладніше з ними можна ознайомитися в описах стандартів [Internet](https://uk.wikipedia.org/wiki/Internet) або в спеціальних книгах.

Компанія «[Хостмастер](https://uk.wikipedia.org/wiki/Хостмайстер)» спільно з [ICANN](https://uk.wikipedia.org/wiki/ICANN) в Україні ввела у дію локальний кореневий сервер DNS, що містить інформацію про домени верхнього рівня. Сервер є «дзеркалом» одного з 13-кореневих серверів ICANN, відомого під назвою «L-root».

Як вже було відмічено, існує домен кореневого рівня, який позначається «„.“».Наступний рівень ієрархії — це домени верхнього рівня. Вся структура служби DNS є ієрархічною. Існують домени першого, другого, третього, n-го рівнів.  
Розглянемо доменне ім'я комп'ютера «www.department.firma.isp.ua».  
Тут доменом першого рівня є ua, isp — другого, firma — третього, а department — четвертого рівня.

Існує три основні типи серверів DNS, які відрізняються покладеними на них завданнями:

* основний сервер DNS;
* резервний (вторинний) сервер DNS;
* кешуючий сервер DNS.

Основний сервер DNS управляє зоною повноважень. Якщо потрібно додати/видалити домен або вузол або якось інакше модифікувати зону, зміни потрібно проводити на основному сервері DNS. Через певний час, який залежить від налаштувань сервера, основний сервер передасть зону резервному серверу DNS. Дане явище називається трансфером зони.

Що ж до резервних серверів, то повинен бути хоч би один резервний сервер DNS. Тому є декілька причин: якщо клієнтів багато, то наявність резервного сервера DNS дозволить знизити навантаження на основний сервер DNS і прискорити доступ фізично віддалених від основного сервера клієнтів до бази даних доменних імен.