Вступ до мереж (Introduction to Networks)

Сучасні мережні технології

Назва теми	Мета вивчення теми
1.1 Мережі впливають на наше життя	Пояснити, як мережі впливають на наше повсякденне життя.
1.2 Компоненти мережі	Пояснити, як використовуються вузли та мережні пристрої.
1.3 Зображення мереж і топології	Пояснити способи подання мереж і те, як вони використовуються у мережних топологіях.
1.4 Основні типи мереж	Порівняти характеристики поширених типів мереж.
1.5 Інтернет-з'єднання	Пояснити, як локальні і глобальні мережі реалізують з'єднання з мережею Інтернет.
1.6 Надійні мережі	Описати чотири основні критерії надійної мережі.
1.7 Тенденції розвитку мереж	Пояснити як такі тенденції як BYOD, онлайн-співпраця, відео і хмарні. обчислення змінюють спосіб нашої взаємодії.
1.8 Безпека мережі	Визначити деякі основні загрози мережній безпеці та рішення для запобігання ним.

1.1 Мережі впливають на наше життя

Серед усіх найважливіших для людського існування потреб, прагнення до взаємодії з іншими посідає трохи нижчий щабель за наші потреби у підтримці життєдіяльності. Спілкування для нас майже так само важливе, як і наша залежність від повітря, води, їжі та притулку.

У сучасному світі завдяки використанню мереж ми пов'язані як ніколи раніше. Люди з новими ідеями мають можливість миттєво взаємодіяти з іншими, задля втілення їх у життя. Новини про події та відкриття за лічені секунди стають відомими у всьому світі. Люди, розділені океанами і континентами, можуть виходити на зв'язок і спільно грати в ігри з друзями.

Досягнення у сфері мережних технологій - це, мабуть, найвагоміші зміни у світі на сьогодні. Вони допомагають створити середовище, у якому національні кордони, географічні відстані та фізичні обмеження втрачають свій зміст, перетворюючись на незначні перешкоди.

Інтернет змінив спосіб нашої соціальної, комерційної, політичної та особистої взаємодії. Безпосередні комунікації через Інтернет заохочують до створення глобальних спільнот, які сприяють соціальній взаємодії, незалежно від місця розташування або часового поясу.

Створення онлайн-спільнот для обміну ідеями та інформацією перспективне з точки зору збільшення продуктивності у всьому світі.

Створення хмари дозволяє нам зберігати документи і зображення, а також отримувати доступ до них будь-де і будь-коли. Отже, незалежно від того, чи подорожуємо ми у потязі, гуляємо в парку або стоїмо на вершині гори, ми можемо безперешкодно отримати доступ до наших даних і застосунків з будь-якого пристрою.

1.2 Компоненти мережі

1.2.1 Ролі вузла

Для того, щоб стати частиною глобальної онлайн-спільноти, ваш комп'ютер, планшет або смартфон спершу потрібно під'єднати до мережі. Зі свого боку, ця мережа повинна мати

з'єднання з Інтернетом. У цій темі ми розглянемо складові частини мережі. Побачимо, чи вдасться вам виявити ці ж компоненти у власній домашній або шкільній мережі!

Усі комп'ютери, що під'єднані до мережі та беруть безпосередню участь у мережному з'єднанні, класифікуються як вузли або хости. Вузли ще називають кінцевими пристроями. Деякі вузли називають клієнтами. Однак, термін "вузол" конкретно стосується пристроїв у мережі, яким призначений номер для потреб зв'язку. Цей номер ідентифікує кожен вузол у межах певної мережі. Його називають адресою Інтернет-протоколу - (IP) адресою. IP-адреса визначає вузол та мережу, до якої він належить.

Сервери - це вузли зі встановленим програмним забезпеченням, яке дозволяє надавати іншим кінцевим пристроям у мережі необхідну інформацію, таку як електронна пошта чи веб-сторінки. Кожен сервіс потребує окремого серверного програмного забезпечення. Наприклад, для надання веб-послуг у мережі, на сервері повинне бути встановлене програмне забезпечення веб-сервера. Комп'ютер із серверними застосунками може постачати послуги одночасно багатьом різним клієнтам.

Як згадувалося раніше, клієнт - це один з типів вузла. Як показано на рисунку, клієнти використовують програмне забезпечення для надсилання запитів та відображення інформації, отриманої від сервера.

Клієнтський ПК і сервер, з'єднані через хмару, яка символізує Інтернет

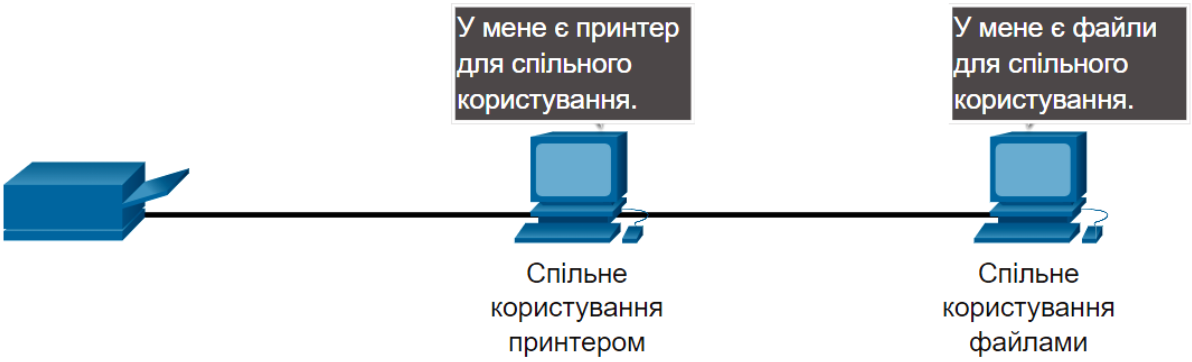
Прикладом клієнтського програмного забезпечення є веб-браузер, такий як Chrome або FireFox. На одному комп'ютері одночасно може працювати декілька типів клієнтських програм. Наприклад, користувач може перевіряти електронну пошту, переглядати веб-сторінки, обмінюватися миттєвими повідомленнями та слухати аудіо трансляцію. Таблиця містить три поширені типи серверного програмного забезпечення.

Тип	Опис
Електронна пошта	Сервер електронної пошти запускає ПЗ поштового сервера. Клієнти використовують поштову клієнтську програму, таку як Microsoft Outlook, для доступу до електронної пошти на сервері.
Веб	На веб-сервері працює спеціальне ПЗ веб-сервера. Клієнти використовують програми-браузери, наприклад Windows Internet Explorer, для доступу до веб-сторінок на сервері.
Файл	Файловий сервер зберігає корпоративні файли та файли користувачів у центральному сховищі. Клієнтські пристрої отримують доступ до цих файлів за допомогою ПЗ клієнта, наприклад диспетчера файлів Windows File Explorer.

1.2.2 Одноранговa мережа

Зазвичай, клієнтське та серверне програмне забезпечення працює на окремих комп’ютерах, проте і один комп'ютер може поєднувати ці дві ролі. У мережах невеликих підприємств чи

організацій, а також у домашніх мережах, багато **комп'ютерів одночасно функціонують і як сервери, і як клієнти**. **Такі мережі називаються одноранговими**.



Переваги одноранговых мереж:

- Легкість налаштування
- Менша складність
- Знижена вартість, через відсутність додаткових мережних пристроїв та виділених серверів
- Підтримка виконання простих завдань, таких як обмін файлами і спільне використання принтерів

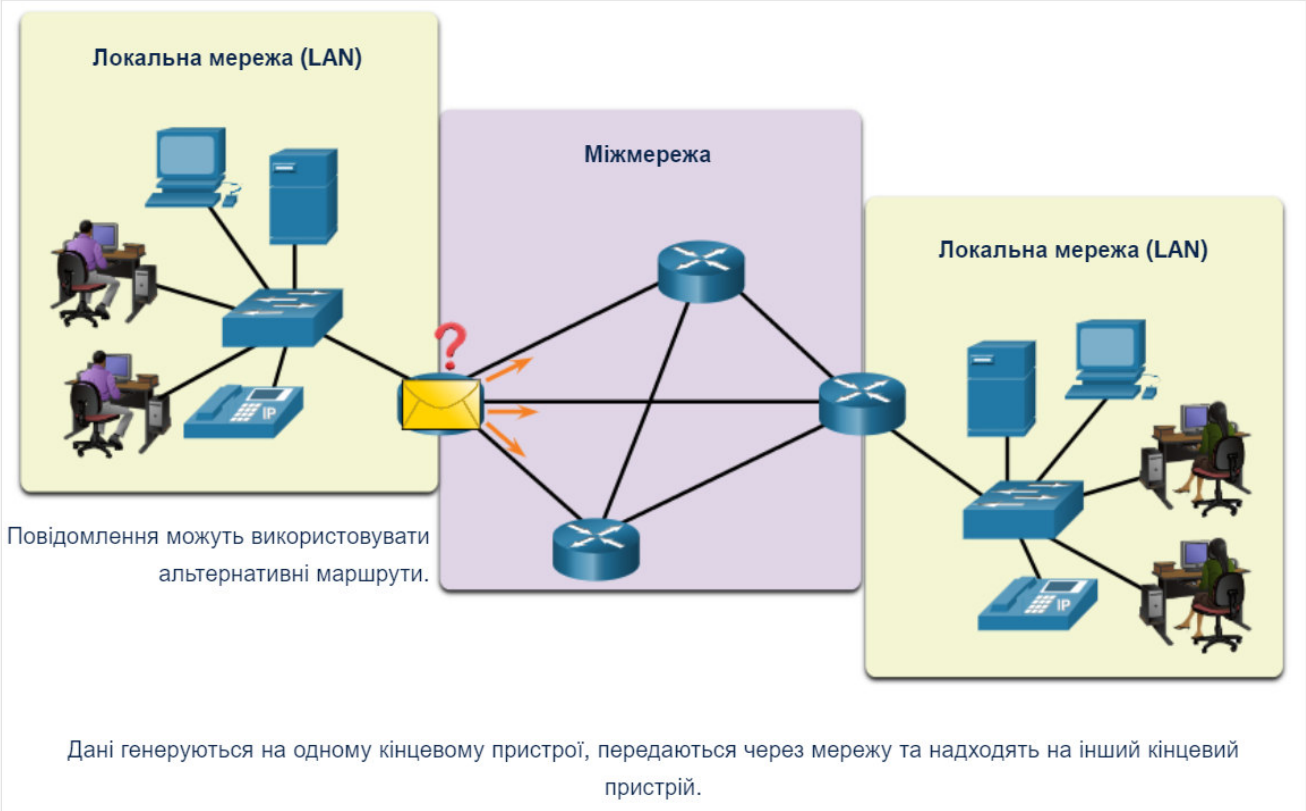
Недоліки одноранговых мереж:

- Відсутність централізованого адміністрування
- Низький рівень безпеки
- Складність масштабування
- Усі пристрої можуть функціонувати і як клієнти і як сервери, що може уповільнити їх роботу

1.2.3 Кінцеві пристрої

Зазвичай мережні пристрої, з якими люди мають справу, називають кінцевими пристроями. Для того, щоб відрізнити у мережі один кінцевий пристрій від іншого, кожен із них ідентифікується за адресою. Коли кінцевий пристрій ініціює обмін даними, використовується адреса кінцевого пристрою призначення, щоб визначити, куди саме має надійти повідомлення.

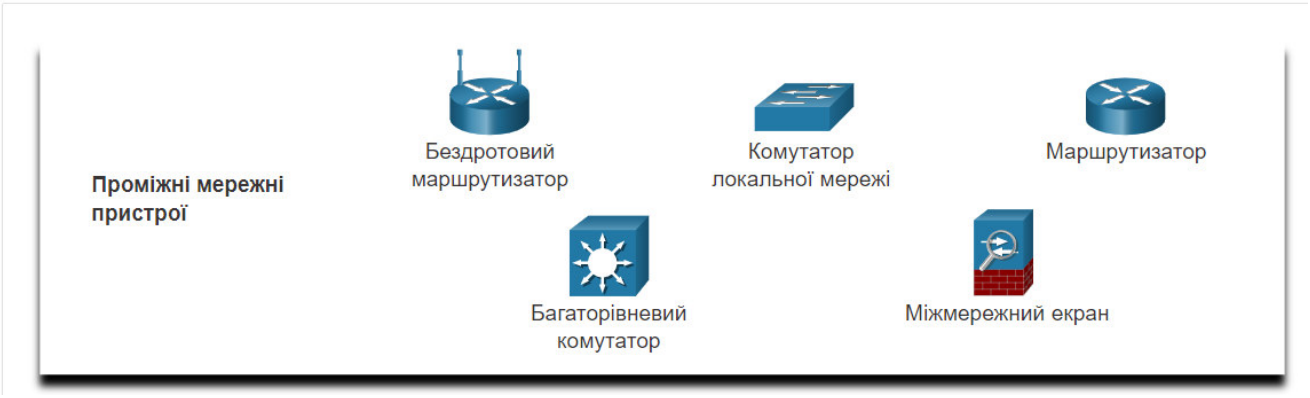
Кінцевий пристрій є або відправником, або отримувачем повідомлення, що передається мережею.



1.2.4 Проміжні мережні пристрої

Проміжні пристрої використовуються для під'єднання кінцевих пристроїв до мережі. Вони можуть з'єднувати декілька окремих мереж для утворення більшої складеної структури. Ці проміжні пристрої забезпечують з'єднання і передавання потоків даних по мережі.

Для визначення шляху надсилання повідомлень проміжні пристрої використовують адресу призначення кінцевого вузла та інформацією про мережні з'єднання. Приклади найпоширеніших проміжних пристроїв та перелік їх функцій наведені на рисунку.



Проміжні мережні пристрої виконують деякі або всі функції, зазначені нижче:

- Відновлення і повторне передавання сигналів зв'язку.
- Підтримка інформації про наявні шляхи передавання даних через мережу або між мережами.
- Інформування інших пристроїв про помилки та вихід з ладу засобів зв'язку.
- Спрямування даних альтернативними шляхами у випадках відмови основних каналів зв'язку.
- Класифікація та надсилання повідомлень відповідно до пріоритетів.
- Дозвіл або заборона на передавання даних на основі параметрів безпеки.

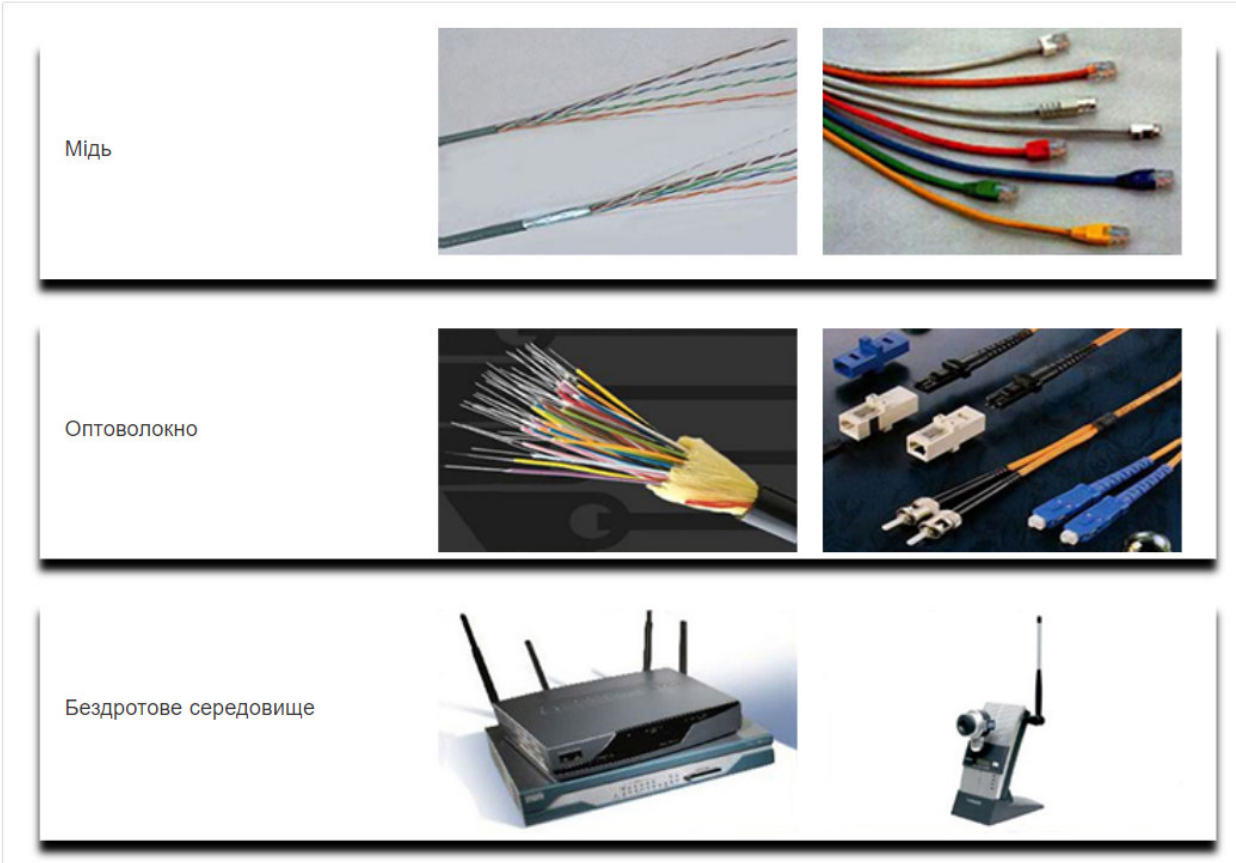
Примітка: Не наведено класичний концентратор Ethernet, також відомий як багатопортовий повторювач. Він відновлює сигнали зв'язку і виконує їх повторне передавання. Варто зазначити, що всі проміжні мережні пристрої виконують функції повторювача.

1.2.5 Мережне середовище

Обмін даними по мережі відбувається у певному середовищі. Середовище забезпечує канал, по якому повідомлення передається від відправника до отримувача.

Як зображено на рисунку, сучасні мережі для з'єднання пристроїв використовують три основні типи середовищ.

- **Кабелі з металевих дротів** - Дані кодуються за допомогою електричних імпульсів.
- **Кабелі з оптичних або пластикових волокон (волоконно-оптичний кабель)** - Дані передаються за допомогою імпульсів світла.
- **Бездротові середовища** - Дані подаються за допомогою модуляції визначених частот електромагнітних хвиль.



Критерії, якими варто керуватися при виборі мережного середовища передавання даних:

- Максимальна відстань, на яку носій може успішно доправити сигнал.
- Умови прокладання кабелів.
- Обсяг даних і швидкість, з якою необхідно передавати дані.
- Вартість середовища та його монтажу.

Різні типи мережних середовищ мають **свої особливості та переваги** використання. Не всі мережні носії забезпечують однакові характеристики і, як правило, використовуються за різним призначенням.

1.2.6 *Питання для самоперевірки – Компоненти мережі*

Перевірте своє розуміння Мережних компонентів, обравши правильну відповідь на такі запитання.

1. Яку назву мають комп'ютери, що під'єднані до мережі і беруть безпосередню участь в обміні даними?

- ◯ сервери
- ◯ проміжні мережні пристрої
- ◯ вузли
- ◯ середовище

2. У якому середовищі передавання дані подаються у вигляді імпульсів світла?

- ◯ бездротове середовище
- ◯ волоконно-оптичний кабель
- ◯ мідний кабель

3. Які два пристрої належать до проміжних пристроїв? (Оберіть два.)

- ☐ вузли
- ☐ маршрутизатори
- ☐ сервери
- ☐ комутатори

Перевірити

Показати

Скинути

1. Яку назву мають комп'ютери, що під'єднані до мережі і беруть безпосередню участь в обміні даними?

Правильно!

- ○ сервери
- ○ проміжні мережні пристрої
- ◉ вузли
- ○ середовище

2. У якому середовищі передавання дані подаються у вигляді імпульсів світла?

Правильно!

- ○ бездротове середовище
- ◉ волоконно-оптичний кабель
- ○ мідний кабель

3. Які два пристрої належать до проміжних пристроїв? (Оберіть два.)

Правильно!

- ☐ вузли
- ☑ маршрутизатори
- ☐ сервери
- ☑ комутатори

1.3 Зображення мереж і топології

Подання мережі

Мережні архітектори і адміністратори повинні мати можливість зображати розроблені ними проекти мереж. Їм потрібно чітко бачити, які компоненти з'єднані між собою, де вони розташовані і в який спосіб взаємодіятимуть. Для подання різних пристроїв та з'єднань на мережних схемах часто використовуються позначення, зображені на рисунку.

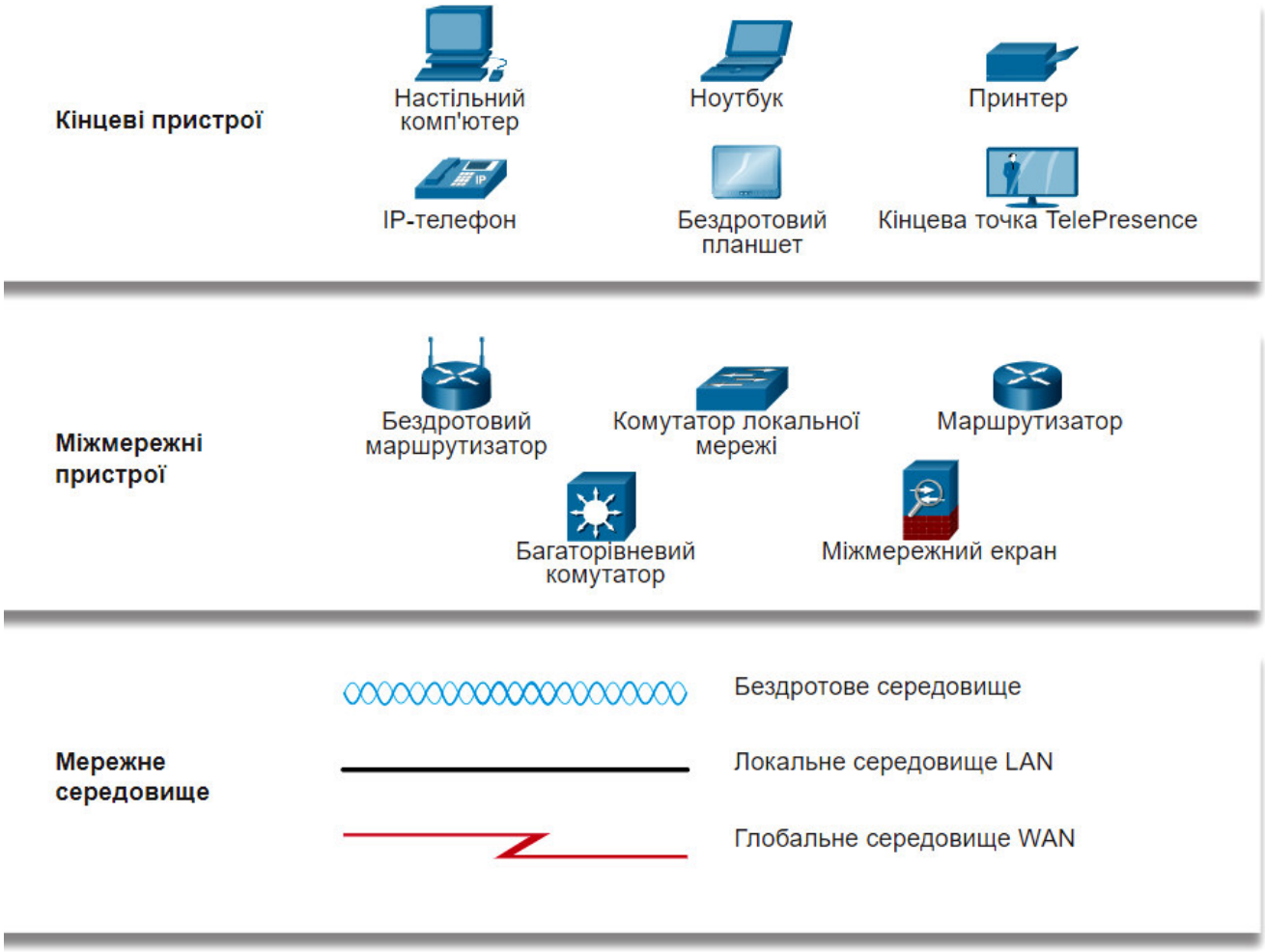


Схема у простий спосіб зображає те, як зв’язані пристрої у великій мережі. Цей тип “зображення” мережі, відомий як **схема топології**. Уміння розпізнавати логічне подання фізичних компонентів мереж є критично важливим для візуалізації способу організації та функціонування мережі.

На додачу до графічних зображень використовується спеціалізована термінологія для позначення того, як ці пристрої та середовища передавання даних пов'язані між собою:

- **Мережний адаптер, мережна карта (NIC)** - NIC фізично під'єднує кінцевий пристрій до мережі.
- **Фізичний порт** - Конектор або роз'єм на мережному пристрої, до якого за допомогою середовища під'єднується кінцевий або інший мережний пристрій.
- **Інтерфейс** - Спеціалізовані порти на мережному пристрої, під'єднані до окремих мереж. Оскільки маршрутизатор об'єднує мережі, його порти називають мережними інтерфейсами.

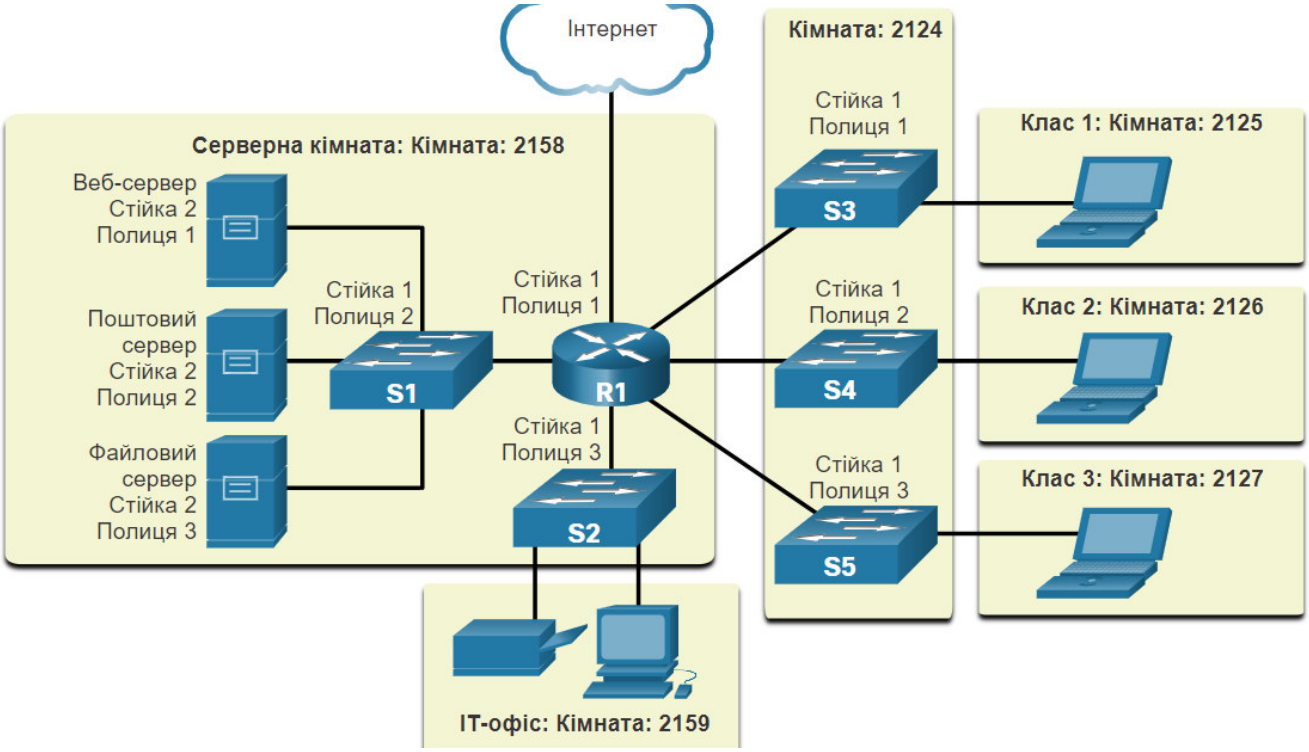
Примітка: Часто терміни порт і інтерфейс використовуються взаємозамінно.

1.3.2 Схеми топологій

Схеми топологій є обов'язковою документацією для усіх, хто має справу з мережами. Вони створюють візуальну карту того, як з'єднана мережа. Розрізняють два типи топологій: фізичну і логічну.

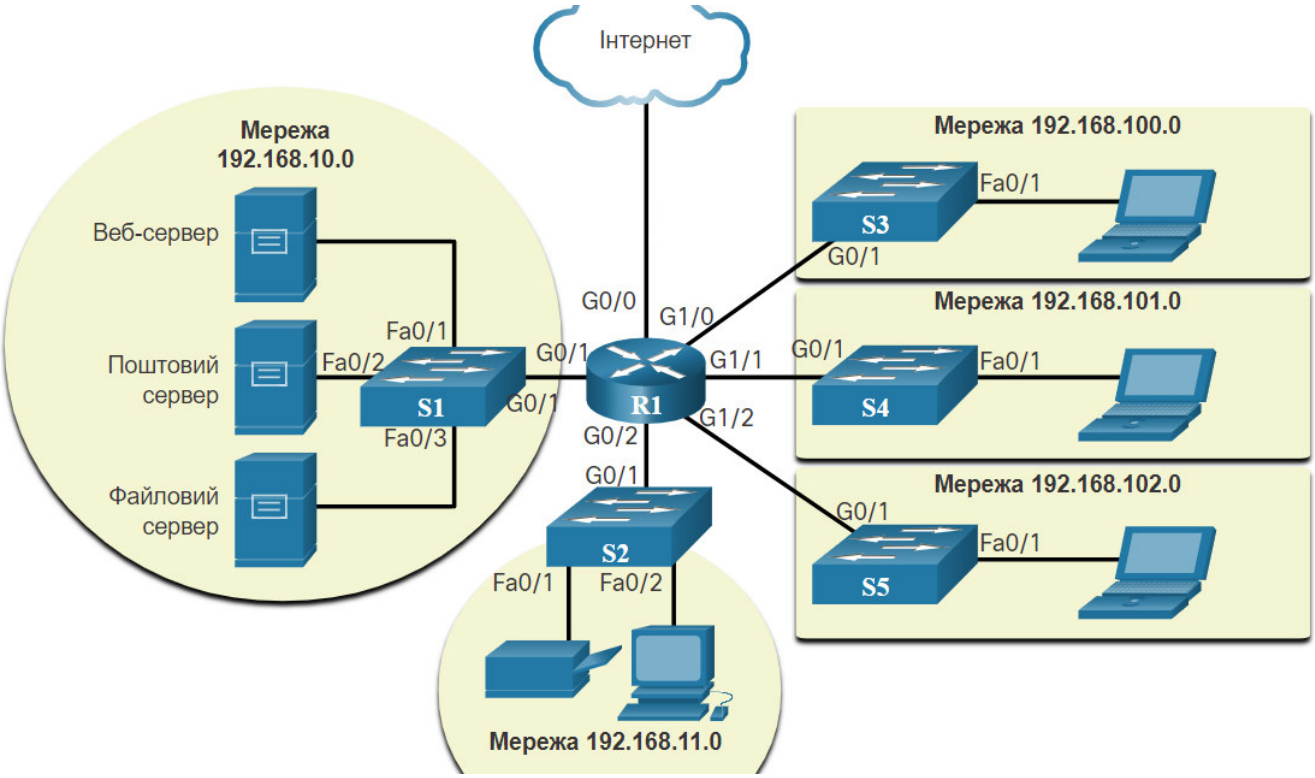
Схеми фізичної топології

Схеми фізичних топологій зображають фізичне розміщення проміжних пристроїв і прокладання кабелів, як показано на рисунку. На цій фізичній топології позначені приміщення, у яких розташовані пристрої, а також їхні маркування.



Схеми логічної топології

Схеми логічних топологій подають пристрої, порти, а також схему адресації мережі, як зображено на рисунку. За допомогою логічної топології можна побачити, до яких проміжних пристроїв під'єднані кінцеві пристрої, а також яке середовище при цьому використовується.



Зображені схеми фізичної та логічної топологій відповідають вашому рівню розуміння на даному етапі курсу. Приклади більш складних топологій можна пошукати в інтернеті, ввівши “network topology diagrams” (топології мереж) у пошуковому рядку. Якщо додати слово “Cisco” до пошукової фрази, ви знайдете багато топологій, у яких використовують графічні позначення, схожі до тих, які ви бачили на наших рисунках.

1.3.3 Питання для самоперевірки - Зображення мереж і топології

1. Який тип з'єднання фізично під'єднує кінцевий пристрій до мережі?

   - ◯ Порт
   - ◯ NIC
   - ◯ Інтерфейс

2. Яке з'єднання належить до спеціалізованих портів мережного пристрою, до яких під'єднуються окремі мережі?

   - ◯ Порт
   - ◯ NIC
   - ◯ Інтерфейс

3. Який тип мережної топології дозволяє побачити, до яких проміжних пристроїв під'єднані кінцеві пристрої, а також яке середовище при цьому використовується.

   - ◯ Фізична топологія
   - ◯ Логічна топологія

4. Який тип мережної топології дозволяє побачити реальне розташування проміжних пристроїв і прокладання кабелю?

   - ◯ Фізична топологія
   - ◯ Логічна топологія

Правильні відповіді:

1. Який тип з'єднання фізично під'єднує кінцевий пристрій до мережі?

Правильно!

- ○ Порт
- ◉ NIC
- ○ Інтерфейс

2. Яке з'єднання належить до спеціалізованих портів мережного пристрою, до яких під'єднуються окремі мережі?

Правильно!

- ○ Порт
- ○ NIC
- ◉ Інтерфейс

3. Який тип мережної топології дозволяє побачити, до яких проміжних пристроїв під'єднані кінцеві пристрої, а також яке середовище при цьому використовується.

Правильно!

- ○ Фізична топологія
- ◉ Логічна топологія

4. Який тип мережної топології дозволяє побачити реальне розташування проміжних пристроїв і прокладання кабелю?

Правильно!

- ◉ Фізична топологія
- ○ Логічна топологія

1.4 Основні типи мереж

1.4.1 Мережі різного розміру

Тепер, коли ви познайомилися з компонентами, з яких складаються мережі, та з їх зображенням на фізичних і логічних топологіях, настав час дізнатися про безліч різних типів мереж.

Мережі бувають різних розмірів. Від простих мереж, що складаються з двох комп'ютерів до мереж, які з'єднують мільйони пристроїв.

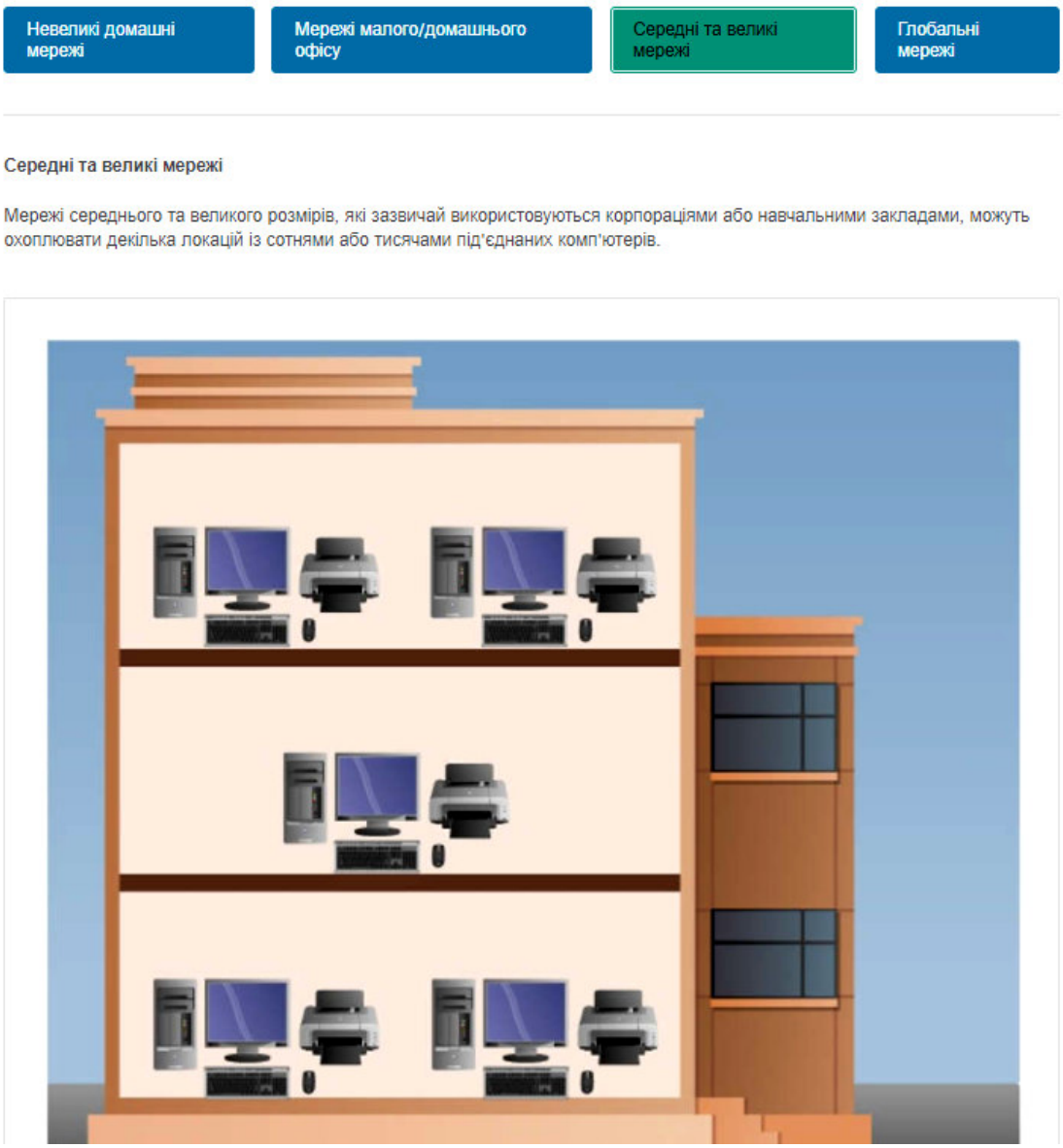
Прості домашні мережі дозволяють локальним кінцевим пристроям спільно використовувати такі ресурси, як принтери, документи, зображення і музику.

Мережі для домашніх і невеликих офісів (SOHO, Small office and home office) підтримують роботу з дому або з віддаленого офісу. Багато самозайнятих працівників використовують мережі цього типу для поширення реклами та продажу товарів, замовлення постачань і спілкування із клієнтами.

Підприємства та великі організації використовують мережі для об'єднання, зберігання та доступу до інформації на мережних серверах. Мережі забезпечують обмін електронними листами і миттєвими повідомленнями та підтримують взаємодію між співробітниками. Багато установ використовують інтернет-з'єднання для надання своїм клієнтам товарів та послуг.

Інтернет є найбільшою з існуючих мереж. Фактично термін Інтернет означає "мережа мереж". Це сукупність взаємозв'язаних приватних і публічних мереж.

У мережах невеликих підприємств чи організацій, а також домашніх мережах багато комп'ютерів одночасно функціонують і як сервери, і як клієнти. Такі мережі називаються одноранговими. **Типи мереж:**

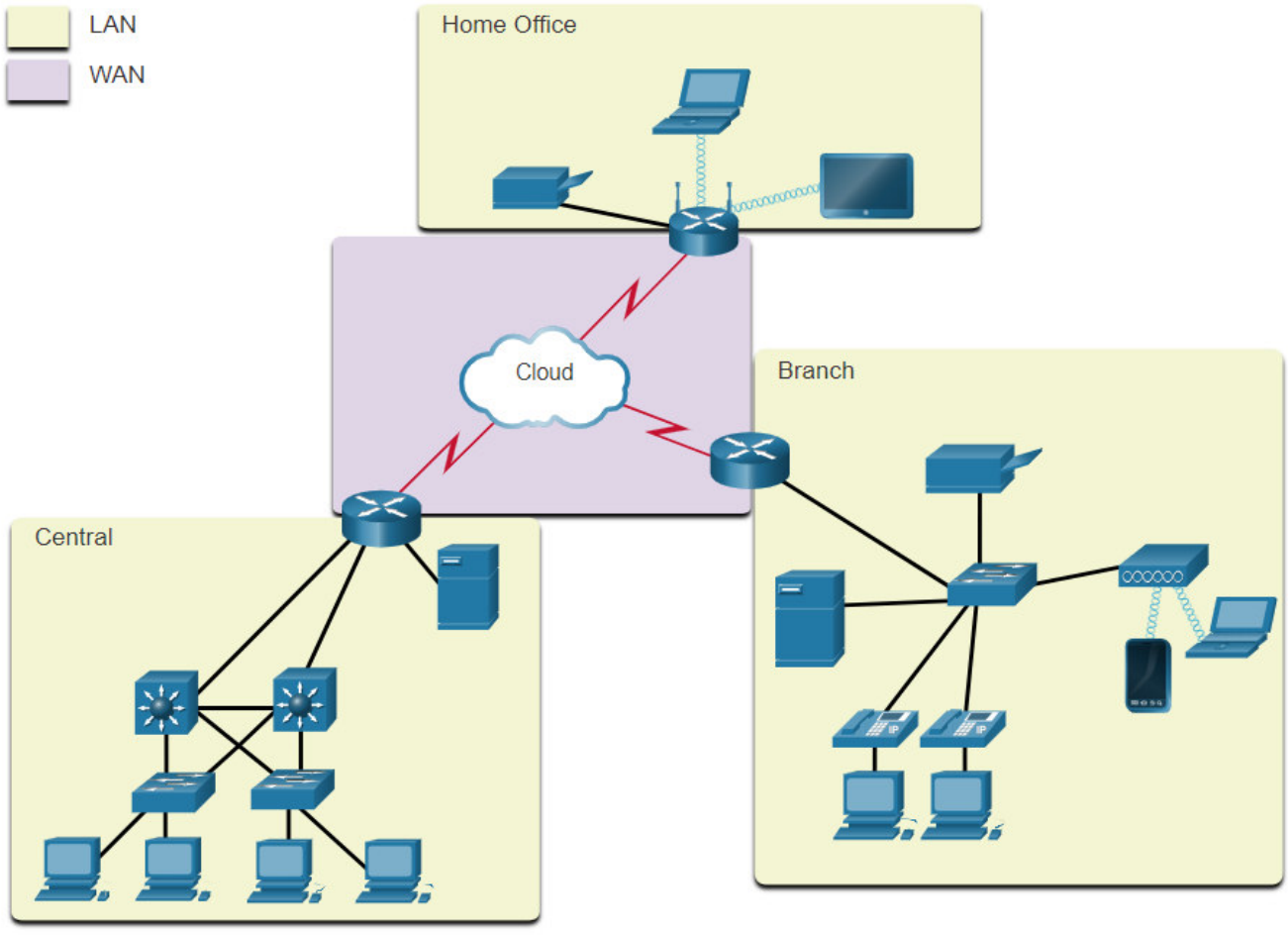


1.4.2 *Мережі LAN і WAN*

Мережні інфраструктури сильно різняться з точки зору:

- площі, яку вони охоплюють
- кількості під'єднаних користувачів
- діапазону і типу доступних послуг
- області відповідальності

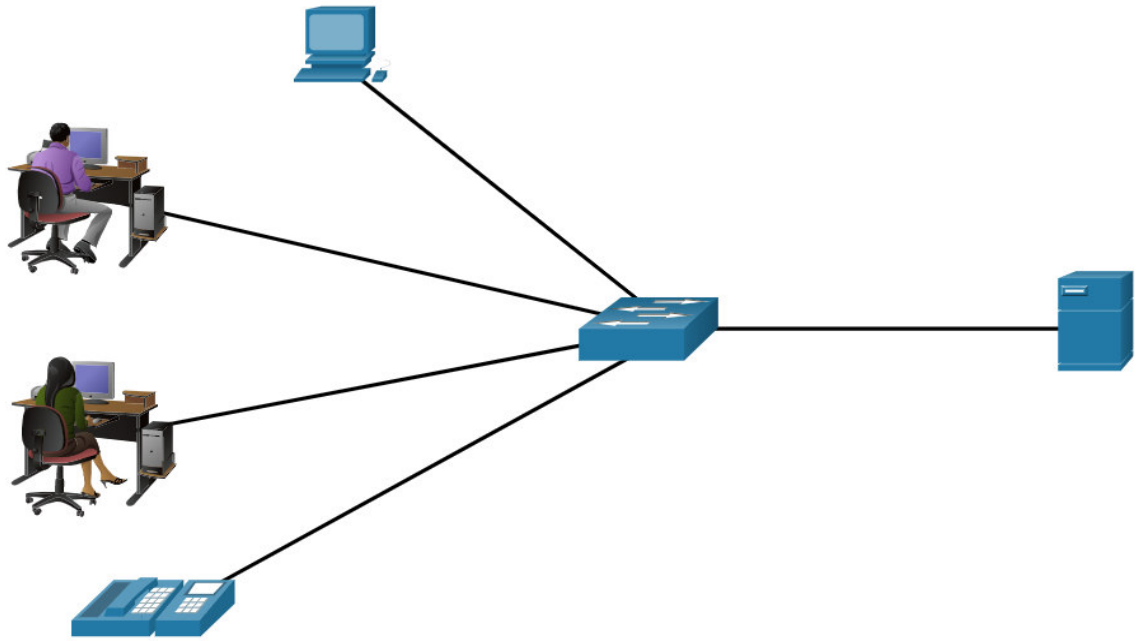
Два найбільш поширені типи мережних інфраструктур включають локальні мережі **(LAN, Local Area Network)** і глобальні мережі **(WAN, Wide Area Network)**. LAN - це мережна інфраструктура, яка надає доступ користувачам і кінцевим пристроям на невеликій географічній площі. LAN зазвичай використовуються підрозділами у складі підприємства, вдома або у невеликих промислових мережах. WAN - це мережна інфраструктура, яка забезпечує доступ до інших мереж на великих географічних відстанях, які належать і обслуговуються великими корпораціями або провайдером телекомунікаційних послуг. На рисунку зображені локальні мережі LANs, під'єднані до WAN.



Локальні мережі

LAN - це мережна інфраструктура, яка охоплює невелику географічну площу. Локальні мережі мають такі визначені характеристики:

- Локальні мережі з'єднують кінцеві пристрої на обмеженій території, наприклад, у будинку, в школі, у приміщенні офісу або кампуса.
- Локальна мережа зазвичай адмініструється окремою організацією або особою. Адміністративний контроль здійснюється на рівні мережі та визначає політики безпеки та доступу.
- Як видно з рисунку, локальні мережі забезпечують високу пропускну здатність для кінцевих і проміжних пристроїв.



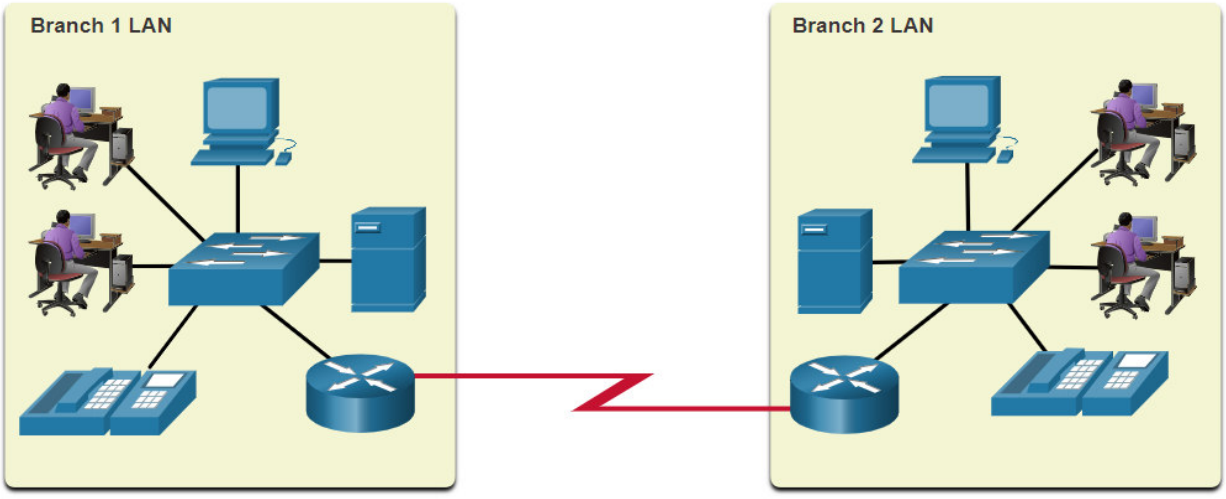
Мережа, яка використовується вдома, обслуговує невелику будівлю або кампус, вважається локальною мережею.

Глобальні мережі

На рисунку зображено WAN, яка з'єднує локальні мережі. WAN - це мережна інфраструктура, що простягається на значні географічні відстані. Глобальні мережі (WANs) зазвичай знаходяться під контролем сервіс-провайдерів (SPs) або провайдерів інтернет-послуг (ISPs).

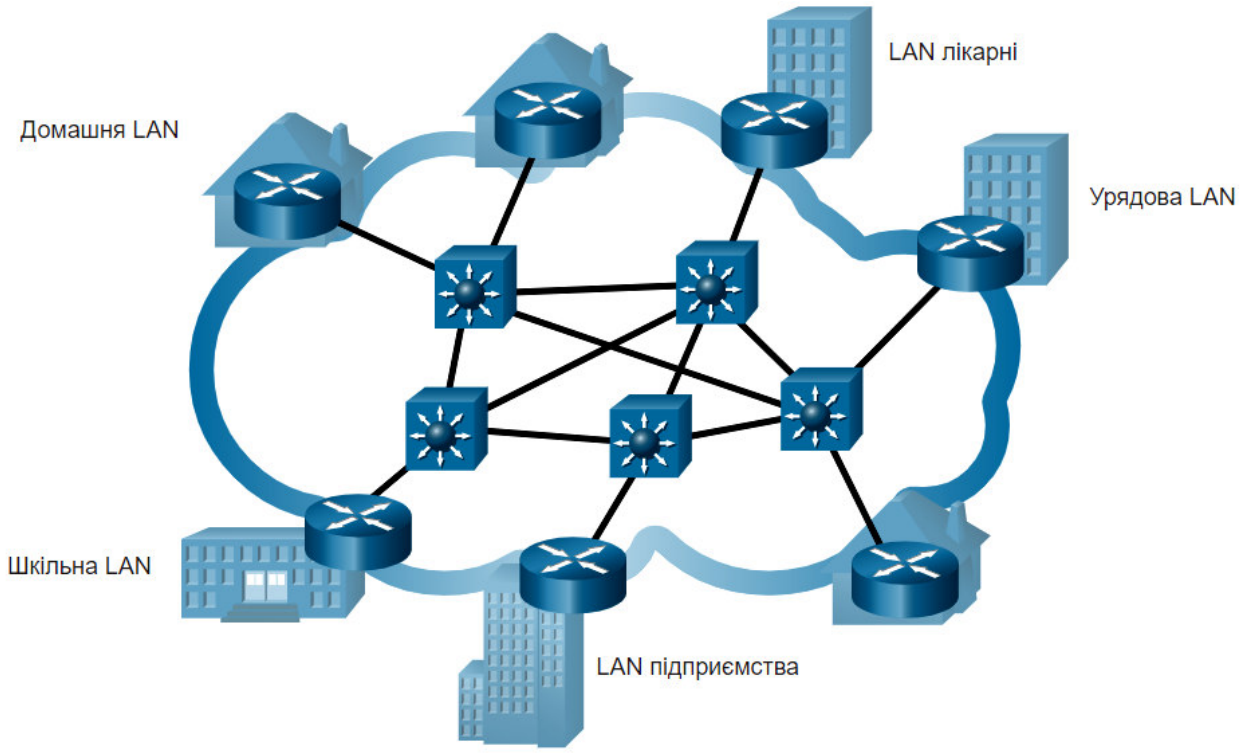
Глобальні мережі мають такі визначені характеристики:

- WAN з'єднують локальні мережі на великих географічних площах, таких як міста, штати, провінції, країни чи континенти.
- Глобальні мережі, як правило, адмініструються декількома постачальниками послуг.
- WAN зазвичай створюють повільніші канали зв’язку між локальними мережами.



1.4.3 Інтернет

Інтернет - це всесвітнє об'єднання взаємопов'язаних мереж (від слова "internetworks", скорочено "internet"). На рисунку зображено один зі способів подання інтернету у вигляді сукупності взаємопов'язаних LANs і WANs.



Локальні мережі використовують послуги WAN для з'єднання.

Деякі локальні мережі підключаються одна до одної через WAN-з'єднання. У свою чергу, WANs з'єднуються між собою. Червоні WAN-з'єднання позначають усі можливі способи під'єднання мереж. Глобальні мережі можуть під'єднуватися за допомогою мідних дротів, волоконно-оптичних кабелів або бездротового з'єднання (не зображено).

Мережа Інтернет не належіть жодній особі чи групі осіб. Забезпечення ефективного з'єднання у цій різноманітній інфраструктурі вимагає застосування послідовних і широковідомих технологій і стандартів, а також співпраці багатьох агенцій з мережного адміністрування. Існують організації, створені для підтримки структури та стандартизації інтернет-протоколів і процесів. До них належать Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), і Internet Architecture Board (IAB), а також багато інших.

1.4.4 Інтранет і Екстранет

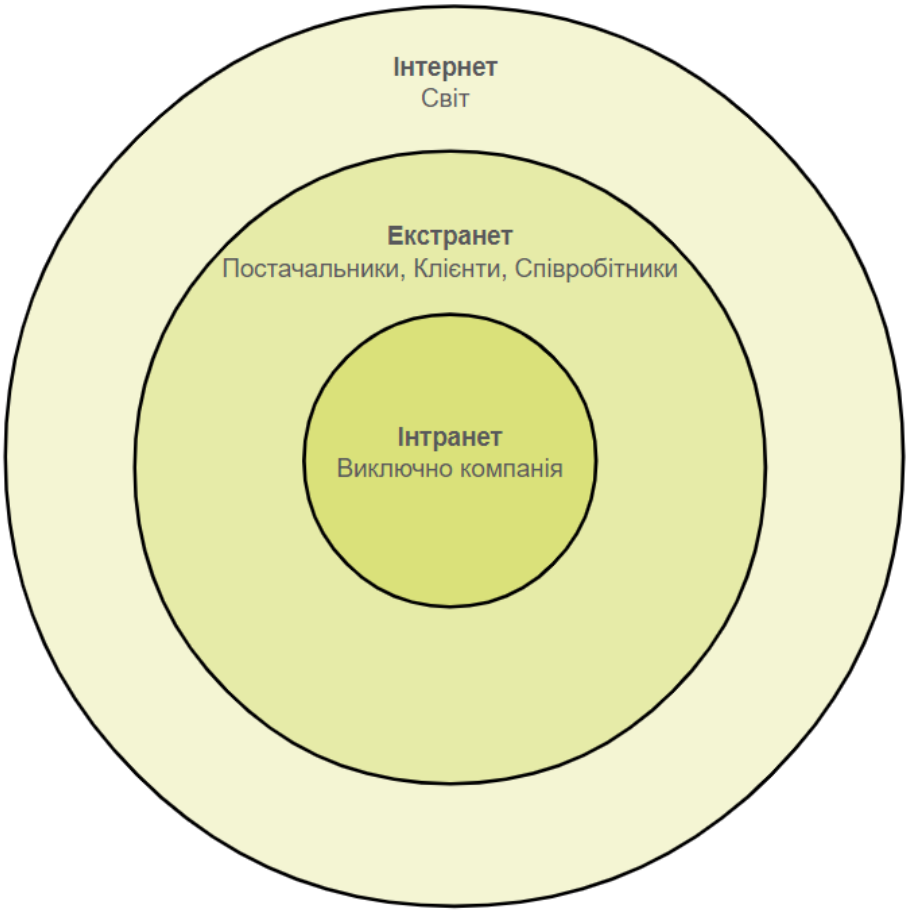
При позначенні мереж часто використовують ще два терміни, схожі на Інтернет: інтранет і екстранет

Інтрамережа (інтранет) — це термін, який використовується для позначення приватного об'єднання локальних і глобальних мереж, що належить організації. Інтранет призначений для доступу лише учасників організації, працівників або інших уповноважених осіб.

Організація може використовувати екстрамережу (екстранет) для забезпечення безпечного і надійного доступу для осіб, які працюють в іншій організації, але потребують доступу до корпоративних даних. Ось кілька прикладів:

- Компанія надає доступ постачальникам і підрядникам
- Лікарня підтримує систему реєстрації на прийом до лікаря для пацієнтів
- Місцеве управління освіти, яке формує бюджет та інформацію про персонал для шкіл свого округу

На рисунку зображено рівні доступу, які різні групи мають до інтрамережі компанії, екстранету компанії та Інтернету.



1.4.5 Питання для самоперевірки - Основні типи мереж

1. Яка мережна інфраструктура забезпечує доступ для користувачів і кінцевих пристроїв на невеликій географічній площі, і як правило, використовується у відділі на підприємстві, вдома або на невеликій фірмі?

   - ◯ Екстранет
   - ◯ Інтранет
   - ◯ LAN
   - ◯ WAN

2. Яку мережну інфраструктуру може використовувати організація для забезпечення безпечного і надійного доступу для осіб, які працюють в іншій організації, але потребують доступу до даних установи?

   - ◯ Екстранет
   - ◯ Інтранет
   - ◯ LAN
   - ◯ WAN

3. Яка мережна інфраструктура забезпечує доступ до інших мереж на значних географічних відстанях, які належать і обслуговуються великими корпораціями або провайдером телекомунікаційних послуг?

   - ◯ Екстранет
   - ◯ Інтранет
   - ◯ LAN
   - ◯ WAN

1. Яка мережна інфраструктура забезпечує доступ для користувачів і кінцевих пристроїв на невеликій географічній площі, і як правило, використовується у відділі на підприємстві, вдома або на невеликій фірмі?

Правильно!

- ○ Екстранет
- ○ Інтранет
- ◉ LAN
- ○ WAN

2. Яку мережну інфраструктуру може використовувати організація для забезпечення безпечного і надійного доступу для осіб, які працюють в іншій організації, але потребують доступу до даних установи?

Правильно!

- ◉ Екстранет
- ○ Інтранет
- ○ LAN
- ○ WAN

3. Яка мережна інфраструктура забезпечує доступ до інших мереж на значних географічних відстанях, які належать і обслуговуються великими корпораціями або провайдером телекомунікаційних послуг?

Правильно!

- ○ Екстранет
- ○ Інтранет
- ○ LAN
- ◉ WAN

1.5 Інтернет-з'єднання

1.5.1 Технології інтернет-доступу

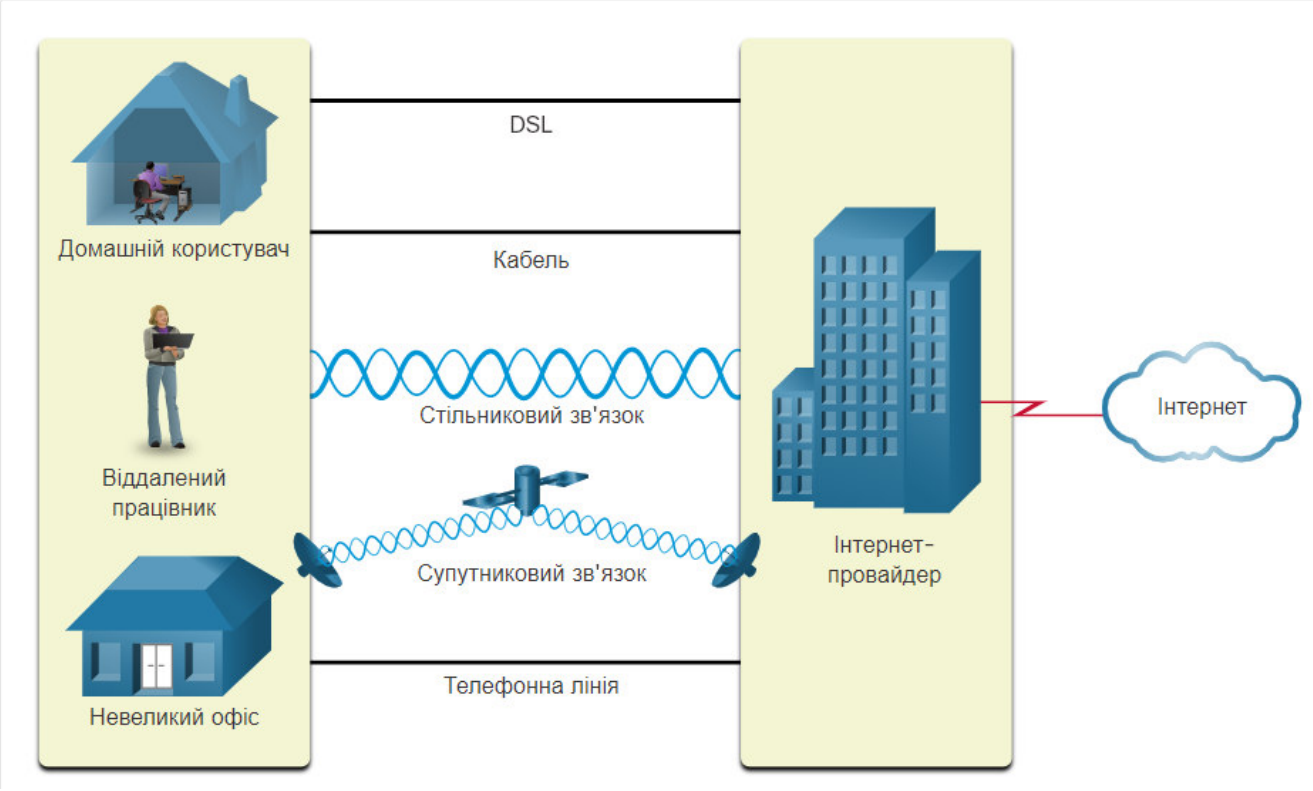
Отже тепер ви маєте базове уявлення про те, з чого складається мережа, а також про різні типи мереж. Але, як насправді під'єднати користувачів та організації до інтернету? Як ви, мабуть, здогадуєтесь, для цього існує багато способів.

Аби отримати доступу до інтернету домашні користувачі, віддалені працівники та невеликі офіси зазвичай потребують зв'язку з Інтернет-провайдером. Існують різні варіанти під'єднання, в залежності від постачальника послуг і географічного розташування. Проте, до найбільш поширених способів належать широкосмугове кабельне з'єднання, широкосмугова цифрова абонентська лінія (DSL), бездротові WAN і мобільні сервіси.

Організаціям зазвичай потрібен доступ до інших корпоративних сайтів, а також до інтернету. Для підтримки бізнес-послуг, включаючи IP-телефони, відеоконференції та сховище даних, потрібні швидкісні з'єднання. Постачальники послуг пропонують з'єднання рівня бізнес-класу. До цих послуг належать DSL для бізнесу, орендовані лінії та Metro Ethernet.

1.5.2 Під'єднання до Інтернету для дому та невеликого офісу

На рисунку зображені типові варіанти під'єднання для користувачів невеликих і домашніх офісів.



- **Кабельне з'єднання** - Зазвичай пропонується постачальниками послуг кабельного телебачення; сигнал даних мережі інтернет передається по тому ж коаксіальному кабелю, що використовується для передавання сигналу кабельного телебачення. Цей спосіб забезпечує під'єднання до мережі інтернет з високою пропускною здатністю і постійним доступом до мережі.
- **DSL** - Цифрові абонентські лінії (Digital Subscriber Lines) також забезпечують постійне високошвидкісне з'єднання з мережею інтернет. DSL використовує телефонну лінію. Загалом, користувачі домашніх і невеликих офісів під'єднуються за допомогою асиметричного DSL

(Asymmetrical DSL, ADSL), при якому швидкість завантаження (download) більша за швидкість передавання (upload).

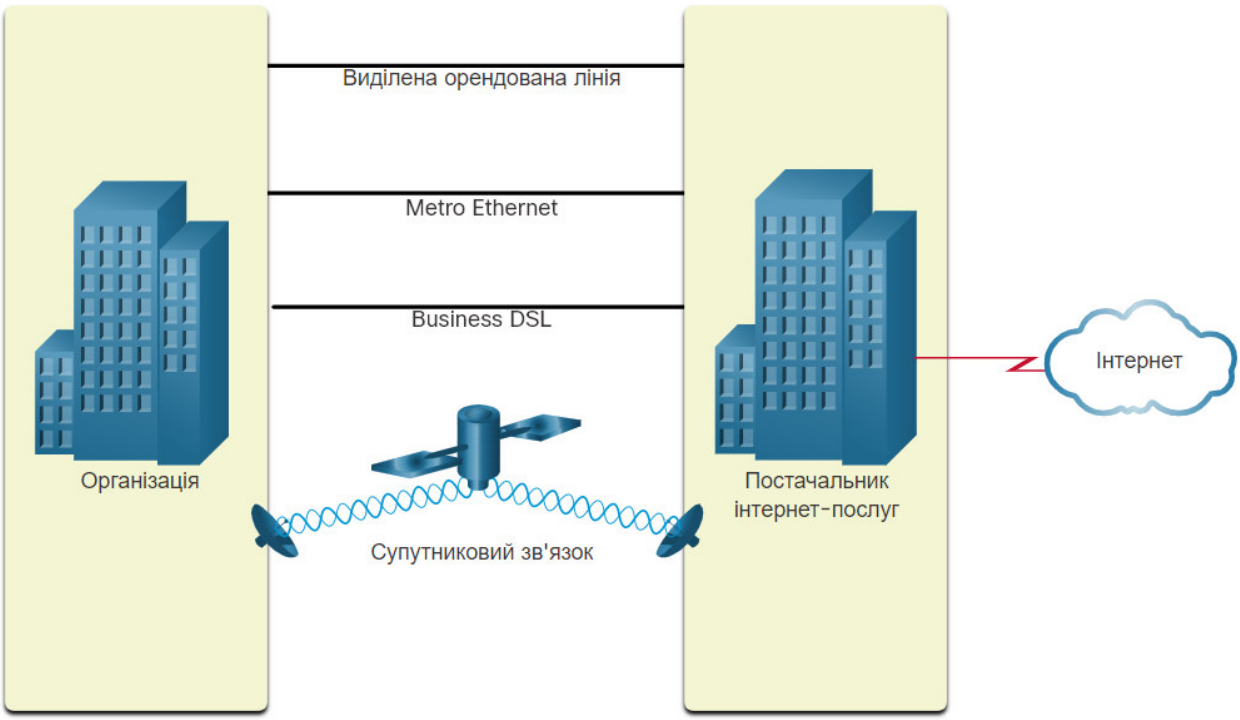
- **Стільниковий зв'язок** - Мобільний інтернет-доступ використовує стільникову мережу для з'єднання. У будь-якій точці, де доступний сигнал стільникової мережі, можна налаштувати інтернет-зв'язок. Продуктивність обмежується можливостями телефону і стільникової базової станції, до якої він під'єднується.
- **Супутниковий зв'язок** - Можливість доступу до мережі Інтернет через супутниковий зв'язок підійде для тих районів, де взагалі немає інших способів підключення до інтернету. Супутникові антени повинні перебувати в зоні прямої видимості супутника.
- **Комутовані телефонні лінії** - Недорогий варіант підключення з використанням телефонної лінії та модему. Низька пропускна здатність телефонної лінії є недостатньою для передавання великого обсягу даних. Однак такий спосіб з'єднання може бути корисний для мобільного доступу під час подорожі.

Вибір способу під'єднання залежить від географічного розташування і доступності постачальника послуг.

1.5.3 Корпоративне інтернет-з'єднання

Варіанти корпоративного з'єднання відрізняються від способів підключення, доступних для домашнього користувача. Компаніям може знадобитися більша пропускна здатність, виділена смуга пропускання та керовані послуги. Можливі варіанти під'єднання залежать від типу послуг, які пропонуються у заданому регіоні.

На рисунку зображені основні варіанти з'єднання для підприємств.



- **Виділена орендована лінія** - Це зарезервовані канали зв'язку в мережі постачальника послуг, які з'єднують географічно віддалені офіси для приватного передавання голосу та / або даних. Ці канали орендують з оплатою щомісяця або щороку.

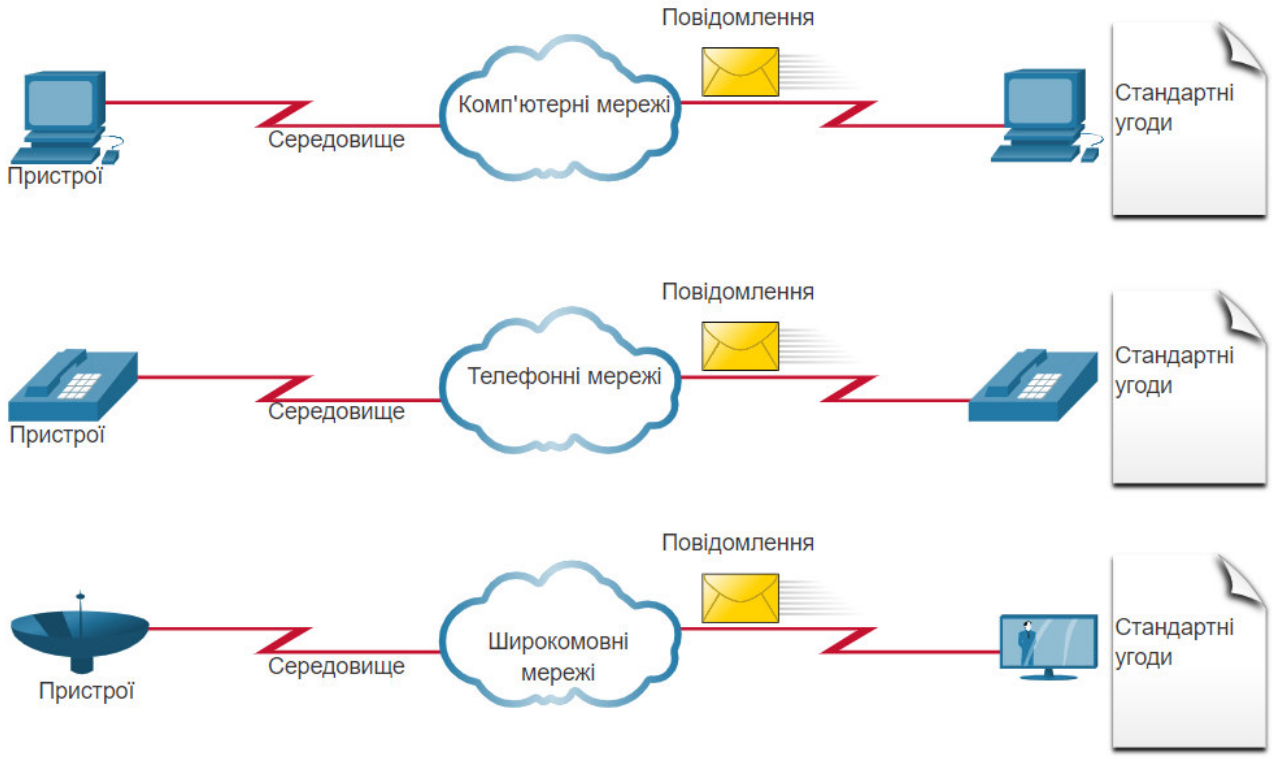
- **Metro Ethernet** - Також відомий як Ethernet WAN. У цьому розділі ми називатимемо його Metro Ethernet. Ця технологія розширює можливості Ethernet до рівня WAN. Ethernet є технологією локальних мереж, про що ви дізнаєтесь далі у розділі.
- **Business DSL** - Комерційний DSL доступний у різних форматах. Популярним вибором є симетрична цифрова абонентська лінія (Symmetric DSL, SDSL), подібна до користувацької версії DSL, проте забезпечує однаково високі швидкості завантаження і передавання.
- **Супутниковий зв'язок** - Супутниковий сервіс забезпечення з'єднання, коли кабельне підведення недоступне.

Вибір способу під'єднання залежить від географічного розташування і доступності постачальника послуг.

1.5.4 Конвергентна мережа

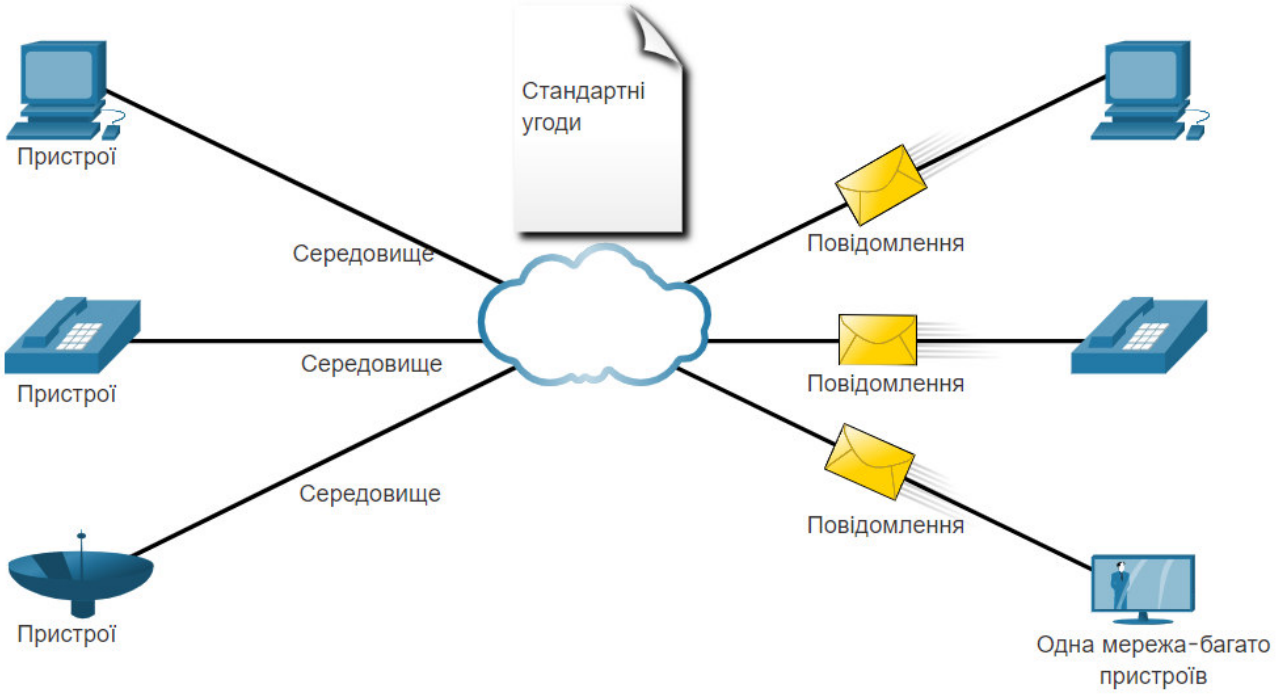
Традиційні відокремлені мережі

Уявіть школу, побудовану тридцять років тому. У ті часи деякі аудиторії під'єднувалися до мережі передавання даних за допомогою кабелю, телефонної мережі та телевізійної відео-мережі. Ці окремі мережі не мали можливості взаємодіяти між собою. Кожна мережа використовувала різні технології передавання сигналу зв'язку. Кожна мережа мала свій власний набір правил і стандартів для забезпечення успішної взаємодії. Різні сервіси надавалися різними мережами.



Конвергентні мережі

Сьогодні відокремлені мережі передавання даних, голосу та відео об'єдналися в одну. На відміну від традиційних мереж, конвергентні або змішані мережі здатні передавати дані, голос та відео між багатьма різними типами пристроїв по одній мережній інфраструктурі. Ця мережна система використовує однаковий набір правил, угод і стандартів впровадження. Конвергентні мережі зв'язку забезпечують функціонування декількох служб на базі однієї мережі.



1.5.5 Завантаження та інсталювання Packet Tracer

Це продемонструє вам як завантажити і встановити Packet Tracer. Ви будете використовувати Packet Tracer для моделювання створення і тестування мереж на вашому комп'ютері. Packet Tracer - це цікава, гнучка програма для роботи вдома, яка надасть вам можливість використовувати принципи подання мереж і теоретичні відомості, які ви щойно опанували, для побудови моделей мереж і дослідження відносно складних локальних і глобальних структур.

Студенти зазвичай використовують Packet Tracer для того, щоб:

- Підготуватися до сертифікаційного іспиту.
- Отримати практичні навички з матеріалу, який вивчається в курсах.
- Вдосконалити свої навички перед співбесідою з приводу працевлаштування.
- Дослідити чи вплине на роботу мережі додавання нових технологій до вже існуючого проекту.
- Отримати навички, необхідні для працевлаштування у галузі Інтернету речей.
- Взяти участь у змаганнях світового рівня (знайдіть на Facebook змагання 2017 PT 7 Design Challenge).

Packet Tracer є важливим інструментом навчання, який використовується під час вивчення багатьох курсах Мережної Академії Cisco.

Щоб отримати та встановити власну копію програми Cisco Packet Tracer, дотримуйтесь таких простих кроків:

Крок 1. Увійдіть до Cisco Networking Academy на сторінку "I'm Learning" ("Я навчаюся").

Крок 2. Перейдіть до вкладки Resources (Ресурси).

Крок 3. Виберіть "Download Packet Tracer" ("Завантажити Packet Tracer").

Крок 4. Виберіть версію Packet Tracer, яка вам підходить.

Крок 5. Збережіть файл на своєму комп'ютері.

Крок 6. Запустіть програму встановлення Packet Tracer.

1.5.6 Початок роботи з Packet Tracer

Packet Tracer - це інструмент для моделювання реальних мережі. Він має три основні меню, які дозволяють:

- додавати пристрої та з'єднувати їх за допомогою кабельного або бездротового зв'язку.
- обирати, видаляти, перевіряти, позначати і групувати компоненти у вашій мережі.
- керувати мережею, відкриваючи існуючі/тестові приклади мереж, зберігати поточну схему налаштувань і змінювати профіль або параметри користувача.

Якщо ви використовували такі програми, як текстовий редактор або електронні таблиці, ви вже знайомі з командами меню File (Файл), розташованими на верхній панелі меню. Команди Open (Відкрити), Save (Зберегти), Save As (Зберегти як), та Exit (Вихід) працюють так само, як у будь-якій іншій програмі, але існують дві команди, визначені саме для Packet Tracer.

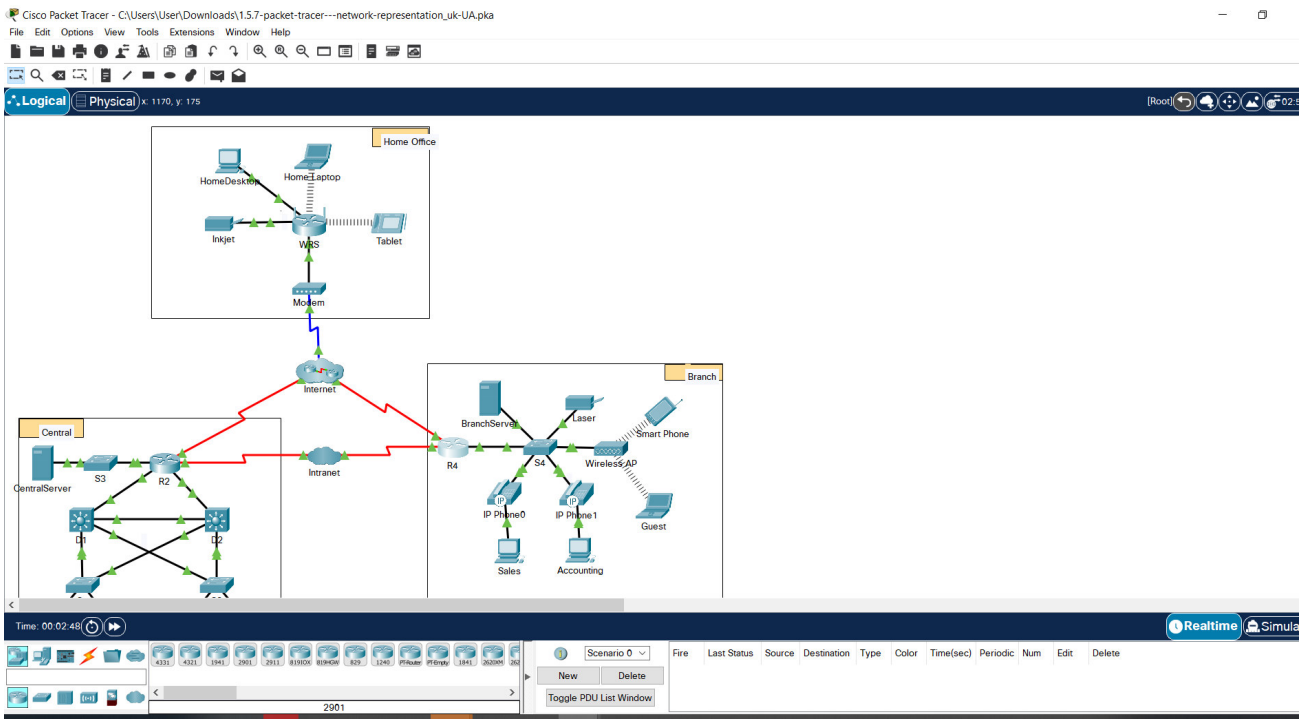
Команда Open Samples відкриє каталог попередньо налаштованих прикладів використання і налаштування різних мережних та IoT-пристроїв, які підтримуються у Packet Tracer.

Команда Exit and Logout видаляє реєстраційну інформацію для даної копії Packet Tracer і вимагає від іншого користувача Packet Tracer повторно виконати процедуру входу.

Подивіться відео, щоб дізнатись, як використовувати меню і як створити свою першу мережу у Packet Tracer.

1.5.7 Packet Tracer - Подання мережі

У цьому завданні ви дізнаєтесь про те, як використовувати Packet Tracer для моделювання мереж.



1.6 Надійні мережі

1.6.1 Мережна архітектура

Чи траплялося вам, щоб під час роботи онлайн, "падав інтернет"? Як ви вже знаєте, інтернет не може впасти, просто ви втрачали з ним зв’язок. Погодьтесь, це дуже засмучує. Оскільки так багато людей у світі покладаються на доступ до мереж у роботі та навчанні, важливо, щоб мережі були надійними. У цьому контексті надійність означає більше ніж просто з'єднання з інтернетом. Ця тема зосереджена на чотирьох аспектах надійності мережі.

Роль мережі змінилася з тих часів, коли мережі використовувалися суто для передавання даних. Зараз це система, яка забезпечує зв'язок між людьми і пристроями для обміну інформацією у конвергентному мережному середовищі. Для ефективного функціонування і розширення у таких умовах, мережа повинна будуватися з дотриманням стандартів мережної архітектури.

Мережі також підтримують широкий діапазон застосунків і сервісів. Вони повинні працювати на основі кабелів різних типів із залученням розмаїття пристроїв, що складають фізичну інфраструктуру. Термін "мережна архітектура" в цьому контексті позначає технології, що підтримують інфраструктуру, і запрограмовані сервіси та правила, або протоколи, які переміщують дані по всій мережі.

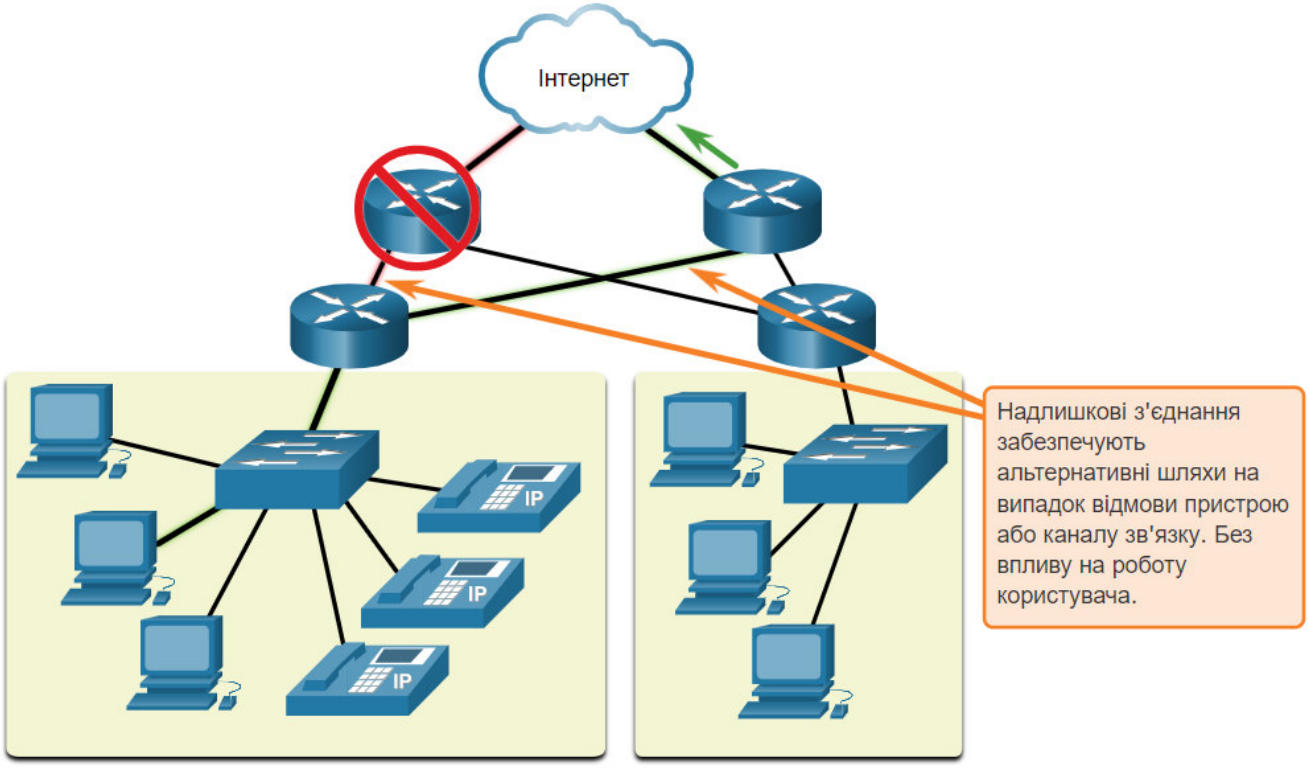
У міру розвитку мереж ми з'ясували, що для задоволення очікувань користувачів існує чотири **основні характеристики, яким повинні відповідати мережні архітектури**:

- Відмовостійкість
- Масштабованість
- Якість обслуговування (QoS)
- Безпека

1.6.2 Відмовостійкість

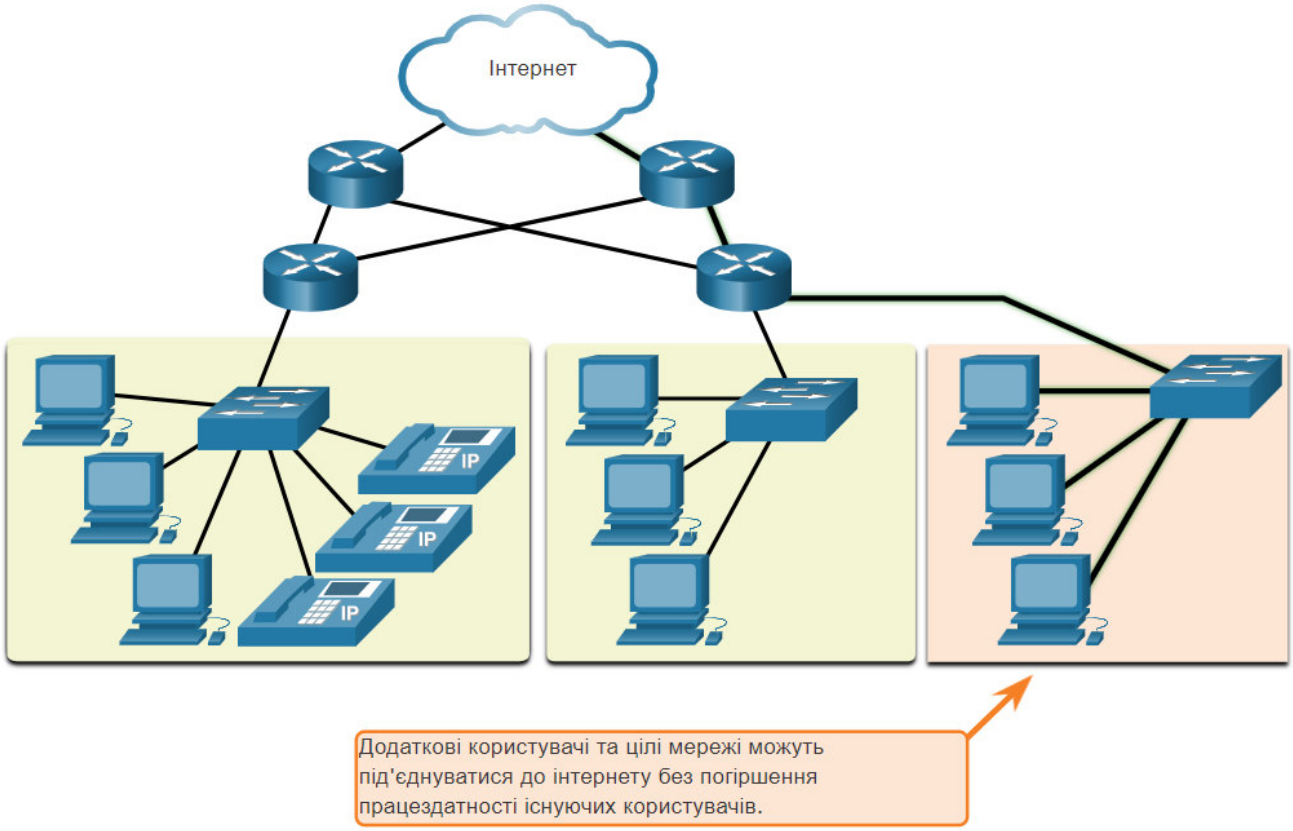
Відмовостійка мережа - це мережа, що обмежує кількість пристроїв, які б відчули на собі вплив відмови. Вона побудована для швидкого відновлення при виникненні такого збою. Такі мережі передбачають створення декількох шляхів, що прокладаються між джерелом та отримувачем повідомлення. При виході з ладу одного каналу зв'язку, повідомлення миттєво надсилатимуться іншим шляхом. Наявність декількох шляхів до пункту призначення відома як надлишковість або резервування (redundancy).

Реалізація мережі з комутацією пакетів є одним зі способів забезпечення надійності мереж. При комутації пакетів трафік розбивається на пакети, які передаються по спільних каналах зв'язку. Окреме повідомлення, таке як електронний лист або відеопотік, розбивається на декілька блоків повідомлень, які називають пакетами. Кожен пакет обов'язково містить адресну інформацію про джерело і отримувача повідомлення. Маршрутизатори в мережі перенаправляють пакети на основі поточних умов передавання даних. Це означає, що всі пакети одного повідомлення, можуть обирати різні шляхи аби дістатися до спільного пункту призначення. Як показано на рисунку, користувач не підозрює і не відчуває впливу динамічної зміни маршруту в разі відмови основного каналу зв'язку.



1.6.3 *Масштабованість*

Масштабована мережа швидко розгортається для підтримки нових користувачів і застосунків, без погіршення працездатності служб, до яких звертаються уже залучені користувачі. На рисунку показано, як нова мережа легко додається до існуючої мережі. Масштабованість мереж досягається завдяки дотриманню проектувальниками прийнятих стандартів і протоколів. Це дозволяє постачальникам програмного й апаратного забезпечення зосередитися на вдосконаленні продуктів та послуг, без необхідності розробки нового набору правил для роботи в мережі.

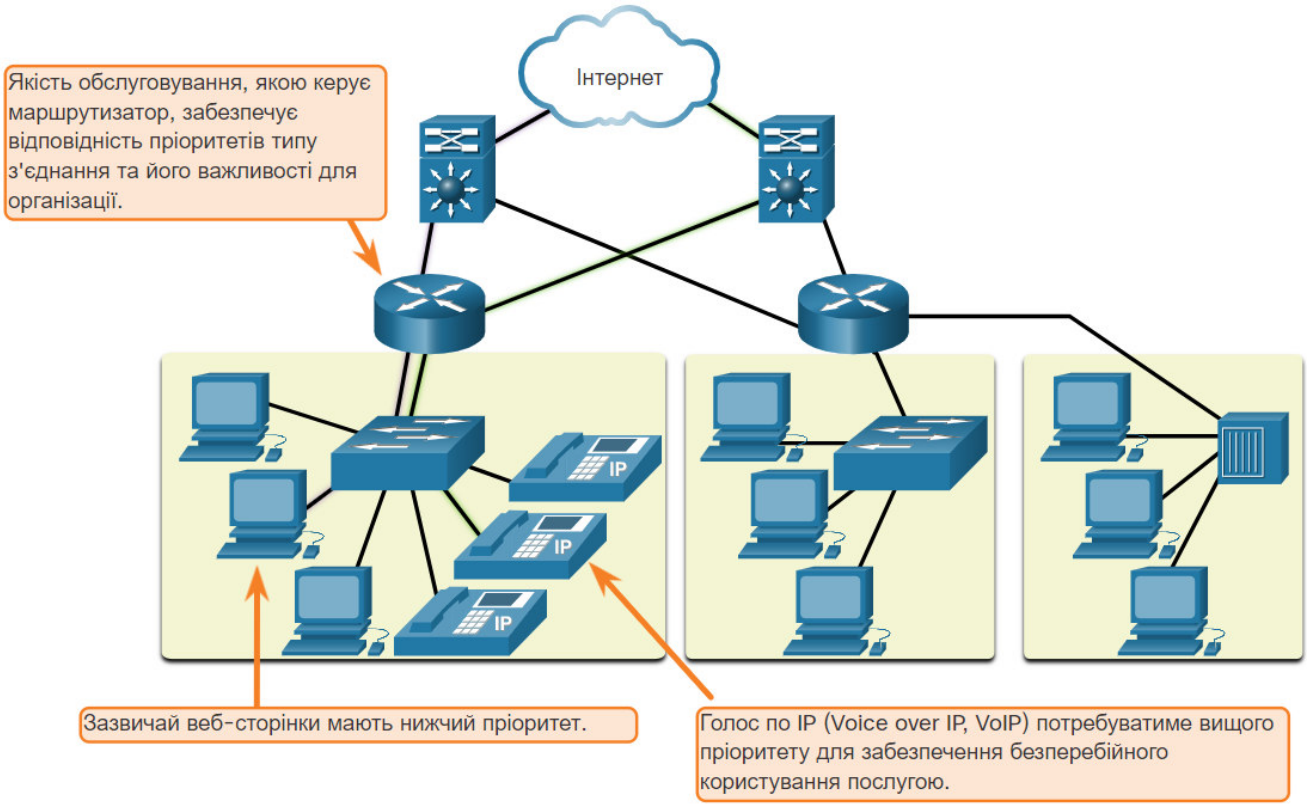


1.6.4 *Якість обслуговування (QoS)*

Якість обслуговування (Quality of Service, QoS) - це надзвичайно актуальна потреба сучасних мереж. Нові, доступні для використання у мережі, програми, такі як передавання голосу та відео у реальному часі, висувають підвищені вимоги щодо якості наданих послуг. Чи траплялося вам переглядати відео з постійним перериванням і затримками? Оскільки дані, голос та відео-контент поєднуються в одній мережі, QoS стає основним механізмом керування перевантаженістю та забезпечення надійної доставки вмісту для усіх користувачів.

Тиснява трапляється коли попит на пропускну здатність перевищує доступні ресурси каналів зв'язку. Пропускна здатність мережі вимірюється в кількості бітів, які можуть передаватися за одну секунду, або у бітах за секунду (bps). При спробі одночасного передавання даних по мережі потреба у пропускній здатності мережі може перевищувати її наявні ресурси, створюючи перевантаженість мережі.

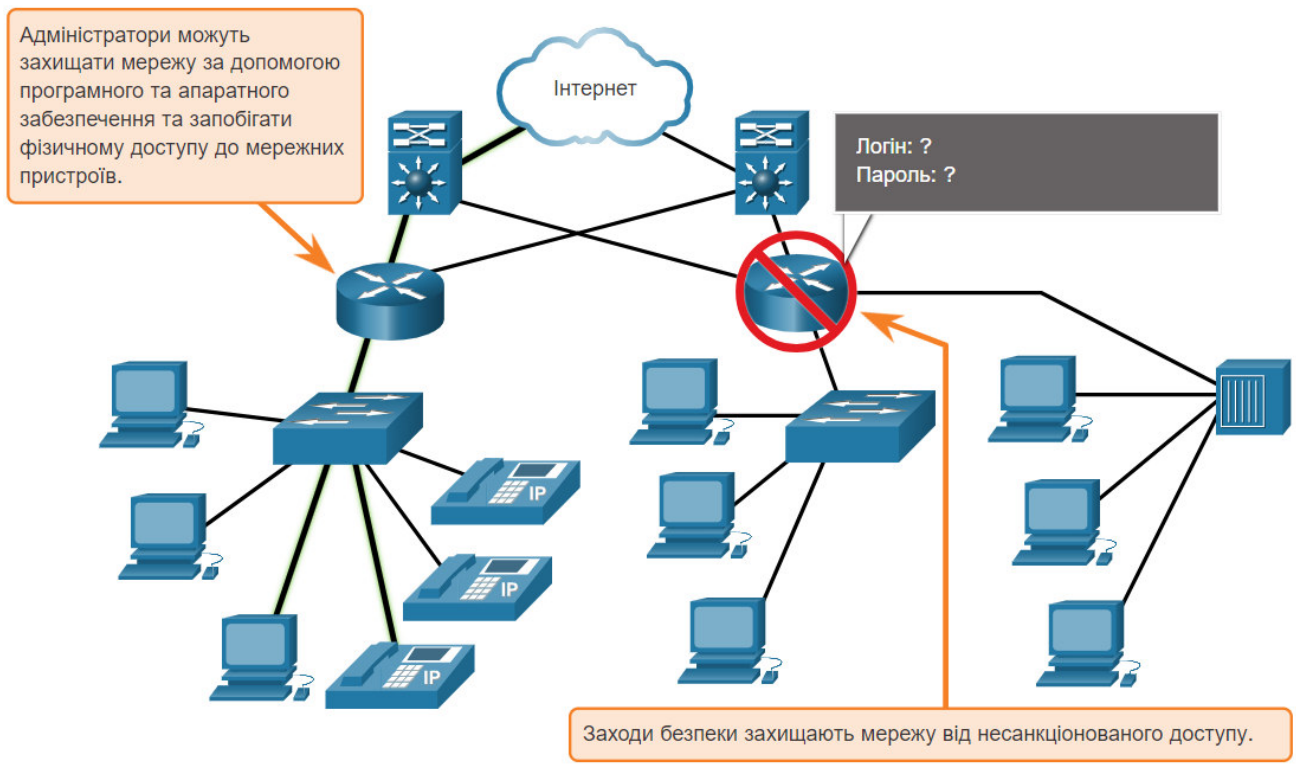
Коли обсяг трафіку більший, за той, що може транспортуватися по мережі, пристрої зберігатимуть пакети у пам'яті, допоки не вивільніться ресурси для їх передавання. На рисунку один користувач запитує веб-сторінку, а інший робить телефонний дзвінок. Згідно з політикою QoS маршрутизатор може керувати потоками даних і голосу, віддаючи перевагу голосовому з’єднанню при виникненні тисняви у мережі.



1.6.5 *Мережна безпека*

Мережна інфраструктура, послуги і дані, що містяться на під'єднаних до мережі пристроях, є важливими особистими і корпоративними активами. Адміністратори мережі повинні вирішувати два типи питань безпеки: безпека мережної інфраструктури та захист інформації.

Як показано на рисунку, убезпечення мережної інфраструктури передбачає фізичний захист пристроїв, які забезпечують з'єднання з мережею та запобігають несанкціонованому доступу до встановленого на них захисного програмного забезпечення.



Адміністратори мережі також повинні захищати інформацію, яка передається у пакетах по мережі, а також ту, що зберігається на під'єднаних до мережі пристроях. Досягти цілей безпеки мережі можна за умов дотримання трьох основних вимог.

- **Конфіденційність** - Конфіденційність даних означає, що лише уповноважені й авторизовані користувачі можуть отримувати доступ до даних.
- **Цілісність** - Цілісність даних запевняє користувачів, що інформація не була змінена під час передавання від джерела до отримувача.
- **Доступність** - Доступність даних гарантує авторизованим користувачам вчасний і надійний доступ до послуг з оброблення даних.

1.6.6 Питання для самоперевірки - Надійні мережі

1. Яка з чотирьох основних характеристик архітектури мережі передбачає дотримання проектувальниками прийнятих стандартів і протоколів?

   - ◯ відмовостійкість
   - ◯ масштабованість
   - ◯ QoS
   - ◯ безпека

2. Конфіденційність, цілісність і доступність є вимогами до якої з чотирьох основних характеристик мережної архітектури?

   - ◯ відмовостійкість
   - ◯ масштабованість
   - ◯ QoS
   - ◯ безпека

3. При застосуванні якої політики маршрутизатор може керувати потоком даних і голосовим трафіком, надаючи пріоритет голосовому зв'язку, якщо в мережі виникає перевантаженість?

   - ◯ відмовостійкість
   - ◯ масштабованість
   - ◯ QoS
   - ◯ безпека

4. Наявність декількох шляхів до пункту призначення відома як надлишковість або резервування. Якій характеристиці мережної архітектури це відповідає?

   - ◯ відмовостійкість
   - ◯ масштабованість
   - ◯ QoS
   - ◯ безпека

Перевірка:

1. Яка з чотирьох основних характеристик архітектури мережі передбачає дотримання проектувальниками прийнятих стандартів і протоколів?

Правильно!

- відмовостійкість
- (•) масштабованість
- QoS
- безпека

2. Конфіденційність, цілісність і доступність є вимогами до якої з чотирьох основних характеристик мережної архітектури?

Правильно!

- відмовостійкість
- масштабованість
- QoS
- (•) безпека

3. При застосуванні якої політики маршрутизатор може керувати потоком даних і голосовим трафіком, надаючи пріоритет голосовому зв'язку, якщо в мережі виникає перевантаженість?

Правильно!

- відмовостійкість
- масштабованість
- (•) QoS
- безпека

4. Наявність декількох шляхів до пункту призначення відома як надлишковість або резервування. Якій характеристиці мережної архітектури це відповідає?

Правильно!

- (•) відмовостійкість
- масштабованість
- QoS
- безпека

1.7 Тенденції розвитку мереж

1.7.1 Останні тенденції

На разі ви вже багато чого дізналися про мережі, а саме, з чого вони складаються, як вони об'єднують нас, і що потрібно для створення надійного з'єднання. Проте мережі, як і все інше, постійно змінюються. Існує декілька тенденцій у роботі мереж, про які ви, як студент NetAcad, повинні знати.

У міру виходу на ринок нових технологій та кінцевих пристроїв, підприємства і користувачі повинні повсякчас пристосовуватися до цього мінливого середовища. Існує кілька тенденцій мереж, які впливають на організації та споживачів:

- **Використання власного пристрою (Bring Your Own Device, BYOD)**
- **Онлайн-співпраця**
- **Відео-зв'язок**
- **Хмарні обчислення**

1.7.2 Використання власного пристрою (BYOD)

Концепція використання будь-якого пристрою, будь-якого складу, у будь-який спосіб, є основною світовою тенденцією, яка потребує значних змін у тому, як ми використовуємо пристрої та безпечно під'єднуємо їх до мереж. Вона має назву Bring Your Own Device, BYOD і дослівно перекладається як "Принеси свій власний пристрій".

BYOD стосується кінцевих користувачів, які вільні використовувати особисті інструменти для доступу до інформації та взаємодії у бізнесовій або корпоративній мережі. У зв'язку зі зростанням кількості користувацьких пристроїв та відповідним зниження їхньої вартості, працівники та студенти можуть мати сучасні обчислювальні та мережні пристрої для особистого користування. До них належать ноутбуки, планшети, смартфони та електронні книжки, окремо або спільно придбані установою/компанією або фізичною особою.

BYOD означає, що будь-який пристрій, належить будь-кому і використовується всюди.

1.7.3 Онлайн-співпраця

Люди під'єднуються до мережі не лише для доступу до застосунків з оброблення даних, але й задля взаємодії один з одним. Співпраця визначається як "акт колективної роботи разом з іншими над спільним проектом". Інструменти співпраці, такі як Cisco WebEx, подані на рисунку, забезпечують працівникам, студентам, викладачам, клієнтам і партнерам спосіб миттєвого з'єднання, взаємодії та досягнення своїх цілей.

Співпраця є важливим стратегічним пріоритетом, який організації використовують, аби залишатися конкурентоспроможними. Співпраця також посідає чильне місце в освіті. Студенти повинні співпрацювати, щоб допомагати одне одному у навчанні, розвивати навички роботи в команді, важливі при працевлаштуванні, та спільно виконувати командні проекти.

Cisco Webex Teams - це багатофункціональний інструмент співпраці, який дозволяє надсилати миттєві повідомлення одному або декільком користувачам, розміщувати зображення, публікувати відео та поширювати посилання. Кожен командний ‘простір’ зберігає історію всього, що у ньому публікувалося.

1.7.4 Відео-зв'язок

Ще одна грань мережних технологій, важлива для спілкування та співпраці, - це відео-з'єднання. Відео найчастіше використовується для передавання даних, взаємодії та розваг. Відеодзвінки можуть надходити до і від будь-кого, хто має інтернет-з'єднання, незалежно від місця перебування.

Відеоконференції є потужним інструментом для спілкування з іншими людьми у локальних і глобальних масштабах. Для організацій, які розширюють свої географічні та культурні границі, відео-зв'язок стає незамінним засобом ефективної співпраці.

1.7.6 Хмарні обчислення

Хмарні обчислення (Cloud computing) - це один зі способів доступу та зберігання даних. Хмарні обчислення дозволяють нам зберігати як особисті файли так і резервні копії диска на серверах в інтернеті. За допомогою хмари можна звертатися до програм обробки текстів і редагування фотографій.

Для бізнес-підприємств хмарні обчислення розширюють можливості IT, позбавляючи необхідності інвестувати у нову інфраструктуру, навчання персоналу або ліцензування нового програмного забезпечення. Ці послуги доступні за запитом і постачаються на будь-який пристрій у будь-яку точку світу без порушення безпеки чи функціональності.

Хмарні обчислення можливі через центри обробки даних. Центри обробки даних (ЦОД) - це засоби, що використовуються для розміщення комп'ютерних систем та пов'язаних з ними компонентів. Один такий центр може розміщуватися в одній кімнаті, або займати декілька поверхів чи навіть цілу будівлю розміром з торговий склад. ЦОД, як правило, дуже дорогі для створення та обслуговування. З цієї причини лише великі організації використовують приватні центри обробки даних для розміщення власних даних та надання послуг користувачам. Невеликі організації, які не можуть дозволити собі підтримувати власний ЦОД, мають змогу знизити загальну вартість власності, орендуючи сервер та послуги зберігання даних у компаній, що надають центри обробки даних у хмарі.

Задля безпеки, надійності та відмовостійкості постачальники хмар часто зберігають дані в розподілених центрах обробки даних. Зазвичай всі приватні або корпоративні дані не зберігаються на одному центрі обробки даних, а розподіляються по декількох ЦОД, розташованих у різних місцях.

Як показано в таблиці, існує чотири основні типи хмар: Публічні хмари (Public clouds), Приватні хмари (Private clouds), Гібридні хмари (Hybrid clouds) та Громадські хмари (Community clouds).

Типи хмар

Заголовок таблиці	
Тип хмар	**Опис**
Публічні хмари	Хмарні застосунки і сервіси, що пропонуються у публічній хмарі, доступні широким верствам населення. Послуги можуть надаватися як на безоплатній основі так і за принципом оплати за користування, наприклад, оплата за онлайн-сховище. Публічна хмара використовує інтернет для надання послуг.
Приватні хмари	Застосунки і сервіси, що пропонуються у приватній хмарі, призначаються конкретній організації або суб'єкту, наприклад уряду. Приватна хмара може налаштовуватися через приватну мережу організації, проте її буде дорого створювати і обслуговувати. Приватною хмарою також можна керувати поза межами організації з жорстким дотриманням правил безпеки.
Гібридні хмари	Гібридна хмара складається з двох або більше хмар (наприклад: частина приватна, частина публічна), де кожна частина залишається самостійним об’єктом, але обидві з'єднані з використанням спільної архітектури. Особам у гібридній хмарі надаватимуть рівні доступу до різних послуг на основі прав доступу користувачів.
Громадські хмари	Громадська хмара створюється виключно для використання певними організаціями. Гібридні хмари відрізняються від громадських за функціональними потребами, налаштованими для певної спільноти.

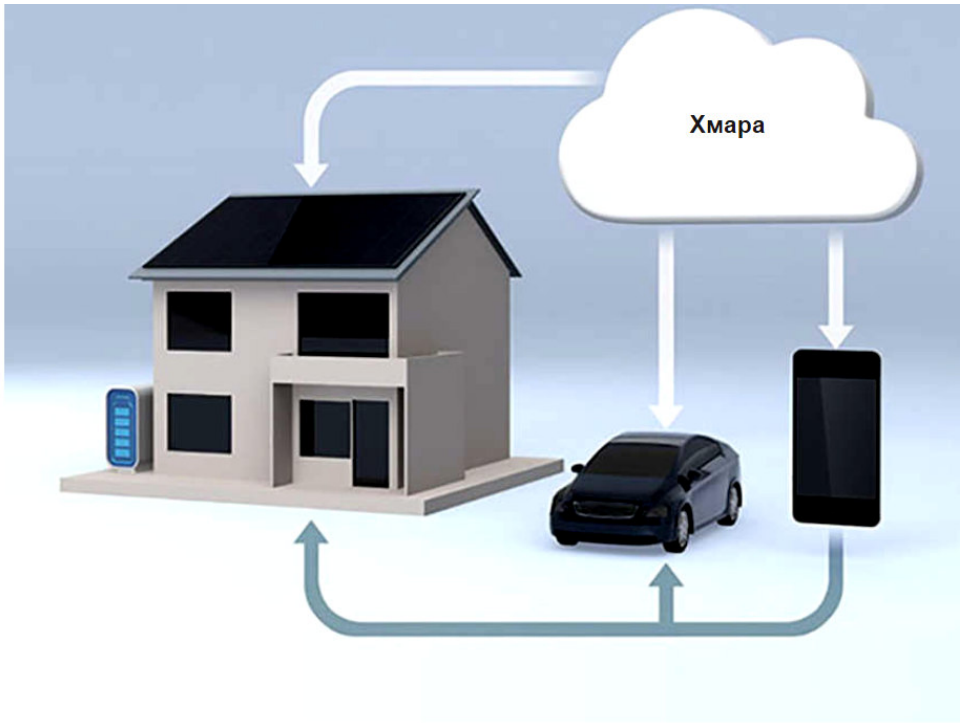
Заголовок таблиці	
Тип хмар	**Опис**
	Наприклад, організації охорони здоров'я повинні дотримуватися політики безпеки та закону (наприклад, HIPAA), які вимагають спеціальної автентифікації та конфіденційності. Громадські хмари використовуються кількома організаціями, які мають схожі потреби та інтереси. Вони схожі на публічне хмарне середовище із визначеними рівнями захисту, конфіденційності, а в дечому відповідають нормативним вимогам приватної хмари.

1.7.7 Технологічні тенденції для домашнього використання

Мережні новації впливають не лише на способи взаємодії на роботі та у навчанні, але й змінюють багато аспектів домашнього побуту. Однією з новітніх тенденцій є «розумний будинок».

Інтегрована до побутових приладів технологія розумного будинку забезпечує їх взаємодію з іншими пристроями, що робить їх більш «розумними» або автоматизованими. Наприклад, йдучи з дому на цілий день, ви можете підготувати страву і розмістити її в духовці. Якщо це розумна духовка, то її необхідно запрограмувати. Зокрема, її можна прив'язати до календаря подій, щоб визначати час, коли ви збираєтесь їсти, і налаштувати відповідний час початку і тривалість приготування. Виходячи зі змін у графіку, розумний прилад може навіть регулювати час і температуру приготування. Крім того, під'єднання через смартфон або планшет дозволяє вам безпосередньо взаємодіяти з духовкою для внесення будь-яких змін. Коли страва готова, піч надсилає вам попереджувальне повідомлення (або комусь, кого ви вказали), що їжа готова і підігрівається.

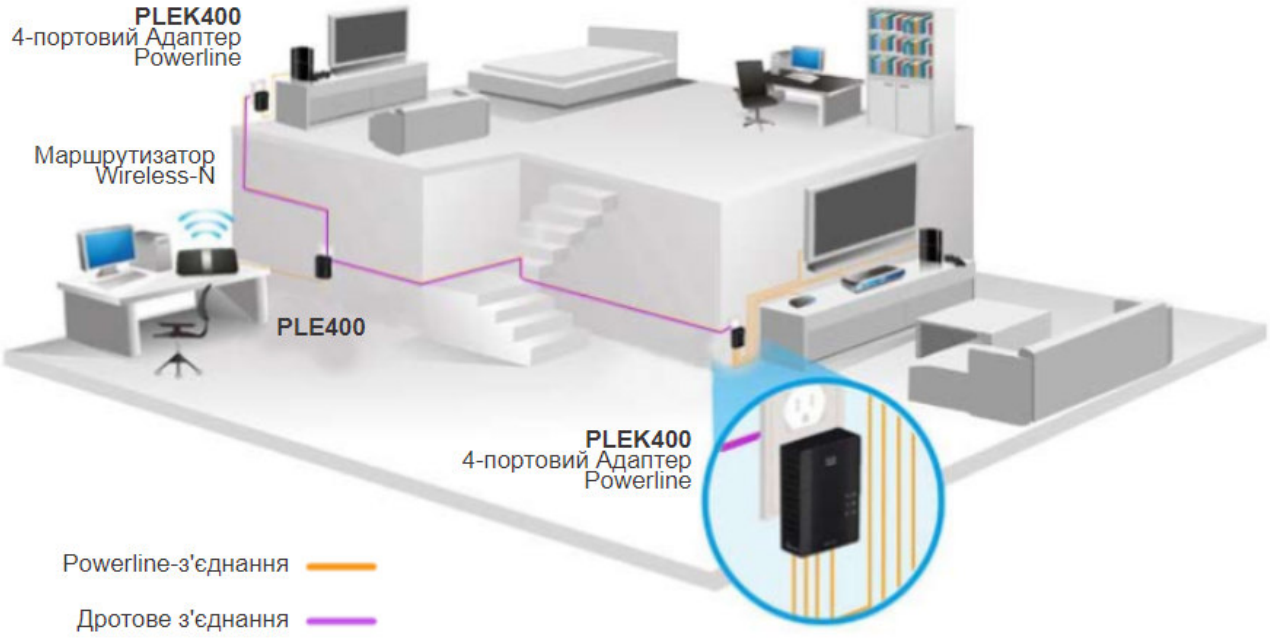
Наразі технологія розумного дому розробляється для усіх кімнат у будинку і стає такою ж звичною, як домашні мережі та швидкісні інтернет-технології.



На смартфоні через хмару оновлюється статус пристроїв розумного будинку та розумного автомобіля. Надалі користувач може взаємодіяти з ними через смартфон.

1.7.8 Мережа електроживлення

Мережа електроживлення (powerline) для домашніх мереж використовує існуючу електричну проводку для під'єднання, як показано на рисунку.



Використовуючи стандартний адаптер живлення, пристрої можуть під'єднуватися до локальної мережі там, де є електрична розетка. Не потрібно прокладати жодних кабелів, а додаткові витрати електроенергії мінімальні. Використовуючи ту ж проводку, що постачає електрику, мережі powerline передають інформацію на певних частотах.

Мережа електроживлення особливо корисна, коли точки бездротового доступу не можуть охопити усі домашні пристрої. Вона не здатна замінити виділений кабель у мережах передавання даних. Проте, ця технологія вважається гарною альтернативою, коли прокладання кабельних мереж або бездротове з’єднання неможливе або неефективне.

1.7.9 Бездротовий широкосмуговий зв'язок

У багатьох районах, де кабельні або DSL-з'єднання недоступні, для під'єднання до інтернету, може використовуватися бездротовий зв'язок.

Постачальник послуг бездротового інтернету

Постачальник послуг бездротового інтернету (Wireless Internet Service Provider, WISP) - це інтернет-провайдер, який під'єднує абонентів до визначеної точки доступу або гарячої точки за допомогою бездротових технологій домашніх

локальних мереж (**WLAN**). WISP найчастіше зустрічаються у сільській місцевості, де DSL або кабельні послуги недоступні.

Окрема передавальна вежа для антени може кріпитися до підвищеної конструкції, як от, водонапірна башта або радіовежа. На даху абонента у межах передавача WISP встановлюється невелика тарілка або антена. Блок доступу абонента під'єднується до дротової мережі всередині будинку. З точки зору домашнього користувача, налаштування не сильно відрізняється від DSL або кабельної служби. Основна відмінність полягає у тому, що замість фізичного кабелю, між домом та інтернет-провайдером прокладається бездротове з'єднання.

Бездротовий широкосмуговий сервіс

Ще одне бездротове рішення для дому та малого бізнесу - це бездротова широкосмугова мережа, зображена на рисунку.

Це рішення використовує ту саму стільникову технологію, що і смартфон. Встановлена зовні антена забезпечує бездротове або дротове з'єднання для домашніх пристроїв. У багатьох районах домашня бездротова широкосмугова мережа конкурує безпосередньо з DSL та кабельними послугами.

1.7.10 *Питання для самоперевірки - Мережні тенденції*

1. Яка технологія вважається гарним інструментом для проведення конференцій, у якій беруть участь колеги як з вашого міста, так і з інших міст або навіть країн?

   - ◯ BYOD
   - ◯ Відео-зв'язок
   - ◯ Хмарні обчислення

2. Яка технологія описує використання особистих інструментів для доступу до інформації та спілкування у мережі підприємства або кампусу?

   - ◯ BYOD
   - ◯ Відео-зв'язок
   - ◯ Хмарні обчислення

3. Яка технологія має такі різновиди, як Публічна, Приватна, Громадська та Гібридна?

   - ◯ BYOD
   - ◯ Відео-зв'язок
   - ◯ Хмарні обчислення

4. Яка технологія забезпечує під'єднання пристрою до мережі за допомогою електричної розетки?

   - ◯ Технологія розумного будинку
   - ◯ Powerline
   - ◯ Бездротовий широкосмуговий зв'язок

5. Яка технологія використовує ту саму стільникову технологію, що і смартфон?

   - ◯ Технологія розумного будинку
   - ◯ Powerline
   - ◯ Бездротовий широкосмуговий зв'язок

1. Яка технологія вважається гарним інструментом для проведення конференцій, у якій беруть участь колеги як з вашого міста, так і з інших міст або навіть країн?

Правильно!

- ○ BYOD
- ◉ Відео-зв'язок
- ○ Хмарні обчислення

2. Яка технологія описує використання особистих інструментів для доступу до інформації та спілкування у мережі підприємства або кампусу?

Правильно!

- ◉ BYOD
- ○ Відео-зв'язок
- ○ Хмарні обчислення

3. Яка технологія має такі різновиди, як Публічна, Приватна, Громадська та Гібридна?

Правильно!

- ○ BYOD
- ○ Відео-зв'язок
- ◉ Хмарні обчислення

4. Яка технологія забезпечує під'єднання пристрою до мережі за допомогою електричної розетки?

Правильно!

- ○ Технологія розумного будинку
- ◉ Powerline
- ○ Бездротовий широкосмуговий зв'язок

5. Яка технологія використовує ту саму стільникову технологію, що і смартфон?

Правильно!

- ○ Технологія розумного будинку
- ○ Powerline
- ◉ Бездротовий широкосмуговий зв'язок

1.8 Безпека мережі
1.8.1 Загрози безпеці

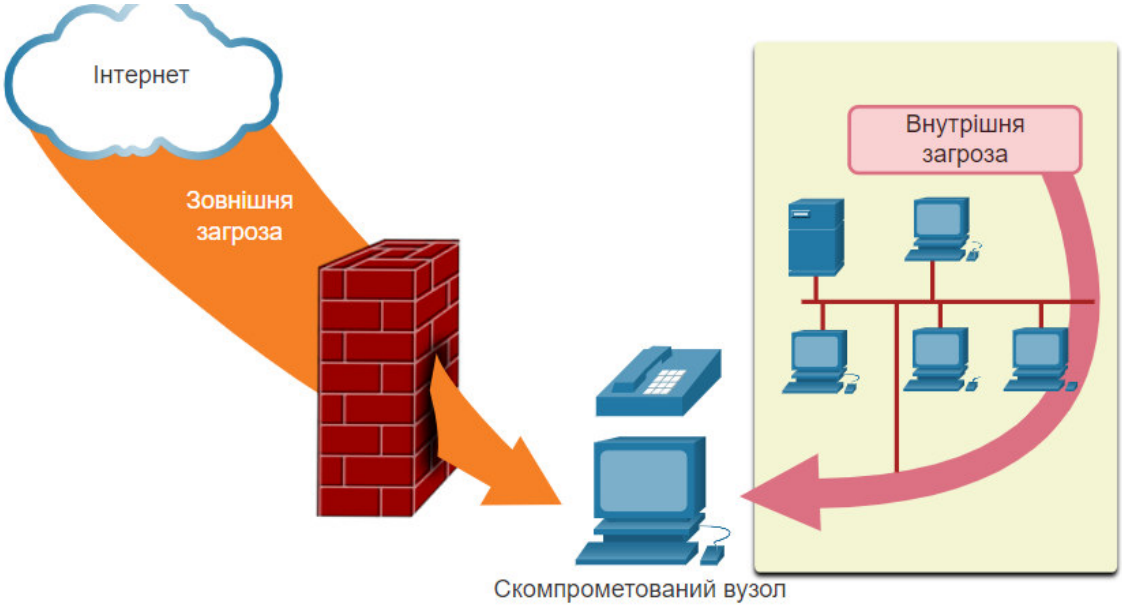
Без сумніву ви чули або читали новини про втручання до мережі компанії, і отримання зловмисниками доступу до особистої інформації тисяч клієнтів. З цієї причини безпека мережі завжди буде пріоритетним завданням для адміністраторів.

Мережна безпека є невід'ємною частиною комп'ютерних мереж, незалежно від того, чи це домашня мережа з єдиним каналом інтернет-зв'язку чи корпоративна мережа з тисячами користувачів. При забезпеченні мережного захисту потрібно брати до уваги середовище, а також інструменти та потреби мережі. Необхідно не лише захищати дані, але й зберегти якість обслуговування, на яку очікують користувачі мережі.

Безпека мережі передбачає використання протоколів, технологій, пристроїв, інструментів і методів, які захищають дані та пом'якшують наслідки загроз. Вектори загроз можуть бути зовнішніми або внутрішніми. Більшість зовнішніх загроз безпеці мережі сьогодні походять саме з інтернету.

Існує кілька поширених зовнішніх загроз для мереж:

- **Віруси, хробаки або троянські коні** - Шкідливе програмне забезпечення або код, запущений на пристрої користувача.
- **Шпигунська або рекламна програма** - Програми цього типу встановлюються на кінцевому пристрої і приховано збирають інформацію про користувача.
- **Атаки нульового дня** - Також відомі як атаки нульової години, виникають у перший день виявлення вразливості.
- **Напади зловмисника** - Зловмисник атакує пристій користувача або мережні ресурси.
- **Атаки з відмови в обслуговуванні** - Ці атаки сповільнюють роботу або зумовлюють відмову застосунків та процесів на мережному пристрої.
- **Перехоплення або крадіжка даних** - Ця атака захоплює приватну інформацію у мережі організації.
- **Крадіжка ідентичності** - Ця атака призначена для крадіжки облікових даних користувача з метою доступу до приватних даних.



Однаково важливо зважати на внутрішні загрози. Було проведено багато досліджень, які показали, що найпоширеніші втрати даних трапляються саме через внутрішніх користувачів

мережі. Сюди можна віднести втрату або викрадення пристроїв, випадкові зловживання з боку працівників, а в бізнес-середовищі - навіть зловмисні наміри деяких працівників. Із розвитком стратегій BYOD, корпоративні дані стають дедалі вразливішими. Тому, як показано на рисунку. розробляючи політику безпеки, важливо вирішувати як зовнішні, так і внутрішні загрози безпеці.

1.8.2 Безпекові рішення

Не існує єдиного рішення, яке б захистило від різного роду наявних загроз. З цієї причини безпека повинна запроваджуватися на декількох рівнях, із використанням більш ніж одного рішення. Якщо один захисний компонент не зможе виявити загрозу та убезпечити мережу, іншим це може вдатися.

Зазвичай для захисту домашньої мережі достатньо базових рішень. Як правило, користувач запроваджує захист на кінцевих пристроях, а також у точці під'єднання до Інтернету, і навіть може покладатися на договірні послуги від Інтернет-провайдера.

Для домашньої або невеликої офісної мережі визначено такі основні компоненти безпеки:

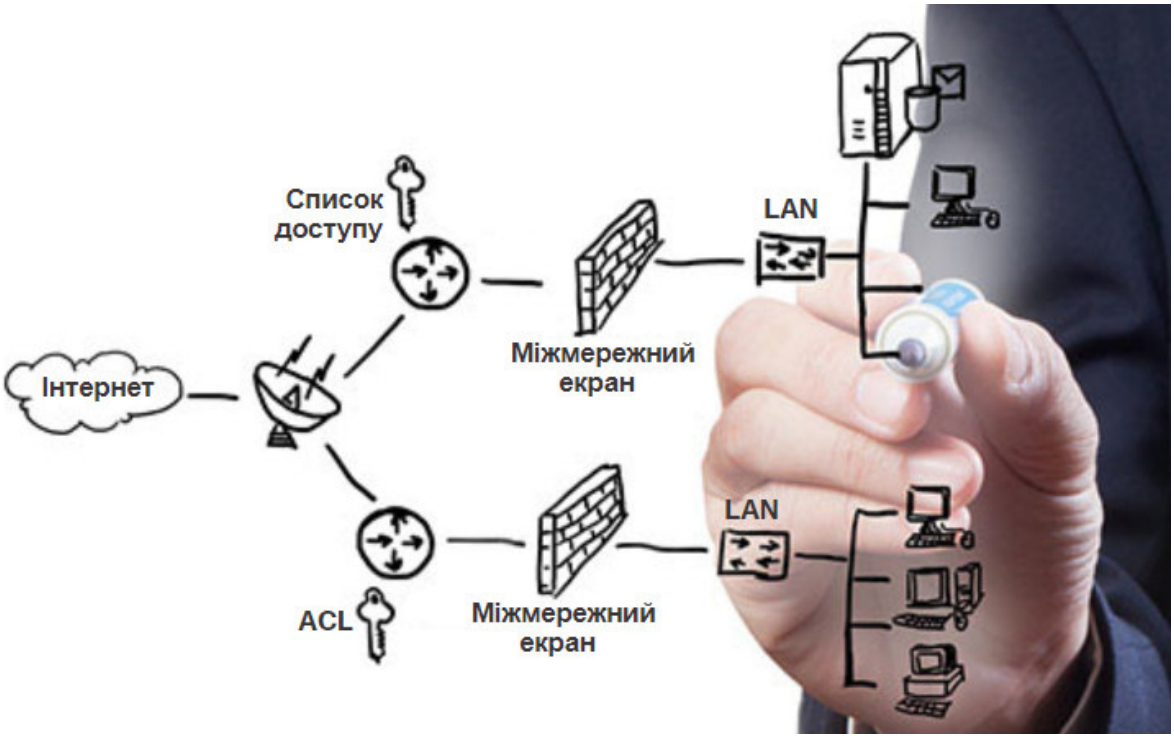
- **Антивірус і антишпигун** - Ці програми допомагають захистити кінцеві пристрої від ураження шкідливим програмним забезпеченням.
- **Фільтрування за допомогою міжмережного екрану** -Міжмережний екран (брандмауер, firewall) блокує несанкціоновані звернення, які надходять до мережі або ініціюються з неї. Може включати в себе систему брандмауера на основі вузла, яка запобігає неавторизованому доступу до кінцевого пристрою, або забезпечення базової фільтрації на домашньому маршрутизаторі, для попередження підозрілих звернень до мережі із зовнішнього світу.

На противагу цьому, реалізація захисту корпоративної мережі зазвичай передбачає використання багатьох компонентів, вбудованих у мережу для контролю та фільтрації трафіку. В ідеалі всі компоненти працюють разом, що мінімізує обслуговування та покращує безпеку. Великі корпоративні мережі використовують антивіруси, антишпигунські програми та фільтрування за допомогою міжмережних екранів, проте вони також вимагають інших засобів безпеки:

- **Спеціалізовані системи міжмережних екранів** - Забезпечують розширені можливості брандмауера, які здатні ретельніше фільтрувати велику кількість трафіку.
- **Списки контролю доступу (Access Control Lists, ACL)** - Додатково перевіряють звернення і потоки трафіку на основі IP-адрес і цільових застосунків.
- **Системи запобігання вторгненням (Intrusion Prevention Systems, IPS)** - Ідентифікують загрози, що швидко поширюються, такі як атаки нульового дня або нульові години.
- **Віртуальні приватні мережі (Virtual Private Networks, VPN)** - Забезпечують захищений віддалений доступ до ресурсів організації.

Вимоги щодо безпеки мережі повинні враховувати середовище, а також різні програми та обчислювальні потреби. Як для домашніх так і корпоративних мереж потрібно мати можливість захистити дані, зберігаючи якість обслуговування, на яку очікують користувачі мережі. Крім того, впроваджені заходи безпеки повинні адаптуватися до щораз більших та мінливих мережних тенденцій.

Вивчення загроз мережній безпеці та методів пом'якшення наслідків починається з чіткого розуміння основної інфраструктури комутації та маршрутизації, яка використовується для організації мережних служб.



1.8.3 *Питання для самоперевірки - Мережна безпека*

1. Яка атака призводить до сповільнення роботи або відмови обладнання та програм?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

2. Яке рішення створює безпечне з'єднання для віддалених працівників?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

3. Який засіб запобігає несанкціонованому доступу до вашої мережі?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

4. Який з варіантів описує мережну атаку, яка виникає у перший день виявлення уразливості?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

5. Який варіант описує шкідливий код, що запускається на пристроях користувача?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

4. Який з варіантів описує мережну атаку, яка виникає у перший день виявлення уразливості?

✓ Правильно!

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◉ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

5. Який варіант описує шкідливий код, що запускається на пристроях користувача?

✓ Правильно!

- ◯ Міжмережний екран
- ◉ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

1. Яка атака призводить до сповільнення роботи або відмови обладнання та програм?

Правильно!

- ○ Міжмережний екран
- ○ Вірус, хробак або троянський кінь
- ○ Нульовий день або нульова година
- ○ Віртуальна приватна мережа (VPN)
- ◉ Відмова в обслуговуванні (DoS)

2. Яке рішення створює безпечне з'єднання для віддалених працівників?

Правильно!

- ○ Міжмережний екран
- ○ Вірус, хробак або троянський кінь
- ○ Нульовий день або нульова година
- ◉ Віртуальна приватна мережа (VPN)
- ○ Відмова в обслуговуванні (DoS)

3. Який засіб запобігає несанкціонованому доступу до вашої мережі?

Правильно!

- ◉ Міжмережний екран
- ○ Вірус, хробак або троянський кінь
- ○ Нульовий день або нульова година
- ○ Віртуальна приватна мережа (VPN)
- ○ Відмова в обслуговуванні (DoS)

1.10.2 Контрольна робота з розділу - Сучасні мережні технології

1. Під час планової перевірки технік виявив, що встановлене на комп'ютері програмне забезпечення таємно збирає дані про веб-сайти, які відвідували користувачі. Який тип загрози впливає на цей комп'ютер?

- ◯ шпигунське ПЗ
- ◯ атака DoS
- ◯ атака нульового дня
- ◯ крадіжка ідентичності

2. Який термін позначає мережу, яка забезпечує постачальникам, замовникам і співробітникам захищений доступ до корпоративних систем?

- ◯ extendednet
- ◯ екстранет
- ◯ Інтернет
- ◯ інтранет

3. Велика корпорація змінила свою мережу, щоб дозволити користувачам отримувати доступ до мережних ресурсів зі своїх персональних ноутбуків і смартфонів. Якій мережній тенденції це відповідає?

- ◯ відеоконференція
- ◯ онлайн-співпраця
- ◯ хмарні обчислення
- ◯ BYOD

4. Що таке ISP?

- ◯ Це орган зі стандартизації, який розробляє стандарти кабельних мереж та їх прокладання.
- ◯ Це протокол, який визначає спосіб взаємодії комп'ютерів у локальній мережі.
- ◯ Це мережний пристрій, який поєднує в собі функціональність декількох різних мережних пристроїв.
- ◯ Це організація, яка надає приватним особам і підприємствам послуги під'єднання до Інтернету.

5. У яких умовах рекомендовано використовувати WISP?

- ◯ квартира у будинку з кабельним виходом в Інтернет
- ◯ будинок з декількома бездротовими пристроями
- ◯ Інтернет-кафе у місті
- ◯ ферма у сільській місцевості без дротового широкосмугового доступу

6. Яка характеристика мережі сприяє її швидкому росту для підтримки нових користувачів і застосунки, без негативного впливу на працездатність послуг, що надаються існуючим користувачам?

- ◯ доступність
- ◯ масштабованість
- ◯ надійність
- ◯ якість обслуговування

7. Коледж будує новий гуртожиток на території кампусу. Робітники риють землю для прокладання нового водопроводу для гуртожитку. В ході робіт випадково пошкоджується оптоволоконний кабель, який з'єднує два гуртожитки із центром обробки даних кампусу. Попри це, студенти в гуртожитках відчули лише нетривале переривання у роботі мережі. Про яку характеристику мережі йдеться?

- ◯ відмовостійкість
- ◯ цілісність
- ◯ безпека
- ◯ масштабованість
- ◯ якість обслуговування (QoS)

8. Які дві характеристики масштабованої мережі? (Оберіть дві.)

- ☐ легко перевантажується при збільшенні обсягів трафіку
- ☐ підходить для модульних пристроїв, які допускають розширення
- ☐ розростається, не впливаючи на існуючих користувачів
- ☐ пропонує обмежену кількість застосунків
- ☐ не така надійна, як невелика мережа

9. Який пристрій забезпечує функцію визначення шляху, яким повинні передаватися повідомлення між різними мережами?

- ◯ міжмережний екран
- ◯ веб-сервер
- ◯ DSL-модем
- ◯ маршрутизатор

10. Які два варіанти Інтернет-з'єднання не вимагають підведення фізичних кабелів до будівлі? (Оберіть два.)

- ☐ DSL-з'єднання
- ☐ стільникове з'єднання
- ☐ супутникове з'єднання
- ☐ комутоване телефонне з'єднання
- ☐ виділена орендована лінія

11. До якого типу мережі повинен мати доступ домашній користувач для здійснення покупок в Інтернеті?

- ◯ Інтернет
- ◯ локальна мережа
- ◯ інтранет
- ◯ екстранет

12. Як BYOD змінює спосіб, у який компанії розгортають мережі?

- ◯ BYOD забезпечує гнучкість у питанні, де і як користувачі можуть отримати доступ до мережних ресурсів.
- ◯ BYOD -пристрої коштують дорожче ніж пристрої, які купує організація.
- ◯ Користувачі BYOD самі несуть відповідальність за свою безпеку в мережі, тим самим зменшуючи необхідність у корпоративних політиках безпеки.
- ◯ BYOD вимагає від організацій купувати ноутбуки замість настільних ПК.

13. Працівник хоче отримати віддалений доступ до мережі організації у найбезпечніший спосіб. Яка мережна технологія забезпечить співробітнику захищений віддалений доступ до корпоративної мережі?

- ◯ ACL
- ◯ VPN
- ◯ BYOD
- ◯ IPS

14. Що таке Інтернет?

- ◯ Це мережа, заснована на технології Ethernet.
- ◯ Це приватна мережа організації з LAN- і WAN-з'єднаннями.
- ◯ Це засіб під'єднання мобільних пристроїв до мережі.
- ◯ Це засіб забезпечення зв'язку через взаємопов'язані глобальні мережі.

15. Які дві функції у мережі виконують кінцеві пристрої? (Оберіть дві.)

- ☐ Вони фільтрують потік даних для підвищення безпеки.
- ☐ Вони є інтерфейсом між людиною і мережею передавання даних.
- ☐ Вони генерують дані, які проходять по мережі.
- ☐ Вони забезпечують канал обміну мережними повідомленнями.
- ☐ Вони направляють дані по альтернативних шляхах у разі відмови каналів зв'язку.