Міністерство освіти і науки України
Центральноукраїнський національний технічний університет

**Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А.,
Буравченко К.О., Смірнова Т.В. Поліщук Л.І.**

ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Навчальний посібник

Кропивницький
Видавець Лисенко В. Ф.
2019

УДК 004.7
ББК 32.973.202
С 50

Рекомендовано Вченою радою Центральноукраїнського національного технічного університету, протокол № 8 від 25 квітня 2019 року

Рецензенти:

Павленко М.А., доктор технічних наук, професор, начальник кафедри математичного та програмного забезпечення АСУ Харківського університету Повітряних Сил ім.. Івана Кожедуба;

Семенов С.Г., доктор технічних наук, старший науковий співробітник, Завідувач кафедрою обчислювальної техніки та програмування Національного технічного університету «Харківський політехнічний університет».

Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І.

С 50 Проектування комп'ютерних систем та мереж : навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2019. — 264 с.

У навчальному посібнику розглянуто теоретичні й практичні питання основ і положень проектування комп'ютерних систем та мереж, програмні та апаратні методи способів підтримки мережевих інформаційних ресурсів, засоби безпеки мереж.

Навчальний посібник призначений для студентів, які навчаються за спеціальностями «Кібербезпека», «Комп'ютерні науки», «Комп'ютерна інженерія», а також аспірантів, науковців та інженерно-технічних працівників з напряму «Інформаційні технології».

ББК 32.973.202

ВСТУП

Сучасний світ насичений великою кількістю комп'ютерів та техніки, і тому особливою актуальністю користуються послуги з проектування комп'ютерних мереж. Комп'ютерна мережа являє собою складну обчислювальну систему, в яку об'єднані різні компоненти та вузли, а отже від того, наскільки ретельно буде сплановано компонування мережі, залежатиме стабільність і довга робота всіх пристроїв. При проектуванні комп'ютерної мережі потрібно врахувати, що вона буде володіти особливими характеристиками і параметрами. На сьогоднішній день комп'ютерна мережа стала одним з основних атрибутів обчислювальних систем, інформаційні технологій супроводжуються збільшенням ролі комп’ютерних мереж. Це пояснюється необхідністю більш швидкої передачі інформації, в тому числі й управлінської, для якої важливе значення мають час її доставки користувачам.

Головні переваги, які можна отримати від локальної мережі, – це можливість спільно використовувати загальні ресурси, обмінюватися даними, мати централізоване сховище, використовувати принтери або виходити в мережу Інтернет. Не менш важливим аспектом є отримання відмовостійкої системи, яка зможе продовжити своє функціонування при виході з ладу окремих її частин. Досягається це за рахунок застосування при проектуванні комп'ютерних мереж так званої надлишковості та дублювання. Як правило, побудова надійної системи, яка буде відповідати всім заявленим вимогам і мати найменшу вартістю, починається з опрацювання плану. У ньому враховуються різні характеристики, підбирається необхідна топологія, програмне та апаратне забезпечення.

При проектуванні комп'ютерної мережі потрібно врахувати, що вона буде володіти особливими характеристиками і параметрами. Серед основних

етапів проектування комп'ютерних мереж виділяється вибір інструментарію, який буде забезпечувати взаємодію вузлів.

Метою даного навчального посібника є отримання досконалих знань у області проектування комп’ютерних систем та мереж, а також отримання студентами навичок створення і розміщення в мережі комерційних чи наукових проектів.

Представлений в навчальному посібнику матеріал надасть фахівцям практичні рекомендації і допоможе навчитися проектувати і розробляти оптимізовані комп’ютерні мережі.

РОЗДІЛ 1. ОСНОВИ ОРГАНІЗАЦІЇ МЕРЕЖ

Комп'ютерна мережа – це об'єднання двох або більше комп'ютерів та/або комп'ютерного обладнання (сервери, маршрутизатори та ін.) з метою спільної обробки, зберігання або передачі даних.

За призначенням комп'ютерні мережі розподіляються на:

– обчислювальні;

– інформаційні;

– змішані.

Обчислювальні мережі призначені головним чином для рішення завдань користувачів з обміном даними між їхніми абонентами.

Інформаційні мережі орієнтовані в основному на надання інформаційних послуг користувачам.

Змішані мережі сполучають функції перших двох.

Мережева модель – теоретичний опис принципів роботи набору взаємодіючих один з одним мережевих протоколів.

Модель звичайно ділиться на рівні, так щоб протоколи більш високого рівня використовували протоколи більш низького рівня, точніше, дані протоколу вище розташованого рівня передавалися за допомогою протоколів нижче розташованих рівнів – цей процес називають інкапсуляцією, в свою чергу, процес добування даних вище розташованого рівня з даних нижче розташованого рівня називають деінкапсуляцією).

Моделі бувають як практичні (що використовуються в мережах, вони іноді заплутані і неповні, але вирішують поставлені задачі), так і теоретичні (що показують принципи реалізації мережевих моделей, вони більш наочні і повні, але заради наочності жертвують продуктивністю та деякими можливостями практичних моделей).

Багаторівнева мережева модель описує взаємодію між різними протоколами всередині кожного рівня, а також взаємодію з верхніми й нижніми рівнями.

Використання багаторівневої мережевої моделі дає ряд переваг:

– спрощує розробку протоколів, тому що протоколи, що працюють на певному рівні, визначають формат оброблюваних даних і надають інтерфейс до верхніх і нижніх рівнів;

– змушує постачальників конкуруючих продуктів створювати уніфіковані рішення;

– виключає можливості зміни технологій або функцій одного рівня без врахування наслідків для верхніх і нижніх рівнів;

– надає загальну мову для опису функцій мережевої взаємодії.

Найбільш відомі мережеві моделі:

– модель OSI (вона ж ЕМ ВВС – еталонна модель взаємозв'язку відкритих систем) – еталонна теоретична модель, описана в міжнародних стандартах і ДСТ;

– модель TCP/IP (Модель DOD) – модель, що використовується на практиці, прийнята для роботи в Інтернеті;

– модель SPX/IPX – модель стека SPX/IPX (сімейство протоколів для ЛОМ);

– модель AppleTalk – модель для мереж AppleTalk (протоколи для роботи мереж з устаткуванням Apple);

– модель Fibre Channel – модель для високошвидкісних мереж Fibre Channel.

Мережева модель TCP/IP

Перша багаторівнева еталонна модель мережевої взаємодії була створена на початку 70-х років і називається моделлю мережі Інтернет. У ній визначені чотири обов'язкових категорії функцій, необхідних для успішної взаємодії. Архітектура протоколів TCP/IP побудована на основі цієї моделі. Тому модель мережі Інтернет звичайно називають моделлю TCP/IP.

Протоколи працюють один з одним у стеку – це означає, що протокол, що розташовується на рівні вище, працює «поверх» нижнього, використовуючи механізми інкапсуляції.

Мережева модель TCP/IP представлена на рисунку 1.1.

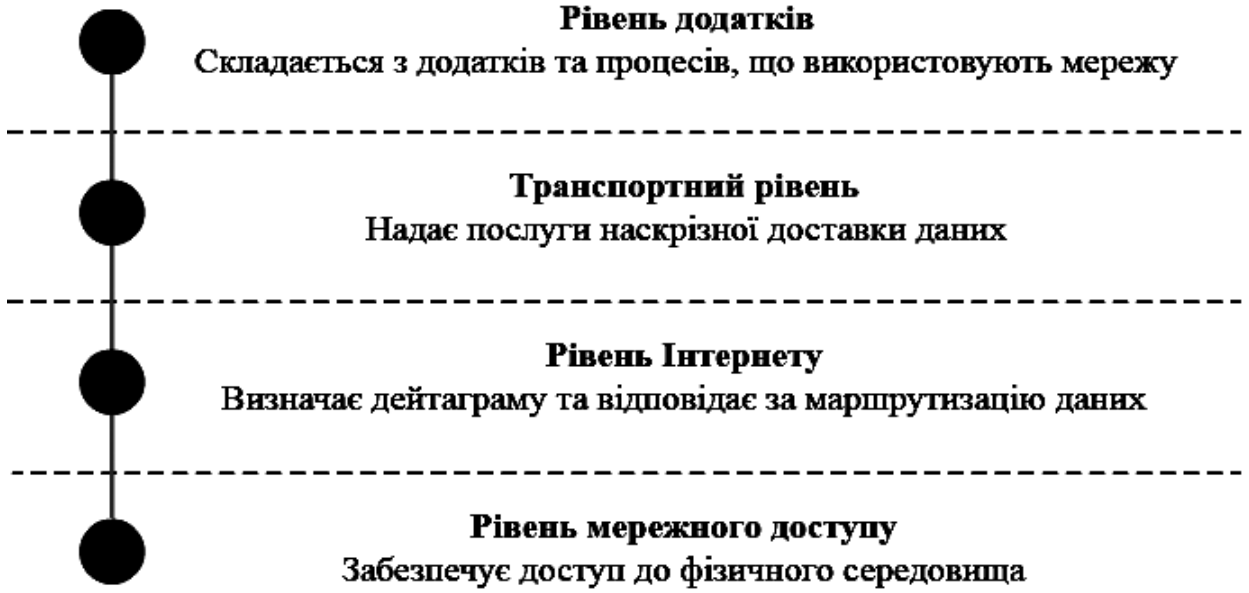


Рисунок 1.1 – Модель TCP/IP

Модель TCP/IP складається із чотирьох рівнів (знизу нагору):

1. Рівень мережевого доступу (Network Access).

2. Рівень Інтернету (Internet).

3. Транспортний рівень (Transport).

4. Рівень додатків (Process/Application).

Кожний із чотирьох рівнів моделі TCP/IP виконує свої функції.

Прикладний рівень (рівень додатків). Верхній рівень моделі, що включає протоколи, які обробляють дані користувачів і здійснюють керування обміном даними між додатками. На цьому рівні стандартизується представлення даних. Приклади протоколів: HTTP, SMTP, POP, IMAP, FTP, DNS, DHCP, Telnet.

Транспортний рівень. Містить протоколи для забезпечення цілісності даних при наскрізній передачі. Забезпечує керування ініціалізацією й закриттям з'єднань. Приклади протоколів: TCP та UDP.

Рівень Інтернету. Містить протоколи для маршрутизації повідомлень у мережі та служить для розміщення даних у дейтаграмі. Приклади протоколів: IP, NAT, ICMP, OSPF, RIP, BGP.

Рівень мережевого доступу. Нижній рівень моделі. Містить протоколи для фізичної доставки даних до мережевих пристроїв. Цей рівень розміщує дані в кадрі. Приклади протоколів: PPP, ARP, Ethernet, ATM.

Мережева модель OSI

Мережева модель OSI (англ. Open Systems Interconnection Basic Reference Model – базова еталонна модель взаємодії відкритих систем) – абстрактна мережева модель для комунікацій і розробки мережевих протоколів. Пропонує погляд на комп'ютерну мережу з точки зору вимірів. Кожний вимір обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережевого обладнання та програмного забезпечення стає набагато простішою й прозорішою.

Модель взаємодії відкритих систем була розроблена Міжнародною Організацією по Стандартизації (ISO) в 1984 році. На відміну від моделі TCP/IP, вона не описує взаємодій між окремими протоколами. Вона була створена як базова архітектура, яку розробники використовували для створення протоколів мережевої взаємодії. Хоча в далеко не всіх стеках протоколів у точності реалізовані всі сім рівнів моделі взаємодії відкритих систем, на сьогоднішній день вона вважається еталонною моделлю міжкомп’ютерних взаємодій.

У моделі OSI представлені всі функції або завдання, асоційовані з мережевими взаємодіями, а не тільки з певними протоколами TCP/IP. На відміну від моделі TCP/IP, у якій представлено тільки чотири рівні, модель OSI складається з семи більш специфічних рівнів (див. рисунок 1.2).

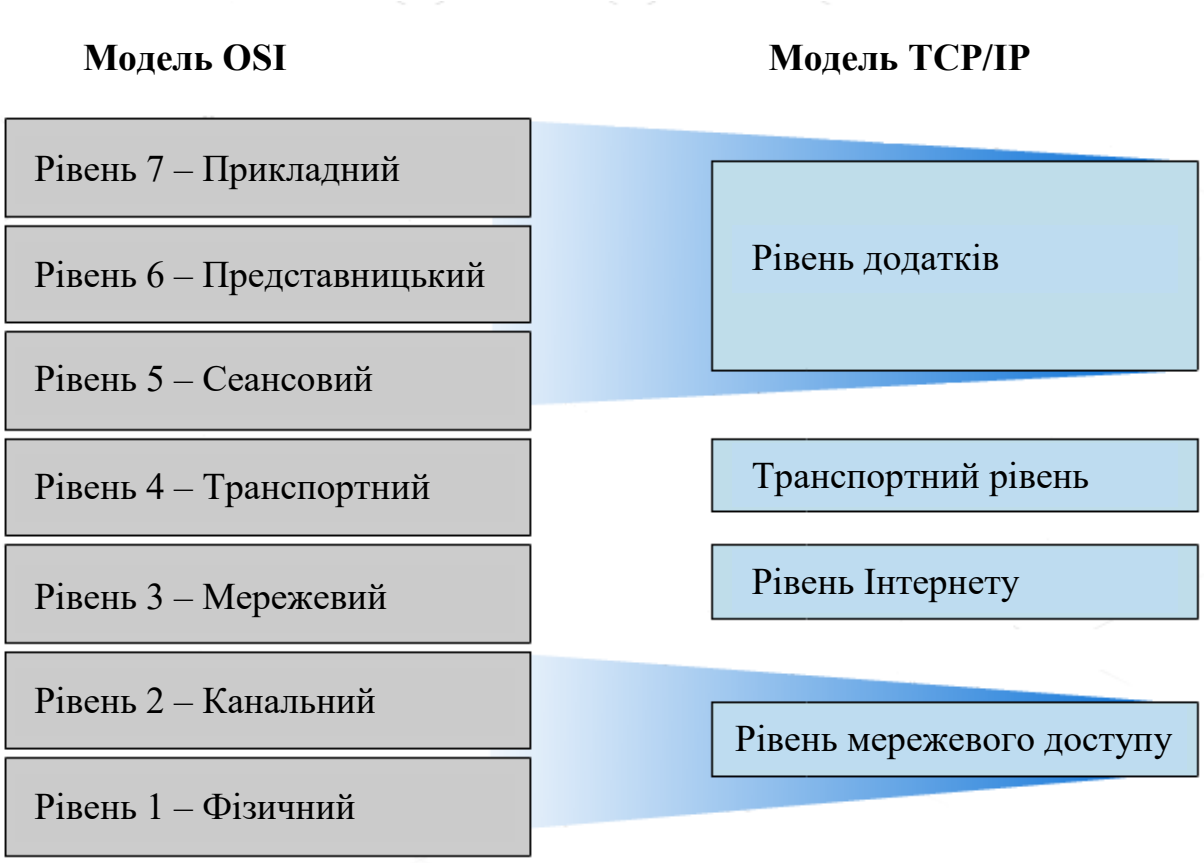


Рисунок 1.2 – Порівняння мережевих моделей OSI та TCP/IP

Кожному рівню присвоюється своя задача або група задач. Поділ функцій забезпечує незалежне функціонування кожного рівня в стеці. Наприклад, доступ до веб-сайту можливий як з портативного комп'ютера, підключеного до домашнього модему, так і з портативного комп'ютера за допомогою бездротового або мобільного телефону з підтримкою функцій бездротового доступу. Нижні рівні не впливають на ефективність роботи рівня додатка.

Точно так само нижні рівні не залежать від інших рівнів. Наприклад, на швидкість з'єднання з Інтернетом не впливає одночасний запуск декількох додатків, наприклад, електронна пошта, перегляд веб-сторінок, обмін миттєвими повідомленнями й завантаження музичних файлів.

У таблиці 1.1 представлені рівні мережевої моделі OSI та їх призначення.

Сім рівнів моделі OSI можна розділити на дві групи: верхні й нижні.

Верхніми рівнями часто називають усе, що перебуває вище транспортного рівня моделі OSI. Верхні рівні відносяться до роботи додатків і звичайно реалізуються тільки на програмному рівні. У рамках моделі OSI найвищий рівень – це прикладний рівень і він найближче розташований до кінцевого користувача.

Таблиця 1.1 – Рівні мережевої моделі OSI та їх призначення

Група	Номер рівня	Назва рівня	Протоколи та технології	Розподілені мережеві компоненти даного рівня
Верхні рівні	7	Прикладний	DNS, NFS, DHCP, SNMP, FTP, TFTP, SMTP, POP3, IMAP, HTTP, Telnet	Додатки для контролю стану мережі, електронна пошта, веб-браузери, передача файлів тощо
	6	Представницький	SSL, оболонки і редиректори, MIME	
	5	Сеансовий	NetBIOS, інтерфейси програм, віддалені виклики процедури	

Продовження таблиці 1.1

Нижні рівні	4	Транспортний	TCP та UDP	Механізми потокового відео та голосового зв’язку, списки фільтрів міжмережевих екранів
	3	Мережевий	IPv4, IPv6, IP NAT	IP-адресація, маршрутизація
	2	Канальний	Сімейство протоколів Ethernet, WLAN, Wi-Fi, ATM, PPP	Мережеві інтерфейсні плати та накопичувачі, мережева комутація, підключення до глобальної мережі
	1	Фізичний	Передача електричних сигналів, форми світлових хвиль, форми радіохвиль	Фізичне середовище передачі даних (мідна вита пара, оптоволоконний кабель, бездротові передавачі), концентратори і повторювачі

Нижні рівні моделі OSI відносяться до передачі даних. Фізичний та канальний рівні реалізовані на апаратному та програмному рівнях. Фізичний рівень ближче всього до фізичного середовища передачі, до мережевих дротів. Він фактично поміщає інформацію в середовище.

Кінцеві станції, наприклад, клієнти й сервери, звичайно працюють на всіх семи рівнях. Мережеві пристрої працюють тільки на нижніх рівнях. Концентратори – це рівень 1, комутатори – рівні 1 і 2, маршрутизатори – рівні від 1 до 3, мережеві екрани – рівні 1, 2, 3 і 4.

Будь-який протокол моделі OSI повинен взаємодіяти або із протоколами свого рівня, або із протоколами на одиницю вище й/або нижче свого рівня. Взаємодії з протоколами свого рівня називаються горизонтальними, а з рівнями на одиницю вище або нижче – вертикальними. Будь-який протокол моделі OSI може виконувати тільки функції свого рівня й не може виконувати функцій іншого рівня, що не виконується в протоколах альтернативних моделей.

На кожному з рівнів одиниці інформації називаються по-різному:

– На фізичному рівні найменша одиниця інформації – біт.
– На канальному рівні інформація об'єднана у фрейми (або пакети).
– На мережевому рівні говорять про дейтаграми.
– На транспортному рівні одиницею вимірювання є сегмент.
– Прикладні рівні обмінюються повідомленнями.

Пряма паралель із файловою системою на диску: локальні зміни намагніченості – біти об'єднані в сектори, що мають заголовки, сектори поєднуються в блоки, а ті, у свою чергу, у файли, що теж мають заголовки, що містять службову інформацію.

Таблиця 1.2 – Функції та одиниці вимірювання інформації різних рівнів моделі OSI

Рівень	**Функції**	**Тип даних**
Прикладний	Доступ до мережевих служб	Дані
Представницький	Подання й кодування даних	
Сеансовий	Керування сеансом зв'язку	
Транспортний	Прямий зв'язок між кінцевими пунктами й надійність	Сегменти
Мережевий	Визначення маршруту й логічна адресація	Пакети
Канальний	Фізична адресація	Кадри
Фізичний	Робота із середовищем передачі, сигналами й двійковими даними	Біти

Розглянемо кожний рівень моделі OSI більш докладно.

Фізичний рівень

Фізичний рівень має справу з передачею бітів по фізичних каналах зв'язку, таких, наприклад, як коаксіальний кабель, кручена пара, оптоволоконний кабель або цифровий територіальний канал. До цього рівня мають відношення характеристики фізичних середовищ передачі даних, такі як смуга пропускання, перешкодозахищеність, хвильовий опір і ін. На цьому ж рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію, наприклад крутизна фронтів імпульсів, рівні напруги або струму переданого сигналу, тип кодування, швидкість передачі сигналів.

Крім цього, тут стандартизуються типи роз’ємів і призначення кожного контакту.

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережевим адаптером або послідовним портом.

Прикладом протоколу фізичного рівня може служити специфікація 10Base-T технології Ethernet, що визначає як використовуваний кабель неекрановану кручену пару категорії 3 із хвильовим опором 100 Ом, роз’ємом RJ-45, максимальну довжину фізичного сегмента 100 м, манчестерський код для представлення даних у кабелі, а також деякі інші характеристики середовища й електричних сигналів.

Канальний рівень

На фізичному рівні просто пересилаються біти. При цьому не враховується, що в деяких мережах, у яких лінії зв'язку використовуються (розділяються) поперемінно декількома парами взаємодіючих комп'ютерів, фізичне середовище передачі може бути зайняте. Тому однією з задач канального рівня є перевірка доступності середовища передачі. Іншим завданням канального рівня є реалізація механізмів виявлення й корекції помилок. Для цього на канальному рівні біти групуються в набори, так звані кадри (frames). Канальний рівень забезпечує коректність передачі кожного кадру, поміщаючи спеціальну послідовність бітів у початок і кінець кожного кадру для його виділення, а також обчислює контрольну суму, обробляючи всі байти кадру певним способом і додаючи контрольну суму до кадру. Коли кадр приходить по мережі, одержувач знову обчислює контрольну суму отриманих даних і порівнює результат з контрольною сумою з кадру. Якщо вони збігаються, кадр вважається правильним і приймається. Якщо ж контрольні суми не збігаються, то фіксується помилка. Канальний рівень може не тільки виявляти помилки, але й виправляти їх за рахунок повторної передачі ушкоджених кадрів. Необхідно відзначити, що функція виправлення

помилок не є обов'язковою для канального рівня, тому в деяких протоколах цього рівня вона відсутній, наприклад в Ethernet і Frame Relay.

У протоколах канального рівня, використовуваних у локальних мережах, закладена певна структура зв'язків між комп'ютерами й способи їхньої адресації.

Хоча канальний рівень і забезпечує доставку кадру між будь-якими двома вузлами локальної мережі, він це робить тільки в мережі із зовсім певною топологією зв'язків, саме тією топологією, для якої він був розроблений. До таких типових топологій, підтримуваних протоколами канального рівня локальних мереж, відносяться загальна шина, кільце й зірка, а також структури, отримані з них за допомогою мостів і комутаторів. Прикладами протоколів канального рівня є протоколи Ethernet, Token Ring, FDDI.

У локальних мережах протоколи канального рівня використовуються комп'ютерами, мостами, комутаторами й маршрутизаторами. У комп'ютерах функції канального рівня реалізуються спільними зусиллями мережевих адаптерів і їхніх драйверів.

У глобальних мережах, які рідко мають регулярну топологію, канальний рівень часто забезпечує обмін повідомленнями тільки між двома сусідніми комп'ютерами, з'єднаними індивідуальною лінією зв'язку. Прикладами протоколів «точка-точка» (як часто називають такі протоколи) можуть служити широко розповсюджені протоколи PPP і LAP-B. У таких випадках для доставки повідомлень між кінцевими вузлами через всю мережу використовуються засоби мережевого рівня. Саме так організовані мережі X.25. Іноді в глобальних мережах функції канального рівня в чистому вигляді виділити важко, тому що в тому самому протоколі вони поєднуються з функціями мережевого рівня. Прикладами такого підходу можуть служити протоколи технологій ATM і Frame Relay.

У цілому канальний рівень являє собою досить потужний і закінчений набір функцій по пересиланню повідомлень між вузлами мережі. У деяких

випадках протоколи канального рівня виявляються самодостатніми транспортними засобами й можуть допускати роботу поверх себе безпосередньо протоколів прикладного рівня або додатків, без залучення засобів мережевого й транспортного рівнів. Наприклад, існує реалізація протоколу керування мережею SNMP безпосередньо поверх Ethernet, хоча стандартно цей протокол працює поверх мережевого протоколу IP і транспортного протоколу UDP. Природно, що застосування такої реалізації буде обмеженим – вона не підходить для складених мереж різних технологій, наприклад Ethernet і X.25, і навіть для такої мережі, у якій у всіх сегментах застосовується Ethernet, але між сегментами існують петлевидні зв'язки. А от у двосегментній мережі Ethernet, об'єднаній мостом, реалізація SNMP над канальним рівнем буде цілком працездатною.

Проте для забезпечення якісного транспортування повідомлень у мережах будь-яких топологій і технологій функцій канального рівня виявляється недостатньо, тому в моделі OSI рішення цього завдання покладає на два наступні рівні – мережевий і транспортний.

Канальний рівень забезпечує передачу пакетів даних, що надходять від протоколів верхніх рівнів, вузлу призначення, адресу якого також указує протокол верхнього рівня. Протоколи канального рівня оформляють передані їм пакети в кадри власного формату, поміщаючи зазначену адресу призначення в одне з полів такого кадру, а також супроводжуючи кадр контрольною сумою. Протокол канального рівня має локальний сенс, він призначений для доставки кадрів даних, як правило, у межах мереж із простою топологією зв'язків і однотипною або близькою технологією, наприклад в односегментних мережах Ethernet або ж у багатосегментних мережах Ethernet і Token Ring ієрархічної топології, розділених тільки мостами й комутаторами. В усіх цих конфігураціях адресу призначення має локальний сенс для даної мережі й не змінюється при проходженні кадру від вузла-джерела до вузла-призначення. Можливість передавати дані між локальними мережами різних технологій пов'язана з тим, що в цих

технологіях використовуються адреси однакового формату, до того ж виробники мережевих адаптерів забезпечують унікальність адрес незалежно від технології.

Іншою областю дії протоколів канального рівня є зв'язки типу «точка-точка» глобальних мереж, коли протокол канального рівня відповідальний за доставку кадру безпосередньому сусідові. Адресу в цьому випадку не має принципового значення, а на перший план виходить здатність протоколу відновлювати викривлені й загублені кадри, тому що погана якість територіальних каналів, особливо телефонних, часто вимагає виконання подібних дій.

Якщо ж перераховані вище умови не дотримуються, наприклад зв'язки між сегментами Ethernet мають петлевидну структуру, або поєднувані мережі використовують різні способи адресації, як це має місце в мережах Ethernet і X.25, то протокол канального рівня не може самостійно впоратися із задачею передачі кадру між вузлами й вимагає допомоги протоколу мережевого рівня.

Мережевий рівень

Мережевий рівень служить для утворення єдиної транспортної системи, що поєднує декілька мереж, причому ці мережі можуть використовувати зовсім різні принципи передачі повідомлень між кінцевими вузлами й мати довільну структуру зв'язків. Функції мережевого рівня досить різноманітні. Почнемо їхній розгляд на прикладі об'єднання локальних мереж.

Протоколи канального рівня локальних мереж забезпечують доставку даних між будь-якими вузлами тільки в мережі з відповідною типовою топологією, наприклад топологією ієрархічної зірки. Це дуже жорстке обмеження, що не дозволяє будувати мережі з розвинутою структурою, наприклад мережі, що поєднують кілька мереж підприємства в єдину мережу, або високонадійні мережі, у яких існують надлишкові зв'язки між вузлами. Можна було б ускладнювати протоколи канального рівня для

підтримки петлевидних надлишкових зв'язків, але принцип розподілу обов'язків між рівнями призводить до іншого рішення. Щоб, з одного боку, зберегти простоту процедур передачі даних для типових топологій, а з іншого боку – допустити використання довільних топологій, вводиться додатковий мережевий рівень.

На мережевому рівні сам термін мережа наділяють специфічним значенням. У цьому випадку під мережею розуміється сукупність комп'ютерів, з'єднаних між собою відповідно до однієї зі стандартних типових топологій і які використовують для передачі даних один із протоколів канального рівня, певний для цієї топології.

В середині мережі доставка даних забезпечується відповідним канальним рівнем, а от доставкою даних між мережами займається мережевий рівень, що і підтримує можливість правильного вибору маршруту передачі повідомлення навіть у тому випадку, коли характер структури зв'язків між складовими мережами відрізняється від прийнятого в протоколах канального рівня.

Мережі з'єднуються між собою спеціальними пристроями, що називаються маршрутизаторами. Маршрутизатор – це пристрій, що збирає інформацію про топологію мережевих з'єднань і на її підставі пересилає пакети мережевого рівня в мережу призначення. Щоб передати повідомлення від відправника, що перебуває в одній мережі, одержувачу, що перебуває в іншій мережі, потрібно зробити деяку кількість транзитних передач між мережами, або хопів (hop – стрибок), щоразу вибираючи підходящий маршрут. Таким чином, маршрут являє собою послідовність маршрутизаторів, через які проходить пакет.

На рисунку 1.3 показані чотири мережі, зв'язані трьома маршрутизаторами. Між вузлами А та В даної мережі пролягають два маршрути: перший через маршрутизатори 1 та 3, а другий через маршрутизатори 1, 2 і 3.

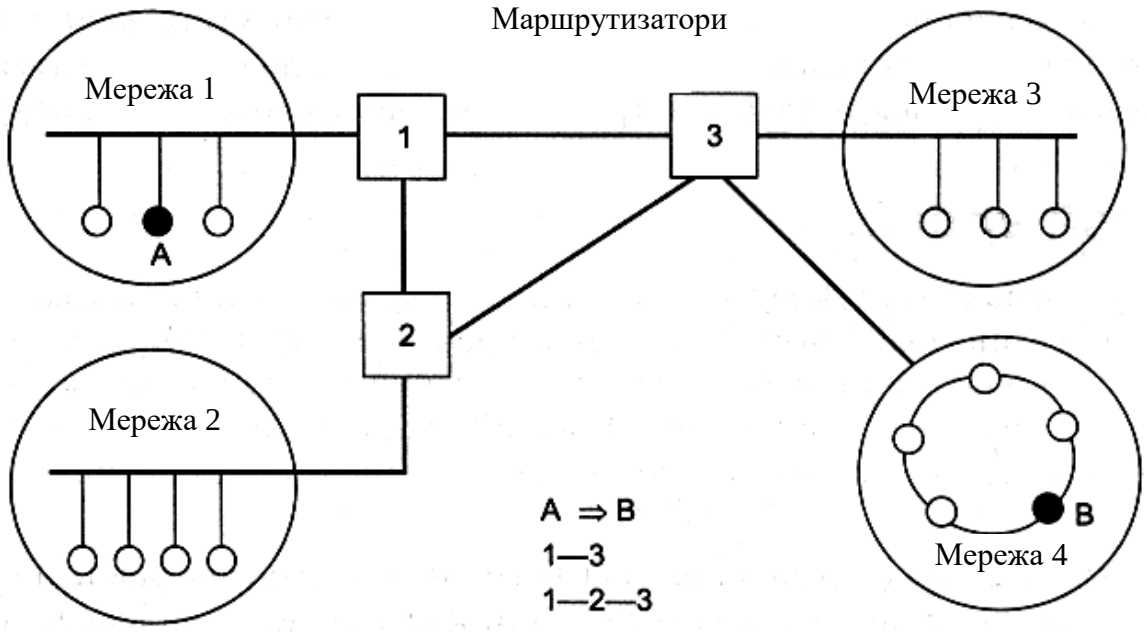


Рисунок 1.3 – Приклад складеної мережі

Проблема вибору найкращого шляху називається маршрутизацією, а її рішення є однією з головних завдань мережевого рівня. Ця проблема ускладнюється тим, що самий короткий шлях не завжди найкращий. Часто критерієм при вибору маршруту є час передачі даних по цьому маршруту; він залежить від пропускної здатності каналів зв'язку та інтенсивності трафіку, що може змінюватися з часом. Деякі алгоритми маршрутизації намагаються пристосовуватися до змін навантаження, у той час як інші приймають рішення на основі середніх показників за тривалий час. Вибір маршруту може здійснюватися й за іншими критеріями, наприклад надійності передачі.

У загальному випадку функції мережевого рівня ширше, ніж функції передачі повідомлень по зв'язках з нестандартною структурою, які ми зараз розглянули на прикладі об'єднання декількох локальних мереж. Мережевий рівень вирішує також задачу узгодження різних технологій, спрощення адресації у великих мережах і створення надійних і гнучких бар'єрів на шляху небажаного трафіку між мережами.

Повідомлення мережевого рівня прийнято називати пакетами (packet). При організації доставки пакетів на мережевому рівні використовується поняття «номер мережі». У цьому випадку адресу одержувача складається зі старшої частини – номера мережі й молодшої – номера вузла в цій мережі. Всі вузли однієї мережі повинні мати ту саму старшу частину адреси, тому терміну «мережа» на мережевому рівні можна дати й інше, більш формальне визначення: мережа – це сукупність вузлів, мережева адреса яких містить той самий номер мережі.

На мережевому рівні визначаються два види протоколів. Перший вид – мережеві протоколи (routed protocols) – реалізують просування пакетів через мережу. Саме ці протоколи звичайно мають на увазі, коли говорять про протоколи мережевого рівня. Однак часто до мережевого рівня відносять і інший вид протоколів, що називаються протоколами обміну маршрутною інформацією або просто протоколами маршрутизації (routing protocols). За допомогою цих протоколів маршрутизатори збирають інформацію про топологію міжмережевих з'єднань. Протоколи мережевого рівня реалізуються програмними модулями операційної системи, а також програмними й апаратними засобами маршрутизаторів.

На мережевому рівні працюють протоколи ще одного типу, які відповідають за відображення адреси вузла, використовуваного на мережевому рівні, у локальну адресу мережі. Такі протоколи часто називають протоколами дозволу адрес (Address Resolution Protocol, ARP). Іноді їх відносять не до мережевого рівня, а до канального, хоча тонкості класифікації не змінюють їхньої суті.

Транспортний рівень

На шляху від відправника до одержувача пакети можуть бути викривлені або загублені. Хоча деякі додатки мають власні засоби обробки помилок, існують і такі, які воліють відразу мати справу з надійним з'єднанням. Транспортний рівень забезпечує додаткам або верхнім рівням стека – прикладному й сеансовому – передачу даних з тим ступенем

надійності, який їм потрібний. Модель OSI визначає п'ять класів сервісу, надаваних транспортним рівнем. Ці види сервісу відрізняються якістю надаваних послуг: терміновістю, можливістю відновлення перерваного зв'язку, наявністю засобів мультиплексування декількох з'єднань між різними прикладними протоколами через загальний транспортний протокол, а головне – здатністю до виявлення й виправлення помилок передачі, таких як викривлення, втрата й дублювання пакетів.

Вибір класу сервісу транспортного рівня визначається, з одного боку, тим, у якому ступені завдання забезпечення надійності вирішується самими додатками й протоколами більш високих, ніж транспортний, рівнів, а з іншого боку, цей вибір залежить від того, наскільки надійною є система транспортування даних у мережі, забезпечувана рівнями, розташованими нижче транспортного – мережевим, канальним і фізичним. Так, наприклад, якщо якість каналів передачі зв'язку дуже висока і ймовірність виникнення помилок, не виявлених протоколами більш низьких рівнів, невелика, то розумно скористатися одним з полегшених сервісів транспортного рівня, не обтяжених численними перевірками, квитуванням та іншими прийомами підвищення надійності. Якщо ж транспортні засоби нижніх рівнів дуже ненадійні, то доцільно звернутися до найбільш розвиненого сервісу транспортного рівня, що працює, використовуючи максимум засобів для виявлення й усунення помилок, включаючи попереднє встановлення логічного з'єднання, контроль доставки повідомлень по контрольних сумах і циклічну нумерацію пакетів, встановлення тайм-аутів доставки й т.п.

Як правило, всі протоколи, починаючи із транспортного рівня й вище, реалізуються програмними засобами кінцевих вузлів мережі – компонентами їх мережевих операційних систем. Як приклад транспортних протоколів можна привести протоколи TCP і UDP стека TCP/IP і протокол SPX стека Novell.

Протоколи нижніх чотирьох рівнів узагальнено називають мережевим транспортом або транспортною підсистемою, тому що вони повністю

вирішують завдання транспортування повідомлень із заданим рівнем якості в складених мережах з довільною топологією й різними технологіями. Три верхні рівні, що залишилися вирішують завдання надання прикладних сервісів на підставі наявної транспортної підсистеми.

Сеансовий рівень

Сеансовий рівень забезпечує керування взаємодією: фіксує, яка зі сторін є активною в даний момент, надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у випадку відмови можна було повернутися назад до останньої контрольної точки, а не починати все з початку. На практиці деякі додатки використовують сеансовий рівень, і він рідко реалізується у вигляді окремих протоколів, хоча функції цього рівня часто поєднують із функціями прикладного рівня й реалізують в одному протоколі.

Представницький рівень

Представницький рівень має справу з формою подання переданої по мережі інформації, не міняючи при цьому її змісту. За рахунок рівня подання інформація, передана прикладним рівнем однієї системи, завжди зрозуміла прикладному рівню іншої системи. За допомогою засобів даного рівня протоколи прикладних рівнів можуть перебороти синтаксичні розходження в поданні даних або ж розходження в кодах символів, наприклад кодів ASCII і EBCDIC. На цьому рівні може виконуватися шифрування й дешифрування даних, завдяки яким таємність обміну даними забезпечується відразу для всіх прикладних служб. Прикладом такого протоколу є протокол Secure Socket Layer (SSL), що забезпечує таємний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

Прикладний рівень

Прикладний рівень – це в дійсності просто набір різноманітних протоколів, за допомогою яких користувачі мережі одержують доступ до поділюваних ресурсів, таких як файли, принтери або гіХарковікстові веб-сторінки, а також організують свою спільну роботу, наприклад, по протоколу

електронної пошти. Одиниця даних, якою оперує прикладний рівень, звичайно називається повідомленням.

Існує дуже велика розмаїть служб прикладного рівня. Наведемо як приклад хоча б декілька найпоширеніших реалізацій файлових служб: NCP в операційній системі Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP і TFTP, що входять у стек TCP/IP.

Мережозалежні та мережонезалежні рівні моделі OSI

Функції всіх рівнів моделі OSI можуть бути віднесені до однієї із двох груп: або до функцій, що залежать від конкретної технічної реалізації мережі, або до функцій, орієнтованих на роботу з додатками.

Три нижніх рівні – фізичний, канальний і мережевий – є мережозалежними, тобто протоколи цих рівнів тісно пов'язані з технічною реалізацією мережі й використовуваним комунікаційним устаткуванням. Наприклад, перехід на устаткування FDDI означає повну зміну протоколів фізичного й канального рівнів у всіх вузлах мережі.

Три верхніх рівні – прикладний, представницький і сеансів – орієнтовані на додатки й мало залежать від технічних особливостей побудови мережі. На протоколи цих рівнів не впливають які б то не було зміни в топології мережі, заміна устаткування або перехід на іншу мережеву технологію. Так, перехід від Ethernet на високошвидкісну технологію lOOVG-AnyLAN не вимагає ніяких змін у програмних засобах, що реалізують функції прикладного, представницького й сеансового рівнів.

Транспортний рівень є проміжним, він приховує деталі функціонування нижніх рівнів від верхніх. Це дозволяє розробляти додатки, що не залежать від технічних засобів безпосереднього транспортування повідомлень.

РОЗДІЛ 2. ТЕХНОЛОГІЇ ФІЗИЧНОГО РІВНЯ

Лінії зв’язку та їх характеристики

При побудові мереж застосовуються лінії зв'язку, що використовують різне фізичне середовище: телефонні й телеграфні дроти, підвішені в повітрі, мідні коаксіальні кабелі, мідні кручені пари, волоконно-оптичні кабелі, радіохвилі. При виборі того чи іншого типу ліній зв'язку розроблювачі насамперед враховують їхні технічні характеристики, вартість, а також простоту монтажу.

Лінія зв'язку (лінія передачі даних) – це фізичне середовище, по якому передаються інформаційні сигнали, апаратура передачі даних та проміжна апаратура. В одній лінії зв'язку можна утворити декілька каналів зв'язку (віртуальних або логічних), наприклад шляхом частотного або часового поділу каналів.

Фізичне середовище передачі даних може являти собою кабель, тобто набір дротів, ізоляційних і захисних оболонок, сполучних роз’ємів, а також земну атмосферу або космічний простір, через які поширюються інформаційні сигнали. У сучасних телекомунікаційних системах інформація передається за допомогою електричного струму або напруги, радіосигналів або світлових сигналів – всі ці фізичні процеси являють собою коливання електромагнітного поля різної частоти й природи.

Залежно від середовища передачі дані лінії зв'язку розділяються на:

– дротові (повітряні);

– кабельні (мідні й волоконно-оптичні);

– бездротові (радіоканали наземного й супутникового зв'язку).

Дротові лінії зв'язку

Дротові (повітряні) лінії зв'язку використовуються для передачі телефонних і телеграфних сигналів, а також для передачі комп'ютерних даних. Ці лінії зв'язку застосовуються як магістральні лінії зв'язку.

По дротових лініях зв'язку можуть бути організовані аналогові й цифрові канали передачі даних. Швидкість передачі по дротових лініях "простої старої телефонної лінії" (POST – Primitive Old Telephone System) є дуже низкою. Крім того, до недоліків цих ліній відносяться низька перешкодозахищеність і можливість простого несанкціонованого підключення до мережі.

Кабельні канали зв'язку

Кабельні лінії зв'язку мають досить складну структуру. Кабель складається із дротів, укладених у декілька шарів ізоляції. У комп'ютерних мережах використовуються три типи кабелів.

Кручена пара – кабель зв'язку, що являє собою кручену пару мідних дротів (або декілька пар дротів), укладених в екрановану оболонку. Пари дротів скручуються між собою з метою зменшення наведень.

Рисунок 2.1 – Приклад крученої пари

Кручена пара є досить завадостійкою. Існує два типи цього кабелю: неекранована кручена пара UTP і екранована кручена пара STP.

Характерним для цього кабелю є простота монтажу. Даний кабель є найдешевшим і розповсюдженим видом зв'язку, що знайшов широке застосування в найпоширеніших локальних мережах з архітектурою Ethernet, побудованих за топологією типу «зірка». Кабель підключається до мережевих пристроїв за допомогою з'єднувача RJ45.

Кабель використовується для передачі даних на швидкості 10 Мбіт/с і 100 Мбіт/с. Кручена пара звичайно використовується для зв'язку на відстань не більше кількох сотень метрів. До недоліків кабелю "кручена пара" можна віднести можливість простого несанкціонованого підключення до мережі.

Коаксіальний кабель – це кабель із центральним мідним дротом, що оточений шаром ізолюючого матеріалу для того, щоб відокремити центральний дріт від зовнішнього екрана (мідної оплітки або шару алюмінієвої фольги). Зовнішній екран кабелю покривається ізоляцією.

Рисунок 2.2 – Приклад коаксіального кабелю

Існує два типи коаксіального кабелю: тонкий коаксіальний кабель діаметром 5 мм і товстий коаксіальний кабель діаметром 10 мм. У товстого коаксіального кабелю згасання менше, ніж у тонкого. Вартість коаксіального кабелю вища вартості крученої пари й виконання монтажу мережі складніше, ніж крученою парою.

Коаксіальний кабель застосовується, наприклад, у локальних мережах з архітектурою Ethernet, побудованих за топологією типу «загальна шина». Коаксіальний кабель більш завадозахищений, ніж кручена пара й знижує власне випромінювання. Пропускна здатність – 50-100 Мбіт/с. Припустима довжина лінії зв'язку – кілька кілометрів. Несанкціоноване підключення до коаксіального кабелю складніше, ніж до крученої пари.

Кабельні оптоволоконні канали зв'язку

Оптоволоконний кабель – це оптичне волокно на кремнієвій або пластмасовій основі, укладене в матеріал з низьким коефіцієнтом переломлення світла, що закритий зовнішньою оболонкою.

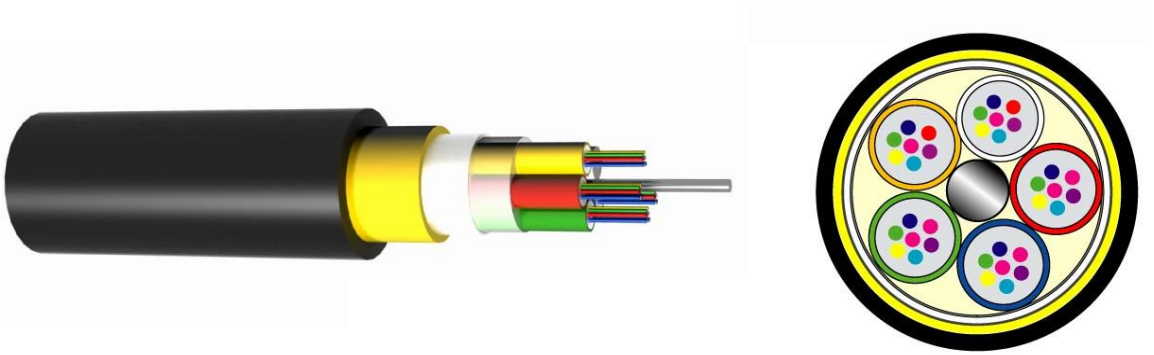


Рисунок 2.3 – Приклад оптоволоконного кабелю

Оптичне волокно передає сигнали тільки в одному напрямку, тому кабель складається із двох волокон. На передаючому кінці оптоволоконного кабелю потрібне перетворення електричного сигналу у світловий, а на приймаючому кінці зворотне перетворення.

Основна перевага цього типу кабелю – надзвичайно високий рівень перешкодозахищеності й відсутність випромінювання. Несанкціоноване підключення дуже складне. Швидкість передачі даних 3 Гбіт/с. Основні недоліки оптоволоконного кабелю – це складність його монтажу, невелика механічна міцність і чутливість до іонізуючих випромінювань.

Бездротові канали зв'язку (радіоканали наземного й супутникового зв'язку)

Радіоканали наземного (радіорелейного й стільникового) і супутникового зв'язку створюються за допомогою передавача й приймача радіохвиль і відносяться до технології бездротової передачі даних.

Радіорелейні канали зв'язку

Радіорелейні канали зв'язку складаються з послідовності станцій, що є ретрансляторами. Зв'язок здійснюється в межах прямої видимості, дальність між сусідніми станціями – до 50 км. Цифрові радіорелейні лінії зв'язку (ЦРРЗ) застосовуються в якості регіональних і місцевих систем зв'язку й передачі даних, а також для зв'язку між базовими станціями стільникового зв'язку.

Супутникові канали зв'язку

У супутникових системах використовуються антени надвисокочастотного діапазону (рос. «СВЧ-диапазона») частот для прийому радіосигналів від наземних станцій і ретрансляції цих сигналів назад на наземні станції. У супутникових мережах використовуються три основних типи супутників, які перебувають на геостаціонарних орбітах, середніх або низьких орбітах. Супутники запускаються, як правило, групами. Рознесені один від одного вони можуть забезпечити охоплення майже всієї поверхні Землі. Робота супутникового каналу передачі даних представлена на рисунку 2.4.

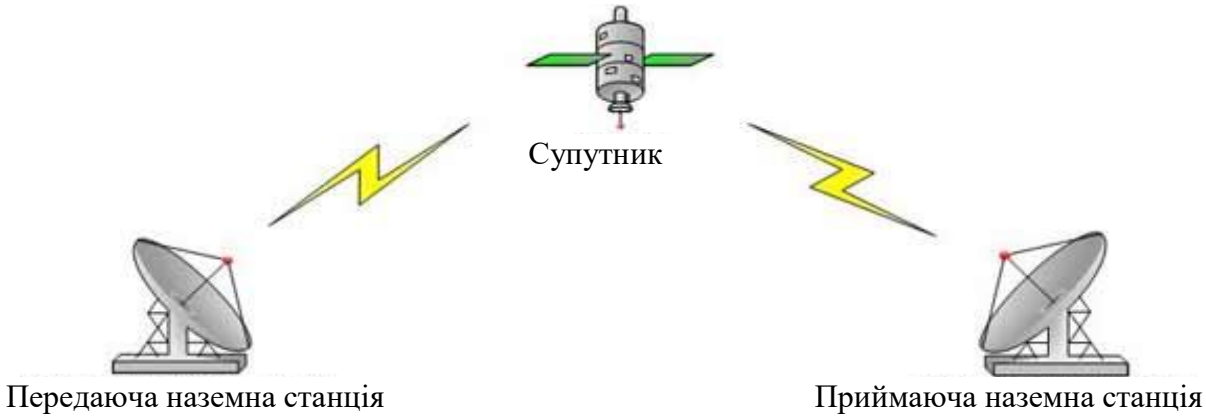


Рисунок 2.4 – Приклад супутникового каналу зв’язку

Доцільніше використовувати супутниковий зв'язок для організації каналу зв'язку між станціями, розташованими на дуже великих відстанях, і можливості обслуговування абонентів у самих важкодоступних точках. Пропускна здатність висока – кілька десятків Мбіт/с.

Стільникові канали зв'язку

Радіоканали стільникового зв'язку будуються за тими ж принципами, що й стільникові телефонні мережі. Стільниковий зв'язок – це бездротова телекомунікаційна система, що складається з мережі наземних базових приймально-передавальних станцій і стільникового комутатора (або центра комутації мобільного зв'язку).

Базові станції підключаються до центра комутації, що забезпечує зв'язок, як між базовими станціями, так і з іншими телефонними мережами й з глобальною мережею Інтернет. По виконуваних функціях центр комутації аналогічний звичайній АТС дротового зв'язку.

LMDS (Local Multipoint Distribution System) – це стандарт стільникових мереж бездротової передачі інформації для фіксованих абонентів. Система будується по стільниковому принципу, одна базова станція дозволяє охопити район радіусом декілька кілометрів (до 10 км) і підключити кілька тисяч абонентів. Самі базові станції поєднуються одна з одною високошвидкісними наземними каналами зв'язку або радіоканалами. Швидкість передачі даних до 45 Мбіт/с.

Радіоканали WiMAX (Worldwide Interoperability for Microwave Access) аналогічні Wi-Fi. WiMAX, на відміну від традиційних технологій радіодоступу, працює й на відбитому сигналі, поза прямою видимістю базової станції. Експерти вважають, що мобільні мережі WiMAX відкривають набагато більш цікаві перспективи для користувачів, ніж фіксований WiMAX, призначений для корпоративних замовників. Інформацію можна передавати на відстані до 50 км зі швидкістю до 70 Мбіт/с.

Радіоканали MMDS (Multichannel Multipoint Distribution System). Ці системи здатні обслуговувати територію в радіусі 50-60 км, при цьому пряма видимість передавача оператора є не обов'язковою. Середня гарантована швидкість передачі даних становить 500 Кбіт/с – 1 Мбіт/с, але можна забезпечити до 56 Мбіт/с на один канал.

Радіоканали для локальних мереж. Стандартом бездротового зв'язку для локальних мереж є технологія Wi-Fi. Wi-Fi забезпечує підключення у двох режимах: точка-точка (для підключення двох ПК) і інфраструктурне з'єднання (для підключення декілька ПК до однієї точки доступу). Швидкість обміну даними до 11 Мбіт/с при підключенні точка-точка й до 54 Мбіт/с при інфраструктурному з'єднанні.

Радіоканали Bluetooth – це технологія передачі даних на короткі відстані (не більше 10 м) і може бути використана для створення домашніх мереж. Швидкість передачі даних не перевищує 1 Мбіт/с.

Апаратура ліній зв'язку

Апаратура передачі даних, або *АПД (Data Circuit Terminating Equipment, DCE)* у комп'ютерних мережах безпосередньо приєднує комп'ютери або локальні мережі користувача до лінії зв'язку і є, таким чином, прикордонним устаткуванням. Традиційно апаратуру передачі даних включають до складу лінії зв'язку. Прикладами DCE є модеми, термінальні адаптери мереж ISDN, пристрої підключення до цифрових каналів. Звичайно DCE працює на фізичному рівні, відповідаючи за передачу інформації у фізичне середовище (у лінію) і прийом з неї сигналів потрібної форми й потужності.

Апаратура користувача лінії зв'язку, що виробляє дані для передачі по лінії зв'язку і підключається безпосередньо до апаратури передачі даних, носить узагальнену назву *кінцеве обладнання (Data Terminal Equipment, DTE).* Прикладом DTE можуть служити комп'ютери, комутатори або маршрутизатори. Цю апаратуру не включають до складу лінії зв'язку.

Поділ устаткування на класи DCE і DTE у локальних мережах є досить умовним. Наприклад, адаптер локальної мережі можна вважати як приналежністю комп'ютера, тобто DTE, так і складовою частиною каналу зв'язку, тобто DCE. Точніше, одна частина мережевого адаптера виконує функції DTE, а інша частина, безпосередньо приймаюча і передаюча сигнали, відноситься до DCE.

Проміжна апаратура звичайно використовується на лініях зв'язку великої довжини. Вона вирішує дві основні задачі:

– поліпшення якості сигналу;

– створення постійного складеного каналу зв'язку між двома абонентами мережі.

У локальних мережах проміжна апаратура може зовсім не використовуватися, якщо довжина фізичного середовища – кабелів або радіоефіра – дозволяє одному мережевому адаптеру приймати сигнали безпосередньо від іншого мережевого адаптера без проміжного посилення. В іншому випадку застосовуються пристрої типу повторювачів і концентраторів.

У глобальних мережах необхідно забезпечити якісну передачу сигналів на відстані в сотні й тисячі кілометрів. Тому без підсилювачів (що підвищують потужність сигналів) і регенераторів (поряд з підвищенням потужності імпульсних сигналів, відновлюють їх форму, що спотворюється при передачі на велику відстань), встановлених через певні відстані, побудувати територіальну лінію зв'язку неможливо. У глобальній мережі необхідна також і проміжна апаратура іншого роду – мультиплексори, демультиплексори та комутатори. Ця апаратура вирішує друге зазначене завдання, тобто створює між двома абонентами мережі безперервний складений канал з відрізків фізичного середовища – кабелів з підсилювачами. Причому деякі із цих відрізків, що володіють широкою смугою пропускання, наприклад відрізки волоконно-оптичного або коаксіального кабелю, одночасно беруть участь в утворенні відразу декількох складених каналів. Такий високошвидкісний канал, по якому передаються одночасно дані від великого числа порівняно низькошвидкісних абонентських ліній, звичайно називають ущільненим каналом. Наявність проміжної комутаційної апаратури рятує творців глобальної мережі від необхідності прокладати окрему кабельну лінію для кожної пари вузлів мережі.

Проміжна апаратура каналу зв'язку прозора для користувача, він її не помічає й не враховує у своїй роботі. Для нього важлива тільки якість отриманого каналу в цілому, що впливає на швидкість і надійність передачі дискретних даних. У дійсності ж невидима користувачами проміжна апаратура утворює складну мережу. Цю мережу називають *первинною мережею,* тому що сама по собі вона ніяких високорівневих служб

(наприклад, файлової або передачі голосу) не підтримує, а тільки є основою для побудови комп'ютерних, телефонних або інших мереж, які іноді називають *накладеними,* або *вторинними,* мережами.

Залежно від типу проміжної апаратури всі лінії зв'язку діляться на аналогові й цифрові. В *аналогових лініях* проміжна апаратура призначена для посилення аналогових сигналів, тобто сигналів, які мають безперервний діапазон значень. Такі лінії зв'язку традиційно застосовувалися в телефонних мережах для зв'язку АТС між собою. Для створення високошвидкісних каналів, які мультиплексують декілька низькошвидкісних аналогових абонентських каналів, при аналоговому підході звичайно використовується техніка частотного мультиплексування (Frequency Division Multiplexing, FDM).

У *цифрових лініях зв'язку* передані сигнали мають кінцеве число станів. Як правило, елементарний сигнал, тобто сигнал, переданий за один такт роботи передавальної апаратури, має 2, 3 або 4 стани, які передаються в лініях зв'язку імпульсами або потенціалами прямокутної форми. За допомогою таких сигналів передаються як комп'ютерні дані, так і оцифровані мова й зображення (саме через загальний вид представлення інформації сучасними комп'ютерними, телефонними й телевізійними мережами стали можливі загальні первинні мережі). У цифрових каналах зв'язку використовується спеціальна проміжна апаратура – регенератори, які поліпшують форму імпульсів і забезпечують їх ресинхронізацію, тобто відновлюють період їхнього проходження. Проміжна апаратура мультиплексування й комутації первинних мереж працює за принципом часового мультиплексування каналів (Time Division Multiplexing, TDM), коли кожному низькошвидкісному каналу виділяється певна частка часу (тайм-слот, або квант) високошвидкісного каналу.

В наш час аналогові канали стали застосовуватися в первинних мережах нового типу, що використовують метод мультиплексування по довжині хвилі (Wavelength Division Multiplexing, WDM). У первинних

мережах WDM кожний канал передає свою інформацію за допомогою світлової хвилі певної довжини (і, відповідно, частоти). Такий канал також називається спектральним каналом, тому що йому виділяється певна смуга спектра світлового випромінювання. Апаратура передачі дискретних комп'ютерних даних по аналогових лініях зв'язку істотно відрізняється від апаратури такого ж призначення, призначеної для роботи із цифровими лініями. Аналогова лінія зв'язку призначена для передачі сигналів довільної форми й не пред'являє ніяких вимог до способу представлення одиниць і нулів апаратурою передачі даних (це справедливо для мереж FDM і WDM/DWDM), а в цифровій – всі параметри переданих лінією імпульсів стандартизовані. Інакше кажучи, на цифрових лініях зв'язку протокол фізичного рівня визначений, а на аналогових лініях – ні (є й виключення із цього правила, деякі мережі DWDM для передачі інформації зі спектрального каналу вимагають цифрового кодування певного виду).

Характеристики ліній зв'язку

До основних характеристик ліній зв'язку відносяться *параметри поширення* й *параметри впливу.* Перші характеризують процес поширення корисного сигналу залежно від внутрішніх параметрів лінії, наприклад погонної індуктивності мідного кабелю. Другі описують ступінь впливу на корисний сигнал інших сигналів – зовнішніх перешкод, перешкод від інших пар дротів у мідному кабелі. Ті й інші характеристики важливі, тому що сигнал на виході лінії зв'язку завжди є результатом впливу на вихідний сигнал як внутрішніх, так і зовнішніх факторів.

У кожній із цих груп можна виділити первинні й вторинні параметри. Первинні параметри описують фізичну природу лінії зв'язку, наприклад погонний активний опір, погонну індуктивність, погонну ємність і погонну дротовість ізоляції мідного кабелю, або ж залежність коефіцієнта переломлення оптичного волокна від відстані від оптичної осі. Вторинні параметри виражають деякий узагальнений результат процесу поширення сигналу по лінії зв'язку й не залежать від її природи. Наприклад, важливим

вторинним параметром поширення будь-якої лінії зв'язку є ступінь ослаблення потужності сигналу при проходженні ним певної відстані уздовж лінії зв'язку – так зване згасання сигналу. Для мідних кабелів не менш важливий і такий вторинний параметр впливу, як ступінь ослаблення, перешкоди від сусідньої крученої пари, – він дозволяє оцінити, чи не будуть викликати передані по одній парі сигнали помилкове спрацьовування приймача, підключеного до сусідньої пари на тій же стороні кабелю, що й передавач.

Згасання й хвильовий опір

Ступінь викривлення синусоїдальних сигналів лініями зв'язку оцінюється за такими характеристиками, як згасання й смуга пропускання.

Згасання показує, наскільки зменшується потужність еталонного синусоїдального сигналу на виході лінії зв'язку стосовно потужності сигналу на вході цієї лінії. Згасання *A* звичайно виміряється в децибелах, дБ (decibel, d) і обчислюється за наступною формулою:

$$A = 10 \log_{10} P_{вих}/P_{вх},$$

де:

$P_{вих}$ – потужність сигналу на виході лінії,

$P_{вх}$ – потужність сигналу на вході лінії.

Тому що потужність вихідного сигналу кабелю без проміжних підсилювачів завжди менша, ніж потужність вхідного сигналу, згасання кабелю завжди є від’ємною величиною.

Увага! Згасання завжди має від’ємне значення, однак знак мінус часто упускають, що може викликати плутанину. Так, абсолютно коректне твердження, що чим більше затухання (з врахуванням знаку), тим краще якість лінії зв’язку. Якщо ж ігнорувати знак, тобто брати абсолютне значення даної величини, то у більш якісної лінії зв’язку затухання менше.

Згасання є більш узагальненою характеристикою лінії зв'язку, тому що дозволяє судити не про точну форму сигналу, а про його потужність (інтегральної результуючої від форми сигналу). Але на практиці згасання

частіше використовується як характеристика ліній зв'язку, зокрема, у стандартах на таку важливу складову лінії зв'язку, як кабель, згасання є однією з основних характеристик.

Звичайно згасанням характеризують пасивні ділянки лінії зв'язку, що складаються з кабелів і кросових секцій, без підсилювачів і регенераторів. Наприклад, кабель для внутрішньої проводки в будинках на крученій парі категорії 5, на якій працюють практично всі технології локальних мереж, характеризується згасанням не нижче –23,6 Дб для частоти 100 Мгц при довжині кабелю 100 м. Оптичний кабель має істотно більш низькі (по абсолютній величині) величини згасання, звичайно в діапазоні від 0,2 до 3 Дб при довжині кабелю в 1000 м.

Як характеристику потужності передавача часто використовують абсолютний рівень потужності сигналу. Рівень потужності, як і згасання, виміряється в децибелах. При цьому як базове значення потужності сигналу, щодо якого виміряється поточна потужність, приймається значення в 1 мВт. Таким чином, рівень потужності *p* обчислюється за наступною формулою:

$$p = 10 \lg P/1 \text{ мВт } [\text{дБм}],$$

де:

P – потужність сигналу в міліватах,

дБм (dBm) – одиниця вимірювання рівня потужності (децибел на 1 мВт).

Важливим вторинним параметром поширення мідної лінії зв'язку є її хвильовий опір. Цей параметр являє собою повний (комплексний) опір, що зустрічає електромагнітна хвиля певної частоти при поширенні уздовж однорідного ланцюга. Хвильовий опір виміряється в омах і залежить від таких первинних параметрів лінії зв'язку, як активний опір, погонна індуктивність і погонна ємність, а також від частоти самого сигналу. Вихідний опір передавача повинний бути погоджений із хвильовим опором лінії, інакше згасання сигналу буде надмірно великим.

Завадостійкість і ймовірність

Завадостійкість лінії визначає її здатність зменшувати рівень перешкод, створюваних у зовнішньому середовищі або на внутрішніх дротах самого кабелю. Завадостійкість лінії залежить від типу використовуваного фізичного середовища, а також від екрануючих й пригнічуючих перешкод засобів самої лінії. Найменш завадостійкими є радіолінії, доброю стійкістю володіють кабельні лінії й відмінною – волоконно-оптичні лінії, малочутливі до зовнішнього електромагнітного випромінювання. Звичайно для зменшення перешкод, що з'являються через зовнішні електромагнітні поля, дроти екранують і/або скручують. Параметри, що характеризують завадостійкість, відносяться до параметрів впливу лінії зв'язку.

Первинними параметрами впливу мідного кабелю є електричний і магнітний зв'язок. Електричний зв'язок визначається відношенням наведеного струму в підданому впливу ланцюзі до напруги, що діє в впливаючому ланцюзі. Магнітний зв'язок – це відношення електрорушійної сили, наведеної в підданому впливу ланцюзі, до струму у впливаючому ланцюзі. Результатом електричного й магнітного зв'язку є наведені сигнали (наведення) у підданому впливу ланцюзі. Існує декілька різних параметрів, що характеризують стійкість кабелю до наведень.

Перехресні наведення на ближньому кінці (Near End Cross Talk, NEXT) визначають стійкість кабелю в тому випадку, коли наведення утворюється в результаті дії сигналу, що генерується передавачем, підключеним до однієї із сусідніх пар на тому ж кінці кабелю, на якому працює підключений до підданого впливу пари приймач (рис. 2.5). Показник NEXT, виражений у децибелах, дорівнює 10 lg $P_{вих}/P_{нав,}$ де $P_{вих}$ – потужність вихідного сигналу, $P_{нав}$ – потужність наведеного сигналу. Чим менше значення NEXT, тим краще кабель. Так, для крученої пари категорії 5 показник NEXT повинен бути менше –27 дб на частоті 100 Мгц.

Перехресні наведення на дальньому кінці (Far End Cross Talk, FEXT) дозволяють оцінити стійкість кабелю до наведень для випадку, коли

передавач і приймач підключені до різних кінців кабелю (рис. 2.5). Очевидно, що цей показник повинен бути краще, ніж NEXT, тому що до далекого кінця кабелю сигнал приходить ослаблений згасанням кожної пари.

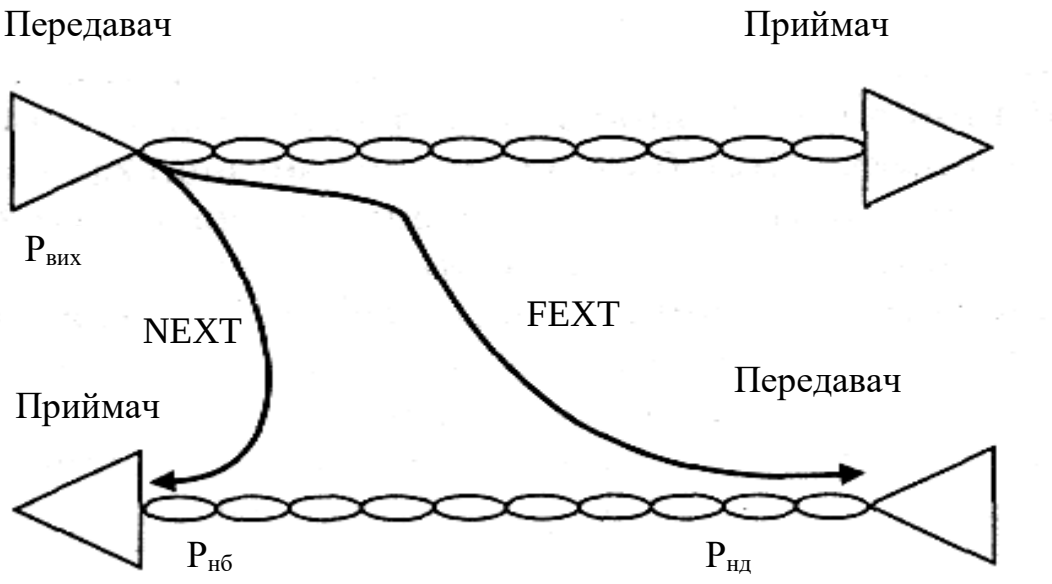


Рисунок 2.5 – Перехідне згасання

$P_{вих}$ – потужність сигналу на виході передавача;

$P_{нб}$ – наведення на ближньому кінці кабеля;

$P_{нд}$ – наведення на дальньому кінці кабеля.

Показники NEXT і FEXT звичайно використовують відносно до кабелю, що складається з декількох кручених пар, тому що в цьому випадку взаємні наведення однієї пари на іншу можуть досягати значних величин. Для одинарного коаксіального кабелю (що складається з однієї екранованої жили) цей показник не має сенсу, а для подвійного коаксіального кабелю він також не застосовується внаслідок високого ступеня захищеності кожної жили. Оптичні волокна також не створюють помітних перешкод один для одного. У зв'язку з тим, що в деяких нових технологіях використовується передача даних одночасно по декількох кручених парах, останнім часом стали застосовуватися також показники перехресних наведень із приставкою

PS *(PowerSUM),* такі як PS NEXT і PS FEXT. Ці показники відображають стійкість кабелю до сумарної потужності перехресних наведень на одну з пар кабелю від всіх інших передаючих пар.

Застосовується також такий практично важливий показник, як *захищеність кабелю (ACR)*. Захищеність визначається як різниця між рівнями корисного сигналу й перешкод. Чим більше значення захищеності кабелю, тим з потенційно більш високою швидкістю можна передавати дані по ньому.

Ймовірність передачі даних характеризує ймовірність викривлення для кожного переданого біта даних. Іноді цей же показник називають *інтенсивністю бітових помилок (Bit Error Rate, BER).* Величина BER для каналів зв'язку без додаткових засобів захисту від помилок (наприклад, самокорегуючих кодів або протоколів з повторною передачею викривлених кадрів) становить, як правило, 10^{-4}-10^{-6}, в оптоволоконних лініях зв'язку – 10^{-9}. Значення вірогідності передачі даних, наприклад, в 10^{-4} говорить про те, що в середньому з 10 000 біт спотворюється значення одного біта.

Викривлення бітів відбуваються як через наявність перешкод на лінії, так і через викривлення форми сигналу обмеженою смугою пропускання лінії. Тому для підвищення вірогідності переданих даних потрібно підвищувати ступінь перешкодозахищеності лінії, знижувати рівень перехресних наведень у кабелі, а також використовувати більш широкосмугові лінії зв'язку.

Смуга пропускання

Смуга пропускання – це ще одна вторинна характеристика, що, з одного боку, безпосередньо залежить від згасання, а з іншого боку, прямо впливає на такий найважливіший показник лінії зв'язку, як максимально можлива швидкість передачі інформації.

Смуга пропускання – це безперервний діапазон частот, для якого згасання не перевищує деяку заздалегідь задану межу. Тобто смуга пропускання визначає діапазон частот синусоїдального сигналу, при яких

цей сигнал передається по лінії зв'язку без значних перекручувань (часто граничними частотами вважаються частоти, на яких потужність вихідного сигналу зменшується у два рази стосовно вхідного, що відповідає загасанню в –3 дБ). Ширина смуги пропускання найбільшою мірою впливає на максимально можливу швидкість передачі інформації з лінії зв'язку.

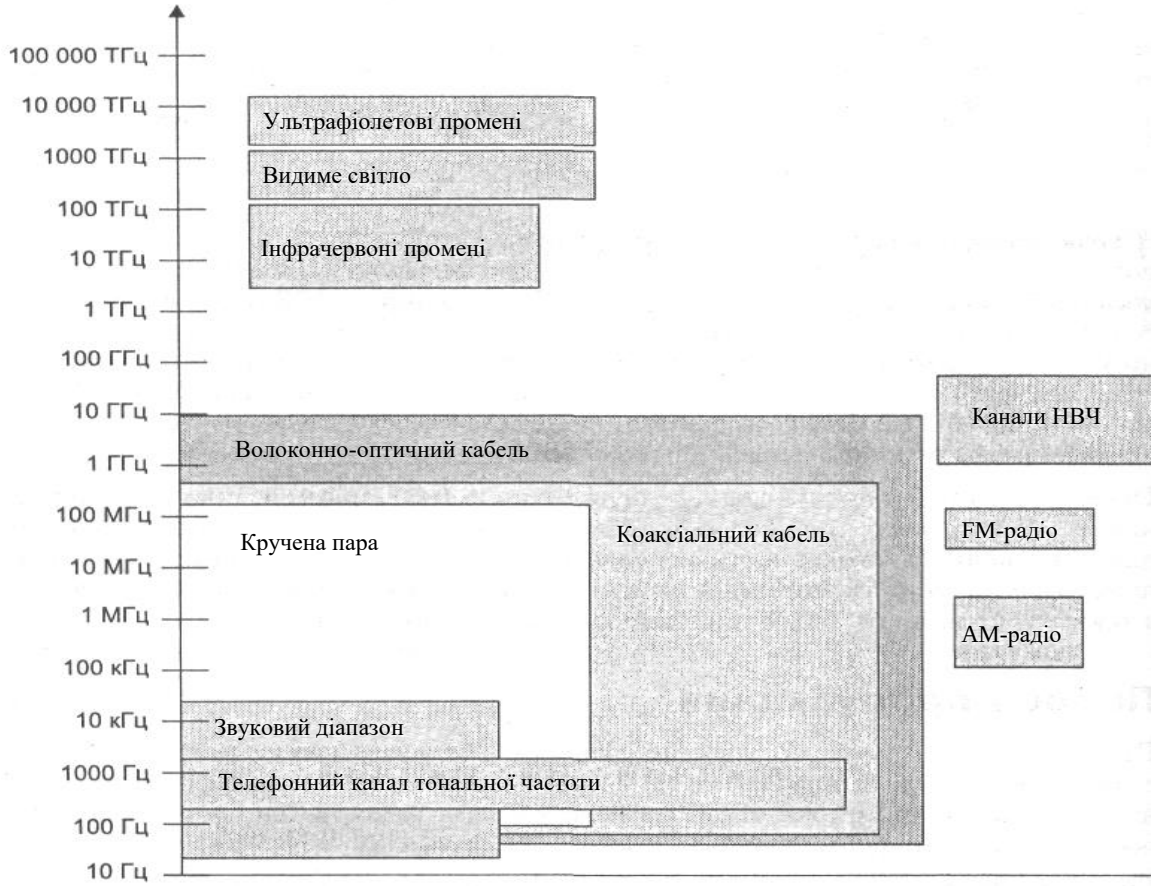


Рисунок 2.6 – Смуги пропускання ліній зв'язку й популярні частотні діапазони

Смуга пропускання залежить від типу лінії і її довжини. На рисунку 2.6 показані смуги пропускання ліній зв'язку різних типів, а також найбільш часто використовувані в техніці зв'язку частотні діапазони.

Пропускна здатність

Пропускна здатність (кількість бітів інформації, передана в одиницю часу) і ймовірність передачі даних (імовірність доставки неспотвореного біта або ж імовірність викривлення біта) цікавлять розроблювача комп'ютерної

мережі в першу чергу, оскільки ці характеристики прямо впливають на продуктивність і надійність створюваної мережі.

Пропускна здатність і ймовірність передачі даних залежать, з одного боку, від характеристик фізичного середовища, а з іншого боку – визначаються характеристиками способу передачі даних. Отже, не можна говорити про пропускну здатність лінії зв'язку, до того як для неї визначений протокол фізичного рівня. Наприклад, оскільки для цифрових ліній завжди визначений протокол фізичного рівня, що задає бітову швидкість передачі даних, то для них завжди відома й пропускна здатність – 64 Кбіт/с, 2 Мбіт/с і т.д.

У тих же випадках, коли тільки має бути визначено, який з множини існуючих протоколів можна використовувати на даній лінії, дуже важливими є інші характеристики лінії, такі як смуга пропускання, перехресні наведення, завадостійкість та інші характеристики.

Пропускна здатність лінії характеризує максимально можливу швидкість передачі даних по лінії зв'язку. Пропускна здатність вимірюється в бітах у секунду (біт/с), а також у похідних одиницях, таких як кілобит у секунду (Кбіт/с), мегабіт у секунду (Мбіт/с), гігабит у секунду (Гбіт/с) і т.д.

Пропускна здатність ліній зв'язку й комунікаційного мережевого устаткування традиційно виміряється в бітах у секунду, а не в байтах у секунду. Це пов'язане з тим, що дані в мережах передаються послідовно, тобто побітно, а не паралельно, байтами, як це відбувається між пристроями усередині комп'ютера. Такі одиниці вимірювання, як кілобіт, мегабіт або гігабіт, у мережевих технологіях суворо відповідають ступеням 10 (тобто кілобіт – це 1000 біт, а мегабіт – це 1 000 000 біт), як це прийнято у всіх галузях науки й техніки, а не близьким до цих чисел ступеням 2, як це прийнято в програмуванні, де приставка «кіло» дорівнює $2^{10} = 1024$, а «мега» – $2^{20} = 1\,048576$.

Пропускна здатність лінії зв'язку залежить не тільки від її характеристик, таких як згасання й смуга пропускання, але й від спектра переданих сигналів. Якщо значимі гармоніки сигналу (тобто ті гармоніки, амплітуди яких вносять основний вклад у результуючий сигнал) попадають у смугу пропускання лінії, то такий сигнал буде добре передаватися даною лінією зв'язку й приймач зможе правильно розпізнати інформацію, відправлену по лінії передавачем. Якщо ж значимі гармоніки виходять за межі смуги пропускання лінії зв'язку, то сигнал буде значно спотворюватися, приймач буде помилятися при розпізнаванні інформації, а виходить, інформація не зможе передаватися із заданою пропускною здатністю.

Вибір способу представлення дискретної інформації у вигляді сигналів, що подаються на лінію зв'язку, називається *фізичним,* або *лінійним, кодуванням.* Від обраного способу кодування залежить спектр сигналів і, відповідно, пропускна здатність лінії. Таким чином, для одного способу кодування лінія може володіти однією пропускною здатністю, а для іншого – іншою. Наприклад, кручена пара категорії 3 може передавати дані із пропускною здатністю 10 Мбіт/с при способі кодування стандарту фізичного рівня 10 Base-T і 33 Мбіт/с при способі кодування стандарту 100 Base-T4.

Теорія інформації говорить, що будь-яка помітна й непередбачена зміна прийнятого сигналу несе в собі інформацію. Відповідно до цього прийом синусоїди, у якої амплітуда, фаза й частота залишаються незмінними, інформації не несе, тому що зміна сигналу хоча й відбувається, але є добре передбачуваним. Аналогічно, не несуть у собі інформації імпульси на тактовій шині комп'ютера, тому що їхні зміни також постійні в часі. А от імпульси на шині даних пророчити заздалегідь не можна, тому вони переносять інформацію між окремими блоками або пристроями комп'ютера.

Більшість способів кодування використовують зміну якого-небудь параметра періодичного сигналу – частоти, амплітуди й фази синусоїди або ж знак потенціалу послідовності імпульсів. Періодичний сигнал, параметри

якого змінюються, називають *несучим сигналом* або *несучою частотою,* якщо в якості такого сигналу використовується синусоїда.

Якщо сигнал змінюється так, що можна розрізнити тільки два його стани, то будь-яка його зміна буде відповідати найменшій одиниці інформації – біту. Якщо ж сигнал може мати більше двох помітних станів, то будь-яка його зміна буде нести декілька бітів інформації.

Кількість змін інформаційного параметра несучого періодичного сигналу в секунду виміряється в бодах (baud). Період часу між сусідніми змінами інформаційного сигналу називається тактом роботи передавача.

Пропускна здатність лінії в бітах у секунду в загальному випадку не збігається із числом бод. Вона може бути як вище, так і нижче числа бод, і це співвідношення залежить від способу кодування.

Якщо сигнал має більше двох помітних станів, то пропускна здатність у бітах у секунду буде вище, ніж число бод. Наприклад, якщо інформаційними параметрами є фаза й амплітуда синусоїди, причому розрізняються 4 стани фази в 0, 90, 180 і 270° і два значення амплітуди сигналу, то інформаційний сигнал може мати 8 різних станів. У цьому випадку модем, що працює зі швидкістю 2400 бод (з тактовою частотою 2400 Гц), передає інформацію зі швидкістю 7200 біт/с, тому що при одній зміні сигналу передається три біти інформації.

При використанні сигналів із двома різними станами може спостерігатися зворотна картина. Це часто відбувається тому, що для надійного розпізнавання приймачем користувальницької інформації кожний біт у послідовності кодується шляхом декількох змін інформаційного параметра несучого сигналу. Наприклад, при кодуванні одиничного значення біта імпульсом позитивної полярності, а нульового значення біта імпульсом негативної полярності фізичний сигнал двічі змінює свій стан при передачі кожного біта. При такому кодуванні пропускна здатність лінії у два рази нижче, ніж число бодів, передане по лінії.

На пропускну здатність лінії впливає не тільки фізичне, але й логічне кодування. Логічне кодування виконується до фізичного кодування й має на увазі заміну бітів вихідної інформації новою послідовністю бітів, що несе ту ж інформацію, але що володіє, крім цього, додатковими властивостями, наприклад можливістю для прийомної сторони виявляти помилки в прийнятих даних. Супровід кожного байта вихідної інформації одним бітом парності – це приклад дуже часто застосовуваного способу логічного кодування при передачі даних за допомогою модемів. Іншим прикладом логічного кодування може служити шифрування даних, що забезпечує їхню конфіденційність при передачі через суспільні канали зв'язку. При логічному кодуванні найчастіше вихідна послідовність бітів замінюється більш довгою послідовністю, тому пропускна здатність каналу стосовно корисної інформації при цьому зменшується.

Зв'язок між пропускною здатністю й смугою пропускання лінії

Чим вище частота несучого періодичного сигналу, тим більше інформації в одиницю часу передається по лінії й тем вище пропускна здатність лінії при фіксованому способі фізичного кодування. Однак, з іншого боку, зі збільшенням частоти періодичного несучого сигналу збільшується й ширина спектра цього сигналу, тобто різниця між максимальною й мінімальною частотами того набору синусоїд, які в сумі дадуть обрану для фізичного кодування послідовність сигналів. Лінія передає цей спектр синусоїд з тими викривленнями, які визначаються її смугою пропускання. Чим більше невідповідність між смугою пропускання лінії й шириною спектра переданих інформаційних сигналів, тим більше сигнали спотворюються й тем ймовірніші помилки в розпізнаванні інформації приймаючою стороною, а виходить, швидкість передачі інформації насправді виявляється менше, ніж можна було припустити.

Зв'язок між смугою пропускання лінії і її максимально можливою пропускною здатністю, поза залежністю від прийнятого способу фізичного кодування, установив Клод Шеннон:

$$C=F \log_2 (1+P_c/P_ш),$$

де:

C – максимальна пропускна здатність лінії в бітах у секунду,

F – ширина смуги пропускання лінії в герцах,

P_c – потужність сигналу,

$P_ш$ – потужність шуму.

Із цього співвідношення видно, що хоча теоретичної межі пропускної здатності лінії з фіксованою смугою пропускання не існує, на практиці така межа є. Дійсно, підвищити пропускну здатність лінії можна за рахунок збільшення потужності передавача або ж зменшення потужності шуму (перешкод) на лінії зв'язку. Обидві ці складові дуже важко піддаються зміні. Підвищення потужності передавача веде до значного збільшення його габаритів і вартості. Зниження рівня шуму вимагає застосування спеціальних кабелів з хорошими захисними екранами, що досить дорого, а також зниження шуму в передавачі й проміжній апаратурі, чого досягти досить не просто. До того ж вплив потужностей корисного сигналу й шуму на пропускну здатність обмежений логарифмічною залежністю, що росте далеко не так швидко, як прямопропорційна. Так, при досить типовому вихідному відношенні потужності сигналу до потужності шуму в 100 разів підвищення потужності передавача у два рази дасть тільки 15 % збільшення пропускної здатності лінії.

Близьким за суттю до формули Шеннона є інше співвідношення, отримане Найквістом, що також визначає максимально можливу пропускну здатність лінії зв'язку, але без врахування шуму на лінії:

$$C = 2 F \log_2 M,$$

де *M* – кількість помітних станів інформаційного параметра.

Якщо сигнал має два помітних стани, то пропускна здатність дорівнює подвоєному значенню ширини смуги пропускання лінії зв'язку. Якщо ж передавач використовує більше двох стійких станів сигналу для

кодування даних, то пропускна здатність лінії підвищується, тому що за один такт роботи передавач передає декілька бітів вихідних даних, наприклад два біти при наявності чотирьох різних станів сигналу (рисунок 2.7).

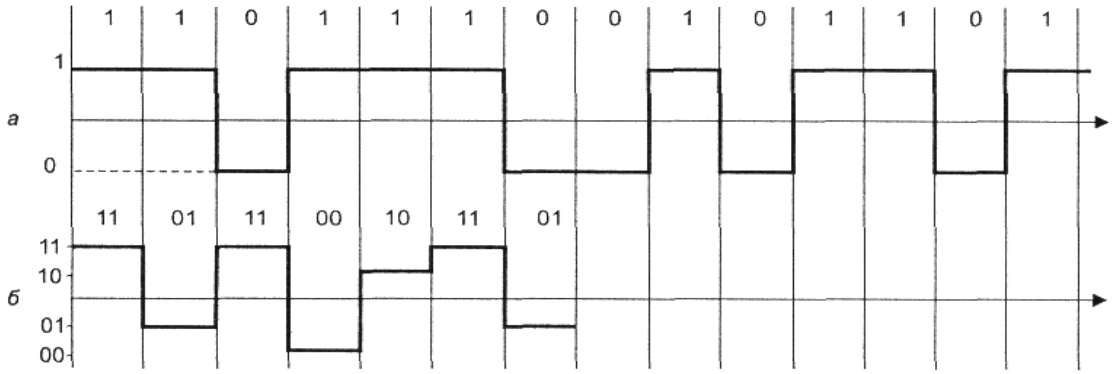


Рисунок 2.7 – Підвищення швидкості передачі за рахунок додаткових станів сигналу

Хоча формула Найквіста явно не враховує наявність шуму, побічно його вплив відбивається у виборі кількості станів інформаційного сигналу. Для підвищення пропускної здатності каналу хотілося б збільшити цю кількість до значних величин, але на практиці ми не можемо цього зробити через шум на лінії. Наприклад, для приклада, наведеного на рисунку 2.7, можна збільшити пропускну здатність лінії ще у два рази, застосувавши для кодування даних не 4, а 16 рівнів. Однак якщо амплітуда шуму часто перевищує різницю між сусідніми 16-ти рівнями, то приймач не зможе стійко розпізнавати передані дані. Тому кількість можливих станів сигналу фактично обмежується співвідношенням потужності сигналу й шуму, а формула Найквіста визначає граничну швидкість передачі даних у тому випадку, коли кількість станів уже обрано з врахуванням можливостей стійкого розпізнавання приймачем.

Наведені співвідношення дають граничне значення пропускної здатності лінії, а ступінь наближення до цієї межі залежить від конкретних методів фізичного кодування, а також потужності шуму, тобто різного роду перешкод.

РОЗДІЛ 3. МЕРЕЖЕВА АДРЕСАЦІЯ. ТИПИ АДРЕС СТЕКУ TCP/IP

Прийнятий в IP-мережах спосіб адресації вузлів істотним чином сприяє масштабованості даної технології, що дозволяє однозначно ідентифікувати мільйони мережевих інтерфейсів. Однак щоб забезпечити таку можливість у технологію TCP/IP, довелося включити цілий ряд спеціальних механізмів і протоколів.

Типи адрес стеку TCP/IP

У стеці TCP/IP використовуються три типи адрес:

– локальні або апаратні адреси – для адресації вузлів у межах підмережі;

– мережеві або IP-адреси – для однозначної ідентифікації вузлів у межах всієї складеної мережі;

– доменні імена – символьні ідентифікатори вузлів, до яких часто звертаються користувачі.

У загальному випадку вузол може мати одночасно одну або декілька локальних адрес і одну або декілька мережевих адрес, а також одне або декілька доменних імен.

MAC-адреси

MAC-адресу (від англ. *Media Access Control* – управління доступом до носія) – це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж. Більшість мережевих протоколів канального рівня використовують один з трьох просторів MAC-адрес, керованих IEEE: MAC-48, EUI-48 і EUI-64. Адреси в кожному з просторів теоретично мають бути глобально унікальними. Не всі протоколи використовують MAC-адреси, і не всі протоколи, що використовують MAC-адреси, потребують подібної унікальності цих адрес.

У широкомовних мережах (таких, як мережі на основі Ethernet) MAC-адресу дозволяє унікально ідентифікувати кожен вузол мережі і доставляти

дані тільки цьому вузлу. Таким чином, MAC-адреси формують основу мереж на канальному рівні, яку використовують протоколи вищого рівня. Для перетворення MAC-адрес в адреси мережевого рівня і назад застосовуються спеціальні протоколи (наприклад, ARP і RARP в мережах TCP/IP).

Адреси типу MAC-48 найбільш поширені; вони використовуються в таких технологіях, як Ethernet, Token ring, FDDI тощо. Вони складаються з 48 бітів, таким чином, адресний простір MAC-48 налічує 2^{48} (або 281 474 976 710 656) адрес. Згідно підрахункам IEEE, цього запасу адрес вистачить щонайменше до 2100 року.

EUI-48 відрізняється від MAC-48 лише семантично: тоді як MAC-48 використовується для мережевого устаткування, EUI-48 застосовується для інших типів апаратного і програмного забезпечення. Ідентифікатори EUI-64 складаються з 64 бітів і використовуються в FireWire, а також в IPv6 як молодші 64 біт мережевої адреси вузла.

Умовний формат для друку MAC-48 у зрозумілій людині формі, визначений стандартом (IEEE 802) являє собою шість груп двох шістнадцяткових цифр, розділених дефісами (-) або двокрапками (:), у порядку передачі, наприклад:

`01-23-45-67-89-ab`, або

`01:23:45:67:89:ab`.

Ця форма також широко використовується для EUI-64. Інша конвенція зазвичай використовується мережевим обладнанням використовуючи три групи чотирьох шістнадцяткових цифр розділених крапками (.), наприклад, `0123.4567.89ab`; також у порядку передачі.

Структура MAC-адреси

Стандарти IEEE визначають 48-розрядну MAC-адресу, яка роздільна на чотири частини.

Перший біт указує, для одиночного (0) або групового (1) адресата призначений кадр, а другий – чи є він універсальним (0) або локально керованим (1).

Третє поле вказує частину адреси, яку виробник отримує (при реєстрації) в IEEE, а три останні октети вибираються виготівником пристрою. Адресу пристрою глобально унікальна і зазвичай зашивається в апаратуру.

Четверте поле показує номер інтерфейсу.

IP-адреси

IP-адреси являють собою основний тип адрес, на підставі яких мережевий рівень передає пакети між мережами.

IP-адресу – це унікальна логічна мережева адреса конкретного вузла в комп'ютерній мережі. Для роботи в мережі Інтернет потрібна глобальна унікальність адреси, у разі роботи в локальній мережі потрібна унікальність адреси в межах мережі.

IP-адресу привласнюється мережевому інтерфейсу вузла. Звичайно це мережева інтерфейсна плата (NIC), встановлена в пристрої. Прикладами пристроїв з мережевими інтерфейсами можуть служити робочі станції, сервери, мережеві принтери й IP-телефони. Іноді в пристрій встановлюють декілька NIC, у кожної з яких є своя IP-адресу. В інтерфейсів маршрутизатора, що забезпечує зв'язок з мережею IP, також є IP-адреси.

У кожному відправленому по мережі пакеті є IP-адресу джерела й адресата. Ця інформація необхідна мережевим пристроям для передачі інформації адресату й передачі джерелу відповіді.

IP-адреси будуються за протоколом IP (англ. internet protocol – мережевий протокол).

У сучасній мережі Інтернет використовується IP четвертої версії – IPv4. У протоколі IPv4 кожному вузлу мережі ставиться у відповідність IP-адресу довжиною 4 октети (4 байти). При цьому комп'ютери у підмережах об'єднуються спільними початковими бітами адреси. Кількість цих бітів, спільна для даної підмережі, називається маскою підмережі.

В даний час вводиться в експлуатацію шоста версія протоколу – IPv6, яка дозволяє адресувати значно більшу кількість вузлів, ніж IPv4. Ця версія

відрізняється підвищеною розрядністю адреси, вбудованою можливістю шифрування і деякими іншими особливостями. Перехід з IPv4 на IPv6 пов'язаний з трудомісткою роботою операторів зв'язку і виробників програмного забезпечення і не може бути виконана миттєво.

IP-адреси четвертої версії – IPv4

IP-адресу четвертої версії являє собою послідовність з 32 двійкових бітів. Оскільки людині працювати з двійковою формою запису досить складно, для зручності читання, запису і запам’ятовування ці 32 біти групуються по чотири 8-бітних байта, у так звані октети, кожний октет представляється у вигляді свого десяткового значення. Октети розділяються десятковою крапкою або комою. Це називається крапково-десятковою нотацією.

При налаштуванні IP-адресу вузла вводиться у вигляді десяткового числа із крапками, наприклад, 192.168.7.3, що набагато зручніше і швидше, ніж вводити – 11000000101010000000001110000011. Якщо помилитися хоча б в одному біті, вийде інша адреса, і вузол, можливо, не зможе працювати в мережі.

Одержуючи IP-адресу, вузол переглядає всі 32 біти в міру надходження на мережевий адаптер. Навпроти, людям доводиться перетворювати ці 32 біти в десяткові еквіваленти, тобто в чотири октети. Кожний октет складається з 8 бітів, кожний біт має значення. У чотирьох груп з 8 бітів є той самий набір значень. Значення крайнього правого біта в октеті – 1, значення інших, зліва направо – 2, 4, 8, 16, 32, 64 і 128 (див. рис. 3.1).

Щоб визначити значення октету, потрібно скласти значення позицій, де є присутньою двійкова одиниця. Нульові позиції в додаванні не беруть участь.

Якщо всі 8 бітів мають значення 0, 00000000, то значення октету дорівнює 0.

Якщо всі 8 бітів мають значення 1, 11111111, значення октету – 255 (128+64+32+16+8+4+2+1).

Якщо значення 8 біт відрізняються, наприклад, 00100111, значення октету – 39 (32+4+2+1).

Таким чином, значення кожного із чотирьох октетів перебуває в діапазоні від 0 до 255.

32-бітова IP-адресу

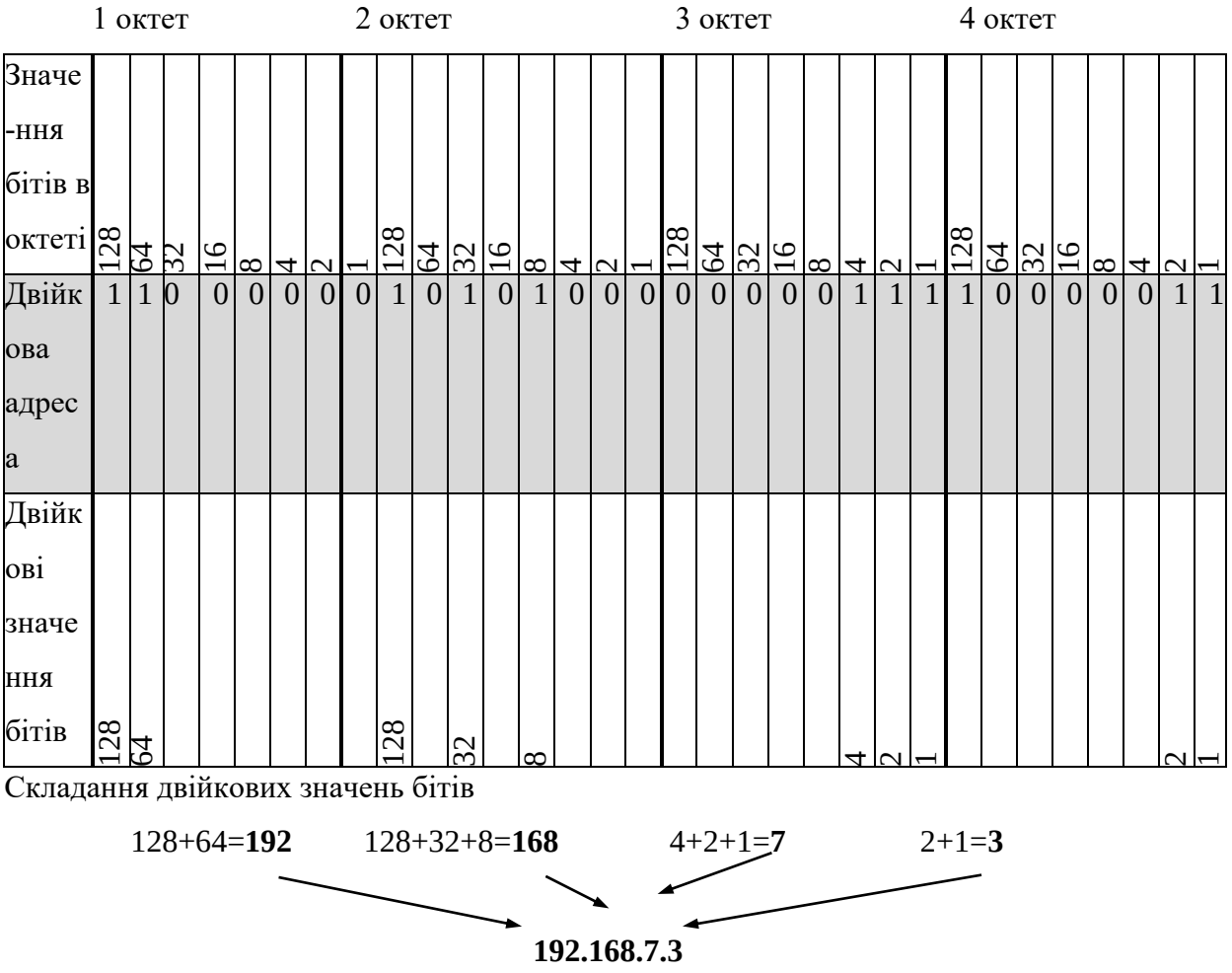


Рисунок 3.1 – Приклад розрахунків для перетворення IP-адреси в крапково-десятковий запис

По 32-бітній схемі адресації можна створити більше 4 мільярдів IP-адрес.

Логічна 32-бітна IP-адреса являє собою ієрархічну систему й складається із двох частин. Перша ідентифікує мережу, друга – вузол у мережі. Обидві частини є обов'язковими.

Наприклад, якщо IP-адресу вузла – 192.168.2.9, то перші три октети, (192.168.2), являють собою мережеву частину адреси, а останній октет, (9) є ідентифікатором вузла (див. рис. 3.2). Така система називається *ієрархічною адресацією*, оскільки мережева частина ідентифікує мережу, у якій перебувають всі унікальні адреси вузлів. Маршрутизаторам потрібно знати тільки шлях до кожної мережі, а не розташування окремих вузлів.

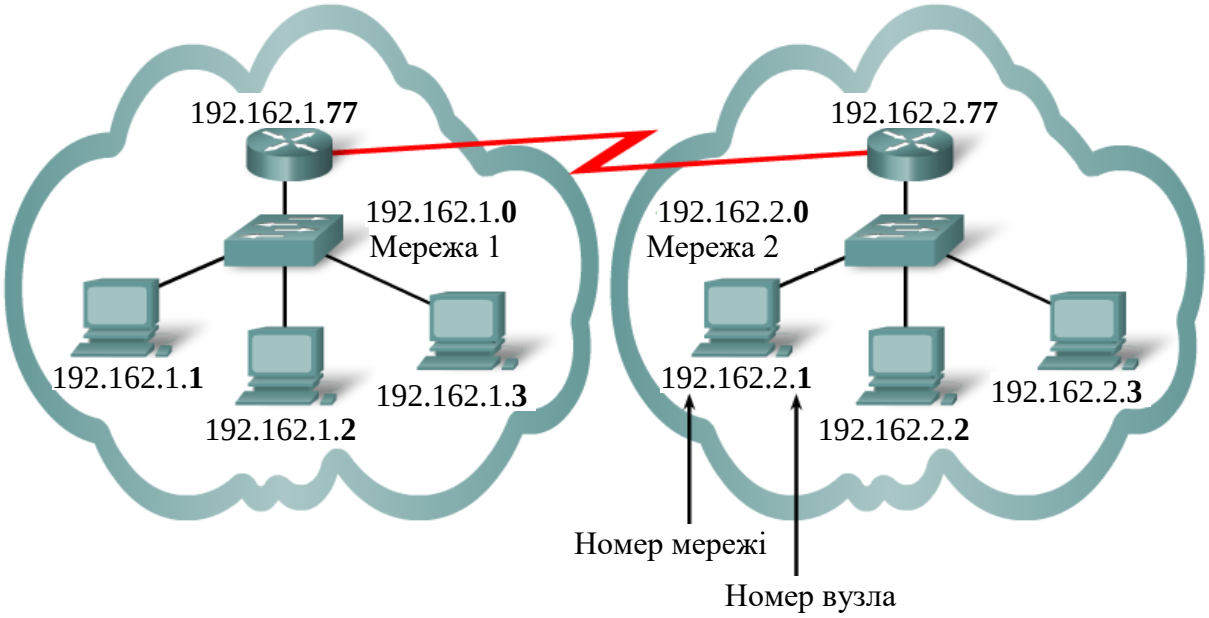


Рисунок 3.2 – Приклад ієрархічної адресації

Кожна IP-адреса складається із двох частин. Для визначення яка частина IP-адреси відноситься до адреси мережі, а яка до адреси вузла використовується *маска підмережі*.

При налаштуванні IP вузлу привласнюється не тільки IP-адресу, але й маска підмережі. Як і IP-адресу, маска складається з 32 бітів.

Маска накладається на IP-адреса побітно, зліва направо. У масці одиниці відповідають мережевій частині, а нулі – адресі вузла.

У наведеному прикладі на рисунку 3.3 перші три октети являють собою адресу мережі, а останній – адресу вузла.

11000000.10101000.00000011.10001111	192.162.3.15	IP-адресу
11111111.11111111.11111111.00000000	255.255.255.0	Маска
11000000.10101000.00000011.00000000	192.162.3.0	Мережева частина адреси

Рисунок 3.3 – Накладання маски на IP-адресу

Відправляючи пакет, вузол порівнює маску підмережі зі своєю IP-адресою й адресою одержувача. Якщо біти мережевої частини збігаються, то вузли джерела й призначення перебувають в одній і тій же мережі, і пакет доставляється локально. Якщо ні, відправляючий вузол передає пакет на інтерфейс локального маршрутизатора для відправлення в іншу мережу.

У невеликих локальних мережах найчастіше зустрічаються наступні маски підмережі:

255.0.0.0 – 8 бітів ідентифікують мережу, а 24 – вузли в мережі;

255.255.0.0 – 16 бітів ідентифікують мережу та 16 – вузли в мережі;

255.255.255.0 – 24 біти ідентифікують мережу, а 8 – вузли в мережі.

Особливі IP-адреси

Не всі комбінації 32 бітів можна використовувати для створення IP-адрес вузлів, так, як існують так звані *особливі IP-адреси*:

0.0.0.0 – адресу того вузла, який згенерував даний пакет (цей режим використовується тільки в деяких повідомленнях ICMP).

255.255.255.255 – 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. Обмеженість у цьому випадку означає, що пакет не вийде за межі маршрутизатора ні при яких умовах.

127.0.0.1 – адресу зворотного зв'язку (loopback), пакети по ній в мережу не відправляються, цій адресі за замовчуванням призначається ім'я localhost. Вона використовується для тестування програм і взаємодії процесів у межах однієї 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 мережевим інтерфейсам IP-адреси, що починаються із числа 127. Можна віднести адресу 127.0.0.0 до внутрішньої мережі модуля маршрутизації вузла, а адреса 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. Необхідність в адресі loopback виникає, наприклад, коли на одному комп'ютері працює й клієнтська, і серверна частини деякого мережевого додатка.

Якщо в полі номера мережі знаходяться тільки нулі, то за замовчуванням вважається, що вузол одержувача належить тій же самій мережі, що й вузол відправника.

Якщо в полі номера вузла призначення знаходяться тільки одиниці, то пакет, що має таку адресу, розсилається всім вузлам мережі із заданим номером мережі. Наприклад, пакет з адресою 192.190.5.255 доставляється всім вузлам мережі 192.190.5.0. Таке розсилання називається широкомовним повідомленням.

Спеціальні адреси, що складаються з послідовностей нулів, можуть бути використані тільки як адреси відправника, а адреси, що складаються з послідовностей одиниць, – тільки як адреси одержувача.

При призначенні адрес кінцевим вузлам і маршрутизаторам 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.

Класи IP-адрес

Існує два рівні ієрархії класових IP-адрес: мережа й вузол. IP-адресу й маска підмережі спільно визначають те, яка частина IP-адреси є мережевою, а яка відповідає адресі вузла.

IP-адреси діляться на 5 класів. До класів A, B і C відносяться комерційні адреси, що привласнюються вузлам. Клас D зарезервований для багатоадресних розсилань, а клас E – для експериментів.

В адресах класу A мережева частина складається всього з одного октету, інші відведені вузлам. Обрана за замовчуванням маска підмережі складається з 8 бітів (255.0.0.0). Звичайно такі адреси привласнюються великим організаціям.

Рисунок 3.4 – структура IP-адрес різних класів.

Приналежність IP-адреси до класу визначається значеннями перших бітів адреси.

Якщо адресу починається з 0, то ця адресу відноситься до класу A, у якому під номер мережі приділяється один байт, а інші три байти інтерпретуються як номер вузла в мережі. Мережі, що мають номери в діапазоні від 1 (00000001) до 126 (01111110), називаються мережами класу A. (Номер 0 не використовується, а номер 127 зарезервований для спеціальних

цілей, про що буде сказано нижче.) Мереж класу A небагато, зате кількість вузлів у них може досягати 2^{24}, тобто 16 777 216 вузлів.

Якщо перші два біти адреси рівні 10, то адресу відноситься до класу B. В адресах класу B під номер мережі й під номер вузла виділяється по два байти. Мережі, що мають номери в діапазоні від 128.0 (10000000 00000000) до 191.255(10111111 11111111), називаються мережами класу B. Таким чином, мереж класу B більше, ніж мереж класу A, але розміри їх менше, максимальна кількість вузлів у них становить 2^{16} (65 536).

Якщо адресу починається з послідовності бітів 110, то це адресу класу C. У цьому випадку під номер мережі виділяється 24 біти, а під номер вузла – 8 біт. Мережі класу C найпоширеніші, але число вузлів у них обмежене значенням 2^8 (256) вузлів.

Ще два класи адрес D і E не зв'язані безпосередньо з мережами.

Якщо адресу починається з послідовності 1110, то вона є адресою класу D і позначає особливу, групову адресу (multicast). Групова адреса ідентифікує групу вузлів (мережевих інтерфейсів), які в загальному випадку можуть належати різним мережам. Інтерфейс, що входить у групу, одержує поряд зі звичайною індивідуальною IP-адресою ще одну групову адресу. Якщо при відправленні пакета як адресу призначення зазначена адреса класу D, то такий пакет повинен бути доставлений всім вузлам, які входять у групу.

Якщо адресу починається з послідовності 11110, то це значить, що дана адреса відноситься до класу E. Адреси цього класу зарезервовані для майбутніх застосувань.

Клас адреси можна визначити за значенням першого октету. Наприклад, якщо значення першого октету IP-адреси перебуває в діапазоні від 192 до 223, то це адресу класу C. Наприклад, адресу 200.14.193.67 відноситься до класу C.

Таблиця 3.1 – Класи IP-адрес

Клас IP-адреси	Діапазон 1 октету (десяткове представлення)	Біти 1 октету (жирним виділені біти, що не змінюються)	Мережева та вузлова частини адреси	Маска підмережі за замовчуванням	Число можливих мереж та вузлів для кожної мережі
A	1-127	**0**0000000 – **0**1111111	M.B.B.B	255.0.0.0	2^7-2 = 126 мереж 2^{24}-2 = 16 777 214 вузлів для кожної мережі
B	128-191	**10**000000 – **10**111111	M.M.B.B	255.255.0.0	2^{14}-2 = 16 382 мереж 2^{16}-2 = 65 534 вузлів для кожної мережі
C	192 – 223	**110**00000 – **110**11111	M.M.M.B	255.255.255.0	2^{21}-2 = 2 097 150 мереж 2^8-2 = 254 вузлів для кожної мережі
D	224 – 239	**1110**0000 – **1110**1111	В якості вузла не для комерційного застосувавння	–	–
E	240 – 255	**1111**0000 – **1111**1111	В якості вузла не для комерційного застосування	–	–

Загальні й приватні IP-адреси

Всім вузлам, підключеним безпосередньо до Інтернету, необхідна унікальна глобальна (публічна) IP-адреса. Існує ризик, що кількості 32-бітних адрес не вистачить. У якості одного з рішень було запропонована зарезервувати деяку кількість приватних адрес для використання тільки всередині організацій. Таким чином, внутрішні вузли зможуть обмінюватися даними один з одним без унікальних загальних IP-адрес.

Таблиця 3.2 – Діапазони приватних адрес

Клас адреси	Діапазони приватних адрес (RFC 1918)	Маска підмережі за замовчуванням	Число мереж	Число вузлів у кожній мережі	Загальна кількість вузлів
A	10.0.0.0 – 10.255.255.255;	255.0.0.0	1	16,777,214	16,777,214
B	172.16.0.0 – 172.31.255.255;	255. 255.0.0	16	85,534	1,048,544
C	192.168.0.0 – 192.168.255.255.	255. 255. 255.0	256	254	85,024

У відповідності зі стандартом RFC 1918 декілька діапазонів адрес класу A, B і C були зарезервовані. У діапазон приватних адрес входить одна мережа класу A, 16 мереж класу B і 256 мереж класу C.

Таким чином, мережеві адміністратори одержали певний ступінь волі в плані надання внутрішніх адрес.

У дуже великій мережі можна використовувати приватну мережу класу A, де можна створити більше 16 мільйонів приватних адрес.

У середніх мережах можна використовувати приватну мережу класу B з більш ніж 65 000 адрес.

У домашній і невеликій комерційній мережах звичайно використовується одна приватна адреса класу C, розрахована на 254 вузла.

Одну мережу класу А, 16 мереж класу В або 256 мереж класу С можуть використовувати організації будь-якого розміру. Багато організацій користуються приватною мережею класу А.

Вузли із внутрішньої мережі організації можуть використовувати приватні адреси доти, поки їм не знадобиться прямий вихід в Інтернет. Відповідно, той самий набір адрес підходить для декількох організацій. Приватні адреси не маршрутизуються в Інтернеті й швидко блокуються маршрутизатором Інтернет-провайдера.

Приватні адреси можна використовувати як міри безпеки, оскільки їх можна побачити тільки в локальній мережі, а сторонні одержати прямий доступ до цих адрес не можуть.

Крім того, існують приватні адреси для діагностики пристроїв, які розглядалися раніше. Вони називаються адресами зворотного зв'язка. Для таких адрес зарезервована мережа 127.0.0.0 класу А.

Адреси одноадресних, широкомовних і багатоадресних розсилань

Крім класів, IP-адреси діляться на категорії, призначені для одноадресних, широкомовних або багатоадресних розсилань. За допомогою IP-адрес вузли можуть обмінюватися даними в режимі "один до одного" (одноадресне пересилання), "один до багатьох"; (багатоадресне розсилання) або "один до всіх" (широкомовне розсилання).

Одноадресне розсилання

Адресу одноадресного розсилання найчастіше зустрічається в мережі IP. Пакет з одноадресним одержувачем призначений конкретному вузлу. Приклад: вузол з IP-адресою 192.168.1.5 (джерело) запитує веб-сторінку із сервера з IP-адресою 192.168.1.200 (адресат).

Для відправлення й прийому одноадресного пакета IP-адреса одержувача повинна перебувати в заголовку IP-пакета. Крім того, у заголовку кадру Ethernet повинна бути MAC-адресу одержувача. IP-адресу й MAC-адресу – це дані для доставки пакета одному вузлу.

Широкомовне розсилання

У пакеті широкомовного розсилання утримується IP-адресу одержувача, де у відведеній вузлу частини є тільки одиниці. Це означає, що пакет одержать і оброблять всі вузли в локальній мережі (домені широкомовного розсилання). Широкомовні розсилання передбачені в багатьох Інтернет-протоколах, наприклад, ARP і DHCP.

У мережі класу C 192.168.1.0 з маскою підмережі за замовчуванням 255.255.255.0 використовується адресу широкомовного розсилання 192.168.1.255. У відведеній вузлу частині стоїть 255, або у двійковому вигляді 11111111 (всі одиниці).

У мережі класу B 172.16.0.0 з маскою підмережі за замовчуванням 255.255.0.0 використовується адресу широкомовного розсилання 172.16.255.255.

У мережі класу A 10.0.0.0 з маскою підмережі за замовчуванням 255.0.0.0 використовується адресу широкомовного розсилання 10.255.255.255.

Для мережевої IP-адреси широкомовного розсилання потрібна відповідна MAC-адресу в кадрі Ethernet. У мережах Ethernet використовується широкомовна MAC-адресу з 48 одиниць, що у шістнадцятковому форматі виглядає як FF-FF-FF.

Багатоадресне розсилання

Адреси багатоадресних розсилань дозволяють джерелу розсилати пакет групі пристроїв.

Пристрої, що належать до багатоадресної групи, одержують її IP-адресу. Діапазон таких адрес – від 224.0.0.0 до 239.255.255.255. Оскільки адреси багатоадресних розсилань відповідають групам адрес (які іноді називаються групами вузлів), вони використовуються тільки як адресати пакета. У відправника завжди одноадресна адреса.

Адреси багатоадресних розсилань використовуються, наприклад, у дистанційних іграх, у яких бере участь декілька людей з різних місць. Інший

приклад – це дистанційне навчання в режимі відеоконференції, де декілька учнів підключаються до одного курсу.

Як і одноадресним, і широкомовним адресам, IP-адресам багатоадресного розсилання потрібна відповідна MAC-адресу, що дозволяє доставляти кадри в локальній мережі. Багатоадресна MAC-адресу – це особливе значення, що у шістнадцятирічному форматі починається з 01-00-5E. Нижні 23 біта IP-адреси багатоадресной групи перетворяться в інші 6 шістнадцятирічних символів адреси Ethernet.

IP-адреси шостої версії – IPv6

CIDR і приватна IP-адресація розроблені для того, щоб тимчасово вирішити проблему з нестачею IP-адрес. Ці методи, хоч і виявилися корисними, але не збільшили кількість IP-адрес. IPv6 це вдалося.

IPv6 був запропонований у 1998 році в RFC 2460.

Хоча спочатку в такий спосіб передбачалося вирішити проблему нестачі IP-адрес IPv4, були й інші причини його появи. З моменту початкової стандартизації IPv4 Інтернет помітно розрісся. При цьому виявилися переваги й недоліки IPv4, а також можливості оновлення й додавання нових можливостей.

Загальний список поліпшень, запропонованих в IPv6:

– розширення адресного простору;

– більш вдале керування адресним простором;

– спрощене керування TCP/IP;

– модернізація функцій маршрутизації;

– удосконалена підтримка багатоадресних розсилань, безпеки й мобільності.

При розробці IPv6 передбачалося вирішити якнайбільше таких проблем.

В IPv6 використовуються 128-бітні IP-адреси, а можливий розмір адресного простору становить 2^{128}. У десятковому вираженні це, приблизно,

3 з 38 нулями. Якщо адресний простір IPv4 представити у вигляді чайної ложки, то простір IPv6 – це щось розміром із планету Сатурн.

Працювати з 128-бітними числами складно, тому в адресах IPv6 128 бітів представлені у вигляді 32 шістнадцятирічних чисел, розділених на вісім груп, у кожній групі 4 числа, і групи розділені між собою роздільником у вигляді двокрапки. Адреси IPv6 складаються із трьох частин. Перші три блоки адреси займає глобальний префікс, привласнений організації реєстратором доменних імен в Інтернеті. Ідентифікатор підмережі й інтерфейсу (ID) привласнює адміністратор мережі.

Адміністраторам буде потрібно якийсь час на те, щоб пристосуватися до нової структури IPv6. До того, як IPv6 стане загальноприйнятим стандартом, адміністраторам ще буде потрібний спосіб більш ефективного використання приватних адресних просторів.

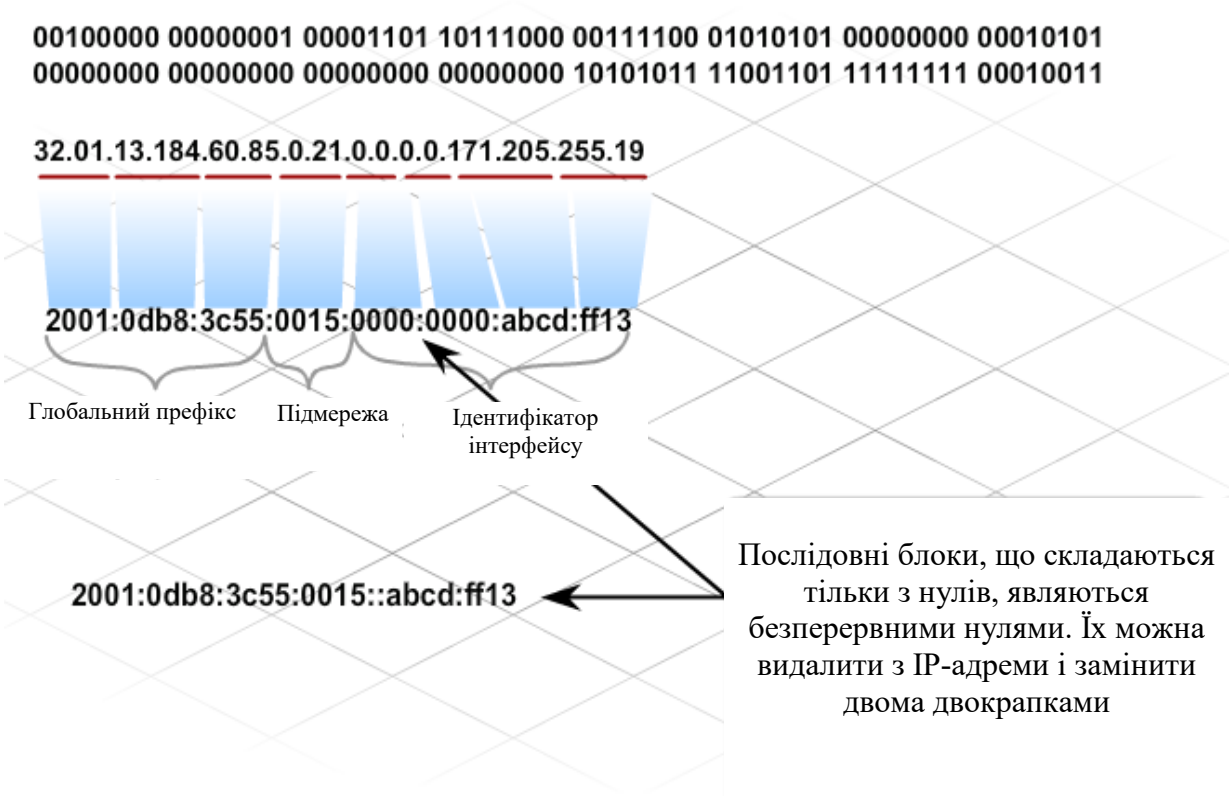


Рисунок 3.5 – Представлення адрес протоколу IPv6

РОЗДІЛ 4. АДРЕСАЦІЯ В КОРПОРАТИВНІЙ МЕРЕЖІ. ПЛОСКІ Й ІЄРАРХІЧНІ МЕРЕЖІ

Впровадження комутаторів дозволяє зменшити число колізій у локальній мережі. Однак при використанні повністю комутованої мережі часто створюється єдиний домен широкомовного розсилання. У єдиному домені широкомовного розсилання (плоскій мережі) всі пристрої розташовані в одній і тій же мережі й одержують всі розсилання. У невеликих мережах використання єдиного домену широкомовного розсилання прийнятне.

При використанні великої кількості вузлів плоска мережа стає менш ефективною. У міру збільшення числа вузлів комутованій мережі збільшується число переданих і одержуваних широкомовних розсилань. Пакети широкомовних розсилань займають більшу частину смуги пропускання, що призводить до затримок при передачі трафіку і тайм-аутів.

Одне з рішень проблем великих плоских мереж – створення мереж VLAN. Мережа VLAN є власним доменом широкомовного розсилання.

Інше рішення – реалізація ієрархічної мережі з використанням маршрутизаторів (рис. 4.1).

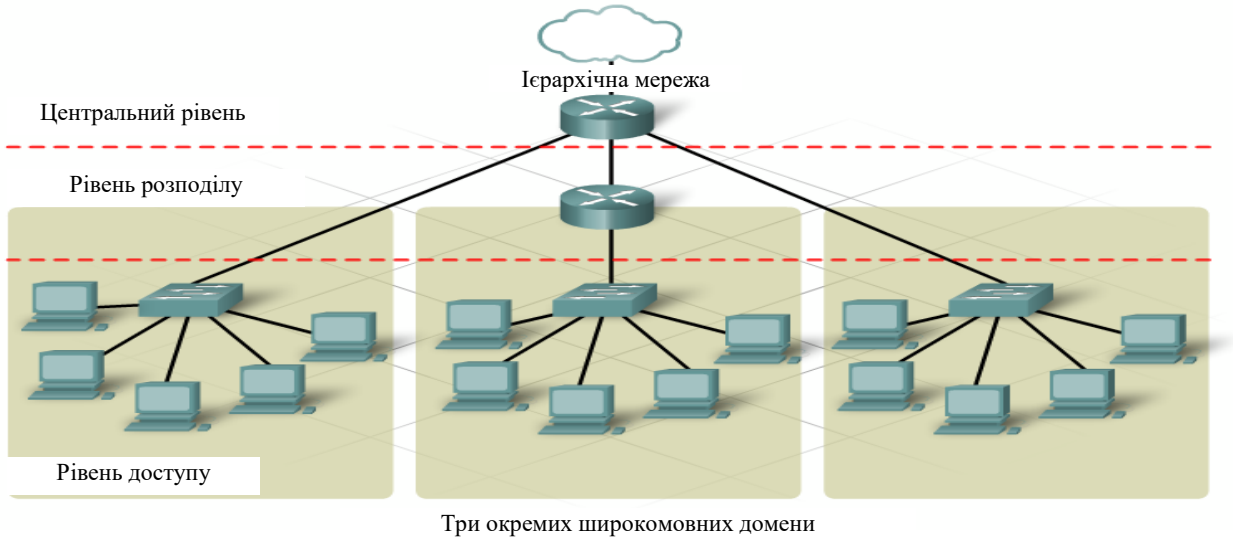


Рисунок 4.1 – Ієрархічна мережа

Дворівнева адресація. Мережі й підмережі. Використання масок при IP-адресації

Постачаючи кожну IP-адресу маскою, можна відмовитися від понять класів адрес і зробити систему адресації більше гнучкою. Наприклад, якщо 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 повинна бути кратною 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-адресу 129.64.134.5 виглядає так:

10000001. 01000000. 10000110. 00000101

А маска 255.255.128.0 так:

11111111. 11111111. 10000000. 00000000

Якщо ігнорувати маску, то відповідно до системи класів адресу 129.64.134.5 відноситься до класу B, а виходить, номером мережі є перші два байти – 129.64.0.0, а номером вузла – 0.0.134.5.

Якщо ж використовувати для визначення кордони номера мережі маску, то 17 послідовних двійкових одиниць у масці 255.255.128.0, «накладені» на IP-адреса, ділять її на наступні дві частини:

	№ мережі	**№ вузла**
IP-адресу 129.64.134.5	10000001. 01000000. 1	0000110. 00000101
Маска 255.255.128.0	11111111. 11111111. 1	0000000. 00000000

У десятковій формі запису номер мережі – 129.64.128.0, а номер вузла – 0.0.6.5. Для стандартних класів мереж маски мають наступні значення:

клас A – 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

клас B – 11111111. 11111111. 00000000. 00000000 (255.255.0.0);

клас C – 11111111. 11111111. 11111111. 00000000 (255.255.255.0).

В 80-ті й 90-ті роки мережі розрослися, багато організацій підключили сотні й навіть тисячі вузлів. Для організації з тисячами вузлів досить мережі класу B. На жаль, виникли проблеми. Ці тисячі вузлів рідко розміщалися в тому самому місці. З метою безпеки деякі організації забажали розділити свої відділи. Для усунення цієї проблеми організації, що займаються розвитком Інтернету, вирішили розділити свої мережі на підмережі. Як розділити одну мережу класу B на декілька окремих мереж?

Стандарт RFC 917 "Підмережі в Інтернеті", передбачає використання масок підмереж як методу ізоляції підмережі від IP-адреси, виконуваної маршрутизатором. Коли маршрутизатор приймає пакет, він визначає відповідний шлях передачі на основі IP-адреси вузла призначення й маски підмережі, пов'язаної з маршрутами в таблиці маршрутизації.

Маршрутизатор побітно зчитує маску підмережі зліва направо. Якщо біт маски підмережі встановлений в 1, виходить, значення даного положення є частиною ідентифікатора мережі. Значення 0 у масці підмережі є частиною ідентифікатора вузла.

У дворівневу ієрархію адресації за класами входить ідентифікатор мережі й вузла. У підмережах, організованих за класами, ідентифікатор мережі залишається без змін, а ідентифікатор вузла ділиться на ідентифікатор підмережі й нового вузла. Наприклад, у мережі класу B є обрана за замовчуванням 16-бітна маска підмережі 11111111 11111111 00000000 00000000, або 255.255.0.0.16 біт залишається для ідентифікатора вузла.

Один зі способів розподілу класу B на декілька мереж – використання чотирьох бітів вузла як ідентифікатору підмережі. Виходить 20-бітна маска підмережі 255.255.240.0, а для ідентифікатора вузла залишається тільки 12 бітів.

При такому розподілі ідентифікатора вузла виходить фіксована кількість підмереж і фіксована кількість вузлів у кожній.

Якщо в організації є мережа класу B з 4 підмережами й у деяких з них усього декілька вузлів, пропадають тисячі IP-адрес. Для більш ефективного

використання IP-адрес була створена технологія безкласової міждоменної маршрутизації (CIDR).

У режимі CIDR класи мереж не використовуються. Для створення підмереж в CIDR використовуються маски підмереж змінної довжини (VLSM). Ідентифікатор мережі не обмежується рамками октету. У мережі з адресацією за класами мережа, представлена IP-адресою 192.168.5.0, відноситься до класу C. Ідентифікатор мережі повинен складатися мінімум з 24 бітів, вузлів не може бути більше 254. При використанні адресації CIDR, що іноді називають безкласовою, кількість бітів в ідентифікаторі мережі не регулюється її класом. Можна створювати мережі з адресним простором 192.168.0.0 і номером мережі, що займає менше 24 біт. Наприклад, адресу 192.168.82.174 є частиною мережі, де перші 18 бітів становлять ідентифікатор мережі. Мережа, де перебуває даний вузол, буде називатися 192.168.64.0/18, де /18 відповідає 18-бітній масці підмережі (255.255.192.0).

Мережа користувача з одним ISR жахливо перевантажена. Пропонується додати ще один мережевий пристрій, більший ISR, і розділити мережу на дві більш дрібні.

З метою безпеки бездротових і дротових користувачів потрібно розділити по різних локальних мережах.

В 90-х роках багато мереж не мали виходу в інші мережі або Інтернет. Щоб зменшити кількість зареєстрованих організаціями унікальних IP-адрес, компанія Internet Engineering Task Force (IETF) вирішила зарезервувати частину адресного простору Інтернет для приватних мереж.

Такі блоки адрес не потрібно маршрутизувати загальнодоступній мережі Інтернет. Це означає, що всі приватні мережі можуть використовувати ті самі адреси, і поки вони не зв'язуються одна з одною, нормально обмінюватися даними.

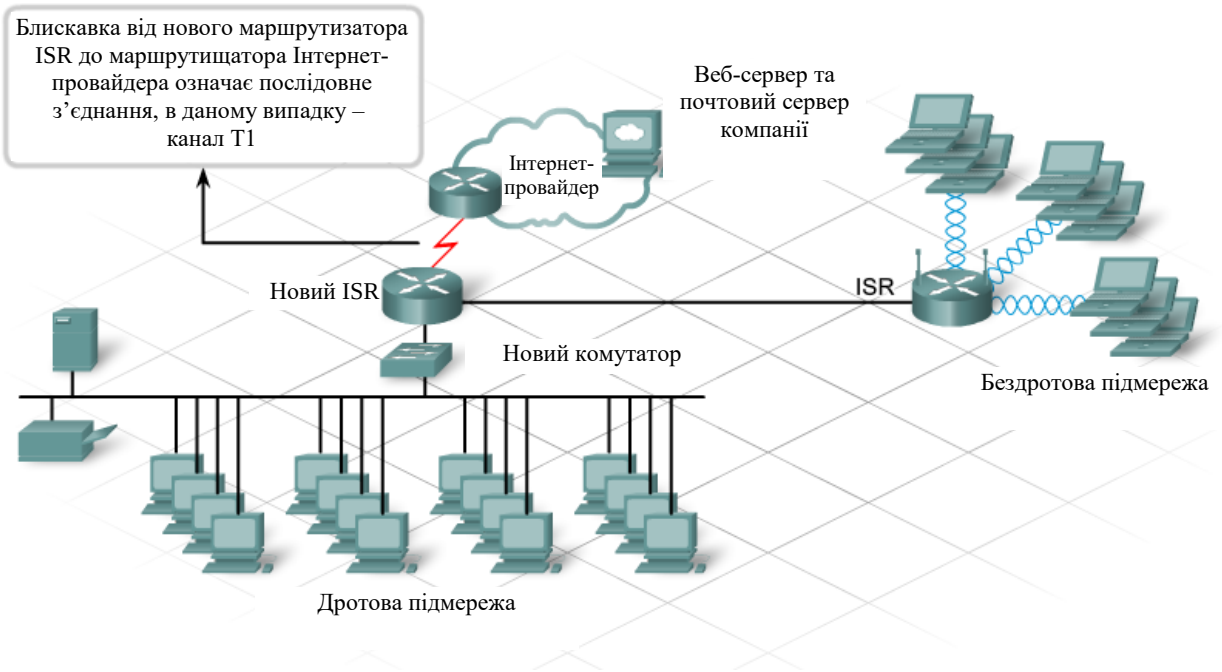


Рисунок 4.2 – Поділ мережі на підмережі

На даний момент у більшості мереж використовується приватна структура адрес. Адреси, що маршрутизуються в Інтернеті привласнюються тільки пристроям, які підключаються безпосередньо до загальнодоступної мережі. За замовчуванням більшість користувальницьких мережевих пристроїв одержує приватні адреси через DHCP.

Обмін даними між підмережами

Уявіть собі підмережу у вигляді невеликої мережі. При розподілі мережі на дві підмережі фактично утворяться окремі мережі. Вони з'єднуються через маршрутизатори. Щоб пристрій з однієї підмережі зміг обмінюватися даними із пристроєм з іншої мережі, необхідний маршрутизатор.

Конфігурацію необхідно побудувати так, щоб інтерфейси маршрутизаторів, підключених один до одного, одержали IP-адреси з однієї й тої ж мережі й підмережі й щоб клієнтам були привласнені шлюзи за замовчуванням, до яких вони можуть підключатися.

Адресація в ієрархічних мережах

Великі корпоративні мережі виграють від впровадження моделі ієрархічної мережі й відповідної структури адрес. Структура ієрархічної адресації логічно ділить мережі на менш великі підмережі.

Ефективна схема ієрархічної адресації складається з адреси класової мережі на центральному рівні, що підрозділяється на менш великі підмережі на рівнях розподілу й доступу.

Можна використовувати ієрархічну мережу без використання ієрархічної адресації. Хоча мережа продовжує функціонувати, ефективність конструкції мережі знижується, а певні функції протоколу маршрутизації (наприклад, підсумовування маршрутів) працюють некоректно.

У корпоративній мережі, що охоплює безліч географічно розкиданих підрозділів, модель і структура адрес ієрархічної мережі спрощує керування мережею й усунення несправностей, а також підвищує масштабованість і ефективність маршрутизації.

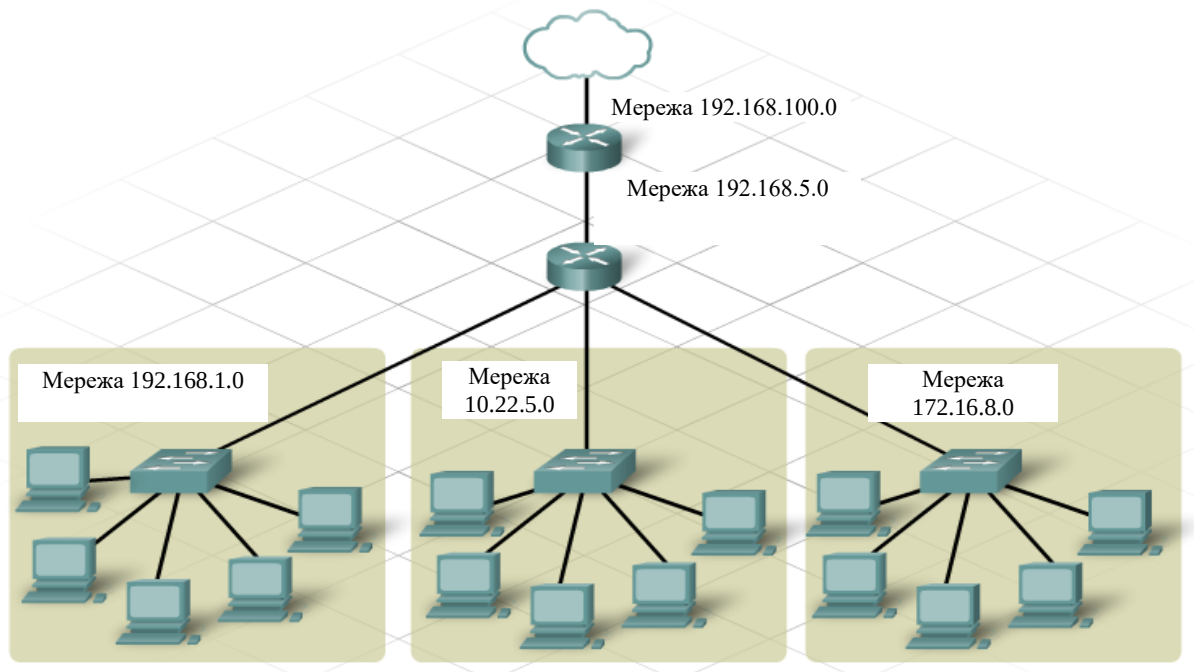


Рисунок 4.3 – Приклад неієрархічної мережі

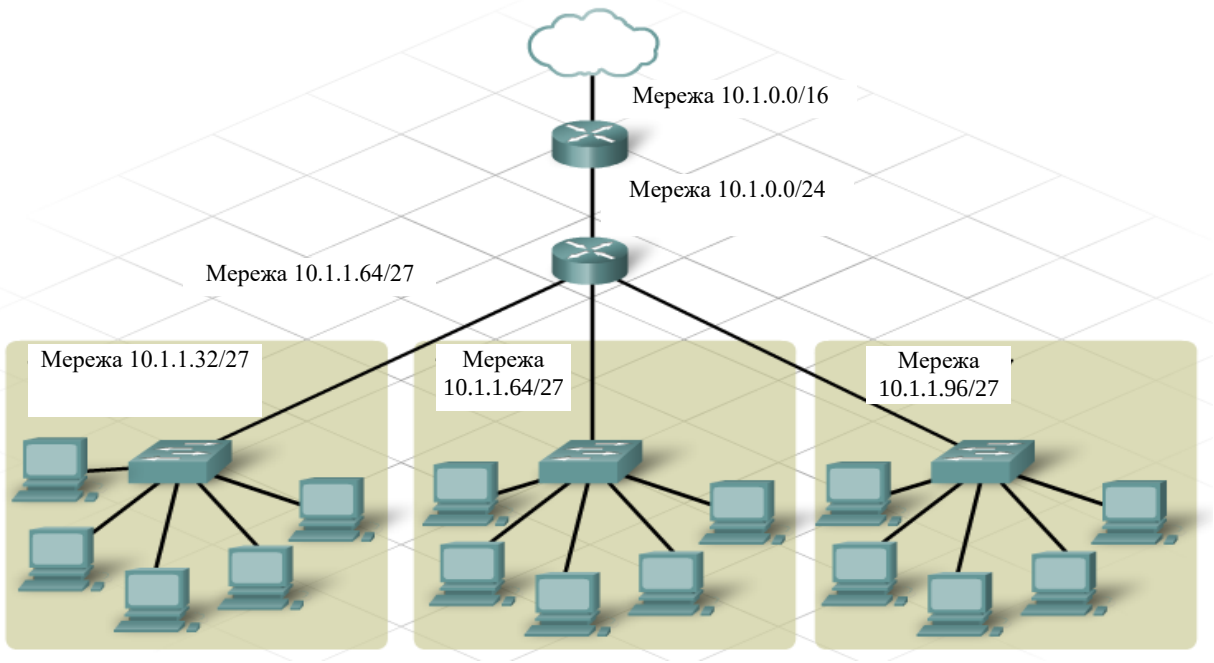


Рисунок 4.4 – Приклад ієрархічної мережі

Існує багато причин розділити мережу на підмережі, включаючи:

– фізичне місце розташування;

– логічне угруповання;

– безпека;

– вимоги додатків;

– обмеження широкомовного розсилання;

– модель ієрархічної мережі.

Наприклад, якщо в організації використовується мережа 10.0.0.0 для всього підприємства, можна використовувати схему адресації 10.X.Y.0, де X відповідає географічному місцю розташування, а Y – будинку або поверху в цьому місці. Ця схема адресації дозволяє використовувати:

– 255 різних географічних місць розташування;

– 255 будинків у кожному місці розташування;

– 254 вузла в кожному будинку.

Маска підмережі

Щоб використовувати поділ мережі на підмережі для створення ієрархічної моделі, необхідно чітко розуміти структуру маски підмережі.

Маска підмережі вказує, чи перебувають вузли в одній і тій же мережі. Маска підмережі – це 32-бітне значення для розрізнення бітів мережі й бітів вузлів. Вона складається з рядка одиниць, за якої треба рядок нулів. Одиниці відповідають мережі, а нулі – вузлу.

Таблиця 4.1 – Представлення маски підмережі та число можливих вузлів

Крапково-десятковий вид маски підмережі	Двійкова маска під мережі	Представ-лення з похилою рискою	Число бітів вузла	Можлива кількість вузлів 2^{n-1}
255.0.0.0	11111111.00000000.00000000.00000000	/8	24	16777214
255.128.0.0	11111111.10000000.00000000.00000000	/9	23	8388606
255.192.0.0	11111111.11000000.00000000.00000000	/10	22	4194302
255.224.0.0	11111111.11100000.00000000.00000000	/11	21	2097150
255.248.0.0	11111111.11110000.00000000.00000000	/12	20	1048574
255.240.0.0	11111111.11111000.00000000.00000000	/13	19	524286
255.252.0.0	11111111.11111100.00000000.00000000	/14	18	262142
255.254.0.0	11111111.11111110.00000000.00000000	/15	17	131070
255.255.0.0	11111111.11111111.00000000.00000000	/16	16	65534
255.255.128.0	11111111.11111111.10000000.00000000	/17	15	32766
255.255.192.0	11111111.11111111.11000000.00000000	/18	14	16382
255.255.224.0	11111111.11111111.11100000.00000000	/19	13	8190
255.255.240.0	11111111.11111111.11110000.00000000	/20	12	4094
255.255.248.0	11111111.11111111.11111000.00000000	/21	11	2046
255.255.252.0	11111111.11111111.11111100.00000000	/22	10	1022
255.255.254.0	11111111.11111111.11111110.00000000	/23	9	510
255.255.255.0	11111111.11111111.11111111.00000000	/24	8	254
255.255.255.128	11111111.11111111.11111111.10000000	/25	7	126
255.255.255.192	11111111.11111111.11111111.11000000	/26	6	62
255.255.255.224	11111111.11111111.11111111.11100000	/27	5	30
255.255.255.240	11111111.11111111.11111111.11110000	/28	4	14
255.255.255.248	11111111.11111111.11111111.11111000	/29	3	6
255.255.255.252	11111111.11111111.11111111.11111100	/30	2	2

В адресах класу А використовується маска підмережі за замовчуванням виду 255.0.0.0 або запис із косою рисою виду /8.

В адресах класу В використовується маска за замовчуванням виду 255.255.0.0 або /16.

В адресах класу С використовується маска за замовчуванням виду 255.255.255.0 або /24.

Запис **/x** означає число бітів у масці підмережі, що становить мережеву частину адреси.

У корпоративній мережі маски підмережі розрізняються довжиною. Сегменти мережі ЛМ часто містять різне число вузлів, отже, неефективно використовувати маску підмережі однієї й тої ж довжини для всіх створюваних підмереж.

Розрахунок підмереж

Для обміну даними між вузлами IP-адресу й маска підмережі вузла-відправника рівняється з IP-адресою й маскою підмережі вузла призначення. Це дозволяє визначити, чи перебувають дві адреси в одній і тій же локальній мережі.

Маска підмережі – це 32-бітне значення для розрізнення бітів мережі й бітів вузла в IP-адресі. Маска підмережі складається з рядка одиниць, за якої треба рядок нулів. Одиниці вказують число мережевих битов, а нулі – число бітів вузла в IP-адресі. Порівнюються мережеві біти адреси відправника й адреси призначення. Якщо виявляється, що вони перебувають в одній і тій же мережі, то пакет можна доставити локально. Якщо вони не збігаються, то пакет направляється на шлюз за замовчуванням.

Наприклад, припустимо, що необхідно передати повідомлення з вузла H1, що має IP-адресу 192.168.1.44 і маску підмережі 255.255.255.0 або /24, на вузол H2, що має IP-адресу 192.168.1.66 і маску підмережі 255.255.255.0. У цьому випадку обидва вузли використовують маску підмережі за замовчуванням, рівну 255.255.255.0, що означає, що мережеві біти закінчуються на кордони третього октету. На обох вузлах використовуються однакові мережеві біти 192.168.1, отже, вони перебувають в одній і тій же мережі.

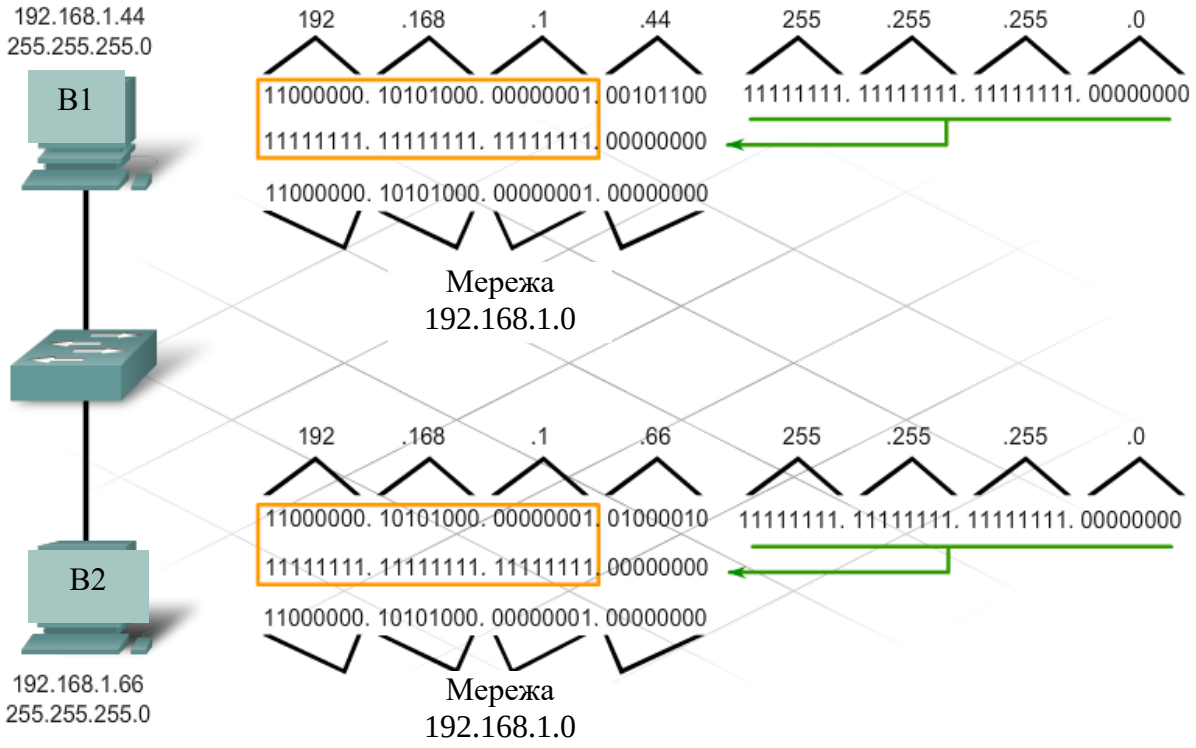


Рисунок 4.5 – Розрахунок підмереж з використанням двійкового представлення

Хоча досить легко визначити мережеву й вузлову частини IP-адреси, коли маска підмережі закінчується на кордони мережі, процес визначення мережевих бітів виконується точно так само, навіть якщо мережева частина становить не цілий октет. Наприклад, IP-адресу вузла H1 – 192.168.13.21 з маскою підмережі 255.255.255.248, або /29. Це означає, що з 32 бітів 29 утворять мережеву частину адреси. Мережеві біти втримуються в перших трьох октетах і частині четвертого октету. У цьому випадку значення ідентифікатора мережі – 192.168.13.16.

Щоб вузол H1 з IP-адресою 192.168.13.21/29 міг обмінюватися даними з іншим вузлом, H2, з адресою 192.168.13.25/29, необхідно порівнювати мережеву частину адреси цих двох вузлів, щоб визначити, чи перебувають вони в одній і тій же локальній мережі. У цьому випадку мережеве значення вузла H1 становить 192.168.13.16, а мережеве значення вузла H2 – 192.168.13.24. Вузли H1 і H2 розташовані в різних мережах, і для обміну даними між ними необхідно використовувати маршрутизатор.

Процес базової розбивки на підмережі

Використовуючи схему ієрархічної адресації, можна багато чого довідатися, дивлячись на IP-адреса й запис маски підмережі косою рискою (/x). Наприклад, IP-адресу 192.168.1.75 /26 містить наступні відомості:

Десяткова маска підмережі

Позначення /26 означає маску підмережі 255.255.255.192.

Число створюваних підмереж

Припустимо, що ми почали з маски підмережі за замовчуванням /24, то тоді 2 додаткових біти вузла запозичені для мережі. Це дозволяє створити 4 підмережі (2^2 = 4).

Число вузлів, придатних для використання в кожної підмережі

Шість бітів залишені для вузла, що дає 62 вузла в кожної підмережі:
(2^6 = 64 – 2 = 62).

Мережева адреса

Використовуючи маску підмережі для визначення розміщення мережевих бітів, можна одержати значення мережевої адреси. У цьому прикладі це значення дорівнює 192.168.1.64.

Перша застосовна адреса вузла

Серед бітів вузла не можуть утримуватися всі нулі, оскільки вони відповідають мережевій адресі підмережі. Отже, першою застосовною адресою вузла в підмережі .64 буде .65.

Широкомовна адреса

Серед бітів вузла не можуть утримуватися всі одиниці, оскільки вони відповідають широкомовній адресі підмережі. У цьому випадку як адресу широкомовного розсилання використовується .127. Мережева адреса наступної підмережі починається з .128.

Підме-режа	Мережева адреса	Діапазон адрес вузлів	Широкомовна адреса
0	192.168.1.0/26	192.168.1.1 – 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 – 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129- 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 – 192.168.1.254	192.168.1.255

Рисунок 4.6 – Приклад схеми адресації для 4-х мереж

Маска підмережі змінної довжини VLSM

Базової розбивки на підмережі досить для невеликих мереж, але воно не забезпечує гнучкості, необхідної для великих корпоративних мереж.

Маски підмережі змінної довжини (VLSM) забезпечують ефективне використання адресного простору. Вони також дозволяють використовувати ієрархічну IP-адресуцію, за рахунок якої маршрутизатори можуть ефективно застосовувати підсумовування маршрутів. Підсумовування маршрутів знижує розмір таблиць маршрутизації в розподільних і основних маршрутизаторах. При зменшенні розміру таблиць маршрутизації ЦПУ потрібно менше часу для пошуку маршрутів.

VLSM – це концепція, використовувана при поділі підмережі на підмережі. Вони були споконвічно розроблені для підвищення ефективності адресації. Із впровадженням приватної адресації основна перевага VLSM у цей час – організація й об'єднання.

VLSM підтримується не всіма протоколами маршрутизації. Класові протоколи маршрутизації (наприклад, RIPv1) не включають поле маски підмережі на відновлення маршрутизації. Якщо маска підмережі призначена інтерфейсу маршрутизатора, він уважає, що всім пакетам одного класу призначена та сама маска підмережі.

Безкласові протоколи маршрутизації підтримують використання VLSM, оскільки маска підмережі передається з усіма пакетами з

відновленням маршрутизації. До безкласових протоколів маршрутизації ставляться RIPv2, EIGRP і OSPF.

Переваги VLSM:

– дозволяє ефективно використовувати адресний простір;

– дозволяє використовувати маски підмережі різної довжини;

– розбиває блок адрес на менш великі блоки;

– дозволяє підсумувати маршрути;

– забезпечує більшу гнучкість при конструюванні мережі;

– підтримує ієрархічні корпоративні мережі.

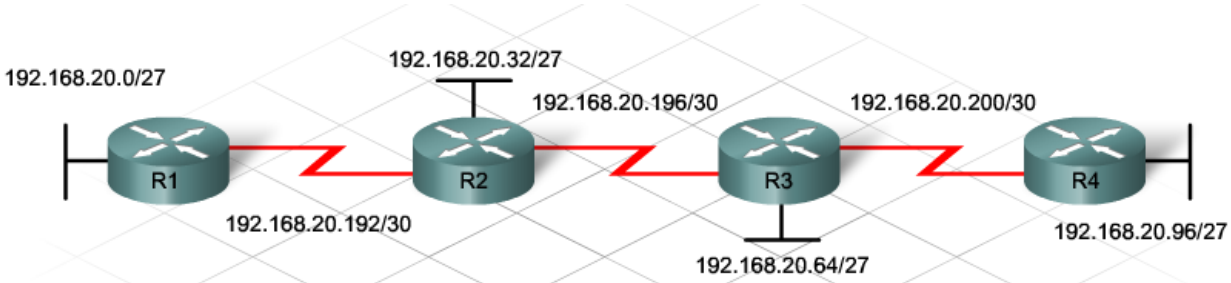
VLSM дозволяє використовувати для кожної підмережі свою маску. Після поділу мережевої адреси на підмережі при подальшому дробленні цих підмереж створюються під-підмережі.

Наприклад, мережа 10.0.0.0/8 з маскою підмережі /16 ділиться на 256 підмереж, кожна з яких може підтримувати 16 382 вузла.

10.0.0.0/16

10.1.0.0/16

10.2.0.0/16 до 10.255.0.0/16



Підмережі 192.168.20.0	
Номер підмережі	Адреса підмережі
Підмережа 0	192.168.20.0/27
Підмережа 1	192.168.20.32/27
Підмережа 2	192.168.20.64/27
Підмережа 3	192.168.20.96/27
Підмережа 4	192.168.20.128/27
Підмережа 5	192.168.20.160/27
Підмережа 6	192.168.20.192/27
Підмережа 7	192.168.20.224/27

Підмережі 192.168.20.192	
Номер підмережі	Адреса підмережі
Підмережа 0	192.168.20.192/30
Підмережа 1	192.168.20.196/30
Підмережа 2	192.168.20.200/30
Підмережа 3	192.168.20.204/30
Підмережа 4	192.168.20.208/30
Підмережа 5	192.168.20.212/30
Підмережа 6	192.168.20.216/30
Підмережа 7	192.168.20.220/30

Рисунок 4.7 – Маска підмережі змінної довжини (VLSM)

Застосувавши маску підмережі /24 до кожної із цих підмереж /16 (наприклад, 10.1.0.0/16), можна одержати розбивку на 256 підмереж. У кожній із цих нових підмереж можна підтримувати 254 вузла.

10.1.1.0/24

10.1.2.0/24

10.1.3.0/24 до 10.1.255.0/24

Застосувавши маску підмережі /28 до кожної із цих підмереж /24 (наприклад, 10.1.3.0/28), можна одержати розбивку на 16 підмереж. У кожній із цих нових підмереж можна підтримувати 14 вузлів.

10.1.3.0/28

10.1.3.16/28

10.1.3.32/28 до 10.1.3.240/28

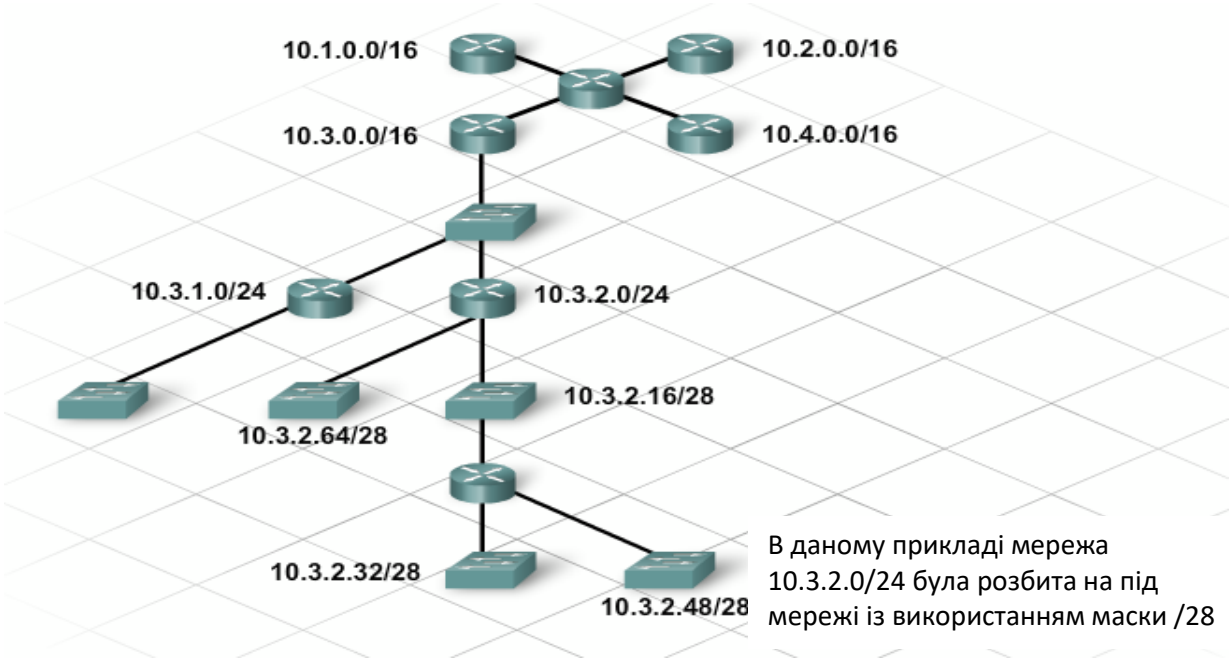


Рисунок 4.8 – Приклад застосування VLSM

Конструювання схеми IP-адресації з використанням VLSM вимагає досвіду й планування. У цій практичній вправі до мережі пред'являються наступні вимоги:

– головний офіс в Києві = 58 адрес вузлів;

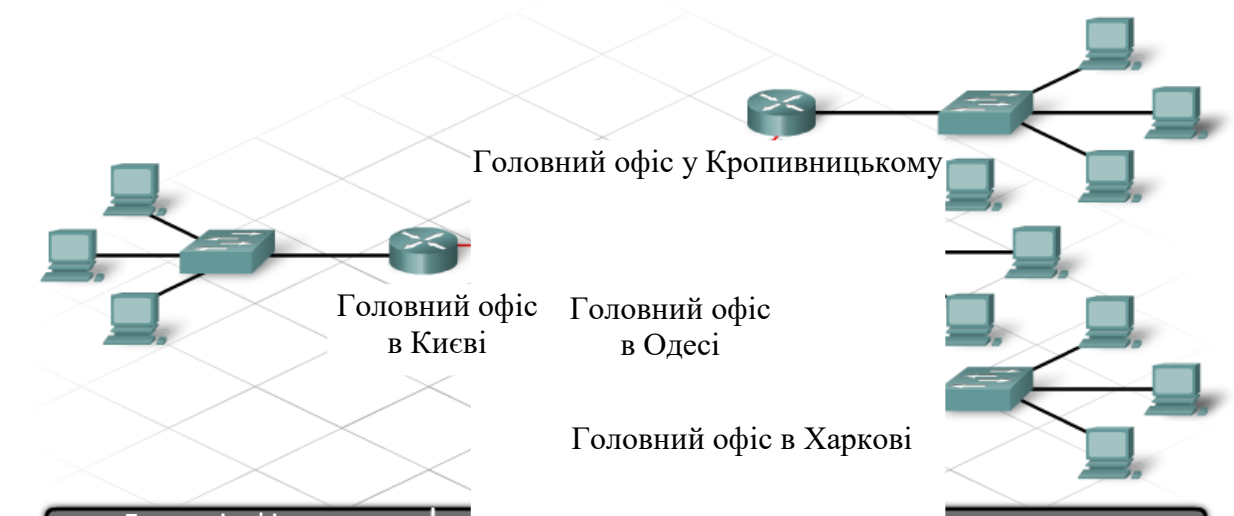
– головний офіс у Харкові = 26 адрес вузлів;

– головний офіс у Одесі = 10 адрес вузлів;

– головний офіс у Кропивницькому = 10 адрес вузлів;

– канали зв'язку через мережі WAN = 2 адреси вузлів (кожний).

Для підтримки найбільшої ділянки мережі, що складає з 58 вузлів, необхідна підмереж /26. Використання схеми базової розбивки на підмережі просто нераціонально, оскільки в результаті створюється тільки чотири підмережі. Цього недостатньо для виділення адрес для кожного із семи необхідних сегментів мережі LAN/WAN. Використання схеми адресації VLSM вирішує цю проблему.



Головні офіси	Фактичні вимоги	Всього втрачених адрес
Головний офіс в Києві	58 адрес вузлів	4 адреси
Головний офіс в Харкові	26 адрес вузлів	36 адрес
Головний офіс в Одесі	10 адрес вузлів	52 адреси
Головний офіс у Кропивн.	10 адрес вузлів	52 адреси
Канали WAN	2 адреси вузлів	60 адрес

Рисунок 4.9 – Приклад застосування VLSM

При реалізації схеми розбивки на підмережі VLSM, плануючи вимоги до підмережі, завжди враховуйте можливе збільшення числа вузлів.

Для допомоги при плануванні адресації існує безліч інструментальних засобів.

Схема VLSM

В одному з методів використовується схема VLSM, щоб визначити, які блоки адрес доступні і які з них уже призначені.

Коло VLSM

В іншому методі використовується підхід кола. Коло ділиться на всі зменшувані сегменти, що відповідають більше дрібним підмережям.

Ці методи запобігають призначення вже виділених адрес. Вони також дозволяють уникнути призначення діапазонів, що перекриваються, адрес.

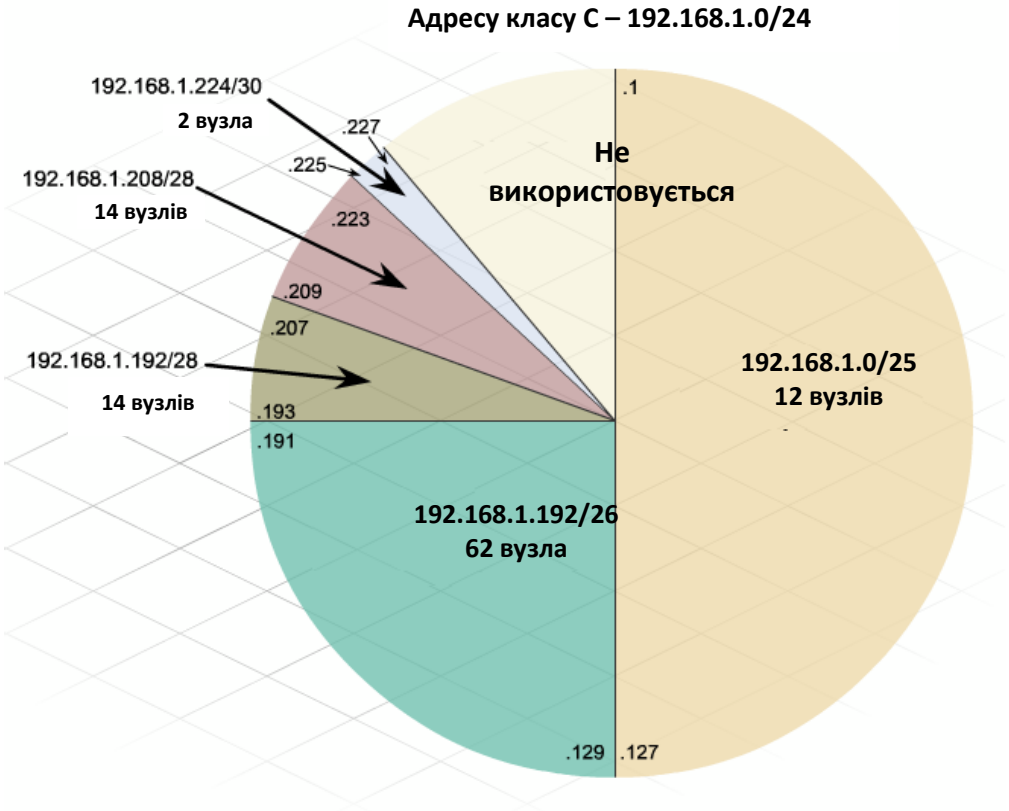


Рисунок 4.10 – Коло VLSM

РОЗДІЛ 5. СТАТИЧНІ ТА ДИНАМІЧНІ IP-АДРЕСИ

IP-адреси можна привласнювати статично або динамічно.

Статична адреса

Використовуючи статичну адресу, мережевий адміністратор може вручну налаштувати мережеві дані вузла. Як мінімум, це буде IP-адресу, маска підмережі й шлюз за замовчуванням.

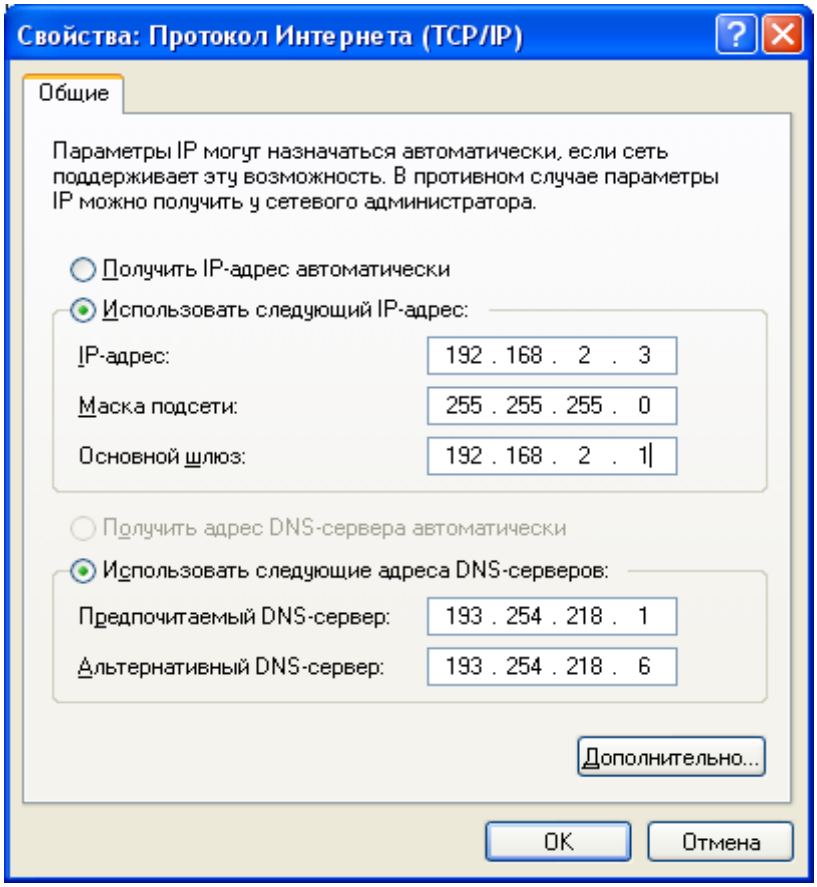


Рисунок 5.1 – Привласнення статичної адреси

У статичних адрес є декілька переваг. Наприклад, їх корисно привласнювати принтерам, серверам та іншим мережевим пристроям, які завжди повинні бути доступні мережевим клієнтам. Якщо звичайно вузли підключаються до сервера з певною IP-адресою, можуть виникнути помилки якщо вона раптом зміниться.

Статичне присвоєння адрес підсилює контроль над мережевими ресурсами, але введення інформації для кожного вузла забирає багато часу. При статичному введенні вузол виконує тільки базовий пошук помилок в IP-адресі. Відповідно, ризик виникнення помилки більше.

При використанні статичної IP-адресації важливо вести точний перелік адрес і пристроїв, яким вони привласнені. Крім того, звичайно ці постійні адреси повторно не використовуються.

Динамічні адреси

Список користувачів локальної мережі часто змінюється. З'являються нові користувачі з ноутбуками, яких потрібно підключити. Інші встановлюють нові робочі станції. Щоб кожній станції не доводилося вручну привласнювати IP-адреси, простіше всього це зробити автоматично. Для цього використовується протокол за назвою Dynamic Host Configuration Protocol (DHCP).

DHCP передбачає механізм автоматичного присвоєння інформації про адресу, наприклад, IP-адреси, маски підмережі, шлюзу за замовчуванням і інші налаштування.

Це найкращий спосіб присвоєння IP-адрес вузлам у великій мережі, оскільки він полегшує роботу фахівців служби підтримки й практично усуває можливість помилки.

Інша перевага DHCP полягає в тому, що адреси привласнюються вузлам тимчасово. Якщо вузол вимикається або йде з мережі, його адресу вертається в пул для повторного використання. Це особливо корисно для мобільних користувачів, які то підключаються, то відключаються.

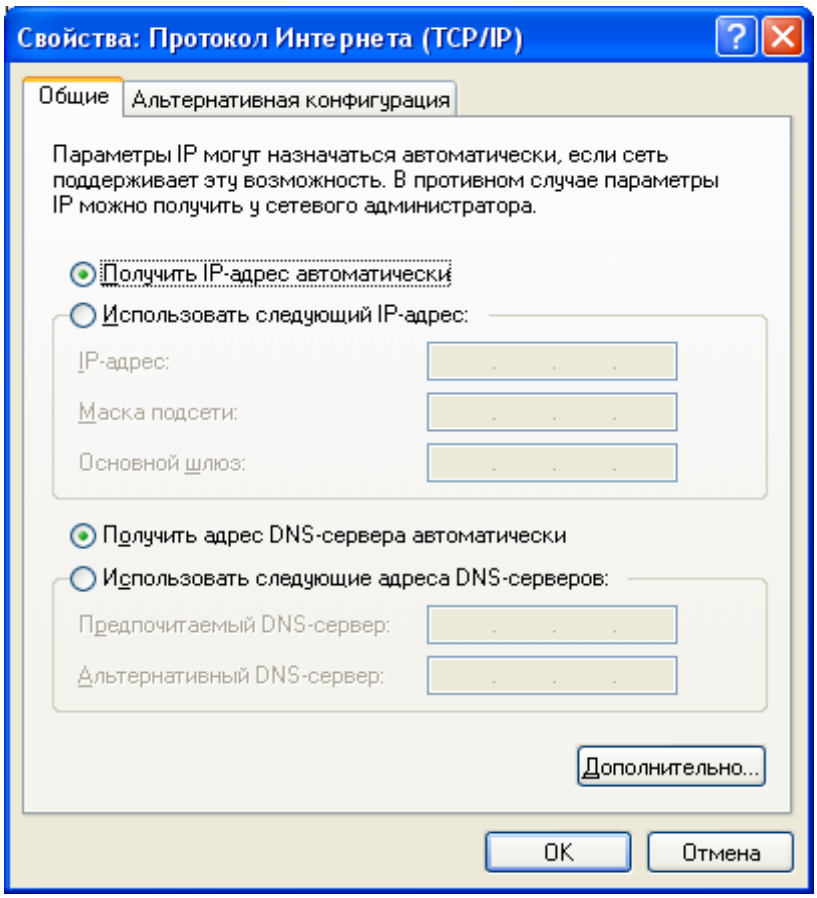


Рисунок 5.2 – Налаштування на отримання динамічної адреси

Сервери DHCP

Коли ви підключаєтеся до бездротової мережі в аеропорті або магазині, доступ в Інтернет забезпечує DHCP. При вході в зону зв'язку встановлений на ноутбуці клієнт DHCP зв'язується з локальним сервером DHCP через бездротове з'єднання. Сервер DHCP привласнює ноутбуку IP-адресу.

У більшості середніх і великих мереж сервер DHCP – це локальний виділений сервер на базі ПК. У домашніх мережах він звичайно перебуває у Інтернет-провайдера. Вузол з домашньої мережі одержує налаштування IP безпосередньо від Інтернет-провайдера.

У багатьох домашніх і невеликих корпоративних мережах для підключення до модему Інтернет-провайдера використовується вбудований маршрутизатор. У цьому випадку він виступає як клієнт і сервер DHCP. Як

клієнт він одержує налаштування IP від Інтернет-провайдера, а потім, уже як сервер DHCP, передає їхнім внутрішнім вузлам локальної мережі.

Крім серверів на базі ПК і вбудованих маршрутизаторів, послуги DHCP можуть надавати клієнтам і інші мережеві пристрої, наприклад, виділені маршрутизатори. Таке зустрічається рідше.

При першому налаштуванні як клієнта DHCP у вузла немає IP-адреси, маски підмережі й шлюзу за замовчуванням. Він одержує ці дані від сервера DHCP, локального або приналежного Інтернет-провайдеру. На сервері DHCP налаштовується діапазон, або пул, IP-адрес, які можна привласнити клієнтам DHCP.

Клієнт, якому потрібна IP-адреса, посилає повідомлення про пошук DHCP у вигляді широкомовного розсилання з IP-адресою одержувача 255.255.255.255 (32 одиниці) і MAC-адресою одержувача FF-FF-FF-FF-FF-FF (48 одиниць). Кадр DHCP одержать всі вузли в мережі, але відповість тільки сервер DHCP. Він відправляє джерелу запропоновану IP-адресу клієнта. Вузол у відповідь посилає на зазначений сервер запит DHCP з підтвердженням використання IP-адреси. Сервер надсилає підтвердження.

Рисунок 5.3 – Налаштування DHCP

У більшості домашніх і невеликих корпоративних мережах послуги DHCP надає локальним мережевим клієнтам багатофункціональний пристрій.

Кордони мережі й простір адрес

Маршрутизатор створює шлюз, через який вузли однієї мережі можуть обмінюватися даними з вузлами інших мереж. Кожний інтерфейс маршрутизатора підключається до окремої мережі.

Привласнена інтерфейсу IP-адресу ідентифікує безпосередньо підключену локальну мережу.

Кожний вузол у мережі обов'язково використовує як шлюз в інші мережі маршрутизатор. Відповідно, кожний вузол повинен знати IP-адресу інтерфейсу маршрутизатора, підключеного до його мережі. Він називається адресою шлюзу за замовчуванням. Адресу можна статично налаштувати на рівні вузла або одержати динамічно, із сервера DHCP.

Коли вбудований маршрутизатор перетворюється в сервер DHCP локальної мережі, він автоматично розсилає всім вузлам IP-адреси потрібного інтерфейсу. Після цього всі вузли в мережі зможуть використовувати цей IP-адресу для передачі повідомлень вузлам Інтернет-провайдера й одержання доступу до вузлів в Інтернеті. Звичайно убудовані маршрутизатори за замовчуванням стають серверами DHCP.

IP-адресу даного інтерфейсу локального маршрутизатора стає адресою шлюзу за замовчуванням у даній конфігурації вузлів. Шлюз за замовчуванням надається статично або через DHCP.

Стаючи сервером DHCP, вбудований маршрутизатор надає клієнтам DHCP свою внутрішню IP-адресу як шлюз за замовчуванням. Крім того, він розсилає вузлам IP-адреси й маски підмережі.

Рисунок 5.4 – Кордони мережі й простір адрес

Механізм присвоєння IP-адреси в локальній мережі

Маршрутизатор, що знаходиться на межі між локальною та глобальною мережею, виступає в якості сервера DHCP для всіх підключених до нього локальних вузлів. Більшість серверів DHCP привласнюють вузлам з внутрішньої мережі приватні адреси. Це означає, що за замовчуванням внутрішня мережа безпосередньо з Інтернету недоступна.

Зазвичай вибрана за замовчуванням IP-адресу інтерфейсу локального вбудованого маршрутизатора є приватною адресою класу С. Внутрішнім вузлам потрібно присвоїти адреси мережі, в якій знаходиться вбудований маршрутизатор (статично або через DHCP). Вбудований маршрутизатор, що працює як сервер DHCP, надає адреси з цього діапазону. Крім того, він надає дані про маску підмережі і IP-адресу свого інтерфейсу (шлюз за замовчуванням).

Крім того, багато Інтернет-провайдерів за допомогою серверів DHCP надають IP-адреси для прямого виходу вбудованого маршрутизатора

користувача в Інтернет. Мережа, до якої маршрутизатор підключений в Інтернеті, називається зовнішньою.

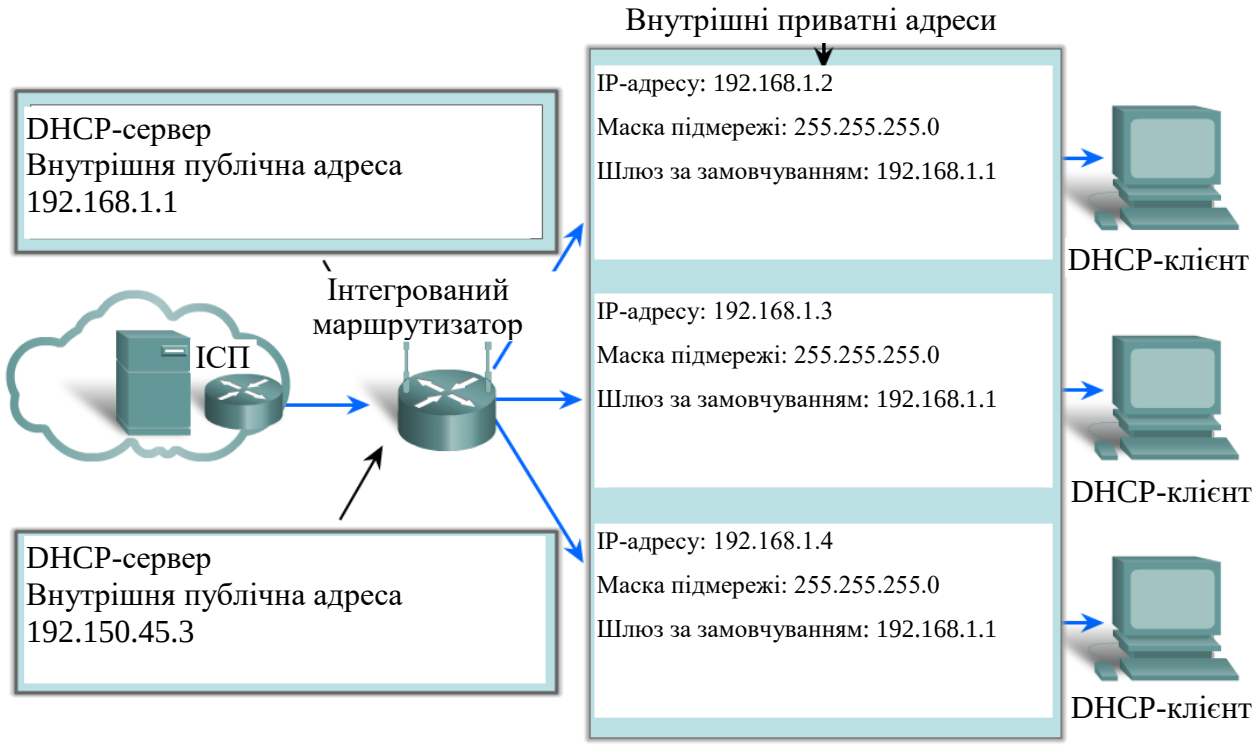


Рисунок 5.5 – Присвоєння IP-адреси в локальній мережі

Підключений до Інтернет-провайдеру вбудований маршрутизатор працює як клієнт DHCP, отримуючи правильну IP-адресу зовнішньої мережі для інтерфейсу Інтернет. Зазвичай Інтернет-провайдер надає маршрутизовану в Інтернеті адресу, за допомогою якої вузли можуть підключатися до вбудованого маршрутизатора і до Інтернету.

Маршрутизатор розмежовує локальну внутрішню мережу і зовнішню мережу.

Вузли можуть підключатися до Інтернет-провайдеру та Інтернету декількома способами. Отримання загальної або приватної адреси залежить від методу підключення вузла.

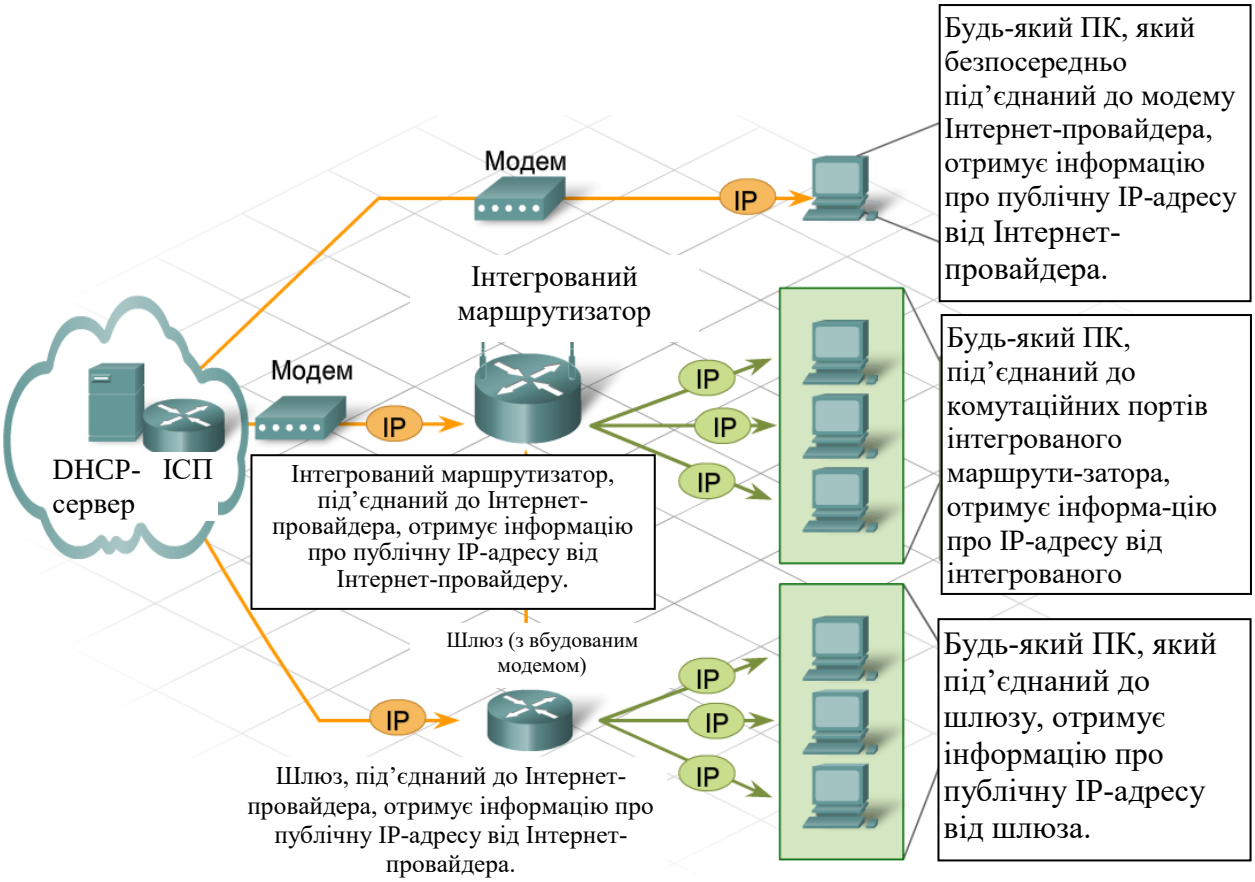


Рисунок 5.6 – Методи підключення локальних вузлів до Інтернету.

Зверху донизу:

– пряме підключення,

– підключення через вбудований маршрутизатор,

– підключення через шлюз

Пряме підключення

У деяких клієнтів є тільки один комп'ютер з безпосереднім підключенням до Інтернет-провайдера через модем. У даному випадку загальна адреса з сервера DHCP Інтернет-провайдера присвоюється тільки одному вузлу.

Підключення через вбудований маршрутизатор

Якщо до Інтернету потрібно підключити декілька вузлів, модем Інтернет-провайдера можна з'єднати не з одним комп'ютером, а безпосередньо з вбудованим модемом. Таким чином створюється домашня

або невелика корпоративна мережа. Вбудований маршрутизатор отримує від Інтернет-провайдера загальні адреси. Внутрішні вузли отримують від маршрутизатора приватні адреси.

Підключення через шлюз

Шлюзи об'єднують в собі вбудований маршрутизатор і модем і підключаються безпосередньо до Інтернет-провайдеру. Як і у випадку з вбудованими маршрутизаторами, шлюз отримує від Інтернет-провайдера загальну адресу, а ПК у внутрішній мережі отримують від шлюзу приватні адреси.

РОЗДІЛ 6. МЕРЕЖЕВІ АДРЕСИ NAT ТА PAT

Перетворення IP-адреси NAT

Перетворення мережевих адрес (NAT) дозволяє великій групі приватних користувачів підключатися до Інтернету через невеликий пул публічних IP-адрес. Ця система працює приблизно так само, як телефонна система усередині компанії. По досягненні певної кількості персоналу співробітники перестають підключатися безпосередньо до загальнодоступної телефонної лінії. Замість цього кожному співробітникові компанії привласнюється додатковий номер. Це можливо тому, що не всі вони одночасно користуються телефоном. При використанні приватних додаткових номерів компанія може скоротити кількість зовнішніх ліній, які орендуються в телефонної компанії.

NAT працює приблизно так само, як внутрішня телефонна лінія. Одна з основних причин створення NAT – можливість заощадити зареєстровані IP-адреси. Крім того, NAT забезпечує безпеку комп'ютерів, серверів і мережевих пристроїв, блокуючи безпосередній доступ в Інтернет з реального IP-адреси вузла.

Основна перевага NAT – можливість повторного використання IP-адрес і спільного використання унікальних у глобальному масштабі IP-адрес численними вузлами всередині однієї локальної мережі. Крім того, NAT забезпечує прозорість роботи користувачів. Інакше кажучи, для того, щоб вийти в Інтернет із приватної мережі, їм не потрібно знати про NAT.

Одна з переваг NAT полягає в тому, що окремі вузли недоступні з Інтернету напряму. Тобто, NAT дозволяє заблокувати доступ до приватної мережі ззовні.

В NAT є певні недоліки, зокрема:

1. Вплив на певні додатки, де в інформаційному наповненні повідомлення використовуються IP-адреси. Такі IP-адреси також потрібно

перетворювати, збільшуючи навантаження на процесор маршрутизатора. Додаткове навантаження знижує ефективність мережі.

2. NAT приховує приватні IP-адреси від загальнодоступних мереж. Контроль доступу в деяких випадках бажаний, але може виявитися й недоліком у тому випадку, якщо потрібний віддалений доступ до пристрою в приватній мережі з Інтернету.

3. У процесі налаштування NAT на маршрутизаторі використовується декілька термінів, що допомагають інтерпретувати процес реалізації NAT.

Внутрішня локальна мережа – будь-яка мережа, підключена до інтерфейсу маршрутизатора й вхідна у локальну мережу із приватною адресацією. IP-адреси вузлів у внутрішніх мережах перетворяться до передачі зовнішнім адресатам.

Зовнішня глобальна мережа – це будь-яка мережа, підключена до зовнішнього стосовно локальної мережі маршрутизатора й не розпізнає приватні адреси вузлів у локальній мережі.

Внутрішня локальна адреса – це приватна IP-адреса вузла по внутрішній мережі. До передачі за межі структури адресації локальної мережі його потрібно перетворити.

Внутрішня глобальна адреса – це IP-адресу внутрішнього вузла, що використовується в зовнішній мережі. Це перетворена IP-адреса.

Зовнішня локальна адреса – це адресу вузла призначення пакета, що перебуває в локальній мережі. Звичайно вона збігається із зовнішньою глобальною адресою.

Зовнішня глобальна адреса – це реальна приватна IP-адреса зовнішнього вузла. Адресу виділяється із простору глобально маршрутизуємих адрес або мережевих адрес.

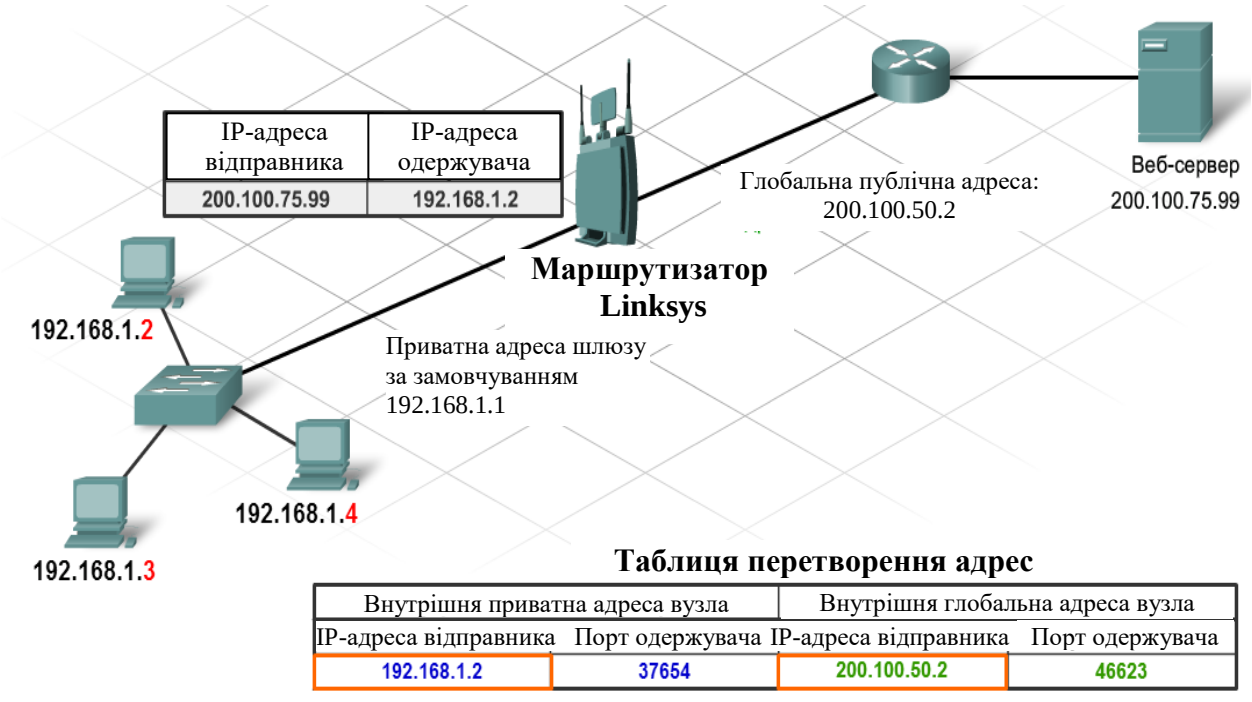
Вбудований маршрутизатор отримує від Інтернет-провайдера загальну адресу, що дозволяє відправляти і отримувати пакети через Інтернет. Він, у свою чергу, надає локальним мережевим клієнтам приватні

адреси. Оскільки в Інтернеті приватні адреси не використовується, при вході клієнтів в Інтернет їх потрібно перетворити в унікальні загальні адреси.

Процес перетворення приватних адрес в маршрутизовані в Інтернеті адреси називається перетворенням мережевих адрес (NAT). За допомогою NAT приватна (локальна) IP-адресу джерела перетворюється на загальну (глобальну) адресу. Вхідні пакети проходять зворотний процес. Використовуючи NAT, вбудований маршрутизатор може перетворити багато внутрішніх IP-адрес в одну загальну.

Перетворювати потрібно тільки адреси пакетів, які йдуть в інші мережі. Вони в обов'язковому порядку проходять через шлюз, де вбудований маршрутизатор замінює приватну IP-адресу вузла-джерела на свою загальну IP-адресу.

Хоча кожному вузлу у внутрішній мережі присвоєно унікальну приватну IP-адресу, вони використовують одну і ту ж маршрутизовану в Інтернеті адресу вбудованого маршрутизатора.



Таблиця перетворення адрес

Внутрішня приватна адреса вузла		Внутрішня глобальна адреса вузла	
IP-адреса відправника	Порт одержувача	IP-адреса відправника	Порт одержувача
192.168.1.2	37654	200.100.50.2	46623

Рисунок 6.1 – Перетворення мережевих адрес

NAT на стороні підприємства

Багато організацій хочуть використовувати переваги приватних адрес при підключенні до Інтернету. Організації створюють величезні локальні і глобальні мережі з приватною адресацією і підключаються до Інтернету з використанням перетворення мережевих адрес (NAT).

Технологія NAT перетворює внутрішні приватні адреси в одну або декілька публічних адрес для маршрутизації в мережі Інтернет. NAT змінює локальну приватну IP-адресу всередині кожного пакету на публічно зареєстровану IP-адресу до передачі його в Інтернет.

Організації малого та середнього бізнесу підключаються до постачальника інтернет-послуг, використовуючи єдине підключення. Локальний прикордонний маршрутизатор, на якому налаштована технологія NAT, підключається до постачальника інтернет-послуг. Більш великі організації можуть використовувати декілька підключень до постачальника інтернет-послуг, і в кожному з цих місць розташування прикордонний маршрутизатор виконує перетворення мережевих адрес.

Використання NAT на прикордонних маршрутизаторах підвищує безпеку. Внутрішні приватні адреси перетворюються щоразу в різні публічні адреси. Це дозволяє приховати реальну адресу вузлів і серверів підприємства. Більшість маршрутизаторів, що використовують перетворення NAT, також блокують пакети, що надходять ззовні приватної мережі за винятком випадків, коли вони надходять у відповідь на запит від внутрішнього вузла.

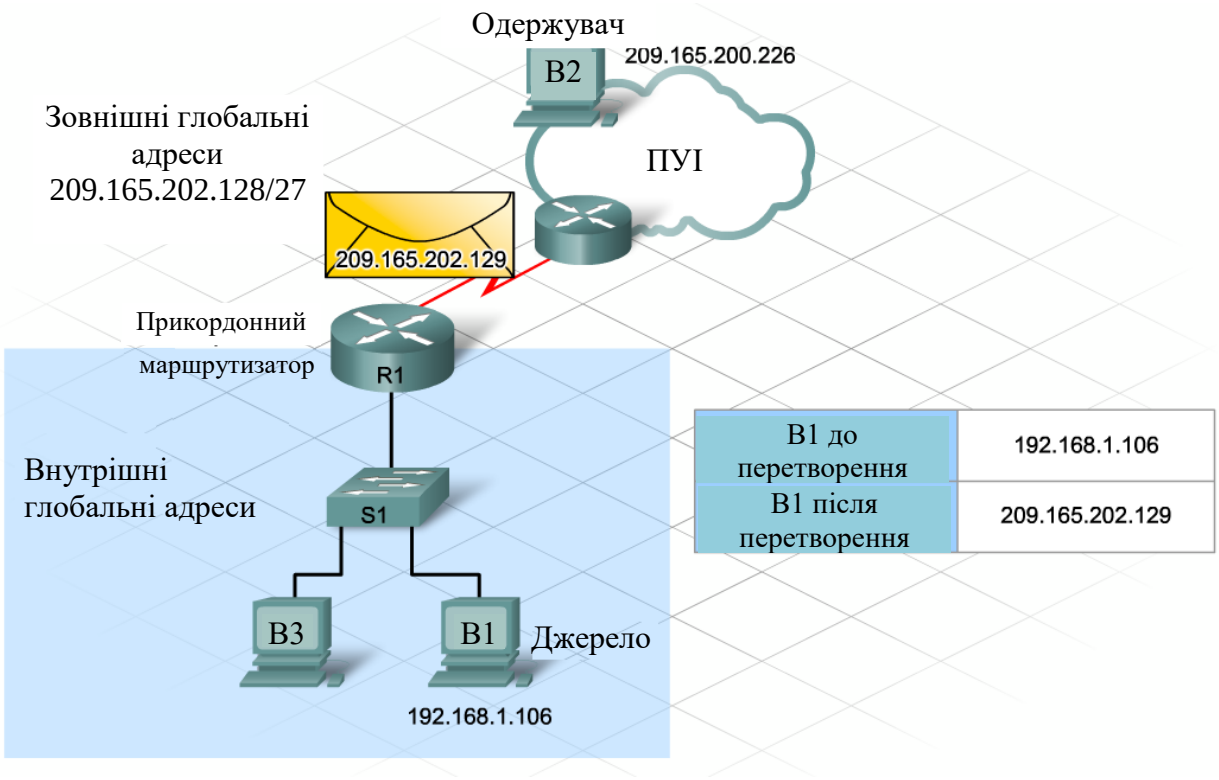


Рисунок 6.2 – NAT на стороні підприємства

Статичне і динамічне перетворення NAT

Можна налаштувати перетворення NAT статично або динамічно.

Статичне перетворення NAT зіставляє єдину внутрішню локальну адресу з єдиною глобальною чи публічною адресою. Це зіставлення дозволяє завжди пов'язувати певну внутрішню локальну адресу з одною і тою ж публічною адресою. Статичне перетворення NAT гарантує, що зовнішні пристрої завжди отримують доступ до внутрішнього пристрою. Як приклад можна привести веб-сервери і FTP-сервери, доступні для публіки.

Динамічне перетворення NAT використовує пул доступних публічних Інтернет-адрес і призначає їх внутрішніми адресами. Динамічне перетворення NAT призначає внутрішньому устрою першу доступну IP-адресу з пулу публічних адрес. Цей вузол використовує призначену глобальну IP-адресу протягом усього сеансу. По завершенні сеансу зовнішня глобальна адреса повертається в пул і може використовуватися іншим вузлом.

Для обміну даними між внутрішніми вузлами використовується внутрішня локальна адреса. Публічна адреса, призначена організації, називається внутрішньою глобальною адресою. Внутрішня глобальна адреса іноді використовується як адресу зовнішнього інтерфейсу прикордонного маршрутизатора.

Маршрутизатор NAT управляє перетвореннями внутрішніх локальних і глобальних адрес, оскільки на ньому зберігається таблиця, що містить всі пари адрес.

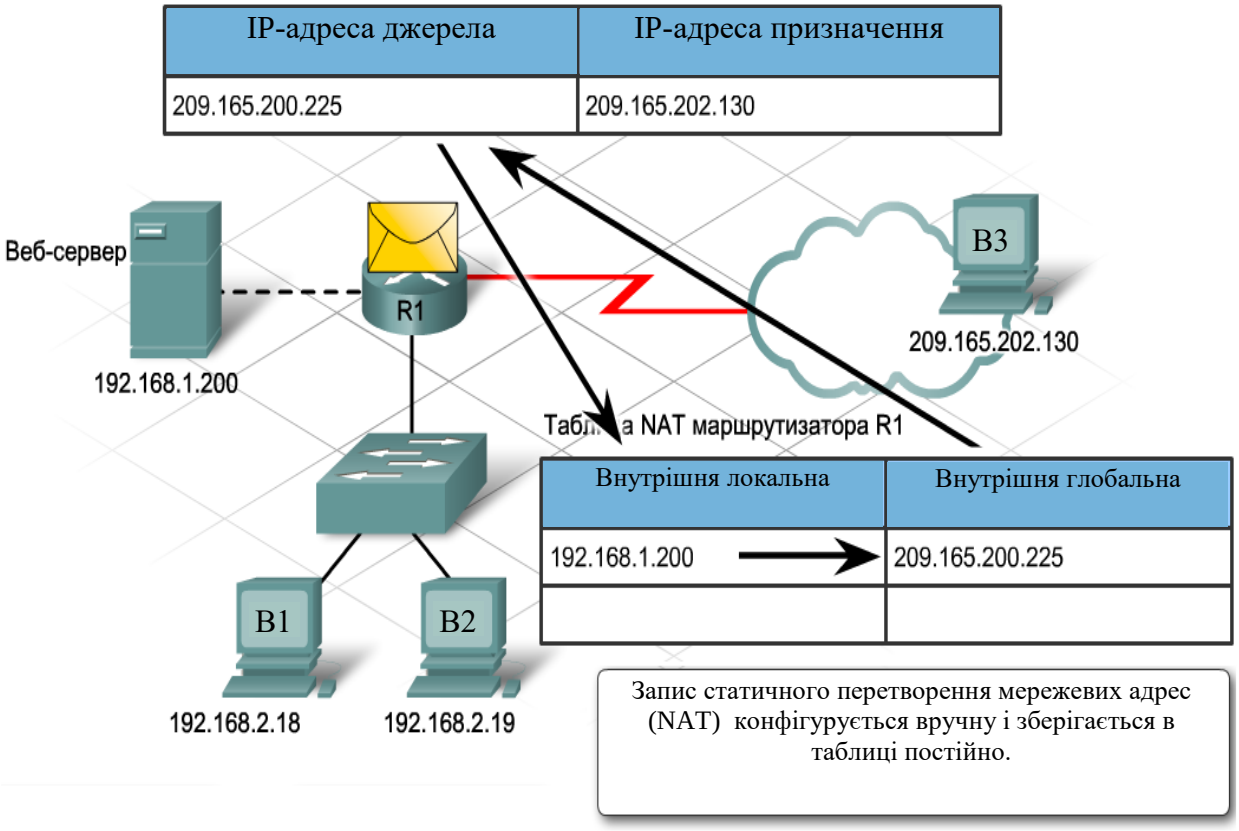


Рисунок 6.3 – Статичне перетворення NAT

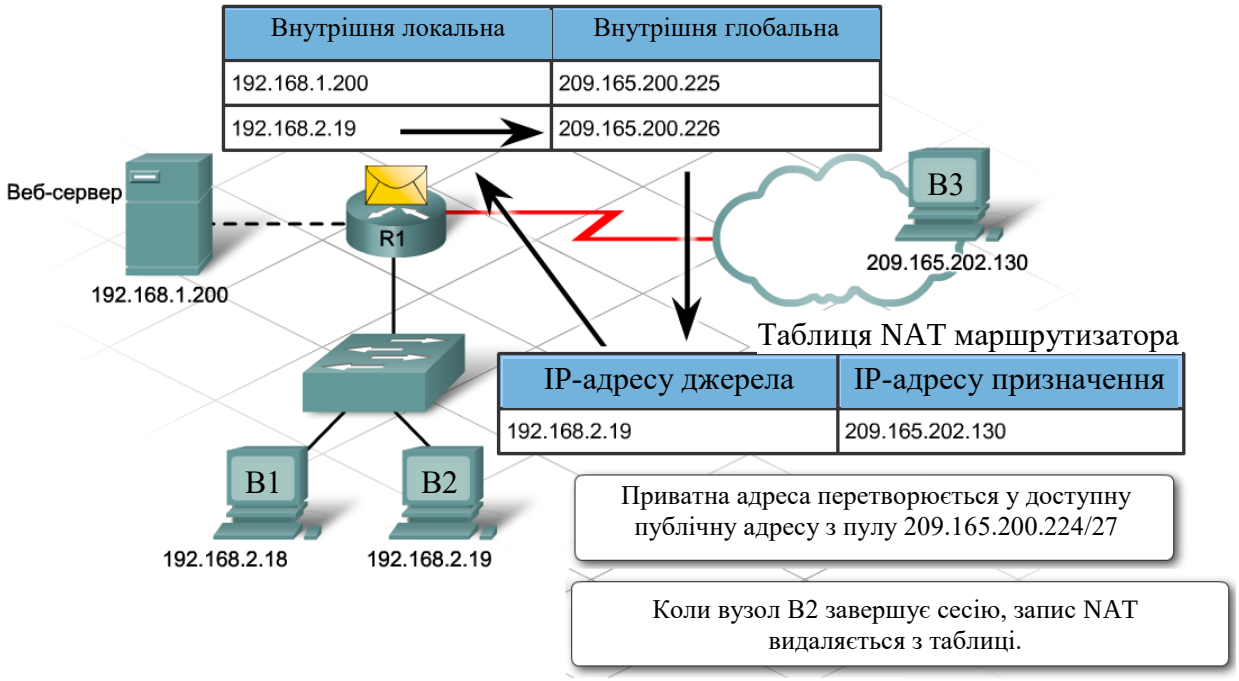


Рисунок 6.4 – Динамічне перетворення NAT

При налаштуванні статичного чи динамічного перетворення NAT:

– перерахуйте всі сервери, для яких необхідна постійна зовнішня адресу;

– визначте, для яких внутрішніх вузлів необхідне перетворення;

– визначте, які інтерфейси є джерелом внутрішнього трафіку (вони стануть внутрішніми інтерфейсами);

– визначте, який інтерфейс передає трафік в Інтернет (він стане зовнішнім інтерфейсом);

– визначте діапазон доступних публічних адрес.

Налаштування статичного перетворення NAT:

1. Визначте публічну IP-адресу, яку повинні використовувати зовнішні користувачі для отримання доступу до внутрішнього пристрою/серверу. Адміністратори зазвичай використовують адреси, розташовані на початку або в кінці діапазону статичного NAT. Зіставте внутрішню (приватну) адресу з публічною адресою.

2. Налаштуйте внутрішній і зовнішній інтерфейси.

Налагодження динамічного NAT:

1. Вкажіть пул доступних публічних IP-адрес.

2. Створіть список контролю доступу (ACL-список) і вкажіть вузли, для яких потрібно виконувати перетворення.

3. Призначте інтерфейси як внутрішні чи зовнішні.

4. Зв'яжіть список доступу і пул адрес.

Важливою частиною налаштування динамічного перетворення NAT є використання стандартних списків контролю доступу. Стандартні ACL-списки використовуються для завдання діапазону вузлів, для яких необхідно виконувати перетворення. Це виконується у формі дозволу або відмови. У ACL-список може входити вся мережа, підмережа або просто певний вузол. ACL-список може варіюватися від одного рядка до набору з декількох дозволів та відмов.

Статичне перетворення адреси гарантує що приватна IP-адреса окремого вузла буде завжди перетворюватися в ту саму зареєстровану глобальну адресу. Крім того, завдяки цьому адресу ніколи не одержить інший локальний вузол.

Динамічне перетворення NAT відбувається в тому випадку, якщо маршрутизатор привласнює IP-адреси з доступного пула зовнішніх глобальних адрес. Поки сесія відкрита, маршрутизатор відслідковує внутрішні глобальні адреси й відправляє підтвердження внутрішнім пристроям. Наприкінці сеансу він просто повертає внутрішню глобальну адресу в пул.

Динамічне перетворення NAT дозволяє вузлам із приватними IP-адресами з Інтранету підключатися до загальнодоступної мережі, наприклад, мережі Інтернет. Статичне перетворення мережевих адрес (NAT) дозволяє вузлам із загальнодоступної мережі підключатися до окремих вузлів із приватної мережі. Це означає, що при налаштуванні NAT для зовнішнього доступу варто використовувати динамічний варіант NAT. Якщо пристрій із

внутрішньої мережі повинен бути доступний ззовні, використовуйте статичний варіант NAT.

При необхідності обидва методи можна використовувати одночасно.

Якщо зареєстрований пул IP-адрес організації дуже невеликий або якщо в неї є всього одна IP-адреса, до загальнодоступної мережі однаково можуть одночасно підключатися декілька користувачів, з використанням механізму, що називається перевантаженням NAT або перетворенням адрес портів (PAT).

Використання PAT

Один з найбільш популярних варіантів динамічного перетворення NAT називається перетворенням адреси та номера порту (PAT), також відоме як *перевантаження NAT*. PAT динамічно перетворює безліч внутрішніх локальних адрес в один публічний адресу.

PAT перетворить декілька локальних адрес в одну глобальну IP-адресу. Коли вузол джерела відправляє повідомлення вузлу призначення, він використовує поєднання IP-адреси й номера порту й у такий спосіб відслідковує кожний окремий сеанс зв'язку з адресатом. У режимі PAT шлюз перетворить адресу локального джерела й номер порту з пакета в одну глобальну IP-адресу й унікальний номер порту вище 1024. Хоча кожний вузол одержує однакову глобальну IP-адресу, номер порту залишається унікальним.

Відповідний трафік адресується на перетворену IP-адресу й номер порту вузла. У таблиці маршрутизатора перебуває список внутрішніх IP-адрес і номерів портів, які перетворяться в зовнішні адреси. Відповідний трафік направляється на відповідну внутрішню адресу й номер порту. Оскільки в наявності є більше 64 000 портів, маршрутизатору навряд чи не вистачить адрес, як це могло б трапитися при динамічному перетворенні NAT.

Перетворення на основі локальної адреси й локального порту виконується окремо для кожного з'єднання, при якому генерується новий

порт джерела. Наприклад, 10.1.1.1:1025 потрібно окремо перетворити з 10.1.1.1:1026.

Перетворення діє тільки на час з'єднання, так що після завершення обміну даними користувач не зберігає дане сполучення глобальної адреси й порту.

Користувачі із зовнішньої мережі не зможуть установити надійне з'єднання з вузлом мережі, де використовується PAT. Справа не тільки в тому, що локальний або глобальний номер порту неможливо прогнозувати, але й у тому, що шлюз навіть не створює перетворення, поки внутрішній вузол не встановить з'єднання.

Коли вузол джерела відправляє повідомлення вузлу призначення, він використовує поєднання IP-адреси і номера порту і, таким чином, відстежує кожен окремий сеанс зв'язку. При використанні PAT шлюз перетворює поєднання локальної адреси і номера порту джерела в єдину глобальну IP-адресу та унікальний номер порту, значення якого перевищує +1024.

У таблиці маршрутизатора знаходиться список внутрішніх IP-адрес і номерів портів, які перетворюються в зовнішні адреси. Хоча всі вузли перетворюються в одну і ту ж глобальну IP-адресу, номер порту, пов'язаний з сеансом зв'язку, унікальний.

Оскільки доступно більше 64000 портів, малоймовірно, що на маршрутизаторі можуть скінчитися адреси.

Функціями PAT можуть ефективно користуватися як корпоративні, так і домашні мережі. PAT вбудовується в інтегровані маршрутизатори і активізується за замовчуванням.

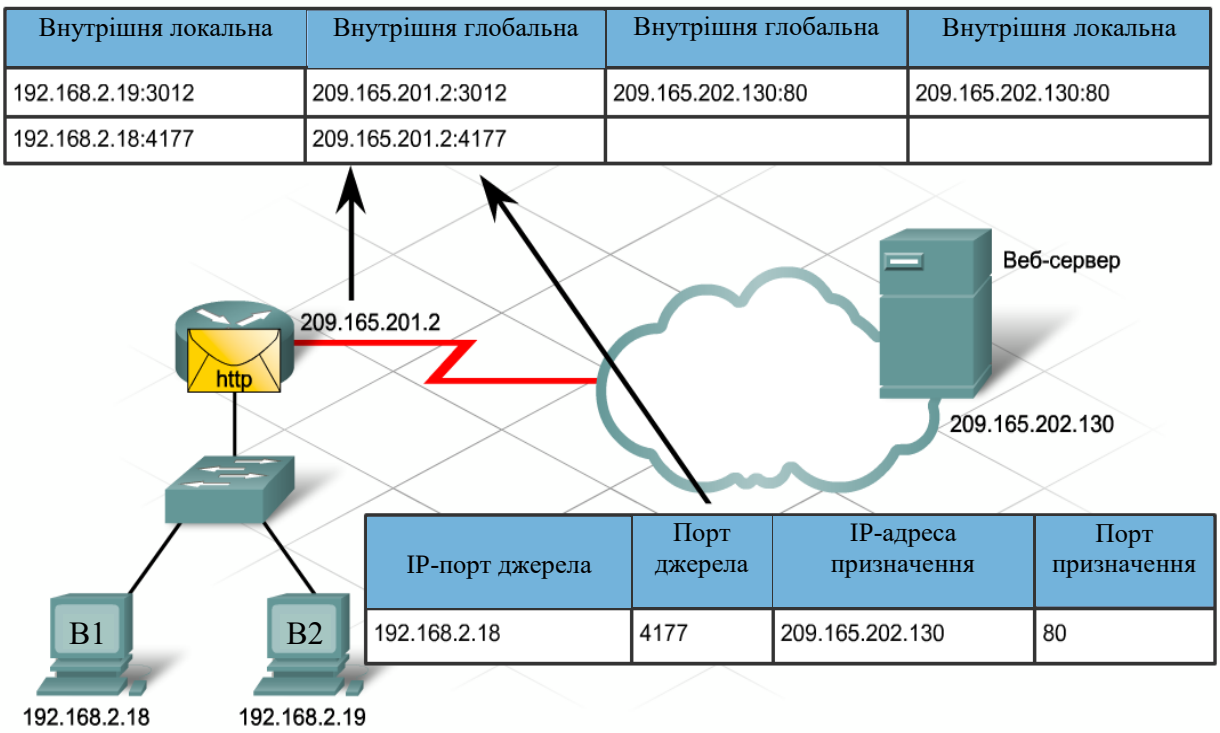


Рисунок 6.5 – Використання PAT

Для налаштування PAT необхідно виконати ті ж самі основні кроки і команди, що і при налаштуванні NAT. Однак замість перетворення в пул адрес PAT перетворює в одну адресу.

Проблеми IP NAT

Більшість операцій NAT відбувається непомітно. Користувачі підключаються до Інтернету із приватних мереж, навіть не знаючи, що для цього робить маршрутизатор. Великий недолік NAT – додаткове навантаження, що створює перетворення IP-адреси й порту.

Деякі додатки збільшують робоче навантаження маршрутизатора, оскільки включають в інкапсульовані дані IP-адресу. Маршрутизатору доводиться замінювати комбінації IP-адрес і портів джерела в пакеті й адреси джерела в заголовку IP.

Через те, що маршрутизатору з підтримкою NAT доводиться виконувати додаткову роботу, для впровадження NAT у мережі потрібне

хороше планування, ретельний підбор устаткування, правильна конфігурація й регулярне обслуговування.

Будучи протоколом з підтримкою IPv4, NAT допоміг відкласти повну відмову від адресного простору IPv4. Функція NAT тепер настільки часто зустрічається в інтегрованих мережевих пристроїв для будинку й невеликих компаній, що деякі думають, що для налаштування потрібно тільки встановити відповідний прапорець. У міру розширення бізнесу й виникнення потреби в більш складних шлюзах і маршрутизаторах налаштування пристроїв для використання NAT і інших функцій стає складніше.

РОЗДІЛ 7. ФІЛЬТРАЦІЯ ТРАФІКУ З ВИКОРИСТАННЯМ СПИСКІВ КОНТРОЛЮ ДОСТУПУ

Фільтрація трафіку

Безпека в корпоративній мережі грає вкрай важливу роль. Важливо запобігти несанкціонованому доступу користувачів і захистити мережу від різного роду атак, таких як DoS-атаки. У випадку несанкціонованого доступу зловмисники можуть змінити, зруйнувати або украсти конфіденційні дані із серверів. DoS-атаки перешкоджають доступу легальних користувачів до ресурсів. В обох випадках компанія гає час і гроші.

Фільтрація трафіку дозволяє адміністраторові контролювати трафік у різних сегментах мережі. Фільтрація являє собою процес аналізу вмісту пакета з метою дозволу або блокування його передачі.

Фільтрація пакетів може бути простою і складною й може забороняти або дозволяти трафік за наступними критеріями:

– вихідна IP-адреса;

– кінцева IP-адреса;

– MAC-адреси;

– протоколи;

– тип додатку.

Фільтрацію пакетів можна зрівняти з фільтрацією небажаної пошти. Багато поштових додатків дозволяють користувачеві налаштовувати автоматичне видалення повідомлень електронної пошти, що приходять із певної вихідної адреси. Фільтрація пакетів може здійснюватися подібним чином шляхом налаштування маршрутизатора на визначення небажаного трафіку.

Фільтрація пакетів дозволяє підвищити продуктивність мережі. Завдяки забороні небажаного або забороненого трафіку близько до його джерела, трафік не передається мережею й не споживає коштовні ресурси.

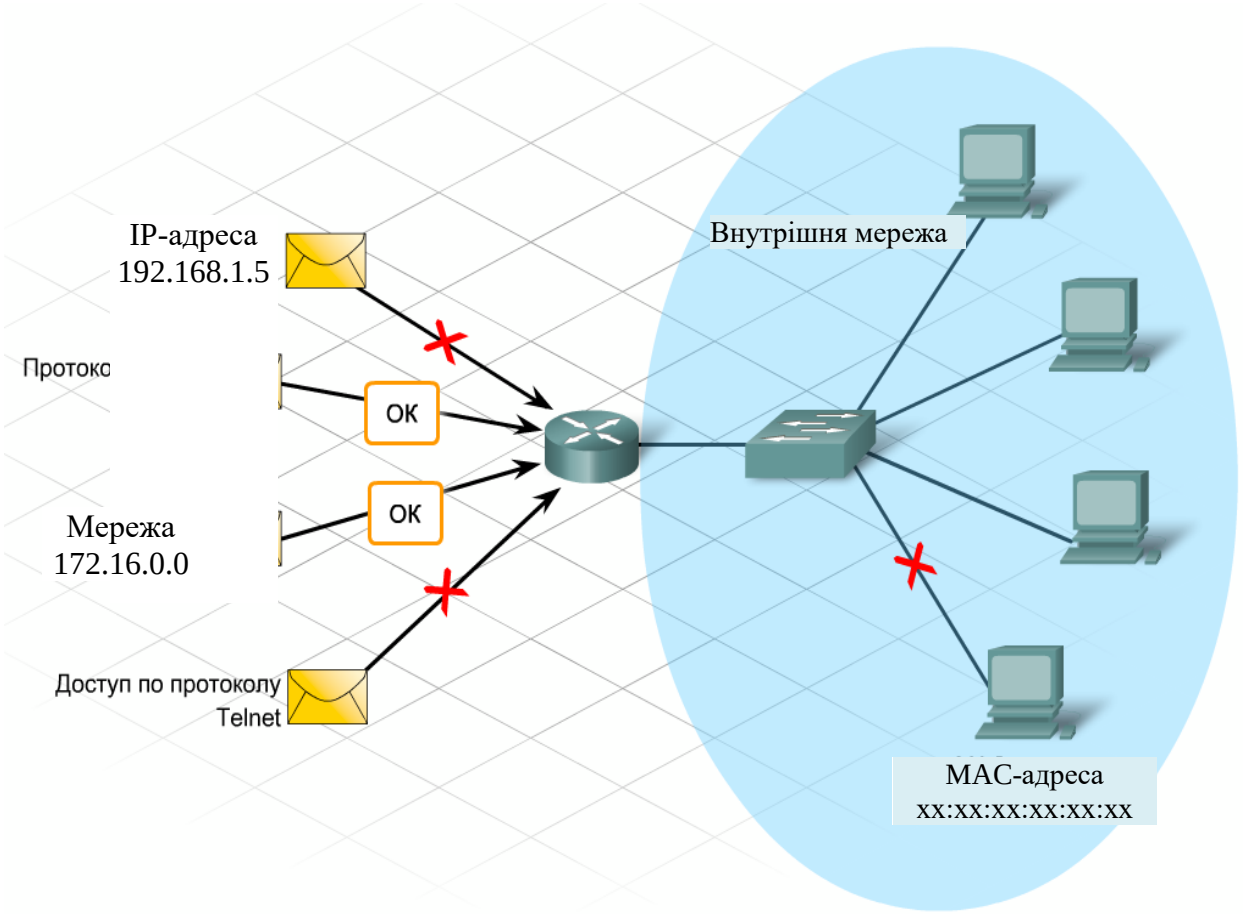


Рисунок 7.1 – Фільтрація пакетів

У число пристроїв, найчастіше використовуваних для фільтрації трафіку, входять наступні:

– брандмауери, вбудовані в інтегровані маршрутизатори;

– виділені пристрої забезпечення безпеки;

– сервери.

Деякі пристрої фільтрують тільки трафік, що виникає у внутрішній мережі. Більше досконалі пристрої безпеки здатні розпізнавати й фільтрувати відомі типи атак із зовнішніх джерел.

Корпоративні маршрутизатори здатні розпізнавати шкідливий трафік і запобігати його втручання в мережу й порушення працездатності мережі. Практично всі маршрутизатори виконують фільтрацію трафіку по вихідним і кінцевим IP-адресах пакетів. Вони також фільтрують певні додатки й протоколи, такі як IP, TCP, HTTP, FTP і Telnet.

Пристрої безпеки Cisco

Серверні міжмережеві екрани

Бездротовий маршрутизатор Linksys з інтегрованим міжмережевим екраном

Маршрутизатор Cisco з міжмережевим екраном Cisco IOS

Рисунок 7.2 – Мережеві пристрої які фільтрують трафік

Списки контролю доступу

Одним з найпоширеніших способів фільтрації трафіку є використання списків контролю доступу (ACL-списків). ACL-списки можна використовувати для керування вхідного й існуючого трафіку у мережі і його фільтрації.

Розмір ACL-списку може варіюватися від однієї інструкції, по якій дозволяється або блокується трафік від одного джерела, до сотні інструкцій, що дозволяють або забороняють пакети з декількох джерел. В основному, ACL-списки використовуються для визначення типів прийнятих або пакетів, що відхиляються.

ACL-списки визначають трафік для декількох цілей:

– вказівка внутрішніх вузлів для NAT;

– виявлення й класифікація трафіку для забезпечення розширених можливостей, таких як QoS і організація черги;

– обмеження вмісту відновлення маршрутизації;

– обмеження налагоджувальних вихідних даних;

– контроль доступу віртуальних терміналів до маршрутизаторів.

Використання ACL-списків може бути сполучене з наступними потенційними проблемами:

– додаткове навантаження на маршрутизатор для перевірки всіх пакетів означають менший час на фактичне пересилання пакетів;

– погано організовані ACL-списки створюють навіть ще більше навантаження на маршрутизатор і можуть порушити працездатність мережі;

– неправильно розміщені ACL-списки блокують допустимий трафік і дозволяють заборонений.

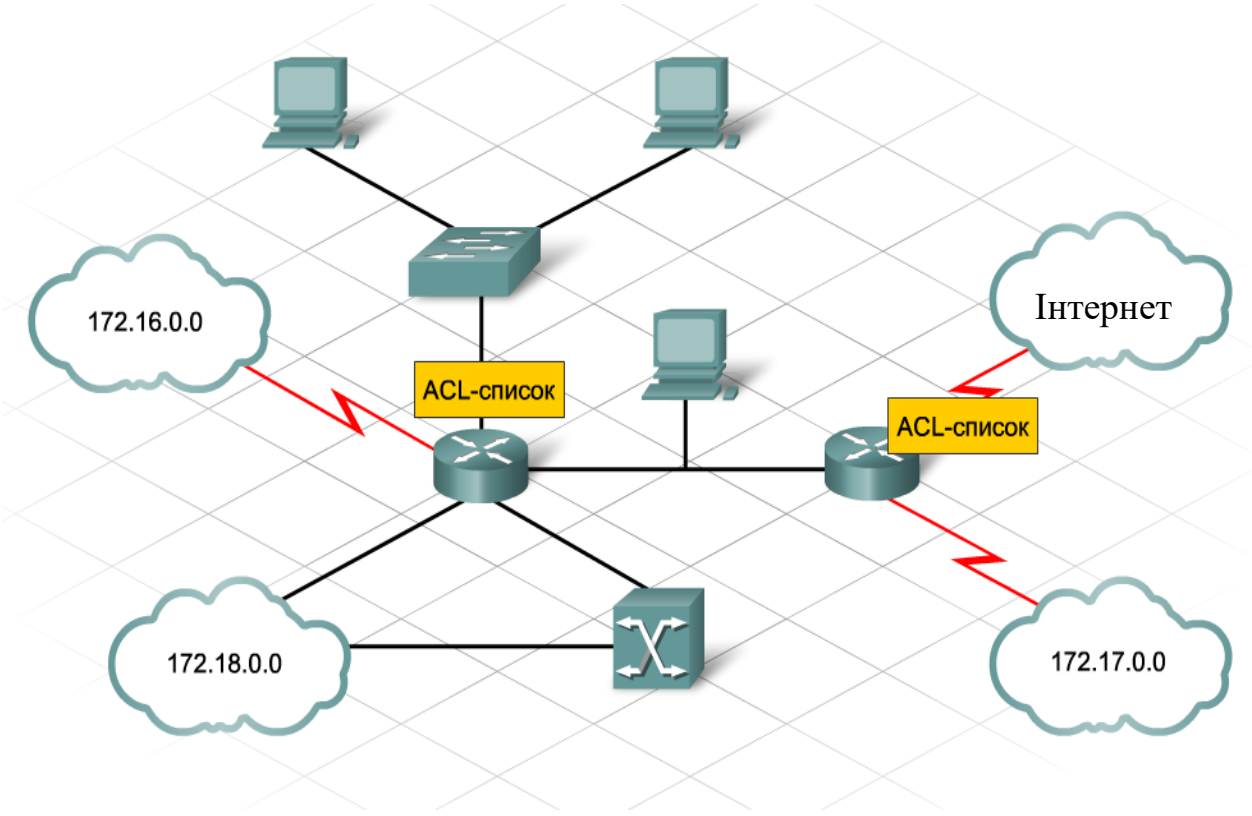


Рисунок 7.3 – ACL-списки

Типи й використання ACL-списків

Адміністраторові доступно кілька варіантів створення списків контролю доступу. Складність вимог до структури визначає тип необхідного ACL-списку.

Існує три типи ACL-списків.

Стандартні ACL-списки

Стандартний ACL-список є найпростішим із трьох типів. При створенні стандартного ACL-списку для IP-протоколу, фільтрація по ACL-списках здійснюється на основі вихідної IP-адреси пакета. Стандартні ACL-списки визначають дозволу пакетів на основі всього протоколу, такого як IP-протокол. Таким чином, при забороні вузлового пристрою стандартним ACL-списком, забороняються всі служби цього вузла. Такий тип ACL-списку корисний для дозволу доступу всіх служб певного користувача або локальної мережі (LAN) через маршрутизатор із забороною доступу з інших IP-адрес. Стандартні ACL-списки визначаються за номерами, що привласнюються їм. Номера з діапазону від 1 до 99 і від 1 300 до 1 999 привласнюються спискам доступу, що дозволяє або блокує IP-трафік.

Розширені ACL-списки

Розширені ACL-списки використовуються для фільтрації не тільки по вихідній IP-адресі, але й по кінцевій IP-адресі, протоколу й номерам портів. Розширені ACL-списки використовуються частіше стандартних, оскільки вони є більше певними й забезпечують більше високий рівень контролю. Розширеним ACL-спискам привласнюються номери з діапазону від 100 до 199 і від 2 000 до 2 699.

Іменовані ACL-списки

Іменовані ACL-списки (NACL-списки) мають формат стандартного або розширеного списку й позначаються описовим ім'ям, а не номером. При налаштуванні іменованих ACL-списків, маршрутизатор IOS використовує режим підкоманди NACL.

Типи списків доступу IOS

Тип ACL-списка	Приклад команди/інструкції ACL-списка	Призначення інструкції
Стандартний	`Router(config)#access-list 1 permit host 172.16.2.88`	• Дозволяє конкретну IP-адресу
Розширений	`Router(config)#access-list 100 deny tcp 172.16.2.0 0.0.0.255 any eq telnet`	• Забороняє доступ із підмережі 172.16.2.0/24 до будь-якого іншого вузла за допомогою telnet
Іменований	`Router(config)#ip access-list standard permit-ip` `Router(config-ext-nacl)#permit host 192.168.5.47`	• Створює стандартний список доступу з ім'ям permit-ip • Дозволяє доступ з IP-адреси 192.168.5.47 • Перша команда переводить маршрутизатор в режим підкоманд NACL-списку.

Рисунок 7.4 – Типи списків доступу

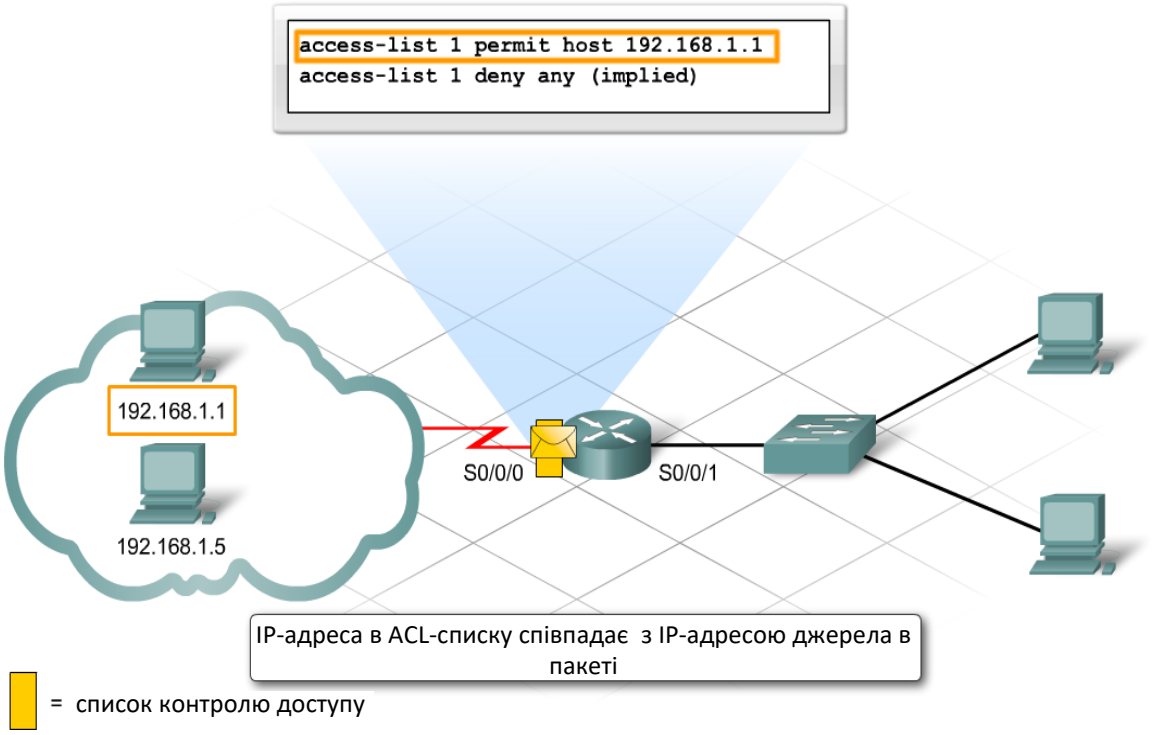
Обробка ACL-списків

У списках контролю доступу втримується одна або більше інструкцій. Кожна інструкція або дозволяє, або забороняє трафік на основі зазначених параметрів. Трафік рівняється з кожною інструкцією в ACL-списку один по одному, поки не буде знайдений збіг або не закінчиться список інструкцій.

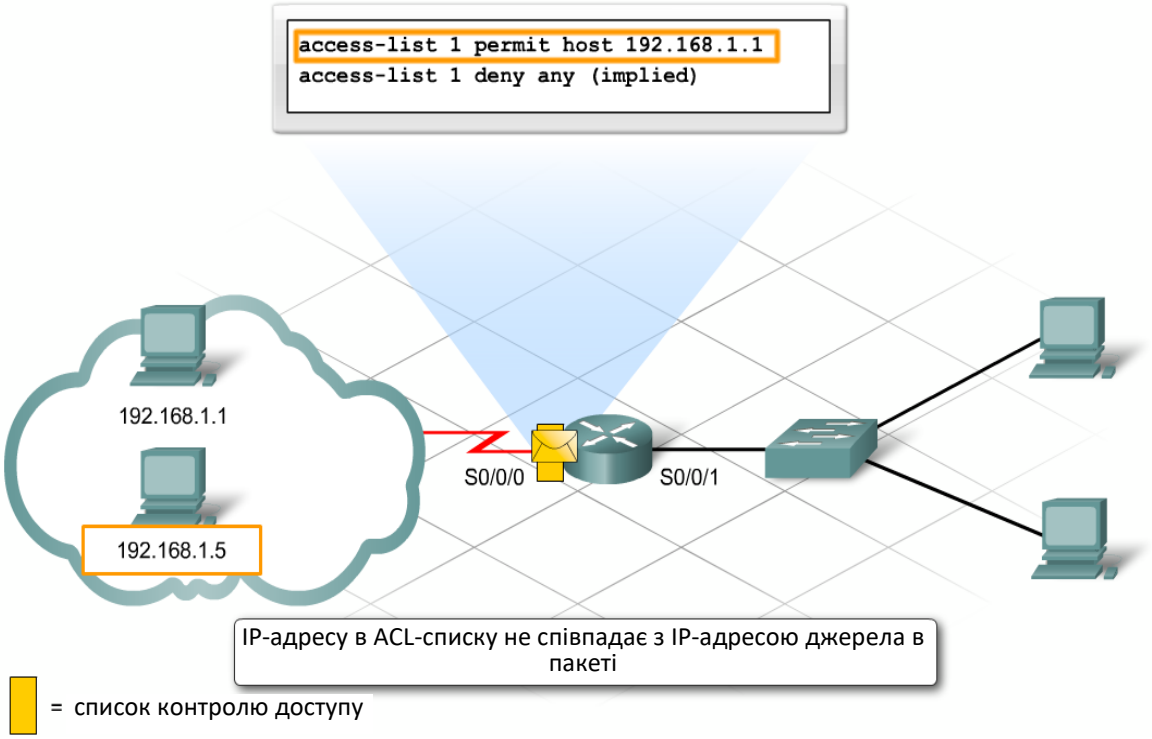
Остання інструкція в ACL-списку завжди неявно забороняє трафік. Ця інструкція автоматично вставляється в кінець кожного ACL-списку, хоча й не є присутнім у ньому фізично. Неявна заборона блокує весь трафік. Ця можливість дозволяє запобігти випадковому влученню небажаного трафіку.

Після створення списку контролю доступу, його необхідно застосувати до інтерфейсу, щоб задіяти його. ACL-список призначений для фільтрації вхідного або вихідного трафіку, що проходить через інтерфейс. Якщо пакет відповідає розв'язній інструкції, то він пропускається маршрутизатором. Якщо він відповідає заборонній інструкції, він зупиняється. ACL-список без єдиної розв'язної інструкції приводить до блокування всього трафіку. Це пояснюється тим, що наприкінці кожного ACL-списку вказується неявна заборона. Таким чином, ACL-список буде

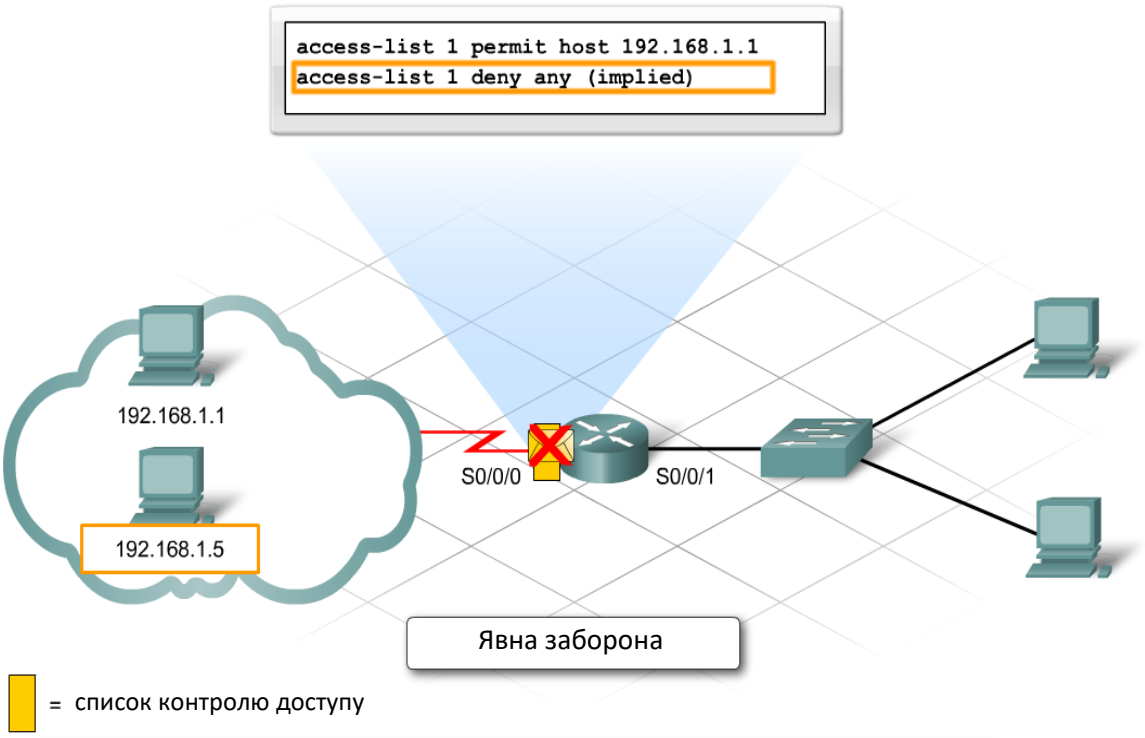
перешкоджати проходженню всього трафіку, якщо не зазначені особливі дозволи.



а)



б)



в)

Рисунок 7.5 – Обробка ACL-списків

Адміністратор може використовувати вхідний або вихідний ACL-список для інтерфейсу маршрутизатора. Вхідний або вихідний напрямок завжди розглядається з погляду маршрутизатора. Трафік, що надходить через інтерфейс, є вхідним, а який відправляється через інтерфейс – вихідний.

При одержанні пакета за інтерфейсом, маршрутизатор перевіряє наступні параметри:

– наявність ACL-списку, пов'язаного з інтерфейсом;

– визначення типу ACL-списку (вхідний/вихідний);

– визначення відповідності трафіку розв'язним або заборонним умовам.

ACL-список, застосовуваний як вихідний до інтерфейсу, не діє для вхідного трафіку по тому ж інтерфейсі.

Для кожного інтерфейсу маршрутизатор може мати один ACL-список для одного напрямку по кожному мережевому протоколі. Для IP-протоколу,

один інтерфейс може мати один вхідний ACL-список і один вихідний ACL-список одночасно.

ACL-списки, застосовувані до інтерфейсу, створюють запізнювання трафіку. Навіть один довгий ACL-список може вплинути на продуктивність маршрутизатора.

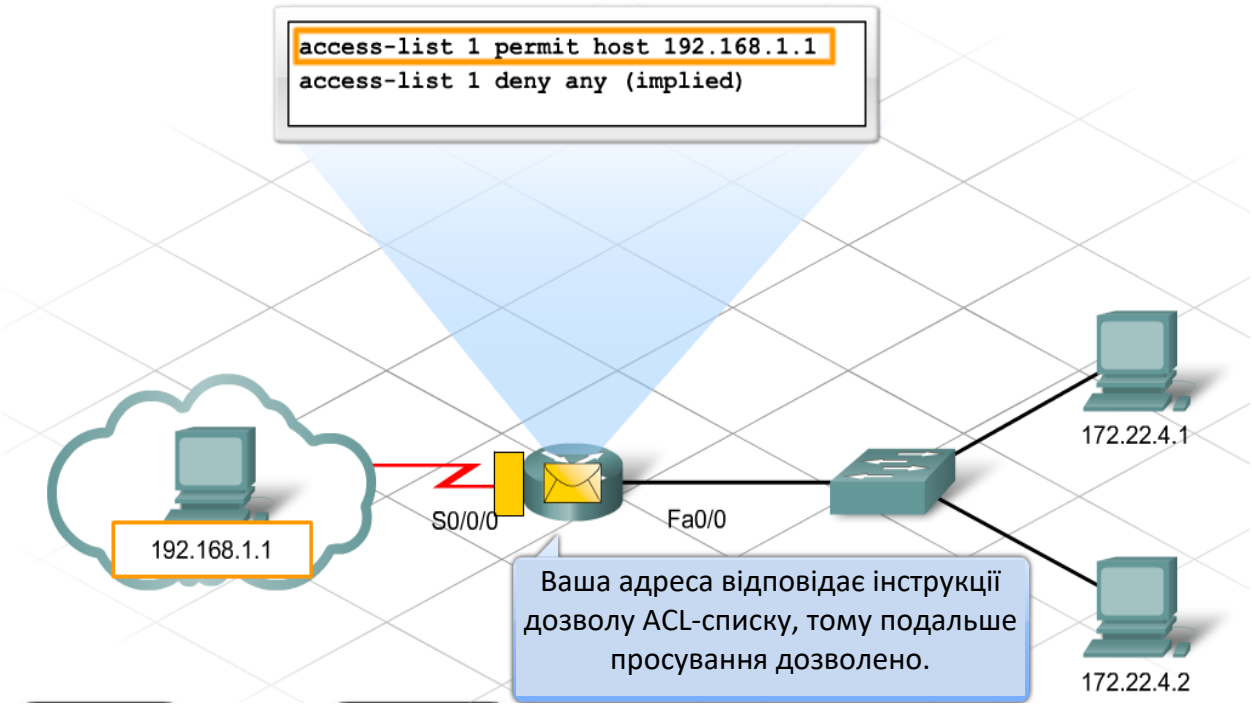
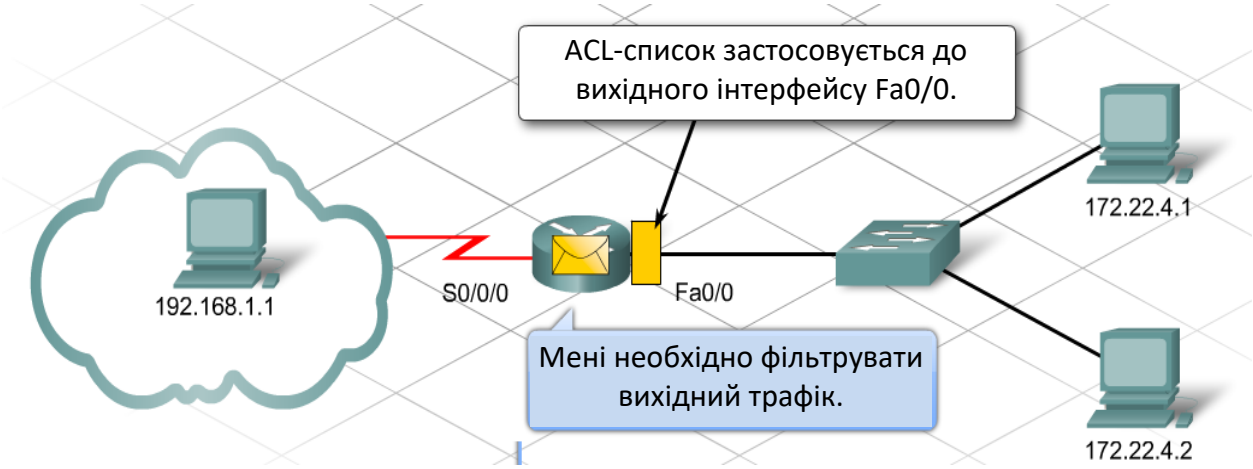


Рисунок 7.6 – Вхідний трафік

а)

б)



в)

Рисунок 7.7 – Вихідний трафік

Ціль використання й структура групової маски ACL-списку

У простих ACL-списках вказується тільки одна дозволена або заборонена адреса. Для блокування декількох адрес або діапазонів адрес необхідно кілька інструкцій або групова маска. Використання IP-адреси мережі із груповою маскою забезпечує набагато більшу гнучкість. За допомогою групової маски можна блокувати діапазон адрес або всю мережу за допомогою всього однієї інструкції.

У груповій масці використовуються символи "0" для вказівки частини IP-адреси, що повинен у точності збігатися, і символи "1" – для частини IP-адреси, що не повинен збігатися з певним номером.

Групова маска типу 0.0.0.0 вимагає точного збігу з усіма 32 бітами IP-адреси. Маска прирівнюється до використання параметра host.

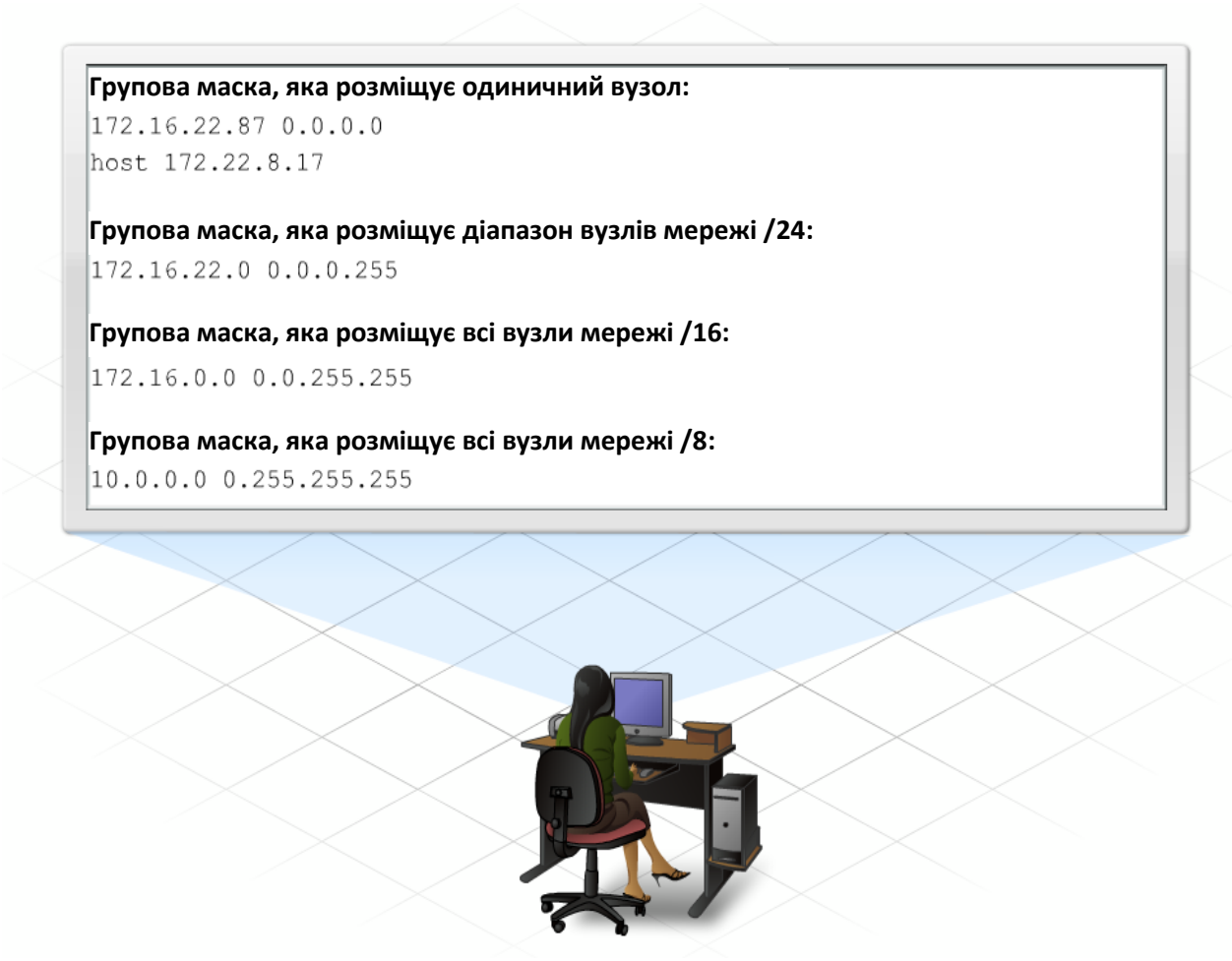


Рисунок 7.8 – Групові маски

Групова маска, використовувана з функціями ACL-списків, аналогічна масці, використовуваної в протоколі маршрутизації OSPF. Однак кожна маска має власну мету. З інструкціями ACL-списку групова маска вказує вузол або діапазон заборонених або дозволених адрес.

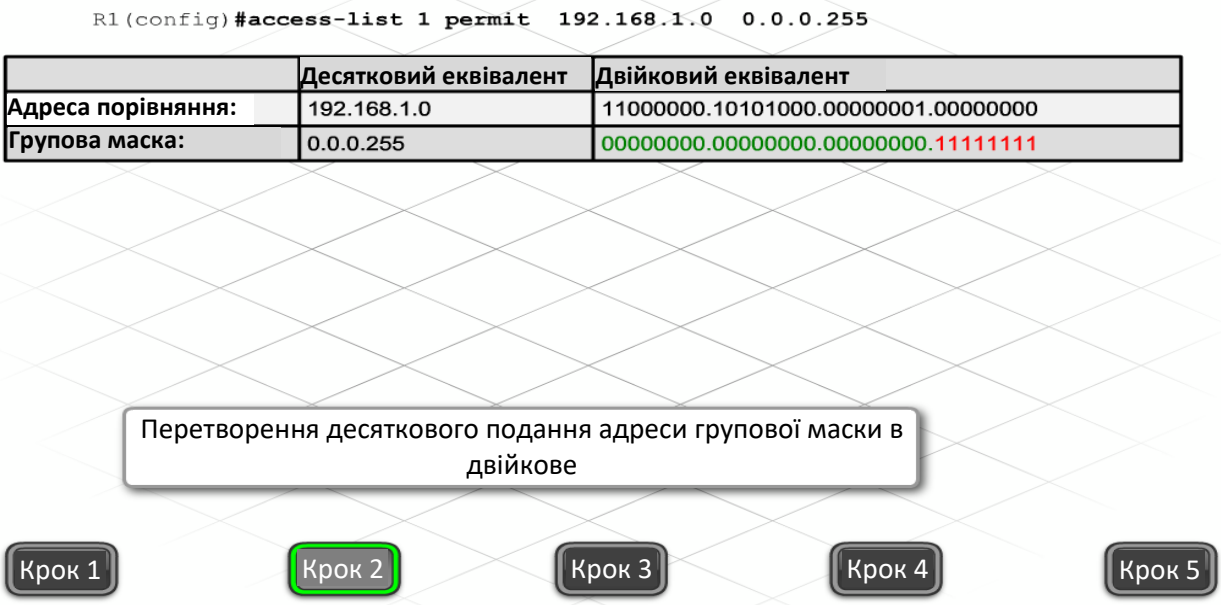
В інструкції ACL-списку IP-адресу й групова маска утворять порівнювані поля. Всі пакети, що входять або виходять через інтерфейс, порівнюються з кожною інструкцією ACL-списку для виявлення збігу. Групова маска визначає, скільки біт вхідної IP-адреси відповідають порівнюваній адресі.

Як приклад, що випливає інструкція дозволяє всі вузли мережі 192.168.1.0 і блокує інші:

access-list 1 permit 192.168.1.0 0.0.0.255

Групова маска вказує, що повинні збігатися тільки перші три октети. Отже, якщо перші 24 біта вхідного пакета збігаються з першими 24 бітами порівнюваного поля, пакет дозволяється. Будь-який пакет з вихідним IP-адресою з діапазону 192.168.1.1 – 192.168.1.255 відповідає сполученню порівнюваної адреси й маски в зазначеному прикладі. Всі інші пакети забороняються ACL-списком за допомогою неявної інструкції deny any.

а)



б)

```
R1(config)#access-list 1 permit  192.168.1.0  0.0.0.255
```

	Десятковий еквівалент	Двійковий еквівалент
Адреса порівняння:	192.168.1.0	11000000.10101000.00000001.00000000
Групова маска:	0.0.0.255	00000000.00000000.00000000.11111111
Біти адреси порівняння для зіставлення:	192.168.1.X	11000000.10101000.00000001.XXXXXXXX

Порівняння бітів зіставлення групової маски (24 нуля) з бітами адреси порівняння

Крок 1 | Крок 2 | Крок 3 | Крок 4 | Крок 5

в)

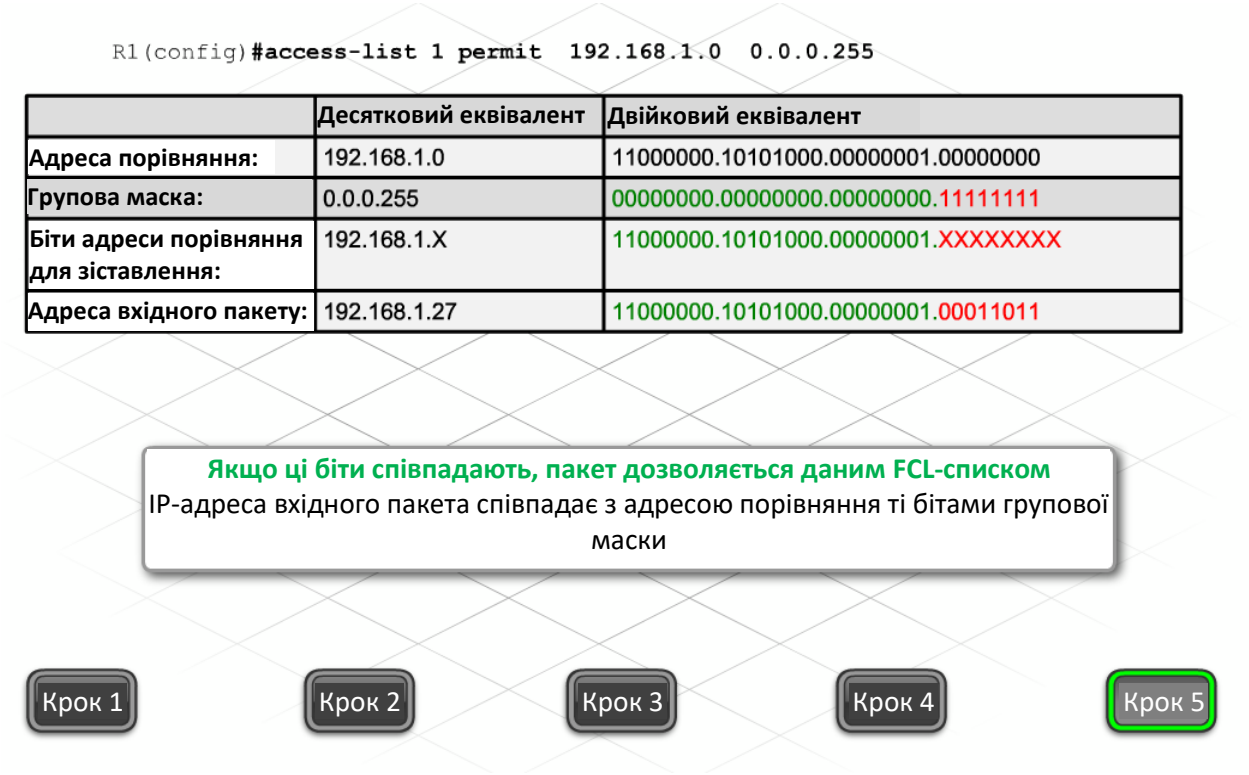
```
R1(config)#access-list 1 permit  192.168.1.0  0.0.0.255
```

	Десятковий еквівалент	Двійковий еквівалент
Адреса порівняння:	192.168.1.0	11000000.10101000.00000001.00000000
Групова маска:	0.0.0.255	00000000.00000000.00000000.11111111
Біти адреси порівняння для зіставлення:	192.168.1.X	11000000.10101000.00000001.XXXXXXXX
Адреса вхідного пакету:	192.168.1.27	11000000.10101000.00000001.00011011

Порівняння перших 24 бітів IP-адреси вхідного пакета з першими 24 бітами адреси порівняння.

Крок 1 | Крок 2 | Крок 3 | Крок 4 | Крок 5

г)



д)

Рисунок 7.9 – Покрокове виконання команди access-list:

1 permit 192.168.1.0 0.0.0.255

При створенні ACL-списку доступно два спеціальних параметри, які можна використовувати на місці групової маски: host і any.

Параметр host

Для фільтрації одного, певного вузла, використовуйте групову маску 0.0.0.0 після IP-адреси або параметр host перед IP-адресою.

R1(config) #access-list 9 deny 192.168.15.99 0.0.0.0

Відповідає наступний:

R1(config) #access-list 9 deny host 192.168.15.99

Параметр any

Для фільтрації всіх вузлів використовуйте всі параметри "1" шляхом налаштування групової маски 255.255.255.255. При використанні групової маски 255.255.255.255, всі біти вважаються збігами, отже, IP-адресу, як

правило, має вигляд 0.0.0.0. Іншим способом фільтрації всіх вузлів є використання параметра any.

R1(config) #access-list 9 permit 0.0.0.0 255.255.255.255

Відповідає наступний:

R1(config) #access-list 9 permit any

Розглянемо наступний приклад, у якому забороняється певний вузол і дозволяються всі інші:

R1(config) #access-list 9 deny host 192.168.15.99

R1(config) #access-list 9 permit any

Команда "permit any" дозволяє весь трафік, спеціально не заборонений ACL-списком. При такому налаштуванні, обробка пакетів не буде виконуватися до неявної команди deny any наприкінці ACL-списку.

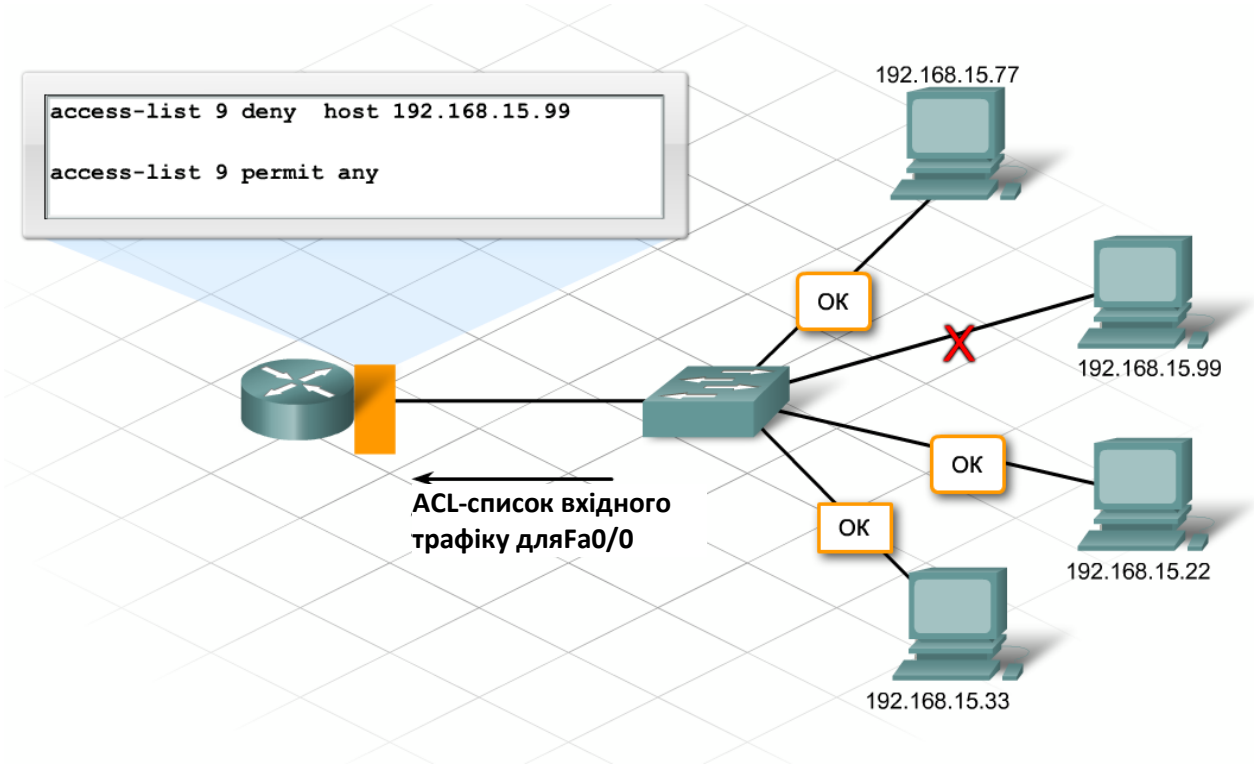


Рисунок 7.10 – Покрокове виконання команд:

R1(config) #access-list 9 deny host 192.168.15.99

R1(config) #access-list 9 permit any

У корпоративній мережі з ієрархічною схемою IP-адресації часто необхідна фільтрація трафіку підмережі.

Якщо 3 біти використовуються для розбивки мережі 192.168.77.0 на підмережі, маскою підмережі буде 255.255.255.224. У результаті вирахування маски підмережі із всіх значень 255 маски виходить групова маска 0.0.0.31. Для дозволу вузлів у підмережі 192.168.77.32 використовується наступна інструкція ACL-списку:

access-list 44 permit 192.168.77.32 0.0.0.31

Перші 27 бітів кожного пакета відповідають першим 27 бітам порівнюваної адреси. Загальний діапазон адрес, припустимих по цій інструкції, починається з 192.168.77.33 і закінчується 192.168.77.63. У нього входять всі адреси підмережі 192.168.77.32.

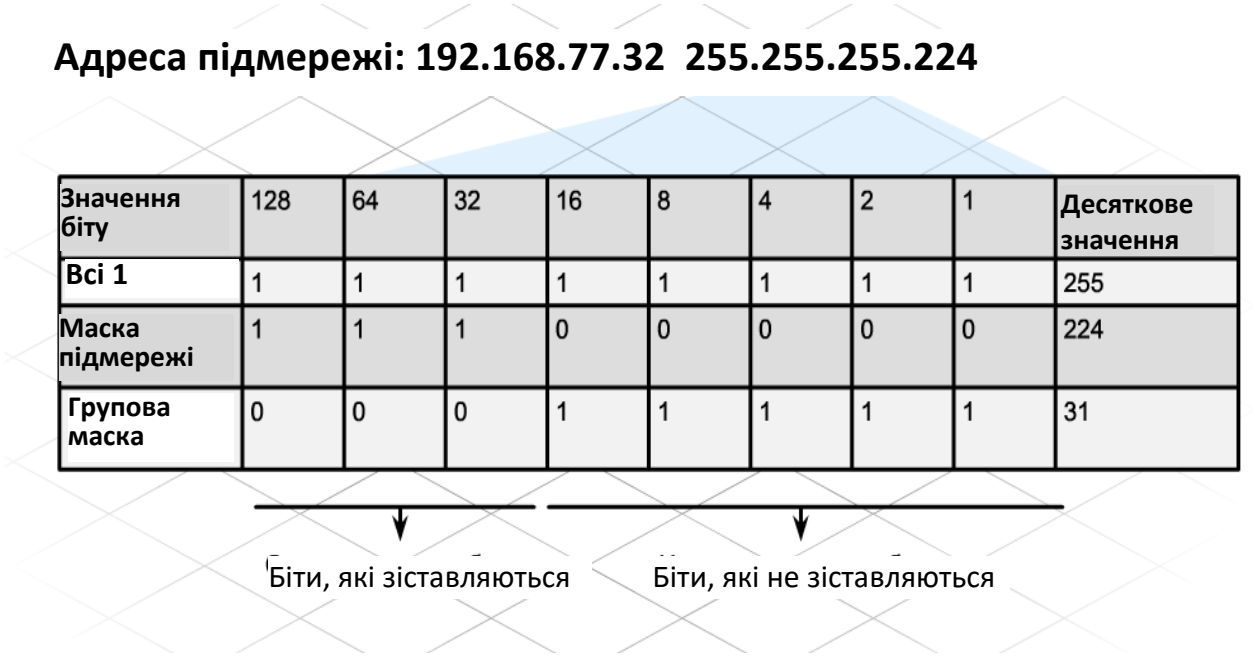


Рисунок 7.11 – Реалізація адресації

Маска підмережі й групова маска мереж класу A, B або C ділять адреси на мережеву й вузлову частину точно по кордони октету. Підмережі, у яких розширений мережевий префікс закінчується не на кордони октету,

використовують інше значення групової маски. Границя октету – це точка між першим і другим або другим і третім октетом.

Приклад. За замовчуванням у підмережі класу А точка розділення перебуває між 8 і 9 бітом. Вона доводиться на кінець одного октету й початок наступного, тобто перебуває на кордони наступного октету.

Створення правильних групових масок для інструкцій ACL-списку дає контроль, необхідний для точної оптимізації потоку трафіку. Фільтрація трафіку різних підмереж є самим складним завданням для починаючих адміністраторів.

Мережа 192.168.77.0 з маскою підмережі 255.255.255.192 або /26 утворить наступні чотири підмережі:

192.168.77.0/26

192.168.77.64/26

192.168.77.128/26

192.168.77.192/26

Щоб створити ACL-список для фільтрації будь-яких із цих чотирьох підмереж, необхідно відняти маску підмережі 255.255.255.192 із всіх значень 255 маски, у результаті чого вийде групова маска 0.0.0.63. Щоб дозволити трафік з перших двох із цих підмереж, використовуйте наступні дві інструкції ACL-списку:

access-list 55 permit 192.168.77.0 0.0.0.63

access-list 55 permit 192.168.77.64 0.0.0.63

Перші дві мережі в сумі утворять 192.168.77.0/25. У результаті вирахування підсумованої маски підмережі 255.255.255.128 зі значень 255 маски виходить групова маска 0.0.0.127. Використання цієї маски дозволяє об'єднати ці дві підмережі в одній інструкції ACL-списку замість двох.

access-list 5 permit 192.168.77.0 0.0.0.127

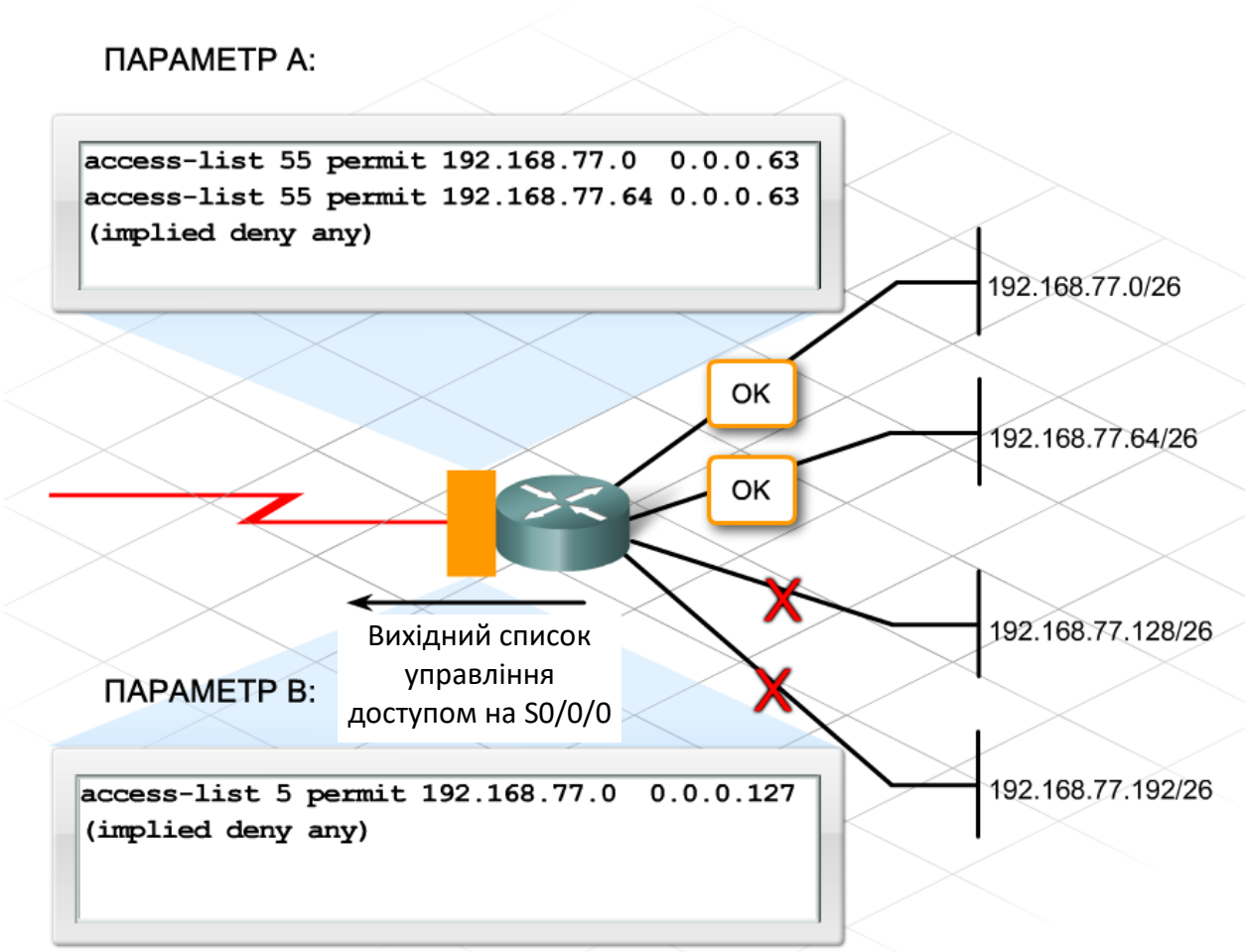


Рисунок 7.12 – Покрокове виконання команд:

access-list 55 permit 192.168.77.0 0.0.0.63

access-list 55 permit 192.168.77.64 0.0.0.63

РОЗДІЛ 8. РОЗМІЩЕННЯ СТАНДАРТНИХ І РОЗШИРЕНИХ ACL-СПИСКІВ

Правильно складені списки контролю доступу позитивно позначаються на продуктивності й доступності мережі. Для досягнення максимальних результатів необхідне планування створення й розміщення списків контролю доступу.

Етап планування включає наступні дії:

1. Визначення вимог до фільтрації трафіку.

2. Вибір типу ACL-списку, що щонайкраще відповідає вимогам.

3. Визначення маршрутизатора й інтерфейсу, для якого буде використовуватися ACL-список.

4. Вибір напрямку фільтрації трафіку.

Крок 1. Визначення вимог до фільтрації трафіку

Складіть список вимог до фільтрації трафіку, опитавши зацікавлені сторони в кожному відділі підприємства. Ці вимоги різні для різних підприємств і ґрунтуються на потребах клієнта, типах і обсягах трафіку, а також завданнях безпеки.

Крок 2. Вибір типу, що відповідає вимогам, ACL-списку

Вибір стандартного ACL-списку або розширеного ACL-списку обумовлений поточними вимогами до фільтрації. Вибір типу ACL-списку може вплинути на гнучкість фільтрації за ACL-списком, також як на продуктивність маршрутизатора й пропускну здатність мережі.

Стандартні ACL-списки легко створювати й впроваджувати. Однак фільтрація по стандартним ACL-списках можлива тільки на основі вихідної адреси й застосовується до всьому трафіку без обліку його типу або призначення. При маршрутизації в кілька мереж занадто близьке розміщення стандартного ACL-списку до джерела може ненавмисно блокувати

припустимий трафік. Отже, важливо розміщати стандартні ACL-списки якнайближче до кінцевого вузла.

У випадку більше складних вимог до фільтрації варто використовувати розширений ACL-список. Розширені ACL-списки дають більший контроль, ніж стандартні. Вони допускають фільтрацію по вихідних і кінцевих адресах. Ці списки також забезпечують фільтрацію за протоколом мережевого рівня, протоколу транспортного рівня й номерам портів, якщо це необхідно. Така більше точна фільтрація дозволяє адміністраторові мережі створювати ACL-списки, що відповідають певним потребам плану по забезпеченню безпеки.

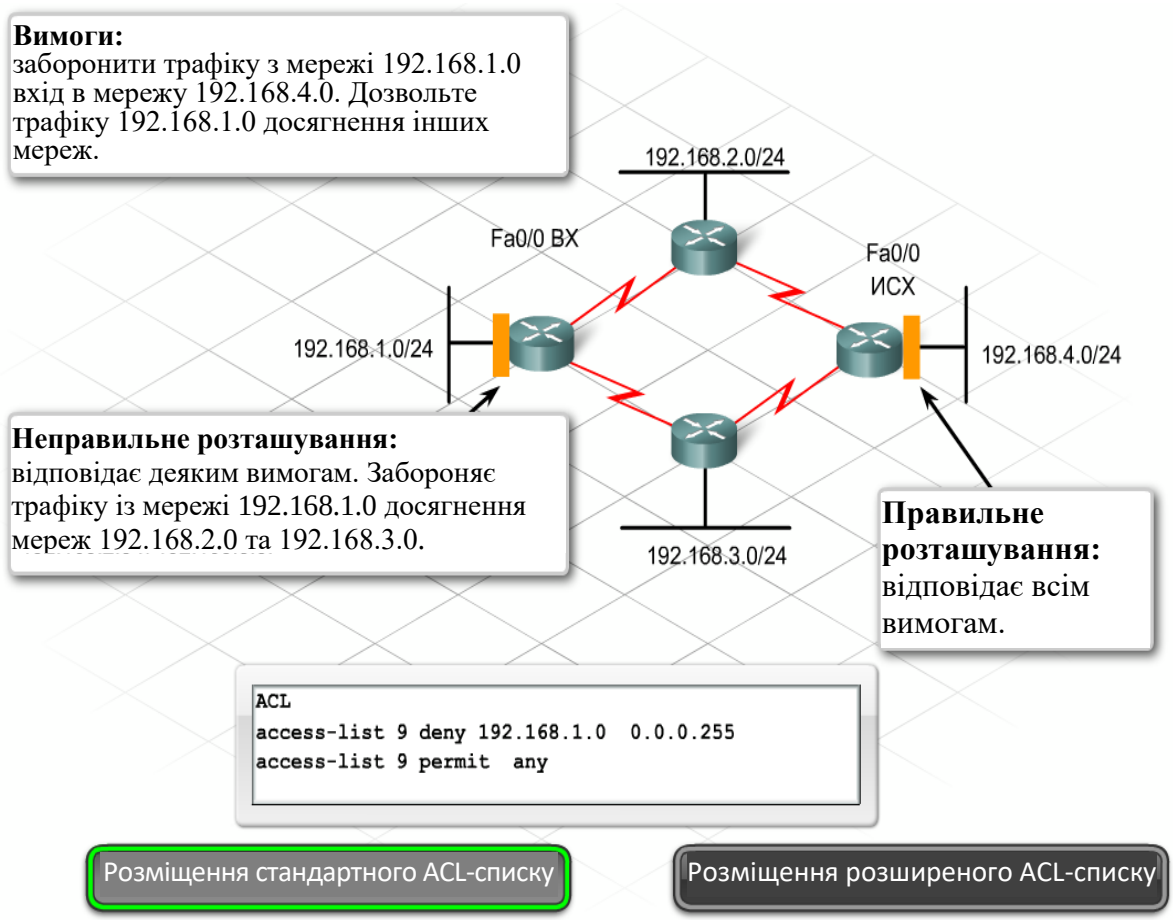


Рисунок 8.1 – Розміщення стандартного ACL-списку

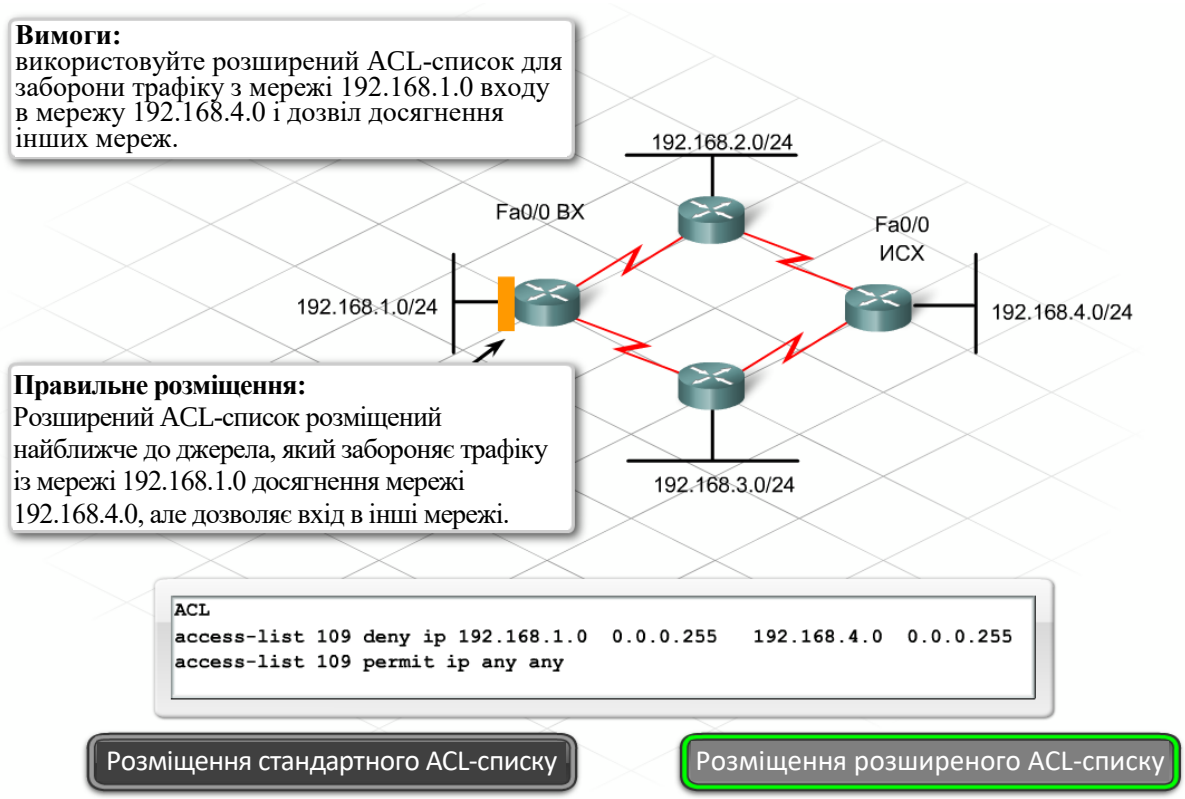


Рисунок 8.2 – Розміщення розширеного ACL-списку

Розміщайте розширений ACL-список ближче до вихідної адреси. Завдяки аналізу по вихідній і кінцевій адресі, ACL-список дозволяє блокувати пакети, що направляються в певну кінцеву мережу перш, ніж вони покинуть вихідний маршрутизатор. Пакети фільтруються перш, ніж вони перетнуть кордони мережі, що допомагає підтримувати пропускну здатність.

Крок 3. Визначення маршрутизатора й підключення, для якого буде використовуватися ACL-список

Розміщайте ACL-списки на маршрутизаторах на рівні доступу або розподілу. Адміністратор мережі повинен мати контроль над цими маршрутизаторами й можливість реалізації політики безпеки. Без доступу до маршрутизатора адміністратор мережі не зможе налаштувати на ньому ACL-список.

Вибір відповідного інтерфейсу залежить від вимог до фільтрації, типу ACL-списку й місця розташування призначеного маршрутизатора. Найкраще організовувати фільтрацію трафіку перш, ніж він досягне послідовної лінії з

меншою пропускною здатністю. Вибір інтерфейсу звичайно є очевидним, якщо обрано маршрутизатор.

Крок 4. Вибір напрямку фільтрації трафіку

При виборі напрямку, для якого буде використовуватися ACL-список, необхідно представити потік трафіку з погляду маршрутизатора.

Вхідний трафік – це трафік, що надходить в інтерфейс маршрутизатора ззовні. Маршрутизатор порівнює вхідний пакет з ACL-списком перед пошуком цільової мережі в таблиці маршрутизації. Пакети, що відкидаються в цій точці, дозволяють виключити зайві операції пошуку маршрутизатора. Це робить вхідний список контролю доступу більше ефективним для маршрутизатора, ніж вихідний список контролю доступу.

Вихідний трафік проходить через маршрутизатор за інтерфейсом. Для вихідного пакета маршрутизатор уже здійснив пошук по таблиці маршрутизації й перемкнув пакет на правильний інтерфейс. Пакет рівняється з ACL-списком безпосередньо перед виходом з маршрутизатора.

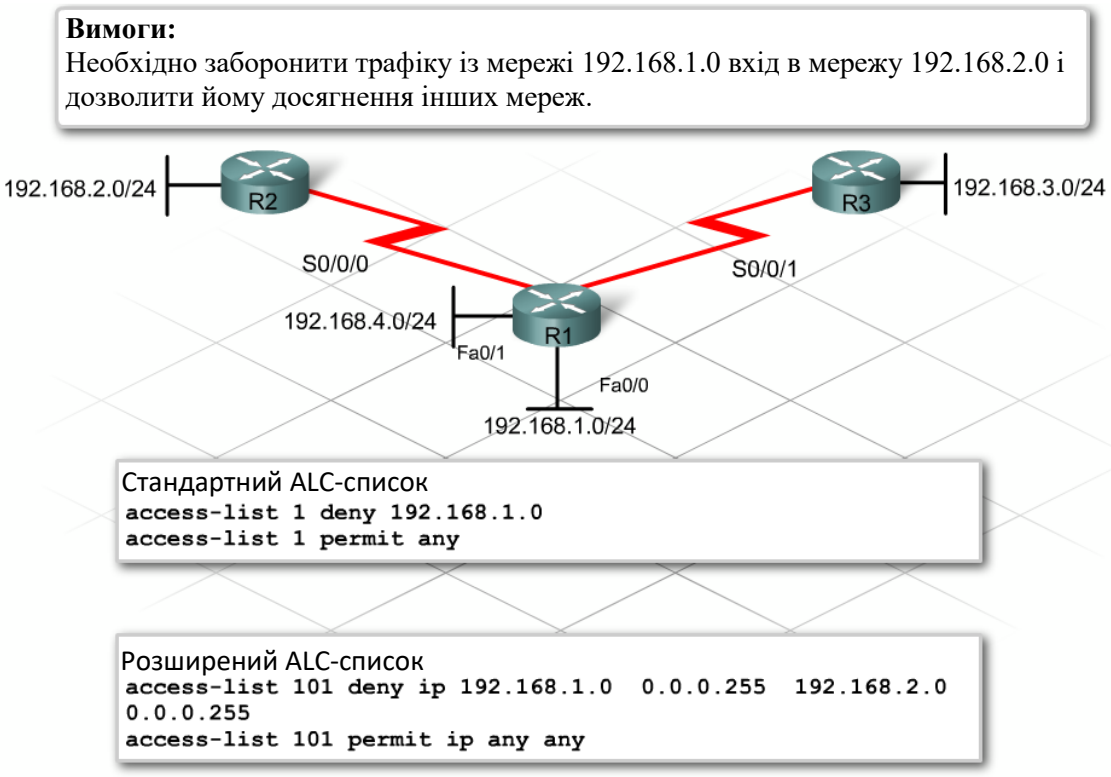


Рисунок 8.3 – Розміщення стандартних і розширених ACL-списків

Основний процес налаштування ACL-списків

Після визначення вимог, планування списку контролю доступу й визначення розташування ACL-список необхідно налаштувати.

Для кожного ACL-списку необхідний унікальний ідентифікатор. Ідентифікатор може бути числом або описовим ім'ям.

У нумерованих списках контролю доступу, номер визначає тип створюваного ACL-списку:

– стандартним ACL-спискам для IP-протоколу привласнюються номери з діапазону від 1 до 99 і від 1300 до 1999;

– розширеним ACL-спискам для IP-протоколу привласнюються номери з діапазону від 100 до 199 і від 2000 до 2699.

Можна також створювати ACL-списки AppleTalk і IPX.

Обмеженням для будь-якого маршрутизатора є один ACL-список для протоколу й напрямку. Якщо на маршрутизаторі IP-протокол виконується в монопольному режимі, кожний інтерфейс може обробляти максимум два ACL-списки: один для вхідні й один для вихідного трафіку. Оскільки кожний ACL-список виконує порівняння кожного пакета, що проходить через підключення, використання ACL-списків створює запізнювання.

Налаштування списку контролю доступу охоплює два етапи: створення й застосування.

Створення ACL-списку

Увійдіть у режим глобального налаштування. За допомогою команди access-list уведіть інструкції списку контролю доступу. Уведіть всі інструкції з однаковим номером ACL-списку, поки список контролю доступу не буде готів.

Синтаксис стандартного ACL-списку наступний:

access-list [номера-списку-доступу] [deny|permit] [вихідна адреса] [вихідна-групова маска][log]

Рекомендації по створенню і обробці ACL-списків

- Задавайте тільки один список доступу для протоколу та направлення.
- Застосовуйте стандартні списки доступу якомога ближче до місця призначення.
- Застосовуйте розширені списки доступу якомога ближче до джерела.
- Використовуйте правильний діапазон номерів для типу списку.
- Визначте вхідні або вихідні направлення, дивлячись на порт зсередини маршрутизатора.
- Інструкції повинні виконуватися послідовно від початку до кінця списку.
- Забороніть пакет, якщо збіг не знайдено.
- Спочатку вводьте конкретні, а потім загальні інструкції списку доступу.
- Задайте в ALC-списку інструкцію дозволу, інакше буде заборонений весь трафік.

Додаткова інформація

- Для відхилених пакетів список доступу IP відправляє повідомлення ICMP-протоколу про недосяжність вузла відправнику і відхиляє даний пакет.
- Фільтри вихідного трафіку не впливають на трафік, який надходить від локального маршрутизатора.
- Явна заборона всього трафіку розміщується в кінці всіх списків доступу (не з'являється в лістингу).
- Створіть ACL-списки в текстовому редакторі, щоб їх можна було легко змінити. Ви можете скопіювати та вставити інструкції ACL-списку

Рисунок 8.4 – Рекомендації зі створення й обробки ACL-списків

Оскільки кожний пакет рівняється з інструкцією ACL-списку до знаходження збігу, порядок розміщення інструкцій в ACL-списку може впливати на створюване запізнювання. Тому розташовуйте інструкції таким

чином, щоб більш часті умови в ACL-списку передували менш частим. Наприклад, інструкції зі збігом по найбільшому обсягу трафіку необхідно розміщати на початку ACL-списку.

При цьому варто пам'ятати, що при збігу пакет більше не рівняється з іншими інструкціями в ACL-списку. Це означає, що якщо один рядок дозволяє пакет, а наступний рядок в ACL-списку забороняє його, пакет буде дозволений. Із цієї причини варто планувати ACL-список таким чином, щоб інструкції з більше певними вимогами розташовувалися перед інструкціями з більш загальними вимогами. Інакше кажучи, забороняйте доступ певному вузлу в мережі, дозволяючи доступ іншим у всій мережі.

Для опису функції кожного розділу або інструкції ACL-списку використовуйте команду remark:

access-list [номер списку] remark [текст]

Для видалення ACL-списку використовуйте наступну команду:

no access-list [номер списку]

Зі стандартного або розширеного ACL-списку не можна видалити один рядок. Замість цього ACL-список видаляється повністю і його необхідно замінити.

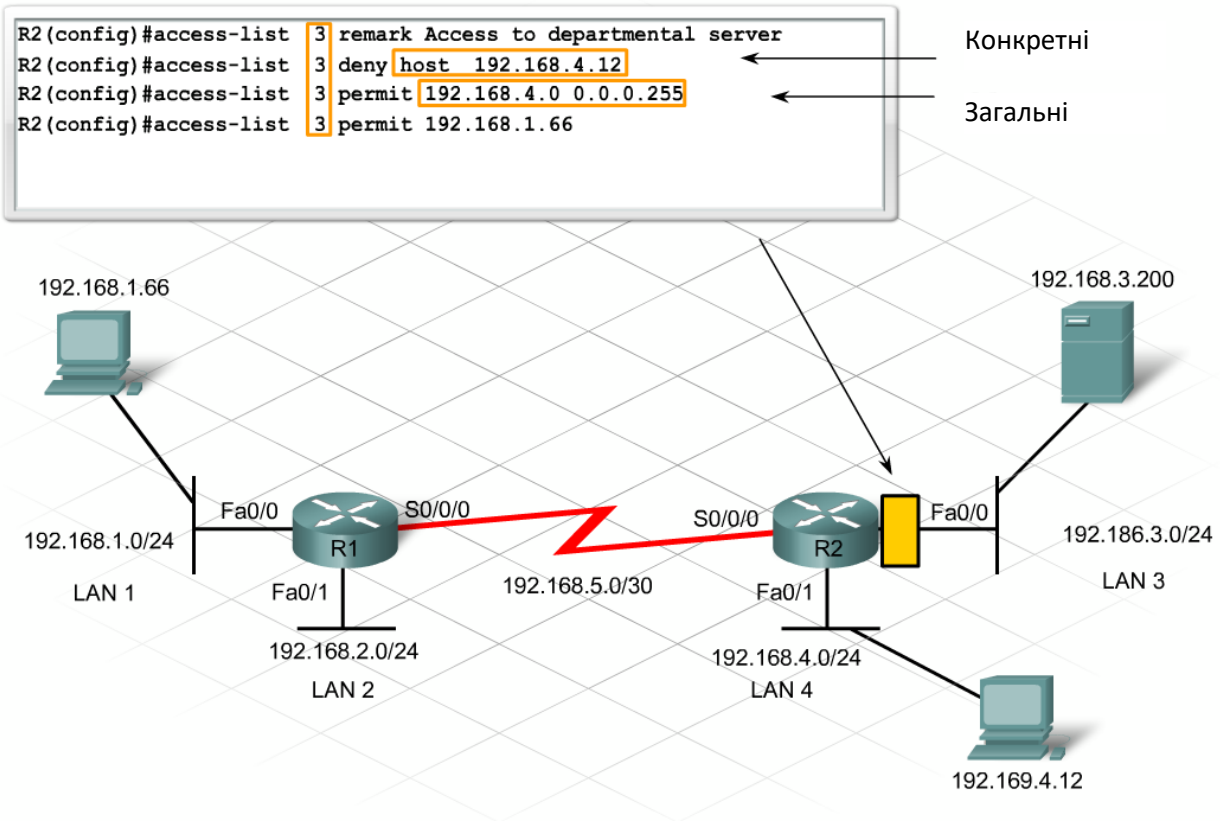


Рисунок 8.5 – Створення ACL-списку

Налаштування нумерованих стандартних ACL-списків

Фільтрація за ACL-списком неможлива до його застосування або призначення інтерфейсу.

Застосування ACL-списку

Привласніть ACL-список одному або більше інтерфейсам, указавши вхідний або вихідний трафік. Застосовуйте стандартний ACL-список якнайближче до кінцевої адреси.

R2(config-if)#ip access-group номер списку доступу [in | out]

Наступні команди дозволяють помістити список доступу access-list 5 для інтерфейсу Fa0/0 маршрутизатора R2 з фільтрацією вхідного трафіку:

R2(config)#interface fastethernet 0/0

R2(config-if)#ip access-group 5 in

За замовчуванням в ACL-списку до інтерфейсу застосовується out напрямок. Незважаючи на те, що out напрямок установлений за замовчуванням, надто важливо вказувати напрямок щоб уникнути плутанини й для забезпечення фільтрації трафіку в правильному напрямку.

Щоб видалити ACL-список з інтерфейсу без зміни самого ACL-списку, використовуйте команду no ip access-group interface.

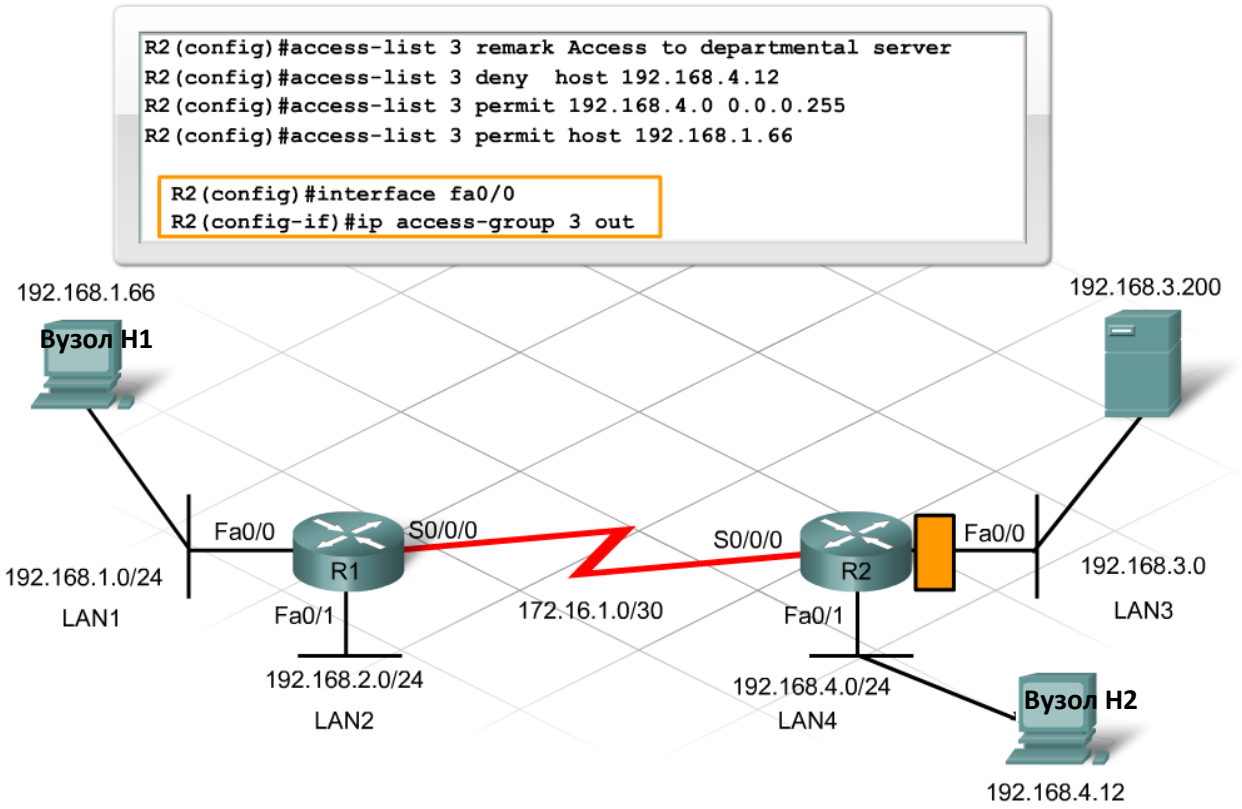


Рисунок 8.6 – Застосування ACL-списку

РОЗДІЛ 9. КОМУТАЦІЯ МЕРЕЖІ

Комутація й сегментація мережі

Хоча для створення корпоративної мережі використовуються як комутатори, так і маршрутизатори, архітектура більшості корпоративних мереж у значній мірі ґрунтується на комутаторах. Вартість комутаторів з розрахунку на порт нижче, ніж у маршрутизаторів, і вони забезпечують швидке пересилання кадрів зі швидкістю передачі даних по кабелю.

Комутатор – універсальний пристрій 2-го рівня. У найпростішому варіанті використання він заміняє концентратор як центральну точку для з'єднання декількох вузлів. У більш складному варіанті комутатор підключається до одного або декількох комутаторів для створення, контролю й обслуговування резервних каналів і з'єднань VLAN. Комутатор однаково обробляє всі типи трафіку, незалежно від їхнього призначення.

Комутатор передає трафік відповідно до MAC-адрес. Кожний комутатор веде таблицю MAC-адрес у високопродуктивній пам'яті, що називається асоціативною пам'яттю (CAM). Комутатор заново створює таблицю при кожній активації, використовуючи MAC-адреси джерела вхідних кадрів і номера портів, через які вони отримані.

Комутатор видаляє записи з таблиці MAC-адрес, якщо вони не використовуються протягом певного періоду часу. Цей період називається таймером старіння, видалення запису називається старінням.

Як тільки одноадресний кадр прибуває на порт, комутатор знаходить MAC-адресу джерела в кадрі. Потім він виконує пошук по таблиці MAC-адрес і знаходить запис, що відповідає адресі.

Якщо MAC-адресу відсутня у таблиці, комутатор додає MAC-адресу й номер порту й активує таймер старіння. Якщо MAC-адресу джерела вже існує, комутатор скидає таймер старіння.

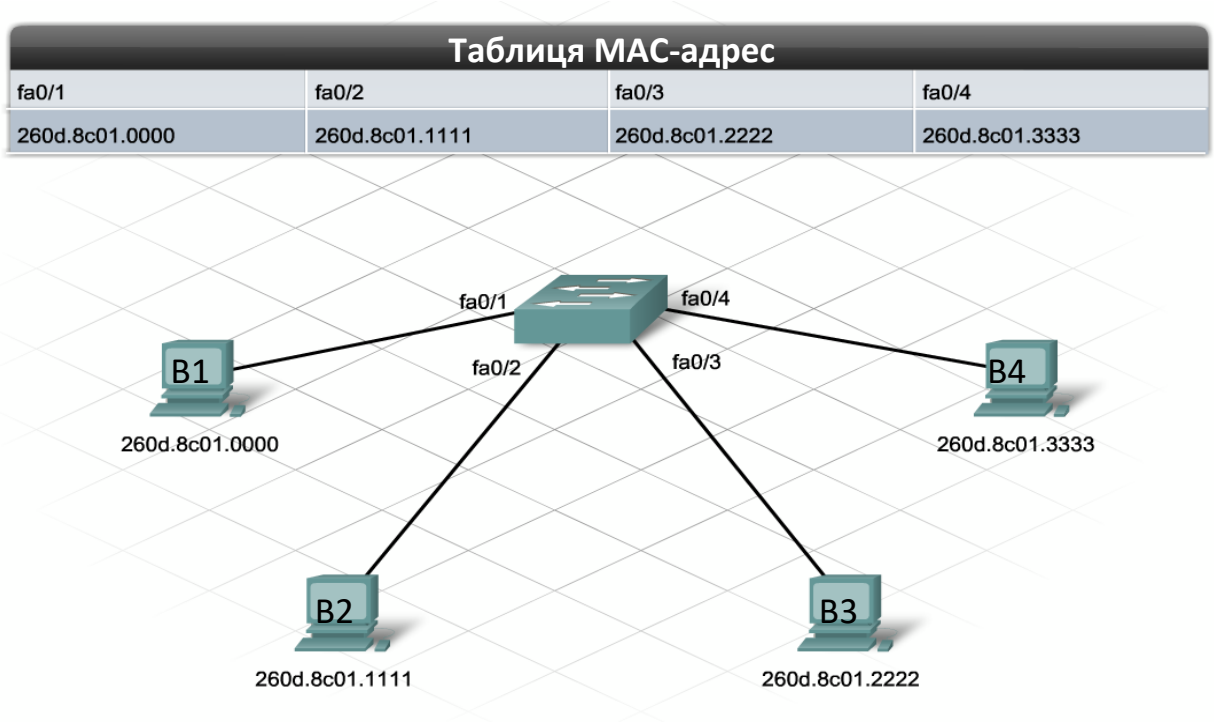


Рисунок 9.1 – Комутація мережі

Потім комутатор шукає MAC-адресу призначення в таблиці MAC-адрес. Якщо запис існує, комутатор пересилає кадр на порт із відповідним номером. Якщо запису ні, комутатор виконує лавинну маршрутизацію кадру із всіх портів, крім порту, на якому він прийнятий.

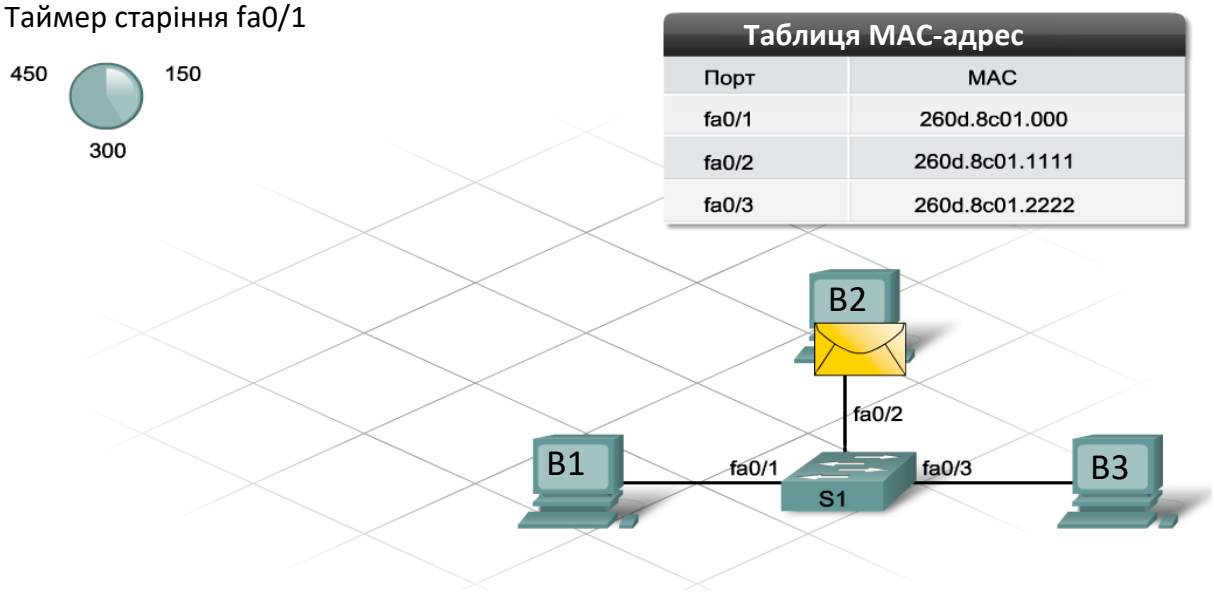


Рисунок 9.2 – Пошук MAC-адрес призначення в таблиці MAC-адрес

У корпоративному середовищі висока доступність, швидкість і смуга пропущення мережі мають першорядне значення. Розмір доменів широкомовного розсилання й колізійних доменів впливає на потоки трафіку. Як правило, великі домени широкомовного розсилання й колізійні домени погіршують ці критично важливі показники.

Якщо комутатор одержує широкомовний кадр, він розсилає його із всіх активних інтерфейсів, так само як кадр із невідомою MAC-адресою призначення. Всі пристрої, що одержують широкомовне розсилання, становлять домен широкомовного розсилання. При збільшенні числа з'єднаних комутаторів розмір домену широкомовного розсилання також збільшується.

Колізійні домени створюють аналогічну проблему. Чим більше пристроїв входить у колізійний домен, тим частіше вони виникають.

Використання концентраторів збільшує колізійні домени. Однак комутатори використовують функцію за назвою мікросегментація, щоб зменшити розмір колізійного домену до одного порту комутатора.

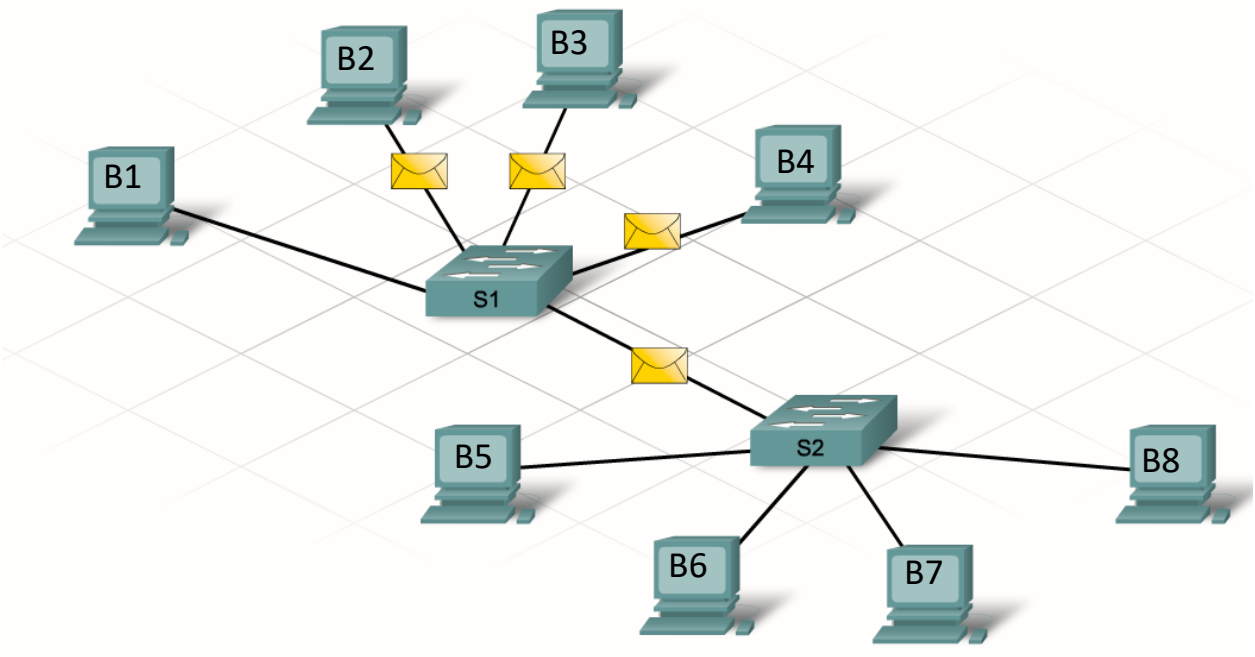


Рисунок 9.3 – Використання концентраторів

Коли вузол підключається до порту комутатора, створюється виділене підключення. Коли два з'єднаних вузли взаємодіють один з одним, комутатор звертається до таблиці комутації й створює віртуальне підключення або мікросегмент між портами.

Комутатор підтримує віртуальний канал до припинення сеансу. Кілька віртуальних каналів можуть бути активні одночасно. Мікросегментація поліпшує коефіцієнт використання смуги пропущення за рахунок зменшення кількості колізій і підтримки декількох паралельних підключень.

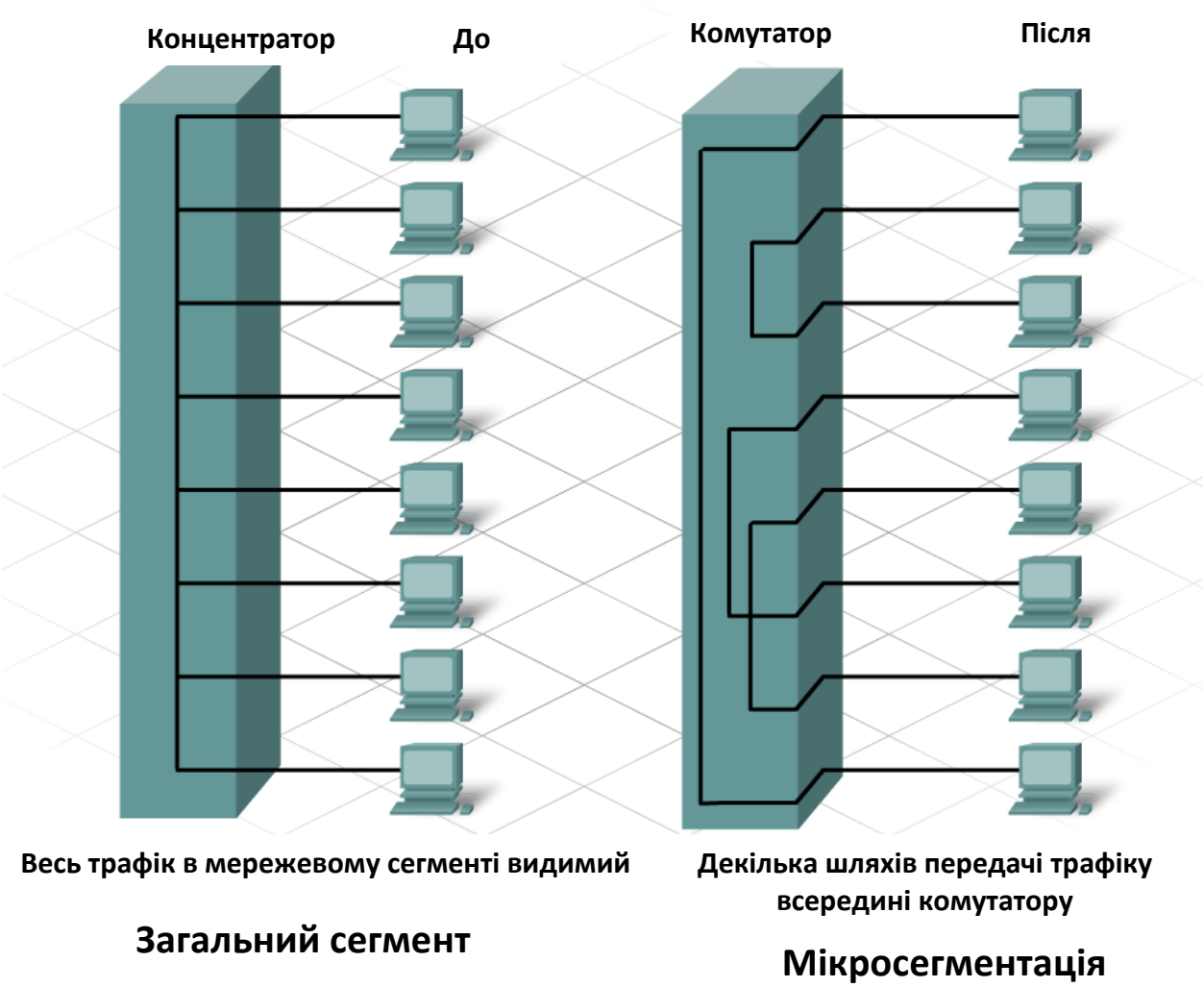
Комутатори можуть підтримувати симетричну й асиметричну комутацію. Комутатори, всі порти яких працюють на однаковій швидкості, називаються симетричними. Однак багато комутаторів мають два або більше високошвидкісні порти. Ці високошвидкісні порти, або порти для каскадування, використовуються для підключення до зон з більш високими вимогами до смуги пропущення. Сфери застосування таких портів:

– підключення до інших комутаторів;

– канали зв'язку із серверами або серверними фермами;

– підключення до інших мереж.

Для з'єднання портів, що працюють на різних швидкостях, використовується асиметрична комутація. При необхідності комутатор зберігає інформацію в пам'яті, щоб створити буфер між портами з різними швидкостями. Асиметричні комутатори широко поширені в корпоративних середовищах.



Традиційно мережі складалися з окремих пристроїв 2-го й 3-го рівняв. Кожний пристрій використовував різні методи обробки й пересилання трафіку.

Рівень 2

Комутатори рівня 2 є апаратними. Вони пересилають трафік зі швидкістю, що відповідає швидкості передачі середовища, використовуючи внутрішні схеми, які фізично з'єднують кожний порт із усіма іншими портами. Процес пересилання використовує MAC-адресу й наявність MAC-адреси призначення в таблиці MAC-адрес. Комутатор 2-го рівня пересилає трафік тільки всередині одного мережевого сегмента або підмережі.

Рівень 3

Маршрутизатори є програмними пристроями й використовують мікропроцесори для маршрутизації на основі IP-адрес. Маршрутизація 3-го рівня забезпечує пересилання трафіку між різними мережами й підмережами. Коли пакет приймається на інтерфейсі маршрутизатора, він використовує програмне забезпечення для пошуку IP-адреси призначення й вибору оптимального шляху до мережі призначення. Потім маршрутизатор передає пакет на потрібний вихідний інтерфейс.

Рисунок 9.5 – Відмінність комутації 2-го рівня й маршрутизації 3-го рівня

Комутація 3-го рівня, або багаторівнева комутація, поєднує апаратну комутацію й апаратну маршрутизацію в одному пристрої.

Багаторівневий комутатор поєднує функції комутатора 2-го рівня й маршрутизатора 3-го рівня. Комутація 3-го рівня виконується в інтегральній схемі прикладної орієнтації (ASIC). Для функцій пересилання кадрів і пакетів використовується одна мікросхема ASIC.

Багаторівневі комутатори часто зберігають або додають у кеш даної маршрутизації по джерелу й місцю призначення, отримані з першого пакета в діалозі. Наступним пакетам не доводиться виконувати пошук у таблиці маршрутизації, тому що вони знаходять дані маршрутизації в пам'яті. Кешування ще більше збільшує продуктивність цих пристроїв.

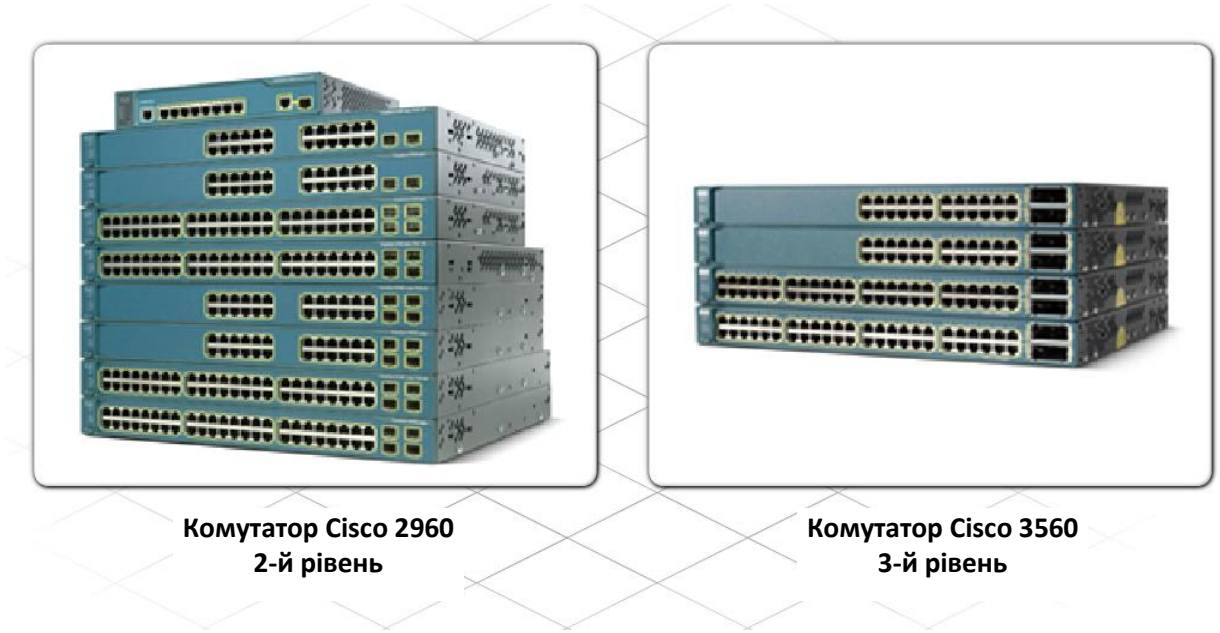


Рисунок 9.6 – Приклади відповідної мережевої апаратури

Типи комутації

Коли комутація тільки з'явилася, комутатори підтримували один із двох методів пересилання кадру з одного порту на інший. Ці методи: пересилання з буферизацією і комутація без буферизації. Кожний з методів має свої переваги й недоліки.

Пересилання з буферизацією

При використанні цього типу комутації повний кадр зчитується й зберігається в пам'яті перед передачею пристрою призначення. Комутатор перевіряє цілісність бітів у кадрі, обчислюючи значення циклічного контролю парності (CRC). Якщо розраховане значення CRC збігається зі значенням у поле CRC кадру, комутатор пересилає кадр через порт призначення. Комутатор не пересилає кадри, якщо значення CRC не

збігаються. Значення CRC перебуває в полі контрольної послідовності кадру (FCS) у кадрі Ethernet.

Хоча цей метод дозволяє запобігти передачі ушкоджених кадрів в інші сегменти, він викликає значне запізнювання. Через це комутація з буферизацією в основному використовується в середовищах з високою ймовірністю виникнення помилок, наприклад у середовищах, що часто піддаються впливу електромагнітних імпульсів.

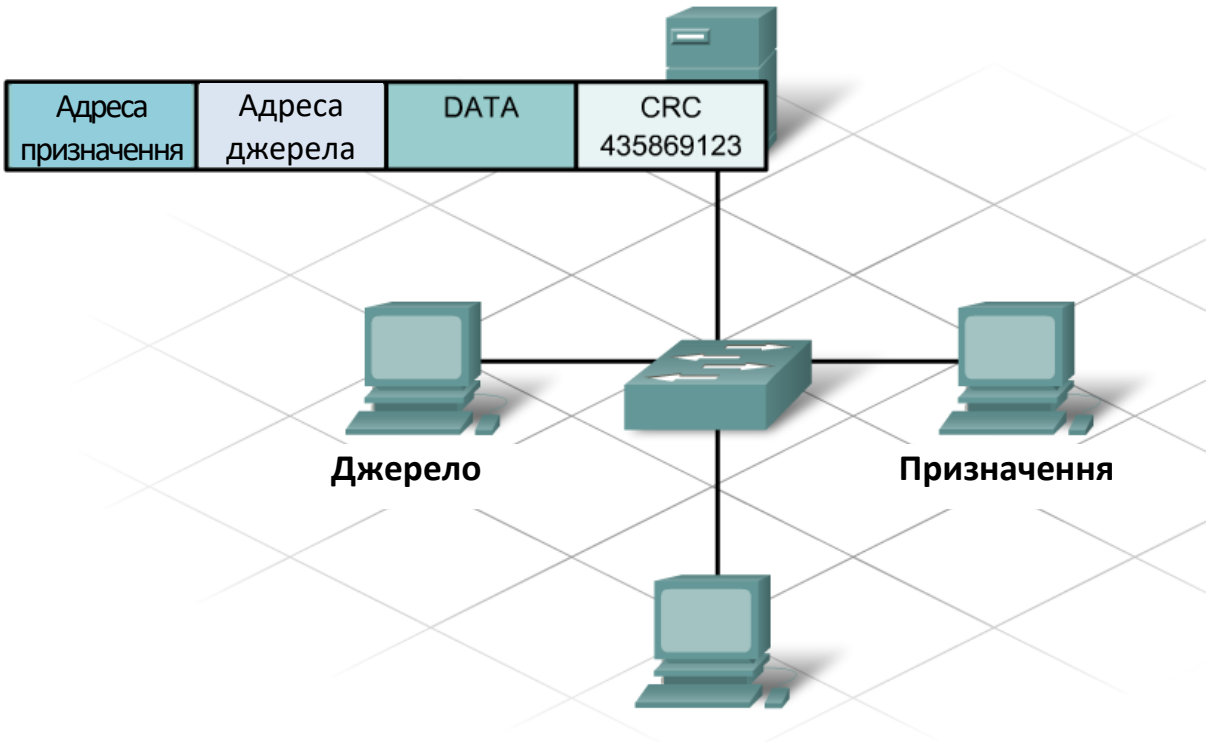


Рисунок 9.7 – Пересилання з буферизацією

Наскрізна комутація

Інший основний метод комутації – наскрізна комутація. Наскрізна комутація включає два методи: швидке пересилання й комутація з виключенням фрагментів. При використанні обох методів комутатор пересилає кадр, не чекаючи його повного прийому. Оскільки комутатор не обчислює й не перевіряє значення CRC, можлива передача ушкоджених кадрів.

Швидке пересилання – найшвидший метод комутації. Комутатор пересилає кадри з порту призначення відразу після зчитування MAC-адреси. Цей метод характеризується найменшим запізнюванням, але може пересилати колізійні й ушкоджені фрагменти. Цей метод комутації найкраще працює в стабільній мережі з невеликою кількістю помилок.

При комутації з виключенням фрагментів комутатор зчитує перші 64 байта кадру перед початком пересилання цього кадру з порту призначення. Мінімальний припустимий кадр Ethernet становить 64 байта. Кадри меншого розміру, як правило, є результатом колізій і називаються кадрами з неприпустимо малою довжиною, або пакет-"коротиш". Перевірка перших 64 байт дозволяє запобігти пересиланню колізійних фрагментів комутатором.

Комутація з буферизацією має найбільше запізнювання, швидке пересилання – найменше. Запізнювання комутації з виключенням фрагментів лежить посередині між цими методами. Комутація з виключенням фрагментів є оптимальним методом у середовищах, у яких виникає багато колізій. У якісно спроектованій мережі, що комутується, колізії не є проблемою, тому кращим методом є швидка комутація.

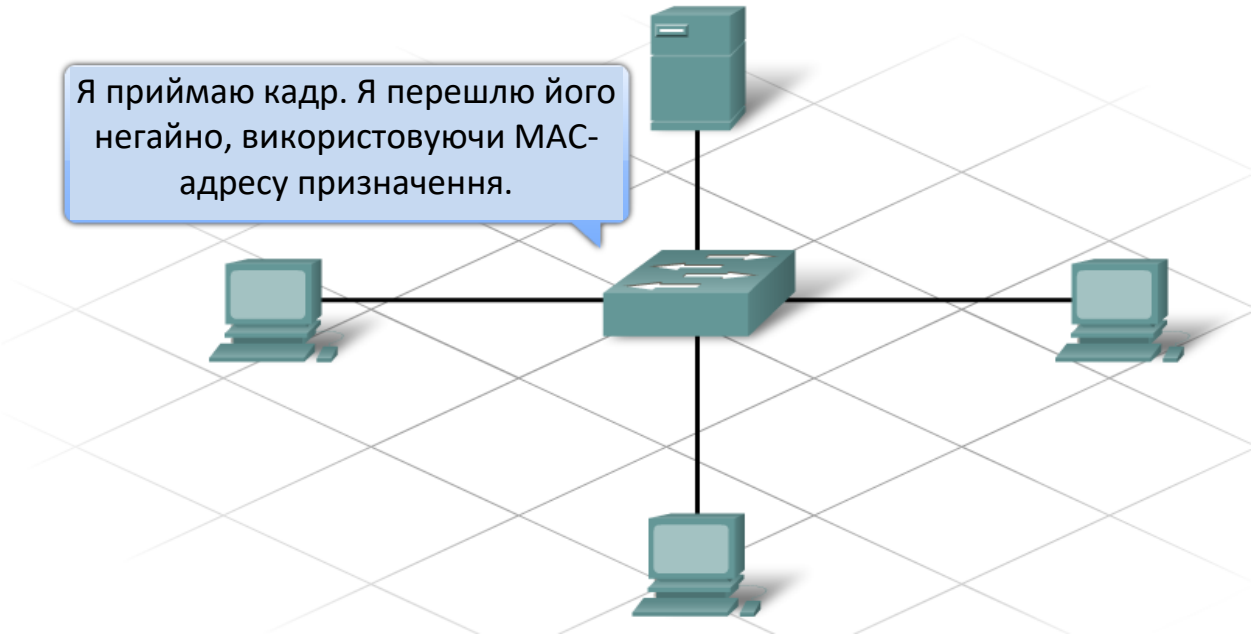


Рисунок 9.8 – Швидка комутація

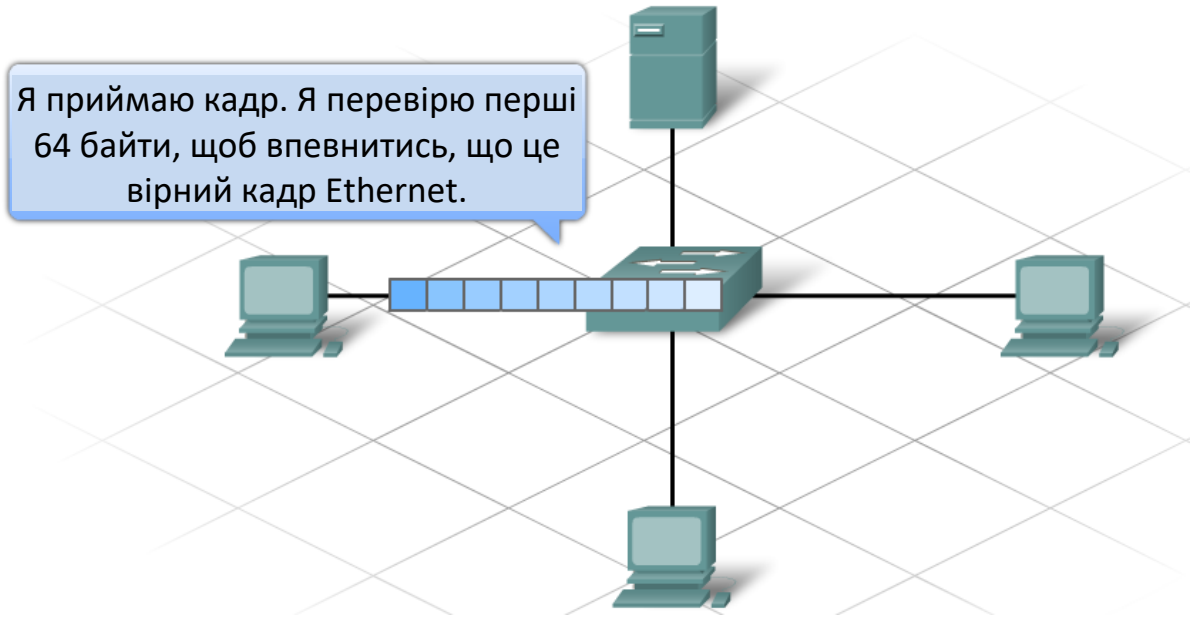


Рисунок 9.9 – Комутація з виключенням фрагментів

У даний момент більшість комутаторів Cisco для локальних мереж використовують метод з буферизацією. Це пов'язане з тим, що нова технологія й низький час обробки дозволяють комутаторам зберігати й обробляти кадри майже так само швидко, як при наскрізній комутації, але без помилок. Крім того, багато функцій вищого класу, такі як багаторівнева комутація, використовують метод комутації з буферизацією.

Крім того, деякі нові комутатори 2-го й 3-го рівнів можуть змінювати метод комутації відповідно до мінливого стану мережі.

Ці комутатори виконують швидке пересилання кадрів, щоб забезпечити мінімальне запізнювання. Незважаючи на те, що комутатор не виявляє помилки перед пересиланням кадру, помилки розпізнаються, і їхня кількість зберігається в пам'яті. Число виявлених помилок рівняється з попередньо заданим граничним значенням.

Якщо кількість помилок перевищує граничне значення, значить комутатор передав неприпустиме число помилкових кадрів. У цьому випадку комутатор перемикається на метод з буферизацією. Якщо кількість помилок опускається нижче граничного значення, комутатор вертається в режим

швидкого пересилання. Цей режим називається адаптивною наскрізною комутацією.

Рисунок 9.10 – Різниця між комутацією з буферизацією і суцільною комутацією

Безпека комутаторів

Підтримуйте безпеку мережі, незалежно від використовуваного методу комутації. Засоби мережевої безпеки часто зосереджують на маршрутизаторах і блокуванні трафіку ззовні. Комутатори є внутрішніми пристроями організації й розроблені для простого доступу, тому до них застосовуються тільки найпростіші міри безпеки або не застосовуються взагалі.

Використовуйте наступні базові міри безпеки комутатора, щоб доступ до нього могли одержати тільки авторизовані співробітники:

– захистіть фізичний доступ до пристрою;

– використовуйте безпечні паролі;

– активуйте доступ через SSH;

– відслідковуйте доступ і трафік;

– відключіть доступ через http;

– відключіть невикористовувані порти;

– включіть захист портів;

– відключіть Telnet.

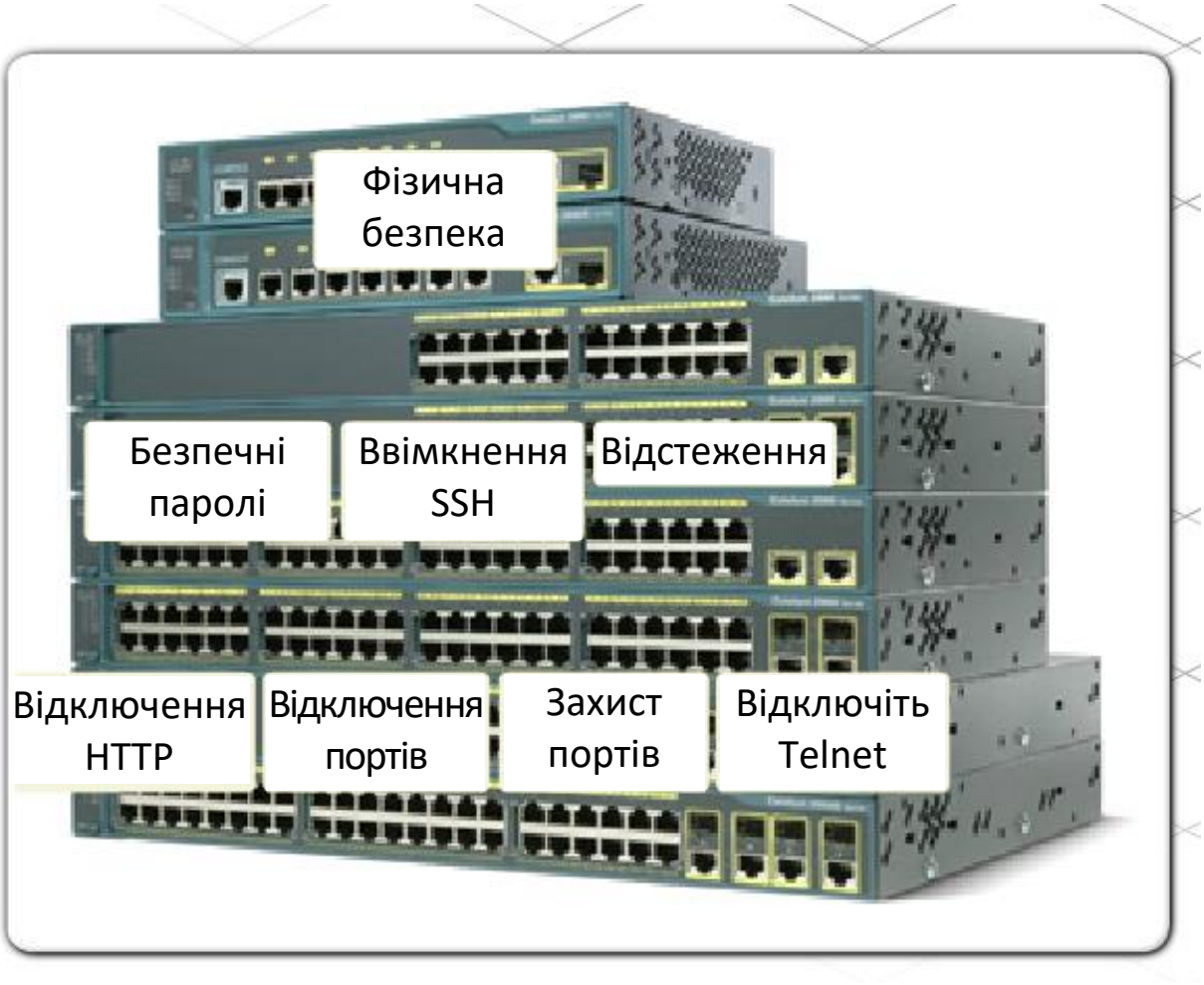


Рисунок 9.11 – Реалізація безпеки мережі на апаратному рівні

Резервування в мережі, що комутується

Сучасні корпорації усе більше покладаються на мережі, іноді від мереж залежить саме їх існування. Мережа – життєво важлива комунікація для багатьох організацій. Простої мережі перетворюються в потенційно катастрофічні втрати бізнесу, прибутку й довіри замовників.

Відмова одного мережевого каналу, одного пристрою або важливого порту комутатора може стати причиною простою мережі. Щоб виключити критичні точки відмови й забезпечити високу надійність, у мережеву архітектуру необхідно ввести резервування. Резервування реалізується

шляхом установки дубльованого устаткування й мережевих пристроїв у важливих областях.

Іноді повне резервування всіх каналів і пристроїв стає невиправдано дорогим. Мережеві інженери часто змушені шукати компроміс між витратами на резервування й вимогами до доступності мережі. Простої мережі перетвориться в потенційно катастрофічні втрати бізнесу, прибутку й довіри замовників.

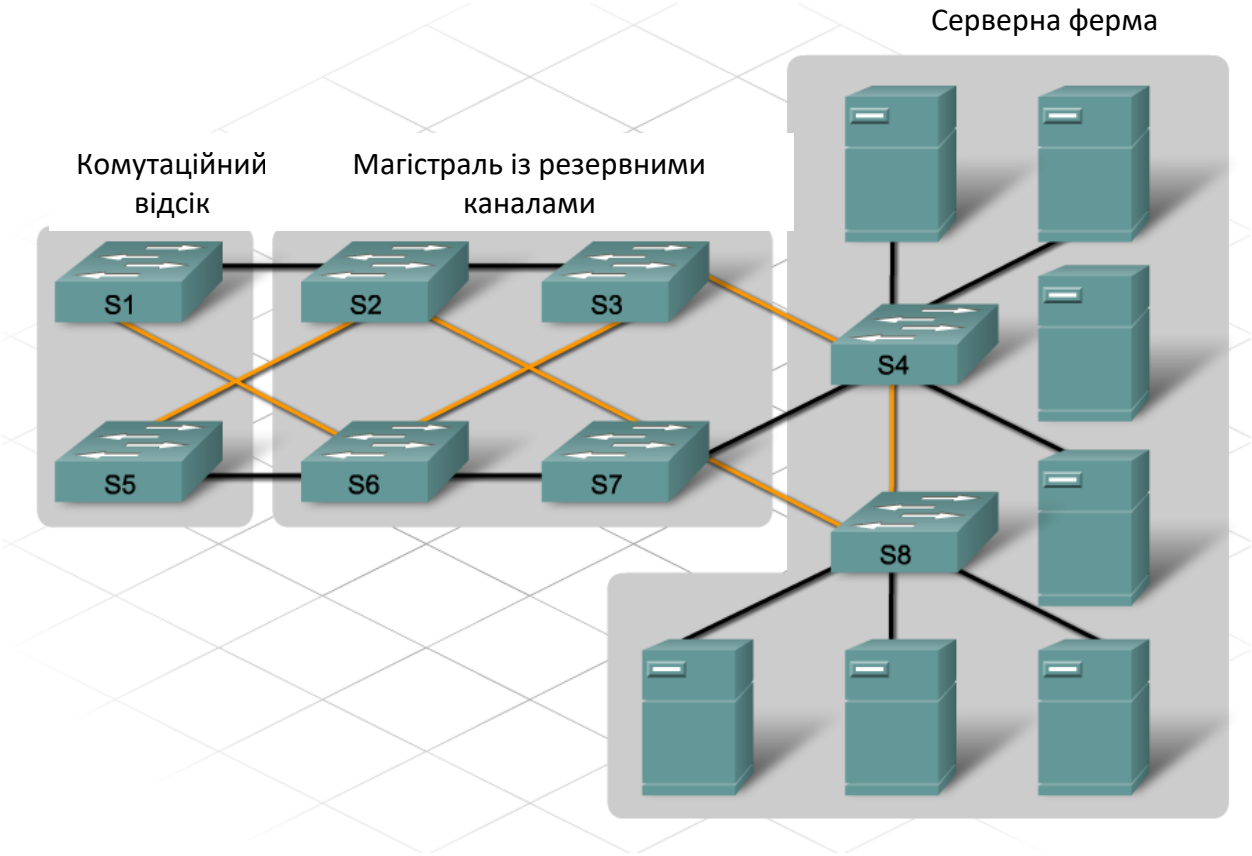


Рисунок 9.12 – Резервування в мережі, що комутується

Резервування позначає наявність двох різних шляхів до одного місця призначення. Приклади резервування в немережевих середовищах: дві дороги в одне місто, два мости через ріку або два виходи в будинку. Якщо один шлях заблокований, другий залишається доступним.

Резервування комутаторів реалізується шляхом створення декількох каналів між ними. Резервні канали в мережі, що комутується, що, знижують перевантаження й підтримують високу доступність і розподіл навантаження.

Однак з'єднання комутаторів може стати причиною проблем. Зокрема, широкомовна природа трафіку Ethernet приводить до утворення петель комутації. Широкомовні кадри циклічно поширюються у всіх напрямках, викликаючи "шторм" широкомовних пакетів. Широкомовні шторми займають всю доступну смугу пропущення, блокують створення нових мережевих підключень і розривають існуючі підключення.

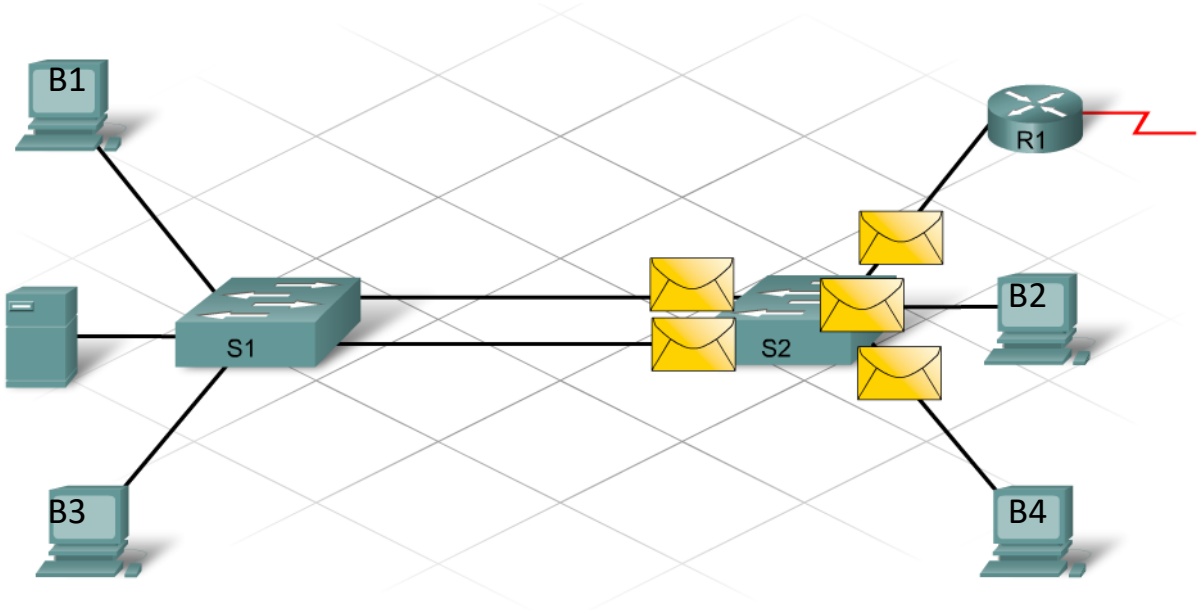


Рисунок 9.13 – Широкомовні шторми

Широкомовні шторми – не єдина проблема, обумовлена резервними каналами в мережі, що комутується. Кадри одноадресного пересилання можуть викликати такі проблеми, як множинна передача кадрів і нестабільність бази даних MAC-адрес.

Множинна передача кадрів

Якщо вузол посилає одноадресний кадр вузлу призначення й MAC-адресу не представлена в жодній з таблиць MAC-адрес підключених

комутаторів, всі комутатори виконують лавинне розсилання цього кадру із всіх портів. У мережі з петлями кадр може повернутися до вихідного комутатора. Цей процес повторюється, що приводить до утворення декількох копій кадру в мережі.

У результаті вузол призначення одержує кілька копій кадру. Це стає причиною трьох проблем: неефективна витрата смуги пропущення, неефективна витрата циклів ЦП і потенційне дублювання транзакційного трафіку.

Нестабільність бази даних MAC-адрес

Комутатори в мережі, що резервується можуть одержувати невірні дані про положення вузла. Якщо в мережі присутня петля, один комутатор може зв'язати MAC-адресу призначення із двома портами. Це приведе до плутанини й неоптимального пересилання кадрів.

Протокол STP

Протокол STP забезпечує механізм відключення резервних каналів у мережі, яка комутується. STP дозволяє використовувати резервування, необхідне для надійної експлуатації, без створення петель комутації.

STP ґрунтується на відкритих стандартах і використовується для створення логічної топології без петель комутації.

Протокол STP відносно самодостатній і вимагає мінімального налаштування. При першому включенні комутатори з підтримкою STP перевіряють мережу, що комутується, на наявність петель. Комутатори, що виявляють потенційну петлю, блокують деякі з підключених портів, залишаючи інші порти активними для пересилання кадрів.

STP задає дерево, що охоплює всі комутатори в топології "ієрархічна зірка". Комутатори постійно перевіряють мережі, щоб гарантувати відсутність петель і ефективну роботу всіх портів.

Щоб запобігти утворенню петель, протокол STP:

– переводить частину інтерфейсів у резервний або заблокований режим;

– залишає інші інтерфейси в режимі пересилання;

– переналаштовує мережа, активуючи відповідний резервний шлях, якщо шлях пересилання стає недоступним.

У термінології STP термін "комутатор" часто заміняється терміном "міст". Наприклад, кореневий міст – це основний міст або центральна точка в топології STP. Кореневий міст взаємодіє з іншими комутаторами за допомогою блоків даних протоколу мосту (BPDU). BPDU – це кадри, які розсилаються іншим комутаторам кожні 2 секунди. BPDU містять наступні відомості:

– ідентифікатор комутатора-джерела;

– ідентифікатор порту-джерела;

– вартість порту-джерела;

– значення таймерів старіння;

– значення таймера вітання.

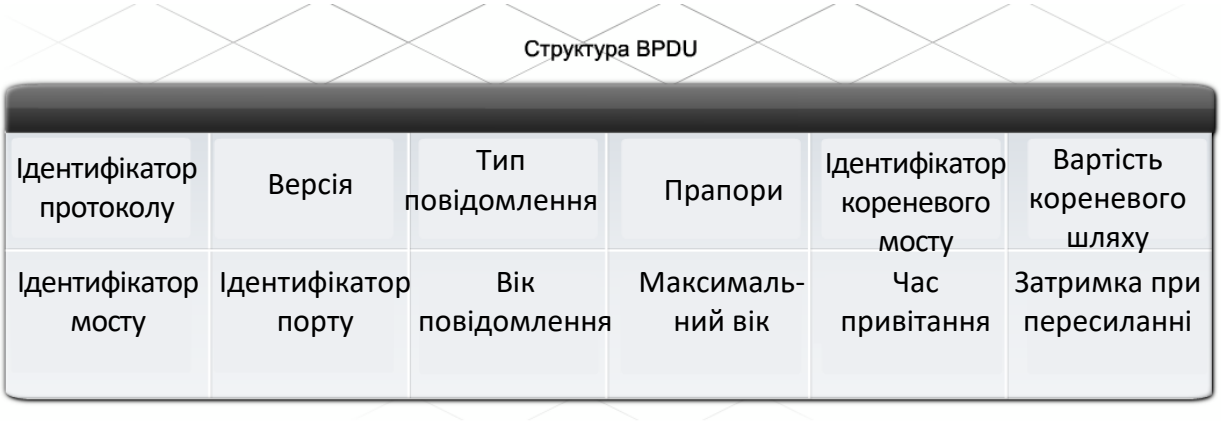


Рисунок 9.14 – Структура BPDU

При включенні комутатора кожний порт проходить через послідовність із 4 режимів: блокування, прослуховування, навчання й пересилання. П'ятий режим, "відключений", указує на те, що адміністратор відключив порт комутатора.

У міру того, як порт проходить через ці режими, колір світлодіодних індикаторів міняється від миготливого жовтогарячого до немиготливого зеленого. Проходження через режими STP може зайняти до 50 секунд, після чого комутатор буде готовий до пересилання кадрів.

При включенні комутатор переходить у режим, що блокує, щоб запобігти негайному утворенню петлі. Потім він переходить у режим прослуховування, що має на увазі прийом BPDU від сусідніх комутаторів. Після обробки цієї інформації комутатор визначає, які порти можуть пересилати кадри, не формуючи петлі. Якщо порт може пересилати кадри, він переходить у режим навчання, а потім у режим пересилання.

Порти доступу не утворять петлі в мережі, що комутується, що, і завжди переходять у режим пересилання при підключенні вузла. Магістральні порти можуть утворювати петлі й переходити в режим, що блокує, або в режим навчання.

Кореневі мости

Комутатори в мережі визначають комутатор, що є центральною точкою мережі, щоб протокол STP міг функціонувати. STP використовує центральну точку мережі, що називається кореневим мостом або кореневим комутатором, для визначення портів, які необхідно блокувати, і портів, які варто перевести в режим пересилання. Кореневий міст розсилає кадри BPDU з інформацією про топологію мережі всім іншим комутаторам. Ця інформація забезпечує переналаштування мережі у випадку відмови.

У кожній мережі працює тільки один кореневий міст, що вибирається на підставі ідентифікатора мосту (BID). BID рівняється сумі значення пріоритету мосту і його MAC-адреси.

Значення пріоритету мосту за замовчуванням рівняється 32 768. Якщо MAC-адресу комутатора AA-11-BB-22-CC-33, BID буде дорівнює 32768: 22-CC-33.

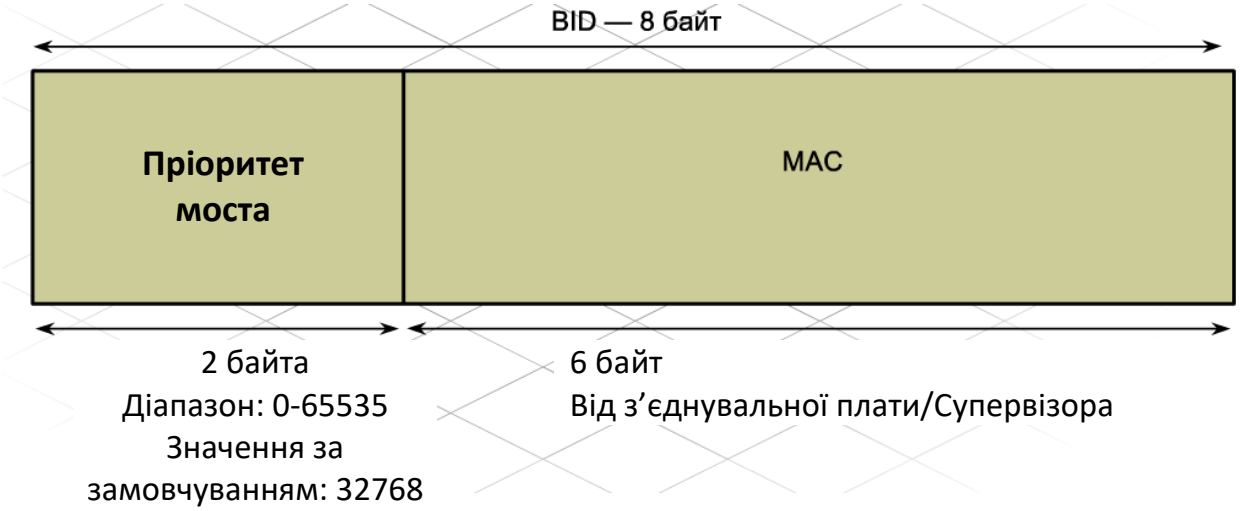


Рисунок 9.15 – Значення BID

Міст із найменшим значенням BID стає кореневим. Оскільки комутатори, як правило, використовують однакове значення пріоритету за замовчуванням, комутатор з найменшим MAC-адресою стає кореневим мостом.

При включенні комутатор припускає, що є кореневим мостом, і розсилає кадри BPDU зі своїм ідентифікатором BID. Наприклад, якщо комутатор S2 повідомляє кореневий ідентифікатор менше, ніж ідентифікатор S1, S1 припиняє оголошення свого ідентифікатора мосту й приймає кореневий ідентифікатор S2. S2 стає кореневим мостом.

STP використовує три типи портів: кореневі порти, призначені порти й заблоковані порти.

Кореневий порт

Порт із маршрутом оптимальної вартості до кореневого мосту призначається кореневим. Комутатори обчислюють шлях з найменшою вартістю, використовуючи вартість смуги пропущення кожного каналу на шляху до кореневого мосту.

Призначений порт

Призначений порт пересилає трафік до кореневого мосту, але не підключений до шляху з найменшою вартістю.

Заблокований порт

Заблокований порт не пересилає трафік.

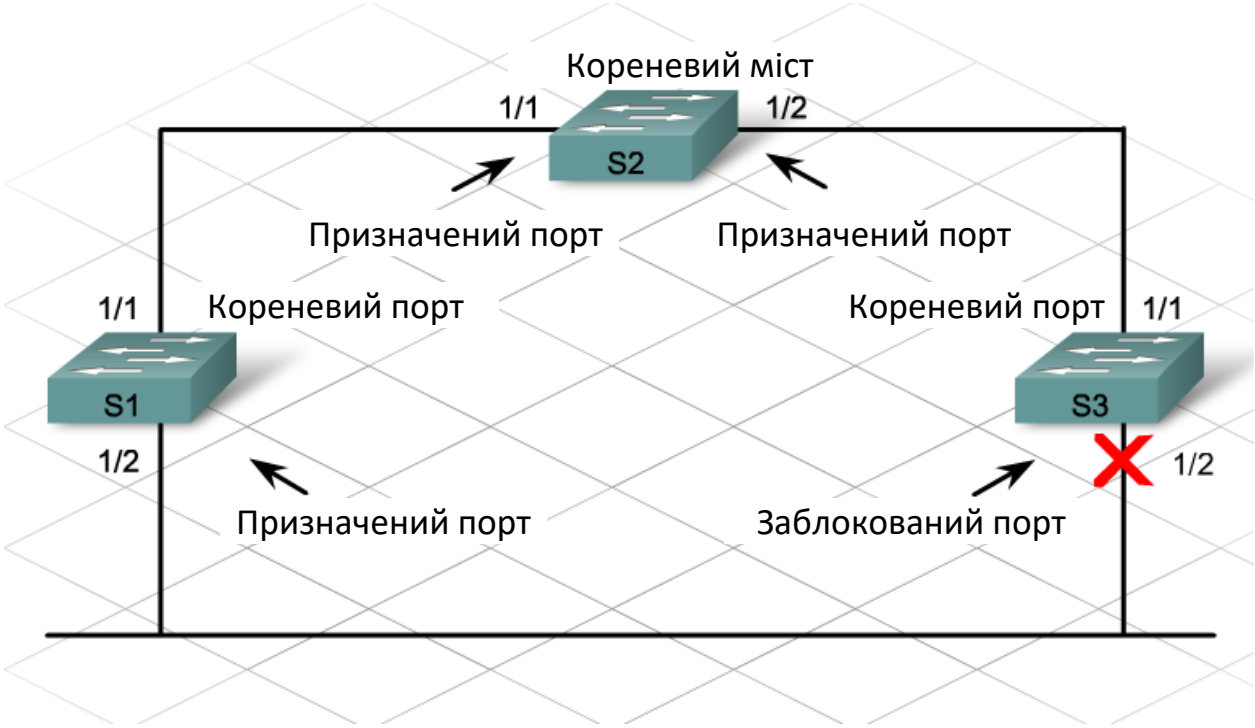


Рисунок 9.16 – Види портів

Перед налаштуванням STP мережевий технік планує й оцінює мережу, щоб вибрати комутатор, що буде оптимальним кореневим мостом STP. Якщо кореневий міст буде обраний по мінімальному MAC-адресу, пересилання може бути неоптимальним.

Як кореневий міст найкраще буде працювати комутатор, розташований у центрі мережі. Блокування порту, розташованого на периферії мережі, приведе до того, що трафік буде передаватися до місця призначення по більш довгому маршруту, ніж при використанні комутатора в центрі мережі.

Щоб задати кореневий міст, для BID обраного комутатора налаштовується мінімальний пріоритет. Для налаштування пріоритету мосту використовується команда bridge priority. Значення пріоритету може перебувати в діапазоні від 0 до 65 535, але крок між значеннями становить 4 096. Значення за замовчуванням – 32 768.

Завдання пріоритету:

S3(config)#bridge priority 4096

Відновлення пріоритету за замовчуванням:

S3(config)#no bridge priority

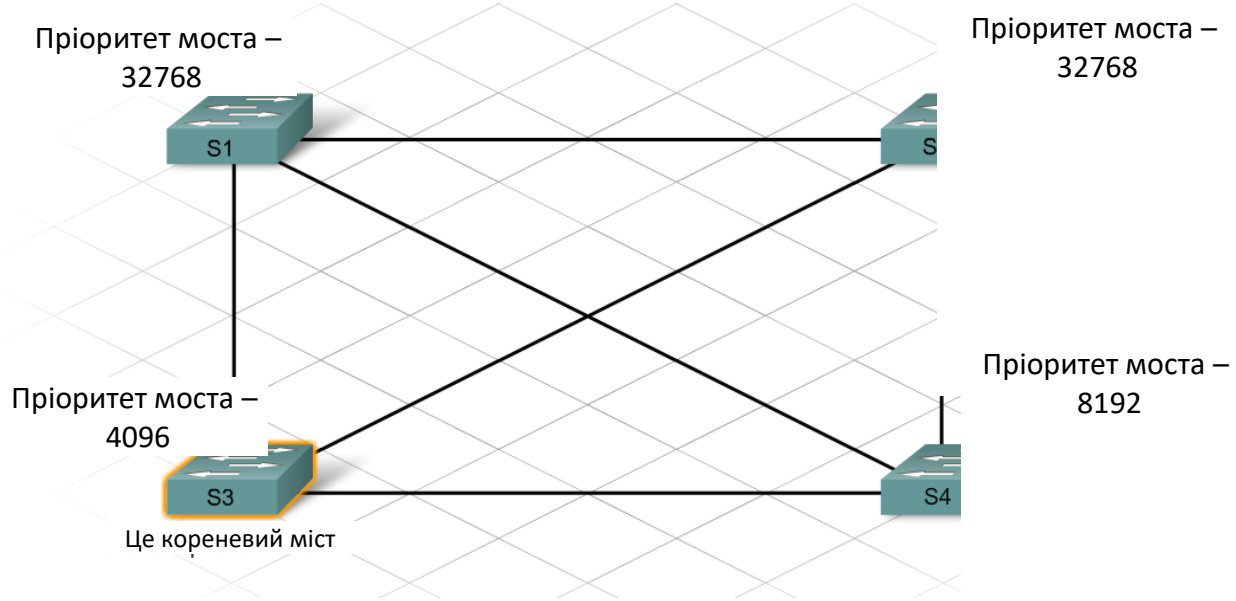


Рисунок 9.17 – Кореневий міст

Протокол STP в ієрархічній мережі

Після завдання кореневого мосту, а також кореневих, призначених і заблокованих портів, STP розсилає кадри BPDU по мережі, що комутується, з 2-секундним інтервалом. STP продовжує відслідковувати ці BPDU, щоб переконатися у відсутності каналів, що відмовили, і нових петель.

Якщо відбувається відмова каналу, STP перераховується шляхом:

– перекладу деяких портів з режиму, що блокує, у режим пересилання;

– перекладу деяких портів з режиму пересилання в режим, що блокує;

– формування нового дерева STP для запобігання утворення петель у мережі.

Протокол STP не є миттєвим. Коли канал відключається, STP виявляє відмову й розраховує найкращі шляхи через мережу. Цей розрахунок і процес переходу займають від 30 до 50 секунд для кожного комутатора. Користувальницькі дані не проходять через порти, для яких виконується перерахунок.

Час очікування деяких користувальницьких додатків може минути під час перерахунку, що може привести до зниження продуктивності й втраті прибутку. Частий перерахунок STP негативно впливає на час роботи систем.

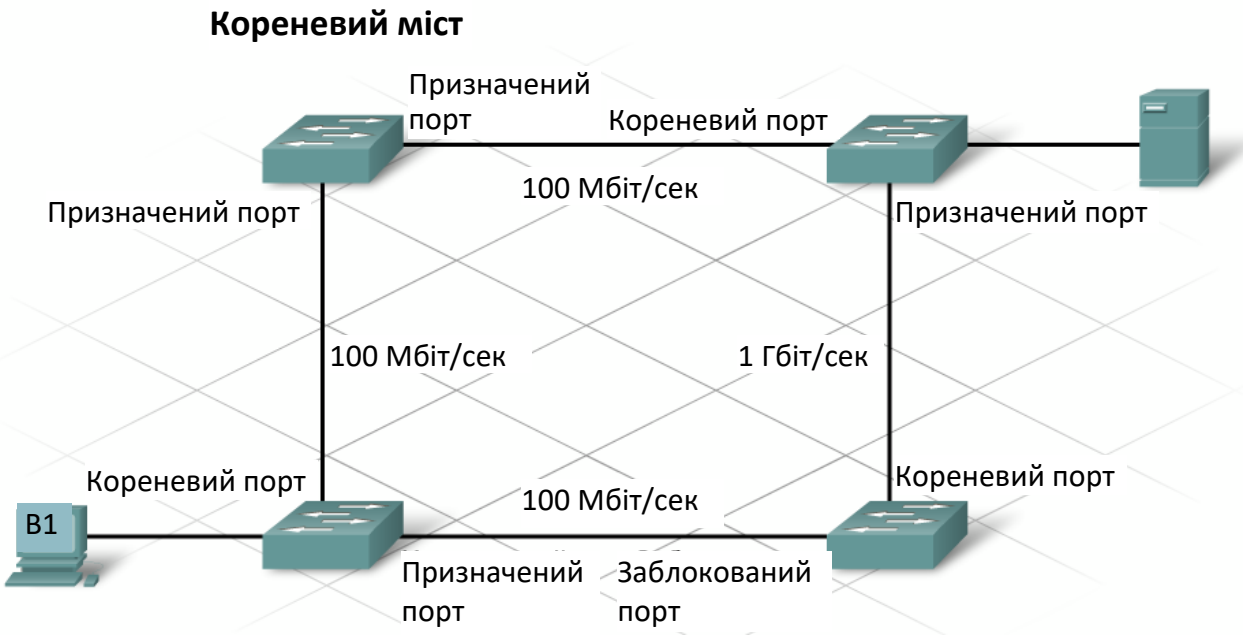


Рисунок 9.18 – Протокол STP в ієрархічній мережі

Великий корпоративний сервер підключений до порту комутатора. Якщо для цього порту виконується перерахунок через STP, сервер буде недоступний протягом 50 секунд. Важко представити, яка кількість транзакцій буде загублена за цей час.

У стабільній мережі перерахунки STP рідкі. Якщо мережа нестабільна, необхідно перевірити стабільність комутаторів і зміни їхніх конфігурацій. Одна з найпоширеніших причин перерахунків STP – несправне джерело живлення або кабель живлення комутатора. Несправність джерела живлення викликає несподіване перезавантаження пристрою.

Ряд удосконалень STP зводить до мінімуму час простоїв, викликаних перерахунком STP.

PortFast

STP PortFast негайно переводить порт доступу в режим пересилання, минаючи режими прослуховування й навчання. Застосування PortFast на портах доступу, підключених до однієї робочої станції або сервера, дозволить їм негайно підключатися до мережі, не очікуючи конвергенції STP.

UplinkFast

STP UplinkFast прискорює вибір нового кореневого порту при відмові комутатора або каналу, а також при перерахунку STP. Кореневий порт негайно переходить у режим пересилання, минаючи режими прослуховування й навчання, які маються на увазі звичайними процедурами STP.

BackboneFast

BackboneFast забезпечує швидку конвергенцію після змін топології STP. Ця функція дозволяє швидко відновлювати підключення до магістралі. Функція BackboneFast використовується на рівні розподілу й центральному рівні, на яких з'єднується кілька комутаторів.

PortFast, UplinkFast і BackboneFast – це функції, правами на які володіє компанія Cisco, тому їх не можна використовувати в мережах, що включає комутатори інших виробників. Крім того, всі ці функції вимагають налаштування.

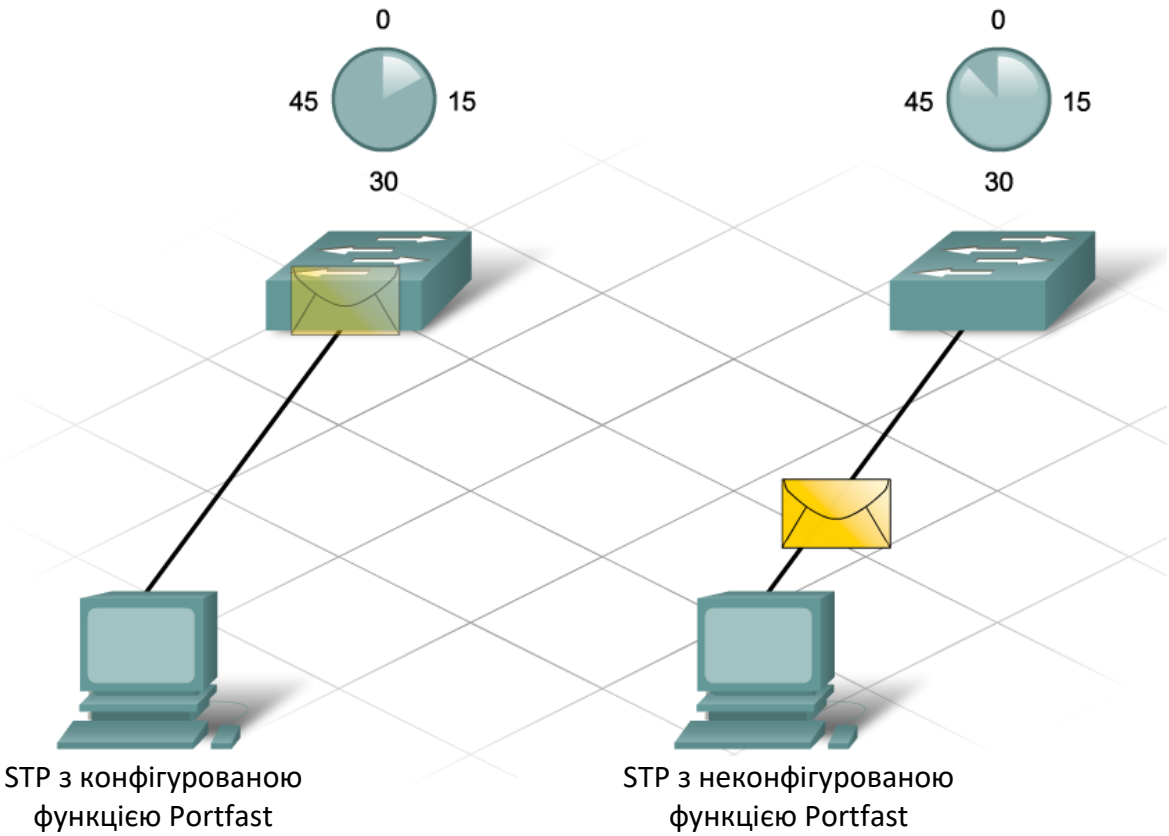


Рисунок 9.19 – Реалізація PortFast

РОЗДІЛ 10. VLAN І ПРОТОКОЛ VTP

VLAN

Вузли й сервери, підключені до комутаторів 2-го рівня, вважаються частиною мережевого сегмента. Така організація характеризується двома серйозними проблемами:

– комутатори виконують лавинне розсилання широкомовних кадрів із всіх портів, що приводить до невиправданого споживання смуги пропущення. Зі збільшенням числа пристроїв, підключених до комутатора, генерується більше широкомовного трафіку, що займає більшу смугу пропущення;

– всі пристрої, підключені до комутатора, можуть пересилати й одержувати кадри від інших пристроїв на цьому комутаторі.

При проектуванні мережі рекомендується обмежувати широкомовний трафік областю мережі, у якій він необхідний. Існують причини організаційного характеру, по яких одні вузли можуть одержувати доступ друг до других, а інші ні. Наприклад, доступ до бухгалтерського сервера можуть мати тільки співробітники бухгалтерії. У мережі, що комутується для обмеження широкомовних розсилань і об'єднання вузлів у групи по інтересах створюються віртуальні локальні мережі (VLAN).

VLAN – це логічний домен широкомовного розсилання, що може охоплювати кілька фізичних сегментів LAN. Вона дозволяє адміністраторові поєднувати станції по логічній функції, проектній групі або додатку незалежно від фізичного положення користувачів.

Різниця між фізичними й віртуальною (логічної) мережами продемонстрована в наступному прикладі:

Учні школи розділені на дві групи. Кожному учневі першої групи дана червона картка для ідентифікації. Кожному учневі другої групи дана синя картка. Директор повідомляє, що учні із червоними картками можуть

говорити тільки з іншими власниками червоних карток, а учні із синіми картками – тільки з іншими власниками синіх карток. Таким чином, учні логічно розділені на дві віртуальні групи або VLAN.

Завдяки такому логічному об'єднанню широкомовний кадр розсилається тільки групі із червоними картками, незважаючи на те, що група із червоними картками й група із синіми картками фізично перебувають в одній школі.

Цей приклад також демонструє іншу функцію VLAN. Широкомовні кадри не пересилаються між VLAN, вони залишаються усередині однієї VLAN.

Кожна VLAN функціонує як окрема локальна мережа. VLAN може охоплювати один або кілька комутаторів, що дозволяє вузлам працювати так, ніби вони перебували в одному сегменті.

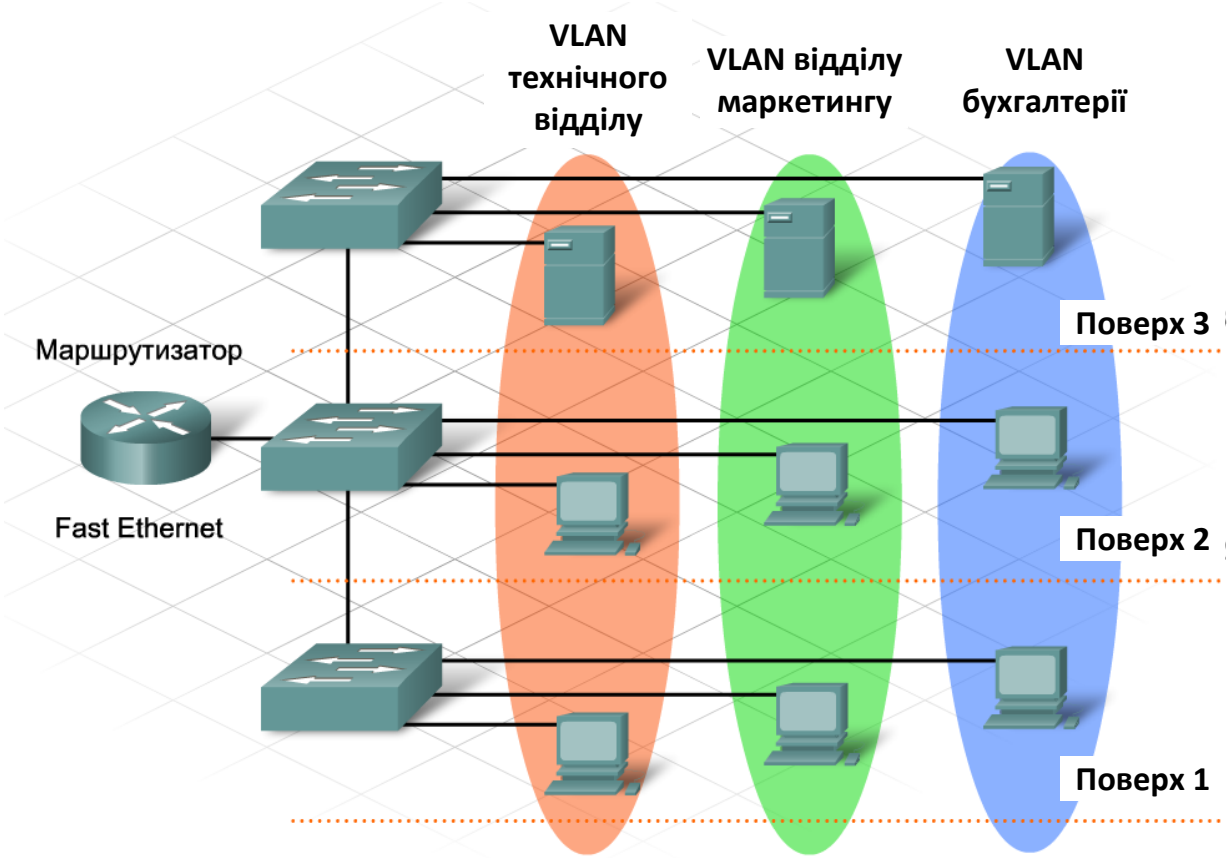


Рисунок 10.1 – Структура VLAN

VLAN виконують дві основні функції:

– обмеження широкомовних розсилань;

– об'єднання пристроїв у групи; пристрою, розташованому в одній VLAN, та невидимі для пристроїв, розташованих в інший VLAN.

Для передачі трафіку між VLAN необхідний пристрій 3-го рівня.

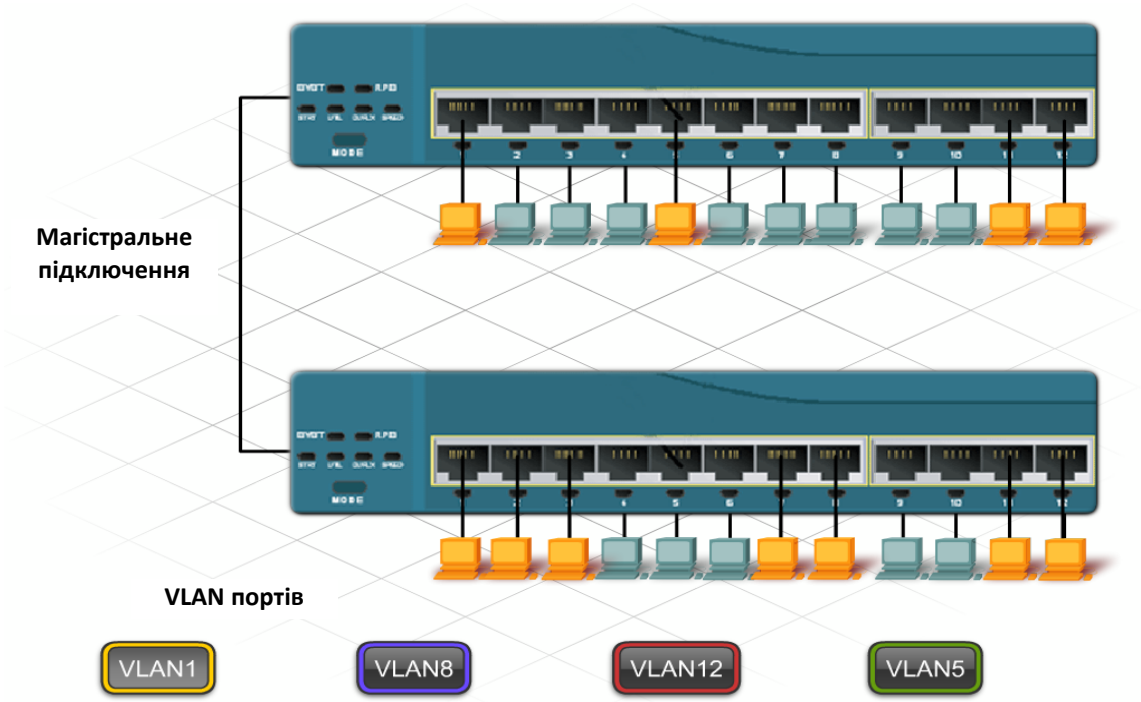
У мережі, що комутується, пристрій можна призначити в VLAN відповідно до його положення, MAC-адресою, IP-адресою або додатками, які він використовує найчастіше. Адміністратори задають приналежність пристрою VLAN статично або динамічно.

Для завдання статичної приналежності VLAN адміністратор повинен вручну призначити кожний порт комутатора в певну VLAN. Наприклад, порт fa0/3 можна призначити в VLAN 20. Будь-який пристрій, що підключається до порту fa0/3, автоматично стає членом VLAN 20.

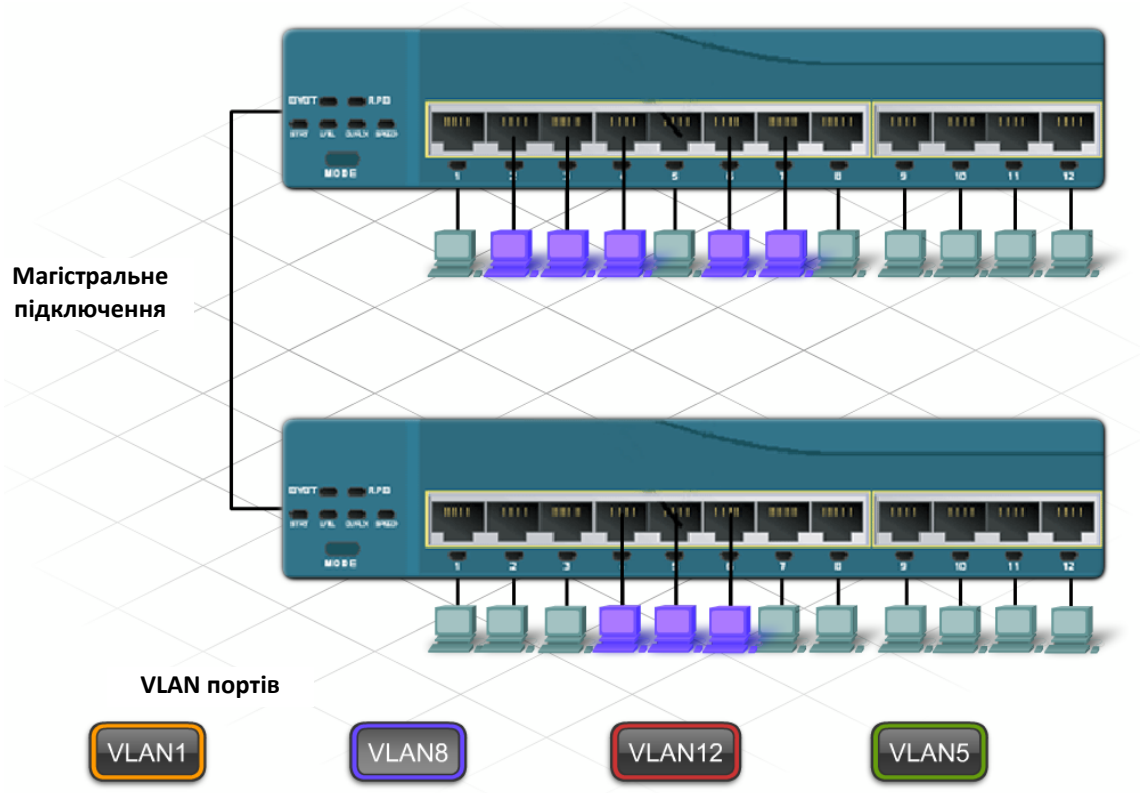
Цей тип приналежності VLAN найпростіше налаштовувати й він найпопулярніший, але додавання, переміщення й зміна пристроїв зажадає значного втручання адміністратора. Наприклад, переміщення вузла з однієї VLAN в іншу зажадає або ручного перепризначення порту комутатора в нову VLAN, або перемикання кабелю робочої станції в інший порт комутатора, що відноситься до нового VLAN.

Приналежність пристрою мережі VLAN повністю прозора для користувачів. Користувачі, які працюють із пристроєм, підключеним до порту комутатора, не знають, що є членами VLAN.

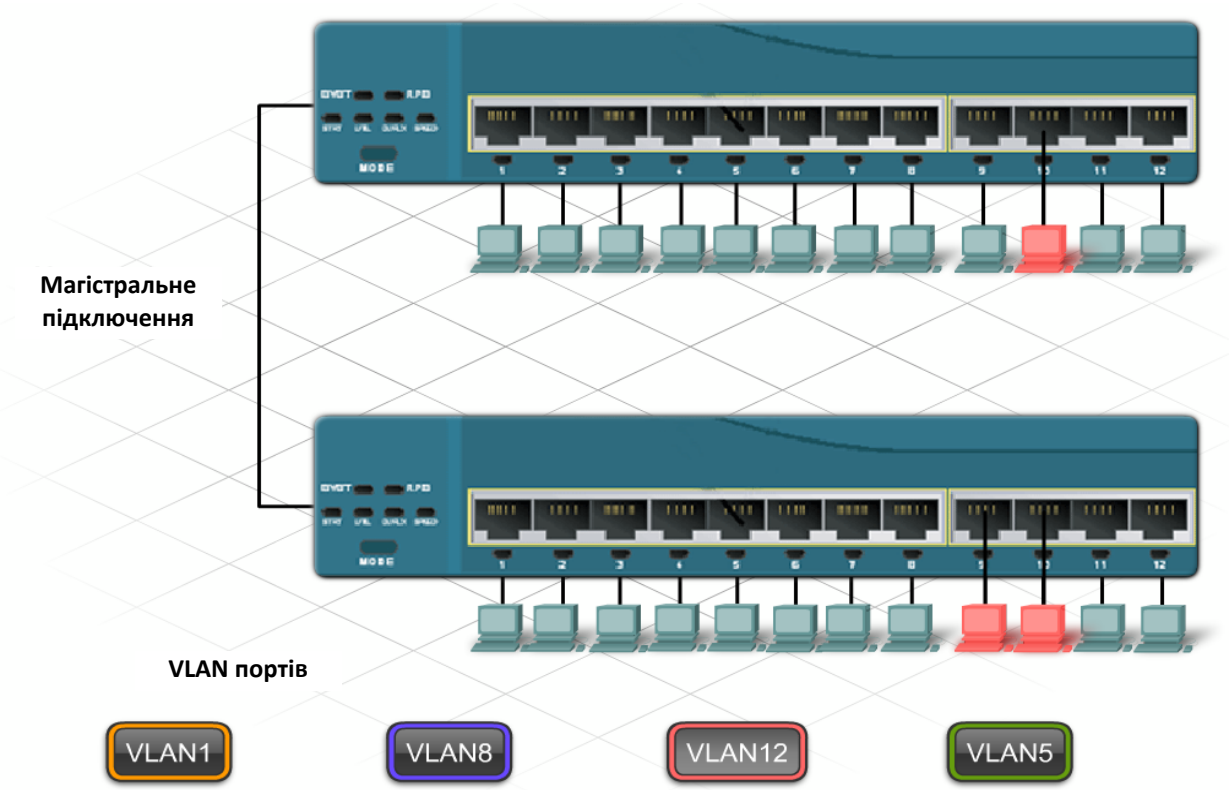
Динамічна приналежність VLAN вимагає наявності сервера керування політикою VLAN (VMPS). VMPS містить базу даних, що зіставляє MAC-адреси з мережами VLAN. Коли пристрій підключається до порту, VMPS шукає його MAC-адресу у своїй базі даних і тимчасово призначає порт у відповідну VLAN.


Магістральне
підключення
VLAN портів
VLAN1
VLAN8
VLAN12
VLAN5

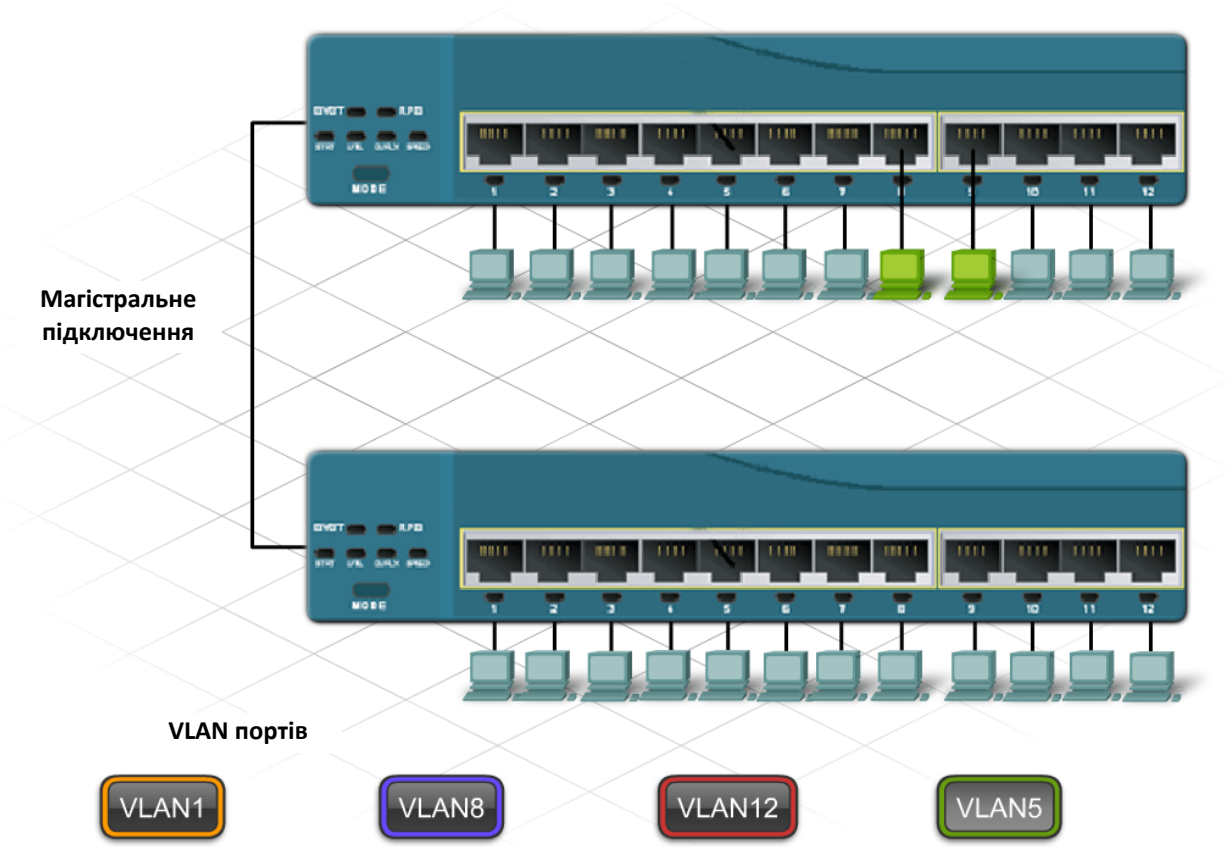
а)


Магістральне
підключення
VLAN портів
VLAN1
VLAN8
VLAN12
VLAN5

б)



в)



г)

Рисунок 10.2 – Розмежування VLAN

Динамічна приналежність VLAN вимагає більше складного налаштування й організації, але формує більше гнучку структуру, ніж статична приналежність VLAN. Переміщення, додавання й зміна компонентів у динамічної VLAN виконується автоматично й не вимагає втручання адміністратора.

Примітка. Не всі комутатори Catalyst підтримують VMPS.

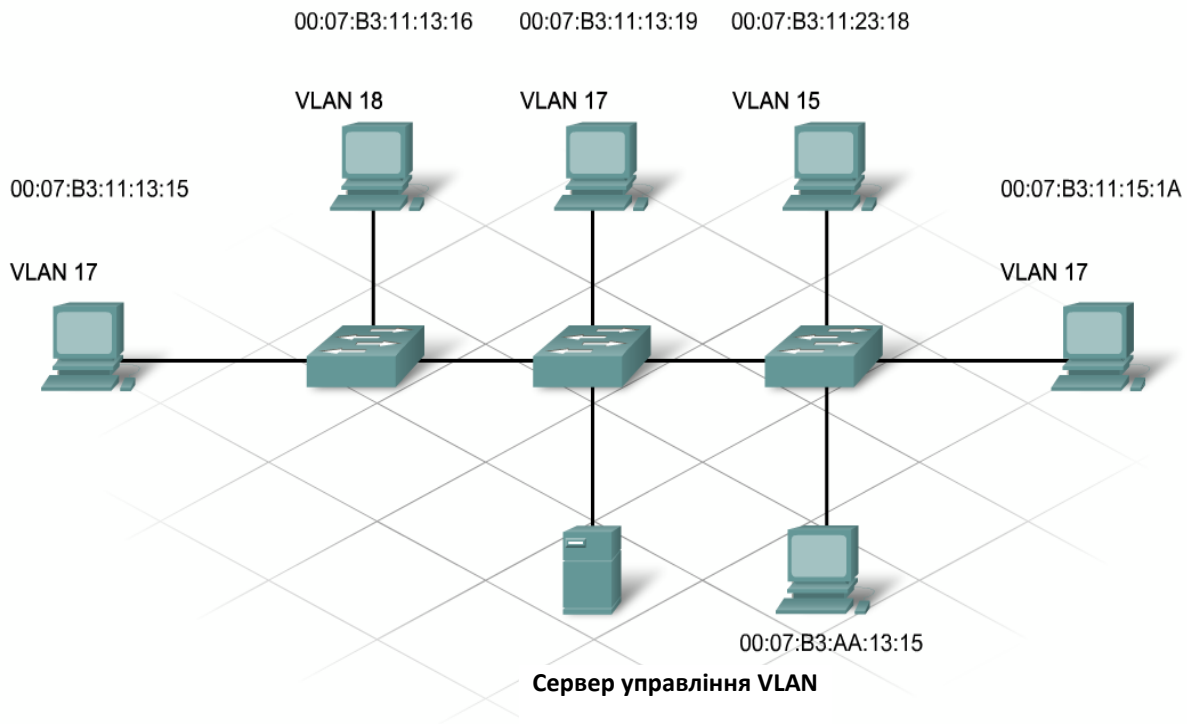


Рисунок 10.3 – Реалізація VMPS

Максимальне загальне число статичних і динамічних VLAN залежить від типу комутатора й версії IOS. За замовчуванням у якості VLAN керування застосовується VLAN1.

Адміністратори використовують IP-адресу VLAN керування для віддаленого налаштування комутатора. Віддалений доступ до комутатора дозволяє адміністраторові мережі налаштовувати й обслуговувати всі конфігурації VLAN.

Крім того, VLAN керування використовується для обміну даними, наприклад трафіком протоколів CDP (Cisco Discovery Protocol) і VTP (VLAN Trunking Protocol), з іншими мережевими пристроями.

При створенні мережі VLAN призначається номер і ім'я. Номер VLAN – це будь-яке число з діапазону, доступного комутатору, крім VLAN1. Деякі комутатори підтримують приблизно 1000 VLAN, інші – більше 4000. Іменування VLAN уважається рекомендується методом, що, керування мережею.

Магістральні порти VLAN виконують три основні функції:

– обмеження розміру широкомовних розсилань;

– поліпшення продуктивності мережі;

– підвищення безпеки.

Щоб повною мірою скористатися перевагами VLAN, необхідно поширити їх на кілька комутаторів.

Для портів комутатора можна задати дві різні ролі. Порт може бути визначений як порт доступу або як магістральний порт.

Порт доступу

Порт доступу належить тільки до однієї VLAN. Як правило, окремі пристрої, такі як комп'ютери й сервери, підключаються до портів такого типу. Якщо кілька комп'ютерів підключаються до одного порту доступу через концентратор, всі пристрої, підключені до концентратора, будуть належати до однієї VLAN.

Магістральний порт

Магістральний порт – це канал типу " точка-точка" між комутатором і іншим мережевим пристроєм. Магістральні підключення служать для передачі трафіку декількох VLAN через один канал і забезпечують ним доступ до всієї мережі. Магістральні порти необхідні для передачі трафіку декількох VLAN між пристроями при з'єднанні двох комутаторів, комутатора й маршрутизатора або комутатора й мережевого адаптера вузла з підтримкою транкінгу 802.1Q.

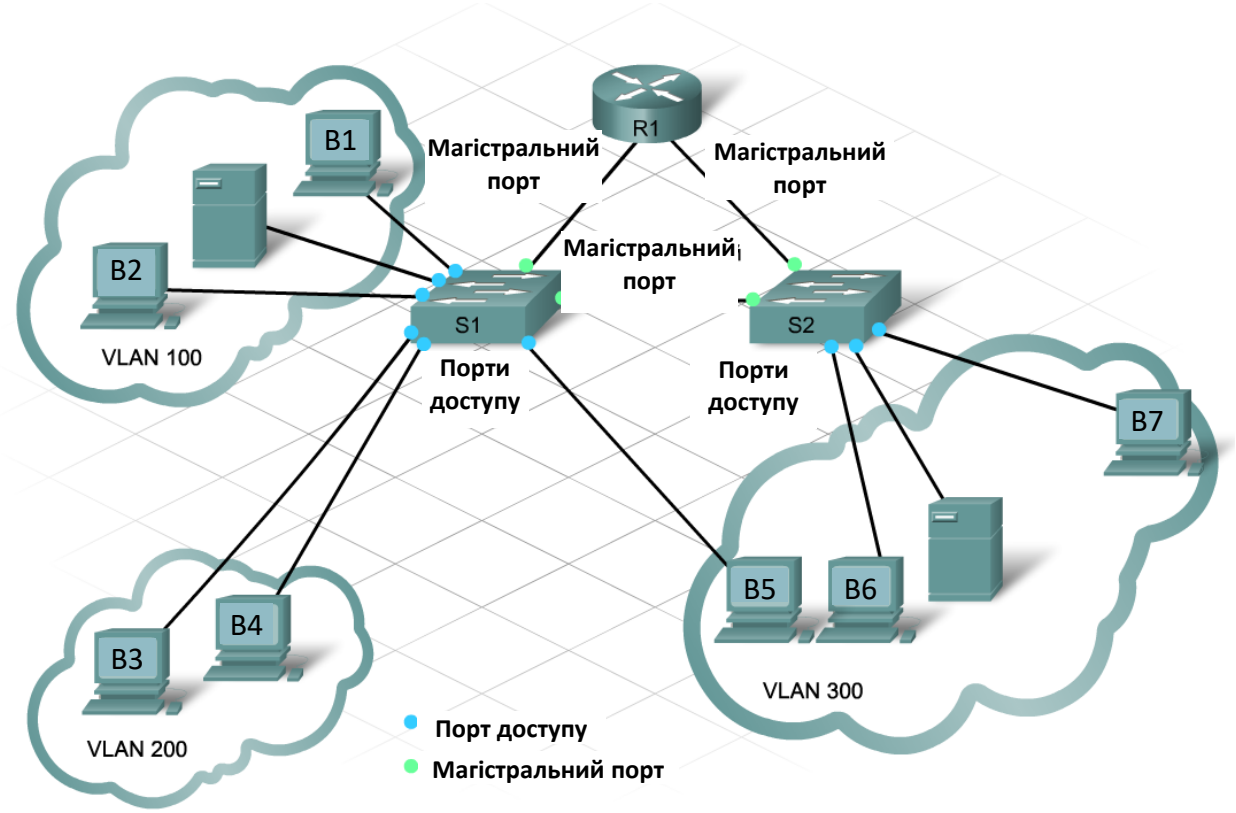


Рисунок 10.3 – Реалізація порту доступу й магістрального порту

Без магістральних портів для кожної VLAN було потрібно б окреме з'єднання між комутаторами. Наприклад, корпорації з 100 VLAN буде потрібно 100 каналів зв'язку. При такій організації мережа не масштабується належним чином і дуже дорога. Магістральні канали дозволяють вирішити цю проблему за рахунок передачі трафіку декількох VLAN через один канал.

Для передачі трафіку декількох VLAN через один канал необхідна їхня ідентифікація. Магістральний порт підтримує маркування кадрів. Маркування кадрів дозволяє додати до кадру дані VLAN.

IEEE 802.1Q – стандартний і затверджений метод маркування кадрів. Корпорація Cisco розробила власний протокол маркування кадрів за назвою міжкомутаторний канал (ISL). Комутатори більше високого класу, такі як Catalyst 6500, підтримують обидва протоколи маркування, однак більшість комутаторів LAN, таких як 2960, підтримують тільки 802.1Q.

Маршрутизація між VLAN

Хоча VLAN можуть охоплювати кілька комутаторів, тільки пристрою, що відносяться до однієї VLAN, можуть взаємодіяти один з одним.

Для з'єднання між VLAN необхідний пристрій 3-го рівня. Така організація дозволяє адміністраторові мережі здійснювати строгий контроль над типами трафіку, які передаються з однієї VLAN в іншу.

Один з методів маршрутизації між VLAN вимагає окремого підключення інтерфейсу до пристрою 3-го рівня для кожної VLAN.

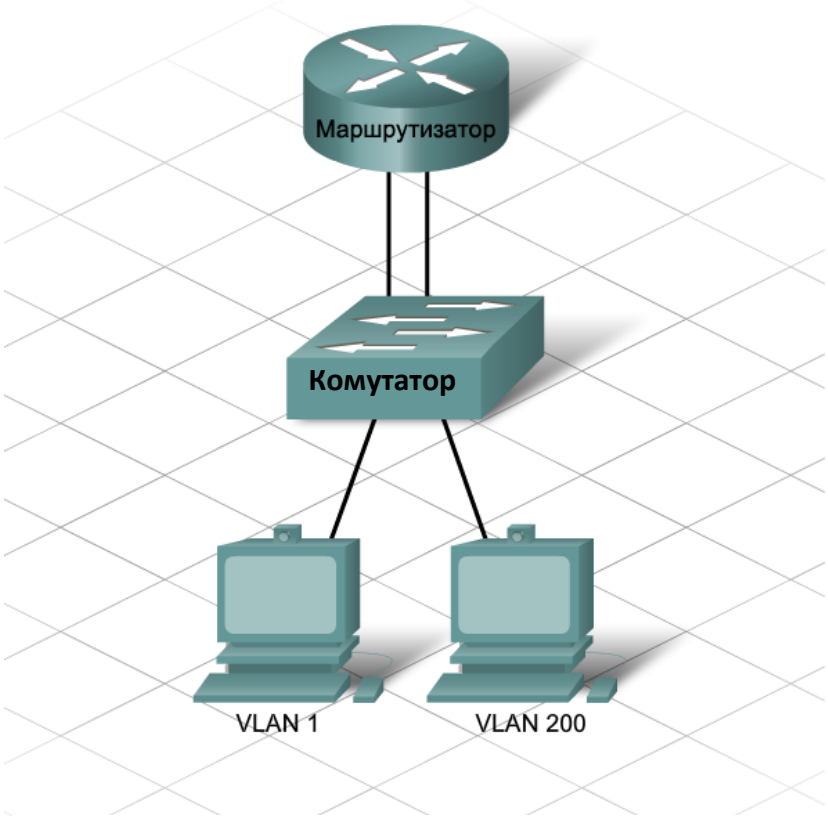


Рисунок 10.4 – Маршрутизація між VLAN

Інший метод з'єднання між VLAN вимагає функції, що називається підінтерфейсами. Підінтерфейси дозволяють логічно розділити один фізичний інтерфейс на кілька логічних шляхів. Для кожної VLAN налаштовується окремий шлях або підінтерфейс.

Взаємодія між VLAN з використанням підінтерфейсів вимагає налаштування як маршрутизатора, так і комутатора.

Комутатор:

Налаштуйте інтерфейс комутатора як магістральний канал 802.1Q.

Маршрутизатор:

– виберіть інтерфейс маршрутизатора не нижче FastEthernet 100 Мбіт/с;

– налаштуйте підінтерфейси з підтримкою інкапсуляції 802.1Q;

– для кожної VLAN налаштовується один підінтерфейс.

Підінтерфейс дозволяє кожній VLAN мати власний логічний шлях і шлюз за замовчуванням до маршрутизатора.

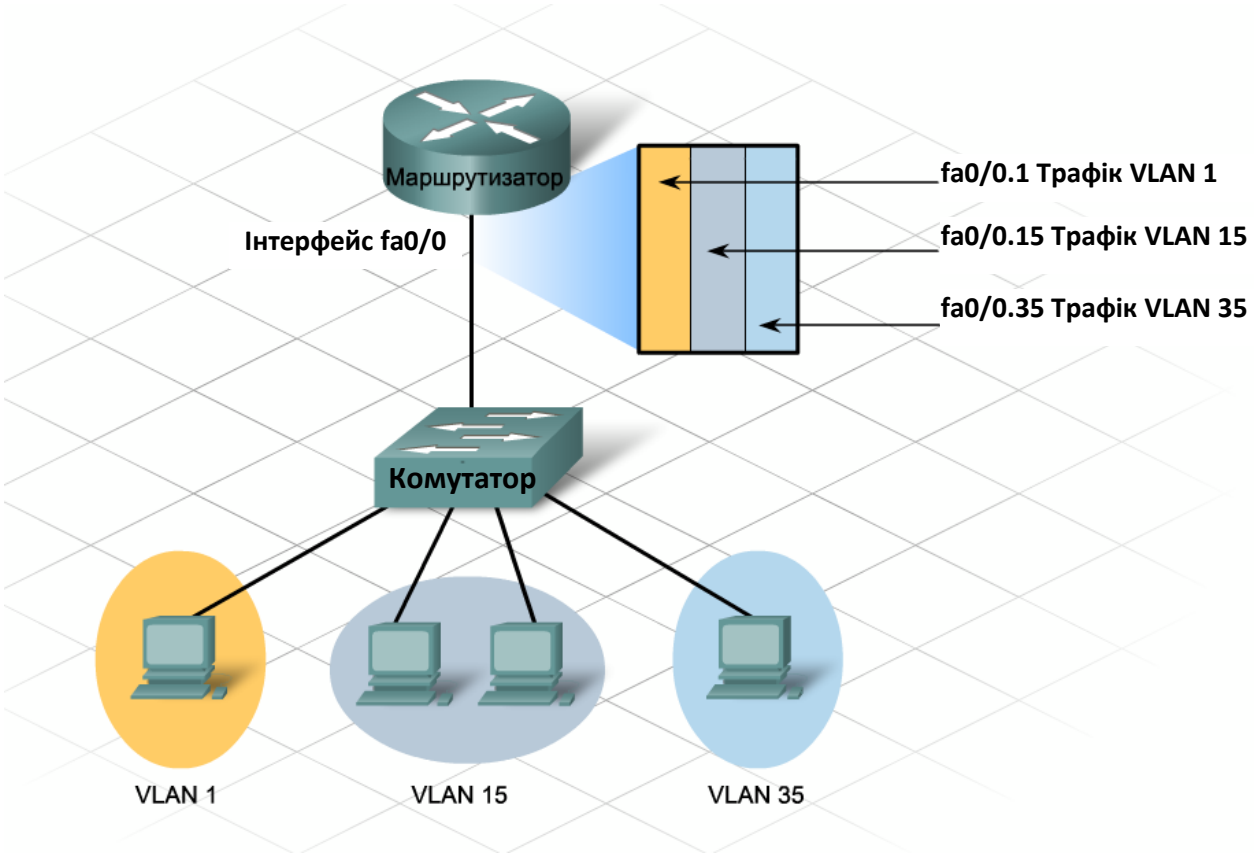


Рисунок 10.5 – Реалізація інтерфейсів

Вузол з передавальної VLAN пересилає трафік маршрутизатору, використовуючи шлюз за замовчуванням. Підінтерфейс VLAN визначає

шлюз за замовчуванням для всіх вузлів цієї VLAN. Маршрутизатор визначає IP-адресу призначення й виконує пошук по таблиці маршрутизації.

Якщо VLAN призначення відноситься до того ж комутатору, що й вихідна VLAN, маршрутизатор пересилає трафік назад до вихідного комутатора, використовуючи параметри підінтерфейсу й ідентифікатора VLAN призначення. Така конфігурація часто називається каскадом маршрутизаторів ("маршрутизатор на паличці") (від англ.: on-a-stick).

Якщо вихідний інтерфейс маршрутизатора сполучимо з 802.1Q, кадр зберігає 4-байтну мітку VLAN. Якщо вихідний інтерфейс несумісний з 802.1Q, маршрутизатор відокремлює мітку від кадру й повертає кадр в оригінальний формат Ethernet.

Протокол VTP

Зі збільшенням розміру й складності мережі централізоване керування структурою VLAN стає критично важливим. Протокол VTP (VLAN Trunking Protocol) – це протокол обміну повідомленнями 2-го рівня, що надає метод керування базою даних VLAN із центрального сервера в мережевому сегменті. Маршрутизатори не пересилають відновлення VTP.

Без автоматизованого методу керування корпоративною мережею із сотнями VLAN потрібно було б ручне налаштування кожної VLAN на кожному комутаторі. Будь-яка зміна структури VLAN зажадало б додаткового ручного налаштування. Один невірно набраний номер може стати причиною нестійкості з'єднань по всій мережі.

Щоб вирішити цю проблему, корпорація Cisco створила протокол VTP, що автоматизує багато завдань конфігурації VLAN. VTP гарантує погоджене обслуговування конфігурації VLAN по всій мережі й зменшує необхідність у керуванні й моніторингу VLAN.

VTP – це протокол обміну повідомленнями з архітектурою " клієнт-сервер", що додає, видаляє й перейменовує VLAN в одному домені VTP. Всі комутатори під загальним керуванням є частиною домену. У кожного домену

є унікальне ім'я. Комутатори VTP обмінюються повідомленнями VTP тільки з іншими комутаторами в домені.

Існує дві різні версії VTP: 1 і 2. Версія 1 – версія за замовчуванням і вона несумісна з версією 2. На всіх комутаторах необхідно налаштувати одну версію протоколу.

VTP використовує три режими: серверний, клієнтський і прозорий. За замовчуванням всі комутатори є серверами. Рекомендується налаштувати хоча б два комутатори в мережі як сервери, щоб забезпечити резервування.

При використанні VTP кожний сервер повідомляє повідомлення через свої магістральні порти. Повідомлення включають домен керування, номер версії конфігурації, відомі VLAN і параметри кожної VLAN. Кадри оголошень відправляються за адресою багатоадресного розсилання, тому їх одержують всі сусідні вузли.

Кожний комутатор VTP зберігає базу даних VLAN, що включає номер версії конфігурації, в енергонезалежній пам'яті (NVRAM). Якщо VTP одержує відновлення з більше високим номером версії, ніж номер у базі даних, комутатор додає нові дані у свою базу даних VLAN.

Номер зміни конфігурації VTP починається з нуля. При внесенні змін номер версії конфігурації збільшується на одиницю. Номер версії продовжує збільшуватися, поки не досягає 2 147 483 648. При досягненні цього значення лічильник скидається в нуль. Крім того, номер версії скидається при перезавантаженні комутатора.

Проблема, пов'язана з номером версії, може виникнути, якщо хтось додасть у мережу комутатор з більше високим номером версії, не перезавантаживши його. Оскільки за замовчуванням комутатор перебуває в серверному режимі, нові, але невірні дані можуть перезаписати коректні дані VLAN на всіх інших комутаторах.

Один зі способів забезпечити захист від цієї критичної ситуації складається в завданні паролів VTP для перевірки комутаторів. Перед додаванням нового комутатора в існуючу мережу завжди перезавантажуйте

його, щоб скинути номер версії. Крім того, при додаванні комутатора в мережу, у якій уже є комутатор у серверному режимі, переконаєтеся, що новий комутатор налаштований у прозорому або клієнтському режимі.

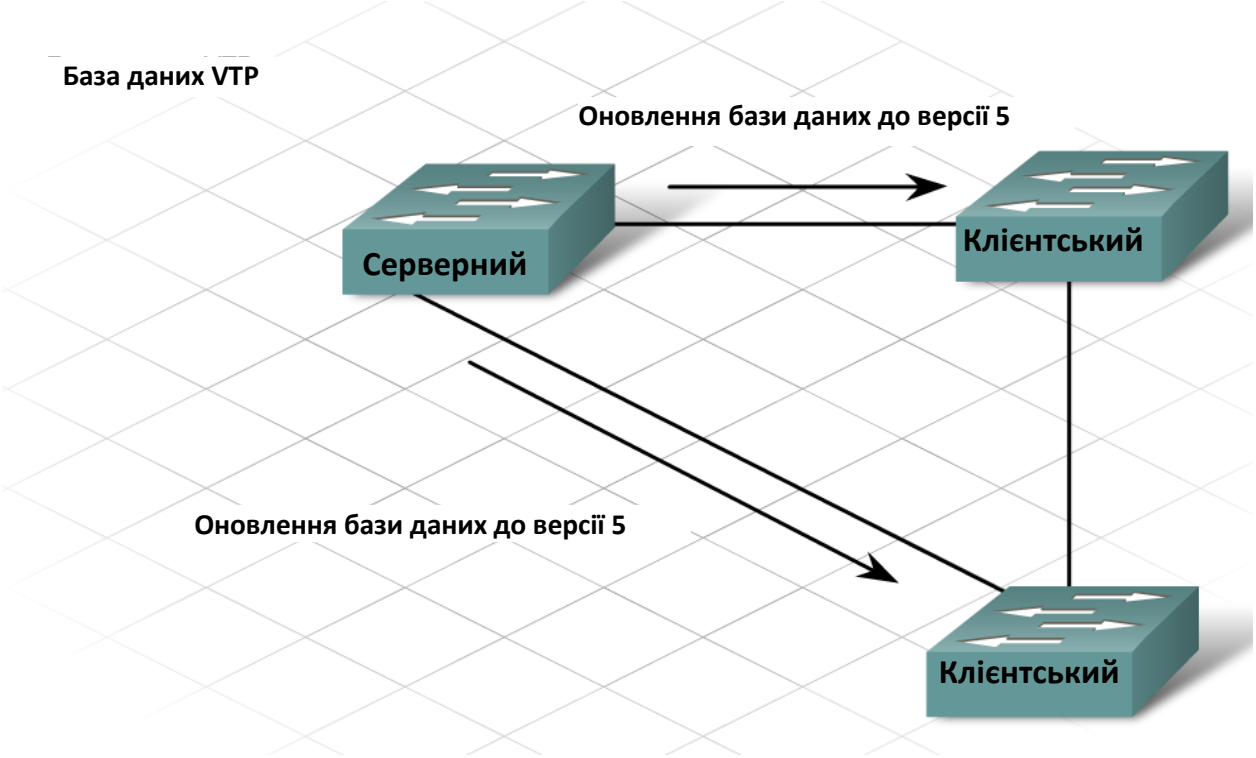


Рисунок 10.6 – Прокол VTP

Існує три типи повідомлень VTP: зведені оголошення, скорочені оголошення й запити оголошень.

Зведені оголошення

Комутатори Catalyst розсилають зведені оголошення кожні 5 хвилин, а також при зміні бази даних VLAN. Зведені оголошення містять поточне ім'я домену VTP і номер версії конфігурації.

При додаванні, видаленні або зміні VLAN сервер збільшує номер версії конфігурації й відправляє зведене оголошення.

При одержанні пакета зведеного оголошення комутатор порівнює ім'я домену VTP зі своїм ім'ям домену VTP. Якщо імена домену збігаються, комутатор порівнює номер версії конфігурації зі своїм номером. Якщо

отриманий номер нижче, комутатор ігнорує пакет. Якщо номер версії вище, відправляється запит оголошення.

Скорочені оголошення

Скорочене оголошення відправляється після зведеного оголошення. Скорочене оголошення містить список даних VLAN.

Скорочене оголошення містить нові дані VLAN, засновані на зведеному оголошенні. Якщо в мережі трохи VLAN, буде потрібно кілька скорочених оголошень.

Запити оголошень

VTP-клієнти використовують запити оголошень, щоб запросити інформацію про VLAN. Запити оголошень необхідні, якщо комутатор скинутий або змінене ім'я домену VTP. Комутатор одержує зведене оголошення VTP з більше високим номером версії конфігурації, ніж його власний.

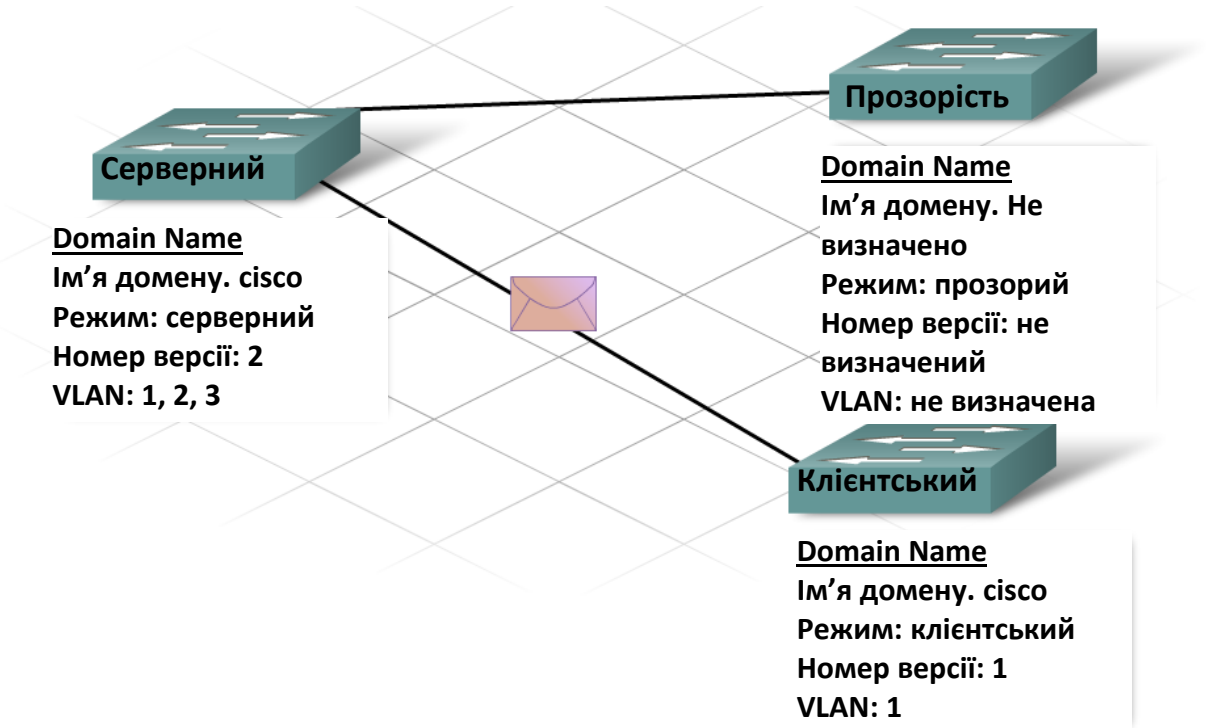


Рисунок 10.7 – Режими VTP-клієнтів

РОЗДІЛ 11. БЕЗДРОТОВІ ТЕХНОЛОГІЇ Й ПРИСТРОЇ

Крім дротових мереж існують різні технології передачі інформації між вузлами без кабелів. Такі технології називаються бездротовими.

Бездротові технології передбачають передачу інформації між пристроями за допомогою електромагнітних хвиль. Електромагнітна хвиля переносить радіосигнали без проводів.

У спектр електромагнітних хвиль входять смуги частот радіо і телевізійних програм, видиме світло, рентгенівське випромінювання й гамма-випромінювання. У кожної з цих частот своя довжина хвилі й відповідний енергетичний рівень, як показано на діаграмі.

Деякі електромагнітні хвилі неприйнятні для передачі даних. Інші області цього спектра регламентуються урядами й надаються різним організаціям по ліцензії для певних цілей. Деякі області спектра виділені для мереж загального користування, можуть використовуватися без обмежень і без необхідності одержання спеціальних дозволів. Для загальнодоступних бездротових мереж використовується інфрачервоний спектр і частина радіочастотного (РЧ) діапазону.

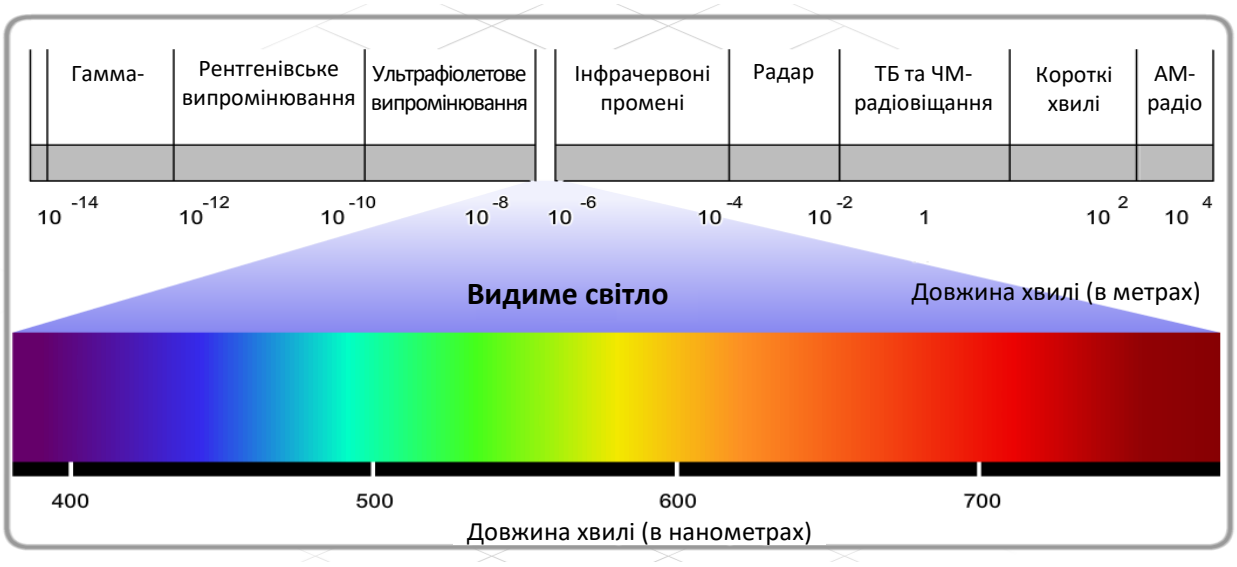


Рисунок 11.1 – Спектр електромагнітних хвиль

Інфрачервоний діапазон

Інфрачервоне випромінювання (IR) відрізняється відносно слабким енергетичним рівнем і не може проникати через стіни або інші перешкоди. Проте, воно звичайно використовується для встановлення з'єднань і передачі даних між пристроями, такими як КПК і ПК. Для обміну інформацією між пристроями за допомогою інфрачервоного випромінювання використовується спеціалізований комунікаційний порт IrDA (Infrared Direct Access). Передача даних по ІЧ-випромінюванню передбачає встановлення з'єднання тільки одного типу.

ІЧ-випромінювання застосовується також у пристроях дистанційного керування, у бездротових маніпуляторах "миша" і в бездротових клавіатурах. Воно забезпечує зв'язок у межах малої дальності й у межах видимості. При цьому ІЧ-сигнали можуть відбиватися від поверхні об'єктів, що збільшує радіус дії. Для більшого радіуса дії потрібні більше високі частоти електромагнітного випромінювання.

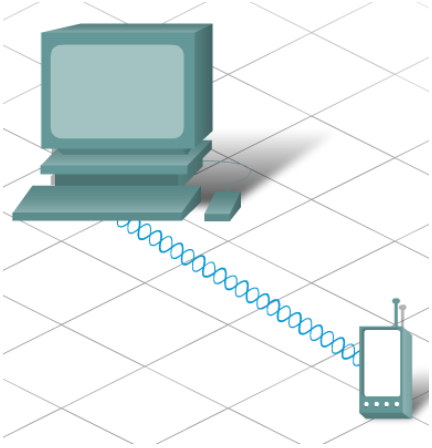


Рисунок 11.2 – Передача даних по ІЧ-випромінюванню передбачає

Радіочастотний діапазон (RF)

Радіохвилі можуть проникати через стіни та інші перешкоди, що дозволяє домогтися більшого радіуса дії, ніж в ІЧ-випромінювання.

Деякі області радіочастотного діапазону зарезервовані для роботи таких неліцензуємих систем, як бездротові локальні мережі, бездротові телефони й периферійні пристрої комп'ютерів. Ці пристрою працюють у діапазонах частот 900 Мгц, 2,4 Ггц і 5 Ггц. Ці смуги називаються ISM-смугами (Industrial, Scientific, Medical) і використовуються з дуже незначними обмеженнями.

Технологія Bluetooth працює в смузі частот 2,4 Ггц. Швидкість передачі даних і радіус дії цієї технології обмежений, але її перевага полягає в тому, що вона дозволяє обмінюватися даними між декількома пристроями одночасно. Завдяки можливості встановлювати зв'язок одного пристрою з багатьма, технологія Bluetooth більш краща в порівнянні з ІЧ-технологією, тому що вона дозволяє забезпечувати зв'язок з периферійними комп'ютерними пристроями, такими як миші, клавіатури й принтери.

До числа інших технологій, що використовують смуги частот 2,4 Ггц і 5 Ггц, ставляться сучасні технології бездротових локальних мереж, що відповідають вимогам різних стандартів IEEE 802.11. На відміну від технології Bluetooth їхня потужність передачі вища й відповідно більше радіус дії.

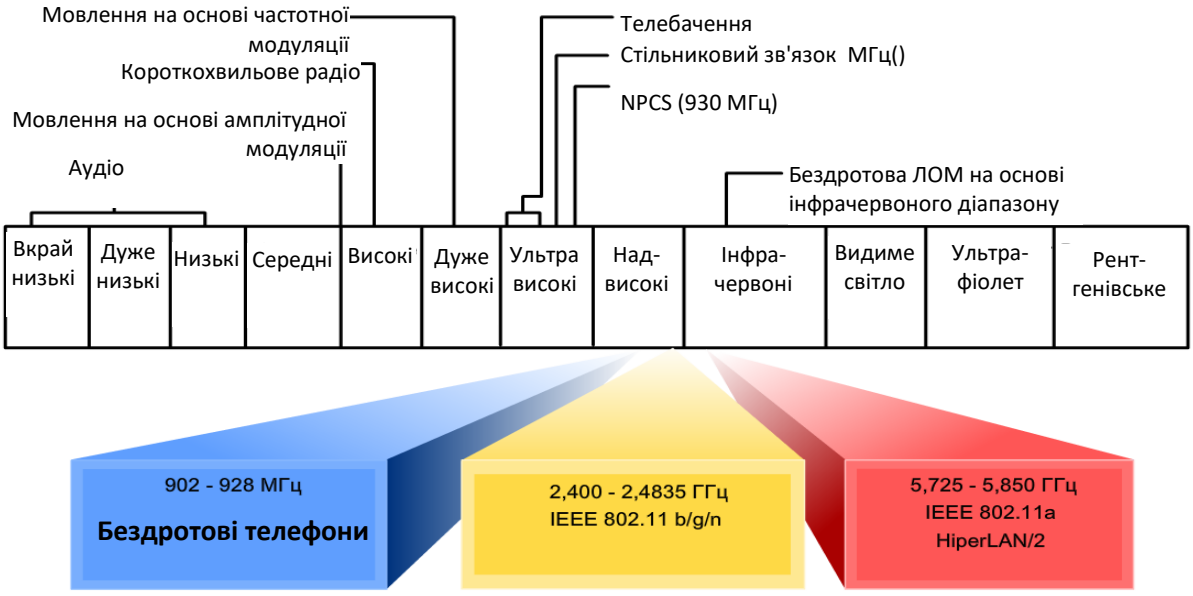


Рисунок 11.3 – Радіочастотний діапазон

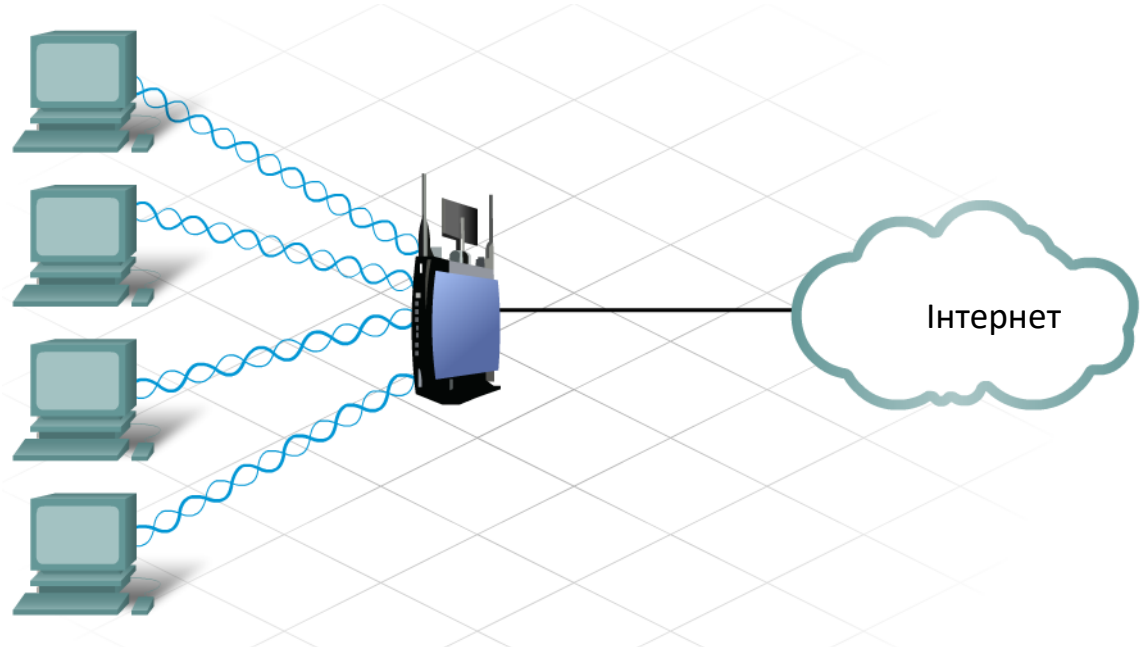
Переваги й обмеження бездротових технологій

У порівнянні із традиційними дротовими мережами бездротова технологія має цілий ряд переваг.

Одним із головних переваг є можливість установлення зв'язку в будь-який час і з будь-якої точки. Широке поширення бездротових мереж у громадських місцях, таких як Інтернет-кафе, дозволяє встановлювати зв'язок з мережею Інтернет, завантажувати інформацію, обмінюватися електронною поштою й файлами.

Бездротова технологія досить проста й недорога в установці. Вартість домашніх і комерційних бездротових пристроїв продовжує знижуватися. При цьому, незважаючи на зниження вартості, швидкість передачі даних збільшується, а функціональність цих пристроїв стає більшою, що забезпечує високу швидкість і надійність зв'язку.

Бездротова технологія розширює кордони мереж без обмежень, властивих кабельним з'єднанням. Вона дозволяє швидко й зручно встановлювати мережеві з'єднання постійно зростаючому числу користувачів.



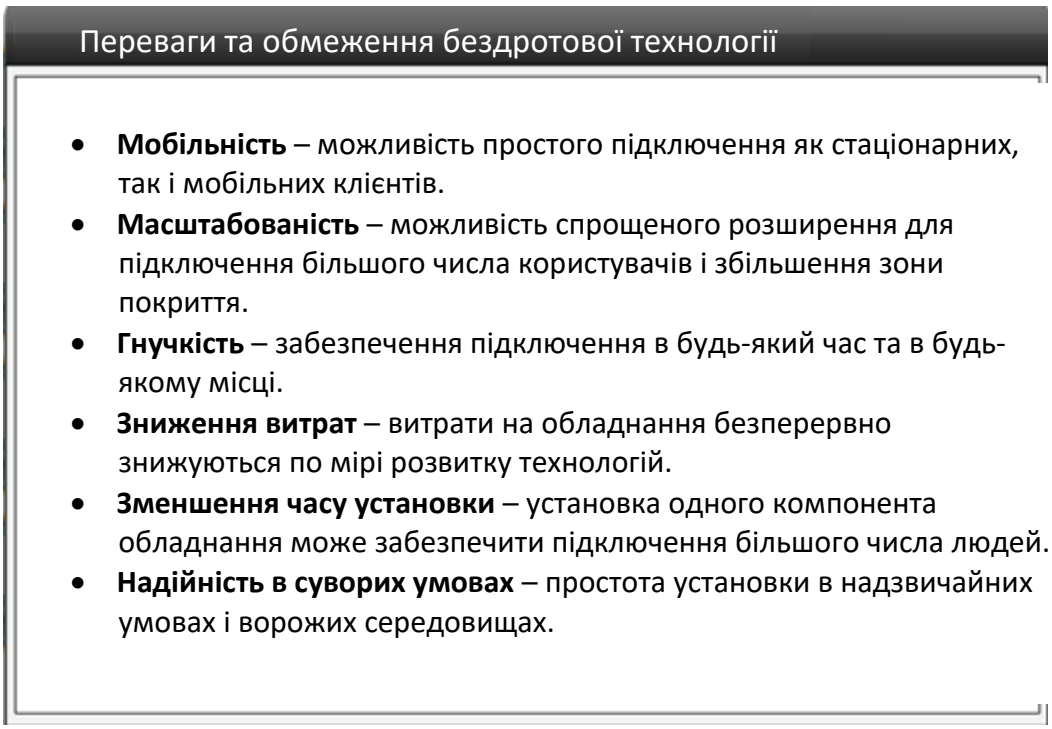


Рисунок 11.4 – Переваги й обмеження бездротових технологій

Незважаючи на гнучкість і значні переваги, для бездротових мереж властиві деякі обмеження й ризики.

По-перше, у технологіях бездротових локальних мереж (WLAN) використовуються неліцензуємі області радіочастотного спектра. Оскільки ці області діапазону не регламентуються, у них використовується безліч різних пристроїв. Це приводить до переповнення областей спектра й перешкодам від різних пристроїв. Крім того, ці частоти використовуються багатьма пристроями, наприклад, мікрохвильовими печами й бездротовими телефонами, які можуть створювати перешкоди роботі бездротових локальних мереж.

Інша проблема бездротового зв'язку – безпека. Доступ у бездротові мережі відкритий. Кожен може одержати доступ до даних, переданих у сеансі широкомовного розсилання. При цьому рівень захисту даних у бездротовій мережі також обмежений. Кожний може перехоплювати потоки даних навіть ненавмисно. Для забезпечення безпеки даних у бездротових

мережах був розроблений ряд методів, таких як шифрування й автентифікація.

Обмеження технології бездротових ЛОМ

- **Інтерференція** – бездротова технологія сприйнятлива до інтерференції, яка викликається іншими пристроями, які генерують електромагнітні хвилі. До них відносяться: бездротові телефони, мікрохвильові мечі, телебачення та інші реалізації бездротової ЛОМ.
- **Безпека мережі та даних –** технологія бездротової ЛОМ призначена для забезпечення доступу до даних, які передаються, але не для їх захисту. Крім того, вона може надати незахищений доступ до дротової мережі.
- **Технологія –** технологія бездротової ЛОМ продовжує розвиватися. В теперішній час технологія бездротової ЛОМ не може забезпечити швидкість і надійність дротових ЛОМ.

Рисунок 11.5 – Обмеження технології мережевих ЛОМ

Типи бездротових технологій

Бездротові мережі діляться на три основні категорії: персональні мережі (Wireless Personal Area), бездротові локальні мережі (Wireless Local Area, WLAN) і глобальні бездротові мережі (Wireless Wide Area, WWAN).

Незважаючи на ці чіткі категорії, важко розмежувати рамки реалізації бездротових технологій. Це пов'язане з тим, що на відміну від дротових мереж для бездротових мереж не потрібні чіткі певні кордони. Діапазон передачі даних у бездротових мережах може мінятися під впливом різних факторів. Бездротові мережі чутливі до зовнішніх джерел перешкод – природних або штучних. Перепади температури й вологості можуть значно впливати на зону покриття бездротових мереж. Перешкоди в середовищі бездротових мереж також впливають на діапазон їхньої дії.

Рисунок 11.6 – Типи бездротових технологій

Типи бездротових мереж і їхньої кордони

WPAN

Бездротові мережі цього типу застосовуються для підключення різних периферійних пристроїв, таких як миші, клавіатури й КПК, до комп'ютера й

мають найменший діапазон дії. Всі ці пристрої підключаються до одного вузла з використанням технологій ІЧ або Bluetooth.

WLAN

Мережі WLAN розширюють кордони локальних дротових мереж (LAN). Мережі WLAN використовують технологію радіочастотного доступу (RF) і відповідають вимогам стандартів IEEE 802.11. У таких мережах користувачі можуть підключатися до дротової мережі за допомогою пристроїв, іменованих точками доступу (Access Point, AP). Точка доступу забезпечує зв'язок між бездротовими вузлами й вузлами в дротовій мережі Ethernet.

WWAN

Мережі WWAN забезпечують зону покриття на дуже великих територіях. Найбільш наочним прикладом мережі WWAN є мережа стільникового зв'язка. У цих мережах використовуються такі технології, як багатостаційний доступ з кодовим поділом каналів (CDMA) або Глобальна система мобільного зв'язку (GSM), і їхня діяльність звичайно регламентується урядовими організаціями.

Таблиця 11.1 – Типи бездротових мереж і їхні кордони

	WPAN	WLAN	WWAN
Стандарти	Bluetooth v2.0+ EDR**	IEEE802.11 a/b/g/n, HiperLAN, HiperLAN2	GSM, GPRS, CDMA
Швидкість	< 3 Мбіт/с	1-540 Мбіт/с	10-384 кбіт/с
Діапазон	Короткі	Середні	Довгі
Додатки	Від рівноправного пристрою до пристрою	Домашні мережі, мережі для малих підприємств і корпоративні мережі	Кишенькові ПК, мобільні телефони, стільниковий доступ

** EDR – Enhanced Data Rate

Швидкість і діапазони постійно розширюються в результаті появи нових технологій.

Стандарти бездротових локальних мереж

Взаємодія бездротових пристроїв регламентується цілим рядом стандартів. У них вказується спектр радіочастотного діапазону, швидкість передачі даних, спосіб передачі даних і інша інформація. Головним розроблювачем технічних стандартів бездротового зв'язку є організація IEEE.

Стандарт IEEE 802.11 регламентує роботу пристроїв у мережах WLAN. З урахуванням різних характеристик бездротового зв'язку в стандарт IEEE 802.11 минулого внесені чотири виправлення. На сьогоднішній день діють наступні виправлення – 802.11a, 802.11b, 802.11g і 802.11n (виправлення 802.11n не ратифікована на момент написання матеріалу). Всі ці технології віднесені до категорії Wi-Fi (Wireless Fidelity).

Організація "Wi-Fi Alliance" відповідає за тестування пристроїв для локальних мереж (LAN) від різних виробників. Логотип Wi-Fi на корпусі пристрою означає, що це устаткування може взаємодіяти з іншими пристроями того ж стандарту.

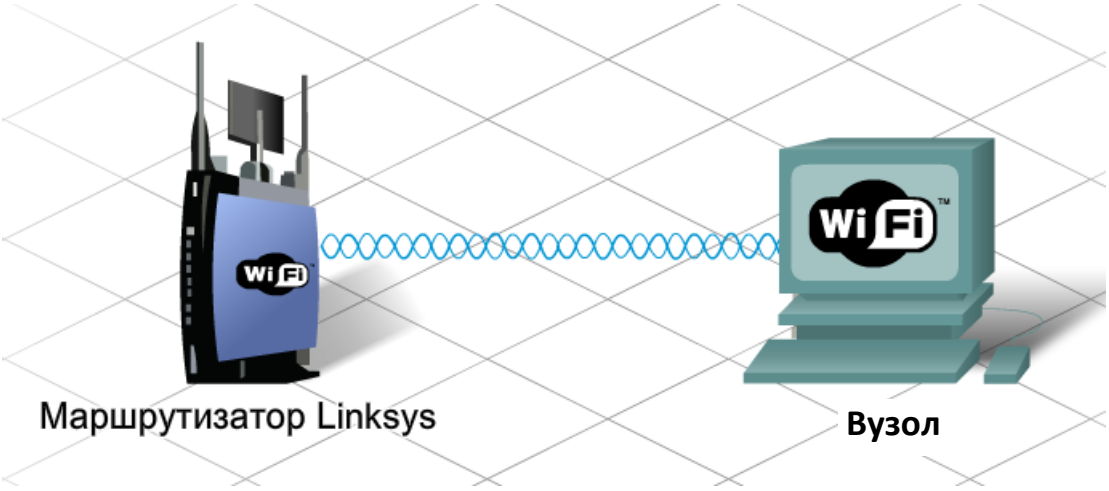


Рисунок 11.8 – Реалізація протоколу 802.11

802.11a:

– використовує смугу частот 5 Ггц;

– не сполучимо зі спектром частот 2,4 Ггц, тобто із пристроями стандарту 802.11 b/g/n;

– діапазон дії приблизно 33% від такого для пристроїв 802.11 b/g;

– відносно дорогою в реалізації в порівнянні з іншими технологіями;

– устаткування, що відповідає вимогам стандарту 802.11a, зустрічається усе рідше.

802.11b:

– перша з технологій 2,4 Ггц;

– максимальна швидкість передачі даних 11 Мбіт/с;

– діапазон дії близько 46 м усередині приміщення й 96 м поза приміщеннями.

802.11g:

– технології 2,4 Ггц;

– максимальна швидкість передачі даних збільшена до 54 Мбіт/с;

– той же діапазон, що й для 802.11b;

– зворотна сумісність із 802.11b.

802.11n:

– новітній стандарт у стадії розробки;

– технології 2,4 Ггц (у проекті стандарту передбачається підтримка смуги 5 Ггц);

– розширено область дії й пропускна здатність пропускна здатність;

– зворотна сумісність із устаткуванням існуючих стандартів 802.11g і 802.11b (у проекті стандарту передбачається підтримка 802.11a).

Таблиця 11.2 – Різниця між версіями протоколу 802.11

Загальні стандарти IEEE WLAN				
Стандарт	Дата випуску	Частота	Швидкість передачі даних (макс.)	Максимальний діапазон*
802.11	Липень 1997 р.	2,4 ГГц	2 Мбіт/с	Не визначено
802.11a	Жовтень 1999 р.	5 ГГц	54 Мбіт/с	50 м
802.11b	Жовтень 1999 р.	2,4 ГГц	11 Мбіт/с	100 м
802.11g	Червень 2003 р.	2,4 ГГц	54 Мбіт/с	100 м
802.11n	Вересень 2009	2,4 ГГц або 5 ГГц	54 Мбіт/с	250 м

*Максимальний діапазон – це значення може широко змінюватися.

Компоненти бездротової локальної мережі WLAN

Після вибору стандарту необхідно переконатися в тім, що всі компоненти в мережі WLAN відповідають його вимогам або, принаймні, сумісні з ним. У мережі WLAN повинне бути кілька обов'язкових компонентів: бездротової клієнт або STA, точка доступу, бездротової міст і антена.

Антени:

– використовуються в точках доступу й у бездротових мостах;

– підвищують потужність вихідного сигналу з бездротового пристрою;

– приймають сигнали з інших пристроїв, наприклад, STA;

– збільшення потужності сигналу з антени називається посиленням;

– більш високий рівень посилення сигнал дозволяє домогтися більшої відстані передачі.

Антени класифікуються по способу випромінювання сигналу. Спрямовані антени концентрують потужність сигналу в одному напрямку.

Всеспрямовані антени випромінюють сигнал у всіх напрямках з рівною інтенсивністю.

Концентруючи сигнал в одному напрямку, спрямовані антени можуть передавати сигнали на більші відстані. Спрямовані антени звичайно використовуються для об'єднання систем, а всеспрямовані антени використовуються в точках доступу.

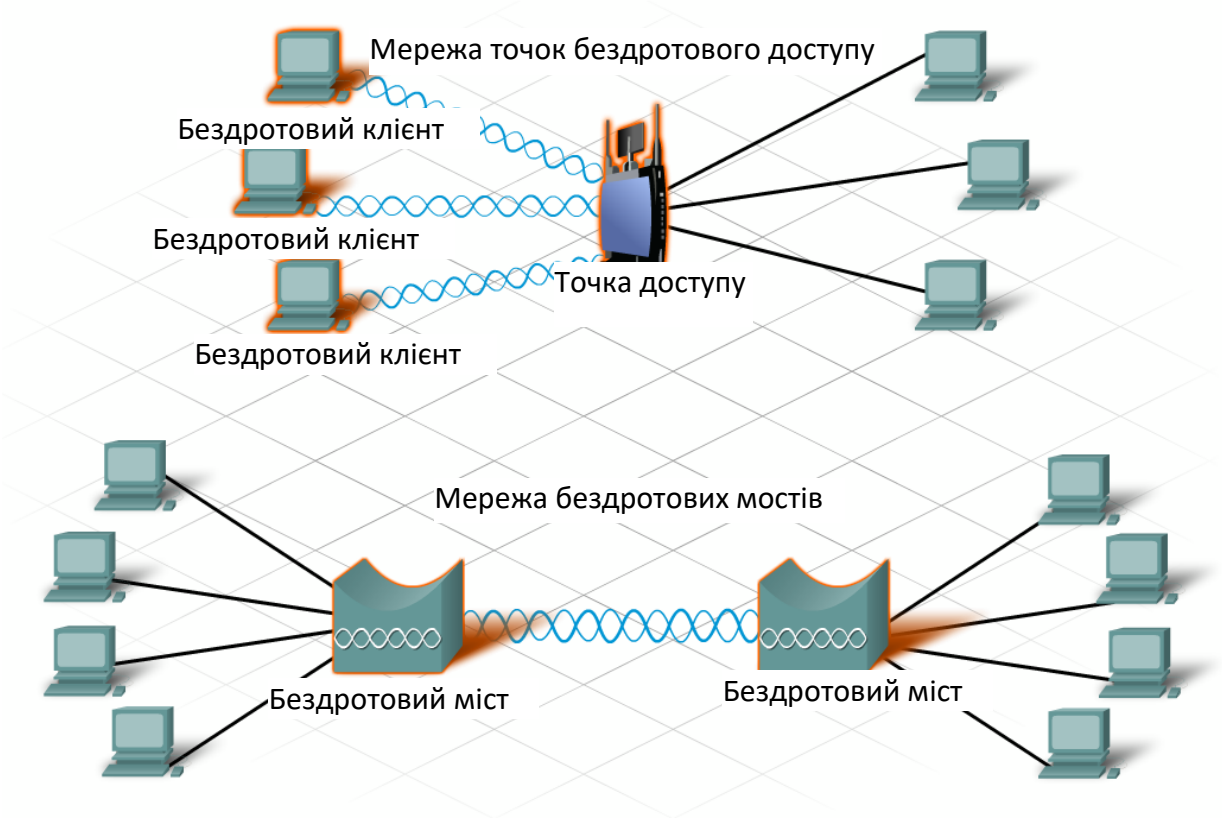


Рисунок 11.10 – Компоненти бездротової локальної мережі WLAN

Рисунок 11.11 – Реалізація точки доступу

Мережі WLAN й імена SSID

При побудові бездротової мережі важливо, щоб бездротові компоненти були підключені до відповідної мережі WLAN. Для цього використовується ідентифікатор набору послуг (SSID).

SSID – це ім'я бездротової мережі, що представляє собою буквено-цифровий рядок, чутливу до регістра, що має довжину до 32 символів. Цей ідентифікатор пересилається в заголовку всіх кадрів, переданих мережею WLAN. Ідентифікатор SSID повідомляє бездротові пристрої, до якої бездротової мережі WLAN вони належать і з якими пристроями вони взаємодіють.

Для забезпечення зв'язку всі бездротові пристрої в мережі WLAN повинні мати загальний ідентифікатор SSID, незалежно від типу установки мережі WLAN.

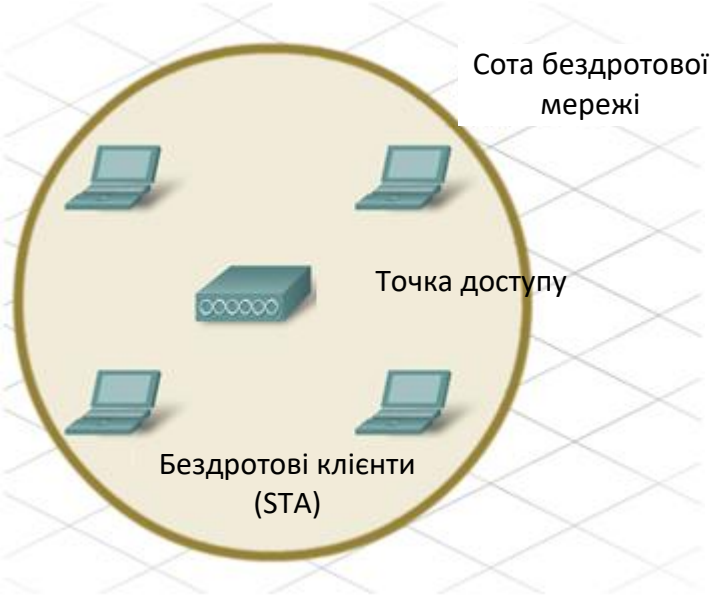


Рисунок 11.12 – Бездротові пристрої в мережі WLAN

Застосовуються два основних види установки мереж WLAN: спеціальний (ad-hoc) і інфраструктурний режими.

Спеціальний режим (Ad-hoc)

Найпростіша бездротова мережа створюється за допомогою об'єднання двох або більше бездротових клієнтів в одноранговій мережі. Бездротова мережа, побудована таким чином, називається спеціалізованою мережею й у ній немає жодної точки доступу. Всі клієнти усередині спеціалізованої мережі рівноправні. Зона покриття цієї мережі називається незалежним базовим набором послуг (IBSS). Проста спеціалізована мережа може використовуватися для обміну файлами й інформацією між пристроями без додаткових витрат і необхідності покупки й налаштування точки доступу.

Інфраструктурний режим

Хоча для малих мереж більше кращими є спеціалізовані конфігурації, у мережах більше високого рівня необхідно використовувати єдиний пристрій, що управляє взаємодією в бездротовій соті. Якщо в мережі є точка доступу, то вона бере ці функції на себе: визначає, які вузли й у який час можуть встановлювати зв'язок. Такий режим називається інфраструктурним режимом бездротового зв'язку; найчастіше вони використовуються в

домашніх умовах і в умовах бізнесу. При такій формі організації бездротових локальних мереж WLAN окремі STA-пристрою не можуть взаємодіяти між собою прямо. Щоб ці пристрої могли взаємодіяти між собою, їм необхідний дозвіл від точки доступу. Точка доступу управляє всіма взаємодіями й забезпечує рівний доступ у середовище всім STA-пристроям. Зона покриття однієї точки доступу називається базовим набором послуг (BSS) або сотої.

Базовий набір послуг (BSS) – це найменший будівельний блок мережі WLAN. Точка доступу має обмежену зону покриття. Для розширення зони покриття можна об'єднати кілька базових наборів послуг через систему розподілу (DS). У такий спосіб створюється розширений набір послуг (ESS). В ESS використовується кілька точок доступу. Кожна точка доступу являє собою окремий базовий набір послуг.

Щоб забезпечити обмін даними між стільниками без втрат сигналів, базові набори послуг повинні перетинатися між собою приблизно на 10%. Це дозволяє клієнтові підключатися до другої точки доступу перед тим, як відключитися від першої точки доступу.

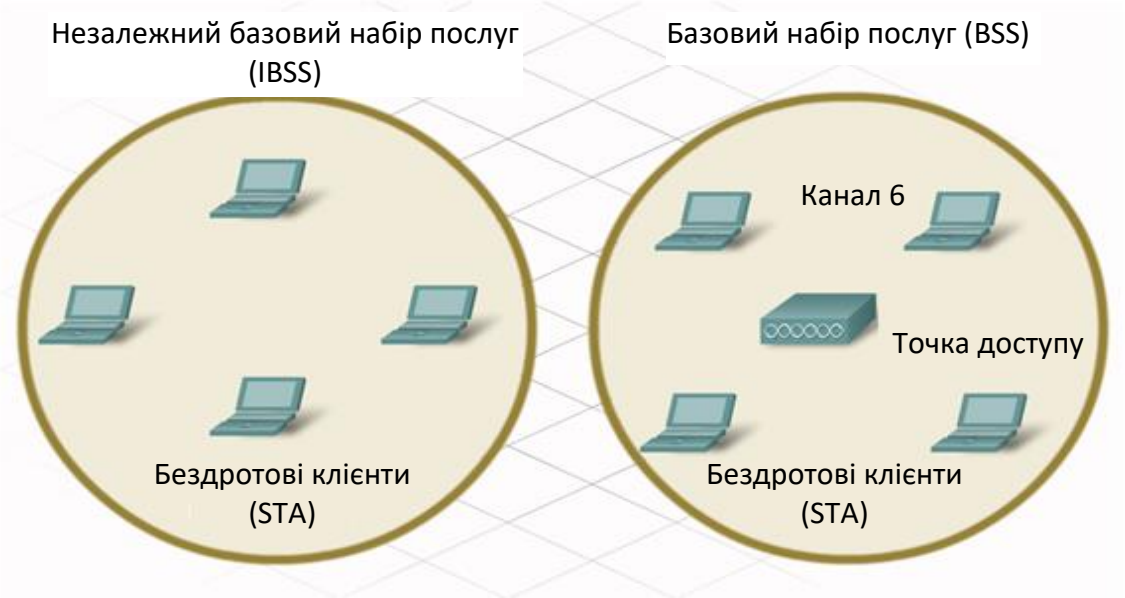


Рисунок 11.13 – Базовий набір послуг (BSS)

У більшості домашніх і комерційних мереж є тільки один базовий набір послуг. Проте, при необхідності збільшення зони покриття й числа вузлів може знадобитися створити розширений набір послуг.

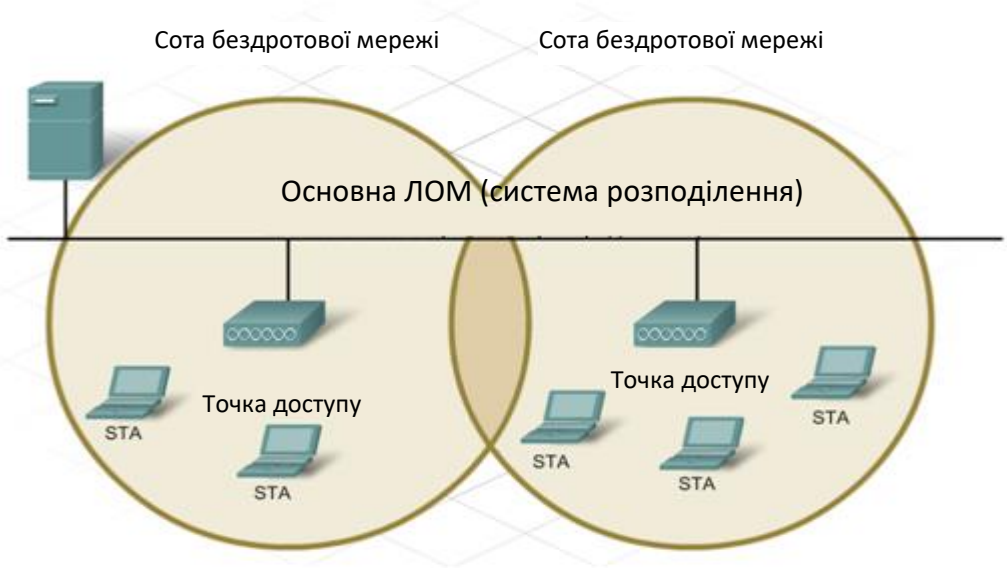


Рисунок 11.14 – Обмін даними між стільниками

Бездротові канали

Незалежно від того, як взаємодіють бездротові клієнти – усередині IBSS, BSS або ESS, – необхідно управляти зв'язком між відправником і одержувачем. Одним із засобів керування зв'язком є канали.

Канали створюються за допомогою розподілу доступного радіочастотного спектра. Кожний канал може використовуватися в якості несучої для іншого сеансу зв'язку. Це можна зрівняти з передачею декількох телевізійних каналів по одному тракті. Кілька точок доступу можуть працювати в безпосередній близькості одна до іншої, якщо вони використовують різні канали зв'язку.

На жаль, частоти, обрані для деяких каналів, можуть перетинатися з каналами, зайнятими іншими пристроями. Різні сеанси зв'язку повинні використовуватися на непересічних каналах. Кількість і розподіл каналів залежить від регіону й вибору технологій. Канал для окремого сеансу зв'язку

можна налаштовувати вручну або автоматично, з огляду на його завантаженість і пропускну здатність.

Звичайно для кожного сеансу бездротового зв'язку виділяється окремий канал. У деяких новітніх технологіях передбачене об'єднання каналів у єдиний канал підвищеної пропускної здатності з більше високою швидкістю передачі даних.

Відсутність чітких границь у мережі WLAN не дозволяє виявляти конфлікти в процесі передачі даних. Тому необхідно використовувати такий метод доступу, який би гарантував відсутність конфліктів.

Для цього в бездротових технологіях застосовується множинний доступ з контролем несучої й запобіганням конфліктів (CSMA/CA). CSMA/CA резервує канал для окремого сеансу зв'язку. Якщо канал зарезервований, ніякий інший пристрій не зможе передавати по ньому дані, що дозволить уникнути можливих конфліктів.

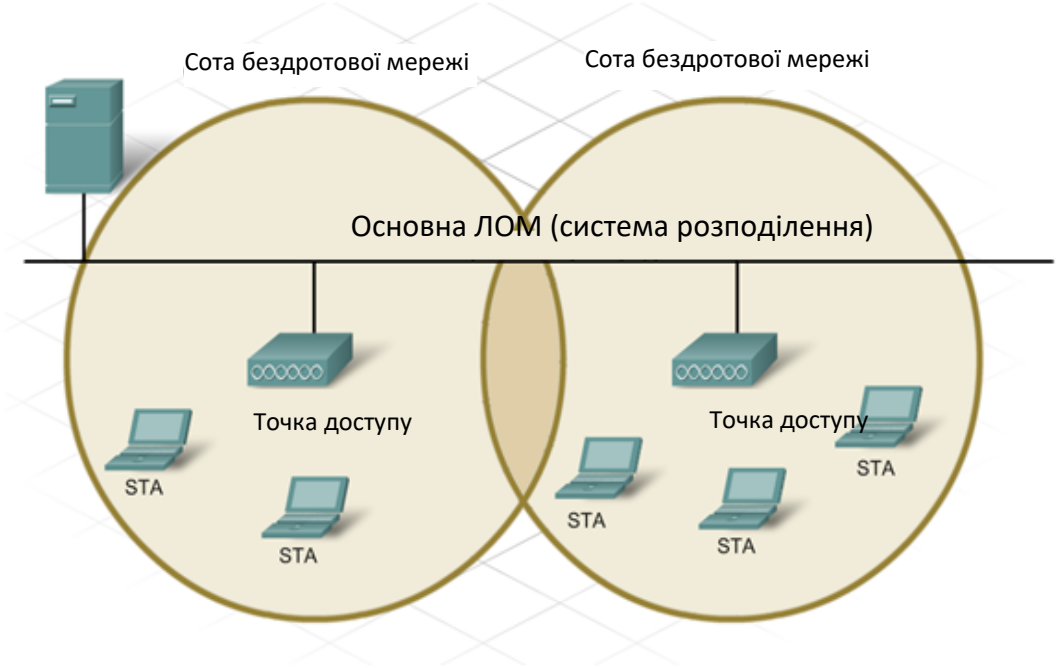


Рисунок 11.15 – Бездротові канали

Як працює процес резервування? Якщо пристрою потрібен спеціальний канал зв'язку в базовому наборі послуг, він звертається до точки

доступу за дозволом. Це називається протокол готовності до передачі (RTS). Якщо канал вільний, точка доступу відправить пристрою повідомлення про готовність до прийому (Clear to Send, CTS), що показує, пристрою дозволена передача по даному каналу. Повідомлення CTS передається всім пристроям у базовому наборі послуг (BSS). Тому всі пристрої в базовому наборі послуг знають, що запитуваний канал у цей момент зайнятий.

Після завершення сеансу зв'язку пристрій, що запросив канал, відправляє в точку доступу ще одне повідомлення, іменоване (ACK) (підтвердження). Повідомлення ACK повідомляє точку доступу, що канал може бути звільнений. Це повідомлення також розсилається всім пристроям у мережі WLAN. Всі пристрої в базовому наборі послуг одержують повідомлення ACK і в такий спосіб сповіщаються про те, що даний канал знову вільний.

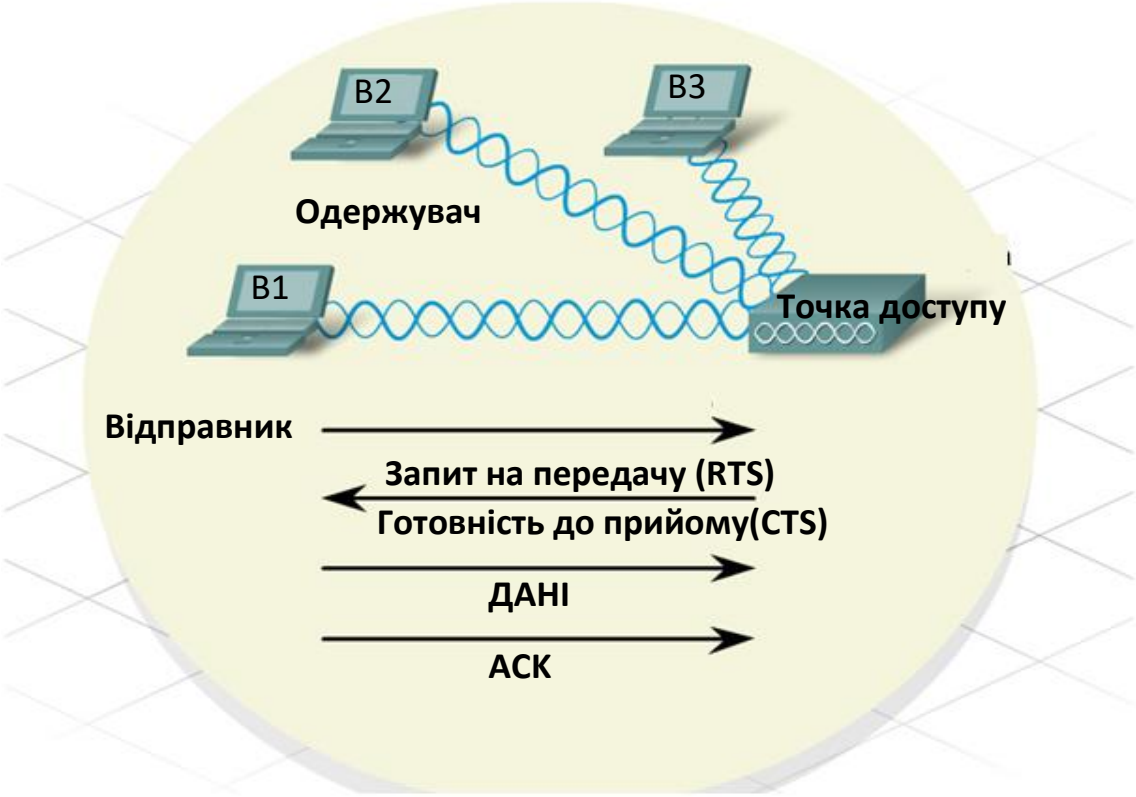


Рисунок 11.16 – Процес резервування

Планування бездротової мережі

При розгортанні рішення бездротової мережі важливо провести планування до початку процесу установки. Це передбачає виконання наступних операцій:

– визначити стандарт бездротового зв'язку;

– визначити найбільш ефективну конфігурацію пристроїв;

– скласти план установки й забезпечення безпеки;

– розробити стратегію резервного копіювання й відновлення мікропрограма бездротових пристроїв.

Стандарт бездротового зв'язку

При виборі стандарту мережі WLAN необхідно розглянути трохи факторів. До числа найбільш загальних факторів ставляться наступні: вимоги до пропускної здатності, зони покриття, що існують реалізації й вартість. Ця інформація збирається в ході вивчення вимог кінцевого користувача.

Кращий спосіб вивчення вимог кінцевого користувача – задавати питання:

– Яка пропускна здатність фактично потрібно додаткам, що працюють у мережі?

– Скільки користувачів будуть мати доступ у мережу WLAN?

– Яка необхідна зона покриття?

– Яка структура існуючої мережі?

– Який бюджет цієї мережі?

Пропускна здатність у базовому наборі послуг повинна бути достатньою для спільного використання всіма користувачами даного BSS. Навіть якщо додаткам не потрібно високошвидкісного підключення, воно може знадобитися у випадку одночасного підключення великої кількості користувачів.

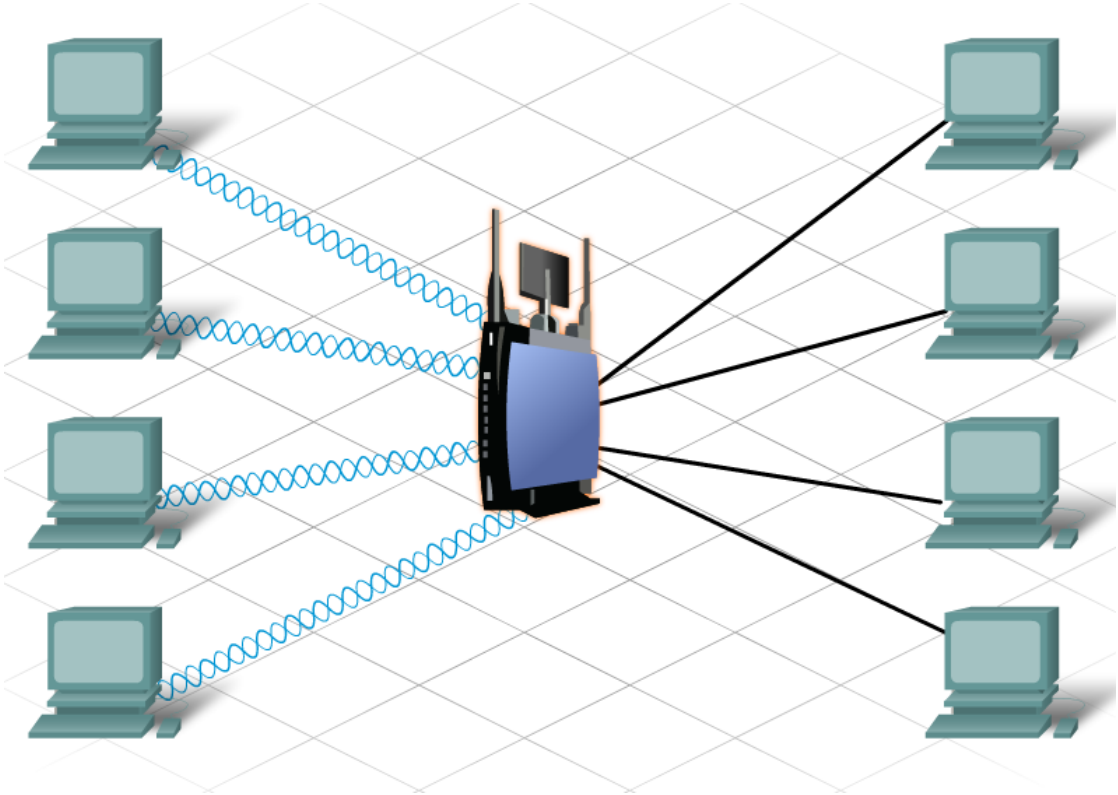


Рисунок 11.16 – Планування бездротової мережі

Для різних стандартів задані різні зони покриття. Сигнал частотою 2,4 Ггц, застосовуваний у технологіях 802.11 b/g/n, передається на більшу відстань, ніж сигнал частотою 5 Ггц, застосовуваний у технологіях 802.11a. Тим самим, 802.11 b/g/n забезпечує більший базовий набір послуг (BSS). Це дозволяє використовувати менше одиниць устаткування й знизити вартість реалізації.

Уже існуюча мережа також впливає на нову реалізацію стандартів WLAN. Наприклад, стандарт 802.11n назад сполучимо зі стандартами 802.11g і 802.11b, але не з 802.11a. Якщо інфраструктура й устаткування існуючої мережі підтримують стандарт 802.11a, те в нових реалізаціях також повинен підтримуватися той же стандарт.

Необхідно також ураховувати вартість. При аналізі витрат необхідно враховувати сукупну вартість володіння, у яку входить вартість покупки устаткування, витрати на установку й технічну підтримку. В умовах підприємств середнього й великого бізнесу сукупна вартість володіння в

більше ступені визначає вибір стандарту WLAN, ніж в умовах домашніх офісів або малих підприємств. Це пов'язане з тим, що в середніх і великих підприємствах потрібно більше одиниць устаткування, необхідні плани установки й додаткові витрати.

Установка бездротових пристроїв

В умовах домашніх офісів і малих підприємств установка звичайно має на увазі обмежене число одиниць устаткування, яке можна безперешкодно переносити для забезпечення оптимальної зони покриття й пропускної здатності.

В умовах великих підприємств перенесення устаткування сполучене з додатковими витратами й проблемами забезпечення необхідної зони покриття. Для забезпечення найкращої зони покриття з мінімумом витрат необхідно вибрати оптимальну кількість і місце розташування точок доступу.

Для цього звичайно проводиться виїзд на об'єкт. Співробітник, відповідальний за обстеження об'єкта, повинен мати необхідні знання в області проектування мереж WLAN і оснащений сучасним устаткуванням для виміру потужності сигналів і виявлення перешкод. При значних масштабах мережі WLAN цей процес може бути досить дорогим. При малих масштабах мережі досить простого обстеження об'єкта за допомогою бездротових STA-пристроїв і утиліт, що поставляються в комплекті з більшістю інтерфейсних плат бездротового зв'язку.

При виборі місця для установки устаткування мережі WLAN у кожному разі необхідно виявити всі відомі джерела інтерференції, як то: високовольтні кабелі, електродвигуни й інші бездротові пристрої.

Установка й забезпечення точки доступу

Після того як обрана сама оптимальна технологія й визначена місце розміщення точки доступу, виконаєте установку пристрою WLAN і налаштування точки доступу, використовуючи засобу забезпечення безпеки. Заходу щодо забезпечення безпеки повинні підбиратися й реалізовуватися до

того, як точка доступу буде підключена до мережі або до Інтернет-провайдеру.

Серед основних заходів щодо забезпечення безпеки можна відзначити наступні:

– Змінити значення SSID, задані за замовчуванням, імена користувачів і паролі.

– Відключити розсилання SSID.

– Налаштувати фільтрацію MAC-адрес.

Серед додаткових заходів забезпечення безпеки варто розглянути наступні:

– налаштування шифрування за допомогою WEP або WPA;

– налаштування автентифікації;

– налаштування фільтрації трафіку.

Пам’ятайте , що жоден із заходів щодо забезпечення безпеки окремо не гарантує повного захисту вашої бездротової мережі. Сполучення різних методів дозволить підвищити надійність і ефективність вашого плану забезпечення безпеки.

При виконанні налаштування клієнтів необхідно переконатися, що їх SSID збігаються з SSID у точці доступу. Крім того, повинні використовуватися загальні ключі шифрування й ключі автентифікації.

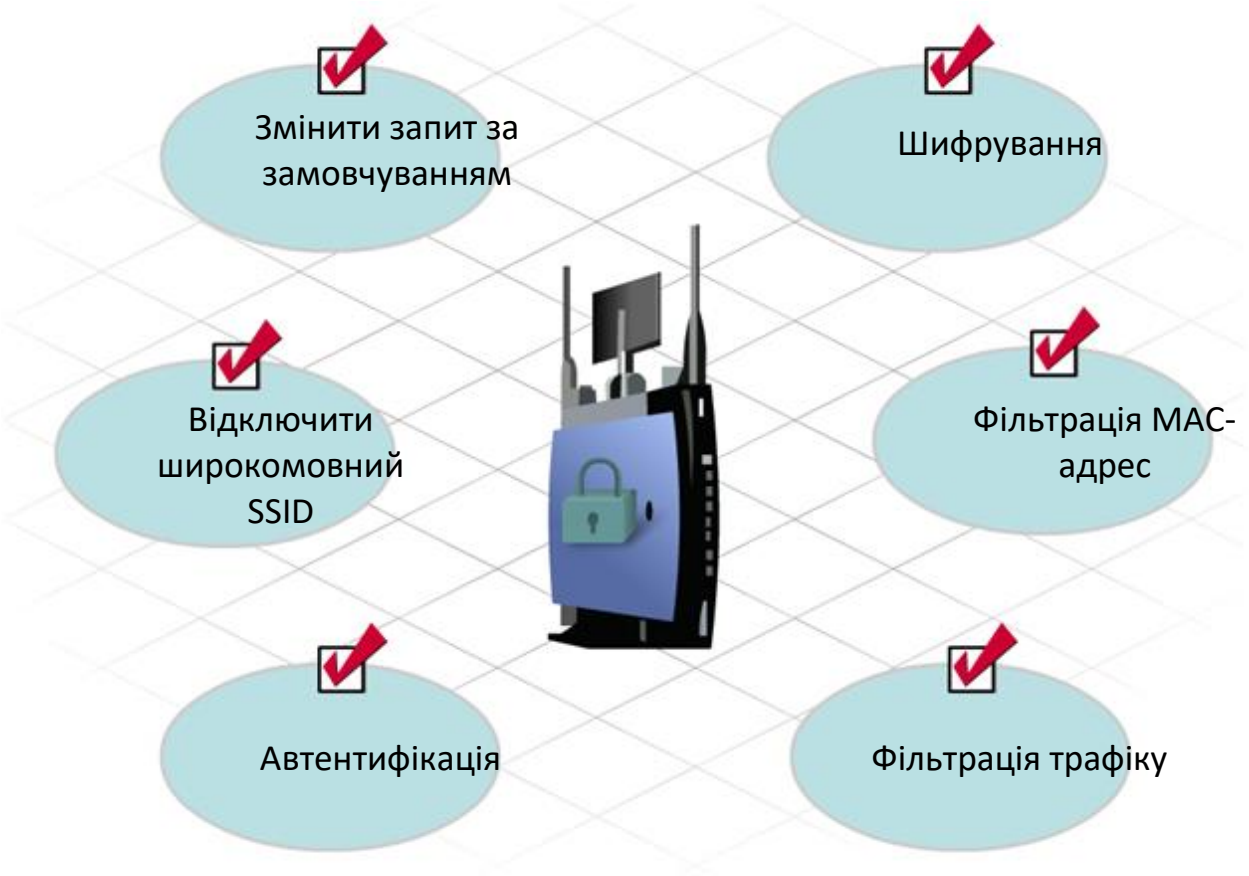


Рисунок 11.17 – Основні заходи щодо забезпечення безпеки точки доступу

Резервне копіювання файлів конфігурації

Після того, як налаштування бездротової мережі виконані й забезпечено рух трафіку даних, варто виконати повне резервне копіювання конфігурації всіх бездротових пристроїв. Це особливо важливо на випадок значного переналаштування конфігурації.

У більшості інтегрованих маршрутизаторів для домашніх офісів і малих підприємств досить вибрати пункт "Backup Configurations" (резервне копіювання конфігурацій) з відповідні меню й указати місце розташування для збереження резервного файлу. Вбудований маршрутизатор пропонує ім'я файлу конфігурації, задане за замовчуванням. Це ім'я файлу можна змінити.

Процес відновлення з резервної копії так само простий. Виберіть пункт "Restore Configurations". Потім перейдіть до місця зберігання

резервного файлу конфігурації й виберіть його. Після вибору файлу натисніть на кнопку "Start to Restore", щоб завантажити файл конфігурації.

Іноді може знадобитися відновити заводські налаштування. Для цього або виберіть пункт "Restore Factory Defaults" у відповідному меню або натисніть і втримуйте натиснутої кнопку RESET протягом 30 секунд. Останній метод особливо корисний, якщо не вдалося підключити точку доступу до інтегрованого маршрутизатора через мережу, але фізичний доступ до цього пристрою є.

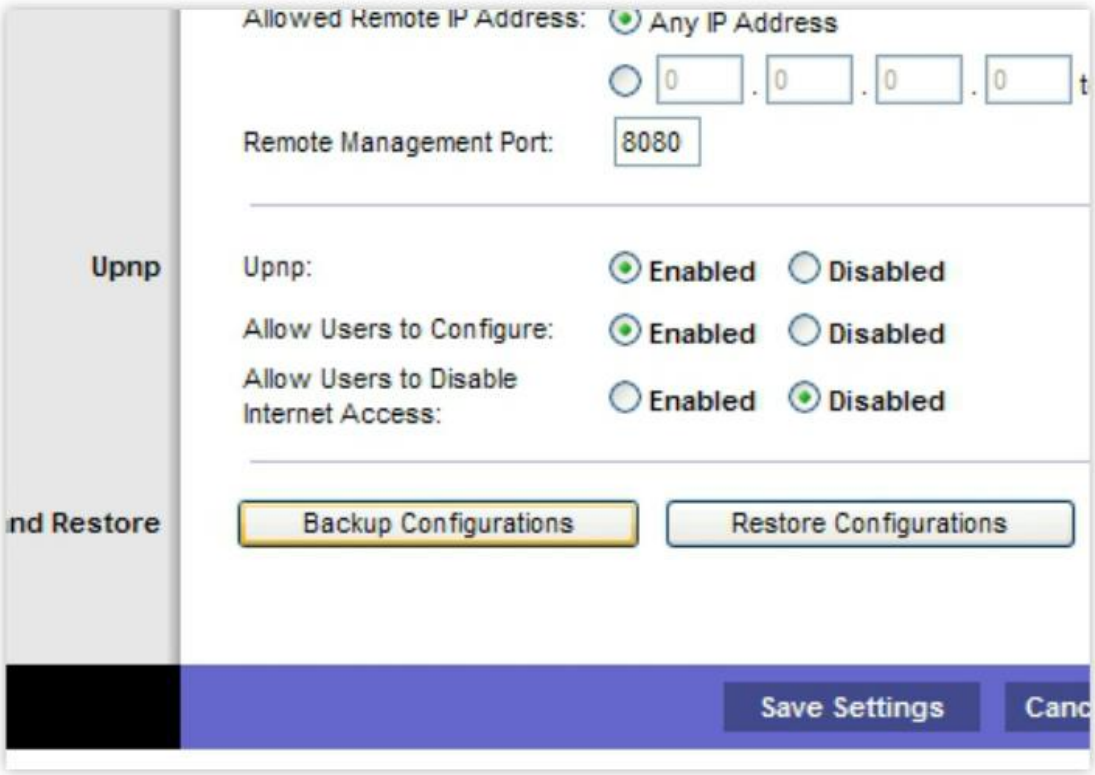


Рисунок 11.18 – Резервне копіювання файлів конфігурації

РОЗДІЛ 12. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ

Чому атакують бездротові мережі

Одним з головних переваг бездротових мереж є зручність у підключенні пристроїв. Але зворотнім боком зручності підключення й можливості передачі інформації без проводів є уразливість вашої мережі для перехоплення інформації й атак з боку зловмисників.

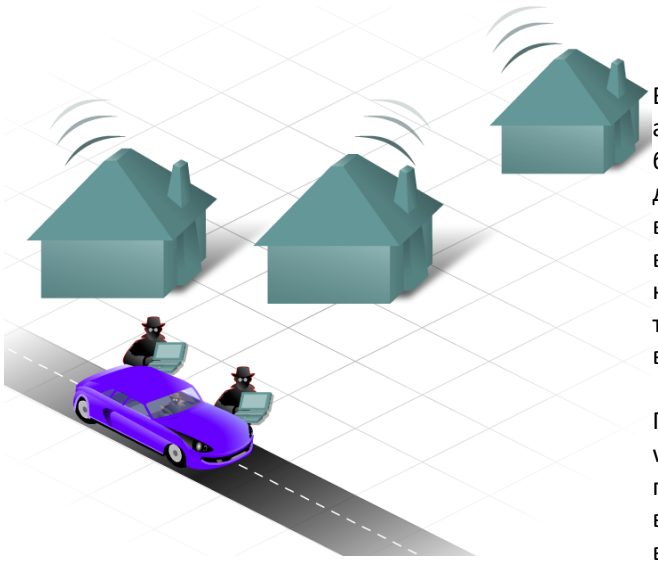
Зломщикові не потрібно фізичного підключення до вашого комп'ютера або до будь-якого іншого пристрою для одержання доступу у вашу мережу. Зловмисник може налаштуватися на сигнали вашої бездротової мережі точно так само як на хвилю радіостанції.

Зломщик може одержати доступ у вашу мережу з будь-якої точки в межах дії бездротового зв'язку. Одержавши доступ до вашої мережі, зловмисники зможуть безкоштовно скористатися вашими Інтернет-сервісами, а також одержати доступ до комп'ютерів у мережі й ушкодити файли, або украсти персональну або конфіденційну інформацію.

Для захисту від цих уразливостей бездротового зв'язку необхідні спеціальні функції забезпечення безпеки й методи захисту бездротової локальної мережі (WLAN) від зовнішніх атак. Для цього досить виконати кілька нескладних операцій у процесі вихідному налаштуванню бездротового пристрою, а також налаштувати додаткові параметри забезпечення безпеки.

Один з найпростіших способів доступу в бездротову мережу – використовувати ім'я мережі або SSID.

Всі комп'ютери, підключені до бездротової мережі, повинні використовувати її SSID. За замовчуванням, бездротові маршрутизатори й точки доступу розсилають ідентифікатори SSID всім комп'ютерам у межах дії бездротової мережі. Якщо функція розсилання SSID активована, то будь-який бездротової клієнт зможе виявити мережу й підключитися до неї, якщо не налаштовані інші функції забезпечення безпеки.



Вардрайвинг/walking/chalking

Вардрайвинг – це процес переміщення на автомобілі по деякій області з одночасним пошуком бездротових ЛОМ. Після виявлення точки доступу до бездротової ЛОМ вона реєструється і відкривається для загального доступу. Ціль вардрайвингу – привернення уваги до незахищеності більшості бездротових мереж, а також демонстрація широкого розповсюдження і використання технології бездротової ЛОМ.

Процес, подібний вардрайвингу, відомий як war-walking (бойова хода), в якій деяка людина переміщається по деякій області пішки з ціллю виявлення точки бездротового доступу. Після виявлення точки доступу в місці виявлення робиться помітка крейдою, щоб відзначити стан бездротового з'єднання.

Рисунок 12.1 – Вардрайвинг

Функцію розсилання SSID можна відключати. Якщо вона відключена, то відомості про доступність мережі вже не є загальнодоступними. Будь-який комп'ютер, що підключається в мережу, повинен використовувати її SSID.

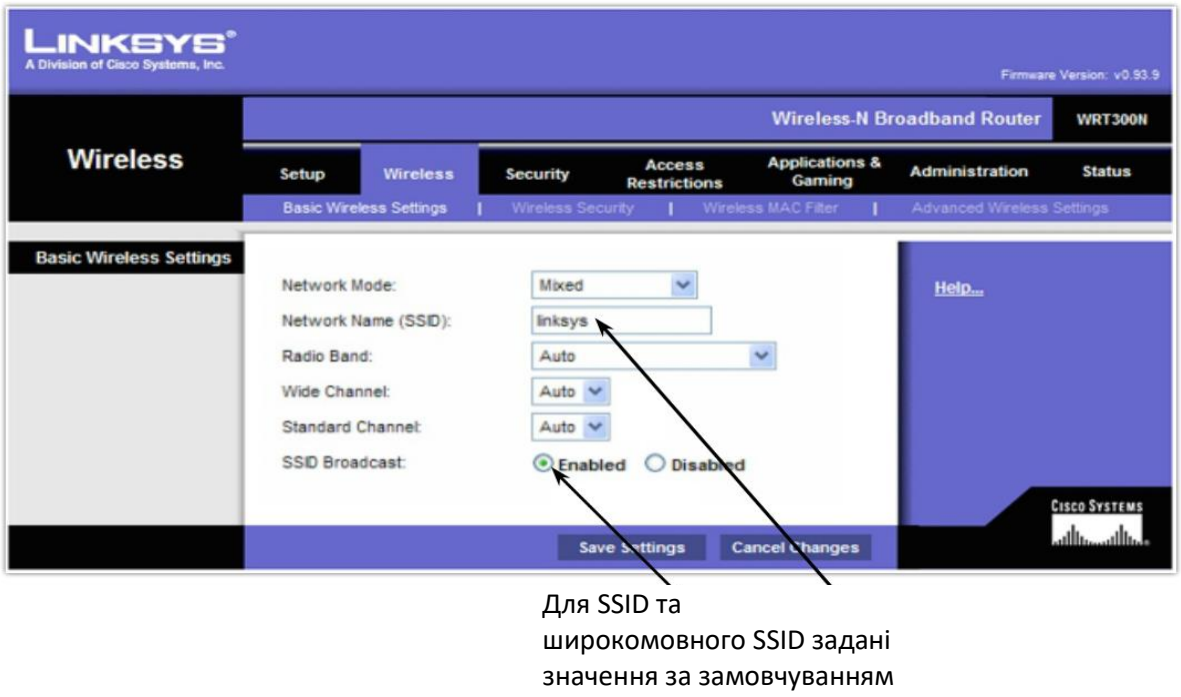


Рисунок 12.2 – Функція розсилання SSID

Як додаткова міра захисту рекомендується змінити налаштування, задані за замовчуванням. Бездротові пристрої поставляються з попередньо налаштованими SSID, паролями й IP-адресами. Використовуючи налаштування за замовчуванням, зловмисник зможе легко ідентифікувати мережа й одержати доступ.

Навіть якщо відключено розсилання SSID, існує ймовірність проникнення в мережу, якщо зловмисникові став відомий SSID, заданий за замовчуванням. Якщо не змінити інші налаштування за замовчуванням, а саме паролі й IP-адреси, то зломщики можуть проникнути в точку доступу й внести зміни в її конфігурацію. Налаштування, задані за замовчуванням, повинні бути змінені на більше безпечні й унікальні.

Ці зміни самі по собі ще не гарантують безпеки вашої мережі. Наприклад, SSID передаються відкритим текстом. Але сьогодні є пристрої для перехоплення бездротових сигналів і читання повідомлень, складених відкритим текстом. Навіть якщо функція розсилання SSID відключена й значення за замовчуванням змінені, зломщики можуть довідатися ім'я бездротової мережі за допомогою таких пристроїв. Використовуючи цю інформацію, вони зможуть підключитися до мережі. Для забезпечення безпеки бездротової локальної мережі (WLAN) варто використовувати комбінацію з декількох методів захисту.

Рисунок 12.3 – Незахищена бездротова мережа

Обмеження доступу в бездротові мережі

Один зі способів обмеження доступу в бездротову мережу – визначити пристроям різний рівень привілеїв доступу в мережу. Для цього застосовується фільтрація MAC-адрес.

Фільтрація MAC-адрес дозволяє задати перелік пристроїв, що мають дозвіл на з'єднання з бездротовою мережею, за допомогою їх MAC-адрес. При кожній спробі бездротового клієнта встановити з'єднання або асоціюватися із точкою доступу він повинен передати свій MAC-адресу. Якщо включено функцію фільтрації по MAC-адресах, те бездротовий маршрутизатор або точка доступу виконає пошук MAC-адреси цього пристрою по своєму попередньо заданому списку. Дозвіл на з'єднання одержать тільки ті пристрої, чиї MAC-адреси були заздалегідь прописані в базі даних маршрутизатора.

Якщо MAC-адресу не знайдена в базі даних, пристрою буде відмовлено у встановленні з'єднання або в доступі в бездротову мережу.

Такий тип забезпечення безпеки має деякі недоліки. Наприклад, він припускає, що MAC-адреси всіх пристроїв, яким повинен бути наданий доступ у мережу, включені в базу даних до того, як буде виконана спроба з'єднання. Пристрій, не розпізнаний по базі даних, не зможе виконати з'єднання. При цьому зломщик може створити клон MAC-адреси пристрою, що має доступ у мережу.

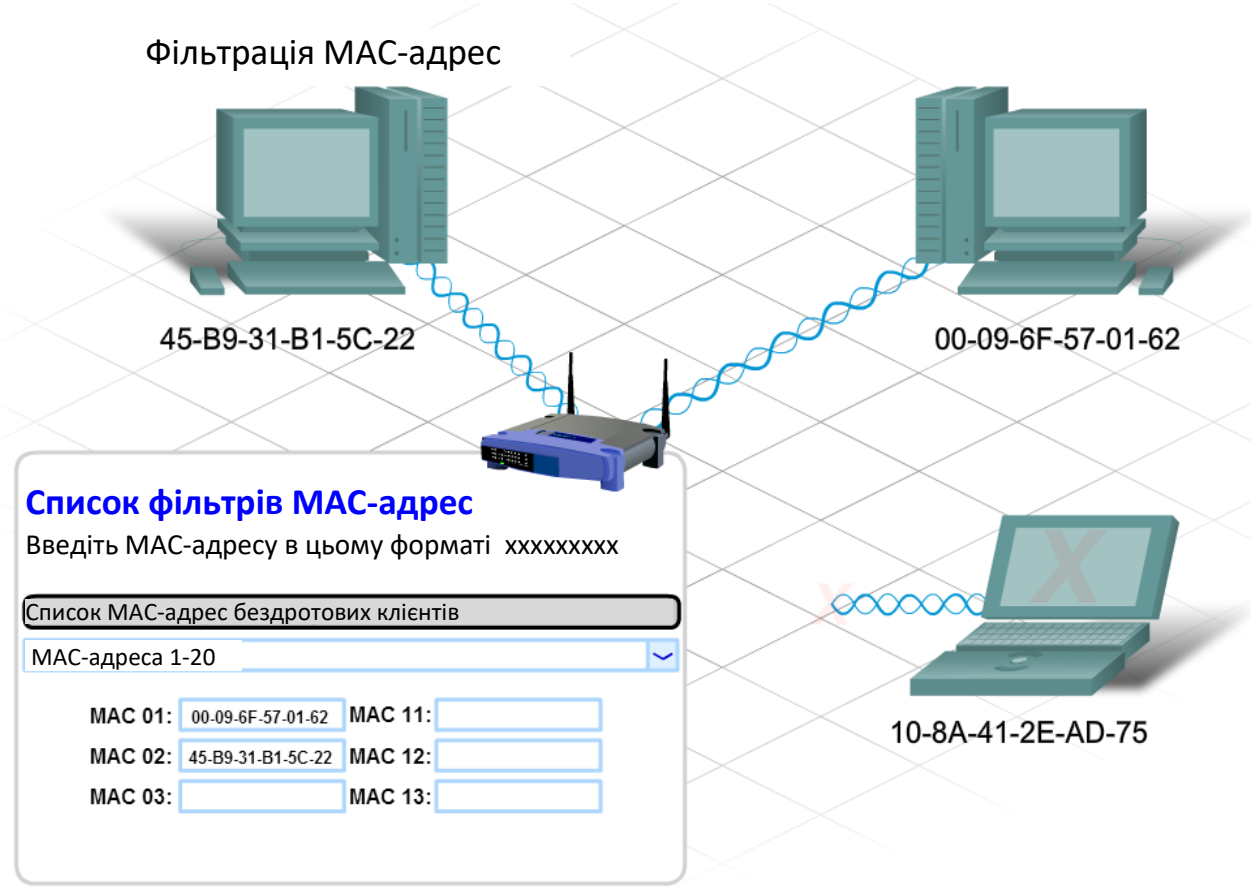


Рисунок 12.4 – Фільтрація MAC-адрес

Інший спосіб адміністрування доступу – автентифікація. Автентифікація – це надання дозволу на вхід у мережу за результатами перевірки дійсності набору облікових даних. Її ціль – з'ясувати, чи є пристрій, що намагається встановити з'єднання, довіреним пристроєм.

Найпоширеніша автентифікація по ім'ю користувача й паролю. У бездротовому середовищі автентифікація дозволяє виконати перевірку дійсності підключеного вузла, але процес перевірки виконується трохи по-іншому. Якщо включено функцію автентифікації, то вона повинна бути виконана до того, як клієнтові буде наданий дозвіл на підключення до мережі WLAN. Існує три групи методів автентифікації бездротових мереж:

– обрив автентифікації;

– PSK;

– EAP.

Відкрита автентифікація

За замовчуванням для бездротових пристроїв автентифікація не потрібна. Всім пристроям дозволено встановлювати з'єднання незалежно від їхнього типу й приналежності. Це називається відкритої автентифікацією. Відкрита автентифікація повинна використовуватися тільки в загальнодоступних бездротових мережах, наприклад, у школах і Інтернет-кафе (ресторанах). Вона може використовуватися в мережах, де автентифікація буде виконуватися іншими засобами після підключення до мережі.

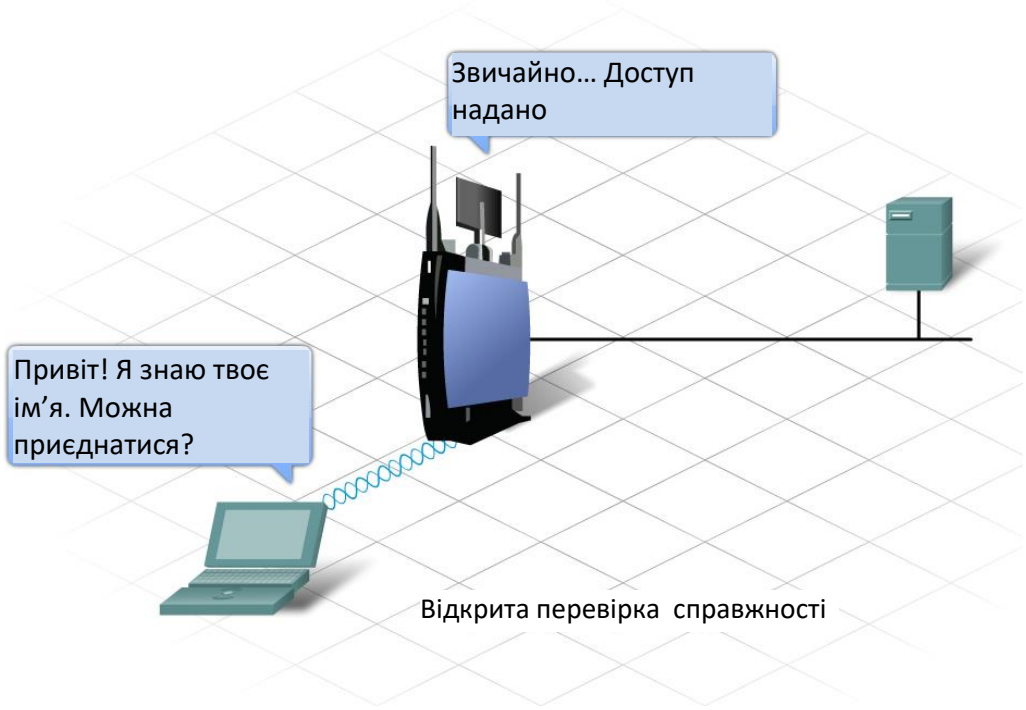


Рисунок 12.5 – Відкрита автентифікація

Режим попередніх ключів (Pre-shared keys, PSK)

При використанні режиму PSK точка доступу й клієнт повинні використовувати загальний ключ або кодове слово. Точка доступу відправляє клієнтові випадковий рядок байтів. Клієнт приймає цей рядок, шифрує її, використовуючи ключ, і відправляє її назад у точку доступу. Точка доступу одержує зашифрований рядок і для її розшифровки використовує свій ключ.

Якщо розшифрований рядок, прийнятий від клієнта, збігається з вихідним рядком, відправленої клієнтові, то клієнтові дається дозвіл установити з'єднання.

PSK виконує однобічну автентифікацію, тобто, точка доступу перевіряє дійсність вузла, що підключається. PSK не має на увазі перевірки вузлом дійсності точки доступу, а також не перевіряє дійсності користувача, що підключається до вузла.

Розширюваний протокол перевірки дійсності (Extensible Authentication Protocol, EAP)

EAP забезпечує взаємну або двосторонню автентифікацію, а також автентифікацію користувача. Якщо на стороні клієнта встановлене програмне забезпечення EAP, клієнт взаємодіє із внутрішнім сервером автентифікації, таким як сервер дистанційної автентифікації мобільного користувача мережі, що комутується, що (RADIUS). Цей обслуговуючий сервер працює незалежно від точки доступу й веде базу даних користувачів, що мають дозвіл на доступ у мережу. При застосуванні EAP користувач, а не тільки вузол, повинен пред'явити ім'я й пароль, які потім перевіряються по базі даних сервера RADIUS. Якщо пред'явлені облікові дані є припустимими, користувач розглядається як минулу перевірку дійсності.

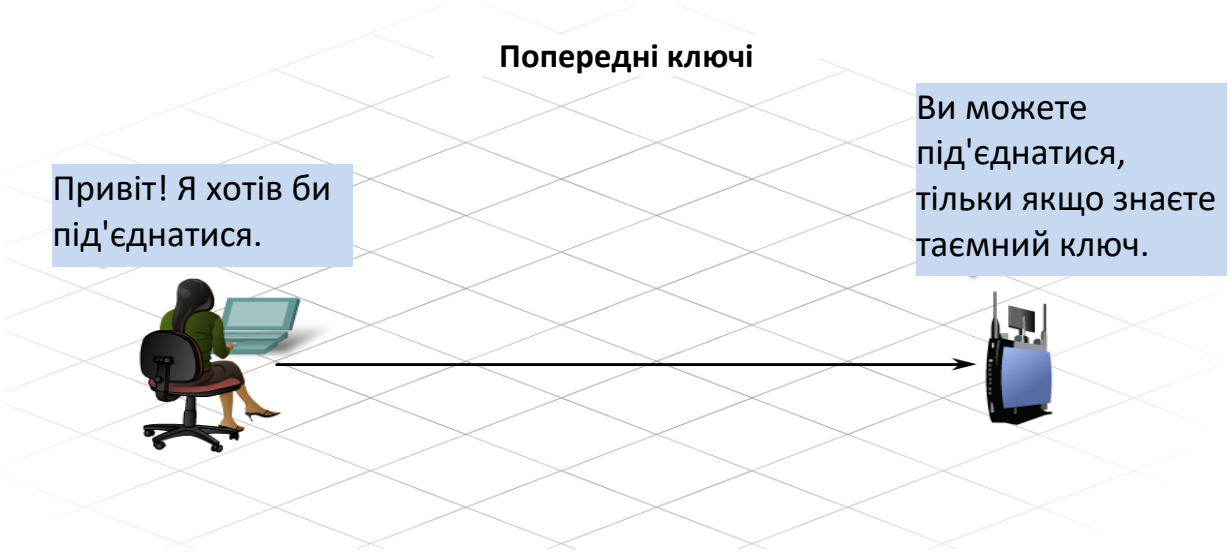


Рисунок 12.6 – Протокол PSK

Рисунок 12.7 – Протокол EAP

Якщо функція автентифікації включена, то незалежно від застосовуваного методу клієнт повинен успішно пройти автентифікацію до того, як йому буде наданий дозвіл на вхід у точку доступу. Якщо включені функції автентифікації й фільтрації MAC-адрес, то в першу чергу виконується автентифікація.

Якщо автентифікація пройшла успішно, точка доступу потім перевіряє MAC-адресу по таблиці MAC-адрес. Після виконання перевірки точка доступу додає MAC-адресу цього вузла у свою таблицю вузлів. Таким чином, передбачається, що клієнт асоційований із точкою доступу й має дозвіл на підключення до мережі.

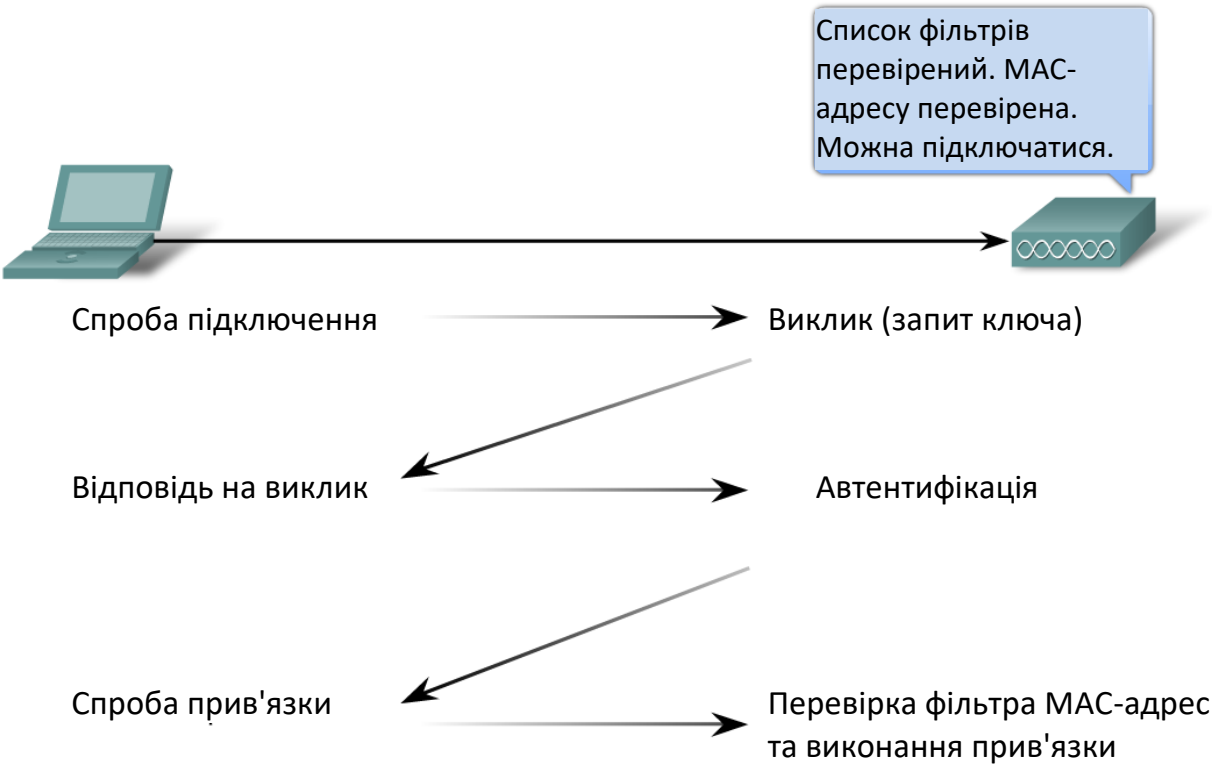


Рисунок 12.8 – Процес автентифікації

Шифрування в бездротових мережах

Автентифікація й фільтрація MAC-адрес можуть блокувати зломщикові доступ у бездротову мережу, але не зможуть запобігти перехопленню переданих даних. Оскільки не існує чітких границь бездротових мереж і весь трафік передається без проводів, то зломщик може легко перехоплювати або прочитати кадри даних бездротової мережі. Шифрування – це процес перетворення даних таким чином, що навіть перехоплення інформація виявляється марним.

Протокол конфіденційності, еквівалентного дротового зв'язка – Wired Equivalency Protocol (WEP)

Протокол WEP – це вдосконалений механізм безпеки, що дозволяє шифрувати мережевий трафік у процесі передачі. У протоколі WEP для шифрування й розшифровки даних використовуються попередньо налаштовані ключі.

WEP-ключ уводиться як рядок чисел і букв довжиною 64 або 128 біт. У деяких випадках протокол WEP підтримує 256-бітні ключі. Для спрощення створення й уведення цих ключів у багатьох пристроях використовуються фрази-паролі. Фраза-пароль – це простий засіб запам'ятовування слова або фрази, використовуваних при автоматичній генерації ключа.

Для ефективної роботи протоколу WEP точка доступу, а також кожний бездротовий пристрій, що має дозвіл на доступ у мережу, повинні використовувати загальний WEP-ключ. Без цього ключа пристрою не зможуть розпізнати дані, передані по бездротовій мережі.

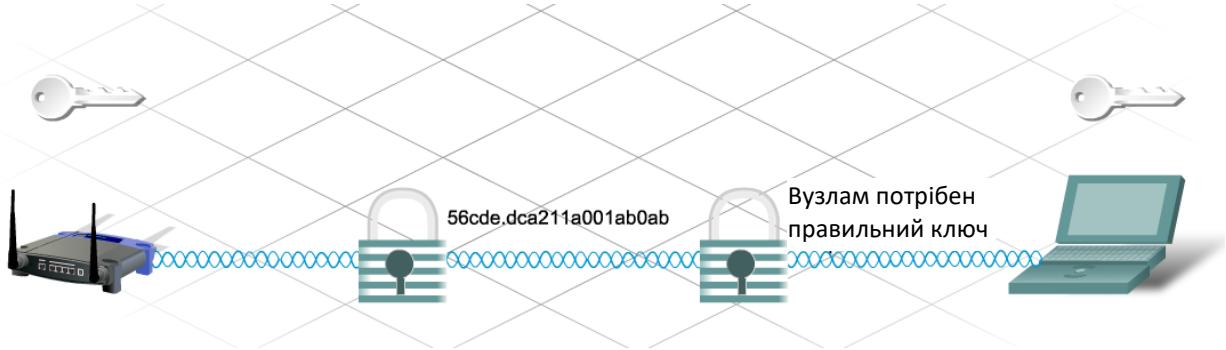


Рисунок 12.9 – Протокол WEP

Протокол WEP – це ефективний засіб захисту даних від перехоплення. Проте, протокол WEP також має свої слабкі сторони, одна з яких полягає у використанні статичного ключа для всіх пристроїв з підтримкою WEP. Існують програми, що дозволяють зломщикові визначити WEP-ключ. Ці програми можна знайти в мережі Інтернет. Після того, як зломщик одержав ключ, він одержує повний доступ до всієї переданої інформації.

Одним із засобів захисту від такої уразливості є часта зміна ключів. Існує вдосконалений і безпечний засіб шифрування – протокол захищеного доступу Wi-Fi (Wi-Fi Protected Access, (WPA)).

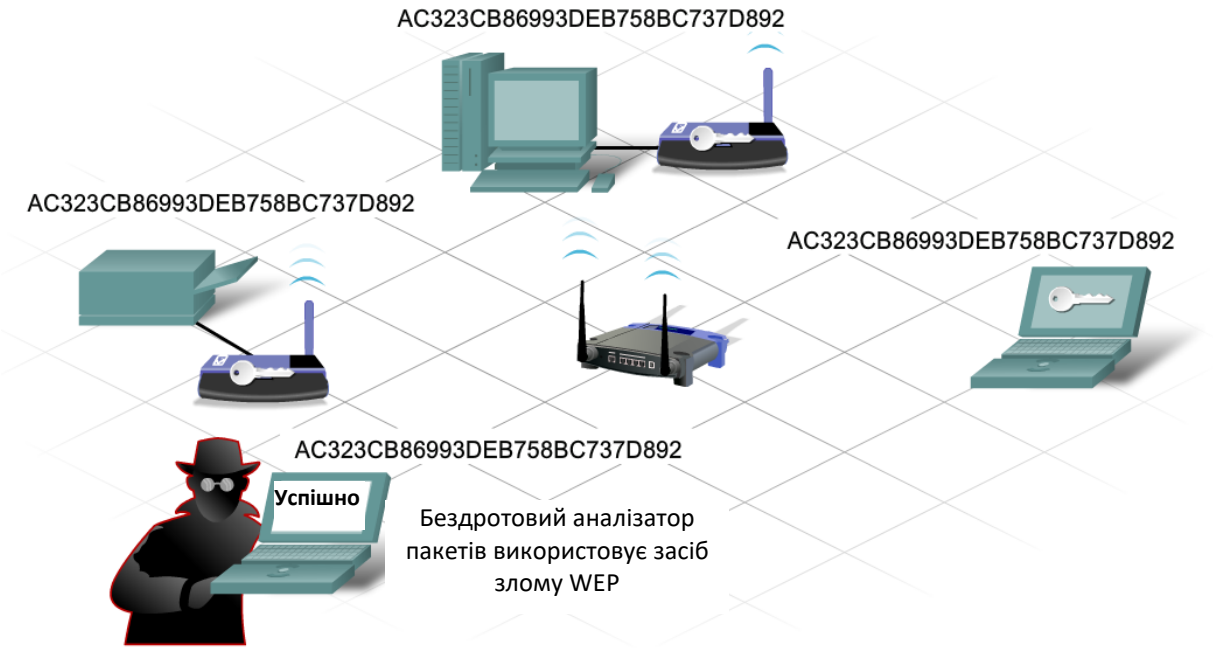


Рисунок 12.10 – Злом WEP

Захищений доступ до Wi-Fi (WPA)

У протоколі WPA використовуються ключі шифрування довжиною від 64 до 256 біт. При цьому WPA, на відміну від WEP, генерує нові динамічні ключі при кожній спробі клієнта встановити з'єднання із точкою доступу. Із цієї причини WPA уважається більше безпечним, ніж WEP, тому що його значно сутужніше зламати.

WPA2

WPA2 визначається стандартом IEEE 802.11i, прийнятим у червні 2004 року, і покликаний замінити WPA. У ньому реалізовано CCMP і шифрування AES, за рахунок чого WPA2 став більш захищеним, ніж свій попередник. З 13 березня 2006 підтримка WPA2 є обов'язковою умовою для всіх сертифікованих Wi-Fi пристроїв

Фільтрація трафіку

Крім керування доступом у мережу WLAN і адміністрування прав на використання переданих даних, необхідно також управляти трафіком, переданим мережею WLAN. Для цього застосовується фільтрація трафіку.

Фільтрація дозволяє блокувати вхід і вихід небажаного трафіку з мережі. Фільтрацію виконує точка доступу в міру проходження трафіку через неї. Цей засіб дозволяє виключати або обмежувати трафік окремих MAC-адрес або IP-адрес. Крім того, фільтрація трафіку дозволяє блокувати окремі програми за номерами портів. Виключення небажаного й підозрілого трафіку з мережі дозволяє підвищити пропускну здатність передачі більше важливих даних і тим самим збільшити продуктивність мережі WLAN. Наприклад, за допомогою фільтрації можна заблокувати весь telnet-трафік, що надходить на окрему машину, наприклад, сервер автентифікації. Будь-які спроби проникнення на сервер автентифікації за допомогою telnet, будуть блокуватися як підозрілі.

РОЗДІЛ 13. УСУНЕННЯ ПРОБЛЕМ З МЕРЕЖАМИ

Усунення проблем складається у виявленні, локалізації й виправленні виникаючих проблем. Досвідчені фахівці при діагностиці неполадок часто покладаються на інтуїцію, але існують і чітко структуровані алгоритми для встановлення найбільш імовірної причини й пошуку рішення.

Процес діагностики варто ретельно документувати. У документації повинне бути відбите якнайбільше відомостей по наступних питаннях:

– виявлена проблема;

– міри, початі для встановлення причини проблеми;

– міри, початі для рішення проблеми й запобігання її повторного виникнення.

Необхідно документувати всі прийняті міри, навіть якщо з їхньою допомогою не вдалося вирішити проблему. Складена документація стане керівництвом на випадок появи схожої проблеми.

Одержавши повідомлення про проблему, перевірте його й оцініть масштаби проблеми. Підтвердивши існування проблеми, можна приступити до її рішення, почавши зі збору інформації.

Збір інформації

У першу чергу для збору інформації можна опитати людини, що повідомили про проблему. Питання можуть стосуватися досвіду кінцевих користувачів, спостережуваних ознак проблеми, повідомлень про помилки й недавніх змін конфігурації пристроїв і додатків.

Далі варто зібрати інформацію про все устаткування, що може бути порушено даною проблемою. Одержати ці відомості можна з документації. Також будуть потрібні копії всіх файлів журналів і перелік недавніх змін у конфігурації устаткування. Варто встановити назву виробника, марку й модель пристроїв, охоплених проблемою, а також їхнього власника й стан гарантії. Крім того, необхідно визначити версію мікропрограми або ПЗ в

пристрої, оскільки може мати місце проблема сумісності з певними апаратними платформами.

Для збору відомостей про мережу можна також застосовувати інструментальні засоби моніторингу мережі – розвинені додатки, що одержали широке поширення у великих мережах для безперервного збору відомостей про стан мережі й мережевих пристроїв. Ці інструментальні засоби можуть бути недоступні для мереж малого масштабу.

Після збору необхідної інформації можна приступитися до усунення проблеми.

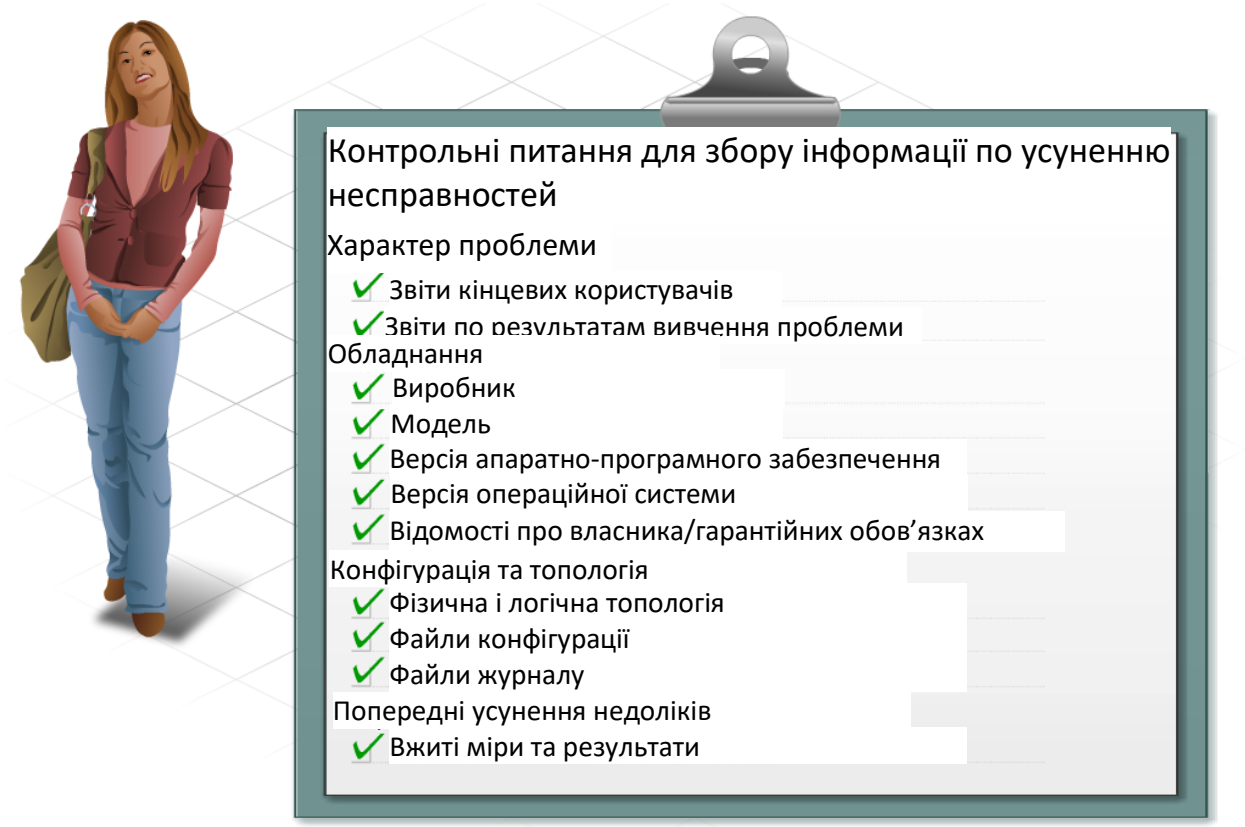


Рисунок 13.1 – Збір інформації

Підходи до усунення проблем

Існує ряд структурованих методів усунення проблем, у тому числі наступні:

– "Зверху долілиць".

– "Знизу нагору".

– "Розділяй і пануй".

Всі ці структуровані методи припускають багаторівнева будова мережі. Прикладом багаторівневої мережі є модель OSI, у якій всі функції обміну даними строго поділені на сім рівнів. Діагностуючи проблему в цій моделі, можна послідовно перевірити працездатність всіх функцій на кожному рівні, поки проблема не буде локалізована.

Підхід "зверху долілиць" припускає рух долілиць із прикладного рівня. Проблема досліджується з погляду користувача й додатки. Не працює тільки один додаток або всі додатки? Наприклад, чи може користувач при неприступності електронної пошти звертатися до веб-сторінок? чи Проявляються подібні явища на інших робочих станціях?

Підхід "знизу нагору" припускає рух з фізичного рівня до більше високого. На фізичному рівні обстежаться устаткування й дротові з'єднання. Чи не випали кабелі із гнізд? Якщо устаткування позначене індикаторами, чи горять індикатори?

При підході "розділяй і пануй" аналіз починається з одного із проміжних рівнів, після чого обстежаться вищестоящі або нижчестоящі рівні. Наприклад, можна почати діагностику проблеми з мережевого рівня, перевіривши конфігурацію IP.

Завдяки своїй структурі подібний підхід щонайкраще підходить для починаючих ремонтників. Багато досвідчених фахівців часто воліють структурованим підходам власну інтуїцію й досвід, застосовуючи менш формальні прийоми, наприклад метод проб і помилок або заміну компонентів.

Підхід до пошуку і усуненню несправностей	Як його використовувати	Випадки, в яких його рекомендується використовувати	Переваги/ Недоліки
Зверху униз	Завжди починається на прикладному рівні і виконується вниз по рівням до знаходження рівня, на якому стався збій.	Більше підходить для вирішення простих проблем, а також якщо є підозри,що проблеми пов’язані з додатками/користувачем, тобто з верхнім рівнем.	Якщо в підсумку з’ясовується, що проблема пов’язана з нижніми рівнями, відбувається непродуктивна трата часу та зусиль на верхньому або прикладному рівнях.

а)

Підхід до пошуку і усуненню несправностей	Як його використовувати	Випадки, в яких його рекомендується використовувати	Переваги/ Недоліки
«Розподіляй і володарюй»	В залежності від обставин (виявлених проблем) і досвіду можна прийняти рішення про початок пошуку на будь-якому рівні і рухатися вгору або вниз по стеку OSI.	Більше підходить для досвідчених користувачів при наявності точних симптомів проблеми.	Він дозволяє швидше інших методів досягти рівня, де стався збій. Для ефективного використання цього підходу потрібен досвід.

б)

Підхід до пошуку і усуненню несправностей	Як його використову-вати	Випадки, в яких його рекомендується використовувати	Переваги/ Недоліки
Знизу вгору	Завжди починається на фізичному рівні і виконується вгору по рівням до знаходження рівня, на якому стався збій.	Більше підходить для важких випадків.	Це повільний, але надійний підхід. Якщо проблема виникла на рівні додатків (або на верхньому рівні), то його використання може вимагати довгого часу.

в)

Рисунок 13.2 – Підходи до усунення проблем

Метод проб і помилок

При методі проб і помилок ремонтник керується своїми знаннями, намагаючись установити найбільш імовірну причину проблеми. Він формулює припущення на основі колишнього досвіду й наявної інформації про структуру мережі. Якщо припущене рішення не працює, ремонтник ураховує цю інформацію при пошуку наступного найбільш імовірного рішення. Процес повторюється доти, поки проблему не вдасться локалізувати й усунути.

Незважаючи на те, що метод проб і помилок потенційно може бути дуже оперативний, важливу роль у ньому грають досвід і здатності ремонтника, без яких можуть бути зроблені невірні припущення й упущені прості рішення.

Заміна

Цей метод використовується в тому випадку, коли можна зв'язати проблему з деяким компонентом або файлом конфігурації. Дефектний

компонент або помилковий код заміняється свідомо справним пристроєм або файлом. Незважаючи на те, що такий підхід не гарантує локалізацію проблеми, він часто виявляється ефективним, допомагаючи в мінімальний строк відновити працездатність мережі. Необхідною умовою є доступність запасних частин, компонентів і резервних файлів конфігурації, що в деяких випадках може бути скрутним.

Приклад способу заміни – заміна Інтернет-провайдером пристрою, справність якого викликає підозри, замість відряджання техніка для діагностики й локалізації проблеми. Заміна найбільш доцільна для недорогих компонентів, наприклад мережевих плат і сполучних кабелів.

Виявлення фізичних неполадок

Значна частина проблем з мережею може бути пов'язана з фізичними компонентами або проблемами на фізичному рівні.

Проблеми на фізичному рівні часто відносяться до апаратної частини комп'ютерів і мережевих пристроїв, а також кабелям, якими вони з'єднуються. Такі проблеми не залежать від логічної (програмної) конфігурації пристроїв.

Проблеми на фізичному рівні виникають і в дротових, і в бездротових мережах. При діагностиці фізичних проблем найкраще покладатися на почуття: зір, нюх, дотик і слух.

1. Зір використовується для виявлення неправильно підключених або погано прокладених кабелів, включаючи:

– непідключені кабелі;

– кабелі, підключені до неправильного порту;

– погано закріплені підключення кабелів;

– ушкоджені кабелі й роз’єми;

– використання кабелю невідповідного типу.

У результаті візуального огляду світлодіодних індикаторів можна також оцінити стан і функціонування різних мережевих пристроїв.

2. Нюх може надати користувачеві сигнал про перегрів компонентів. Запах горілої ізоляції або компонентів дуже помітний і є вірною ознакою серйозної несправності.

3. Користувач може використовувати дотик для знаходження перегрітих компонентів, а також виявляти механічні проблеми таких пристроїв, як холодні вентилятори. Ці пристрої звичайно створюють легку вібрацію компонентів, яку можна відчути, доторкнувшись до них. Відсутність вібрації або занадто сильна вібрація можуть указувати на те, що вентилятор не працює або от-от зламається.

4. Слух використовується для виявлення серйозних проблем з електричними компонентами й роботою холодних вентиляторів і дискових накопичувачів. Робота цих пристроїв характеризується певними звуками, і будь-які зміни нормальних звуків звичайно вказують на якусь проблему.

Програмні засоби діагностики мереж

Для діагностики проблем у мережах доступна безліч програмних засобів. Багато хто з них реалізуються операційною системою й доступні у вигляді команд в інтерфейсі командного рядка (CLI). Синтаксис команд у різних операційних системах розрізняється.

Крім інших, доступні наступні засоби:

– ipconfig – перегляд відомостей про конфігурацію IP;

– ping – перевірка зв'язку з іншими IP-вузлами;

– tracert – перегляд маршруту до місця призначення;

– netstat – перегляд інформації про мережеві з'єднання;

– nslookup – запит інформації про конкретний домені безпосередньо із сервера доменних імен.

Діагностика мереж за допомогою команди ipconfig

Команда ipconfig дозволяє переглянути поточні параметри конфігурації IP для вузла. Ця команда в інтерфейсі командного рядка використовується для перегляду основних відомостей про конфігурацію, включаючи IP-адресу вузла, маску підмережі й шлюз за замовчуванням.

ipconfig /all

Команда ipconfig /all displays служить для перегляду додаткової інформації, до якої ставляться MAC- і IP-адреси шлюзу за замовчуванням і DNS-серверів. У виводі команди також вказується, чи включена підтримка DHCP, і приводяться відомості про адресу DHCP-сервера й оренді адрес.

Як цей програмний засіб допомагає діагностувати проблеми? Без правильно налаштованих параметрів IP вузол не зможе обмінюватися даними мережею. Під час відсутності інформації про адреси DNS-серверів вузол не зможе перетворювати імена в IP-адреси.

ipconfig /release і ipconfig /renew

Якщо застосовується динамічне призначення IP-адрес, команда ipconfig /release дозволяє зняти існуючі прив'язки адрес DHCP. Команда ipconfig /renew запитує конфігурацію з DHCP-сервера. Вузол може мати невірну або застарілу конфігурацію IP. У цьому випадку для відновлення зв'язку необхідно тільки обновити цю інформацію.

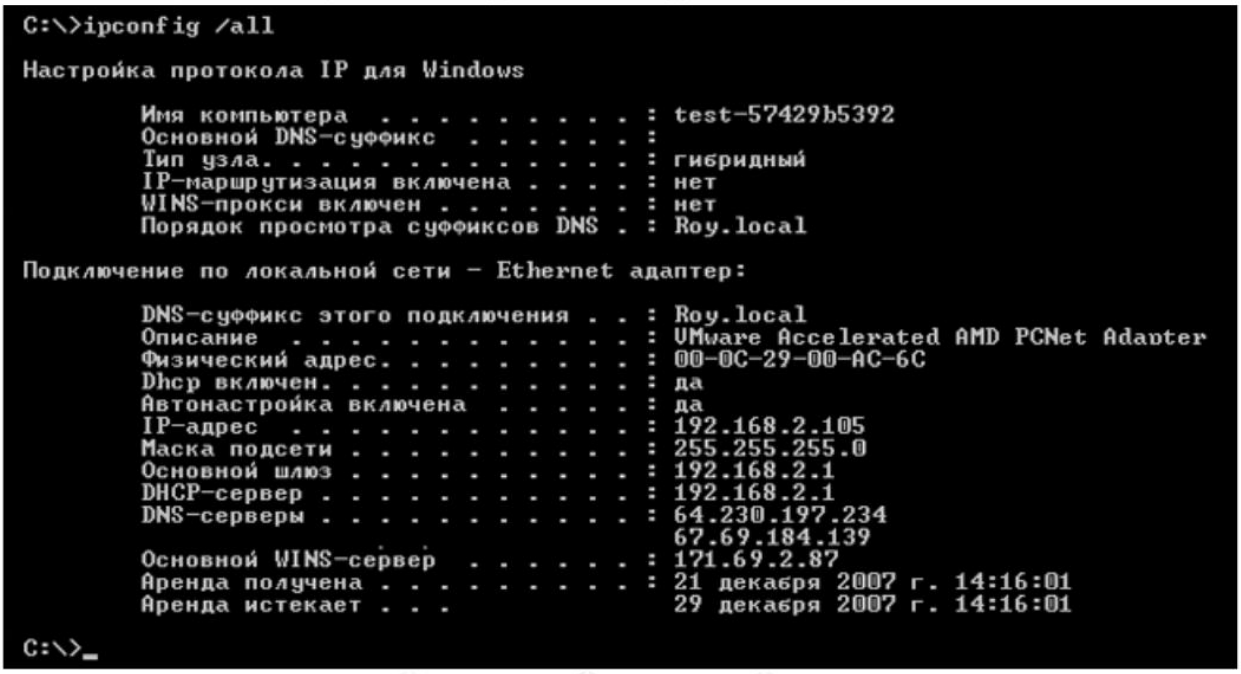


Рисунок 13.3 – Виконання команди ipconfig /all

Якщо після скасування конфігурації IP вузол не може одержати поточну інформацію з DHCP-сервера, проблема може складатися у втраті зв'язку з мережею. У цьому випадку необхідно переконатися, що на мережевій платі горить індикатор фізичного з'єднання з мережею (LINK). Якщо описаними мірами усунути проблему не вдалося, її джерелом може бути DHCP-сервер або мережеві з'єднання з DHCP-сервером.

Діагностика проблем за допомогою команди ping

Якщо параметри IP на локальному вузлі налаштовані вірно, наступний етап складається в перевірці з'єднання з вузлом командою ping. Команда ping відправляє луну-запит для перевірки доступності вузла. У команді ping вказується IP-адресу або ім'я вузла, що потрібно перевірити, наприклад:

ping 192.168.7.5

ping www.cisco.com

Якщо в команді ping зазначена IP-адреса, на нього мережею буде відправлений пакет луни-запиту. Одержавши луну-запит, вузли-призначення повертає пакет з відгуком. Якщо джерело одержує відгук на луну-запит, наявність з'єднання підтверджується.

При відправленні луна-запиту на певне ім'я вузла, наприклад www.cisco.com, спочатку відсилається пакет на DNS-сервер для перетворення ім'я в IP-адресу. Після визначення IP-адреси луна-запит пересилається на цей IP-адресу й обробляється звичайним образом. Якщо луна-запит вдається відправити на IP-адреса, але не на ім'я вузла, може мати місце проблема з DNS.

Якщо луна-запит проходить на ім'я вузла й на його IP-адресу, але користувач не може працювати з додатком, джерелом проблеми з великою ймовірністю є додаток або вузол призначення. Наприклад, може бути недоступна запитана мережева служба.

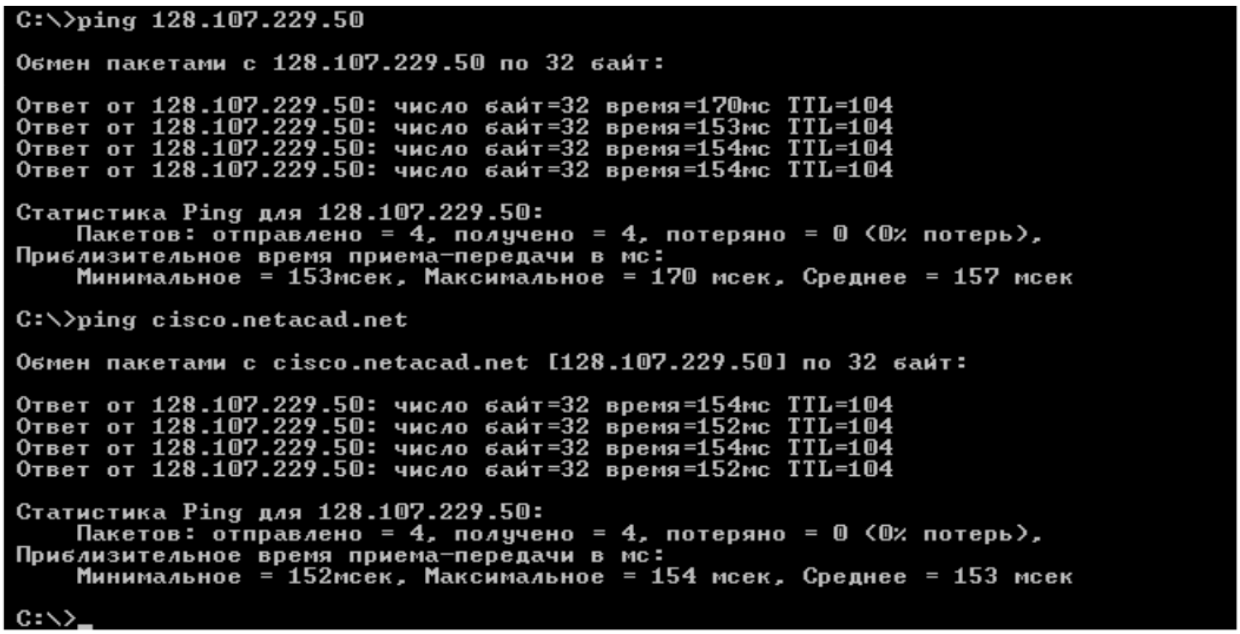


Рисунок 13.4 – Виконання команди ping

Якщо луна-запит не вдається відправити жодним зі способів, проблема, швидше за все, локалізована на проміжній ділянці шляху до вузла призначення. У цьому випадку рекомендується відправити луна-запит на шлюз за замовчуванням. Якщо луна-запит проходить на шлюз за замовчуванням, проблема не пов'язана з локальною мережею. Якщо луна-запит не проходить на шлюз за замовчуванням, проблема має місце в локальній мережі.

У базовій формі команда ping звичайно відправляє чотири луни-запиту й очікує відгуку на кожний з них. Однак цю команду можна зробити більше практичної за допомогою додаткових параметрів. Параметри, наведені на рисунку, дозволяють довідатися про інші доступні функції.

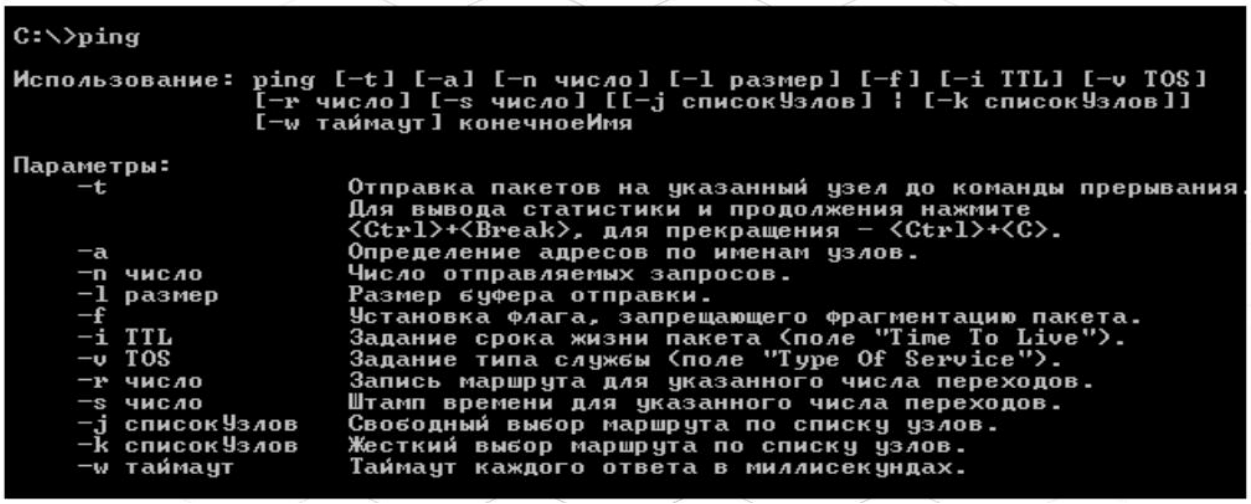


Рисунок 13.5 – Функції команди ping

Діагностика проблем за допомогою команди tracert

Команда ping перевіряє тільки просту наявність зв'язку між вузлами. Однак якщо проблема виражається в неможливості відправлення луна-запиту, команда ping не дозволяє встановити, у якому місці з'єднання обривається. Для цього використовується інший програмний засіб – tracert.

Команда tracert повідомляє про стан з'єднання на кожній ділянці маршруту, по якому пакет проходить через маршрутизатори до адресата. Також повідомляється час проходження пакета від джерела до кожної ділянки (в обидва боки). Команда tracert допомагає встановити місця втрати або затримки пакетів через обмеження пропускної здатності або із трафіку в мережі.

У базовій формі команда tracert простежує не більше 30 ділянок маршруту від джерела до адресата. При перевищенні цього числа ділянок вона повідомляє про неприступність адресата. Число ділянок налаштовується параметром –h. Також доступні інші модифікатори, наведені в числі параметрів на рисунку.

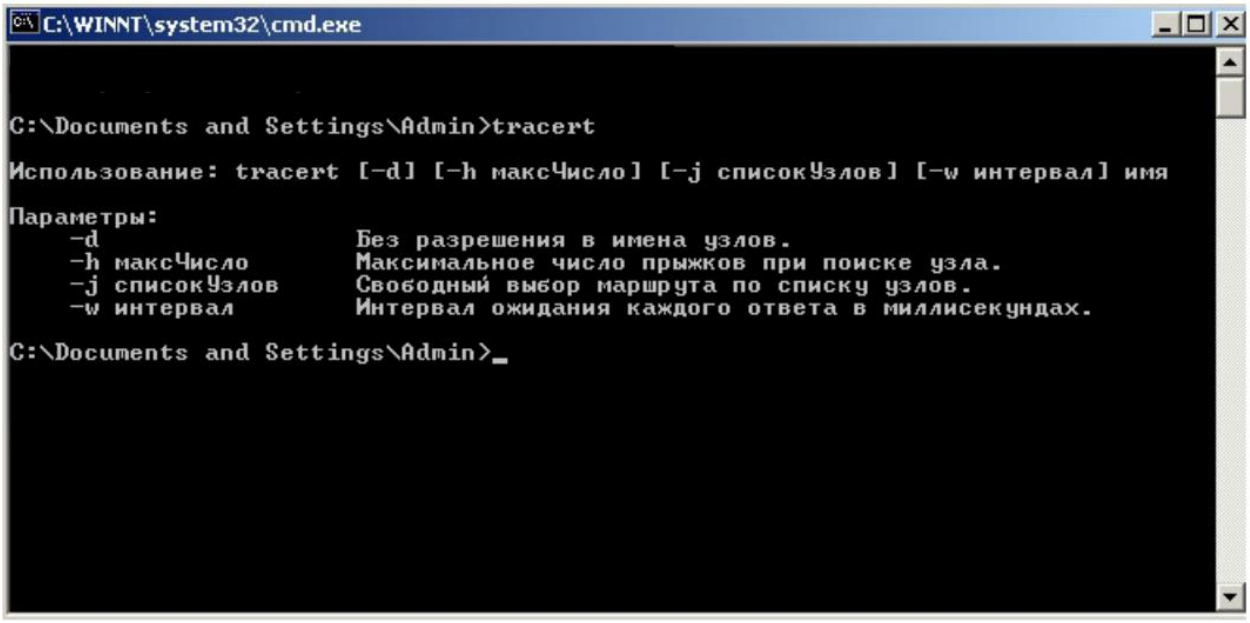


Рисунок 13.6 – Функції команди tracert

Діагностика проблем за допомогою команди netstat

У деяких випадках потрібно визначити, які TCP-з'єднання відкриті й діють на мережевому вузлі. Перевірити стан цих з'єднань допомагає важливий програмний засіб – netstat. Команда netstat перераховує використовувані протоколи, локальні адреси й номери портів, адресу й номер порту на віддаленому вузлі й повідомляє стан з'єднань.

Непояснені TCP-з'єднання можуть являти значну загрозу безпеки. Вони свідчать про наявність сторонніх підключень до локального вузла. Крім того, зайві TCP-з'єднання створюють навантаження на системні ресурси й здатні істотно сповільнити роботу вузла. За допомогою команди netstat можна одержати інформацію про відкриті з'єднання з вузлом у випадку помітного погіршення продуктивності.

Команда netstat має ряд корисних параметрів.

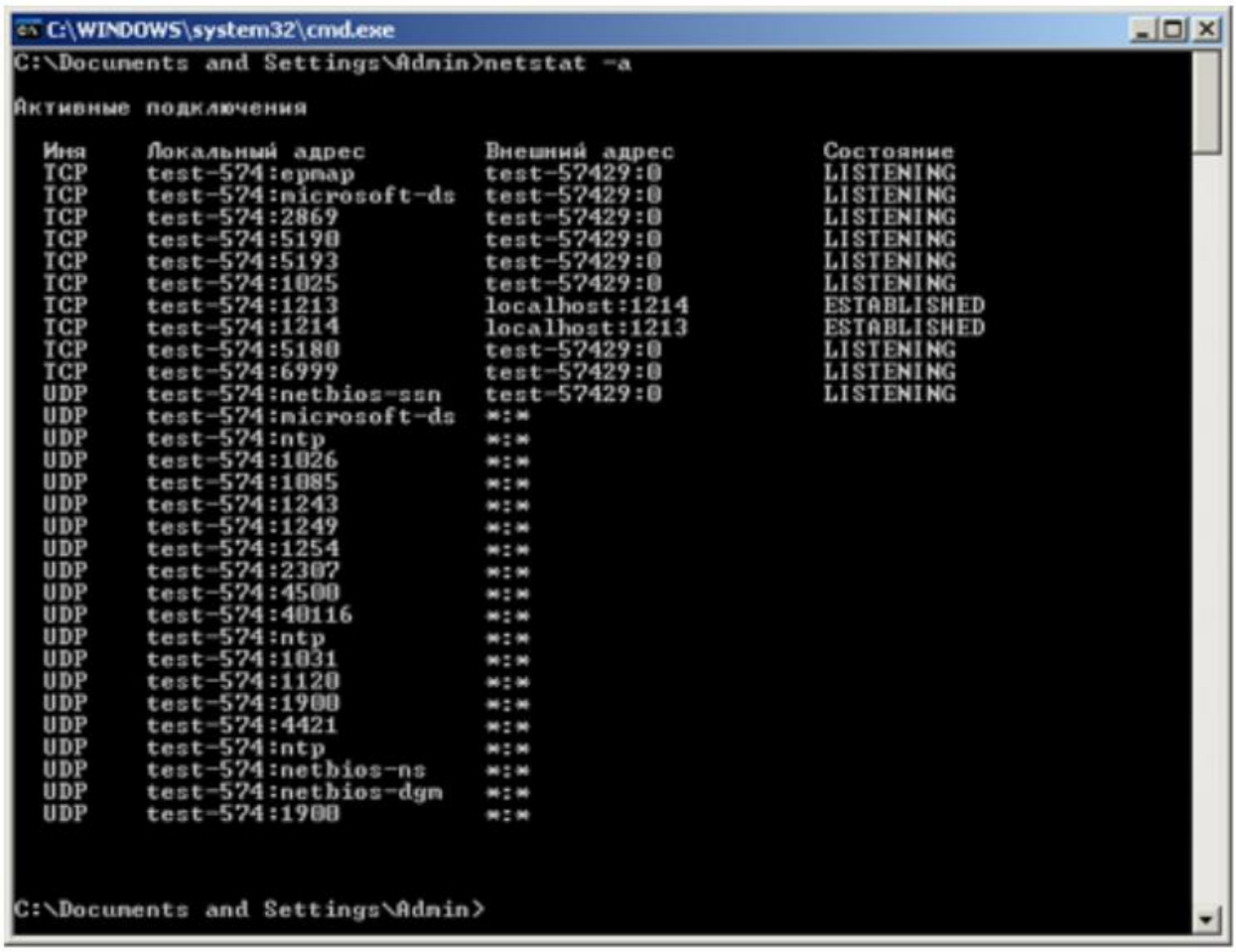


Рисунок 13.7 – Функції команди netstat

Діагностика проблем за допомогою команди nslookup

Користувачі мережевих додатків і сервісів звичайно замість IP-адрес указують DNS-імена. У цьому випадку перед відправленням запиту вузол повинен звернутися до DNS-сервера для перетворення імені у відповідну IP-адресу. Потім вузол доставляє інформацію у вигляді пакета за протоколом IP.

Програмний засіб nslookup дозволяє кінцевим користувачам самостійно відправляти запити DNS-серверам для перетворення імен. Відомості, що повертаються командою nslookup, містять у собі IP-адресу використовуваного DNS-сервера, а також IP-адресу вузла, пов'язаний із зазначеним DNS-Ім'ям. Команда nslookup часто використовується для діагностики правильності перетворення імен DNS-серверами.

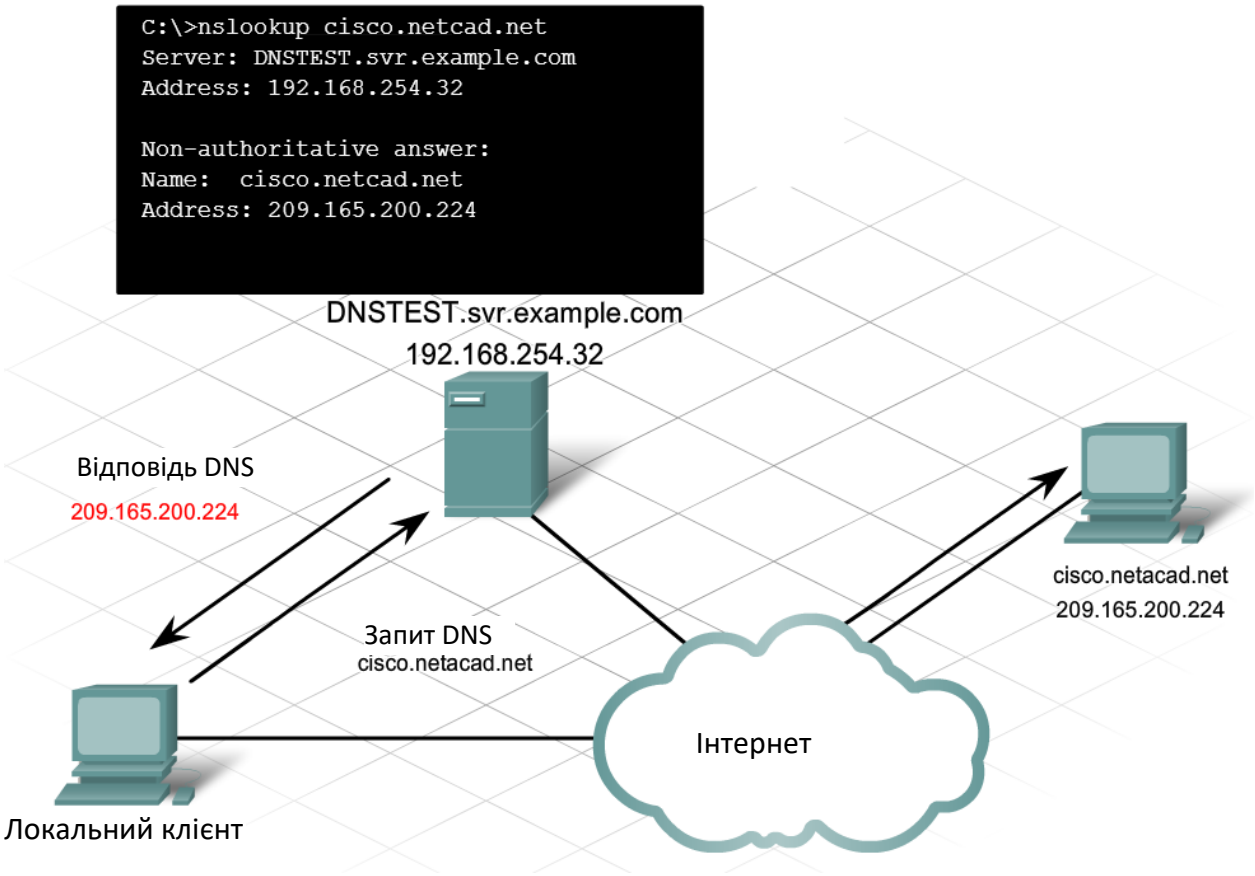


Рисунок 13.8 – Реалізація команди nslookup

Проблеми підключення

Проблеми підключення виникають у бездротових, дротових і змішаних мережах. При діагностиці мережі, у якій застосовуються й дротові, і бездротові з'єднання, оптимальної найчастіше виявляється стратегія "розділяй і пануй", що дозволяє локалізувати проблему на дротовій або бездротовій ділянці. Найпростіший алгоритм визначення ділянки мережі, на якому виникла проблема:

1. Відправте луну-запит з бездротового клієнта на шлюз за замовчуванням, щоб перевірити правильність підключення бездротового клієнта.

2. Відправте луну-запит із дротового клієнта на шлюз за замовчуванням, щоб перевірити правильність підключення дротового клієнта.

3. Відправте луну-запит з бездротового клієнта на дротового клієнта, щоб перевірити працездатність інтегрованого маршрутизатора.

Локалізувавши проблему, можна приступитися до її усунення.

Мережеві індикатори

Незалежно від того, на якій ділянці – дротовій або бездротовій – є присутня проблема, один з першочергових кроків у її діагностиці повинен полягати в перевірці показань світлодіодів, по яких можна зробити висновок про поточний стан або режим пристрою чи з'єднання. Світлодіоди індикують стан зміною кольору або миготінням. Точна конфігурація й призначення світлодіодів залежать від конкретного виробника й пристрою.

Звичайно пристрої забезпечуються трьома групами світлодіодів, які індикують живлення, стан і виконувані дії. На деяких пристроях один світлодіод залежно від поточного стану пристрою повідомляє різну інформацію. Призначення індикаторів слід завжди уточнювати по документації, але деякі загальні стани індикуються однаково.

Погаслі світлодіоди можуть указувати на вихід з ладу пристрою або порту, або проблеми з кабелями. Причиною непрацездатності пристрою може бути апаратна несправність. Порт також може перестати функціонувати через апаратну несправність або невірне налаштування ПЗ. Незалежно від того, чи є мережа дротовою або бездротової, важливо спочатку переконатися у функціонуванні пристрою й портів, щоб не витратити значний час на діагностику по інших напрямках.


Світлодіодний індикатор безпеки
Світлодіодний індикатор бездротової активності
Світлодіодний індикатор активності Internet
Світлодіодний індикатор активності Ethernet
Світлодіодний індикатор мережі

а)


Світлодіодний індикатор безпеки
• Показує поточний стан налаштувань безпеки пристрою.
• Рівний зелений колір означає, що безпека включена.
Світлодіодний індикатор безпеки
Світлодіодний індикатор бездротової активності
Світлодіодний індикатор активності Internet
Світлодіодний індикатор активності Ethernet
Світлодіодний індикатор мережі

б)

в)

г)

Рисунок 13.9 – Мережеві індикатори

Проблеми з підключенням

Неможливо підключити дротовий вузол до інтегрованого маршрутизатора

При неможливості підключення дротового клієнта до інтегрованого маршрутизатора одним з перших дій повинна стати перевірка фізичного з'єднання й кабелів. Кабелі – "нервова система" дротових мереж і найбільш часта причина їхнього простою.

При роботі з кабелями варто приділяти увагу декільком моментам.

1. Переконаєтеся, що використовується відповідний тип кабелю. У мережах поширені два типи кабелів: прямі й перехресні. Невірно обраний тип кабелю може привести до неможливості встановлення з'єднання.

2. Невірне оброблення кабелів – часта причина проблем з мережами. Щоб уникнути цих проблем варто дотримуватися стандартів оброблення кабелів:

Оброблення кабелів повинно здійснюватися у відповідності зі стандартом 568A або 568B.

1. Під час оброблення не слід розплітати жили кабелю на велику довжину.

2. Роз’єми повинні бути обтиснуті в кабельній манжеті для зняття механічної напруги.

3. Максимально припустима довжина кабелю залежить від характеристик кабелю. Перевищення припустимої довжини істотно погіршує робочі параметри мережі.

4. При проблемах зі зв'язком варто переконатися, що між пристроями, що з’єднуються, вірно обрані порти.

5. Кабелі й роз’єми повинні бути захищені від фізичного ушкодження. Щоб уникнути механічних навантажень на роз’єми необхідно забезпечити опору для кабелів і прокладати їх так, щоб вони не заважали руху людей.

Усунення проблем з бездротовим підключенням

Бездротовий вузол не може підключитися до точки доступу

Якщо бездротовий клієнт не може підключитися до точки доступу, можуть мати місце проблеми з бездротовим каналом зв'язку. У бездротових мережах для передачі даних використовуються радіочастотні (РЧ) сигнали. Можливість установлення РЧ з'єднання з вузлами визначається багатьма факторами.

1. Не всі стандарти бездротового зв'язку сумісні один з одним. Стандарт 802.11a (діапазон 5 Ггц) несумісний зі стандартами 802.11b/g/n (діапазон 2,4 Ггц). У діапазоні 2,4 Ггц діє кілька стандартів, що використовують різні технології. Без спеціальних налаштувань два пристрої, що відповідають різним стандартам, можуть не встановити зв'язок один з одним.

2. Всі сеанси бездротового зв'язку реалізуються по роздільним, що не перекриваються каналам. Деякі точки доступу можна налаштувати на вибір найменш завантаженого або найбільш швидкісного каналу. Незважаючи на можливість застосування автоматичних режимів налаштування, ручне налаштування каналу точки доступу забезпечує більше точний контроль і в певних умовах може бути необхідним.

3. Потужність РЧ сигналу падає зі збільшенням відстані. Слабкий сигнал може перешкодити надійному встановленню зв'язку між пристроями й обміну даними. Сигнал може перериватися. Програмний засіб для клієнтів з мережевими адаптерами дозволяє визначити потужність сигналу і якість з'єднання.

4. РЧ сигнали придушуються перешкодами від зовнішніх джерел, включаючи пристрої, що працюють на однаковій частоті. Виявити ці перешкоди можна при обстеженні об'єкта.

5. Точки доступу ділять доступну смугу пропущення між пристроями. У міру того, як росте число пристроїв, пов'язаних із точкою доступу, зменшується смуга пропущення, доступна кожному пристрою, і

погіршується продуктивність мережі. Ця проблема вирішується шляхом зменшення числа бездротових клієнтів на кожному каналі.

Усунення проблем з реєстрацією й автентифікацією у бездротовій мережі

Проблеми з налаштуванням бездротових мереж

У сучасних бездротових мережах використовуються різні технології, що допомагають захистити передані мережею дані. Помилки в їхньому налаштуванні можуть перешкодити встановленню зв'язку. Найчастіше налаштовуються такі параметри безпеки, як SSID, режим автентифікації й режим шифрування.

1. Ідентифікатор SSID являє собою алфавітно-цифровий рядок з 32 символів, сприйманих з урахуванням регістра. Точка доступу й клієнт повинні мати однакові ідентифікатори. Цієї проблеми не виникає, якщо використовуються широкомовне розсилання й прийом SSID. У іншому випадку необхідно вручну вказати SSID у клієнті. Якщо ідентифікатор SSID клієнта налаштований невірно, клієнт не зможе зв'язатися із точкою доступу. Крім того, клієнт автоматично зв'яжеться з будь-якою іншою точкою доступу, якщо вона має співпадаючий ідентифікатор SSID.

2. У більшості точок доступу за замовчуванням діє відкритий режим автентифікації, що дозволяє підключати будь-які пристрої. При використанні більше захищених режимів автентифікації необхідно налаштувати однаковий ключ у клієнта й точці доступу. При розбіжності ключів автентифікація не проходить, і зв'язок між пристроями не встановлюється.

Шифрування – це процес модифікації даних, у результаті якого вони не можуть бути перехоплені третіми сторонами без відповідного ключа шифрування. Якщо включено режим шифрування, у точці доступу й бездротовому клієнті повинні бути налаштовані однакові ключі. Якщо клієнт встановлює зв'язок із точкою доступу, але не може пересилати або приймати дані, джерелом проблеми може бути ключ шифрування.

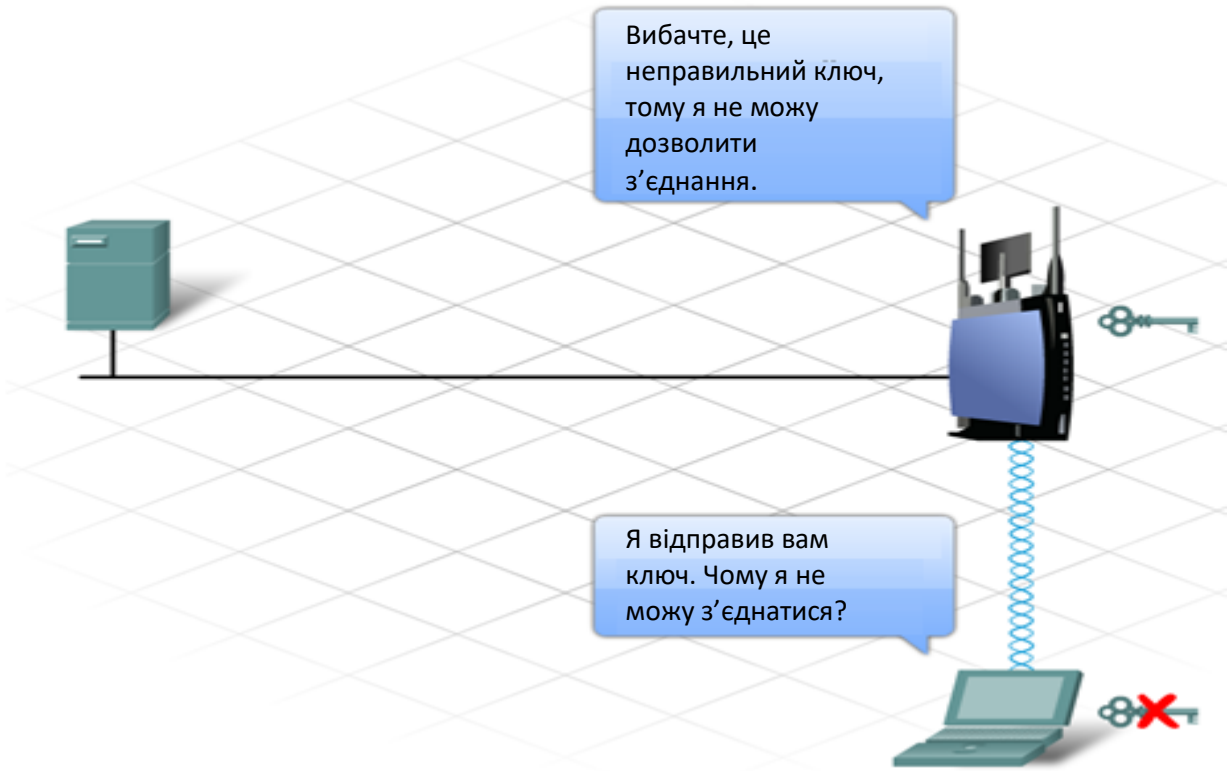


Рисунок 13.10 – Проблеми автентифікації

Проблеми пов'язані з DHCP

Перевірка правильності IP-адреси, одержуваного комп'ютером

Якщо фізичне з'єднання із дротовим або бездротовим вузлом справно, варто перевірити налаштування IP з боку клієнта.

Конфігурація IP істотно впливає на можливість підключення вузла до мережі. Інтегрований маршрутизатор, наприклад бездротовий маршрутизатор Linksys, виступає в якості DHCP-сервера для локальних дротових і бездротових клієнтів, повідомляючи їм параметри IP, у тому числі IP-адресу, маску підмережі, адресу шлюзу за замовчуванням і, можливо, IP-адреси DNS-серверів. DHCP-сервер прив'язує IP-адресу до MAC-адреси клієнта й зберігає ці відомості в таблиці клієнта. На домашньому маршрутизаторі Linksys переглянути вміст цієї таблиці можна на сторінці графічного інтерфейсу "Status | Local Network" (Стан | Локальна мережа).

Вміст клієнтської таблиці повинен відповідати інформації про локальний вузол, повідомлюваної по команді ipconfig /all. Крім того, IP-адресу клієнта повинен перебувати в одній підмережі з адресою пристрою Linksys у локальній мережі. Інтерфейс локальної мережі на пристрої Linksys повинен бути обраний як шлюз за замовчуванням. Якщо відомості про конфігурацію клієнта розходяться з вмістом клієнтської таблиці, адресу необхідно зняти (ipconfig /release) і обновити (ipconfig /renew), щоб установити нову прив'язку.

Якщо дротові й бездротові клієнти одержують вірну конфігурацію IP і можуть встановлювати зв'язок із пристроєм Linksys, але не можуть пересилати один одному луна-запити, проблема з великою ймовірністю полягає в пристрої Linksys. Необхідно перевірити всі параметри конфігурації пристрою Linksys, переконавшись у відсутності обмежень безпеки, які могли б стати причиною проблеми.

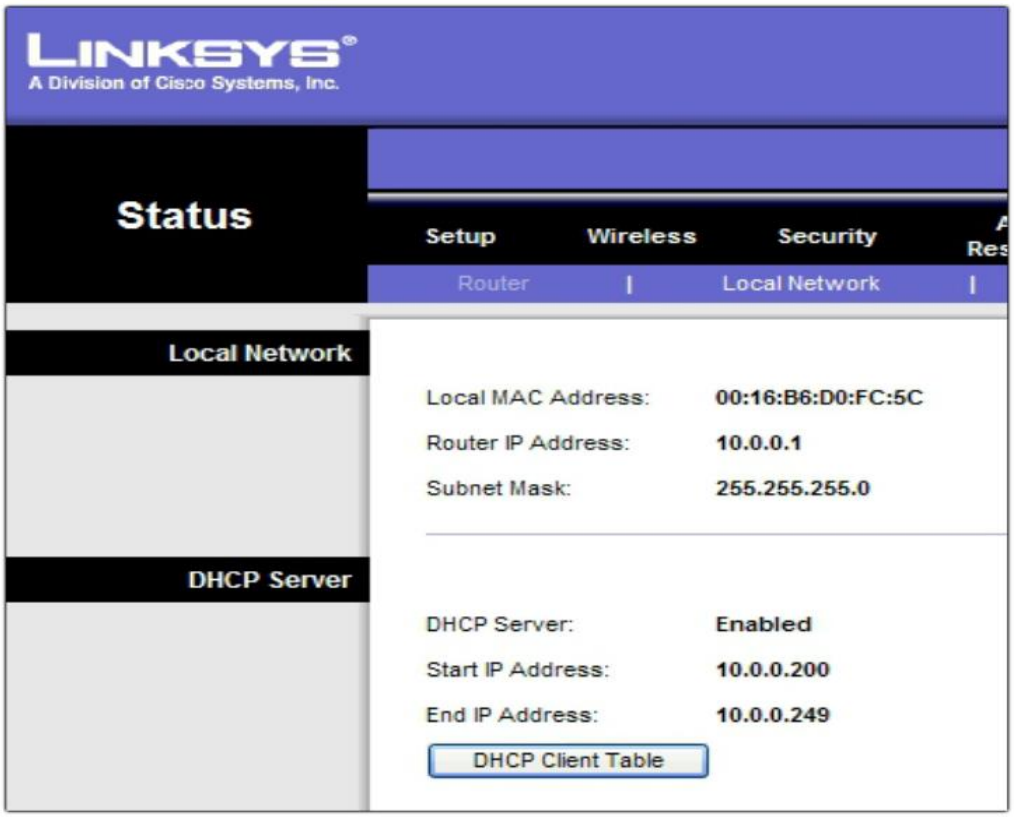


Рисунок 13.11 – Всі параметри конфігурації пристрою Linksys

Усунення проблем, пов'язаних з підключенням ISR до Інтернет-провайдеру

Дротові й бездротові вузли мають зв'язок один з одним, але не з Інтернетом.

Якщо вузли в дротовому й бездротовому сегментах мережі можуть з'єднуватися з інтегрованим маршрутизатором і іншими вузлами в локальній мережі, але не з Інтернетом, проблема може бути локалізована на ділянці від інтегрованого маршрутизатора до Інтернет-провайдеру.

Перевірити зв'язок між інтегрованим маршрутизатором і Інтернет-провайдером можна декількома способами. У графічному інтерфейсі перевірити з'єднання можна на сторінці стану маршрутизатора. На ній повинна бути зазначена IP-адреса, привласнена провайдером, і поточний стан з'єднання.

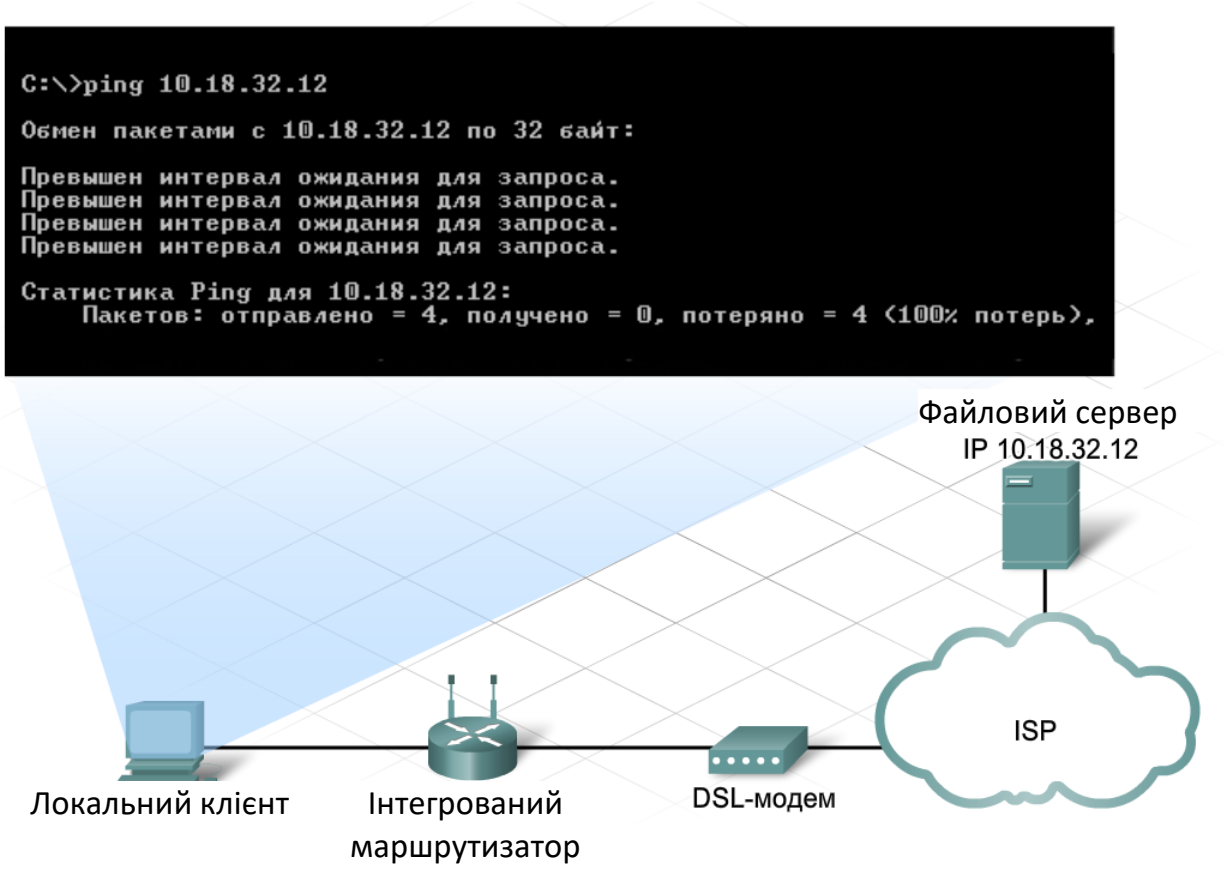


Рисунок 13.11 – Реалізація ping

Якщо на цій сторінці повідомляється про відсутність з'єднання, інтегрований маршрутизатор може бути не відключений. Варто перевірити всі дротові з'єднання й стан світлодіодів. Якщо DSL-модем або кабельний модем реалізований у вигляді окремого пристрою, необхідно також перевірити підключення й стан індикаторів цього пристрою. Якщо Інтернет-провайдер для доступу в мережу вимагає вказувати ім'я користувача й пароль, варто переконатися, що ці реквізити налаштовані в точності так, як зазначено провайдером. У графічному інтерфейсі налаштування пароля звичайно викликається зі сторінки підготовки до роботи (Setup). Далі варто спробувати повторно встановити з'єднання, нажавши на сторінці стану кнопку "Connect" (Підключити) або "IP address renew" (Обновити IP-адресу). Якщо інтегрований маршрутизатор як і раніше не з'єднується, звернетеся до Інтернет-провайдеру й переконаєтеся у відсутності проблем з боку провайдеру.

Якщо на сторінці стану повідомляється, що з'єднання встановлене, але луна-запити до сайтів в Інтернеті не проходять, причиною може бути неприступність окремого сайту. Для перевірки відправте луну-запит на інший сайт. Якщо він також не проходить, перевірте налаштування безпеки, які можуть ставитися до даної проблеми, наприклад фільтрацію по портах.

Документація

Документація до мережі при усуненні проблем завжди відіграє важливу роль. У документації до мережі повинні бути відбиті нормальні або базові показники продуктивності, у порівнянні з якими можна зробити висновок про можливі проблеми.

Разом з базовими показниками продуктивності можуть бути зазначені очікувані типи трафіку, а також обсяги обміну трафіком із серверами й мережевими пристроями. Базові показники документуються після початкового налаштування мережі й виходу її в оптимальний робочий режим. Базові показники повинні бути оцінені повторно у випадку великомасштабних змін у мережі.

Така додаткова документація, як топологічні карти, схеми мережі й опису схем адресації, може виявитися коштовної для ремонтників, що аналізують фізичну структуру мережі й логічні потоки інформації.

Всі міри, що вживаються в ході рішення проблеми, також повинні документуватися. Документація послужить коштовним довідковим матеріалом при рішенні питань, які можуть виникнути в майбутньому. Для повноцінного документування рішення проблеми рекомендується відбити наступні відомості:

– вихідна проблема;

– міри, початі для локалізації проблеми;

– результати всіх вжитих заходів, незалежно від їхньої успішності;

– остаточно встановлена причина проблеми;

– остаточний спосіб рішення проблеми;

– профілактичні міри.

Допомога зовнішніх джерел

Якщо в процесі діагностики ремонтникові не вдається визначити суть проблеми й спосіб її рішення, може знадобитися допомога із зовнішніх джерел. Найбільш популярні джерела допомоги:

– колишня документація;

– онлайн-збірники питань, що задаються часто (FAQ);

– колеги й інші професіонали в області мереж;

– інтернет-форуми.

Звернення до довідкової служби

Довідкова служба – першочергове джерело допомоги кінцевим користувачам. Довідкова служба – це колектив професіоналів, що володіють знаннями й технічними засобами для діагностики й усунення часто виникаючих проблем. Довідкова служба сприяє кінцевому користувачеві у встановленні наявності проблеми, діагностиці її причини й виробітку рішення.

Багато компаній і Інтернет-провайдери мають штатну мережеву довідкову службу, готову вирішити проблеми користувачів. Багато великих IT-компаній мають у своєму розпорядженні довідкові служби, що спеціалізуються на конкретних пропонованих продуктах і технологіях. Наприклад, компанія Cisco Systems має довідкову службу, що сприяє в інтеграції устаткування Cisco у мережу й наступний його супровід.

Звернутися в довідкову службу можна декількома способами, у тому числі по електронній пошті, в онлайн-чаті й по телефоні. Електронна пошта зручна при нетермінових проблемах з мережами, а телефон і онлайн-чат краще підходять для екстрених ситуацій. Оперативний зв'язок особливо важливий у таких установах, як банки, де тривалий простій може обернутися величезними збитками.

При необхідності довідкова служба може одержати доступ до локального вузла за допомогою ПЗ для віддаленого доступу. Тим самим фахівці одержують можливість запустити діагностичні програми для взаємодії з вузлом і мережею без фізичного виїзду на об'єкт. У підсумку значно скорочується час очікування рішення проблеми, а довідкова служба встигає допомогти більшому числу користувачів.

Для кінцевого користувача особливо важливо повідомити довідковій службі максимум інформації. Довідковій службі буде потрібно інформація про всі використовувані сервіси й плани підтримки, а також докладні відомості про устаткування, порушеній проблемою. До цих відомостей можуть відноситися марка, модель і серійний номер пристрою, а також версія використовуваної на ньому мікропрограми або операційної системи. Також можуть знадобитися IP- і MAC-адреси несправного пристрою. Довідкова служба попросить надати конкретний опис проблеми з наступними відомостями:

– прояву проблеми;

– ким виявлена проблема;

– коли проявляється проблема;

– міри, початі для виявлення проблеми;

– результати вжитих заходів.

При повторному зверненні варто також мати інформацію про дату й час попереднього звернення, номері завдання й ПІБ фахівця. Необхідно перебувати поруч із устаткуванням, на якому виникла проблема, і бути готовим надати доступ до устаткування фахівцям довідкової служби, якщо це буде потрібно.

Організаційна структура довідкової служби звичайно підрозділяється на кілька рівнів знань і досвіду. Якщо персонал першого рівня не може розв'язати проблему самотужки, проблема передається на вищестоящий рівень. Фахівці більше високого рівня мають більше високу кваліфікацію й, на відміну від співробітників 1-го рівня, мають доступ до бази ресурсів і інструментальних засобів.

Відомості про взаємодію з довідковою службою завжди необхідно протоколювати в такий спосіб:

– час/дата звернення;

– ПІБ/код фахівця;

– предмет звернення;

– вжиті заходи;

– рішення / передача на більше високий рівень;

– наступні дії (повторні звернення).

При сприянні довідкової служби вдається швидко й легко усунути значну частину проблем. Після рішення проблеми не забудьте обновити документацію на майбутнє.

РОЗДІЛ 14. ПЛАНУВАННЯ ВІДНОВЛЕННЯ МЕРЕЖІ

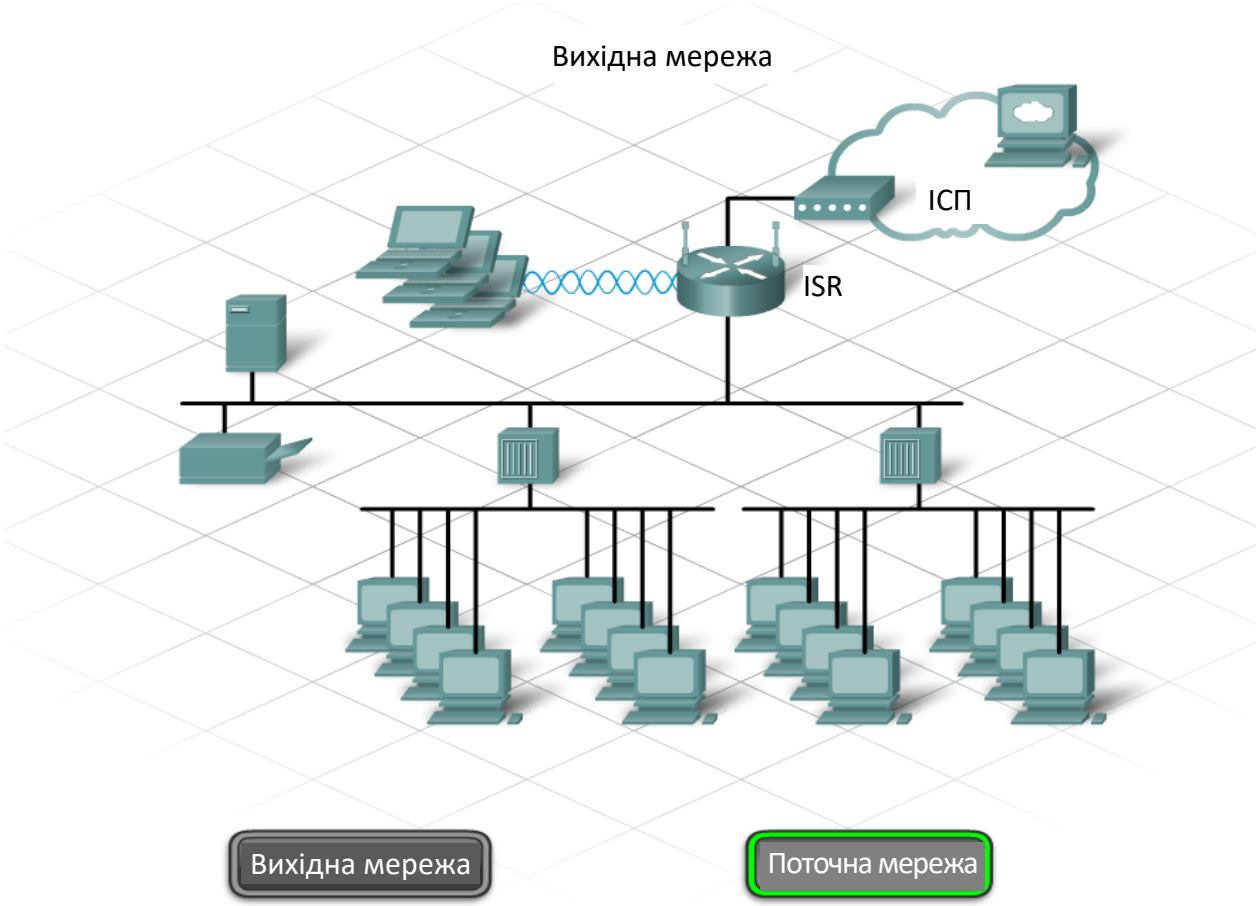
Огляд на місці

Коли невелика компанія швидко розростається, можливостей первісної мережі починає не вистачати. Співробітники компанії не завжди розуміють, як важливо спланувати відновлення мережі. Іноді для підключення нових користувачів просто додають різні мережеві пристрої або використовують пристрої іншої якості, від інших виробників, з іншими технологіями підключення до мережі. При додаванні кожного нового користувача якість існуючої мережі іноді знижується, система перестає підтримувати наявний трафік.

Більшість невеликих компаній починає замислюватися про перепланування мережі відповідно до нових вимог з того моменту, як починаються збої. Для консультації, установки й допомоги у відновленні мережі можна запросити Інтернет-провайдеру або постачальника послуг адміністрування.

Перед початком планування відновлення мережі на місце відправляється технічний фахівець, що виконує перевірку й документує наявну структуру мережі. Крім того, потрібно досліджувати й документувати фізичне розташування приміщень і визначити, де встановити нове обладнання.

а)



б)

Рисунок 14.1 – Вихідна й поточна мережа

Огляд місця установки надає проектувальникові мережі багато інформації і є вдалою початковою точкою проекту. Він показує, що вже встановлено, і дозволяє більш-менш точно визначити, що буде потрібно. Торговельний представник може приїхати на місце разом з технічним фахівцем і поговорити із клієнтом.

Крім того, у процесі огляду можна одержати й більше важливу інформацію про:

– кількість користувачів і типи устаткування;

– проектований ріст;

– поточне підключенні до Інтернету;

– вимоги додатків;

– існуючу мережеву інфраструктуру й фізичну схему мережі;

– потреби в нових службах;

– питання безпеки й охорони особистої інформації;

– очікування надійності й часу безперебійної роботи;

– бюджетні обмеження.

По можливості рекомендується одержати план по поверхам. Якщо ж ні, технічний фахівець може накреслити схему з розмірами й розташуванням всіх кімнат. Крім того, для визначення загальних вимог корисно скласти список наявного апаратного й програмного забезпечення.

При проведенні огляду технічний фахівець повинен бути готовий до всього. Мережі не завжди відповідають будівельним нормам і правилам, що відносяться до електропроводки, будинкам або вимогам по безпеці, або яким-небудь стандартам взагалі.

Іноді мережі розширюють як прийдеться, а в підсумку виходить суміш різних технологій і протоколів. Прибувши на підприємство клієнта, технічний фахівець повинен ретельно оглянути мережу й перевірити налаштування комп'ютера. Іноді присутні очевидні проблеми, наприклад, непомічені кабелі, низький рівень фізичної безпеки мережевих пристроїв, недолік резервного живлення або джерел безперебійного живлення найважливіших пристроїв. Ці умови потрібно відзначити в технічному звіті так само, як і інші вимоги, певні в процесі огляду й спілкування із клієнтом.

Рисунок 14.2 – Вимоги до мережі

Після завершення огляду технічному фахівцеві необхідно разом із клієнтом переглянути результати й переконатися, що нічого не упущене й у звіті немає помилок. Звіт, що містить тільки точні дані, є відмінною основою нової конструкції мережі.

Таблиця 14.1 – Вимоги до клієнтів мережі

Вимоги	**Відповідь**
Кількість користувачів	У нас 19 користувачів.
Обладнання постачальника послуг	Ми використовуємо DSL, обладнання належить постачальнику послуг.
Міжмережевий екран	У нас використовується інтегрований із мережевий екран.
Локальний сервер	Ми плануємо розмістити в компанії файловий сервер.
Веб-сервери або поштові сервери	У нас немає веб-серверів або поштових серверів.

Продовження таблиці

Вимоги до додатків	У нас використовуються текстові редактори, електронні таблиці та графічні додатки. У майбутньому ми плануємо використовувати IP-телефони.
Дротовий/Бездротовий	Нам необхідне і дротове, і бездротове підключення.
Число дротових настільних комп'ютерів	У нас 15 настільних комп'ютерів.
Кількість принтерів	У нас немає мережевих принтерів.
Бездротові портативні ПК	У нас 4 бездротових портативних ПК.
Площа бездротової локальної мережі	Площа наших офісів складає 15 000 квадратних футів.

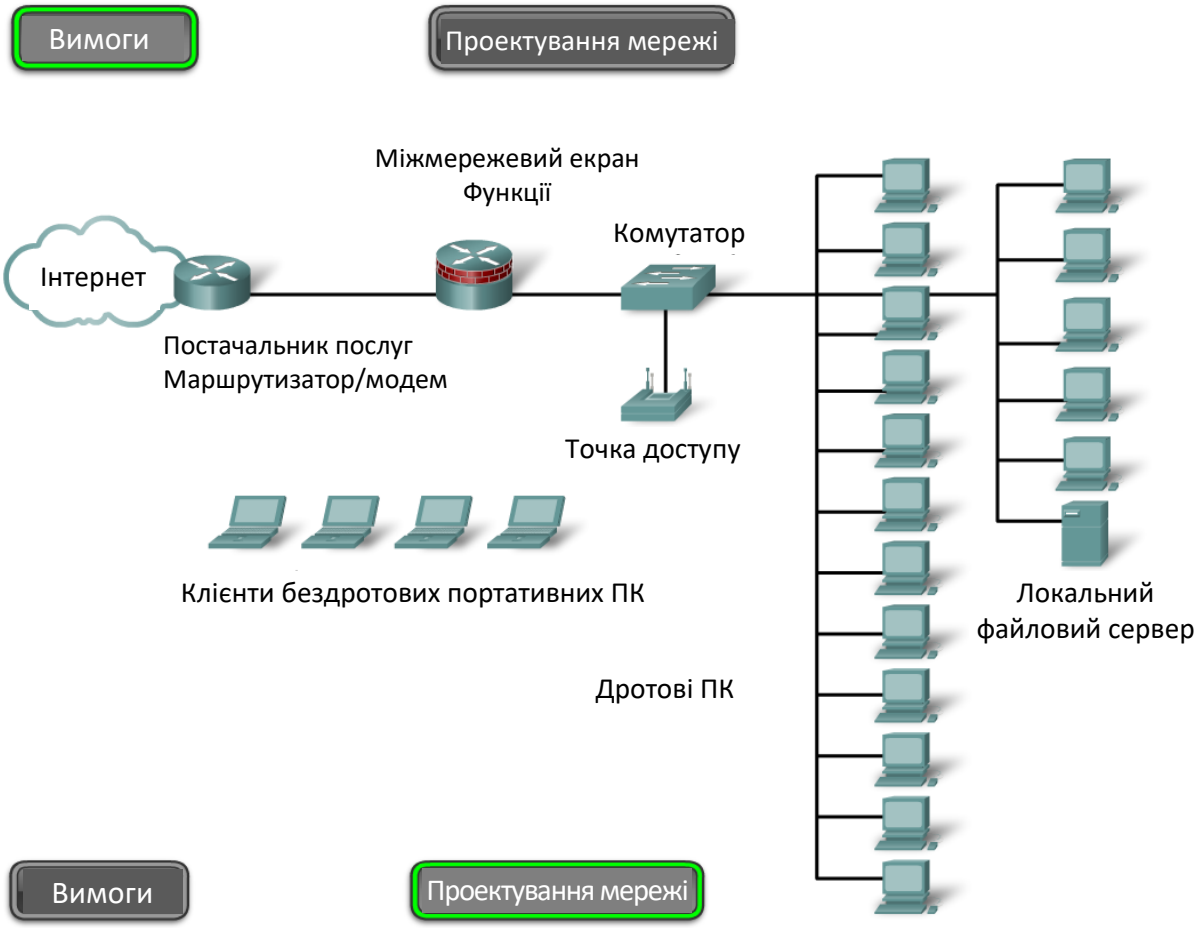


Рисунок 14.3 – Проектування мережі

Фізична й логічна топологія

Документувати потрібно фізичну й логічну топологію існуючої мережі. У процесі огляду технічний фахівець збирає інформацію, що дозволяє створити фізичну й логічну карту мережі. Фізична топологія – це схема реального розташування кабелів, комп'ютерів і інших периферійних пристроїв. Логічна топологія документує шлях даних мережею й місця, де виконуються функції мережі (наприклад, маршрутизація).

У дротовій мережі карта фізичної топології містить у собі комутаційну шафу й проводку до окремих станцій кінцевого користувача. У бездротовій мережі карта фізичної топології містить у собі комутаційну шафу й точку доступу. Оскільки проведення відсутні, у фізичній топології вказується область покриття бездротового сигналу.

Логічна топологія дротової й бездротової мережі звичайно збігається. До неї входить система присвоєння імен і адресації кінцевих станцій рівня 3, шлюзів маршрутизатора й інших мережевих пристроїв, незалежно від фізичного розташування. На ній зазначені положення, де виконується маршрутизація, перетворення мережевих адрес і фільтрація міжмережевого екрана.

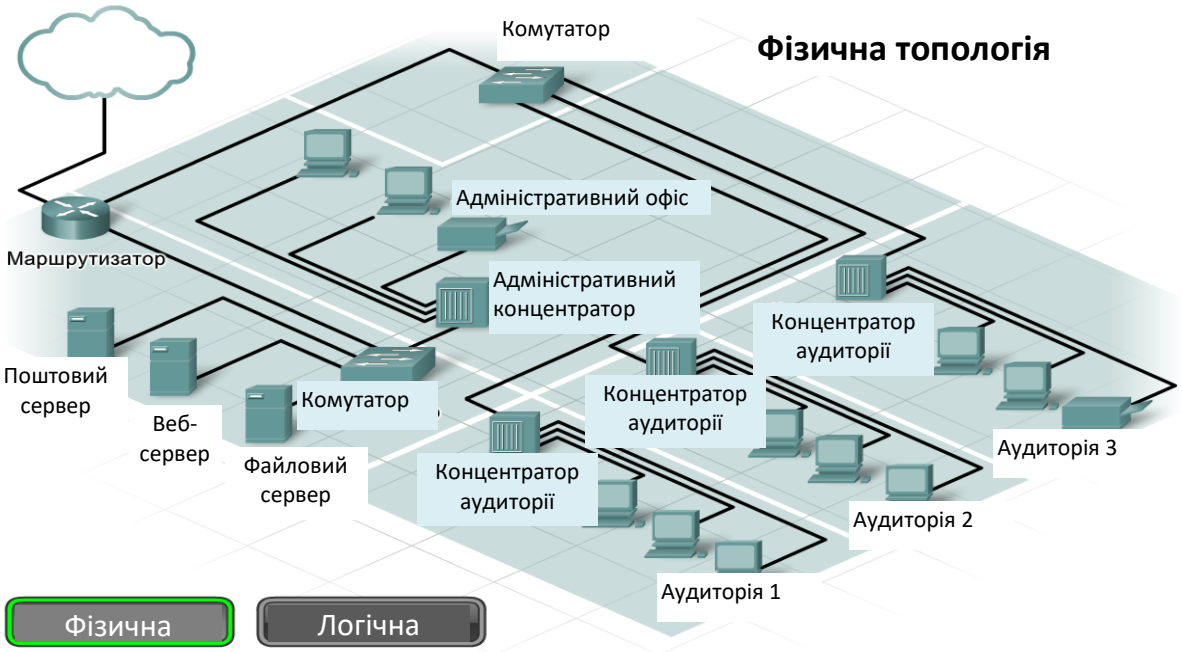
Документування мережевих вимог

Крім створення топологічних карт існуючої мережі, важливо одержати додаткову інформацію про вже встановлені вузли й мережеві пристрої. Її потрібно занести в короткий інвентарний список. Крім уже встановленого устаткування, впишіть параметри запланованого в найближчому майбутньому розширення.

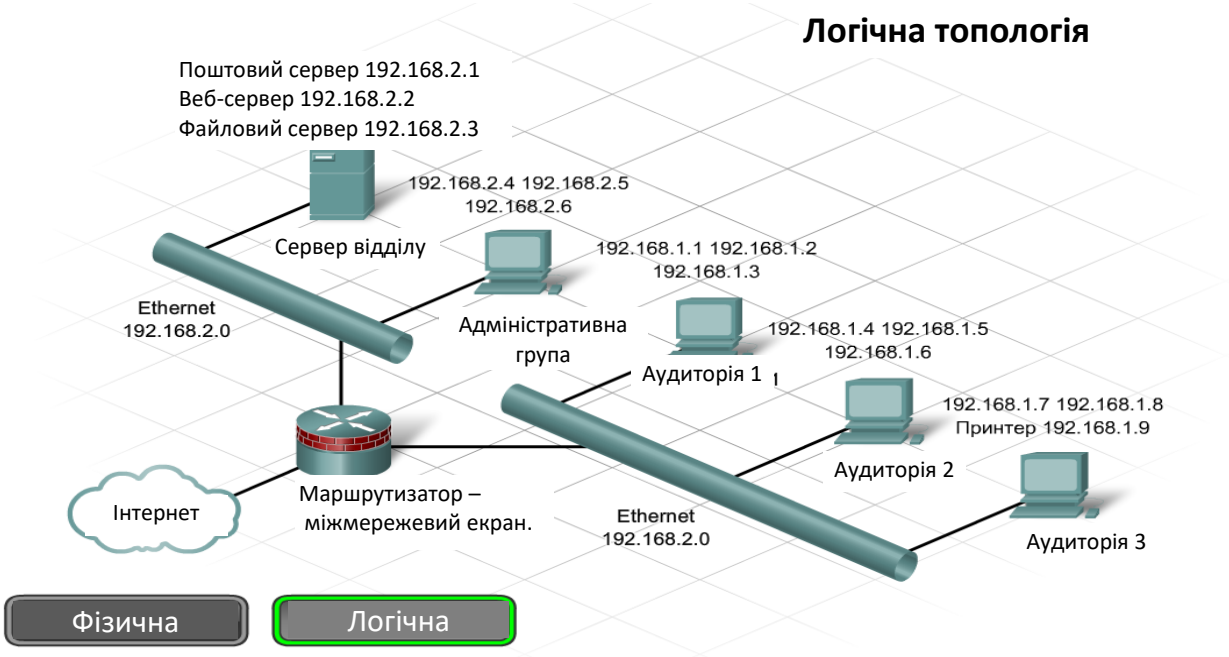
Ця інформація допоможе конструкторові мережі визначити потреби в новому обладнанні й оптимальній структурі мережі з урахуванням запланованого розширення.

В інвентарний список установлених мережевих пристроїв потрібно включити:

– назви пристроїв; положення; марки й моделі; операційна система; дані про логічну адресацію; методи підключення; дані про безпеку.



а)



б)

Рисунок 14.4 – Фізична й логічна структура мережі

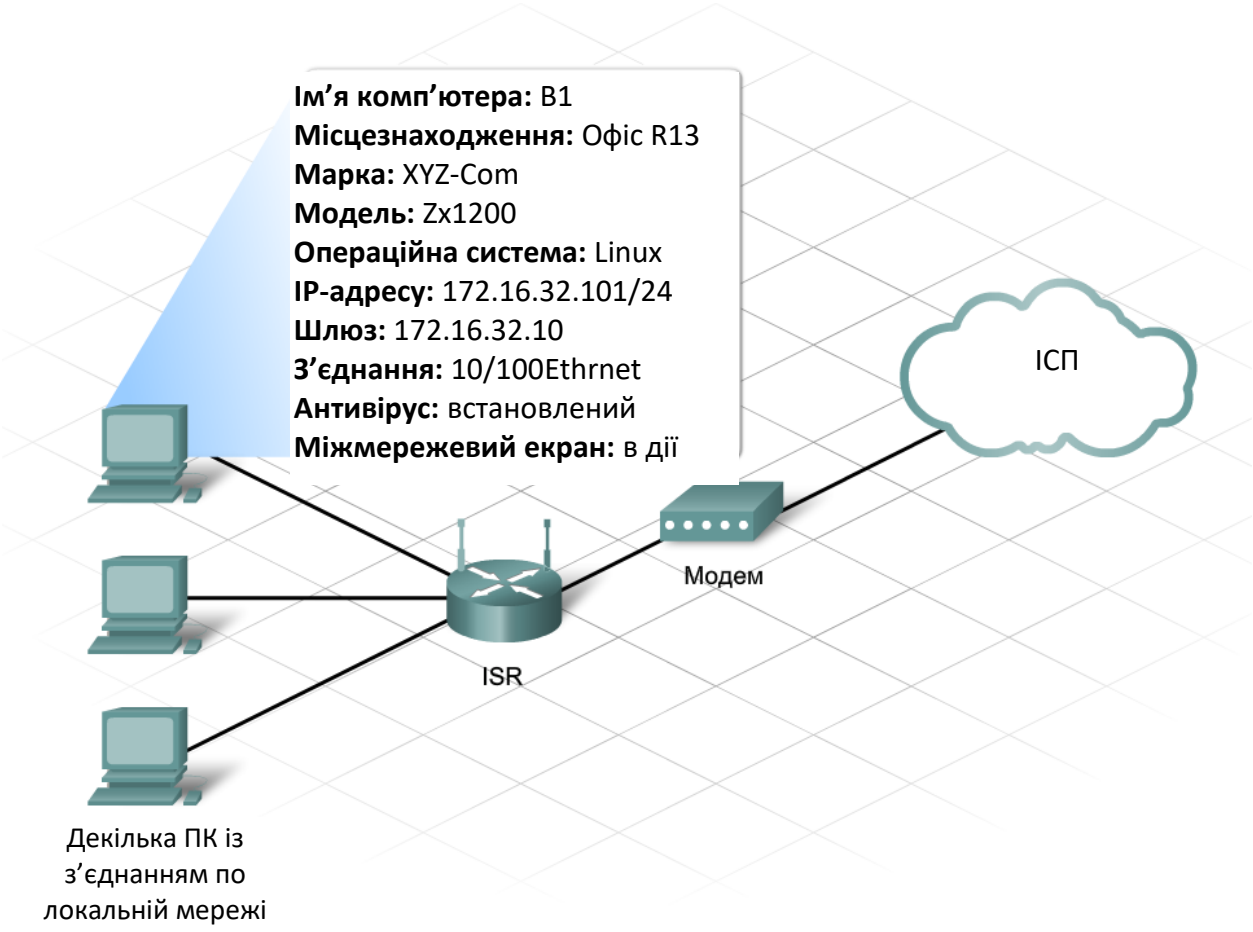


Рисунок 14.5 – Інвентарний список установлених мережевих пристроїв

Відновлення мережі

Відновлення мережі вимагає серйозного планування. Як і в будь-якому іншому проекті, потрібно визначити потреби й спланувати процес від початку до кінця. Гарний план проекту допоможе виявити всі сильні й слабкі місця, можливості й ризики (SWOT). У плані необхідно чітко вказати завдання й порядок їхнього виконання.

Приклади правильного планування:

– спортивні команди, що випливають з плану гри;

– будівельники, що працюють по кресленнях;

– церемонії й зустрічі, що проходять відповідно до повістки дня.

Мережа, що представляє собою суміш різнорідних пристроїв, технологій і протоколів, звичайно є результатом помилок у первісному плані. Такі мережі часто простоюють, їх важко обслуговувати й ремонтувати.

Планування відновлення мережі починається після завершення огляду й складання звіту. Існує п'ять чітко певних етапів:

Етап 1: збір вимог

Зібрана при огляді й спілкуванні із клієнтом інформація аналізується, визначаються вимоги до мережі. Аналіз проводить група конструкторів Інтернет-провайдеру. Вони створюють звіт про аналіз

Етап 2: вибір і конструювання

Вибір пристроїв і кабелів на основі вимог зі звіту про аналіз. Створення декількох варіантів конструкції й регулярний обмін даними між учасниками проекту. Це дозволяє членам групи подивитися на ЛОМ у перспективі й оцінити можливі варіанти продуктивності й вартості. Саме на цьому етапі можна виявити й усунути всі недоліки конструкції.

Крім того, у процесі створюються й перевіряються прототипи. Вдалий прототип – гарний показник того, як буде працювати нова мережа.

Коли клієнт схвалить конструкцію, можна почати неї впроваджувати.

Етап 3: впровадження

Якщо перші два етапи виконані правильно, фаза впровадження пройде без збоїв. Якщо на ранніх етапах щось було пропущено, у фазі впровадження потрібно усунути ці недоліки. Наявність гарного графіка впровадження, що залишає час на несподівані події, дозволяє звести до мінімуму перешкоди в роботі клієнта. Для успіху проекту в процесі установки надто важливо постійно спілкуватися із клієнтом.

Етап 4: експлуатація

Мережа вводиться в експлуатацію в так званому робочому оточенні. Уважається, що до цього вона перебуває на етапі перевірки або впровадження.

Етап 5: перевірка й оцінка

Коли мережа заробить, потрібно буде перевірити й оцінити конструкцію й впровадження. Це рекомендується робити в наступному порядку:

– зрівняйте досвід користувача з наведеними в документах цілями й оцініть, чи підходить конструкція для роботи;

– зрівняйте запроектовані конструкції й вартість із реальними результатами розгортання, що дозволить застосувати досвід даного проекту в майбутньому;

– простежте за роботою й зафіксуйте зміни. Це гарантує, що всі характеристики системи документуються й включаються у звіт.

Ретельне планування важливо на кожному етапі – це дозволяє впевнено впроваджувати проект і успішно виконувати установку. У плануванні часто беруть участь технічні фахівці, оскільки вони займаються всіма етапами відновлення.

Фізичне середовище

Вибираючи устаткування й конструкцію нової мережі, конструктор мережі, насамперед, оглядає наявні системи й кабелі. До систем відноситься фізичне середовище, приміщення далекого зв'язку й існуюча проводка. Приміщення далекого зв'язку або комутаційна шафа в невеликій мережі, розташованої на одному поверсі, звичайно називається головною розподільною шафою (MDF).

Звичайно MDF складається з багатьох мережевих пристроїв, включаючи комутатори або концентратори, маршрутизатори, точки доступу й т.д. Саме тут всі мережеві кабелі сходяться в одній точці. Часто в MDF перебуває точка доступу в мережу (POP) Інтернет-провайдеру, де локальна мережа підключається до Інтернету через постачальника телекомунікаційних послуг.

Додаткові комутаційні шафи (IDF) називаються проміжними розподільними шафами (IDF). Звичайно IDF менше MDF і підключаються до MDF.

У багатьох невеликих компаній немає ні телекомунікаційних приміщень, ні шаф. Мережеве устаткування можна встановити на столі або іншій поверхні, а проведення просто провести по підлозі. Мережеве устаткування необхідно встановити надійно. При розширенні мережі важливо передбачити створення телекомунікаційного приміщення, оскільки це забезпечить безпека й надійність мережі.

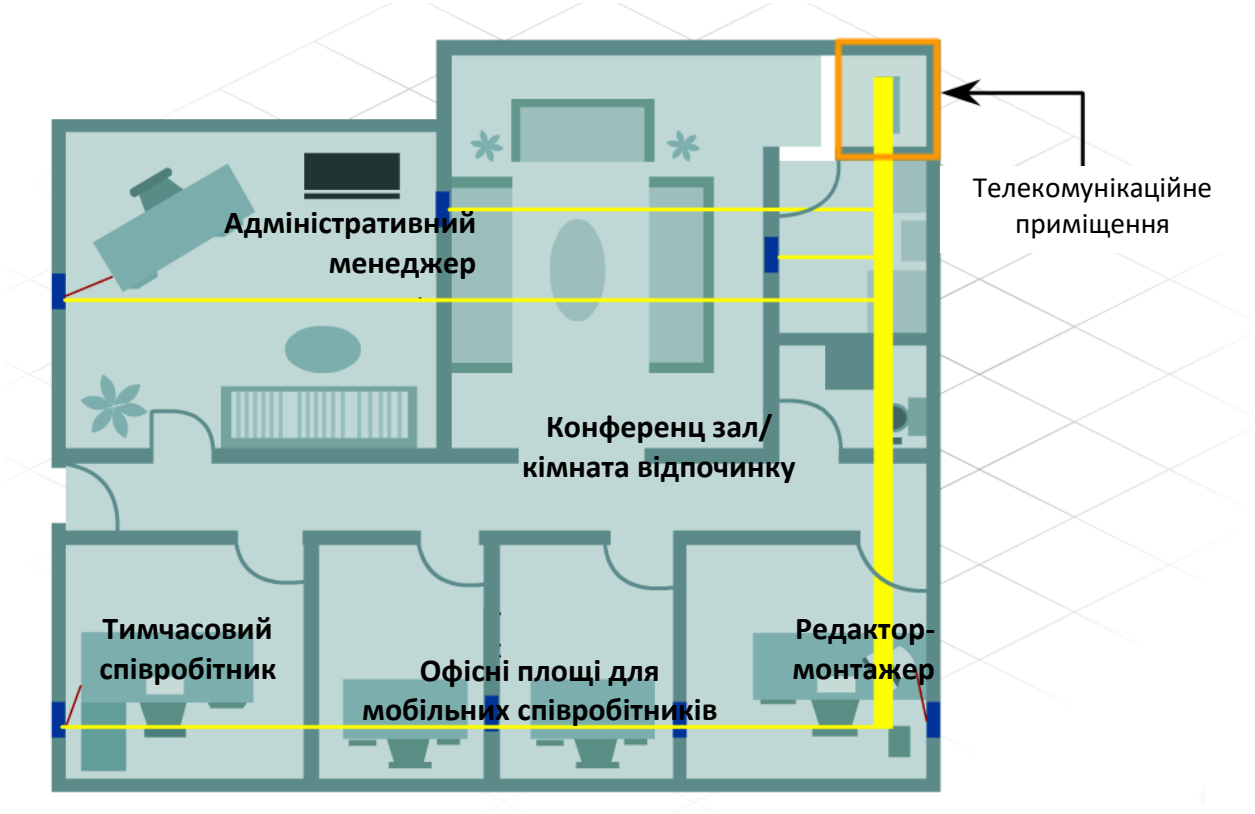


Рисунок 14.6 – Планування мережі у фізичному середовищі

Стандарти ISO описують головні розподільні шафи (Main Distribution Frame – MDF) і проміжні розподільні шафи (Intermediate Distribution Frame – IDF) за допомогою різної термінології. Головні й проміжні розподільні шафи можуть також називатися комутаційними шафами.

Головна розподільна шафа = розподільна шафа всього будинку

Проміжна розподільна шафа = розподільна шафа поверху

Питання прокладки кабелів

Якщо наявні кабелі не відповідають специфікації нового обладнання, потрібно запланувати й установити нові. Стан існуючих кабелів можна швидко визначити методом огляду мережі. При плануванні установки мережевих кабелів потрібно врахувати чотири моменти:

– робочі місця користувачів;

– телекомунікаційне приміщення;

– магістральна область;

– область розподілу.

Існує багато різних типів мережевих кабелів. Одні поширені більше, інші – менше.

Екранована кручена пари (STP). Звичайно використовуються кабелі категорії 5, 5e або 6 з екраном з фольги, що захищає від зовнішніх електромагнітних перешкод (ЕМП). Максимальна відстань – близько 100 метрів.

Неекранована кручена пари (UTP). Звичайно використовуються кабелі категорії 5, 5e або 6 без додаткового екранування від ЕМП, але більше дешеві. Кабелі не слід прокладати поруч із джерелами електричних перешкод. Максимальна відстань – близько 100 метрів.

Коаксіальний кабель. Кабель із цільною мідною жилою й декількома захисними шарами, включаючи полівінілхлорид (ПВХ), оплітку й пластикове покриття. Максимальна відстань – до декількох кілометрів, залежно від області застосування.

Оптоволоконний кабель. У середовищі, де немає ЕМП, передає дані швидше й далі, ніж мідний кабель. Залежно від типу оптоволокна максимальна відстань – до декількох кілометрів.

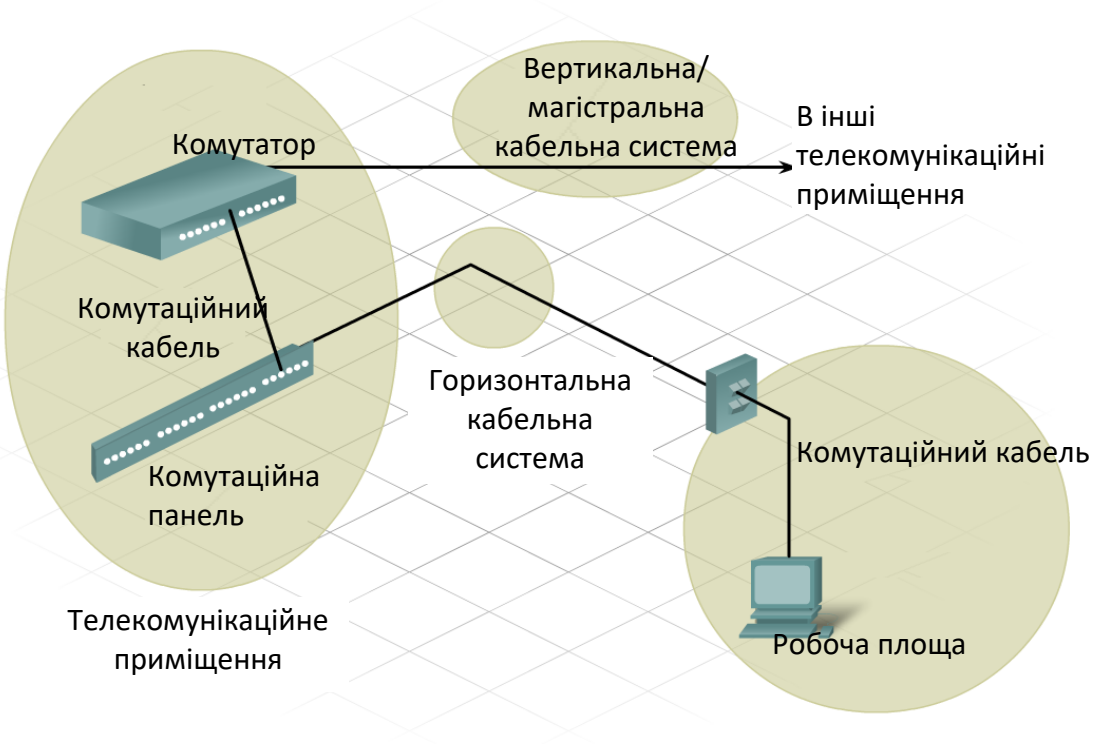


Рисунок 14.7 – Види кабельних систем

У світі є кілька організацій, що надають специфікації кабелів ЛОМ.

Telecommunications Industry Association (TIA) і Electronic Industries Alliance (EIA) спільно працювали над специфікацією кабелів ЛОМ TIA/EIA. Дві найпоширеніші специфікації TIA/EIA – стандарти 568-A і 568-B. Обоє звичайно передбачають використання однакового кабелю категорії 5 або 6, але з різними колірними кодами терміналів.

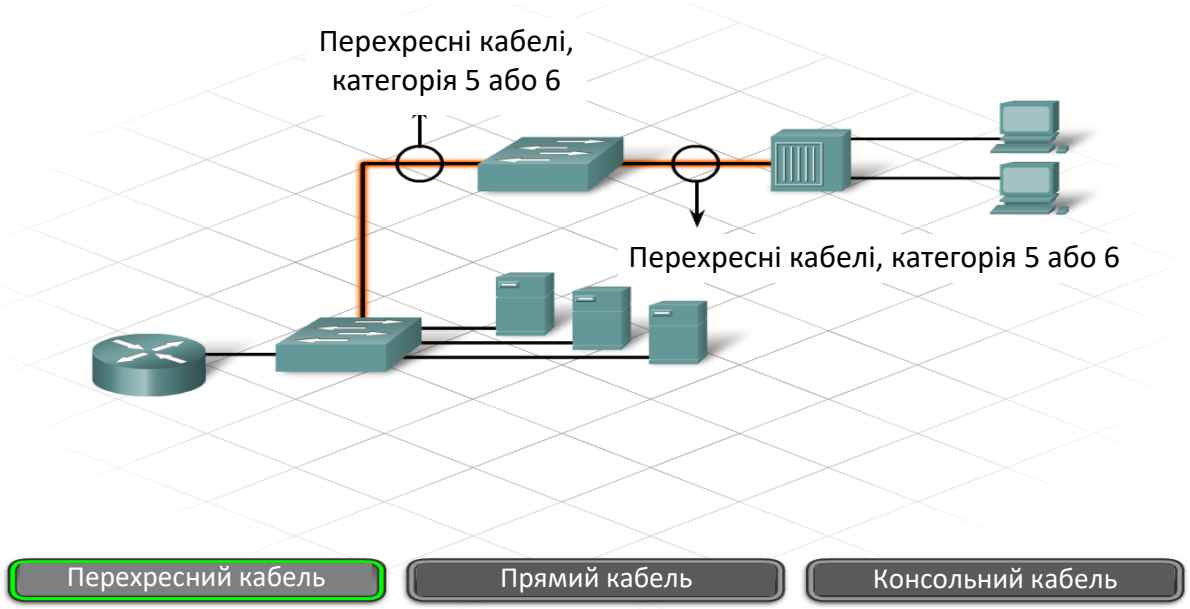
У мережах використовуються три різних типи кабелів "кручена пари".

– Прямий кабель. З'єднує різні пристрої, наприклад, комутатор і комп'ютер або комутатор і маршрутизатор.

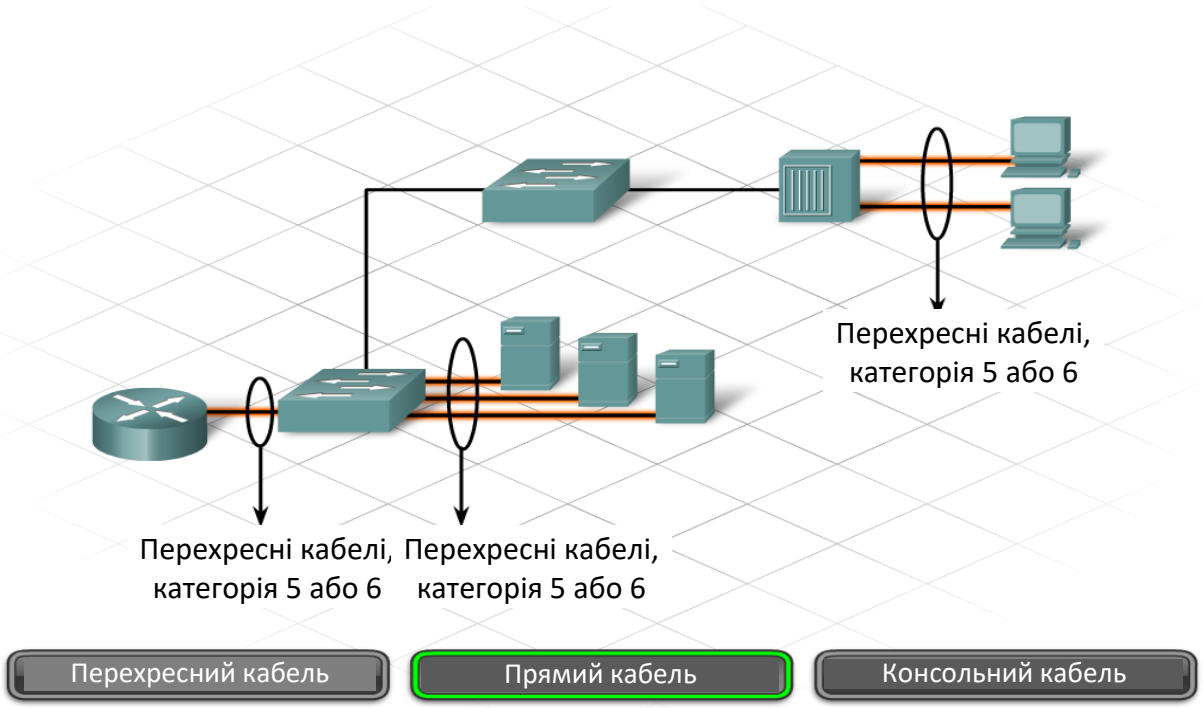
– Перехресний кабель. З'єднує однакові пристрої, наприклад, два комутатори або два комп'ютери.

– Консольний (або "перевернений") кабель. З'єднує комп'ютер з консольним портом маршрутизатора або комутатора для початкової конфігурації.

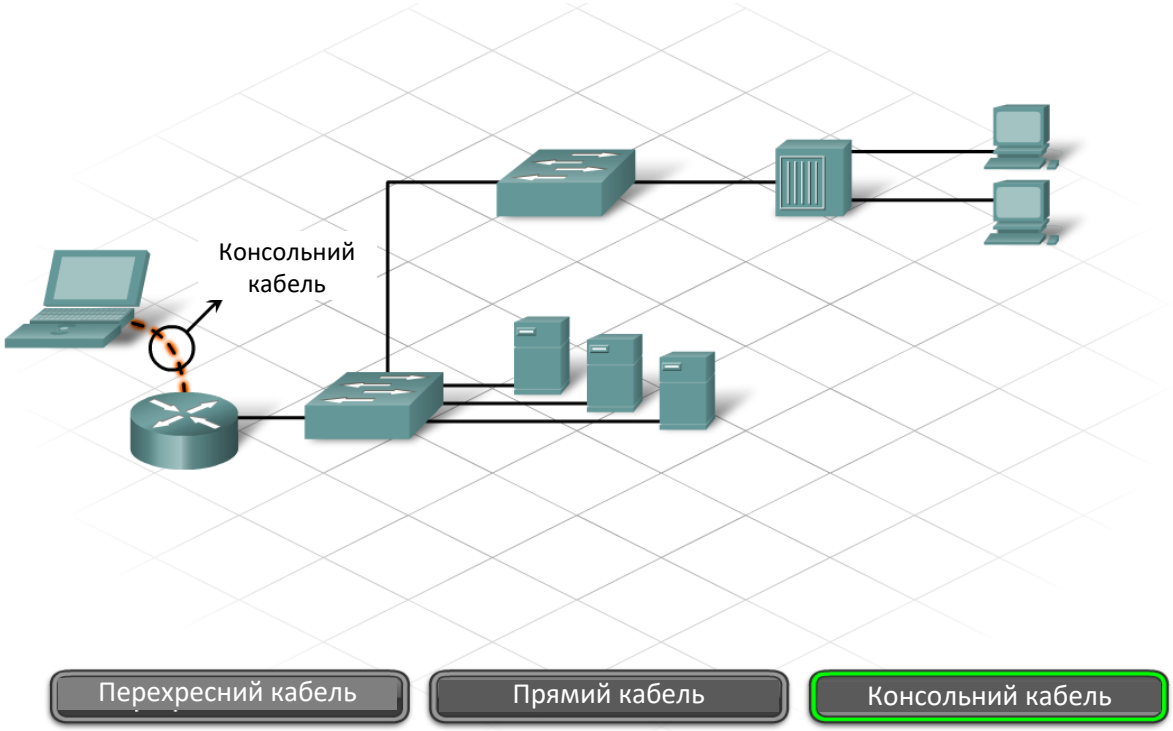
Крім того, у мережах часто зустрічається послідовний кабель. Звичайно таким кабелем маршрутизатор з'єднується з портом Інтернет. Це може бути роз’єми телефонної компанії, кабельній компанії або приватній мережі Інтернет-провайдеру.



а)



б)



в)

Рисунок 14.8 – Три різних типи кабелів "кручена пари"

Структурований кабель

При розробці проекту прокладки структурованих кабелів, насамперед, потрібно одержати точний поверховий план. З його допомогою технічні фахівці зможуть знайти місце для можливої установки комутаційних шаф, прокладки кабелів і місця із джерелами електричних перешкод, яких потрібно уникати.

Після того, як технічний фахівець визначить і перевірить місцезнаходження мережевих пристроїв, можна буде намалювати на поверховому плані майбутню мережу. Зокрема, у документи потрібно включити кілька важливих моментів.

Сполучні кабелі: короткий кабель, що йде від комп'ютера до стінної панелі на місці роботи користувача.

Горизонтальний кабель: кабель, що йде від стінної панелі до IDF в області розподілу.

Вертикальний кабель: кабель від IDF до MDF в області магістралі організації.

Магістральний кабель: частина мережі, по якій проходить основна частина трафіку.

Положення комутаційного відсіку: область, де збираються кабелі, що йдуть до концентратора або комутатора.

Система керування кабелями: серії лотків або джгутів, що направляють і захищають кабелі.

Система маркування кабелів: підходяща система або схема маркування, призначене для ідентифікації кабелів.

Питання електропостачання: у приміщеннях повинне бути досить розеток для мережевого устаткування.

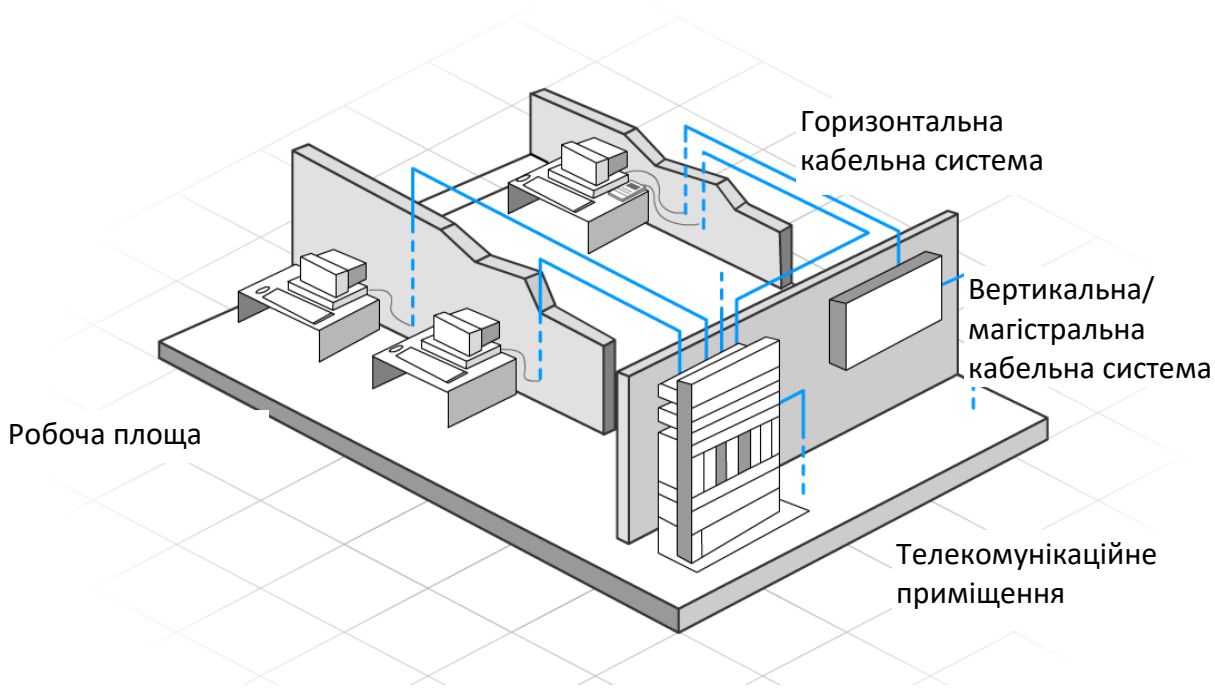


Рисунок 14.9 – Поверховий план

Придбання устаткування

При плануванні відновлення мережі групі Інтернет-провайдеру потрібно розглянути питання закупівлі нового обладнання й обслуговування

нового й існуючого устаткування. У цілому, варіантів одержання устаткування два:

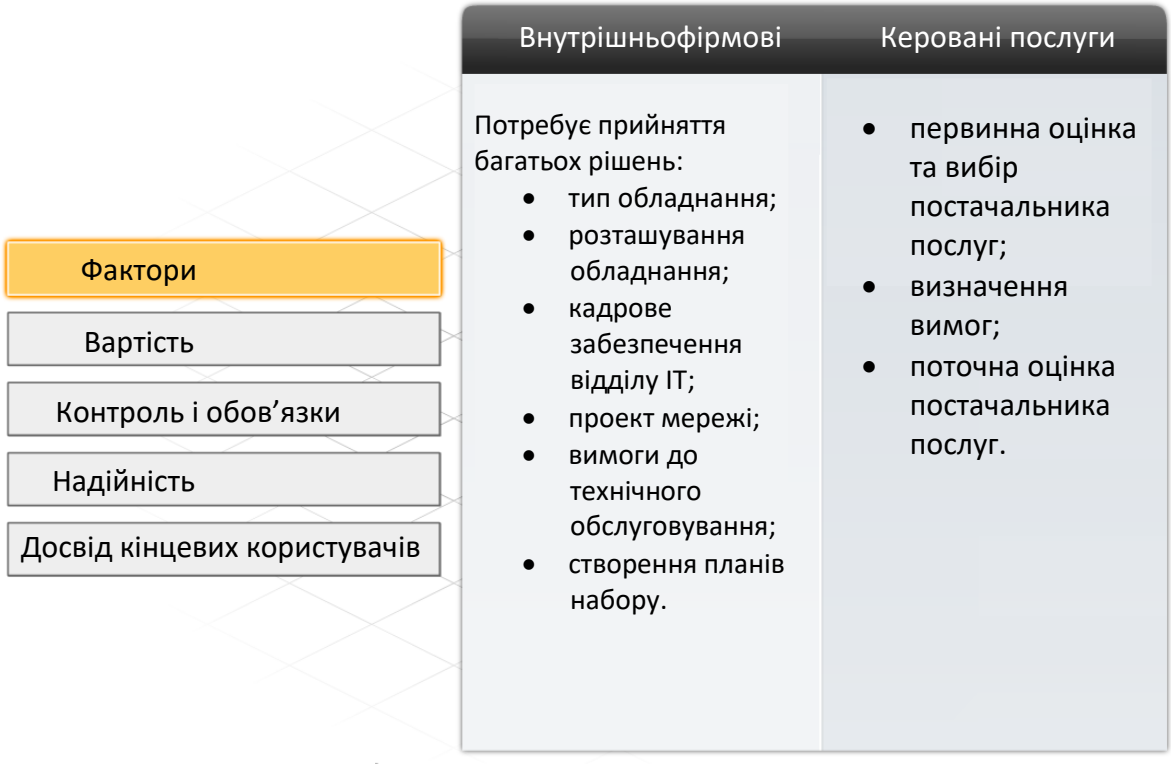
– послуги адміністрування – у такому варіанті клієнт одержує устаткування від Інтернет-провайдеру за договором оренди або іншій угоді, а Інтернет-провайдер займається відновленням і обслуговуванням;

– придбання – у такому варіанті клієнт закуповує все устаткування й сам займається відновленням, гарантіями й обслуговуванням.

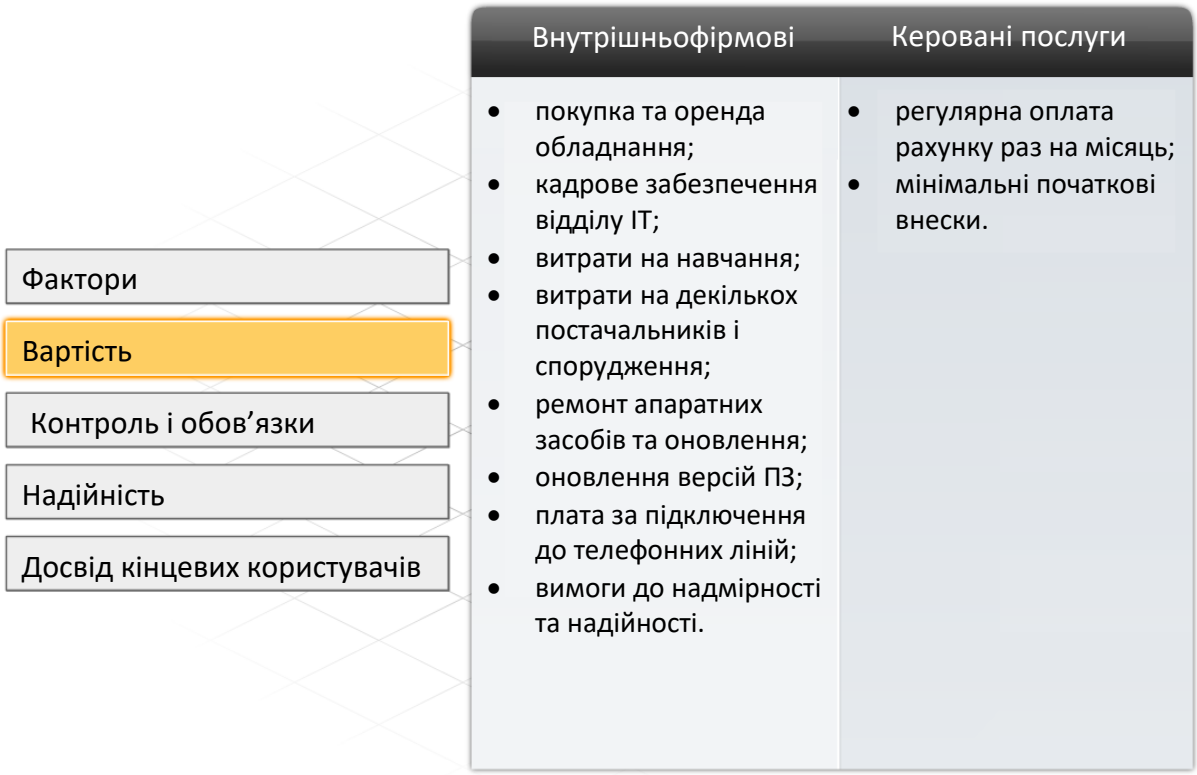
При придбанні устаткування велике значення має ціна. Правильно проведений аналіз витрат у різних варіантах придбання – гарна основа для остаточного рішення.

При виборі послуг адміністрування виникають витрати на оренду й обслуговування відповідно до угоди про рівень обслуговування (SLA).

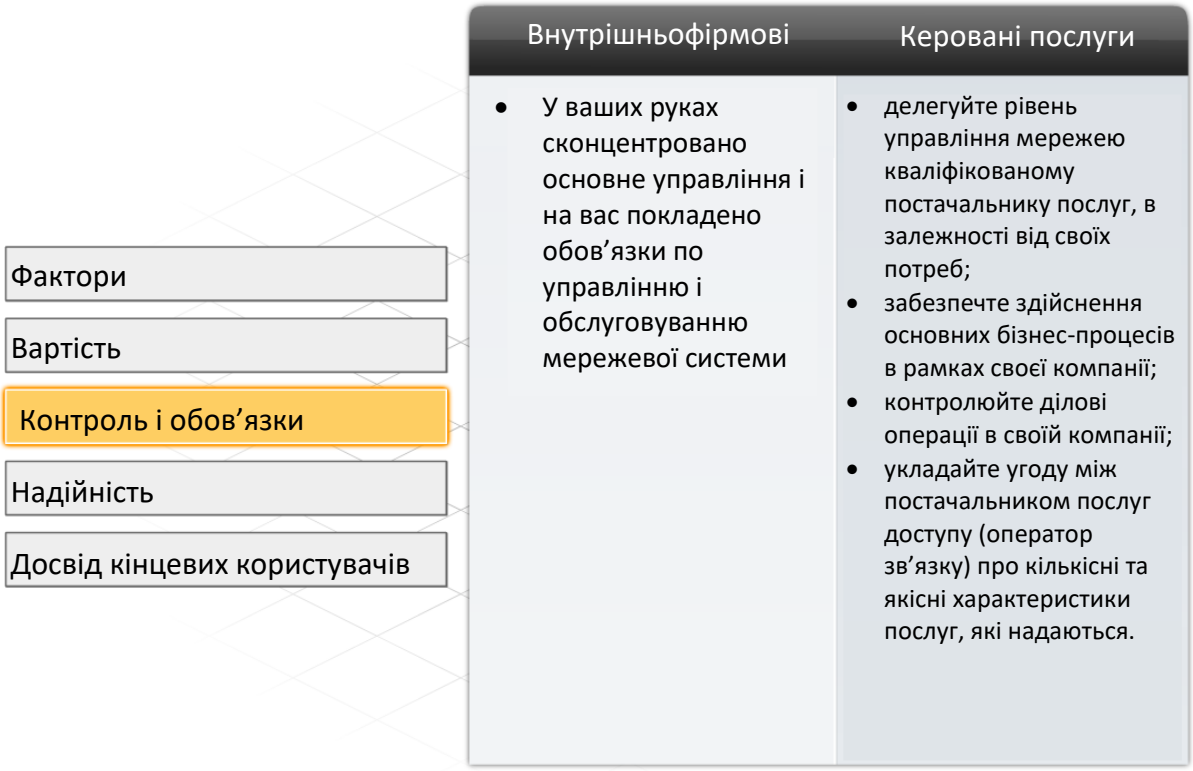
Купуючи устаткування, клієнт повинен урахувати його вартість, гарантійне покриття, сумісність із існуючим устаткуванням і витрати на відновлення й обслуговування. Все це коштує грошей, і все потрібно проаналізувати при виборі найбільш вигідного варіанта.



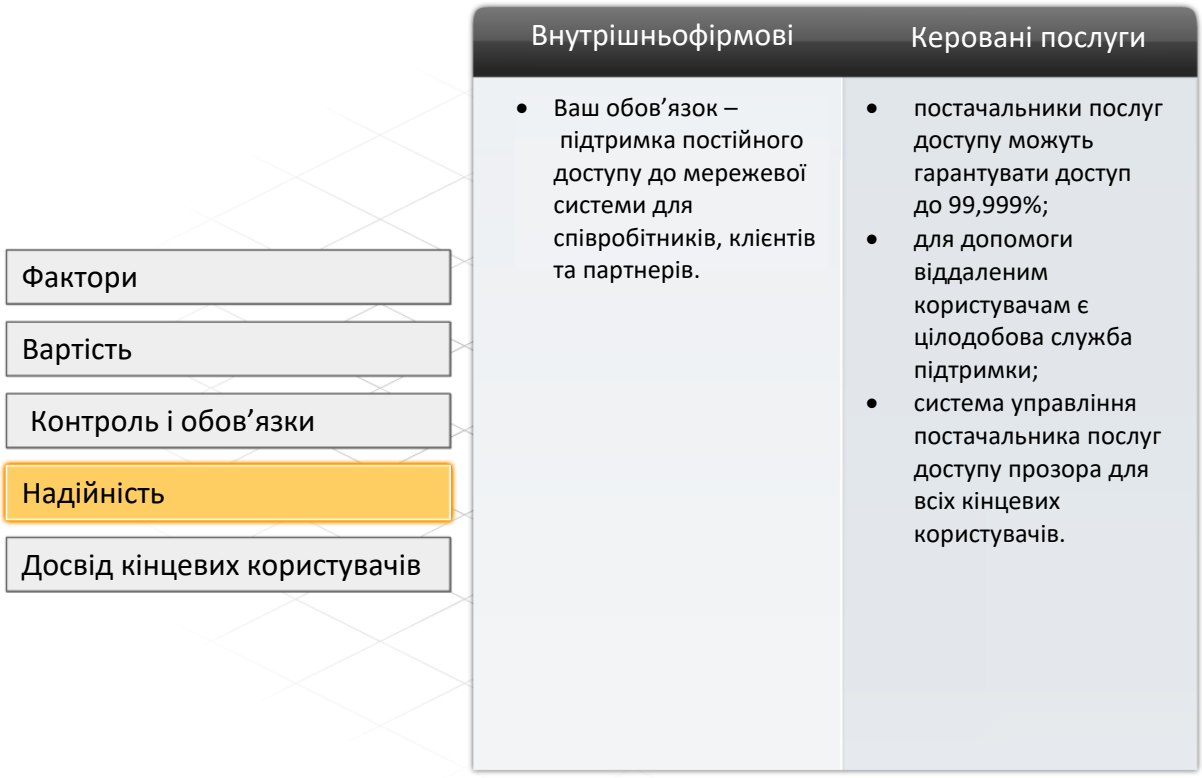
а)


Фактори
Вартість
Контроль і обов’язки
Надійність
Досвід кінцевих користувачів
Внутрішньофірмові
Керовані послуги
покупка та оренда обладнання;
кадрове забезпечення відділу IT;
витрати на навчання;
витрати на декількох постачальників і спорудження;
ремонт апаратних засобів та оновлення;
оновлення версій ПЗ;
плата за підключення до телефонних ліній;
вимоги до надмірності та надійності.
регулярна оплата рахунку раз на місяць;
мінімальні початкові внески.

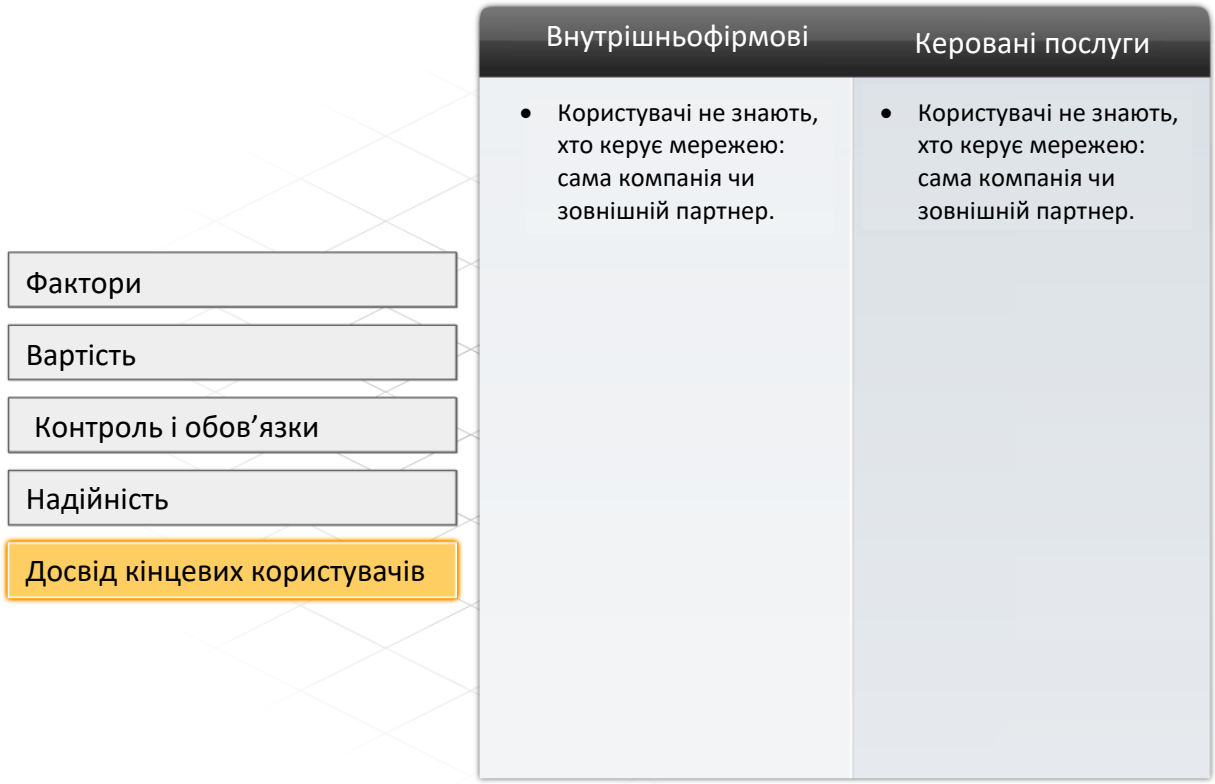
б)


Фактори
Вартість
Контроль і обов’язки
Надійність
Досвід кінцевих користувачів
Внутрішньофірмові
Керовані послуги
У ваших руках сконцентровано основне управління і на вас покладено обов’язки по управлінню і обслуговуванню мережевої системи
делегуйте рівень управління мережею кваліфікованому постачальнику послуг, в залежності від своїх потреб;
забезпечте здійснення основних бізнес-процесів в рамках своєї компанії;
контролюйте ділові операції в своїй компанії;
укладайте угоду між постачальником послуг доступу (оператор зв’язку) про кількісні та якісні характеристики послуг, які надаються.

в)



г)



д)

Рисунок 14.10 – Придбання устаткування

Вибір мережевих пристроїв

Проаналізувавши вимоги, конструктори рекомендують клієнтові відповідні мережеві пристрої для підключення й підтримки роботи нової мережі.

У модемних мережах для підключення використовуються самі різні пристрої. У кожного є певні можливості контролю переміщення даних мережею. Як правило, ніж вище рівень пристрою в моделі OSI, тим різноманітніше його функції. Це означає, що пристрій вищого рівня краще аналізує трафік і передає його на основі інформації, що низькорівневим пристроям недоступна. Наприклад, концентратор рівня 1 може тільки передавати дані всім портам, а комутатор рівня 2 фільтрує дані й передає тільки порту, з'єднаному з адресатом (на основі MAC-адреси).

По мірі вдосконалювання продукції різниця між концентраторами й комутаторами розмивається. Залишається одна проста відмінність: комутатори ЛОМ забезпечують зв'язок усередині локальної мережі організації, а маршрутизатори зв'язують локальні й глобальні мережі.

Крім комутаторів і маршрутизаторів для ЛОМ існують і інші варіанти підключення. Бездротові точки доступу дозволяють комп'ютерам і іншим пристроям (наприклад, ручним IP-телефонам) підключатися до мережі без використання проводів або користуватися одним широкополосним з'єднанням.

Міжмережеві екрани захищають від мережевих погроз і забезпечують безпеку додатків і зв'язку, контролюють і ізолюють мережу. Інтернет-провайдери використовують об'єднані в одному мережевому пристрої комутатори, маршрутизатори, точки доступу й міжмережеві екрани.

Вибір пристроїв ЛОМ

Хоча зв'язок на рівні доступу до мережі забезпечують і концентратори, і комутатори, для підключення пристроїв до ЛОМ краще вибрати другий варіант. Комутатори дорожче, але й значно ефективніше й, отже, вигідніше. Як правило, концентратори використовують тільки в дуже

невеликих ЛОМ із невеликою пропускною здатністю або при обмеженому бюджеті.

Вибираючи комутатор для конкретної ЛОМ, потрібно врахувати трохи факторів. Зокрема, це:

– швидкість і типи портів/інтерфейсів;

– розширюваність;

– керованість;

– ціна.

Швидкість і типи портів/інтерфейсів

При наявності пристроїв рівня 2, що підтримують більшу швидкість, можна розширювати мережу без заміни центральних пристроїв.

При виборі комутатора важливо визначити кількість і тип портів.

Конструктори мережі повинні ретельно продумати необхідну кількість портів UTP і/або оптоволоконних портів. Важливо врахувати, скільки приблизно портів знадобиться для розширення мережі.

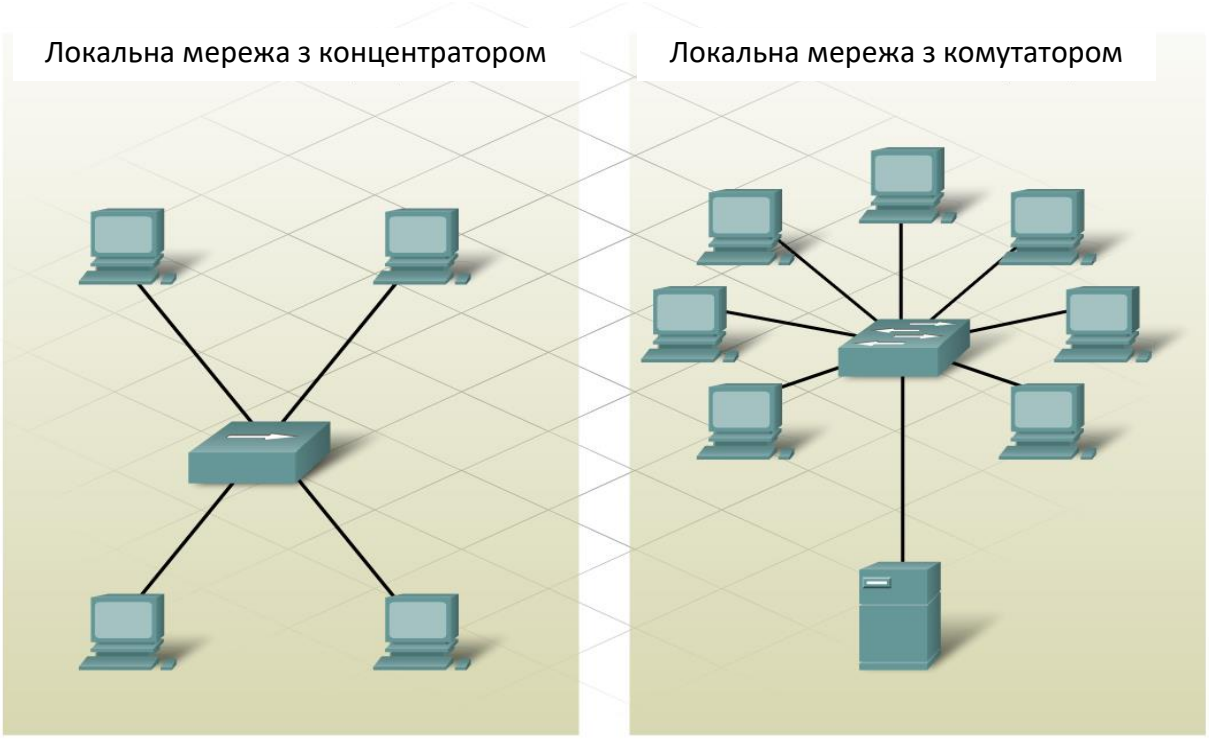


Рисунок 14.11 – Заміна концентратора на комутатор

Розширюваність

Мережеві пристрої випускаються в блоковій і модульній конфігурації. У блоковій конфігурації передбачені певна кількість і тип портів або інтерфейсів. У модульних пристроїв є слоти розширення, що дозволяють додавати нові модулі. Більшість модульних пристроїв поставляється з базовим набором портів і слотів розширення.

Звичайно до слотів розширення підключають оптоволоконні модулі для пристроїв з наявними портами UDP. Використання модульних комутаторів – вигідний спосіб масштабування ЛОМ.

Керованість

Керований комутатор дозволяє контролювати окремі порти або пристрій у цілому. Типова система контролю дозволяє відслідковувати роботу й міняти налаштування пристрою. Продуктивність і безпека керованого пристрою можна відслідковувати. Як правило, у нього є більше зроблені функції моніторингу й забезпечення безпеки.

Наприклад, порти керованого комутатора можна включати й відключати. Крім того, адміністратори можуть вибирати комп'ютери або пристрої, яким можна підключатися до порту.

Вартість

Вартість комутатора залежить від ємності й функцій. Поняття "ємність" містить у собі кількість і типи портів, а також загальна пропускна здатність. Крім того, на вартість впливають можливості мережевого керування, убудовані технології безпеки й додаткові, більше зроблені, технології комутування.

Рисунок 14.12 – Вимоги до мережі

При простій калькуляції вартості кожного порту може здатися, що вигідніше всього встановити один великий централізований комутатор. Однак цю очевидну економію можуть знизити витрати на довгі кабелі, використовувані для підключення кожного пристрою в мережі до одного комутатора. Даний варіант потрібно зрівняти з вартістю декількох менших комутаторів, підключених до центрального комутатора декількома кабелями.

Крім того, при розгортанні декількох невеликих пристроїв замість одного великого скорочується домен збоїв. Це область мережі, на яку впливає неполадка конкретного мережевого пристрою.

Вибравши комутатори для ЛОМ, потрібно підібрати підходящий для клієнта маршрутизатор.

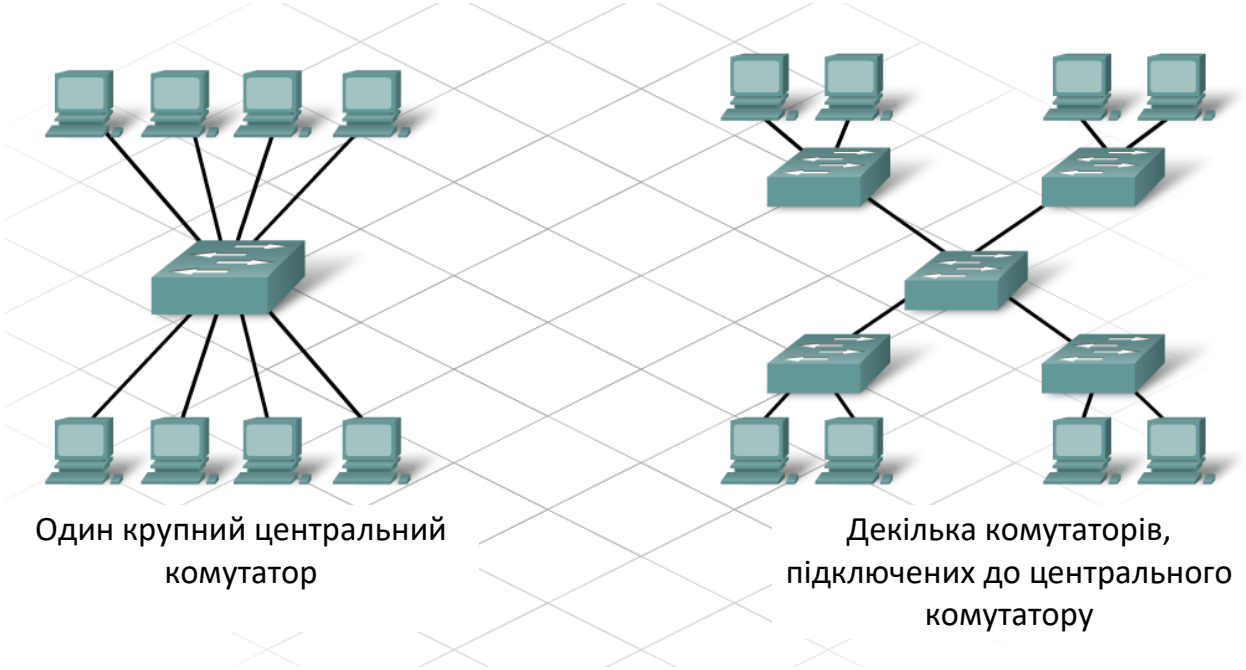


Рисунок 14.13 – Вибір міжмережевих пристроїв

Вибір міжмережевих пристроїв

Маршрутизатор – це пристрій рівня 3. Він виконує всі функції пристроїв нижніх рівнів і вибирає оптимальний маршрут до адресата на основі інформації рівня 3. Маршрутизатори в першу чергу з'єднують мережі. Кожний порт підключений до своєї мережі й маршрутизує пакети між мережами. Маршрутизатори можуть розділяти домени широкомовних розсилань і колізій.

При виборі маршрутизатора важливо підібрати характеристики відповідно до вимог мережі. Зокрема, ураховуються наступні фактори:

– необхідний тип зв'язку;

– доступні функції;

– ціна.

Зв'язок

Маршрутизатори з'єднують мережі, у яких використовуються різні технології. У них є інтерфейси LAN і WAN.

Інтерфейси LAN використовуються для підключення до середовища ЛОМ. Звичайно в ній застосовуються кабелі UTP, але є й можливість додати

оптоволоконні модулі. Залежно від серії й моделі маршрутизатора, можлива наявність декількох типів інтерфейсів для підключення кабелів LAN і WAN.

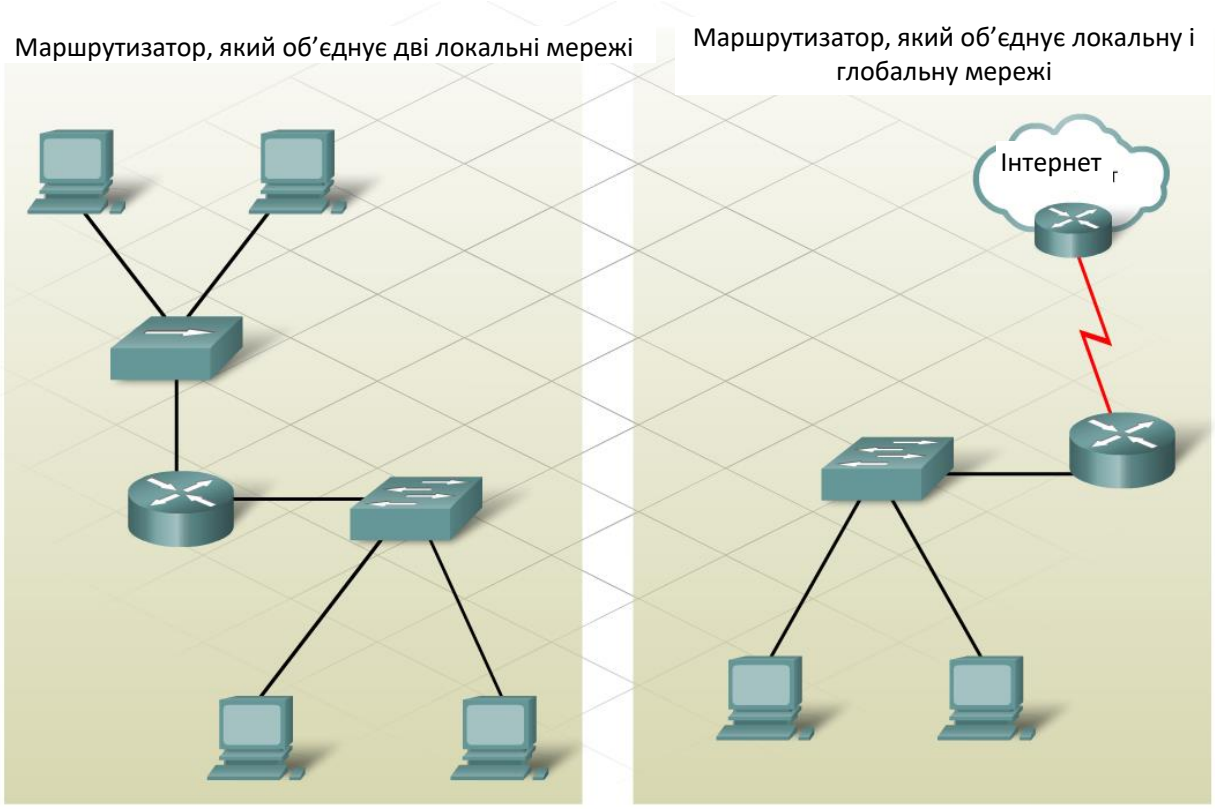


Рисунок 14.14 – Види підключення маршрутизатора

Функції

Характеристики маршрутизатора повинні відповідати вимогам мережі. Можливо, що за результатами аналізу підприємству знадобиться маршрутизатор з певними функціями. Крім базової маршрутизації, зустрічаються наступні функції:

– безпека;

– якість обслуговування (QoS);

– Voice over IP (VoIP);

– перетворення мережевих адрес (NAT);

– протокол динамічного налаштування вузлів (DHCP).

Ціна

При виборі міжмережевих пристроїв потрібно врахувати вимоги бюджету. Маршрутизатори бувають дорогими. Їхню вартість можуть підвищити додаткові модулі, наприклад, оптоволоконні. Середовище підключення маршрутизатора повинна підтримуватися без додаткових модулів. Це зведе до мінімуму витрати.

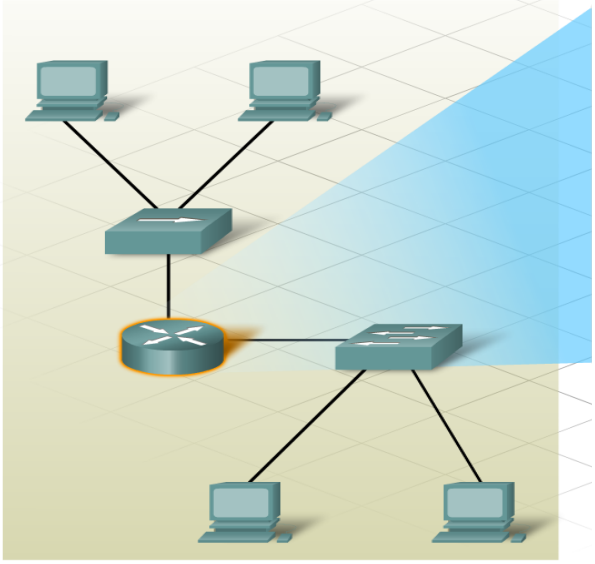
Маршрутизатор з інтегрованими мережевими службами (ISR) – це порівняно новий пристрій, що виконує функції різного устаткування. До винаходу ISR для підтримки роботи з даними, дротовими й бездротовими системами, голосом і відео, міжмережевими екранами й VPN потрібно було кілька пристроїв. ISR виконує функції декількох пристроїв, необхідних невеликому й середньому підприємствам і філіям великих організацій. Цей пристрій полегшує роботу. З його допомогою можна легко й швидко забезпечити захист користувачів, додатків, мережевих кінцевих точок і бездротових ЛОМ. Можливо, вартість ISR буде менше, ніж в окремих пристроїв.

Відновлення мережевого устаткування

Спочатку невеликі мережі для дротових і бездротових користувачів часто створюються з використанням недорогих убудованих маршрутизаторів. Такі пристрої розроблялися для невеликих мереж. Звичайно вони складаються з декількох дротових вузлів і, іноді, чотирьох або п'яти бездротових пристроїв. Коли невелике підприємство переростає можливості існуючих мережевих пристроїв, доводиться купувати більше складне устаткування. У цьому курсі, зокрема, приводяться наступні приклади:

– ISR Cisco 1841;

– комутатор Cisco 2960.



Маршрутизатор ISR
Функції:

- Безпека
- Бездротова точка доступу
- Віртуальна частинна мережа
- DHCP
- NAT
- Система виявлення вторгнень
- IP-телефонія
- Гарантована якість обслуговування

Рисунок 14.15 – Маршрутизатор з інтегрованими мережевими службами (ISR)

Маршрутизатор Cisco 1841 розроблений для філій і середніх підприємств. Будучи універсальним маршрутизатором початкового рівня, він підтримує різні варіанти підключення. Це пристрій з модульним дизайном і різними службами безпеки.

ISR Cisco 1841

Комутатор Cisco 2960

Рисунок 14.16 – Маршрутизатор і комутатор Cisco

У серію інтелектуальних комутаторів Ethernet Cisco Catalyst 2960 входять автономні пристрої із блоковою конфігурацією, що дозволяють використовувати Fast Ethernet і Gigabit Ethernet на настільних комп'ютерах. От деякі функції серії комутаторів Catalyst 2960:

– комутировані початкового корпоративного рівня, з фіксованою конфігурацією, оптимізоване для розгортання на рівні доступу;

– Fast Ethernet і Gigabit Ethernet для настільних комп'ютерів;

– ідеально підходить для невеликих і середніх підприємств і філій;

– компактні комутатори для комутаційних шаф.

Високошвидкісне й високоплотне комутування, що не забезпечують ISR з убудованим комутуванням. Відповідно, вони добре підходять для відновлення мереж на основі концентраторів і невеликих ISR.

Надійність і доступність

Придбання мережевих пристроїв і прокладка кабелів – це тільки початок відновлення мережі. Мережі, крім того, повинні бути надійними й доступними. Для надійності звичайно встановлюють дублюючі компоненти, наприклад, два маршрутизатори замість одного. При цьому утвориться альтернативний шлях передачі даних. Відповідно, якщо на одному маршрутизаторі виникають неполадки, дані можуть досягти адресата іншим способом.

При підвищенні надійності підвищується й доступність. Наприклад, телефонним системам необхідна доступність класу "п'ять дев'яток". Це означає, що система повинна працювати 99,999% часу. Телефонні системи не можуть простоювати або бути недоступними більше 0,001% часу.

Для підвищення надійності мережі звичайно використовуються відказостійкі системи. У такі системи входять, наприклад, джерела безперебійного живлення (UPS), що дублюються джерела змінного струму, пристрою з можливість гарячої заміни й додаткові мережеві адаптери. Якщо один із пристроїв ламається, спрацьовує дублююча або резервна система, що забезпечує мінімальну втрату надійності.

План IP-адресації

При плануванні мережі потрібно передбачити схему логічної адресації. Зміна IP-адресації третього рівня – це серйозна проблема відновлення мережі. Якщо в процесі відновлення структура мережі міняється, можливо, прийде змінити схему IP-адрес і дані мережі.

Потрібно буде врахувати всі пристрої, яким тепер або в майбутньому знадобляться IP-адреси. IP-адреси потрібні наступним вузлам і мережевим пристроям:

– користувальницькі комп'ютери;

– комп'ютери адміністраторів;

– сервери;

– інші кінцеві пристрою, наприклад, принтери, IP-телефони й IP-камери;

– інтерфейси LAN-маршрутизаторів;

– інтерфейси WAN-маршрутизаторів (послідовні).

Крім того, бувають пристрою, які відкриваються й управляються з використанням IP-адрес. До цієї категорії ставляться:

– автономні комутатори;

– бездротові точки доступу.

Наприклад, коли в мережу додається новий маршрутизатор, створюються нові локальні мережі або підмережі. Для них знадобляться відповідні IP-адреси й маски підмережі. Іноді мережі доводиться привласнювати зовсім нову систему адресації.

Після завершення планування й конструювання процес відновлення входить у фазу впровадження, і починається фізичний монтаж мережі.

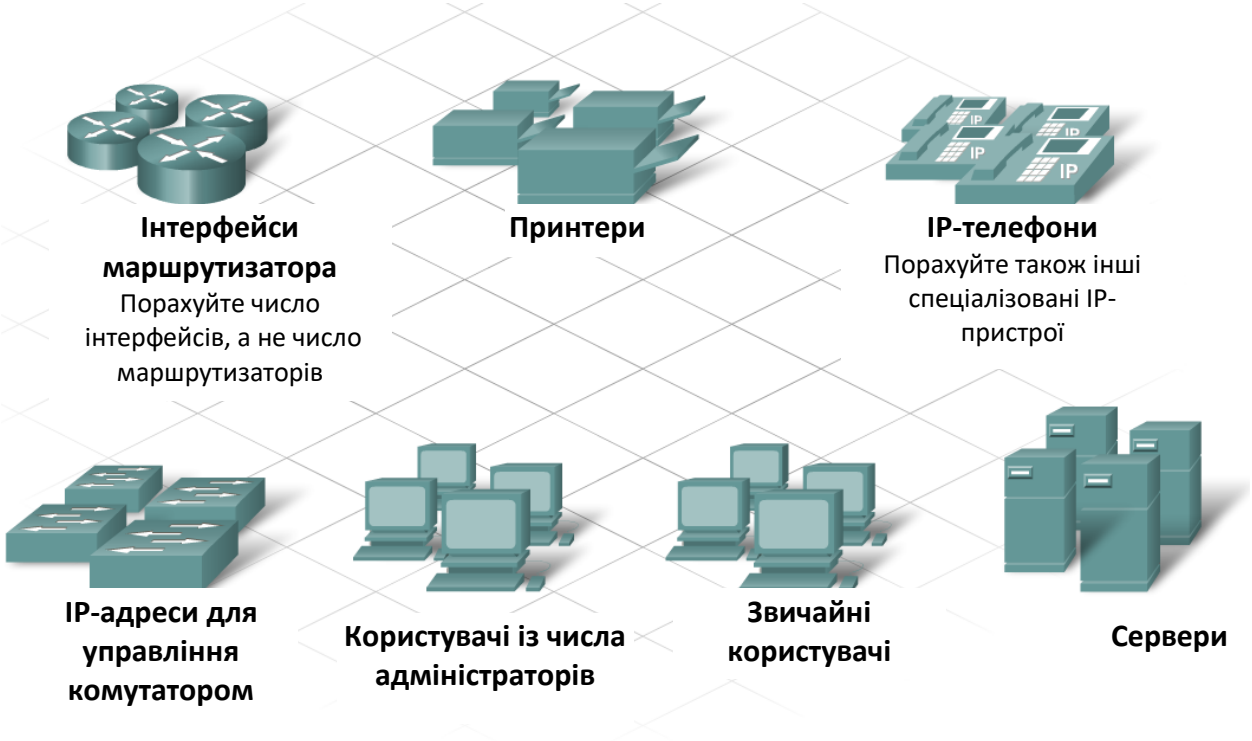


Рисунок 14.16 – Підготовчий етап для планування мережі

Список використаних джерел

1. Куприянов А. О. «Обеспечение защиты персональных данных в информационных системах» // Програм. инженерия и информ. безопасность. – 2013. – № 4.

2. Таненбаум Э, Уэзеролл Д. «Компьютерные сети.» – Питер, 2014. – 960 с.

3. «Абонентские сети доступа и технологии высокоскоростных сетей», Берлин А. Н. Национальный Открытый Университет «ИНТУИТ» – 2016 год – 277 страниц

4. «Администрирование сетей Microsoft Windows XP Professional»,Элсенпитер Р., Велт Национальный Открытый Университет «ИНТУИТ» – 2016 год – 650 стр.

5. «Компьютерные сети : учебно-методическое пособие по выполнению расчетно-графической работы»,Фомин Д. В. Директ-Медиа – 2015 год – 66 стр.

6. «Характеристика и особенности локальных компьютерных сетей»,Кожемяк М. Э.Лаборатория книги – 2012 год – 157 стр.

7. «Безопасность сетей», Мэйволд Э., Национальный Открытый Университет «ИНТУИТ» – 2016 год – 572 стр.

8. «Протоколы безопасного сетевого взаимодействия», Лапонина О.Р., Национальный Открытый Университет «ИНТУИТ» – 2016 год – 462 страницы

9. «Компьютерные сети и сетевые технологии», Николай Кузьменко,368 стр.,2013

10. «Компьютерные сети. Принципы, технологии, протоколы.», 992стр., 2016

11. Кунинець А.І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній / А.І. Кунинець, Ю.І. Грицюк

// Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.2. – С. 352-360.

12. Мониторинг утечек информации. [Электронный ресурс]. – Доступный с http://www. infowatch.ru/analytics/leaks_monitoring

13. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal / Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

14. Чудінова Н.В. Особливості використання мережі Інтернет для отримання конфіденційної інформації / Н.В. Чудінова, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.- техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.3. – С. 337-346.

15. Nicholas Rosasco and David Larochelle. How and Why More Secure Technologies Succeed in Legacy Markets: Lessons from the Success of SSH. Quoting Barrett and Silverman, SSH, the Secure Shell: The Definitive Guide, O'Reilly & Associates . Dept. of Computer Science, Univ. of Virginia. Архів оригіналу за 2013-06-25.

16. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. 4-е изд./ В.Г. Олифер, Н.А. Олифер. — СПб. : Питер, 2010. — 918 с.

17. Столлингс В. Безпроводные линии связи и сети. – М.: «Вильямс», 2003. – 640 с.

18. Кландер Л. Hacker Proof: Полное руководство для безопасно- сти компьютера / Пер. с англ. – Мн.: Попурри, 2002. – 688 с.

19. Шиндер Д.Л. Основы компъютерных сетей. – М.: Вильямс, Cisco Press, 2003. – 656 с.

20. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.

21. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.

22. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.

23. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.

24. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.

25. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2014. – № 4(17). – С. 90-95.

26. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.

27. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.

28. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.

29. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. – № 3(20). – С. 134-141.

30. Смирнов С. А. Комплекс GERT-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. - практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.

31. Смирнов С. А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, А. К. Дидык, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2016. – № 2 (46). – С. 146-149.

32. Смирнов С. А. Модели системы нейросетевых экспертов безопасной маршрутизации в облачных антивирусных системах /

А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2016. – Вип. 3 (140). – С. 36-39.

33. Смирнов С. А. Метод безопасной маршрутизации на базовом множестве путей передачи метаданных в облачные антивирусные системы / В. Л. Бурячок, С. А. Смирнов // Системи управління, навігації та зв'язку. – Полтава, 2016. – Вип. 4(40). – С. 57-62.

34. Смирнов С. А. Способ контроля линий связи телекоммуникационной системы облачного антивируса / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2016. – № 2 (47). – С. 148-152.

Зміст

промені