Лабораторна робота №2

Тема: Складання карти мережі Інтернет

Мета роботи: навчитись перевіряти підключення до мережі за допомогою ехо-запиту з використанням команди ping; навчитись відстежувати маршрути до віддалених серверів за допомогою утиліти Windows «Traceroute», а також спеціалізованих програмних і веб-засобів.

Теоретичні відомості

Об'єднані мережі

Сучасні мережі безперервно удосконалюються для задоволення потреб користувачів. Раніше мережі передачі даних обмежувалися символьно-орієнтованим обміном інформацією між підключеними комп'ютерними системами. Традиційні телефонні, радіо- і телевізійні мережі були реалізовані окремо від мереж передачі даних. У минулому кожен з цих сервісів використовував виділені мережеві ресурси з різними каналами зв'язку і різними технологіями для передачі певного сигналу зв'язку. Кожен сервіс мав власний набір правил і стандартів, що забезпечували успішний зв'язок.

Розглянемо навчальний корпус, побудований 40 років тому. В аудиторії були прокладені кабелі для передачі даних, телефонної мережі і телебачення. Ці окремі мережі були розрізнені, це означає, що вони не могли взаємодіяти одна з одною, як показано на рис. 2.1.

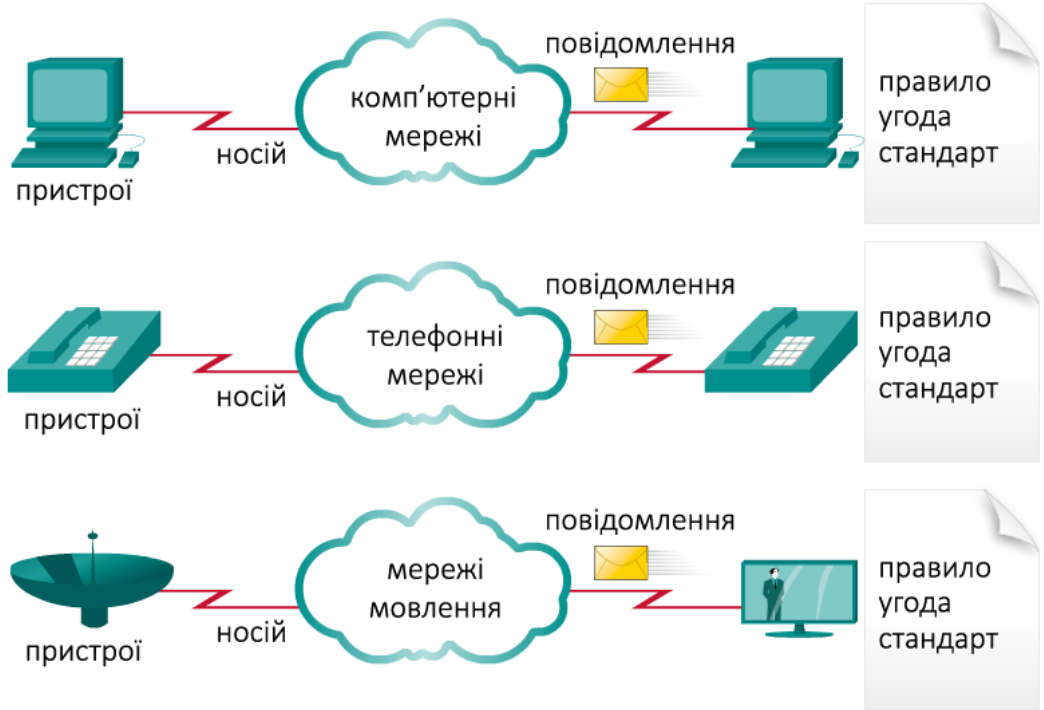

Рис. 2.1. Кожен сервіс реалізовано в окремій мережі

Розвиток технологій дозволяє нам об'єднати ці різні типи мереж в єдину платформу, далі іменовану «об'єднана мережа». На відміну від виділених мереж об'єднані мережі можуть передавати голос, потокове відео, текст і графічні зображення між великою кількістю різних типів пристроїв по одному і тому ж каналу зв'язку і структурі мережі, як показано на рис. 2.2. Форми обміну інформацією, які сформувались раніше, змогли об'єднатись на базі спільної платформи. Ця платформа надає доступ до широкого діапазону альтернативних і нових способів комунікації, які дозволяють співробітникам взаємодіяти безпосередньо один з одним практично миттєво.

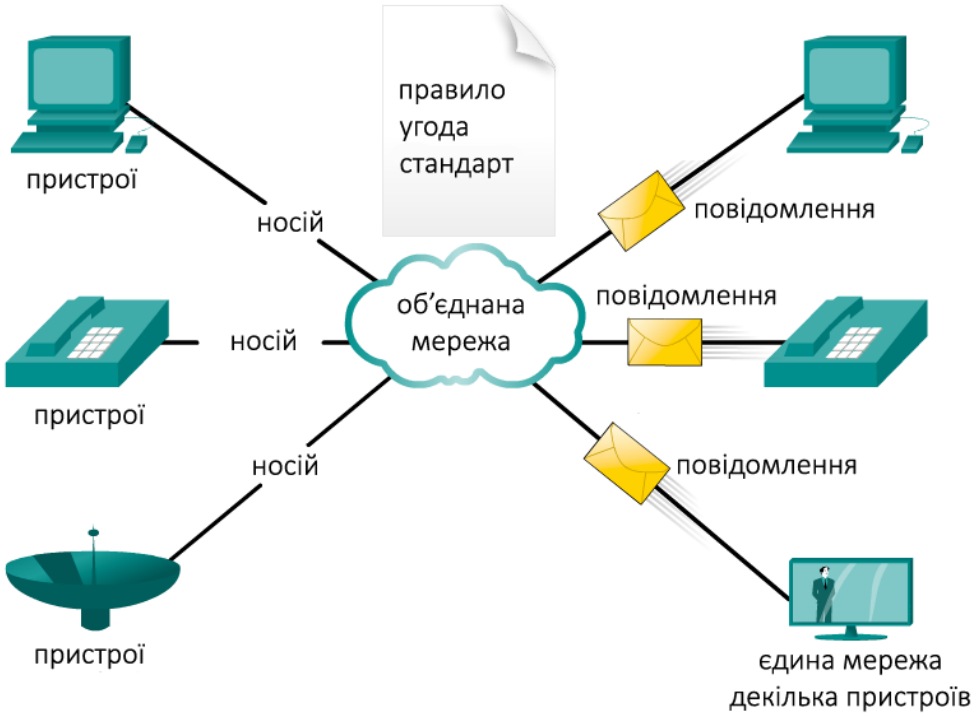

Рис. 2.2. Об'єднані мережі передачі даних забезпечують функціонування декількох сервісів в одній мережі

У об'єднаній мережі як і раніше існує багато контактних точок і багато спеціалізованих пристроїв, таких як персональні комп'ютери, телефони, телевізори і планшетні комп'ютери, але є загальна мережева інфраструктура. Мережева інфраструктура використовує один і той же набір правил, угоди і стандарти реалізації.

Допоміжна архітектура мережі

Мережі повинні підтримувати широкий набір додатків і сервісів, а також велику кількість типів кабелів і пристроїв, з яких складається фізична інфраструктура. Термін «мережева архітектура» в цьому контексті відноситься до технологій, які підтримують інфраструктуру, а також до запрограмованих сервісів і правил або протоколів, які переміщують повідомлення в мережі.

З розвитком мереж стає очевидним, що для задоволення потреб користувачів архітектури повинні відповідати чотирьом основним вимогам.

- стійкість до збоїв (рис. 2.3);
- масштабованість (рис. 2.4);
- якість обслуговування (QoS) (рис. 2.5);
- безпека (рис. 2.6).

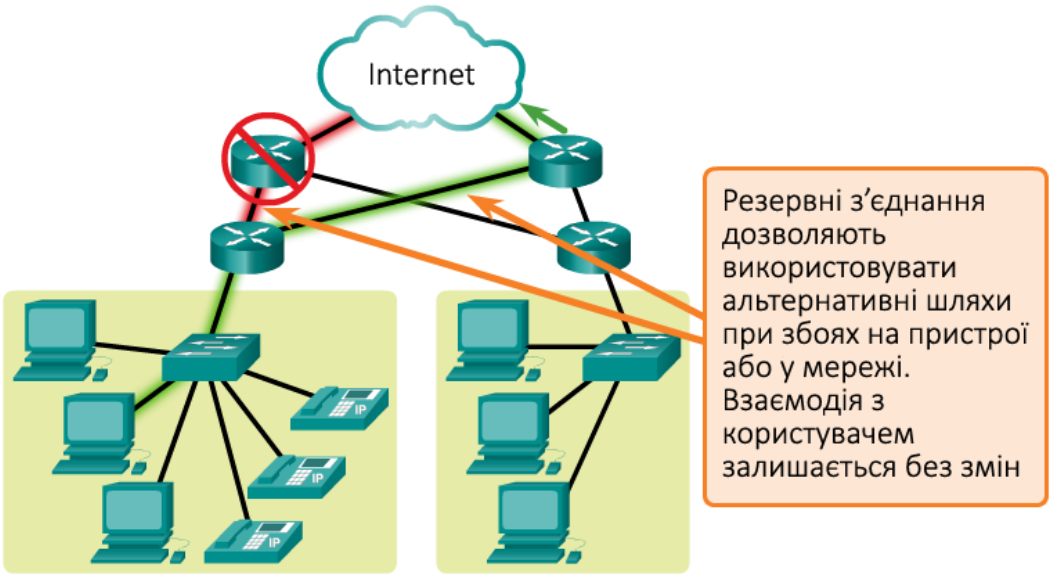

Рис. 2.3. Стійкість до збоїв

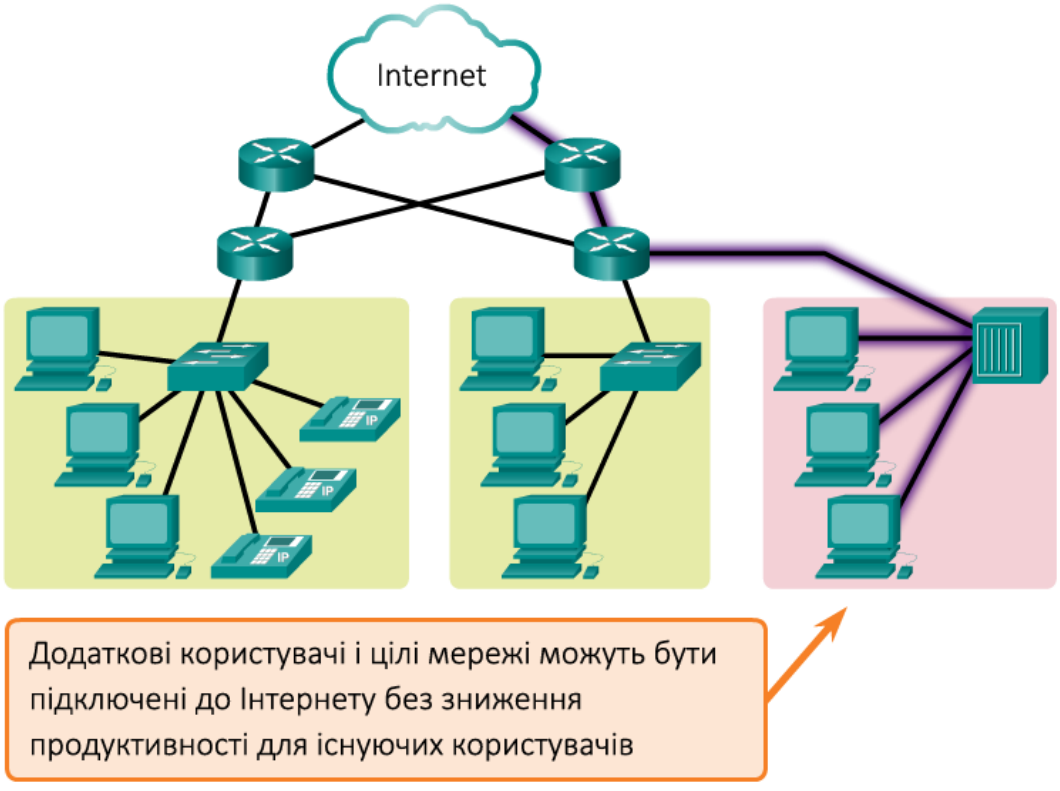

Рис. 2.4. Масштабованість

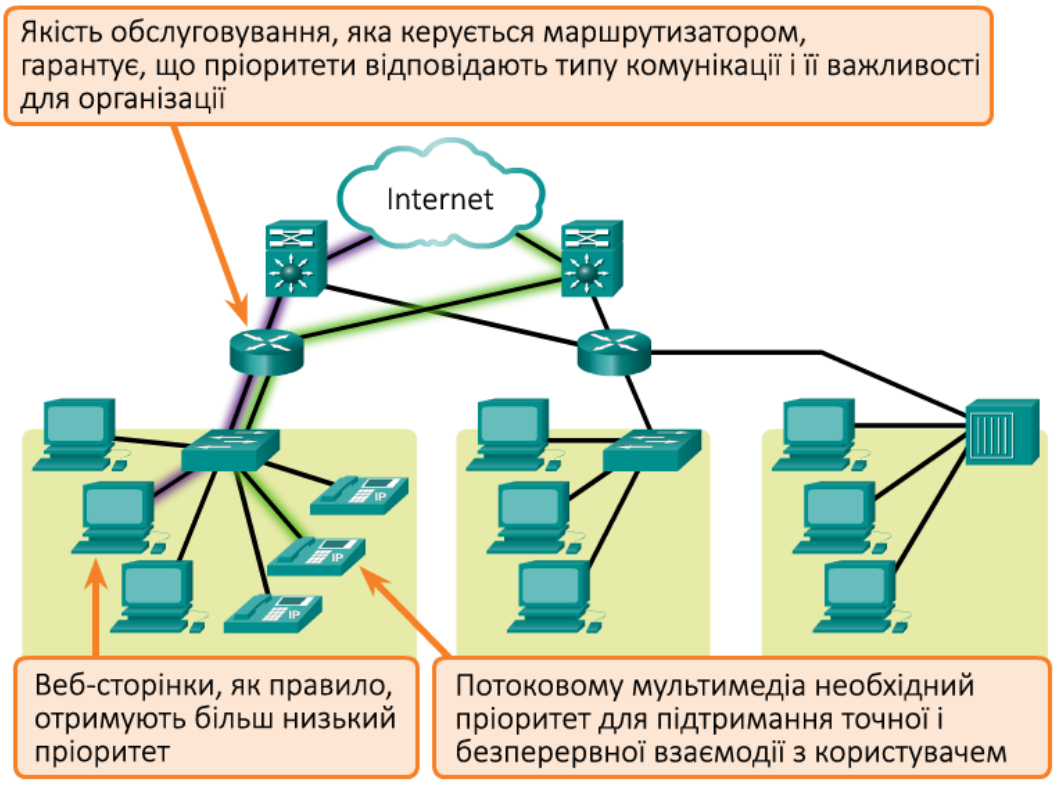

Рис. 2.5. Якість обслуговування

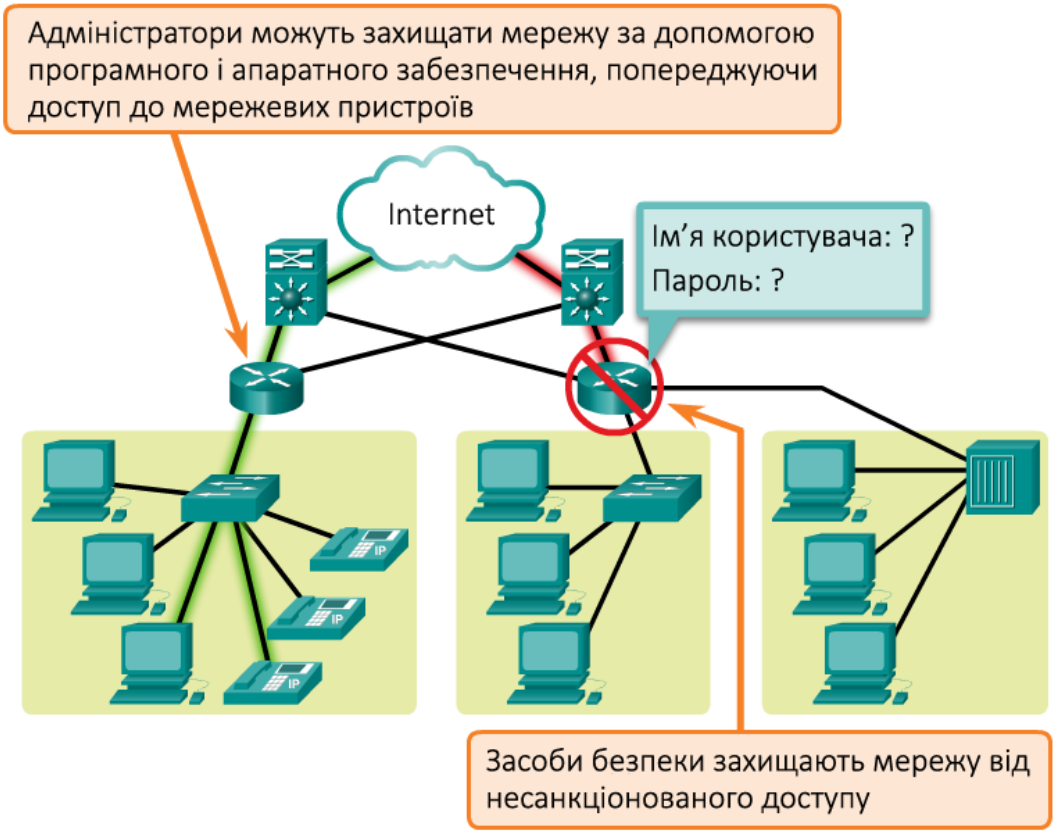

Рис. 2.6. Безпека

Стійкість до збоїв в мережах з комутацією каналів

Очікується, що Інтернет завжди доступний мільйонам користувачів, які розраховують на його безперебійну роботу. Для цього потрібна відмовостійка мережева архітектура. Відмовостійка мережа обмежує вплив збоїв таким чином, щоб вони торкнулися якомога меншої кількості пристроїв. Вона також побудована так, щоб швидко відновлюватися при виникненні відмови. Ці мережі покладаються на наявність декількох шляхів між джерелом і місцем призначення повідомлення. Якщо один шлях недоступний, повідомлення можна негайно відправити по іншій лінії зв'язку. Наявність декількох шляхів до місця призначення називається **резервуванням**.

Щоб зрозуміти потребу в резервуванні, слід вивчити роботу ранніх телефонних систем. Якщо користувач здійснював виклик за допомогою традиційного телефонного апарату, виклик спочатку проходив процес встановлення з'єднання. Цей процес встановлював місця комутації між абонентом (джерело) і телефонним апаратом, що викликається (одержувач). Під час дзвінка створювався тимчасовий канал або лінія. Якщо доступ до будь-якого з ресурсів або пристроїв в каналі отримати не вдавалося, виклик скидався. Для повторного підключення необхідно було зробити новий виклик з новим каналом. Цей процес встановлення з'єднання називається **процесом комутації каналів** і проілюстровано на рис 2.7.

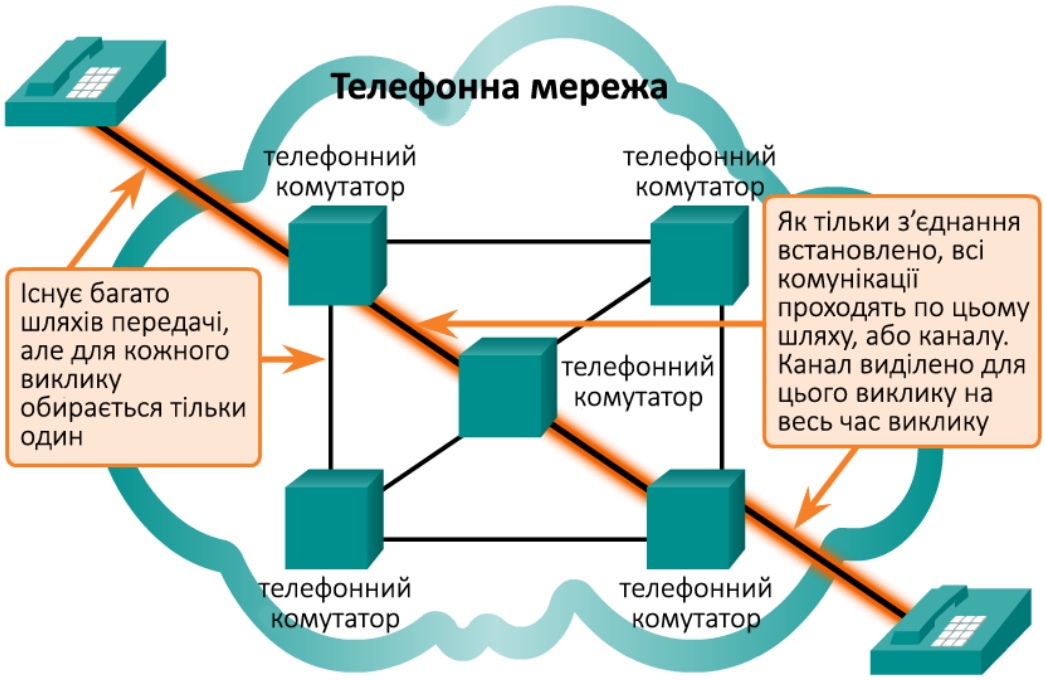

Рис 2.7. Комутація каналів в телефонній мережі

Багато мереж з комутацією каналів надають пріоритет існуючим каналам підключення за рахунок нових запитів. Після того як канал створений, і навіть якщо між абонентами на двох кінцях каналу не відбувається обмін повідомленнями, канал залишається підключеним, а ресурси зайнятими до тих пір, поки виклик не буде завершений однією зі сторін. Через те що число каналів обмежено, можна отримати повідомлення про те, що всі канали зайняті і виклик не може бути виконаний. Вартість створення альтернативних маршрутів з достатньою пропускною здатністю для підтримки великого числа паралельних каналів і технології, необхідні для динамічного відновлення розірваних каналів в разі збою, пояснюють, чому ця технологія не була оптимальна для Інтернету.

Стійкість до збоїв в мережах з пакетною комутацією

У пошуках більш відмовостійкої моделі мережі розробники Інтернету звернули увагу на мережі з комутацією пакетів. Основним аргументом для цього типу мережі є те, що одне повідомлення можна розділити на кілька окремих блоків, причому кожен з блоків повідомлення містить інформацію про адресацію, що ідентифікує відправника, і пункт призначення. Блоки повідомлення з вбудованою інформацією називаються **пакетами**, вони можуть бути відправлені через мережу по різних шляхах, а потім на місці отримання зібрані в вихідне повідомлення, як це показано на рис. 2.8.

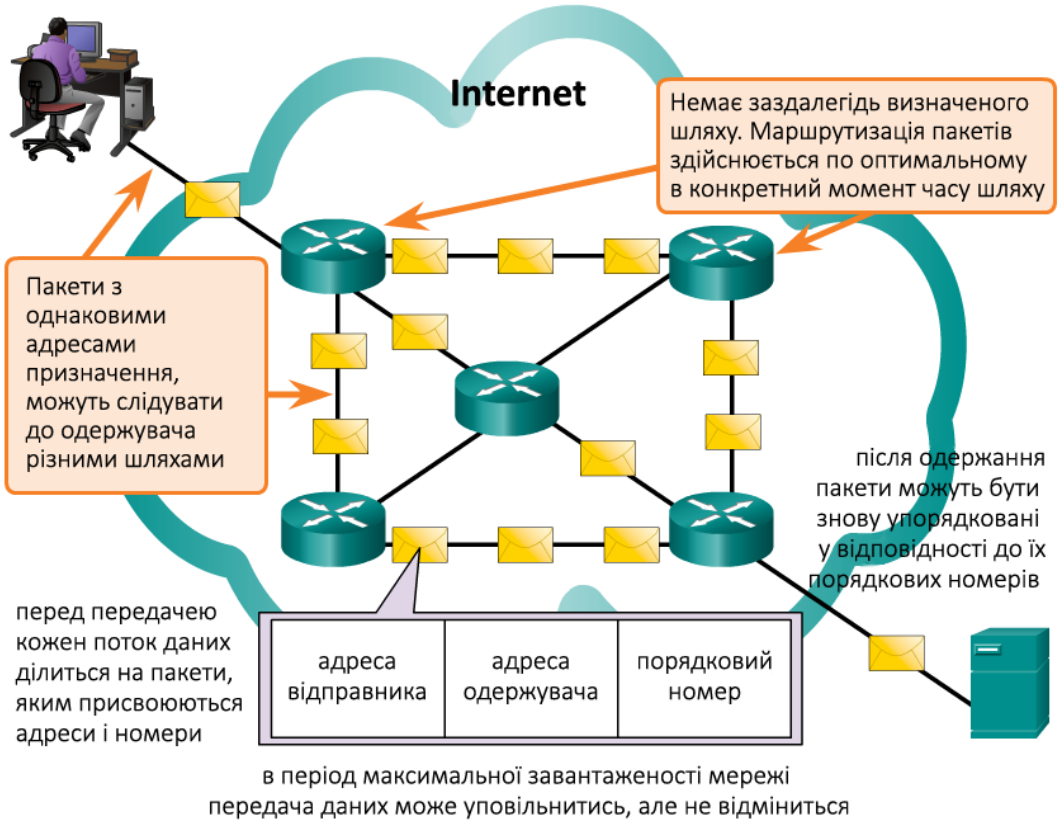

Рис. 2.8. Комутація пакетів у мережі передачі даних

Самі пристрої в мережі, як правило, не інформовані про зміст окремих пакетів. Їм видно тільки адреси джерела і кінцевого місця призначення. Ці адреси часто називають IP-адресами, представленими в точково-десятковому форматі, наприклад: 10.10.10.10. Кожен пакет відправляється незалежно з одного пункту до іншого. У кожному проміжному пункті приймається рішення про перенаправлення (маршрутизацію), тобто про вибір шляху, який слід використовувати для передачі пакетів до місця призначення. Наприклад, ви написали довгий лист товаришу на десяти листівках. Кожна листівка містить адресу призначення. По мірі того, як листівки пересилаються по звичайній поштовій системі, адреса призначення використовується для визначення наступного відрізку шляху, по якому повинна бути відправлена листівка. В кінцевому підсумку, вони будуть доставлені за адресою на листівках.

Якщо шлях, що використовувався раніше, стає недоступним, функція маршрутизації може динамічно вибрати наступний найбільш підходящий доступний шлях. Так як повідомлення відправляються по частинах, а не як одне ціле повідомлення, деякі з пакетів можуть бути втрачені, в цьому випадку їх можна повторно відправити до місця призначення за іншими маршрутами. У багатьох випадках пристрої призначення не поінформовані про те, чи мали місце

відмови або зміни маршруту. З використанням нашої аналогії з листівками, якщо одна з листівок втрачена в дорозі, тільки цю одну листівку необхідно вислати повторно.

В мережі з комутацією пакетів немає необхідності в єдиному зарезервованому шляху від відправника до одержувача. Будь-які частини повідомлення можна відправляти через мережу по будь-якому доступному шляху. Крім того, пакети з частинами повідомлень з різних джерел можуть передаватися по мережі в один і той же час. За рахунок реалізації способу динамічного використання надлишкових маршрутів без втручання користувача, Інтернет став відмовостійким видом зв'язку. У нашій аналогії з поштою, наприклад, коли наша листівка передається по звичайній поштовій системі, вона буде переміщатися на загальному транспорті з іншими листівками, листами і посилками. Наприклад, одна з листівок може виявитися в літаку з великою кількістю інших посилок і листів, які транспортуються до місця призначення.

Незважаючи на те, що мережі з комутацією пакетів без встановлення з'єднання є основою інфраструктури сучасного Інтернету, орієнтовані на підключення системи, такі як комутована телефонна мережа, мають свої переваги. Оскільки ресурси в різних місцях комутації орієнтовані на надання кінцевого числа каналів, можна гарантувати якість і узгодженість повідомлень в мережі з встановленням з'єднання.

Масштабовані мережі

Тисячі нових користувачів і операторів зв'язку підключаються до Інтернету щотижня. Щоб Інтернет міг підтримувати швидке зростання, йому необхідна масштабованість. Масштабовану мережу можна швидко розширити, забезпечивши підтримку нових користувачів і додатків без зниження ефективності обслуговування існуючих. На рис. 2.9-2.11 представлена рівнева структура Інтернету.

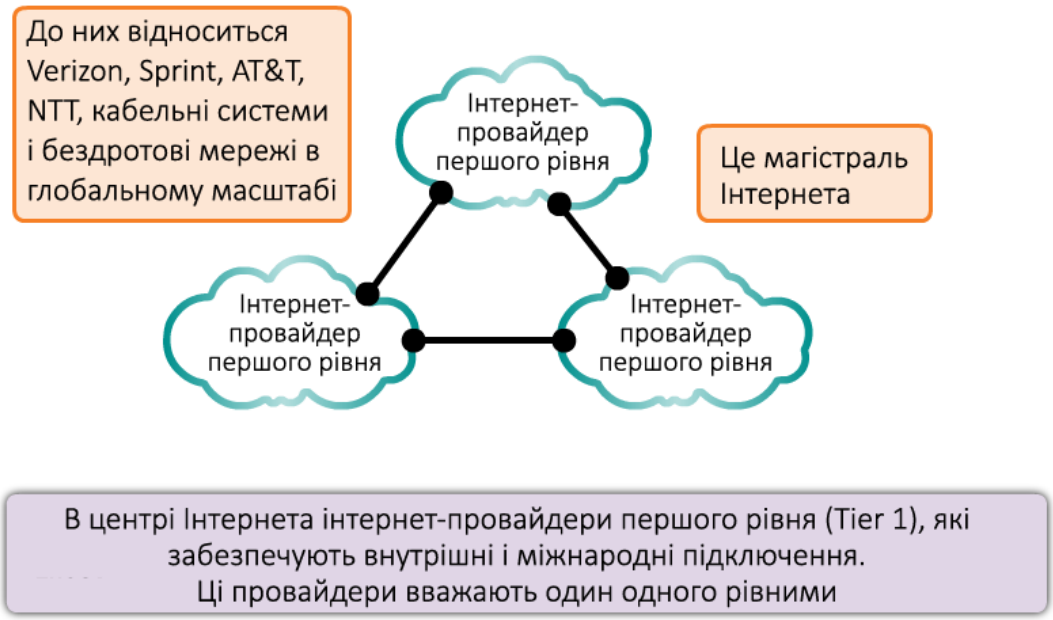

Рис. 2.9. Інтернет-провайдери першого рівня

Той факт, що Інтернет може розширюватися такими темпами без серйозного зниження ефективності для окремих користувачів, є результатом застосування вдалих підходів до розробки протоколів і технологій, на яких він побудований. Інтернет має ієрархічну багаторівневу структуру для адресації, іменування, а також для сервісів підключення. В результаті мережевому трафіку, адресованому місцевим і регіональним сервісам, не потрібно проходити через будь-яку

центральну точку. Поширені сервіси можуть дублюватися в різних регіонах, що дозволяє зменшити трафік на магістралях вищого рівня.

Рис. 2.10. Інтернет-провайдери другого рівня

Під масштабованістю також мається на увазі здатність розгортати нові продукти і додатки. Незважаючи на те, що не існує жодної організації, що управляє Інтернетом, багато окремих мереж, які забезпечують підключення до Інтернету, спільно працюють над дотриманням прийнятих стандартів і протоколів. Дотримання стандартів дозволяє виробникам апаратного і програмного забезпечення сконцентруватися на створенні нових і модернізації існуючих продуктів в області продуктивності і пропускної здатності, при цьому нові продукти можуть інтегруватися в існуючу інфраструктуру і вдосконалювати її.

Поточна архітектура Інтернету, незважаючи на високий рівень масштабованості, не завжди може впоратися зі зростаючими потребами користувачів. Для задоволення потреб в отриманні нових сервісів від сучасних інтернет-додатків розробляються нові протоколи і структури адресації.

Забезпечення якості обслуговування (QoS)

Вимоги до якості обслуговування (QoS) в мережі постійно зростають. Нові додатки, доступні користувачам через Інтернет, наприклад, передача голосу і відео в режимі реального часу, як показано на рис. 2.12, створюють більш високі вимоги до якості сервісів.

Мережі повинні забезпечувати передбачуваний, вимірний, а іноді і гарантований рівень сервісів. Архітектура мережі з комутацією пакетів не гарантує, що всі пакети, з яких складається

повідомлення, будуть доставлені в правильному порядку, а також те, що вони будуть доставлені без втрат.

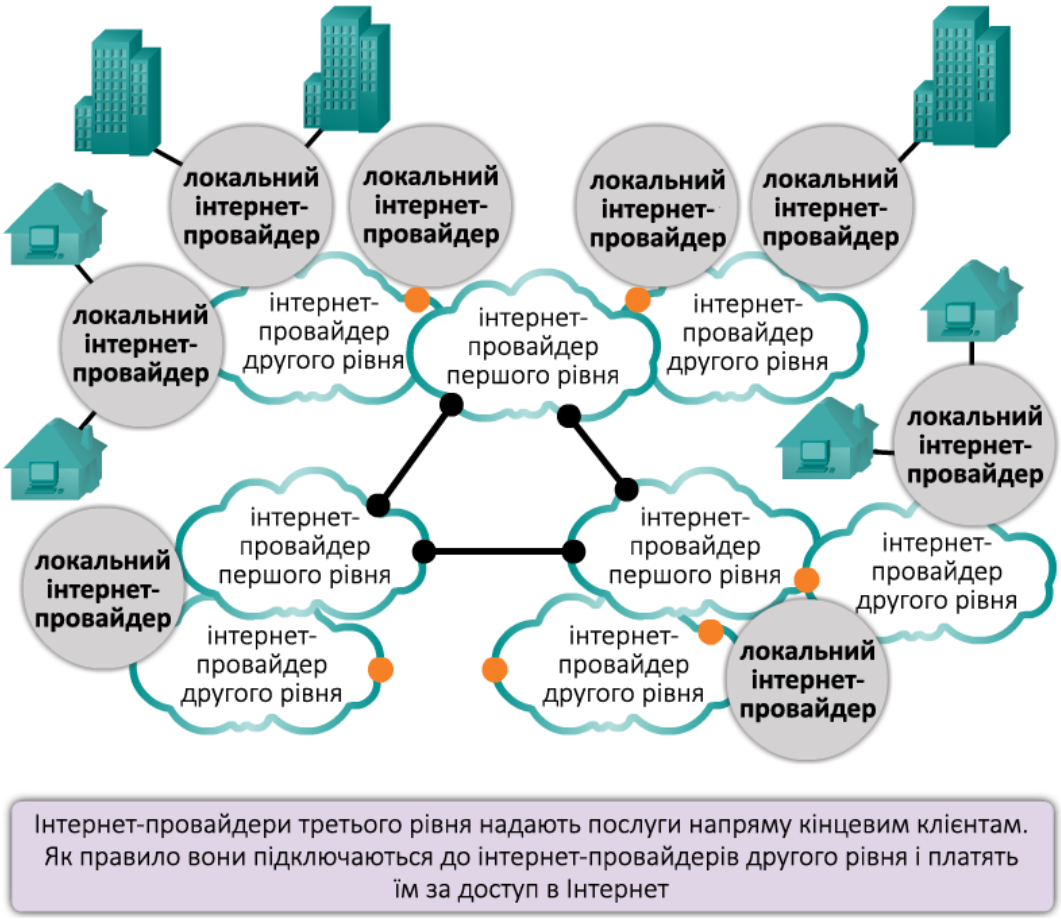

Рис. 2.11. Інтернет-провайдери третього рівня

Крім того, мережам необхідні механізми управління високоінтенсивним мережевим трафіком. **Пропускна здатність мережі** – це міра здатності мережі передавати дані. Іншими словами, пропускна здатність визначає, скільки інформації можна передати за певний час. Пропускна здатність мережі вимірюється в кількості біт, що передаються за одну секунду, або в бітах в секунду (біт/с). При паралельних спробах передачі повідомлень по всій мережі попит на пропускну здатність може перевищувати доступну величину, що створює перевантаження мережі. Мережа просто отримує більше біт, ніж смуга пропускання каналу зв'язку дозволяє доставити.

У більшості випадків, коли кількість пакетів перевищує можливості доставки по мережі, пристрої поміщають пакети в черги в пам'яті до тих пір, поки не з'являться доступні ресурси для передачі, як показано на рис. 2.13. Черги пакетів викликають затримки, оскільки нові пакети не можуть бути відправлені до тих пір, поки не відправлені попередні. Якщо кількість пакетів, поставлених в чергу, продовжує збільшуватися, пам'ять (буфер) заповнюються, і пакети відкидаються.

Забезпечення необхідної якості обслуговування (QoS) за допомогою управління затримками і параметрами втрати пакетів в мережі є ключем до забезпечення необхідної якості обслуговування для наскрізних додатків. Одне з рішень – застосування **класифікації**. Щоб створити класифікацію даних для цілей QoS, ми використовуємо поєднання комунікаційних характеристик і відносної важливості, призначеної додаткам, як показано на рис. 2.14. Потім ми обробляємо всі дані в одному і тому ж класі за одними і тими ж правилами. Так, з'єднання,

чутливе до часу доставки пакетів (наприклад, голосовий зв'язок), буде класифіковано не так, як з'єднання, що допускає затримки (наприклад, передача файлів).

Рис. 2.12. Об'єднані мережі

Приклади пріоритетних рішень для організації можуть включати в себе:

- **з'єднання, чутливе до часу передачі**: підвищений пріоритет для сервісів IP-телефонії та передачі відео;
- **з'єднання, не чутливе до часу передачі**: знижений пріоритет для отримання веб-сторінки або відправки листа по електронній пошті;
- **висока важливість для організації**: підвищений пріоритет для отримання інформації, що відноситься до управління виробництвом або торговельних операцій;
- **небажаний обмін даними**: зниження пріоритету або блокування несанкціонованої активності, наприклад, обмін файлами між одноранговими вузлами або інтерактивні розваги.

Забезпечення безпеки мережі

Інтернет перетворився з жорстко контрольованої освітніми та державними організаціями об'єднаної мережі в широкодоступний засіб ділового та особистого спілкування. В результаті змінилися вимоги до безпеки мережі. Мережева інфраструктура, сервіси та дані, що містяться в пристроях, підключених до мереж, представляють важливу складову особистих і ділових активів. Втрата цілісності цих ресурсів може привести до серйозних наслідків, таких як:

- збої в роботі мережі, які не дозволяють здійснювати комунікації і транзакції, що призводить до втрати ділових можливостей;
- розкрадання і використання конкурентами інтелектуальної власності компанії (ідеї, патенти або дослідження);
- порушення конфіденційності та публікація без згоди користувача його особистої або приватної інформації;
- неправильне використання і втрата особистих або корпоративних коштів;
- втрата даних, які вимагають істотних трудовитрат на їх відновлення або є невідновними.

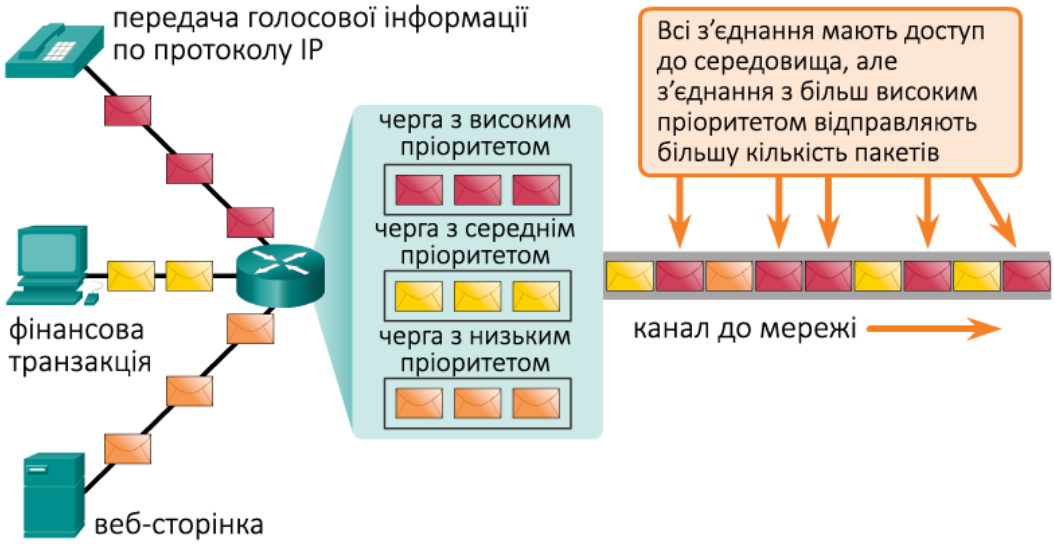

Рис. 2.13. Використання черг для призначення пріоритетів комунікацій

Існує два типи проблем безпеки мережі, які необхідно врахувати: безпека мережевої інфраструктури і безпека інформації. Забезпечення безпеки **інфраструктури мережі** включає в себе забезпечення фізичної безпеки всіх пристроїв, які необхідні для підключення до мережі, і запобігання несанкціонованого проникнення в керуюче програмне забезпечення, яке виконується на них. **Безпека інформації** означає захист даних, що містяться в пакетах, переданих по мережі, а також інформації, що зберігається на підключених до мережі пристроях. Заходи безпеки в мережі повинні:

- запобігати несанкціонованому розголошенню інформації;
- запобігати розкраданню інформації;
- запобігати несанкціонованим змінам інформації;
- запобігати відмовам в обслуговуванні (DoS-атака).

Для досягнення цілі забезпечення безпеки мережі, існує три основні вимоги:

- **забезпечення конфіденційності даних** означає, що тільки визначені й авторизовані одержувачі (співробітники, процеси або пристрої) можуть отримати доступ до даних. Це досягається за рахунок надійної системи аутентифікації користувачів, реалізації вимог до паролів, які складно підібрати, а також вимог частої зміни паролів. Шифрування даних, які міг би прочитати тільки вказаний одержувач, також входить в конфіденційність;

- **підтримка цілісності** означає надання гарантій, що інформація не була змінена в процесі передачі від вихідного пункту до місця призначення. Цілісність даних може бути порушена, коли інформація пошкоджена, навмисно або ненавмисно. Цілісність даних забезпечується шляхом перевірки відправника і використання механізмів перевірки того, що пакет не змінився при передачі;
- **забезпечення доступності** означає використання засобів забезпечення своєчасного і надійного доступу до даних для авторизованих користувачів. Пристрої з мережевими екранами, а також з настільним і серверним антивірусним програмним забезпеченням, дозволяють підвищити надійність і стійкість системи, виявляючи атаки і захищаючись від них. Створення мережевих інфраструктур, що повністю резервуються, з малим числом точок відмови може зменшити наслідки цих загроз.

Типи обміну даними	Без QoS	З QoS
потокове відео і аудіо	 зображення починає завантажуватись з артефактами і зупиняється	 безперебійне, безперервне обслуговування
життєво важливі транзакції	співвідношення часу і ціни 14:18:33 – 2,25$ тільки на одну секунду раніше...	співвідношення часу і ціни 14:18:32 – 2,21$ ціна може бути кращою
завантаження веб-сторінок (часто більш низький пріоритет)	 сторінка з'явиться трохи пізніше...	 але кінцевий результат однаковий

Рис. 2.14. Поєднання комунікаційних характеристик і відносної важливості, призначеної додаткам

Для закріплення та контролю знань, здобутих під час вивчення теоретичних відомостей, виконайте завдання «**Вимоги до мережевої архітектури**», що знаходиться у відповідному розділі форми **LW №2 CN Quiz**.

Завдання

Програмне забезпечення для трасування маршруту – це утиліта, яка містить списки мереж, по яким повинні пройти дані від відправника (користувача) до віддаленого мережевого пристрою призначення. Як правило, для запуску цього мережевого засобу в командний рядок необхідно ввести наступне:

```
tracert <destination network name or end device address>
```

(для операційних систем сімейства Microsoft Windows)

або

```
traceroute <destination network name or end device address>
```

(для Unix і подібних систем)

Утиліти трасування маршруту дозволяють визначати шляхи або маршрути, а також обчислювати час затримки в IP-мережі. Для виконання цієї функції існує декілька засобів.

Інструмент traceroute (або tracert) часто використовується для пошуку та усунення неполадок в мережі. Він відображає список пройдених маршрутизаторів і дозволяє визначити, який шлях використовувався для досягнення певного пункту призначення в одній мережі або переходу між декількома мережами. Кожен маршрутизатор – це точка з'єднання двох мереж, через яку пересилаються пакети даних. Кількість маршрутизаторів – це кількість «переходів», що відбулись під час передачі даних на шляху від джерела до пункту призначення.

Список маршрутизаторів допоможе визначити, які проблеми з потоком даних виникають при спробі доступу до якого-небудь сервісу, наприклад веб-сайту. Також список може стати в нагоді при виконанні таких завдань, як завантаження даних. Якщо один і той же файл доступний на кількох веб-сайтах (дзеркалах), можна перевірити маршрут для кожного дзеркала і вибрати найбільш швидкий варіант.

Два трасування маршруту, виконані між одними і тими ж вузлами джерела і адресата, але в різний час, можуть дати різні результати. Це може бути пов'язано з «повнозв'язним» характером взаємно підключених мереж, що складаються з можливостей Інтернету і протоколів Інтернету вибирати різні кабельні канали для відправки пакетів.

Засоби трасування маршруту за допомогою командного рядка зазвичай реалізовані в операційній системі прикінцевого пристрою. Інші інструменти, такі як VisualRoute™, є пропрієтарними програмами і дозволяють отримувати більш детальну інформацію. VisualRoute формує графічне відображення маршруту, використовуючи доступну інформацію в мережі.

Для виконання даної лабораторної роботи необхідна програма VisualRoute Lite Edition. Якщо на вашому комп'ютері програма VisualRoute Lite Edition не встановлена, завантажте її, перейшовши за наступним посиланням: http://www.visualroute.com/download.html.

Використовуючи інтернет-підключення і три різні утиліти трасування маршруту, ви повинні будете відстежити шлях проходження пакетів даних через Інтернет до мереж призначення. Для цього вам знадобиться комп'ютер, підключення до Інтернету і доступ до командного рядка. Спочатку ви скористаєтесь утилітою «tracert», вбудованою в ОС Windows, потім веб-засобом для трасування маршруту (http://www.subnetonline.com/pages/network-tools/online-traceroute.php) і, нарешті, програмою VisualRoute.

Частина 1: Перевірка підключення до мережі за допомогою ехо-запиту з використанням команди ping

Крок 1: Визначте, чи доступний віддалений сервер.

Для трасування маршруту до віддаленої мережі ваш ПК повинен бути підключений до Інтернету.

a. Спочатку ми скористаємося ехо-запитом за допомогою команди ping. Ехо-запит за допомогою команди ping – це засіб для перевірки доступності вузла. Пакети інформації пересилаються віддаленому вузлу з вимогою відповіді. Локальний ПК визначає, чи отримано відповідь для кожного пакету, і розраховує, який час знадобився для пересилання цих пакетів по мережі. Назва «ехо-запит» прийшла з області активної гідролокації, де вона позначала звуковий сигнал, який відправляється під воду і відбивається від дна або інших кораблів.

b. Натисніть комбінацію кнопок **Windows + R**, на екрані з'явиться вікно **Виконати** (рис. 2.15), введіть в полі команду **cmd** і натисніть клавішу **Enter**.

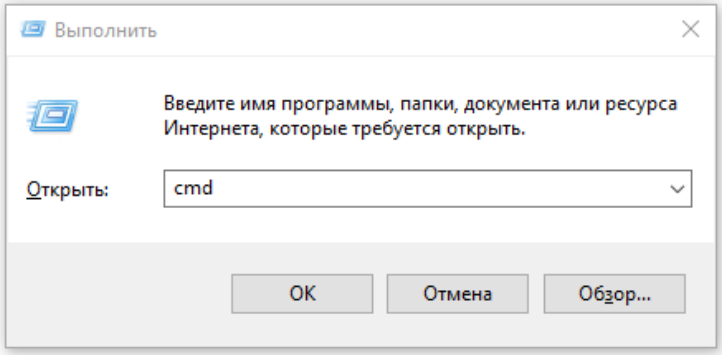

Рис. 2.15. Запуск командної оболонки у Windows

c. У командному рядку введіть **ping www.cisco.com** (рис. 2.16).

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Рис. 2.16. Результат виконання команди ping www.cisco.com

d. У першому рядку отриманих даних відображається повне доменне ім'я (FQDN) e144.dscb.akamaiedge.net. Потім показано IP-адресу 23.1.48.170. Веб-сайти компанії Cisco, що містять одну і ту ж інформацію, розміщуються на різних серверах (так званих дзеркалах) по всьому світу. Це означає, що ім'я FQDN і IP-адреса будуть відрізнятися в залежності від вашого місцезнаходження.

e. Візьмемо наведену на рис. 2.17 частину отриманих результатів.

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Рис. 2.17. Статистика виконання команди ping www.cisco.com

З неї видно, що було відправлено чотири ехо-запити за допомогою команди ping, на кожен з яких була отримана відповідь. Втрати пакетів відсутні (0% втрат). В середньому для передачі пакетів по мережі знадобилось 54 мс (мілісекунди). Мілісекунда – це 1/1000 секунди. Від втрати пакетів або повільного з'єднання з мережею в першу чергу страждає якість потокового відео і онлайн-ігор. Щоб визначити швидкість інтернет-підключення більш точно, можна відправити не 4 ехо-запити, передбачених за замовчуванням в утиліті **ping**, а, наприклад, 100 ехо-запитів. Для цього використовується зазначена на рис. 2.18 команда. Результат можна побачити на рис. 2.19.

```
C:\>ping -n 100 www.cisco.com
```

Рис. 2.18. Збільшення кількості ехо-запитів

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

Рис. 2.19. Статистика виконання команди ping www.cisco.com при 100 ехо-запитах

f. Тепер відправте ехо-запити за допомогою команди **ping** на веб-сайти регіональних інтернет-реєстраторів (RIR), які розташовані в різних частинах світу.
   Африка:
   `C:\>` **`ping www.afrinic.net`** (рис. 2.20)

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

Рис. 2.20. Результат виконання команди ping www.afrinic.net

Австралія:
`C:\>` **`ping www.apnic.net`** (рис. 2.21)

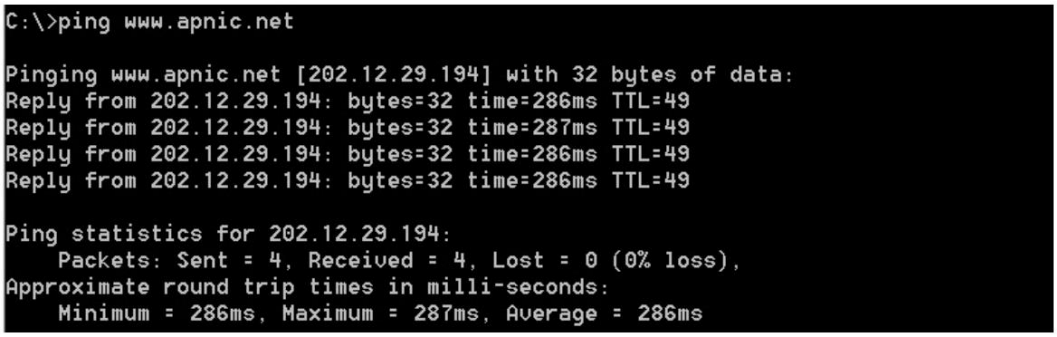

Рис. 2.21. Результат виконання команди ping www.apnic.net

Європа:
C:\> **ping www.ripe.net** (рис. 2.22)

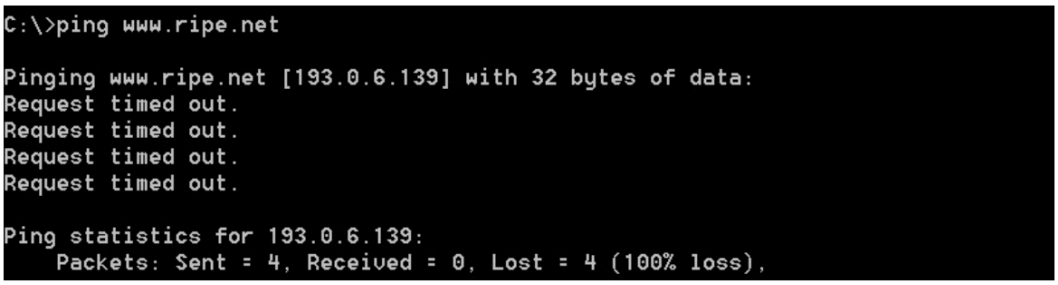

Рис. 2.22. Результат виконання команди ping www.ripe.net

Південна Америка:
C:\> **ping lacnic.net** (рис. 2.23)

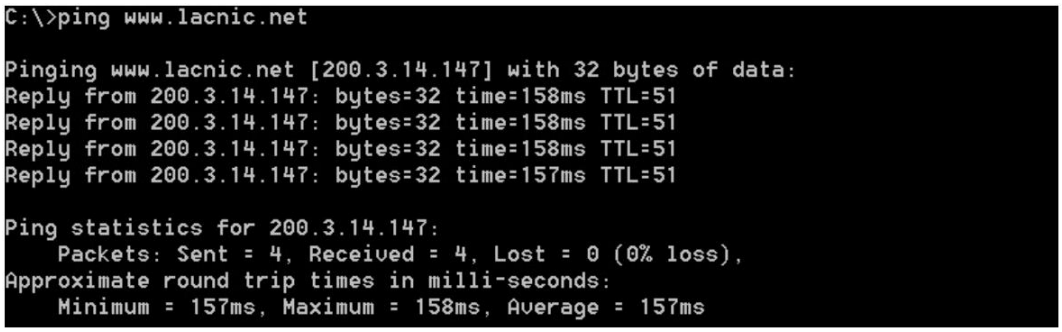

Рис. 2.23. Результат виконання команди ping lacnic.net

Дайте відповідь на питання «**1.1f.1**» та «**1.1f.2»**, в наступному розділі форми **LW №2 CN Quiz**.

Частина 2: Відстеження маршруту до віддаленого сервера за допомогою утиліти «traceroute»

Крок 1: Визначте, який маршрут з усього інтернет-трафіку спрямований до віддаленого сервера.

Перевіривши досяжність за допомогою утиліти **ping**, варто більш уважно розглянути кожен сегмент мережі, через який проходять дані. Для цього скористаємося утилітою **tracert**.

a. У командному рядку по черзі введіть **tracert** www.cisco.com, **tracert** www.afrinic.net і **tracert** www.lacnic.net.

   Збережіть результати, отримані після введення команди «tracert», в текстовий файл, виконавши такі дії:

   1) натисніть правою кнопкою миші на рядок заголовка вікна командного рядка і виберіть параметри **Змінити** -> **Виділити все**;
   2) ще раз натисніть правою кнопкою миші на рядок заголовка вікна командного рядка і виберіть параметри **Змінити** -> **Копіювати**;
   3) відкрийте **Блокнот Windows**;
   4) щоб вставити дані в **Блокнот**, виберіть у меню **Правка** команду **Вставити**.

b. Проінтерпретуйте дані, отримані за допомогою утиліти **tracert**.

   В залежності від зони охоплення вашого інтернет-провайдера і розташування вузлів джерела і призначення, відстежені маршрути можуть перетинати велику кількість переходів і мереж. Кожен перехід – це один маршрутизатор. Маршрутизатор являє собою особливий комп'ютер, який використовується для перенаправлення трафіку через Інтернет. Уявіть, що ви вирушили в поїздку по автодорогах кількох країн. Під час своєї подорожі ви постійно потрапляєте на розвилки, де потрібно вибирати один з кількох напрямків. Тепер уявіть собі, що на кожній такій розвилці є пристрій, який вказує правильний шлях до кінцевої мети вашої подорожі. Те ж саме робить маршрутизатор для пакетів в мережі.

   Оскільки комп'ютери використовують мову цифр, а не слів, маршрутизаторам присвоюються унікальні IP-адреси (номери в форматі x.x.x.x). Утиліта **tracert** показує, яким шляхом проходить пакет даних до кінцевого пункту призначення. Крім того, за допомогою утиліти **tracert** можна визначити, з якою швидкістю проходить трафік через кожен сегмент мережі. Кожному маршрутизатору на шляху проходження даних відправляються три пакети, час відповіді на які вимірюється в мілісекундах. Використовуючи дану інформацію, проаналізуйте результати, отримані за допомогою утиліти **tracert** при відправці пакетів до www.cisco.com, наведені на рис. 2.24.

   У наведеному на рис. 2.25 прикладі пакети, відправлені утилітою **tracert**, пересилаються з ПК джерела на основний шлюз локального маршрутизатора (перехід 1: 192.168.1.1), а потім на маршрутизатор в точці підключення (POP) до інтернет-провайдера (перехід 2: 10.18.20.1).

   У кожного провайдера може бути велика кількість маршрутизаторів POP. Вони відмічають кордони мережі інтернет-провайдера і служать точками підключення до Інтернету для клієнтів. Пакети передаються по мережі компанії Verizon, перетинають два переходи і потрапляють в маршрутизатор, який належить alter.net. Це може означати, що пакети досягли іншого інтернет-провайдера. Цей момент дуже важливий, оскільки при пересиланні пакетів від одного до іншого провайдера можливі втрати, а також важливо пам'ятати, що не всі інтернет-провайдери здатні забезпечити однакову швидкість передачі даних. Як визначити, чи є alter.net тим же самим або іншим інтернет-провайдером?

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Рис. 2.24. Результат виконання команди tracert www.cisco.com

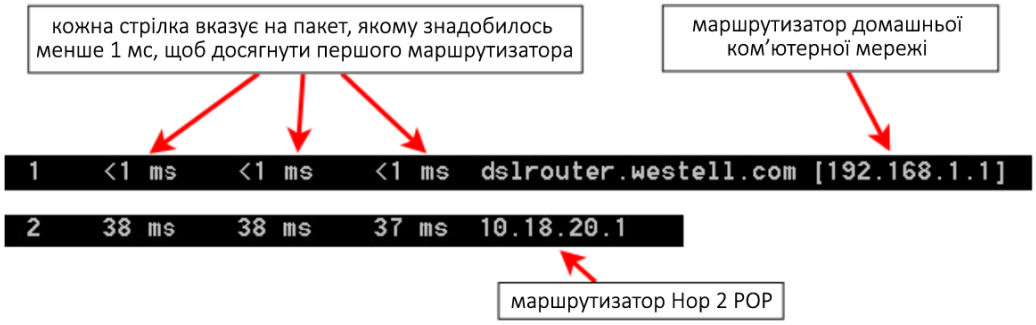

Рис. 2.25. Деталізація результату виконання команди tracert www.cisco.com

c. Існує інтернет-сервіс **whois**, за допомогою якого можна дізнатися власника доменного імені. Сервіс whois доступний за адресою http://whois.domaintools.com. Згідно з інформацією, отриманою за допомогою **whois**, домен alter.net також належить компанії Verizon (рис. 2.26).

Registrant Org	Verizon Business Global LLC is associated with ~406 other domains

Рис. 2.26. Перевірка власника домену alter.net за допомогою інтернет-сервісу whois

Таким чином, інтернет-трафік починається на домашньому ПК і проходить через домашній маршрутизатор (перехід 1). Потім він підключається до інтернет-провайдера і передається по його мережі (переходи 2-7), поки не досягне віддаленого сервера (перехід 8). Це досить нетиповий приклад, в якому від початку до кінця задіяний тільки один провайдер. Як видно з наступних прикладів, найчастіше в пересиланні даних беруть участь два і більше інтернет-провайдерів.

d. Тепер розглянемо приклад з пересилкою інтернет-трафіку через кілька інтернет-провайдерів. На рис. 2.27 ви побачите результати застосування утиліти «tracert» до вузла www.afrinic.net.

Дайте відповідь на питання «**2.1d.1**», «**2.1d.2**» та «**2.1d.3**», в наступному розділі форми **LW №2 CN Quiz**.

g. Ознайомтесь з результатами застосування утиліти «tracert» до вузла www.lacnic.net, які наведені на рис. 2.28.
Дайте відповідь на питання «**2.1g.1**» у формі **LW №2 CN Quiz**.

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

Рис. 2.27. Результат виконання команди tracert www.afrinic.net

Частина 3: Відстеження маршруту до віддаленого сервера за допомогою програмних і веб-засобів

Крок 1: Скористайтеся веб-засобом для трасування маршруту.

a. За допомогою сайту http://www.subnetonline.com/pages/network-tools/online-tracepath.php відстежте маршрут до наступних веб-сайтів: www.cisco.com, www.afrinic.net.
Скопіюйте дані і збережіть їх в файл Блокнота.
Дайте відповідь на питання «**3.1a.1**», «**3.1a.2**» та «**3.1a.3**», в наступному розділі форми **LW №2 CN Quiz**.

Крок 2: Робота з програмою VisualRoute Lite Edition.

VisualRoute – це пропрієтарна програма, що дозволяє відобразити результати трасування маршруту наочно.

a. Якщо програма VisualRoute 2010 Lite Edition ще не встановлена на вашому комп'ютері, завантажте її за наступним посиланням: http://www.visualroute.com/download.html.
b. За допомогою програми VisualRoute 2010 Lite Edition відстежте маршрути до www.afrinic.net.
c. Збережіть отримані IP-адреси у файлі Блокнота.

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

Рис. 2.28. Результат виконання команди tracert www.lacnic.net

Частина 4: Порівняння результатів трасування

Крок 1: Порівняння результатів трасування маршруту до www.afrinic.net, отриманих в частинах 2 і 3.

a. Дайте відповідь на питання «**4.1a.1**», «**4.1a.2**», «**4.1a.3**» та «**4.1a.4**», в наступному розділі форми **LW №2 CN Quiz**.