НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут комп’ютерних інформаційних технологій

Кафедра комп'ютерних систем та мереж

# Лабораторна робота № 3

з дисципліни «Комп’ютерні мережі»

Виконав: Клокун В. Д. Роботу захищено:

Група: СП-425

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

Київ 2019

**Маршрутизація в мережах TCP/IP**

**Поняття та алгоритми маршрутизації**

Маршрутизація в мережах TCP / IP має 2 значення:

1. Процедура пошуку мережевої адреси в спеціальній таблиці для передачі пакета в вузол призначення.

2. Процес побудови такої таблиці

Маршрутизація існує як перенаправлення IP-пакетів і маршрутизація як управління таблицями маршрутизації.

Хости посилають пакети тільки тим шлюзів, які фізично підключені до тієї ж мережі.

Локальні хости можуть переміщувати пакети тільки на 1 крок в напрямку вузла призначення.

Кожен шлюз через який проходить пакет приймає рішення про його переміщення, аналізуючи власну таблицю маршрутизації.

Таблиці маршрутизації ведуться статичним, динамічним і комбінованим способом.

Статичний маршрут фіксується в таблиці маршрутизації і не змінюється протягом усього часу роботи хоста. Статичний маршрут використовується у відносно стабільній локальної мережі. Вона проста в управлінні і надійна у використанні, але вимагає від персоналу знання топології мережі на момент створення таблиці маршрутизації.

У мережах з більш складною топологією, коли з'являються додаткові шлюзи, коли з'являються додаткові канали зв'язку між хостами, пропускна здатність між каналами висока.

У разі динамічної маршрутизації на відповідних шлюзах постійно працює спеціальний процес (демон). Процес веде і модифікує таблицю маршрутизації. Крім цього, він постійно взаємодіє з іншими процесами демонами інших шлюзів для того, щоб визначати топологію мережі і приймати рішення доставки пакетів до хостів шлюзів.

Комбінована маршрутизація. Для простих маршрутизаторів - статична маршрутизація, для складних - динамічна маршрутизація.

Існує 4 рівня складності характеризують процес управління маршрутизацією в мережі:

1. 0 рівень. Відсутність маршрутизації як такої

2. Тільки статична маршрутизація

3. Переважно статична маршрутизація з періодичними оновленнями маршрутів, які змінюють статичні таблиці маршрутизації (здійснюється за допомогою протоколу RIP)

4. Динамічна маршрутизація

фіксована маршрутизація

є одним з методів динамічної маршрутизації і використовується в мережах з простою топологією зв'язку. При фіксованій маршрутизації однопутевие таблиці, в яких для кожного адресата є один шлях. в багатоколійні таблицях для кожного адресата є кілька альтернативних шляхів і обов'язково має бути присутнім правило вибору шляхів.

Алгоритм простий маршрутизації

1. Випадкова маршрутизація, коли пакети перенаправляються в будь-якому випадковому (одному) напрямку, крім вихідного.

2. Лавинна маршрутизація - пакети передаються у всіх напрямках крім вихідного

3. Маршрутизація з попереднього досвіду. Цей метод динамічної маршрутизації працює на основі пакетів, які проходили через цей маршрут.

**Адаптивна маршрутизація**

Основний вид алгоритмів маршрутизації застосовується в сучасних мережах зі складною топологією. Алгоритми цього виду засновані на періодичний обмін інформацією про наявні в інтермережі мережах. А також про зв'язки між маршрутизаторами. Крім цього алгоритми враховують не тільки топологію зв'язку шлюзів, а й продуктивність і стан цих зв'язків. Серед алгоритмів адаптивної маршрутизації розрізняють:

1. Дистанційно-векторні алгоритми

2. Алгоритми стану зв'язку

**Дистанційно-векторні алгоритми**

Кожен маршрутизатор передає і широкомовно розсилає по мережі вектор відстаней від себе до всіх відомих йому мереж. Під відстанню тут розуміється число прокладених маршрутів через які пакет повинен пройти перш ніж потрапить у відповідну мережу. Отримуючи такий вектор інший маршрутизатор додає свої відомості про відомі йому мережах і теж розсилає цей вектор всім іншим.

Другий алгоритм пов'язаний із забезпеченням кожного маршрутизатора інформацією на основі якої будується точний граф стану мережі. Всі маршрутизатори працюють на основі однакових графів.

**Таблиці маршрутизації**

**Таблиця маршрутизації** ([англ.](https://uk.wikipedia.org/wiki/Англійська_мова) *routing table*)  — електронна таблиця (файл) або [база даних](https://uk.wikipedia.org/wiki/База_даних), що зберігається на [маршрутизаторі](https://uk.wikipedia.org/wiki/Маршрутизатор) або мережевому комп'ютері, що описує відповідність між адресами призначення і [інтерфейсами](https://uk.wikipedia.org/wiki/Інтерфейс), через які слід відправити пакет даних до наступного [маршрутизатора](https://uk.wikipedia.org/wiki/Маршрутизатор). Є найпростішою формою правил маршрутизації.

Таблиця маршрутизації зазвичай містить:

* Адресу мережі або вузла призначення, або вказівку, що маршрут є маршрутом за замовченням (default route)
* [Маску мережі](https://uk.wikipedia.org/wiki/Маска_підмережі) призначення (для IPv4-мереж маска / 32 (255.255.255.255) дозволяє вказати одиничний вузол мережі)
* Шлюз, що позначає адресу маршрутизатора в мережі, на яку необхідно надіслати пакет, що прямує до вказаної адреси призначення
* Інтерфейс (залежно від системи це може бути порядковий номер, GUID або символьне ім'я пристрою)
* Метрику — числовий показник, що задає перевагу маршруту. Чим менше число, тим кращий маршрут (інтуїтивно представляється як відстань).

У таблиці може бути один, а в деяких операційних системах і кілька шлюзів за замовченням. Такий шлюз використовується для мереж для яких немає більш конкретних маршрутів в таблиці маршрутизації.

|  |
| --- |
| ===========================================================================  Interface List  0x1 ........................... MS TCP Loopback interface  0x2 ...00 14 2a 8b a1 b5 ...... NVIDIA nForce Networking Controller  0x3 ...00 50 56 c0 00 01 ...... VMware Virtual Ethernet Adapter for VMnet1  0xd0005 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface  ===========================================================================  ===========================================================================  Active Routes:  Network Destination Netmask Gateway Interface Metric  0.0.0.0 0.0.0.0 89.223.67.129 89.223.67.131 20  60.48.85.155 255.255.255.255 89.223.67.129 89.223.67.131 20  60.49.71.132 255.255.255.255 89.223.67.129 89.223.67.131 20  89.223.67.128 255.255.255.192 89.223.67.131 89.223.67.131 20  89.223.67.131 255.255.255.255 127.0.0.1 127.0.0.1 20  89.255.255.255 255.255.255.255 89.223.67.131 89.223.67.131 20  192.168.192.0 255.255.255.0 192.168.192.251 192.168.192.251 1  192.168.192.251 255.255.255.255 127.0.0.1 127.0.0.1 50  212.113.96.250 255.255.255.255 89.223.67.129 89.223.67.131 20  219.95.153.243 255.255.255.255 89.223.67.129 89.223.67.131 20  224.0.0.0 240.0.0.0 89.223.67.131 89.223.67.131 20  224.0.0.0 240.0.0.0 192.168.23.1 192.168.23.1 20  224.0.0.0 240.0.0.0 192.168.192.251 192.168.192.251 50  255.255.255.255 255.255.255.255 89.223.67.131 89.223.67.131 1  255.255.255.255 255.255.255.255 192.168.23.1 192.168.23.1 1  255.255.255.255 255.255.255.255 192.168.192.251 192.168.192.251 1  Default Gateway: 89.223.67.129  =========================================================================== |
| Приклад таблиці маршрутизації (loopback, дві мережні карти та VPN-з'єднання) |

Типи записів в таблиці маршрутизації:

* маршрут до мережі
* маршрут до хоста
* маршрут за замовчанням

**Маршрутизація без використання масок**

Розглянемо на прикладі IP-мережі (рис. 5.14) алгоритм роботи засобів мережного рівня по просуванню пакета в складеній мережі. При цьому будемо вважати, що всі вузли мережі, яка розглядається в прикладі, мають адреси, засновані на класах, без використання масок. Особлива увагу буде приділено взаємодії протоколу IP із протоколами дозволу адрес ARP й DNS.

|  |
| --- |
| Мал. 5.14. Приклад взаємодії комп'ютерів через мережу |
| Рис. 5.14. Приклад взаємодії комп'ютерів через мережу |

|  |  |
| --- | --- |
| **1.** | Отже, нехай користувач комп'ютера cit.dol.ru, що перебуває в мережі Ethernet і має IP-адресу 194.87.23.17 (адреса класу З), звертається за протоколом FTP до комп'ютера sl.msk.su, що належить іншій мережі Ethernet і має IP-адресу 142.06.13.14 (адреса класу В): ftp sl.msk.su  Модуль FTP упаковує своє повідомлення в сегмент транспортного протоколу TCP, що у свою чергу поміщає свій сегмент у пакет протоколу IP. У заголовку IP-пакета повинна бути зазначена IP-адреса вузла призначення. Тому що користувач комп'ютера cit.dol.ru використовує символьне ім'я комп'ютера sl.msk.su, те стек TCP/IP повинен визначити IP-адресу вузла призначення самостійно.  При конфігуруванні стека TCP/IP у комп'ютері cit.dol.ru була задана його власна IP-адреса, IP-адреса маршрутизатора за замовчуванням й IP-адреса DNS- сервера. Модуль IP може зробити запит до сервера DNS, але звичайно спочатку проглядається локальна таблиця відповідності символьних імен й IP-адрес. Така таблиця зберігається найчастіше у вигляді текстового файла простої структури - кожен його рядок містить запис про одне символьне ім'я і його IP-адресу. В ОС Unix такий файл традиційно має ім'я hosts і перебуває в каталозі /etc. |
| **2.** | Будемо вважати, що комп'ютер cit.dol.ru має файл hosts, а в ньому є рядок 142.06.13.14 sl.msk.su  Таким чином, дозвіл імені виконується локально, і протокол IP може тепер формувати IP-пакети з адресою призначення 142.06.13.14 для взаємодії з комп'ютером sl.msk.su. |
| **3.** | Модуль IP комп'ютера cit.dol.ru перевіряє, чи потрібно маршрутизувати пакети з адресою 142.06.13.14. Тому що адреса мережі призначення (142.06.0.0) не збігається з адресою (194.87.23.0) мережі, якій належить комп'ютер-відправник, то маршрутизація необхідна. |
| **4.** | Комп'ютер cit.dol.ru починає формувати кадр Ethernet для відправлення IP-пакета маршрутизатору за замовчуванням, IP-адреса якого відома - 194.87.23.1, але невідома Мас-адреса, необхідна для переміщення кадру в локальній мережі. Для визначення Мас-адреси маршрутизатора протокол IP звертається до протоколу ARP, що переглядає ARP-таблицю. Якщо останнім часом комп'ютер cit.dol.ru виконував які-небудь міжмережні обміни, то швидше за все шуканий запис, що містить відповідність між IP- і Мас-адресами маршрутизатора за замовчуванням уже перебуває в кеш-таблиці протоколу ARP. Нехай у цьому випадку потрібний запис був знайдений саме в кеш-таблице  194.87.23.1 008048ЕВ7Е60  Позначимо знайдену МАС-адресу 008048ЕВ7Е60 відповідно до номера маршрутизатора і його порту через МАС11. |
| **5.** | В результаті комп'ютер cit.dol.ru відправляє по локальній мережі пакет, упакований у кадр Ethernet, що має наступні поля:  http://matveev.kiev.ua/archnet/gl5/images/p1.jpg |
| **6.** | Кадр приймається **портом 1маршрутизатора 1** відповідно до протоколу Ethernet, тому що Мас-вузол цього порту розпізнає свою адресу. Протокол Ethernet витягає із цього кадру IP-пакет і передає його програмному забезпеченню маршрутизатора, що реалізує протокол IP. Протокол IP витягає з пакета адресу призначення 142.06.13.14 і переглядає запису своїй таблиці маршрутизації. Нехай маршрутизатор 1 має у своїй таблиці маршрутизації запис  142.06.0.0 135.12.0.11 2, яка говорить про те, що пакети для мережі 142.06.0.0 потрібно передавати маршрутизатору 135.12.0.11, що перебуває в мережі, підключеній до **порту 2маршрутизатори 1**. |
| **7.** | **Маршрутизатор 1** переглядає параметри **порту 2** і знаходить, що до нього підключена мережа FDDI. Тому що мережа FDDI має значення MTU більше, ніж мережа Ethernet, тому фрагментація IP-пакета не потрібна. Тому**маршрутизатор 1** формує кадр формату FDDI. На цьому етапі модуль IP повинен визначити Мас-адресу наступного маршрутизатора по відомій IP-адресі 135.12.0.11. Для цього він звертається до протоколу ARP. Припустимо, що потрібного запису в кеш-таблиці не виявилося, тоді в мережу FDDI відправляється широкомовний ARP-запит, що містить поряд з іншої наступну інформацію. http://matveev.kiev.ua/archnet/gl5/images/p2.jpg **Порт 1 маршрутизатора 2** розпізнає свою IP-адресу й посилає ARP-відповідь за адресою вузла, що запросив: http://matveev.kiev.ua/archnet/gl5/images/p3.jpg Тепер, знаючи Мас-адресу наступного маршрутизатора 00E0F77F51A0, **маршрутизатор 1** відсилає кадр FDDI у напрямку до **маршрутизатора 2**. Помітимо, що в поле IP-адреси призначення ніяких змін не відбулося. http://matveev.kiev.ua/archnet/gl5/images/p4.jpg |
| **8.** | Аналогічно діє модуль IP на **маршрутизаторі 2**. Одержавши кадр FDDI, він відкидає його заголовок, а із заголовка IP витягає IP-адресу мережі призначення й переглядає свою таблицю маршрутизації. Там він може знайти запис про конкретну мережу призначення:  142.06.0.0 203.21.4.12 2  або при відсутності такого запису буде використаний запис про маршрутизатор за замовчуванням: default 203.21.4.12 2, Визначивши IP-адресу наступного маршрутизатора 203.21.4.12, модуль IP формує кадр Ethernet для передачі пакета **маршрутизатору 3** по мережі Ethernet.  За допомогою протоколу ARP він знаходить Мас-адресу цього маршрутизатора й поміщає його в заголовок кадру. IP-адреса вузла призначення, природно, залишається незмінною. http://matveev.kiev.ua/archnet/gl5/images/p5.jpg |
| **9.** | Нарешті, після того як пакет надійшов у маршрутизатора мережі призначення - **маршрутизатор 3**, - з'являється можливість передачі цього пакета комп'ютеру призначення. **Маршрутизатор 3** визначає, що пакет потрібно передати в мережу 142.06.0.0, що безпосередньо підключена до його першого порту. Тому він посилає ARP-запит по мережі Ethernet з IP-адресою комп'ютера s1.msk.su. ARP-відповідь містить Мас-адресу кінцевого вузла, що модуль IP передає канальному протоколу для формування кадру Ethernet:  http://matveev.kiev.ua/archnet/gl5/images/p6.jpg |
| **10.** | Мережевий адаптер комп'ютера sl.msk.su захоплює кадр Ethernet, виявляє збіг Мас-адрес, що міститься в заголовку, зі своєю власною адресою й направляє його модулю IP. Після аналізу полів IP-заголовка з пакета витягаються дані, які у свою чергу містять повідомлення вище лежачого протоколу. Оскільки в даному прикладі розглядається обмін даними за протоколом FTP, що використовується як транспортний протокол TCP, то в полі даних IP-пакета перебуває TCP-сегмент. Визначивши з TCP-заголовка номер порту, модуль IP переправляє сегмент у відповідну чергу, з якої даний сегмент потрапить програмному модулю FTP-сервера. |

**Маршрутизація з використанням масок і технологія CIDR**

Поява безкласової міждоменної маршрутизації CIDR (Classless Inter-Domain Routing) була викликана різким збільшенням числа мереж в Інтернет і, як наслідок, збільшенням кількості маршрутів на магістральних маршрутизаторах, що призводило до зменшення їх продуктивності і гранично підвищених вимог до об'єму пам'яті.

Технологія CIDR дозволяє відійти від класової схеми адресації, ефективніше використовувати адресний простір протоколу IP. Крім того, технологія CIDR забезпечує можливість підсумовування маршрутних записів. Одним записом в таблиці маршрутизації можуть описуватися шляхи до багатьох мереж.

Суть технології CIDR полягає у тому, що кожному постачальнику послуг Інтернет (або, для корпоративних мереж, якому-небудь структурно-територіальному підрозділу) повинен бути призначений нерозривний діапазон IP-адрес.

Розподіл IP-адреси на номер мережі і номер вузла в технології CIDR відбувається не на основі декількох старших бітів, що визначають клас мережі (А, В або С), а на основі маски змінної довжини (узагальнений мережевий префікс, що визначає загальну частину всіх адрес), що призначається постачальником послуг.

Неодмінною умовою застосування CIDR є наявність у організації, що розпоряджається адресами, безперервних діапазонів адрес. Такі адреси мають однаковий мережевий префікс, тобто однакові цифри в декількох старших розрядах. Нехай у розпорядженні деякого постачальника послуг є безперервний простір IP адрес в кількості https://konspekta.net/infopediasu/baza9/1549741396691.files/image035.gif. Звідси витікає, що префікс постачальника має довжину (https://konspekta.net/infopediasu/baza9/1549741396691.files/image037.gif) бітів.

Коли споживач звертається до постачальника послуг з проханням про виділення йому деякого числа адрес, то в наявному пулі адрес «вирізається» безперервна область S1, S2 або S3, залежно від необхідної кількості адрес. При цьому завжди повинні виконуватися такі умови:

- кількість адрес в області, що виділяється, повинна дорівнювати степені числа два;

- початкова межа пулу адрес (в десятковому виді), що виділяється, повинна бути кратною необхідній кількості вузлів.

Очевидно, що префікс кожної з показаних на рисунку 5.7 областей має власну довжину - чим менше кількість адрес в даній області, тим довше її префікс.

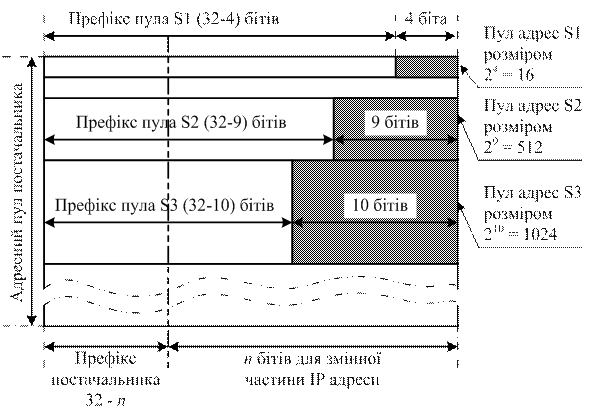


Рисунок – Розподіл адрес на основі технології CIDR

**Приклад.** Нехай постачальник послуг має в своєму розпорядженні пул адрес в діапазоні 193.20.0.0 - 193.23.255.255 (11000001. 00010100. 00000000. 00000000 – 11000001. 00010111. 01111111. 11111111), тобто кількість адрес дорівнює 218. Відповідно префікс постачальника послуг має довжину 14 розрядів - 11000001. 000101, або в іншому вигляді - 193.20.0.0/14.

Якщо клієнту цього постачальника послуг потрібно зовсім небагато адрес, наприклад 13, то постачальник міг би запропонувати йому різні варіанти: мережа 193.20.30.0/28, мережа 193.20.30.16/28 або мережа 193.21.204.48/28. У всіх випадках у розпорядженні клієнта для нумерації вузлів є 4 молодші біти. Таким чином, якнайменше число, що задовольняє потребам клієнта (13), яке можна представити степеню двійки, є 16 (24). Префікс для кожного з пулів в усіх цих випадках виконує роль номера мережі, він має довжину 32 - 4 = 28 розрядів.

Розглянемо інший варіант: необхідний блок адрес в 4000 вузлів. Для нумерації такої кількості вузлів потрібно 12 двійкових розрядів, отже, розмір виділеного пулу адрес буде дещо більше що вимагається - 4096. Межа, з якою повинна починатися виділювана ділянка повинна бути кратна розміру ділянки, тобто це можуть бути будь-які адреси з наступних: 193.20.0.0, 193.20.16.0, 193.20.32.0, 193.20.48.0 і інші числа, що закінчуються на 12 нулів. Нехай постачальник послуг запропонував споживачу діапазон адрес 193.20.16.0 - 193.20.31.255. Для цього діапазону сумарний номер мережі (префікс) має довжину 20 двійкових розрядів і дорівнює 193.20.16.0/20.

Таким чином, завдяки технології CIDR постачальник послуг має можливість «нарізати» безперервні блоки адрес з виділеного йому адресного простору відповідно до дійсних вимог кожного клієнта.

При використанні технології CIDR маршрутизація на магістральному рівні може реалізовуватися на основі узагальненого мережевого префікса. Результатом є підсумовування маршрутних записів, зменшення розміру таблиць маршрутних записів і збільшення швидкості обробки пакетів.

З рисунку видно, що маршрутизатор R2 містить у своїй таблиці маршрутизації тільки один запис для всіх мереж, що мають префікс В, а маршрутизатор R4 містить в своїй таблиці маршрутизації тільки один запис для всіх мереж з префіксом А (якщо В1 - 172.16.0.0/16, В2 - 172.17.0.0/16, В3 - 172.18.0.0/16, В4 - 172.19.0.0/16, то В - 172.16.0.0/14). Відзначимо, що в маршрутизаторі R1 підсумовування даних маршрутів не здійснюється, оскільки він є граничним і в його таблиці мережа, що починається на B1, позначена як безпосередньо підключена.

Таким чином, за своєю суттю технологія CIDR споріднена VLSM. Тільки якщо у випадку з VLSM є можливість рекурсивного розподілу на підмережі, невидимі ззовні, то CIDR дозволяє рекурсивно адресувати цілі адресні блоки.

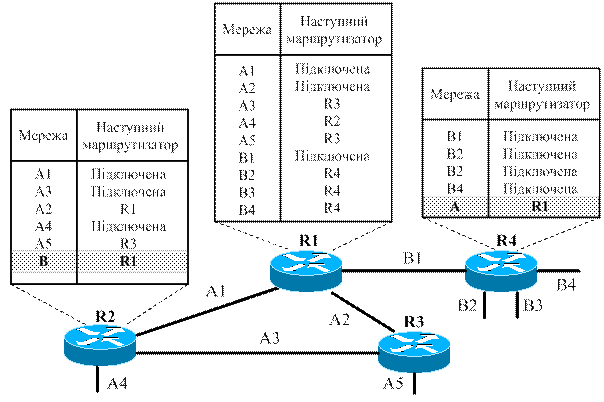


Рисунок – Приклад підсумовування маршрутів

Використання CIDR дозволяє розділяти великі мережі (у тому числі і Інтернет) на адресні домени, усередині яких передається інформація виключно про внутрішні мережі. Поза доменом використовується тільки загальний префікс мережі. В результаті багатьом мережам відповідає один запис в таблиці маршрутизації.

**Протокол RIP**

**Routing Information Protocol**, **RIP** — один із найрозповсюдженіших [протоколів](https://uk.wikipedia.org/wiki/Мережевий_протокол) [маршрутизації](https://uk.wikipedia.org/wiki/Маршрутизація) в невеликих [комп'ютерних мережах](https://uk.wikipedia.org/wiki/Комп'ютерна_мережа), який дозволяє [маршрутизаторам](https://uk.wikipedia.org/wiki/Маршрутизатор)динамічно оновлювати маршрутну інформацію (напрямок і дальність в [хопах](https://uk.wikipedia.org/wiki/Хоп_(процес))), отримуючи її від сусідніх маршрутизаторів.

RIP — так званий [дистанційно-векторний протокол](https://uk.wikipedia.org/w/index.php?title=Дистанційно-векторний_протокол&action=edit&redlink=1), який оперує [*хопами*](https://uk.wikipedia.org/wiki/Хоп_(процес)) як [метрикою маршрутизації](https://uk.wikipedia.org/wiki/Метрика). Максимальна кількість [хопів](https://uk.wikipedia.org/wiki/Хоп_(процес)), дозволений RIP — 15 (метрика 16 означає «нескінченно велику метрику», тобто недосяжний сегмент мережі). Кожен RIP-маршрутизатор за замовчуванням сповіщає в мережу свою повну таблицю маршрутизації раз на 30 секунд, генеруючи досить багато [трафіку](https://uk.wikipedia.org/wiki/Трафік) на низькошвидкісних лініях зв'язку. RIP працює на мережевому рівні стека [TCP/IP](https://uk.wikipedia.org/wiki/TCP/IP), використовуючи [UDP](https://uk.wikipedia.org/wiki/UDP) [порт 520](https://uk.wikipedia.org/w/index.php?title=Порт_520&action=edit&redlink=1).

У сучасних мережних середовищах RIP — не найкраще рішення для вибору як протоколу маршрутизації, тому що його можливості поступаються сучаснішим протоколам, таким як [EIGRP](https://uk.wikipedia.org/wiki/EIGRP), [OSPF](https://uk.wikipedia.org/wiki/OSPF). Обмеження в 15 хопів не дає застосовувати його у великих мережах. Перевага цього протоколу — простота конфігурування. Внаслідок простоти його підтримують практично всі маршрутизатори початкового рівня.

### Формат RIP пакету

0 1 2 3

0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| command (1) | version (1) | must be zero (2) |

+---------------+---------------+-------------------------------+

| |

~ RIP Entry (20) ~

| |

+---------------+---------------+---------------+---------------+

command — Команда, визначає призначення датаграми (1 — request; 2 — response)

version — Номер версії, залежно від версії, визначається формат пакета

must be zero — повинно бути нулем;

RIP Entry — (RTE) Запис маршрутної інформації RIP. RIP пакет може містити від 1 до 25 записів RIP Entry.

**Протокол OSPF**

**OSPF**([англ.](https://uk.wikipedia.org/wiki/Англійська_мова) *Open Shortest Path First*) — протокол динамічної [маршрутизації](https://uk.wikipedia.org/wiki/Маршрутизація), заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху [Алгоритм Дейкстри](https://uk.wikipedia.org/wiki/Алгоритм_Дейкстри) (Dijkstra's algorithm).

Протокол OSPF був розроблений [IETF](https://uk.wikipedia.org/wiki/IETF) в [1988](https://uk.wikipedia.org/wiki/1988) році. Остання версія протоколу представлена в [RFC 2328](https://tools.ietf.org/html/rfc2328). Протокол OSPF являє собою протокол внутрішнього шлюзу (Interior Gateway Protocol — IGP). Протокол OSPF поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи.

Властивості OSPF:

* Висока швидкість збіжності
* Підтримка мережних масок змінної довжини [VLSM](https://uk.wikipedia.org/wiki/VLSM)
* Відсутність обмежень досяжності
* Оптимальне використання пропускної здатності мережі
* Оптимальний вибір шляху маршрутизації

Згідно з [RFC](https://uk.wikipedia.org/wiki/RFC) 2328 є незапатентований тобто відкритий для громадськості протокол, таким же, як є протокол [RIP](https://uk.wikipedia.org/wiki/RIP). Але OSPF на відміну від RIP, має значно більшу швидкість збіжності (рекалькуляції таблиці маршрутизації), немає обмеження на довжину шляху 15-ма *хопами* (англ. *hop*, укр. *стрибок*), враховує пропускну здатність мережі при виборі маршруту. Все це робить OSPF потужним, масштабованим протоколом маршрутизації.

**Опис роботи протоколу**

1. Маршрутизатори обмінюються hello-пакетами через всі інтерфейси, на яких активований OSPF. Маршрутизатори, що розділяють загальний канал передачі даних, стають сусідами, коли вони приходять до домовленості при певних параметрах, зазначених в їх hello-пакетах.
2. На наступному етапі роботи протоколу маршрутизатори будуть намагатися перейти в стан суміжності зі своїми сусідами. Перехід у стан суміжності визначається типом маршрутизаторів, які обмінюються hello-пакетами, і типом мережі, по якій передаються hello-пакети. OSPF визначає кілька типів мереж і кілька типів маршрутизаторів. Пара маршрутизаторів, що знаходяться в стані суміжності, синхронізує між собою базу даних стану каналів.
3. Кожен маршрутизатор посилає оголошення про стан каналу маршрутизаторам, з якими він знаходиться в стані суміжності.
4. Кожен маршрутизатор, який отримав оголошення від суміжного маршрутизатора, записує передану в ньому інформацію в базу даних стану каналів маршрутизатора і розсилає копію оголошення всім іншим суміжним з ним маршрутизаторам.
5. Розсилаючи оголошення всередині однієї OSPF-зони, всі маршрутизатори будують ідентичну базу даних стану каналів маршрутизатора.
6. Коли база даних побудована, кожен маршрутизатор використовує алгоритм «найкоротший шлях першим» для обчислення графа без петель, який буде описувати найкоротший шлях до кожного відомого пункту призначення із собою як кореня. Цей граф - дерево найкоротших шляхів.
7. Кожен маршрутизатор будує таблицю маршрутизації зі свого дерева найкоротших шляхів.

**Маршрутизація в неоднорідних мережах**

В одній і тій же мережі можуть одночасно працювати кілька різних протоколів маршрутизації. Це означає, що на деяких (не обов'язково всіх) маршрутизаторах мережі встановлено і функціонує кілька протоколів маршрутизації, але при цьому через мережу взаємодіють тільки однойменні протоколи.

У маршрутизаторі при роботі декількох протоколів маршрутизації кожен запис в таблиці є результатом роботи одного з цих протоколів. Якщо інформація про деяку мережі з'являється від декількох протоколів, то для однозначності вибору маршруту встановлюються пріоритети протоколів. У деяких ОС при виведенні на екран таблиці маршрутизації навпаки кожного запису є відмітка, від якого протоколу надійшли відомості. Однак навіть якщо така відмітка на екран не виводиться, вона обов'язково там є.

За замовчуванням кожен протокол маршрутизації поширює тільки власну інформацію, тобто ту інформацію, яка була отримана даним маршрутизатором з даного протоколу. Наприклад, якщо про маршрут до деякої мережі маршрутизатор дізнався по протоколу RIP, то і розсилати по мережі оголошення про цей маршрут він буде за допомогою протоколу RIP. При такому «виборчому» режимі можуть створюватися області взаємної недосяжності в складових мережах. Завдання маршрутизації буде вирішуватися ефективніше при використанні такого режиму роботи маршрутизаторів, в якому вони б могли обмінюватися маршрутною інформацією, отриманою різними протоколами. Такий режим називається перерозподілом. Для реалізації такого режиму навіть в межах невеликої складовою мережі адміністратору потрібно провести певну роботу з налаштування кожного маршрутизатора.

Очевидно, що для великих складових мереж потрібно якісно інше рішення. Таке рішення було знайдено для найбільшої складовою мережі, і воно грунтується на понятті автономної системи.

Автономна система (Autonomous System, AS) або Домен маршрутизації - це сукупність мереж під єдиним адміністративним керуванням, що забезпечує загальну політику маршрутизації для всіх вхідних в неї маршрутизаторів.

Зазвичай автономною системою керує один постачальник послуг Інтернету, самостійно обираючи, які протоколи маршрутизації повинні використовуватися в деякій автономній системі, і яким чином має виконуватися перерозподіл маршрутної інформації. Реєстрація автономних систем відбувається централізовано, також як реєстрація IP-адрес, і здійснюється тими ж організаціями. Відповідно до цієї концепції Інтернет виглядає як набір автономних систем, з'єднаних зовнішніми шлюзами.

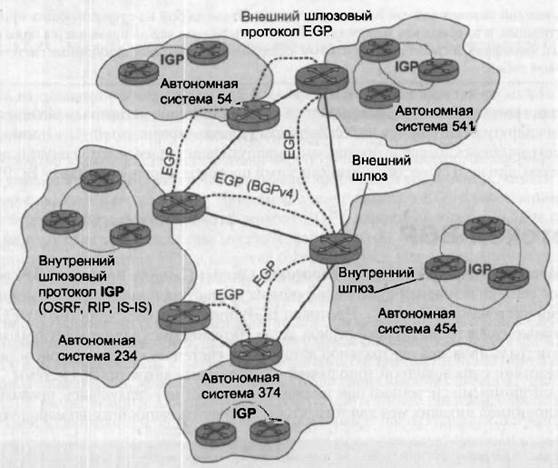


Рисунок -Мережа, складена з декількох автономних систем

Кожна автономна система характеризується своїм номером. Передбачена 16-разрадная нумерація автономних систем, їх теоретичне максимальну кількість 216 = 65 536. Номер автономної системи ніяк не пов'язаний з IP-адресами входять до неї мереж.

Основна мета поділу мережі Інтернет на автономні системи - забезпечення багаторівневого підходу до маршрутизації. До введення автономних систем передбачався дворівневий підхід, тобто спочатку маршрут визначався як послідовність мереж, а потім вів безпосередньо до заданого вузла в кінцевій мережі. З появою автономних систем з'являється третій, верхній рівень маршрутизації - послідовність автономних систем.

За маршрутизацію всередині автономної системи відповідають внутрішні шлюзові протоколи (Interior Gateway Protocols, IGP). До їх числа відносяться протоколи RIP, OSPF, IS-IS і ін. В разі транзитної автономної системи ці протоколи вказують послідовність маршрутизаторів від точки входу в автономну систему до точки виходу з неї.

Вибір маршруту між автономними системами здійснюють зовнішні шлюзи, які використовують особливий тип протоколу маршрутизації - зовнішній шлюзовий протокол (Exterior Gateway Protocol, EGP). В даний час для роботи в такій ролі в мережі Інтернет затверджений стандартний прикордонний шлюзовий протокол - BGP (Border Gateway Protocol). В якості адреси наступного маршрутизатора в протоколі BGP вказується адреса точки входу в сусідню автономну систему.

Усередині кожної автономної системи може застосовуватися будь-який з існуючих протоколів маршрутизації, в той час як між автономними системами завжди застосовується один і той же протокол, на якому автономні системи «спілкуються між собою».

**Протокол BGP**

BGP є [протоколом міждоменної маршрутизації](https://uk.wikipedia.org/w/index.php?title=Протоколи_міждоменної_маршрутизації&action=edit&redlink=1) та належить до класу [дистанційно-векторних протоколів](https://uk.wikipedia.org/w/index.php?title=Дистанційно-векторні_протоколи&action=edit&redlink=1). Як протокол міждоменної маршрутизації використовується усіма [інтернет-провайдерами](https://uk.wikipedia.org/wiki/Інтернет-провайдер), а також великими компаніями та організаціями, які мають власні публічні [номери автономних систем (ASN)](https://uk.wikipedia.org/wiki/Автономна_система_(Інтернет)" \l "ASN) та користуються послугами більш ніж одного інтернет-провайдера ([мултіхомінг](https://uk.wikipedia.org/w/index.php?title=Мултіхомінг&action=edit&redlink=1)) або мають прямі [IP](https://uk.wikipedia.org/wiki/IP)-з'єднання з багатьма іншими великими компаніям, що також мають власні публічні номери автономних систем, без використання послуг інтернет-провайдерів.

Разом з тим немає ніяких обмежень на використання BGP в [локальних мережах](https://uk.wikipedia.org/wiki/Локальна_мережа) крім рекомендацій про приватні ASN (64512-65534), але використання BGP як [протоколу внутрішньодоменної маршрутизації](https://uk.wikipedia.org/w/index.php?title=Протоколи_внутрішньодоменної_маршрутизації&action=edit&redlink=1) є недоцільним через значний час [конвергенції (збіжності)](https://uk.wikipedia.org/w/index.php?title=Конвергенція_(маршрутизація)&action=edit&redlink=1) у порівнянні з іншими протоколами маршрутизації, що закладено в його дизайні.

На відміну від класичного дистанційно-векторного протоколу [RIP](https://uk.wikipedia.org/wiki/RIP), метрикою якого є кількість [хопів](https://uk.wikipedia.org/wiki/Хоп_(процес)) (відрізків шляху) між маршрутизаторами, найкращий маршрут BGP [обирається](https://uk.wikipedia.org/wiki/BGP" \l ".D0.90.D0.BB.D0.B3.D0.BE.D1.80.D0.B8.D1.82.D0.BC_.D0.B2.D0.B8.D0.B1.D0.BE.D1.80.D1.83_.D0.BC.D0.B0.D1.80.D1.88.D1.80.D1.83.D1.82.D1.83) по точно визначеному пріоритету [атрибутів](https://uk.wikipedia.org/wiki/BGP" \l "BGP-.D0.B0.D1.82.D1.80.D0.B8.D0.B1.D1.83.D1.82.D0.B8), одним із яких, але не найпріоритетнішим, є кількість хопів між автономними системами — *найкоротший шлях між автономними системами* ([англ.](https://uk.wikipedia.org/wiki/Англійська_мова) *shortest AS path*). Тому іноді цей протокол зараховують до окремого класу [шляхо-векторних протоколів](https://uk.wikipedia.org/w/index.php?title=Шляхо-векторні_протоколи&action=edit&redlink=1)

Алгоритм вибору маршруту:

1. Перевага надається маршруту з найбільшим значенням параметра (атрибута) WEIGHT (*Вага*). Застосовується лише на маршрутизаторах [Cisco](https://uk.wikipedia.org/wiki/Cisco).
2. Маршрут, що має найбільше значення атрибуту LOCAL\_PREF (*Локальна Перевага*), за замовченням цей атрибут має значення 100.
3. Маршрутизатори [Cisco](https://uk.wikipedia.org/wiki/Cisco) надають перевагу своїм власним маршрутам над маршрутами отриманими від BGP-сусідів. Маршрутизатори інших виробників можуть ігнорувати цей крок, або мати свої власні правила.
4. Надання переваги найкоротшому шляху до конкретної IP-мережі на основі атрибуту AS\_PATH (*Шлях по*[*автономних системах*](https://uk.wikipedia.org/wiki/Автономна_система_(Інтернет))). Тобто найкращим маршрутом є той до якого веде шлях через мінімальну кількість [автономних систем](https://uk.wikipedia.org/wiki/Автономна_система_(Інтернет))
5. Вибір на основі атрибуту ORIGIN (*Джерело*). Якщо [IP-префікс](https://uk.wikipedia.org/wiki/CIDR) якоїсь мережі спочатку був отриманий BGP із [протоколу внутрішньодоменної маршрутизації](https://uk.wikipedia.org/w/index.php?title=Протоколи_внутрішньодоменної_маршрутизації&action=edit&redlink=1)[[en]](https://en.wikipedia.org/wiki/Interior_gateway_protocol) тоді маршрут, що веде до цієї мережі, є пріоритетнішим, ніж маршрути, які отримали [IP-префікс](https://uk.wikipedia.org/wiki/CIDR) цієї мережі з [EGP](https://uk.wikipedia.org/wiki/EGP) (протокол наразі не використовується) або джерело отримання невідоме.
6. Надання переваги маршруту з найменшим значенням атрибута MED (*multi-exit discriminator, дискримінатор мульти-виходу*)
7. Перевага маршруту, отриманому через eBGP (*Exterior, Зовнішній BGP*) над iBGP (*Interior, Внутрішній BGP*) тобто маршрут отриманий від BGP-сусіда з іншої автономної системи має перевагу над маршрутом отриманим від BGP-сусіда тієї ж самої AS.
8. Обирається маршрут, який отриманий від ближчого BGP-сусіда. Ближчим сусідом є той до якого є найменшою відстань в таблиці маршрутизації сформованій на основі прямих з'єднань, [статичних маршрутів](https://uk.wikipedia.org/w/index.php?title=Статична_маршрутизація&action=edit&redlink=1) та протоколів внутрішньодоменної маршрутизації (*IGP*).
9. Цей пункт виконується, коли ми використовуємо [Багатошляховий](https://uk.wikipedia.org/w/index.php?title=Багатошляхова_маршрутизація&action=edit&redlink=1) (*Мultipath*) BGP, тобто коли для цілей [балансування навантаження](https://uk.wikipedia.org/w/index.php?title=Балансування_навантаження&action=edit&redlink=1) використовується окрім найкращого один чи більше додаткових маршрутів до конкретної IP-мережі. Якщо претендент на найкращий маршрут має такі ж самі характеристик згідно з попередніми пунктами, як і раніше обраний, то він не стає новим найкращим, але може бути обраним, як додатковий. Маршрутизатори CISCO можуть мати до 6 BGP-маршрутів до конкретної IP-мережі.
10. Маршрут отриманий першим має пріоритет.
11. Перевага маршруту, що отриманий від BGP сусіда з найменшим значенням його [ідентифікатора](https://uk.wikipedia.org/wiki/Ідентифікатор) (*Router ID*)
12. Цей пункт виконується лише при використанні багатошляхової маршрутизації. Надається перевага маршруту, що проходить через мінімальну довжину кластерного списку.
13. Перевага маршруту, отриманому від сусіда з найменшою IP-адресою інтерфейсу.

**Протокол ICMP**

**ICMP** ([англ.](https://uk.wikipedia.org/wiki/Англійська_мова) Internet Control Message Protocol — міжмережевий протокол керуючих повідомлень) — [мережевий протокол](https://uk.wikipedia.org/wiki/Мережевий_протокол), що входить в [стек протоколів TCP/IP](https://uk.wikipedia.org/wiki/Стек_протоколів_TCP/IP). В основному ICMP використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних. Також на ICMP покладаються деякі сервісні функції, зокрема на основі цього протоколу заснована дія таких загальновідомих утиліт як [ping](https://uk.wikipedia.org/wiki/Ping) та [traceroute](https://uk.wikipedia.org/w/index.php?title=Traceroute&action=edit&redlink=1).

Протокол ICMP описаний в [RFC 792](https://tools.ietf.org/html/rfc792) (з доповненнями в [RFC 950](https://tools.ietf.org/html/rfc950)) і є стандартом Інтернету (входить в стандарт STD 5 разом з протоколом [IP](https://uk.wikipedia.org/wiki/IP)). Хоча формально ICMP використовує [IP](https://uk.wikipedia.org/wiki/IP) (ICMP пакети [інкапсулюються](https://uk.wikipedia.org/wiki/Інкапсуляція) в [IP](https://uk.wikipedia.org/wiki/IP) пакети), він є невід'ємною частиною [IP](https://uk.wikipedia.org/wiki/IP) й обов'язковий при реалізації [стека TCP/IP](https://uk.wikipedia.org/wiki/Стек_протоколів_TCP/IP). Поточна версія ICMP для [IPv4](https://uk.wikipedia.org/wiki/IPv4) називається ICMPv4. В [IPv6](https://uk.wikipedia.org/wiki/IPv6) існує аналогічний протокол [ICMPv6](https://uk.wikipedia.org/wiki/ICMPv6).

Протокол ICMP не є протоколом орієнтованим на з'єднання (як наприклад [TCP](https://uk.wikipedia.org/wiki/TCP)), тобто при втраті пакету ICMP не буде робити ніяких спроб по його відновленню. ICMP повідомлення (тип 12) генеруються при знаходженні помилок у заголовку [IP](https://uk.wikipedia.org/wiki/IP) пакета (за винятком самих ICMP пакетів, щоб не призвести до нескінченно зростаючого потоку ICMP повідомлень про ICMP повідомлення).

ICMP повідомлення (тип 3) генеруються [маршрутизатором](https://uk.wikipedia.org/wiki/Маршрутизатор) при відсутності маршруту до адресата.

Типи ICMP пакетів:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **Тип** | **Код** | **Назва** | **Запит** | **Помилка** |
| 0 | 0 | Ехо-відповідь | х |  |
| 1 та 2 |  | Зарезервовано |  |  |
| 3 | 0 | Мережа недоступна |  | х |
| 3 | 1 | Хост недоступний |  | х |
| 3 | 2 | Протокол недоступний |  | х |
| 3 | 3 | Порт недоступний |  | х |
| 3 | 4 | Потрібна [фрагментація](https://uk.wikipedia.org/wiki/Фрагментація_(інформаційні_технології)), але DF (прапорець «не фрагментувати») встановлено |  | х |
| 3 | 5 | Маршрутування джерелом не вдалося |  | х |
| 3 | 6 | Мережа призначення невідома |  | х |
| 3 | 7 | Хост призначення невідомий |  | х |
| 3 | 8 | Хост призначення ізольовано (застарів) |  | х |
| 3 | 9 | Мережа призначення адміністративно заборонена |  | х |
| 3 | 10 | Хост призначення адміністративно заборонено |  | х |
| 3 | 11 | Мережа недоступна для TOS |  | х |
| 3 | 12 | Хост недоступний для TOS |  | х |
| 3 | 13 | Зв'язок адміністративно заборонено (фільтрування запобігає маршрутуванню) |  | х |
| 3 | 14 | Порушення передування хосту (бажане передування не дозволено для комбінації хоста або мережі та порту) |  | х |
| 3 | 15 | Порушення передування в дії (передування датаграми нижче рівня встановленого адміністраторами) |  | х |
| 4 | 0 | Вгамовування джерела (управління заторами) |  |  |
| 5 | 0 | Переадресація для мережі |  |  |
| 5 | 1 | Переадресація для хосту |  |  |
| 5 | 2 | Переадресація для TOS та мережі |  |  |
| 5 | 3 | Переадресація для TOS та хосту |  |  |
| 6 |  | Змінна адреса хосту |  |  |
| 7 |  | Зарезервовано |  |  |
| 8 | 0 | Ехо-запит | х |  |
| 9 | 0 | Оголошення маршрутизатора |  |  |
| 10 | 0 | Клопотання маршрутизації |  |  |
| 11 | 0 | Час життя пакету став рівний 0 під час транзиту |  | х |
| 11 | 1 | Час збірки фрагментів пакету закінчився |  | х |
| 12 | 0 | Помилка заголовку IP-пакету |  | х |
| 12 | 1 | Відсутня необхідна опція заголовку |  | х |
| 12 | 2 | Погана довжина заголовку |  | х |
| 13 | 0 | Запит мітки часу | х |  |
| 14 | 0 | Мітка часу | х |  |
| 15 | 0 | Запит інформації | х |  |
| 16 | 0 | Відповідь інформацією | х |  |
| 17 | 0 | Запит маски адреси | х |  |
| 18 | 0 | Маска адреси | х |  |

**Правила генерації ICMP-пакетів:**

1 .При втраті ICMP-пакета ніколи не генерується новий.

2. ICMP-пакети ніколи не генеруються у відповідь на IP-пакети з широкомовною або груповою адресою, щоб не викликати перевантаження в мережі (так званий «широкомовний шторм»).

3. При пошкодженні фрагментированного IP-пакета ICMP-повідомлення відправляється тільки після отримання першого пошкодженого фрагмента, оскільки відправник все одно повторить передачу всього IP-пакета цілком.

**Утиліти tracerout, ping.**

**Traceroute** - це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP / IP. Traceroute може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери з встановленою операційною системою Windows використовують ICMP-протокол, при цьому операційні системи Linux і маршрутизатори Cisco - протокол UDP.

Traceroute входить в поставку більшості сучасних мережевих операційних систем. У системах Microsoft Windows ця програма носить назву tracert, а в системах GNU / Linux, Cisco IOS і Mac OS - traceroute.

Розглянемо приклад роботи програми в операційній системі Windows. Програма tracert виконує відправку даних вказаному вузлу мережі, при цьому відображаючи відомості про всіх проміжних маршрутизаторах, через які пройшли дані на шляху до цільового вузла. У разі проблем при доставці даних до будь-якого вузла програма дозволяє визначити, на якій саме ділянці мережі виникли неполадки. Необхідно відзначити, що програма працює тільки в напрямку від джерела пакетів і є вельми грубим інструментом для виявлення неполадок в мережі. В силу особливостей роботи протоколів маршрутизації в мережі Інтернет, зворотні маршрути часто не збігаються з прямими, причому це справедливо для всіх проміжних вузлів в Трейсі. Тому ICMP відповідь від кожного проміжного вузла може йти своїм власним маршрутом, загубитися або прийти з великою затримкою, хоча в реальності з пакетами, які адресовані кінцевому вузлу, цього не відбувається. Крім того, на проміжних маршрутизаторах часто стоїть обмеження числа відповідей ICMP в одиницю часу, що призводить до появи помилкових втрат.

Принцип роботи traceroute:

Для визначення проміжних маршрутизаторів traceroute відправляє цільового вузла серію ICMP-пакетів (за замовчуванням 3 пакети), з кожним кроком збільшуючи значення поля TTL ( «час життя») на 1. Це поле зазвичай вказує максимальну кількість маршрутизаторів, яке може бути пройдено пакетом. Перша серія пакетів відправляється з TTL, рівним 1, і тому перший же маршрутизатор повертає назад ICMP-повідомлення «time exceeded in transit», яке вказує на неможливість доставки даних. Traceroute фіксує адресу маршрутизатора, а також час між відправленням пакета і отриманням відповіді (ці відомості виводяться на монітор комп'ютера). Потім traceroute повторює відправку серії пакетів, але вже з TTL, рівним 2, що змушує перший маршрутизатор зменшити TTL пакетів на одиницю і направити їх до другого маршрутизатора. Другий маршрутизатор, отримавши пакети з TTL = 1, так само повертає «time exceeded in transit».

Процес повторюється до тих пір, поки пакет не досягне цільового вузла. При отриманні відповіді від цього вузла процес трасування вважається завершеним.

На крайовому хості IP-датаграмма з TTL = 1 цієї статті не відкидається і не викликає ICMP-повідомлення типу термін закінчився, а повинна бути віддана додатком. Досягнення пункту призначення визначається наступним чином: відсилаються traceroute датаграми містять UDP-пакет зі свідомо невживаних номером порту на адресується хості. Номер порту буде дорівнює 33434 + (максимальна кількість транзитних ділянок до вузла) - 1. В пункті призначення UDP-модуль, отримуючи подібні датаграми, повертає ICMP-повідомлення про помилку «порт недоступний». Таким чином, щоб дізнатися про завершення роботи, програмою traceroute досить виявити, що надійшло ICMP-повідомлення про помилку цього типу.

**Пінг** ( Packet Inter-Network Groper*, PING*)— службова [комп'ютерна програма](https://uk.wikipedia.org/wiki/Комп'ютерна_програма), призначена для перевірки з'єднань в [мережах](https://uk.wikipedia.org/wiki/Комунікаційна_мережа) на основі [TCP/IP](https://uk.wikipedia.org/wiki/TCP/IP).

Вона відправляє запити (*Echo-Request*) [протоколу](https://uk.wikipedia.org/wiki/Мережевий_протокол) [ICMP](https://uk.wikipedia.org/wiki/ICMP) зазначеному вузлу мережі й фіксує відповіді ([англ.](https://uk.wikipedia.org/wiki/Англійська_мова) *Echo-Reply*). Час між відправленням запиту й одержанням відповіді (RTT- *Round Trip Time*) дозволяє визначати двосторонні затримки у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

Повна відсутність ICMP-відповідей може також означати, що віддалений вузол (або якийсь із проміжних [маршрутизаторів](https://uk.wikipedia.org/wiki/Маршрутизатор)) блокує ICMP Echo-Reply або ігнорує ICMP Echo-Request.

Програма ping є одним з основних діагностичних засобів у мережах TCP/IP і входить у поставку всіх сучасних [мережевих операційних систем](https://uk.wikipedia.org/wiki/Мережева_операційна_система). Функціональність ping також реалізована в деяких вбудованих [операційних системах](https://uk.wikipedia.org/wiki/Операційна_система) маршрутизаторів, доступ до результатів виконання ping для таких пристроїв за протоколом [SNMP](https://uk.wikipedia.org/wiki/SNMP) визначається стандартами.

Практичне застосування

* можна дізнатися [IP-адресу](https://uk.wikipedia.org/wiki/IP-адреса) по [доменному імені](https://uk.wikipedia.org/wiki/Доменне_ім'я);
* можна перевірити, чи є зв'язок з віддаленим вузлом;
* можна визначити, чи є на поточному комп'ютері проблеми з налаштуванням [DNS](https://uk.wikipedia.org/wiki/Доменна_система_імен), задавши ping спочатку доменне ім'я, а потім IP-адресу;
* можна перевірити якість каналу, подивившись, скільки пакетів не дійшло або час відклику. Ця можливість часто використовується в мережевих [багатокористувацьких іграх](https://uk.wikipedia.org/wiki/Багатокористувацька_гра), оскільки якість зв'язку дуже важлива для них. Ігровий [сервер](https://uk.wikipedia.org/wiki/Сервер) вимірює час, за який необхідний для гри пакет досягне [клієнта](https://uk.wikipedia.org/wiki/Клієнт_(інформатика)) і відповідь буде отримана. Цей час прийому-передачі, як правило, називають ping гравця. Проте це не завжди можна вважати показником, оскільки в деяких мережах протокол ICMP може блокуватися.