Комп'ютерні мережі

Матеріали для самостійного вивчення (частина 1)

Створено на засадах курсів академії CISCO

Зміст

Сучасні мережні технології. Поняття комп’ютерних мереж, класифікація та характеристика

Завдання розділу

Назва розділу: Сучасні мережні технології

Завдання розділу: Пояснити переваги сучасних мережних технологій.

Назва теми	Мета вивчення теми
Мережі впливають на наше життя	Пояснити, як мережі впливають на наше повсякденне життя.
Компоненти мережі	Пояснити, як використовуються вузли та мережні пристрої.
Зображення мереж і топології	Пояснити способи подання мереж і те, як вони використовуються у мережних топологіях.
Основні типи мереж	Порівняти характеристики загальновідомих типів мереж.
Інтернет-з'єднання	Пояснити, як локальні і глобальні мережі реалізують з'єднання з мережею Інтернет.
Надійні мережі	Описати чотири основні критерії надійної мережі.
Тенденції розвитку мереж	Пояснити як такі тенденції як BYOD, онлайн-співпраця, відео і хмарні обчислення змінюють спосіб нашої взаємодії.
Безпека мережі	Визначити деякі основні загрози безпеці та рішення для усіх мереж.
IT-фахівець	Окреслити можливості працевлаштування у сфері мереж.

Мережі впливають на наше життя

Мережі об'єднують нас

Спілкування для нас майже так само важливе, як і наша залежність від повітря, води, їжі та притулку. У сучасному світі за допомогою мереж ми поєднані як ніколи раніше.

Без кордонів

- Світ без меж
- Глобальні спільноти
- Мережа людей

Компоненти мережі

Ролі вузлів

Кожен комп'ютер у мережі називається вузлом, хостом або кінцевим пристроєм.

Сервери - це комп'ютери, які надають інформацію кінцевим пристроям:

- поштові сервери
- веб-сервери
- файлові сервери.

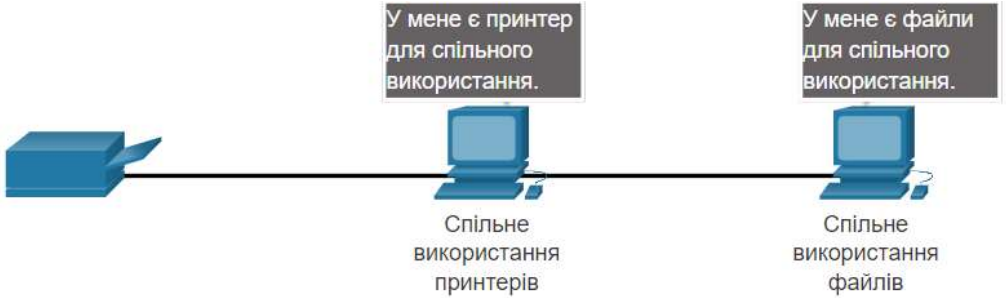
Клієнти - це комп'ютери, які надсилають запити серверам для отримання:

- веб-сторінки з веб-сервера
- email з поштового сервера

Тип сервера	Опис
Email	На сервері електронної пошти працює ПЗ поштового сервера. Клієнти використовують клієнтське ПЗ для доступу до електронних повідомлень.
Веб	На веб-сервері працює серверне ПЗ веб-сервера. Клієнти використовують ПЗ браузера для доступу до веб-сторінок.
Файл	Файловий сервер зберігає корпоративні та користувацькі файли. Клієнтські пристрої отримують доступ до цих файлів.

Одноранговa мережа

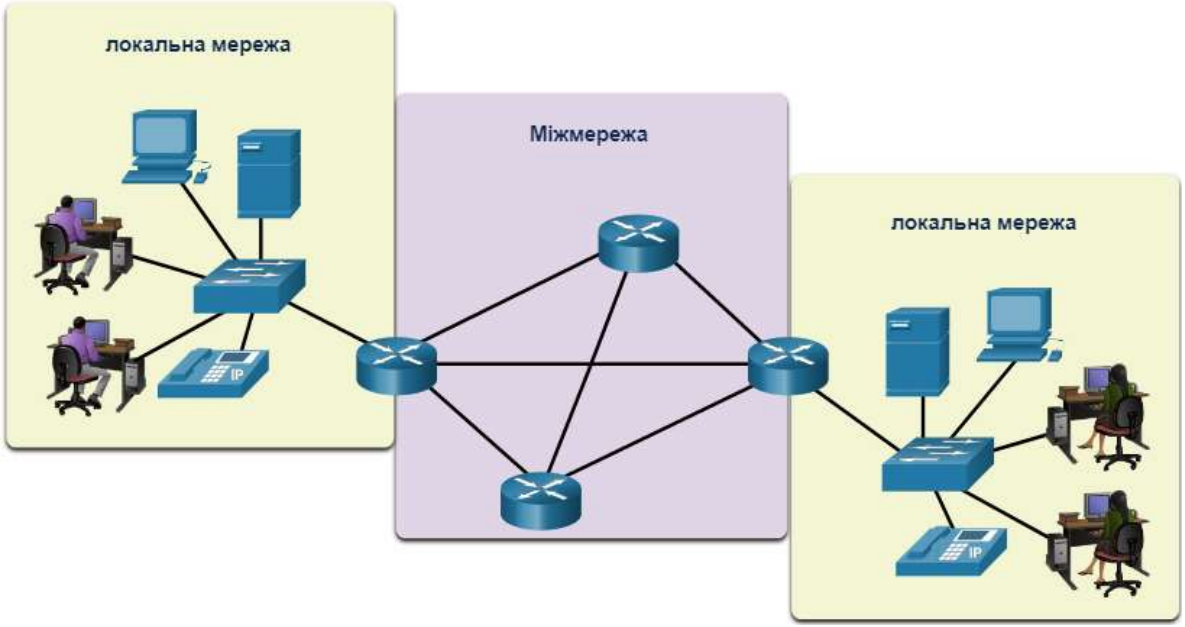
В одноранговій мережі пристрій може виконувати функції як клієнта, так і сервера. Цей тип архітектури мережі рекомендується для застосування у дуже малих мереж.



Переваги	Недоліки
Легкість налаштування	Відсутність централізованого адміністрування
Менша складність	Не так безпечно
Низька вартість	Не масштабується
Можна використовувати для виконання простих завдань: передавання файлів і спільного використання принтерів	Низька ефективність

Кінцеві пристрої

Кінцевим вважають пристрій, який є джерелом повідомлення, або кінцевим пунктом призначення, на якому воно одержується. Дані генеруються на одному кінцевому пристрої, передаються мережею та надходять на інший кінцевий пристрій.



Проміжні мережні пристрої

Проміжний пристрій з'єднує кінцеві пристрої. Прикладами є комутатори, точки бездротового доступу, маршрутизатори і міжмережні екрани.

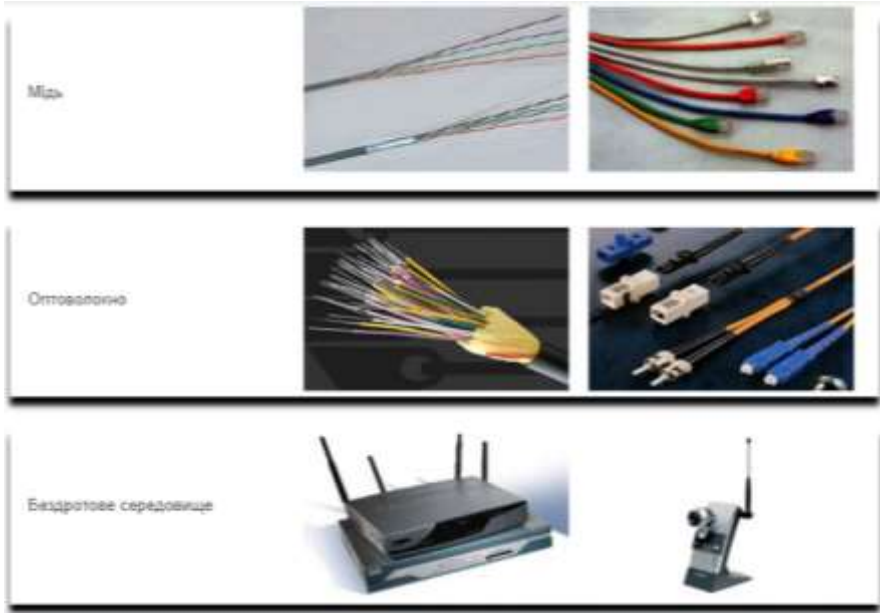
На проміжні пристрої покладена функція керування даними під час проходження мережею, а також:

- Відновлення та повторне передавання сигналів даних.
- Підтримка інформації про наявні шляхи передавання даних по мережі.
- Інформування інших пристроїв про помилки та вихід з ладу засобів зв'язку.

Мережне середовище передавання даних

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

Типи середовищ передавання даних	Опис
Кабелі з металевих дротів	Використовують електричні імпульси
Кабелі з оптичних або пластикових волокон (волоконно-оптичний кабель)	Використовують імпульси світла
Бездротові середовища	Використовують модуляцію електромагнітних хвиль на визначених частотах.



Зображення мереж і топології

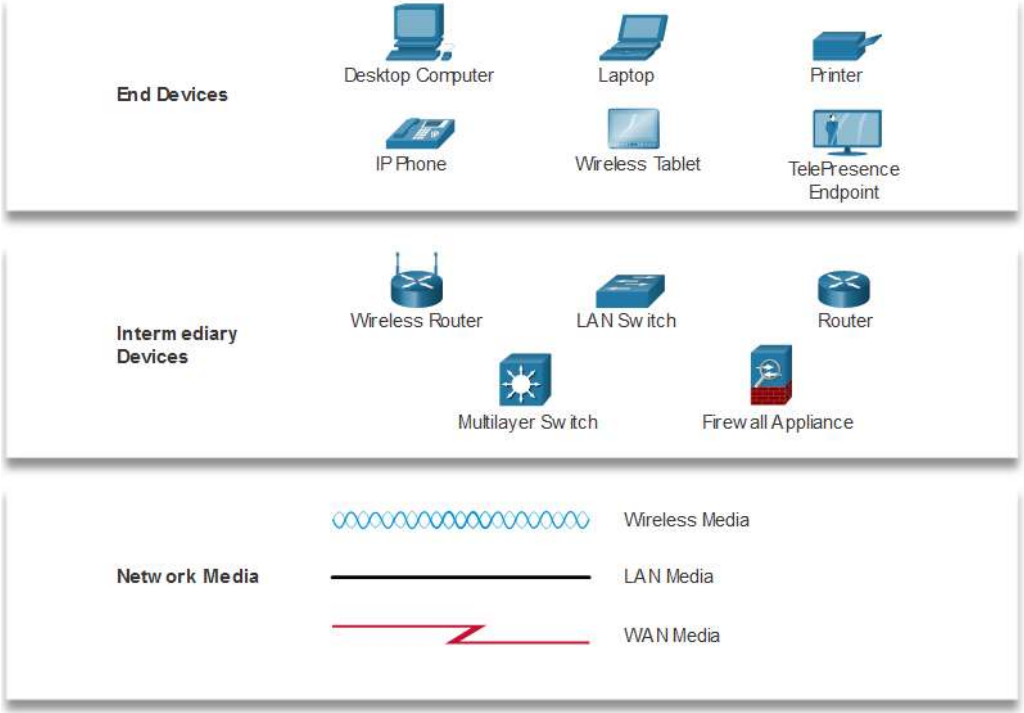
Зображення мережі

Схема мережі, яку часто називають топологією, використовує спеціальні позначення пристроїв у мережі.

Важливі терміни, які слід знати:

- Мережний адаптер (NIC)
- Фізичний порт
- Інтерфейс.

Примітка: Часто терміни порт і інтерфейс використовуються взаємозамінно.



Схеми топологій

Схема фізичної топології подає фізичне розташування проміжних пристроїв і прокладання кабельних з'єднань.

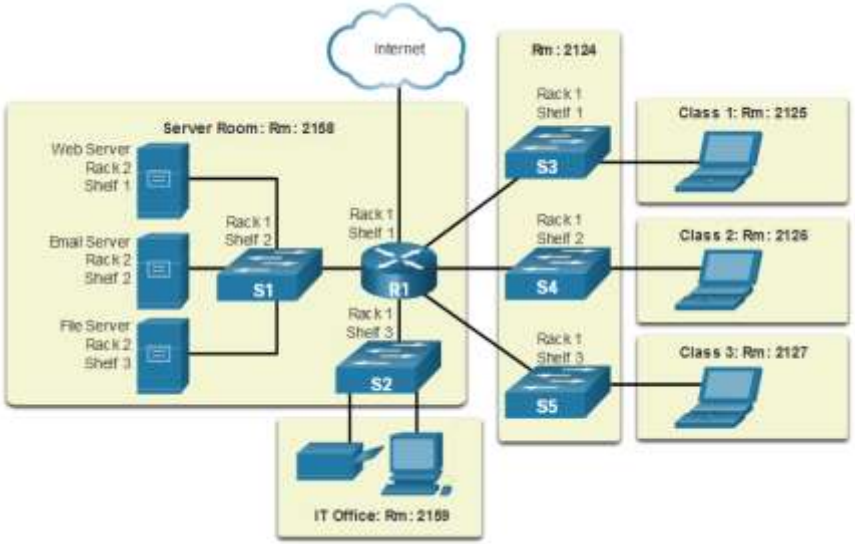
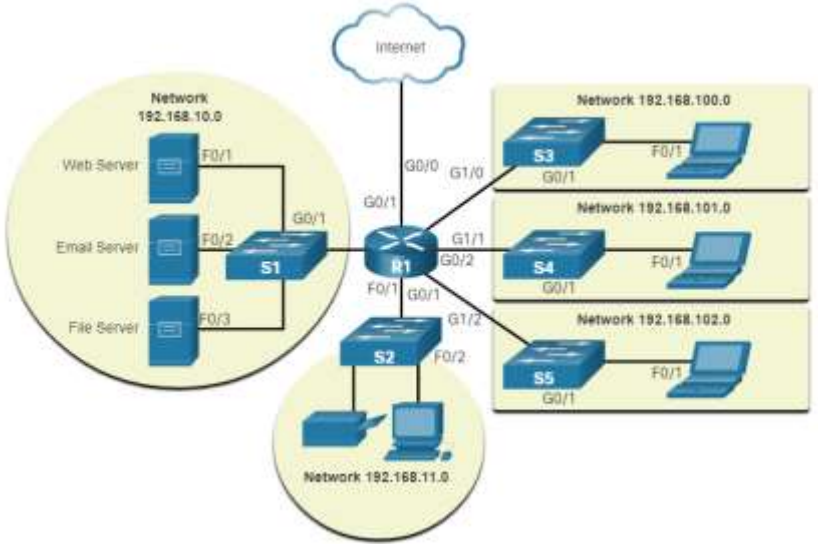


Схема логічної топології зображає пристрої, порти, а також схему адресації мережі.



Основні типи мереж

Мережі різного розміру

Мережі SOHO

Середні/великі та всесвітні мережі

- Невелика домашня мережа – з'єднує декілька комп'ютерів один з одним та з Інтернетом.
- Мережа невеликого/домашнього офісу (SOHO) – підтримує роботу з дому або з віддаленого офісу і забезпечує під'єднання до корпоративної мережі.
- Мережі середнього та великого розмірів можуть охоплювати декілька локацій із сотнями або тисячами з'єднаних комп'ютерів.
- Всесвітні мережі, так як Інтернет - з'єднують сотні мільйонів комп'ютерів у всьому світі.

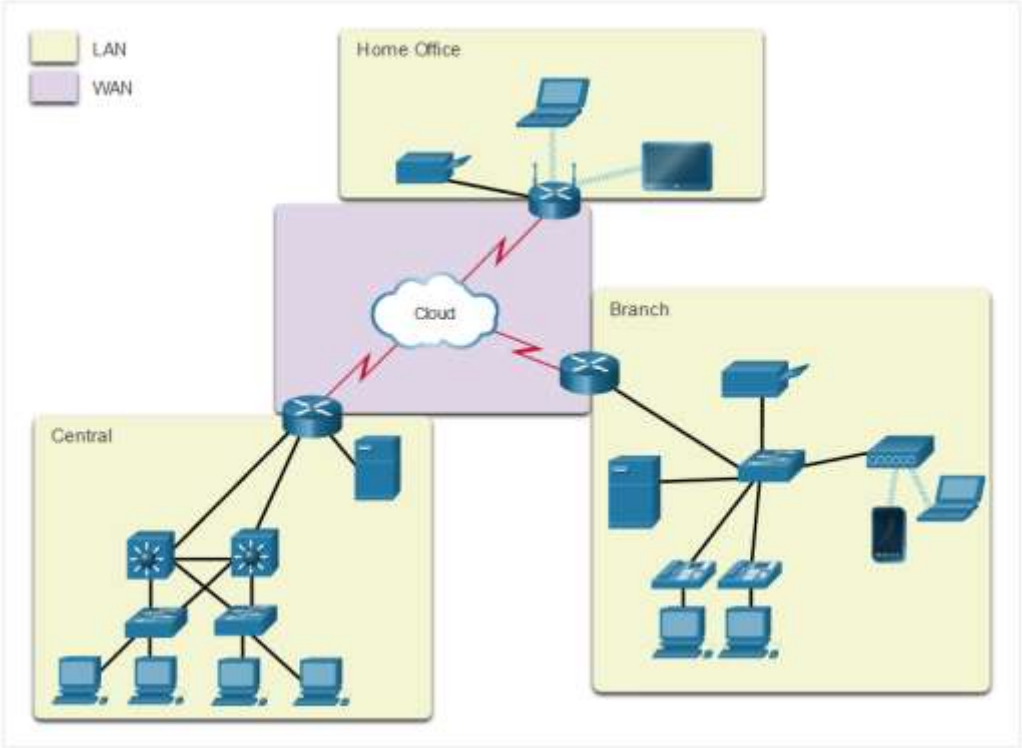
Мережі LAN і WAN

Мережні інфраструктури сильно різняться з точки зору:

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

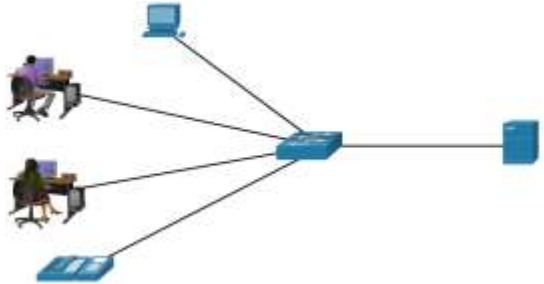
Два основні типи мереж:

- Локальна мережа (LAN)
- Глобальна мережа (WAN)

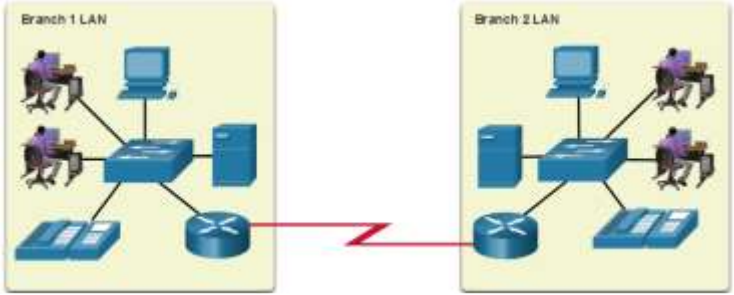


Мережі LAN і WAN

LAN - це мережна інфраструктура, що охоплює невелику географічну площу.



WAN - це мережна інфраструктура, що простягається на значні географічні відстані.



LAN	WAN
З'єднує кінцеві пристрої на обмеженій території.	З'єднує локальні мережі на значних географічних відстанях.
Адмініструється окремою організацією або особою.	Зазвичай адмініструється одним або декількома постачальниками послуг.
Забезпечує високошвидкісну пропускну здатність для внутрішніх пристроїв.	Як правило створює повільніші канали зв’язку між локальними мережами.

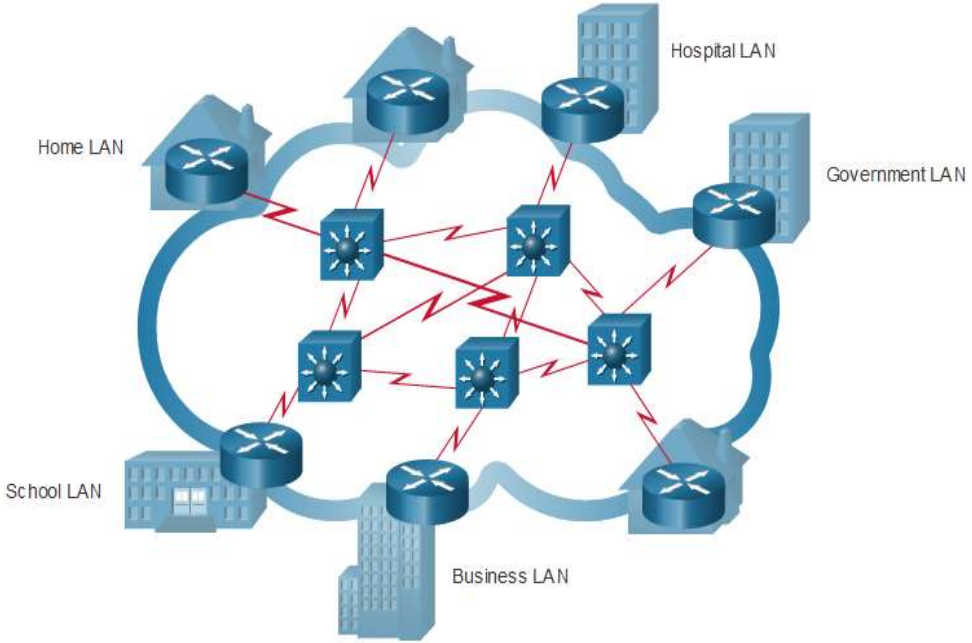
Інтернет

Інтернет - це всесвітнє об’єднання взаємопов'язаних локальних і глобальних мереж.

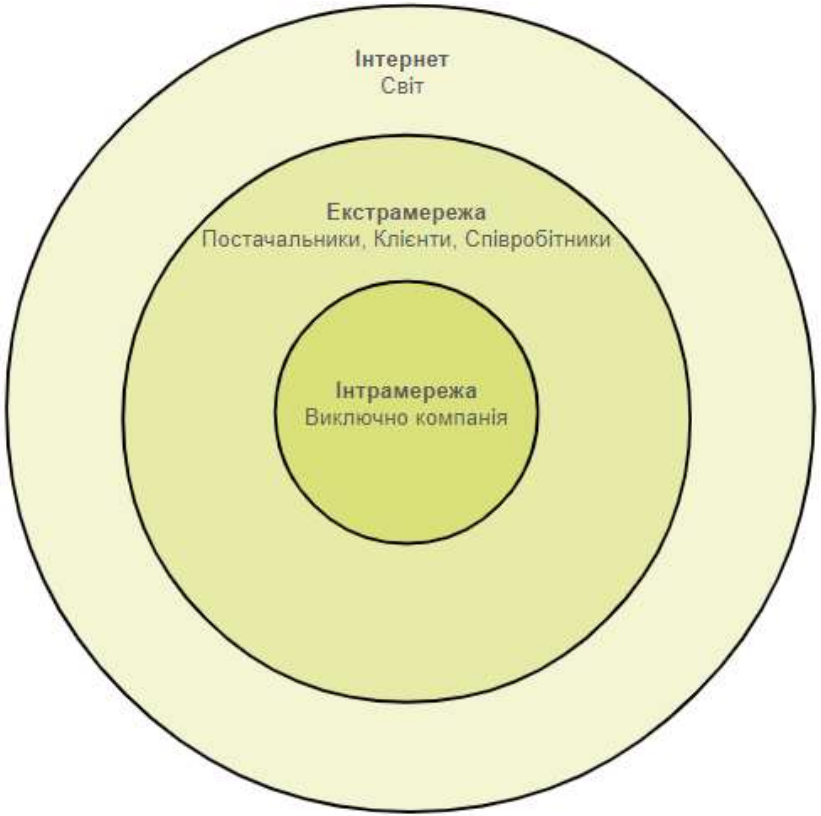
- Локальні мережі з’єднуються між собою за допомогою WAN.
- При побудові глобальних мереж можуть використовуватися мідні дроти, волоконно-оптичні кабелі або бездротові з'єднання.

Мережа Інтернет не належіть жодній особі або групі осіб. Для підтримки структури в Інтернеті були створені такі організації:

- IETF
- ICANN
- IAB



Інтранет і Екстранет



Інтранет - це приватні локальні та глобальні мережі організації, відкриті для членів організацій та інших авторизованих осіб.

Організація може використовувати екстранет для надання безпечного доступу до своєї мережі особам, які працюють в іншій організації та потребують звернення до корпоративних даних.

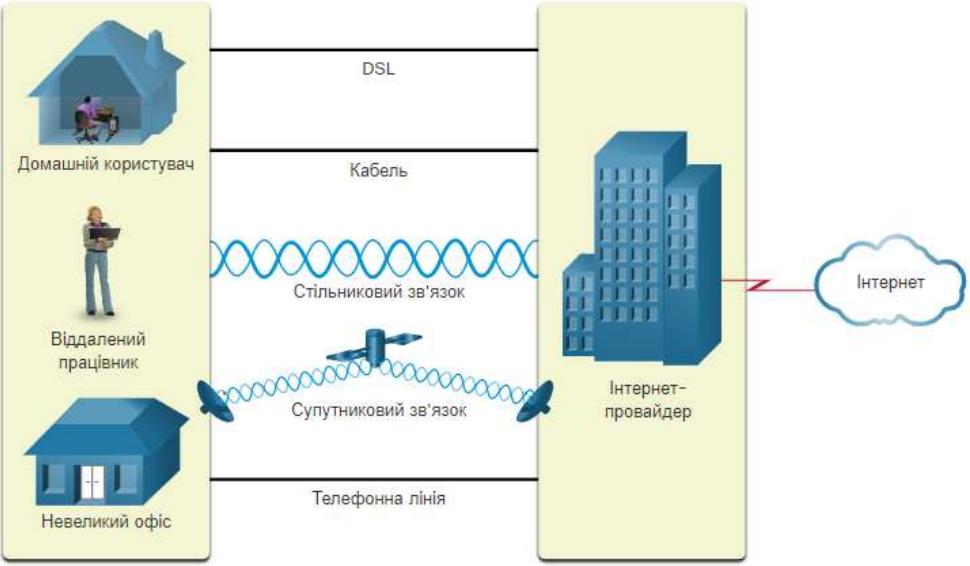
Інтернет-з'єднання

Технології інтернет-доступу

Існує багато способів під’єднання користувачів та організацій до Інтернету:

- Популярними сервісами для домашніх користувачів та невеликих офісів є широкосмугове кабельне з'єднання, широкосмугова цифрова абонентська лінія (DSL), бездротові WAN і мобільні сервіси.
- Організації потребують більш швидкісних з’єднань для підтримки IP-телефонії, відеоконференцій та центрів обробки даних.
- Зв'язок рівня бізнес-класу зазвичай надається постачальниками послуг (SP) і може включати: бізнес-DSL, орендовані лінії та Metro Ethernet.

Під'єднання до Інтернету для дому та невеликого офісу

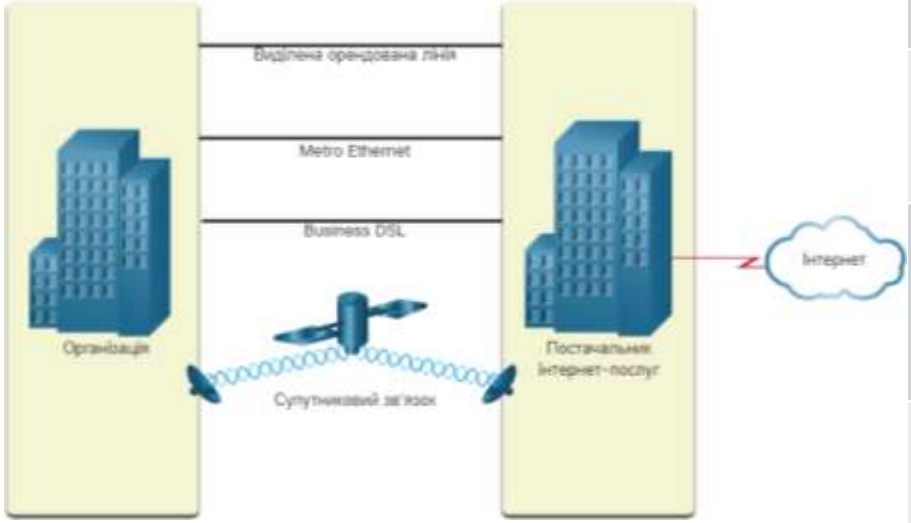


З'єднання	Опис
Кабельне	висока пропускна здатність, завжди увімкнене, пропонується постачальниками послуг кабельного телебачення.
DSL	висока пропускна здатність, завжди увімкнене, працює по телефонних лініях – зараз НЕ АКТУАЛЬНО.
Стільникове	використовує мережу стільникового оператора для під'єднання до Інтернету.
Супутникове	в основному надає переваги для сільської місцевості, де відсутні постачальники Інтернет-послуг.
Комутоване телефонне	недорогий варіант з низькою пропускною здатністю, потребує використання модему. – зараз НЕ АКТУАЛЬНО.

Корпоративне інтернет-з'єднання

Корпоративне з'єднання може потребувати:

- високої пропускної здатності
- виділених каналів зв’язку
- керованих сервісів.

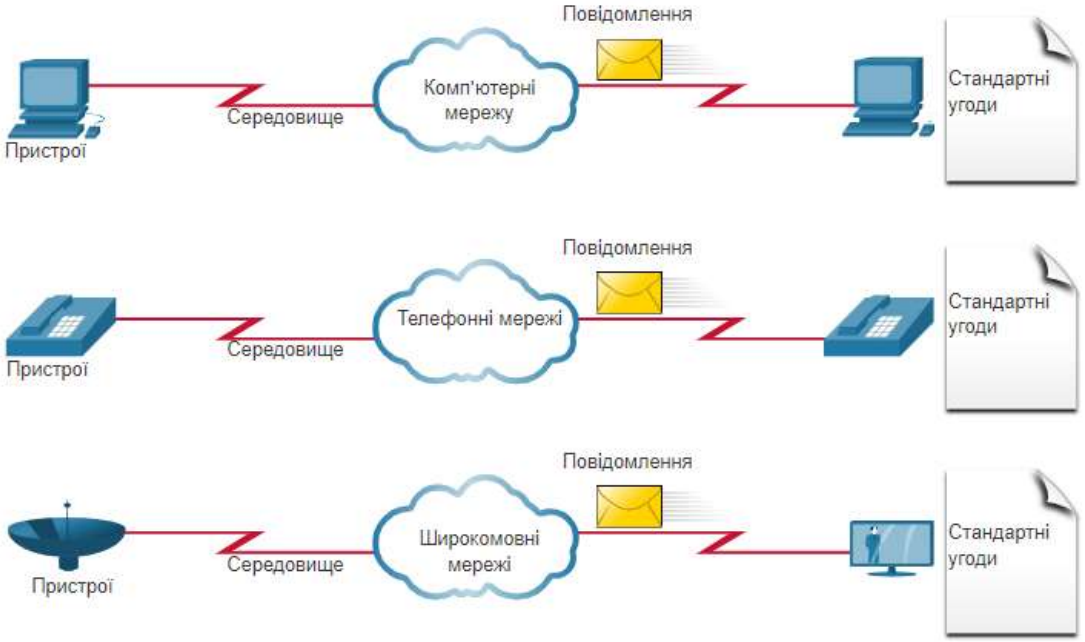


Типи з'єднань	Опис
Виділена орендована лінія	Це зарезервовані канали зв'язку в мережі постачальника послуг, які з'єднують географічно віддалені офіси для приватного передавання голосу та / або даних.
Ethernet WAN	Ця технологія розширює можливості Ethernet до рівня WAN.
DSL	Бізнес-DSL доступний у різних форматах, включаючи симетричні цифрові абонентські лінії (SDSL).- НЕ АКТУАЛЬНО
Супутниковий зв’язок	Може забезпечувати з'єднання, коли кабельне підведення недоступне.

Конвергентна мережа

До появи конвергентних мереж організація мала окремі кабельні системи для телефонного зв'язку, транслювання відео та передавання даних.

Кожна з цих мереж використовувала визначені технології передавання сигналу зв'язку, а також різні набори правил і стандартів.

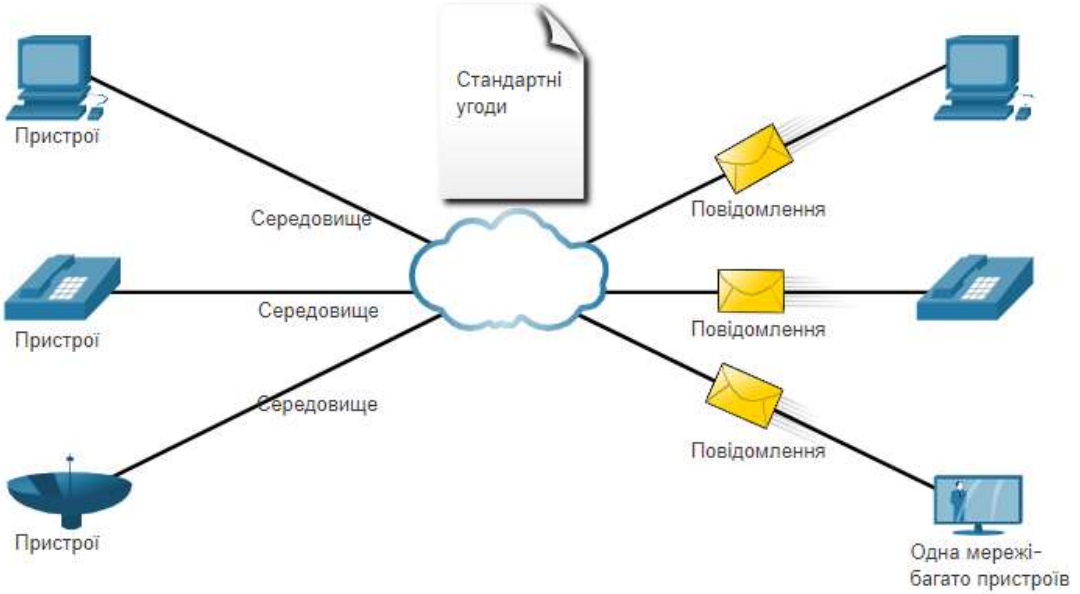


Конвергентна мережа (Продовж.)

Конвергентні мережі зв'язку забезпечують функціонування декількох служб на базі однієї мережі, включно з передаванням:

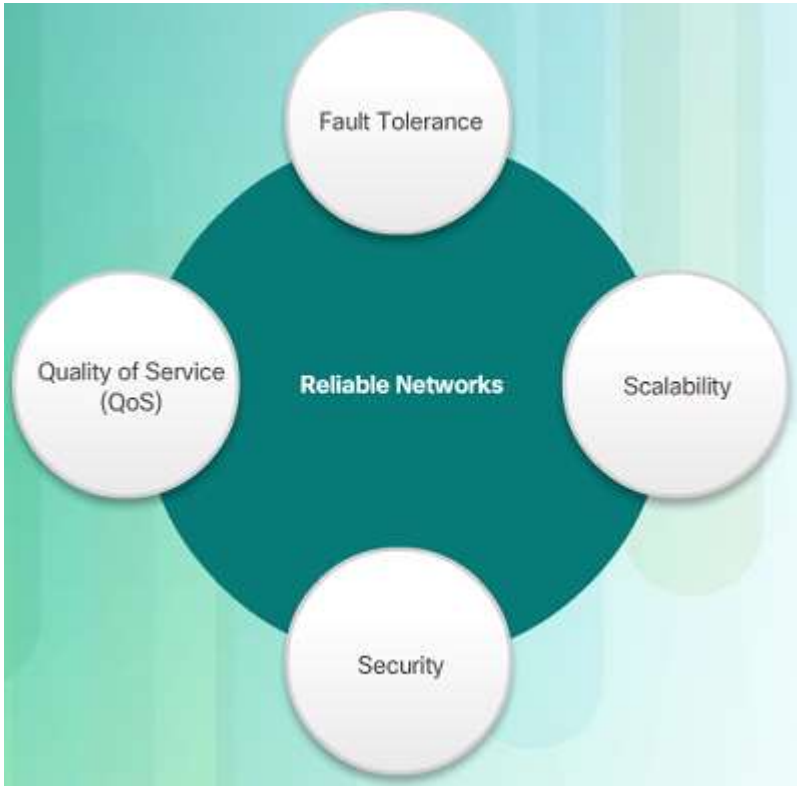
- даних
- голосу
- відео.

Конвергентні мережі використовують єдину мережну інфраструктуру з однаковим набором стандартів і правил.



Надійні мережі

Мережна архітектура



Архітектура мережі позначає технології, що підтримують інфраструктуру, якою дані передаються по мережі.

Для задоволення очікувань користувачів існує чотири основні характеристики, яким повинні відповідати сучасні мережні архітектури:

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

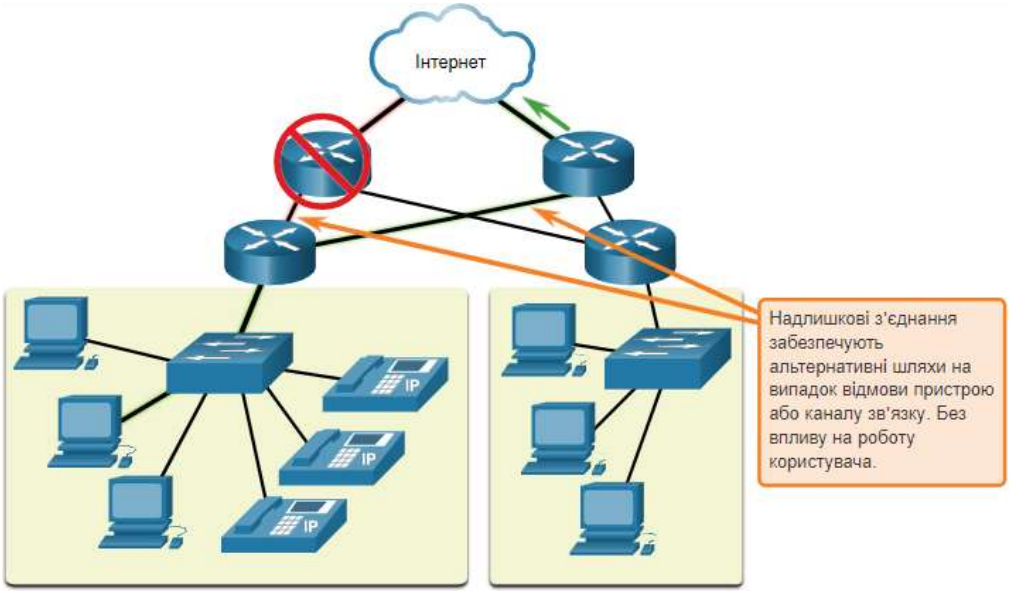
Відмовостійкість

Відмовостійка мережа обмежує кількість пристроїв, на які впливає відмова. Відмовостійкість вимагає наявності декількох шляхів.

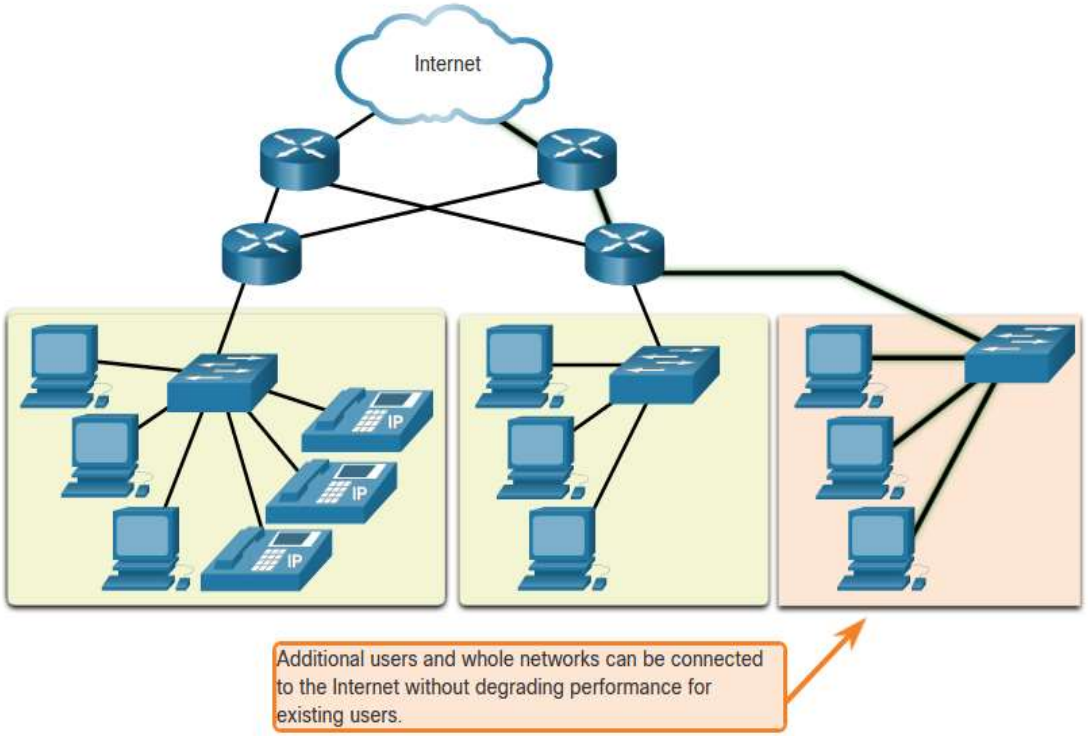
Надійність мережі може забезпечувати резервування (надлишковість) через використання технології комутації пакетів:

- При комутації пакетів трафік розбивається на пакети, які маршрутизуються по мережі.
- Теоретично пакети можуть надходити до пункту призначення різними шляхами.

Це неможливо у мережах з комутацією каналів, у яких передавання здійснюється по визначених каналах зв'язку.



Масштабованість



Масштабована мережа може швидко та легко розширюватися задля підтримки нових користувачів і застосунків, без впливу на рівень послуг, які надаються існуючим користувачам.

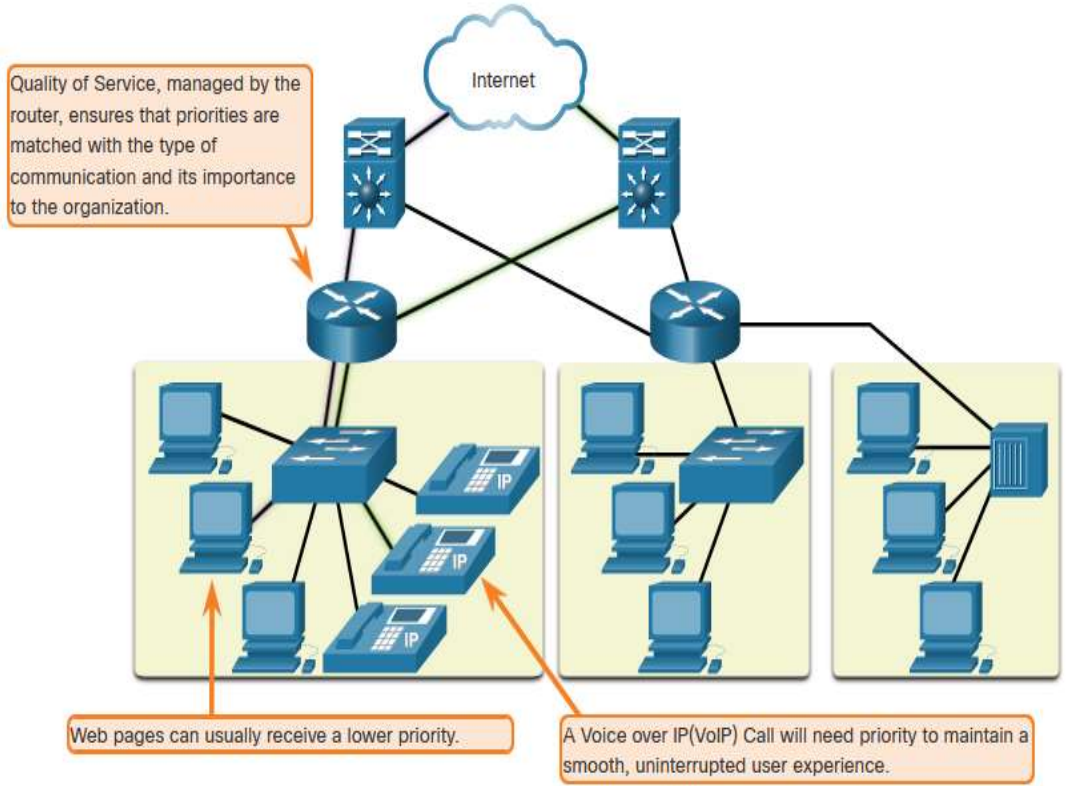
Мережі є масштабованими завдяки дотриманню проектувальниками визначених стандартів і протоколів.

Якість обслуговування (QoS)

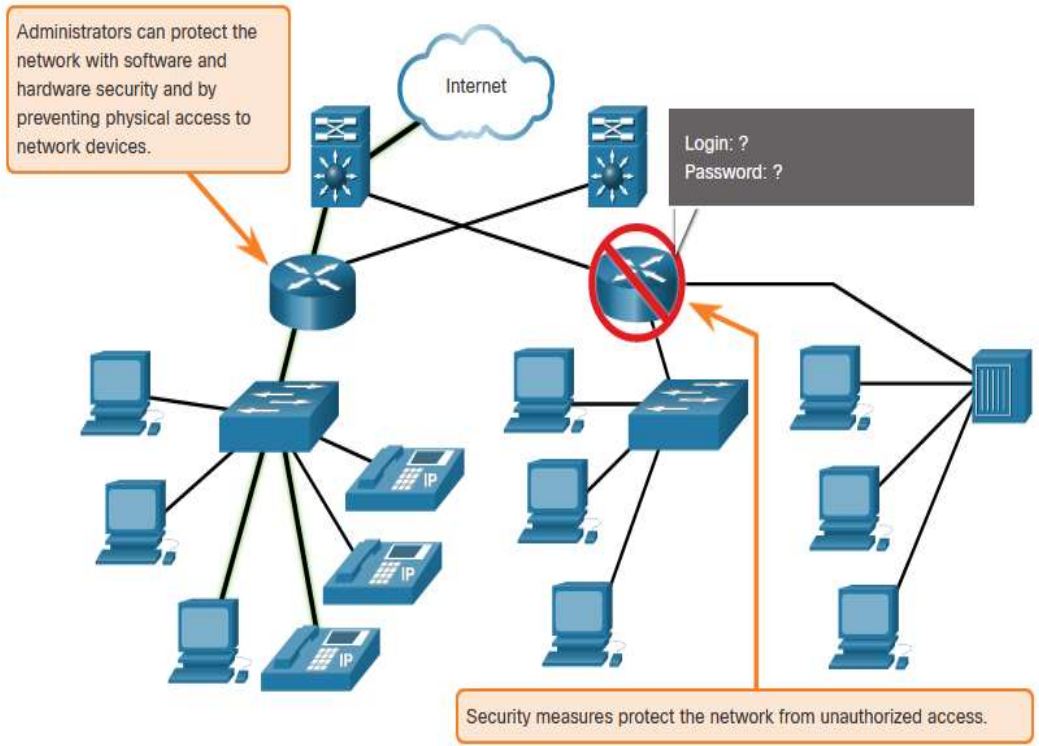
Передавання голосу та відео у реальному часі висувають підвищені вимоги щодо якості наданих послуг.

Чи траплялося вам переглядати відео з постійним перериванням і затримками? Це має місце в умовах, коли попит на пропускну здатність перевищує наявні ресурси каналів зв'язку, а політика QoS не застосовується.

- Якість обслуговування (QoS) - це основний механізм, який використовується для забезпечення надійної доставки контенту для усіх користувачів.
- При застосуванні політики QoS маршрутизатору легше керувати потоком даних і голосовим трафіком.



Безпека мережі



Існують такі основні типи мережного захисту, які потрібно забезпечити:

- Безпека мережної інфраструктури
  - Фізична безпека мережних пристроїв
  - Попередження неавторизованого доступу до пристроїв
- Інформаційна безпека
  - Захист інформації або даних, що передаються мережею.

Три мети мережної безпеки:

- Конфіденційність – дані доступні лише уповноваженим і авторизованим користувачам.
- Цілісність - запорука того, що дані під час передавання не були змінені.
- Доступність - гарантує авторизованим користувачам вчасний і надійний доступ до даних.

Тенденції розвитку мереж

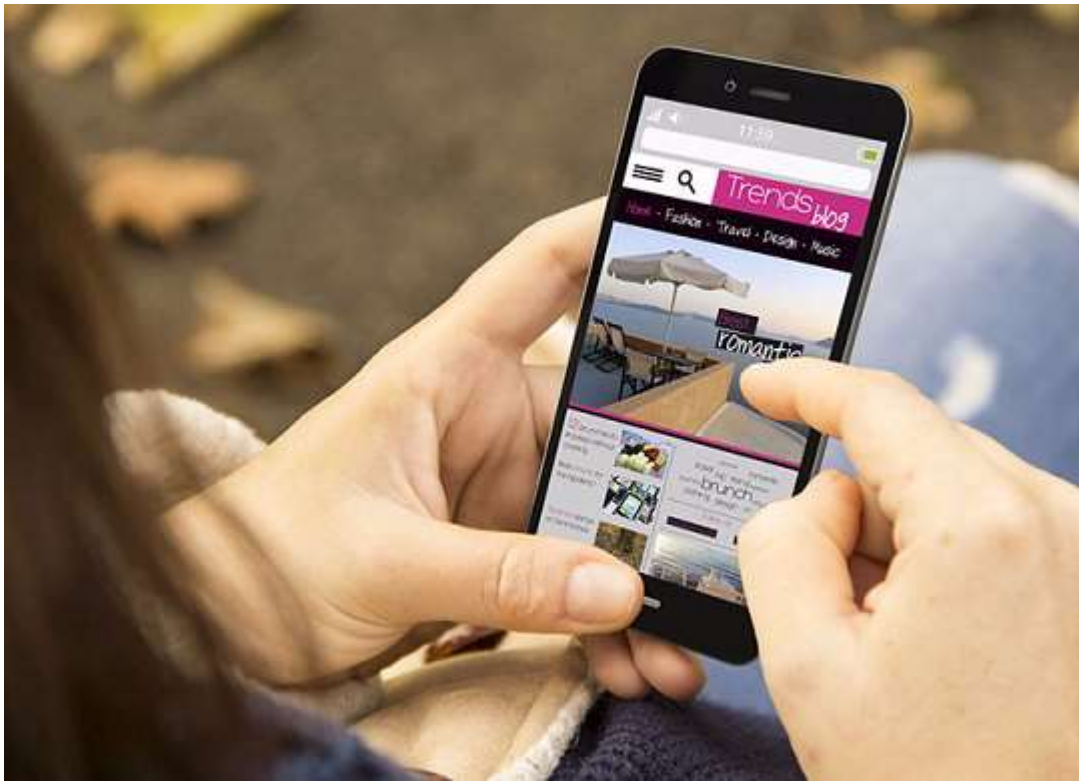
Останні тенденції

У міру виходу на ринок нових технологій та кінцевих пристроїв, роль мережі повинна повсякчас пристосовуватися до цього мінливого середовища.

Ось деякі тенденцій мереж, які впливають на організації та споживачів:

- Bring Your Own Device (BYOD)
- Онлайн-співпраця
- Відео-зв’язок
- Хмарні обчислення.

Використання власного пристрою (BYOD)



Використання власних пристроїв (BYOD) надає користувачам більше можливостей та гнучкості.

BYOD дозволяє кінцевим користувачам вільно користуватися особистими інструментами для доступу до інформації та взаємодії за допомогою власних:

- Ноутбуків
- Нетбуків
- Планшетів
- Смартфонів
- Електронних книжок.

BYOD означає, що будь-який пристрій може належати будь-кому і використовуватися будь-де.

Онлайн-співпраця

- Працюйте разом з іншими людьми у мережі над спільними проектами.
- Інструменти співпраці, такі як Cisco WebEx (див. рисунок), забезпечують користувачам можливості миттєвого з'єднання та взаємодії.
- Співпраці надається пріоритет у бізнесі та освіті.
- Cisco Webex Teams - це багатофункціональний інструмент співпраці, який дозволяє:
  - надсилати миттєві повідомлення
  - розміщувати зображення
  - поширювати відео та посилання.

Відео-зв'язок

- За допомогою відеодзвінка можна звернутися до будь-кого, незалежно від його місця перебування.
- Відеоконференції є потужним інструментом для спілкування з іншими людьми.
- Відео стає критично важливою вимогою для ефективної співпраці.
- Потужний інструмент Cisco TelePresence - це один зі способів взаємодії між будь-ким будь-де.

Хмарні обчислення

Хмарні обчислення дозволяють нам зберігати особисті файли або резервні копії даних на серверах в Інтернеті.

- Застосунки також можуть бути доступні, з використанням хмари.
- Дозволяє компаніям доправляти дані на будь-який пристрій у будь-якій точці світу.

Хмарні обчислення стають можливими завдяки центрам обробки даних (ЦОД).

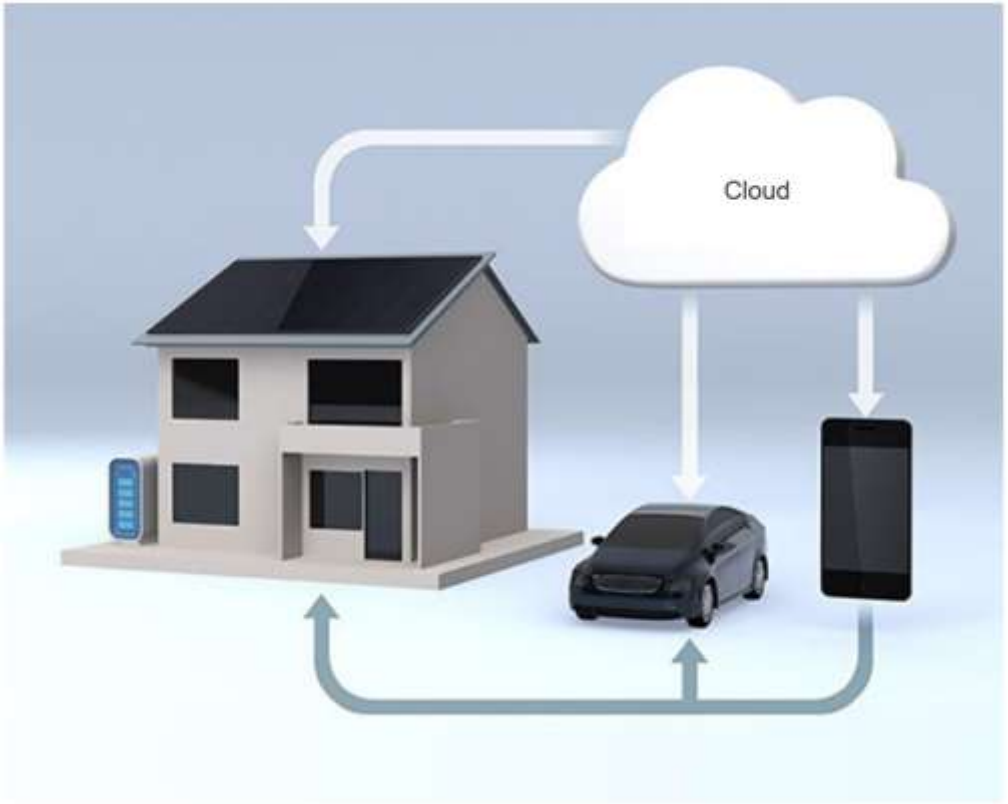
- Менші компанії, які не можуть дозволити собі власні ЦОД, орендують сервери та послуги зберігання даних у дата-центрах великих організацій у хмарі.

Хмарні обчислення (Продовж.)

Чотири типи хмар:

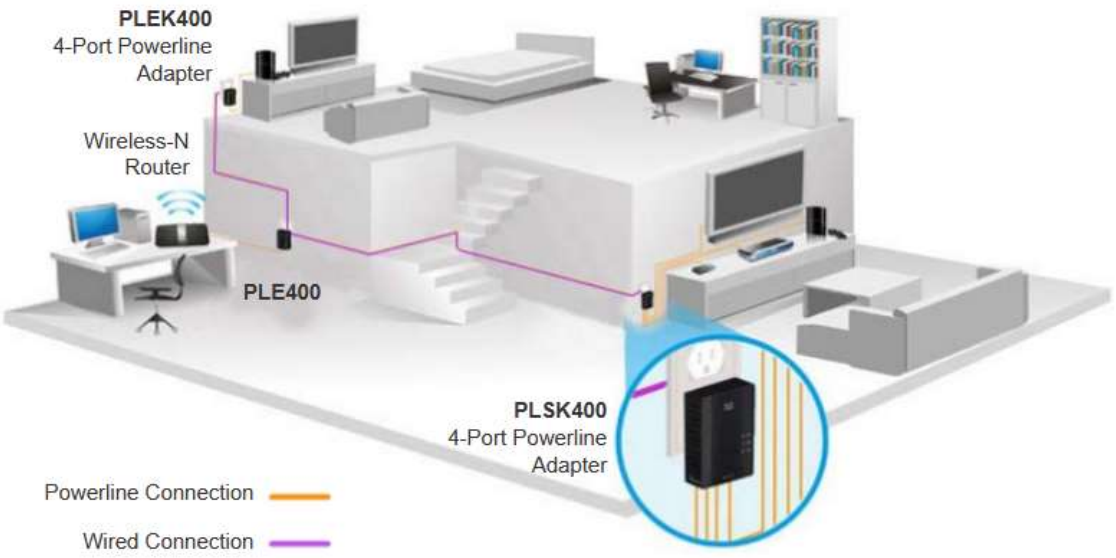
- Публічні хмари
  - Доступні для широкого загалу безкоштовно або з тарифікацією на основі використаних послуг.
- Приватні хмари
  - Призначені для конкретної організації або суб'єкту, наприклад уряду.
- Гібридні хмари
  - Складаються з двох або більше типів хмари - наприклад, частина галузева і частина публічна.
  - Кожна частина залишається окремим об'єктом, але обидві з'єднані з використанням єдиної архітектури.
- Галузеві/ Громадські Хмари
  - Створені для задоволення потреб певної галузі, наприклад, сфери охорони здоров’я чи засобів масової інформації.
  - Можуть бути приватними або публічними.

Технологічні тенденції для домашнього використання



- Технологія розумного будинку - це тренд, який стрімко розвивається, і дозволяє інтегрувати сучасні технології до побутових приладів, з метою їх взаємодії з іншими пристроями.
- Духовка може приготувати страву до вашого повернення додому, встановивши час приготування згідно із записами у вашому календарі.
- Наразі технологія розумного дому розробляється для усіх кімнат у будинку.

Мережа електроживлення – рідко використовується



- Мережа електроживлення (Powerline) може забезпечувати під'єднання пристроїв до локальної мережі там, де кабелі мережі або бездротовий зв’язок недоступні.
- Використовуючи стандартний адаптер живлення, пристрої можуть під'єднуватися до локальної мережі через електричну розетку, надсилаючи дані на певних частотах.
- Мережа електроживлення особливо корисна, коли точки бездротового доступу не можуть охопити усі домашні пристрої.

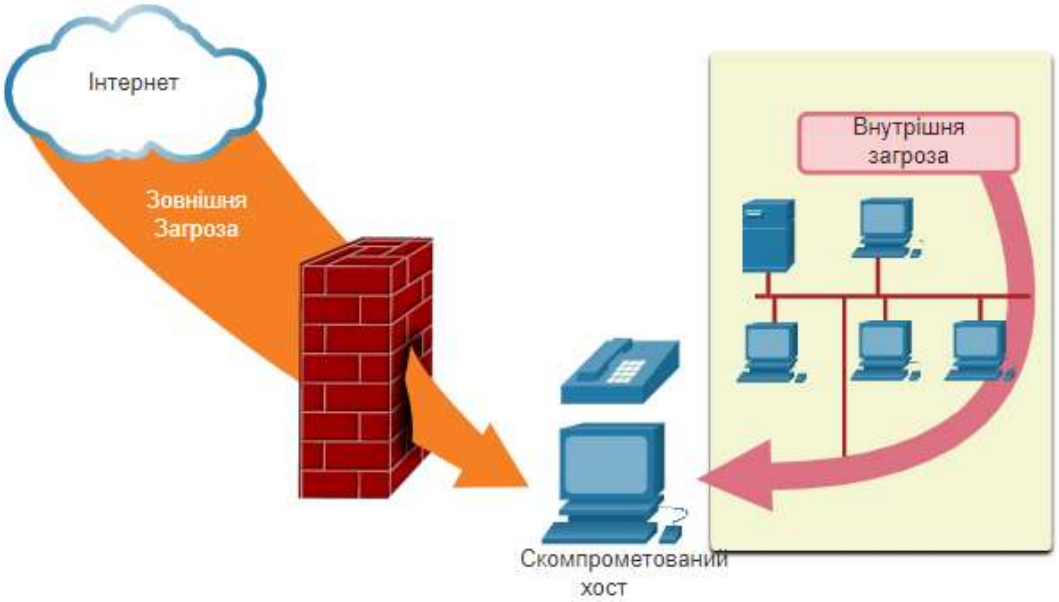
Бездротовий широкосмуговий зв'язок

Окрім DSL та кабелю, бездротовий зв’язок - це ще один варіант, який використовується для під’єднання будинків та невеликих підприємств до Інтернету.

- Найчастіше зустрічається у сільській місцевості. Постачальник послуг бездротового Інтернету (WISP) - це Інтернет-провайдер, що під’єднує абонентів до визначених точок доступу або hopspots.
- Бездротовий широкосмуговий зв'язок (Wireless broadband) - це одне бездротове рішення для дому та невеликого підприємства.
  - Використовує ту саму стільникову технологію, що і смартфон.
  - Антена встановлюється поза будинком, що забезпечує домашнім пристроям бездротовий або дротовий зв’язок.

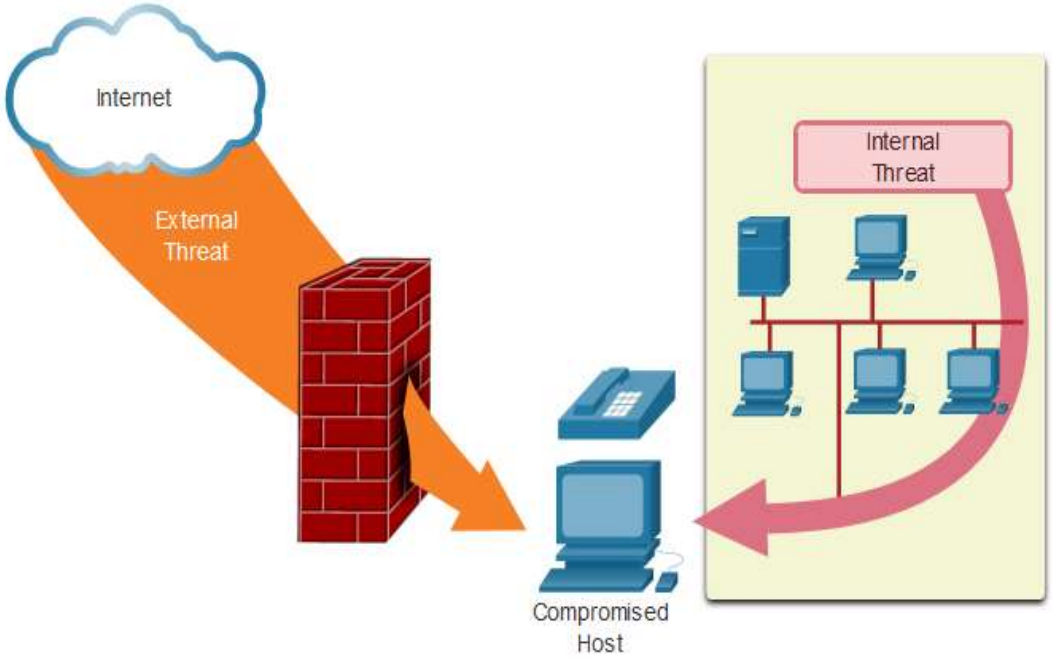
Безпека мережі

Загрози безпеці



- Безпека мережі - це невід'ємна частина мереж, незалежно від її розміру.
- При реалізації безпеки мережі потрібно брати до уваги середовище, у якому захищаються дані, а також забезпечувати належну якість обслуговування користувачів.
- Захист мережі включає в себе багато протоколів, технологій, пристроїв, інструментів та методів, які захищають дані та пом'якшують наслідки загроз.
- Вектори загроз можуть бути зовнішніми або внутрішніми.

Загрози безпеці (Продовж.)



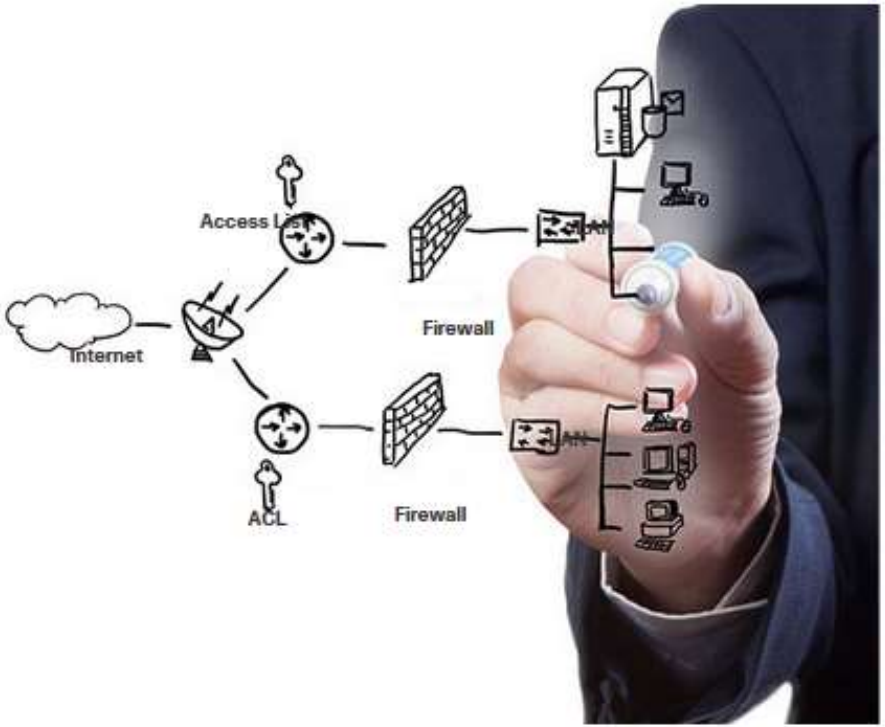
Зовнішні загрози:

- Віруси, хробаки і троянські коні
- Шпигунське і рекламне ПЗ
- Атаки нульового дня
- Напади зловмисників
- Атаки відмови в обслуговуванні
- Перехоплення і крадіжка даних
- Крадіжка ідентичності.

Внутрішні загрози:

- втрачені або викрадені пристрої
- випадкові зловживання працівників
- співробітники зі зловмисними намірами.

Безпекові рішення

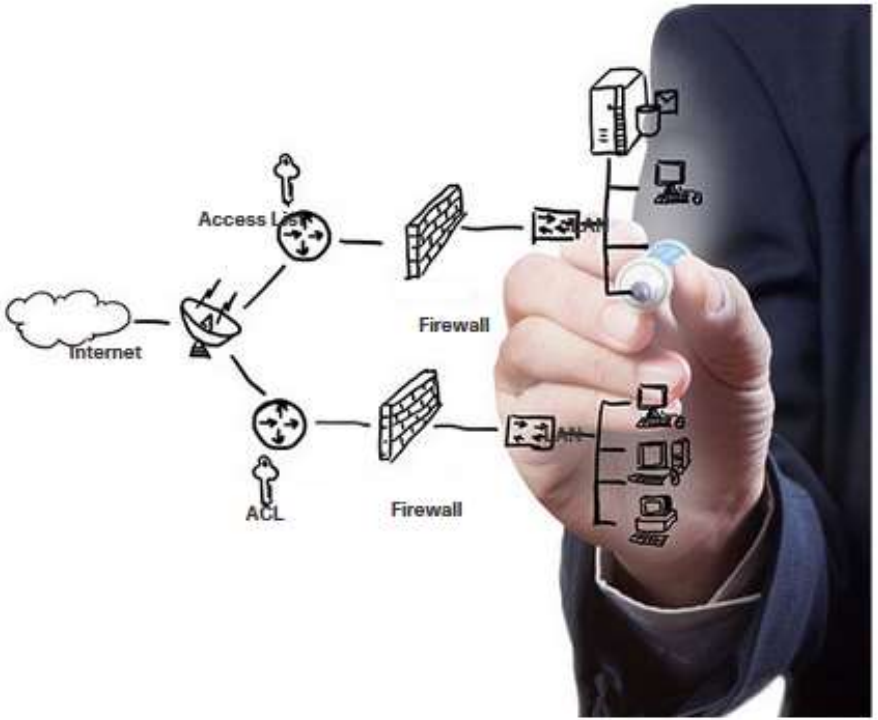


Безпека повинна запроваджуватися на декількох рівнях, з використанням більше ніж одного рішення.

Компоненти безпеки для домашньої або невеликої офісної мережі:

- На кінцевих пристроях має бути встановлене антивірусне та анти-шпигунське ПЗ.
- Фільтрація за допомогою брандмауера використовується для блокування несанкціонованого доступу до мережі.

Безпекові рішення (Продовж.)



Більші мережі висувають додаткові вимоги до безпеки:

- Спеціалізовані системи міжмережних екранів
- Списки контролю доступу (ACL)
- Системи запобігання вторгненням (IPS)
- Віртуальна приватна мережа (VPN).

Вивчення загроз мережній безпеці починається з чіткого розуміння основної інфраструктури комутації та маршрутизації.

Що ми вивчили?

- У сучасному світі за допомогою мереж ми поєднані як ніколи раніше.
- Всі комп'ютери, що під'єднані до мережі та безпосередньо беруть участь у мережному з'єднанні, класифікуються як вузли (хости).
- Схеми мереж часто використовують спеціальні позначення для зображення різних пристроїв та з'єднань, з яких складається мережа.
- Топологія у простий спосіб зображає те, як з’єднані пристрої у великій мережі.
- Розрізняють два типи мережних інфраструктур: локальні (LAN) і глобальні (WAN) мережі.
- Інтернет-з'єднання для SOHO утворюються за допомогою кабельного з'єднання, DSL, стільникового зв'язку, супутникового з'єднання і комутованих телефонних ліній.
- Корпоративне інтернет-з'єднання використовує виділені орендовані лінії, Metro Ethernet, комерційний DSL і супутниковий зв'язок.

Що ми вивчили? (Продовж.)

- Архітектура мережі позначає технології, що підтримують інфраструктуру, і запрограмовані сервіси та правила, або протоколи, які переміщують дані по всій мережі.
- Існує чотири основні характеристики архітектури мережі: відмовостійкість, масштабованість, якість обслуговування (QoS) та безпека.
- Останні мережні тренди, які впливають на організації та користувачів: Bring Your Own Device (BYOD), онлайн-співпраця, відео-зв'язок і хмарні обчислення.
- Для мереж існує кілька поширених зовнішніх і внутрішніх загроз.
- Великі корпоративні мережі використовують антивіруси, антишпигунське ПЗ та фільтрацію за допомогою брандмауерів, а також висувають додаткові вимоги щодо захисту: спеціалізовані системи міжмережних екранів, списки контролю доступу (ACL), системи запобігання вторгненням (IPS) та віртуальні приватні мережі (VPN).

Сучасні комп'ютерні мережі Типи клієнтів, їх порівняльна характеристика. Програмне забезпечення Vmware Загальна структура Vmware Horizon

Особливості хмарних обчислень – розподілені обчислення

Хмарні обчислення – це різновид розподілених обчислен

1. Додавання потужності ПОМ
2. Додавання програмного забезпечення
3. Пошук інформації
4. Резервування даних

Сучасні системи хмарних обчислень (2)

Існує декілька типів хмарних сервісів:

IaaS - (інфраструктура як послуга)

Paas - (платформа як послуга)

SaaS - (програмне забезпечення як послуга).

Серверна

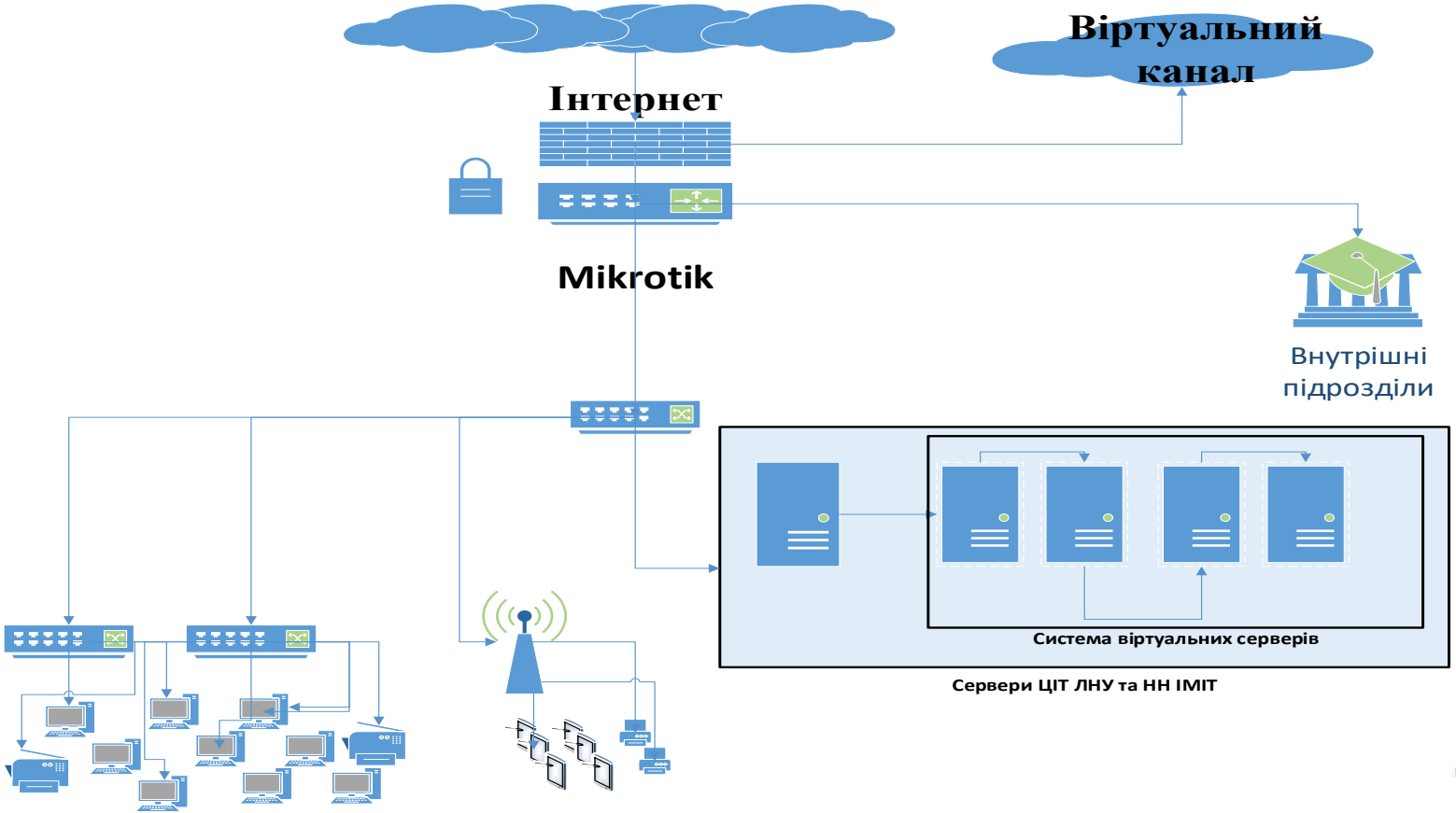
Структура

- два **двох процесорних** сервера;
- система **безперебійного живлення**;
- два спеціалізованих мережених **роутери Mikrotik** та комутатори 1ГБ.

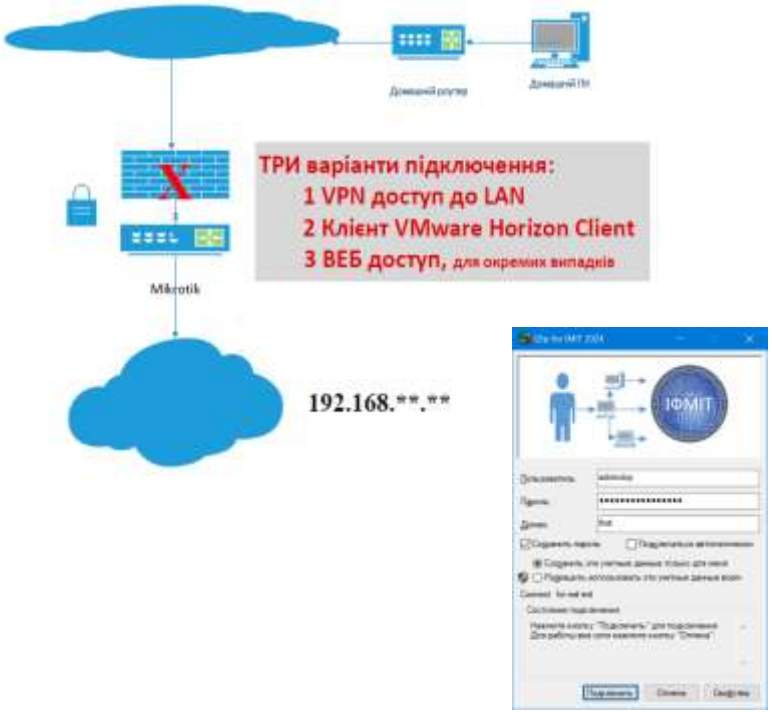
Загальний обсяг кластера складає:

- **96 ядер** процесорів Intel Xeon;
- понад **360 ГБ** оперативної пам'яті;
- понад **60 000 ГБ** дискового простору
- 8 кошиків для накопичувачів
- тип SSD - 0,8ТБ та HDD-9.8ТБ - 12Гб/с

Створено мережу та налагоджено систему безпеки

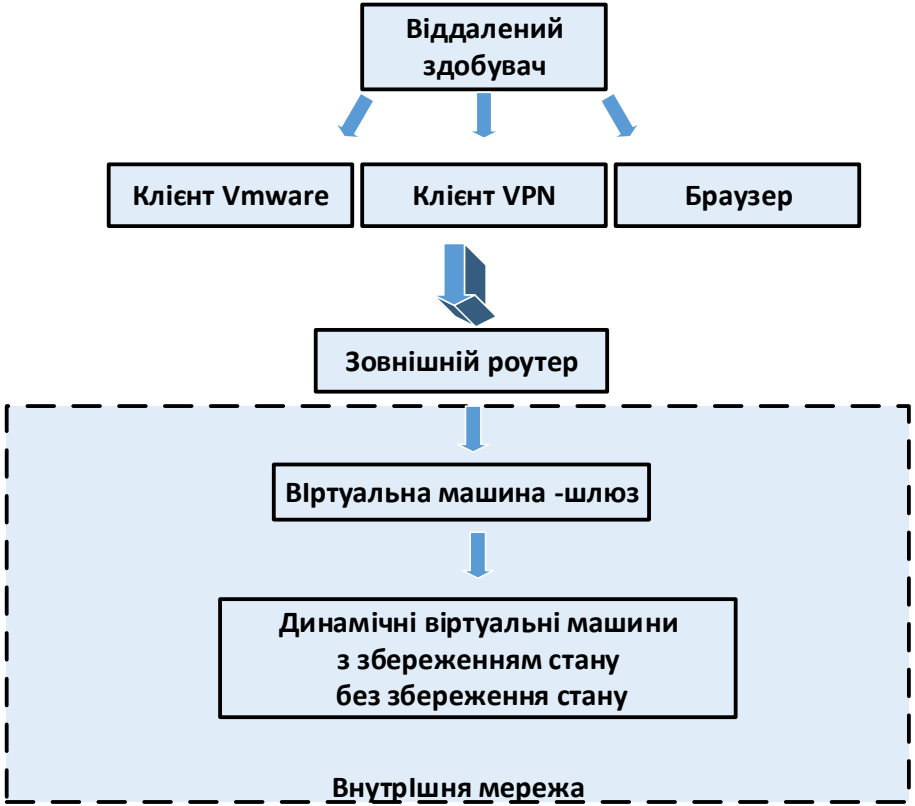


Варіанти доступу

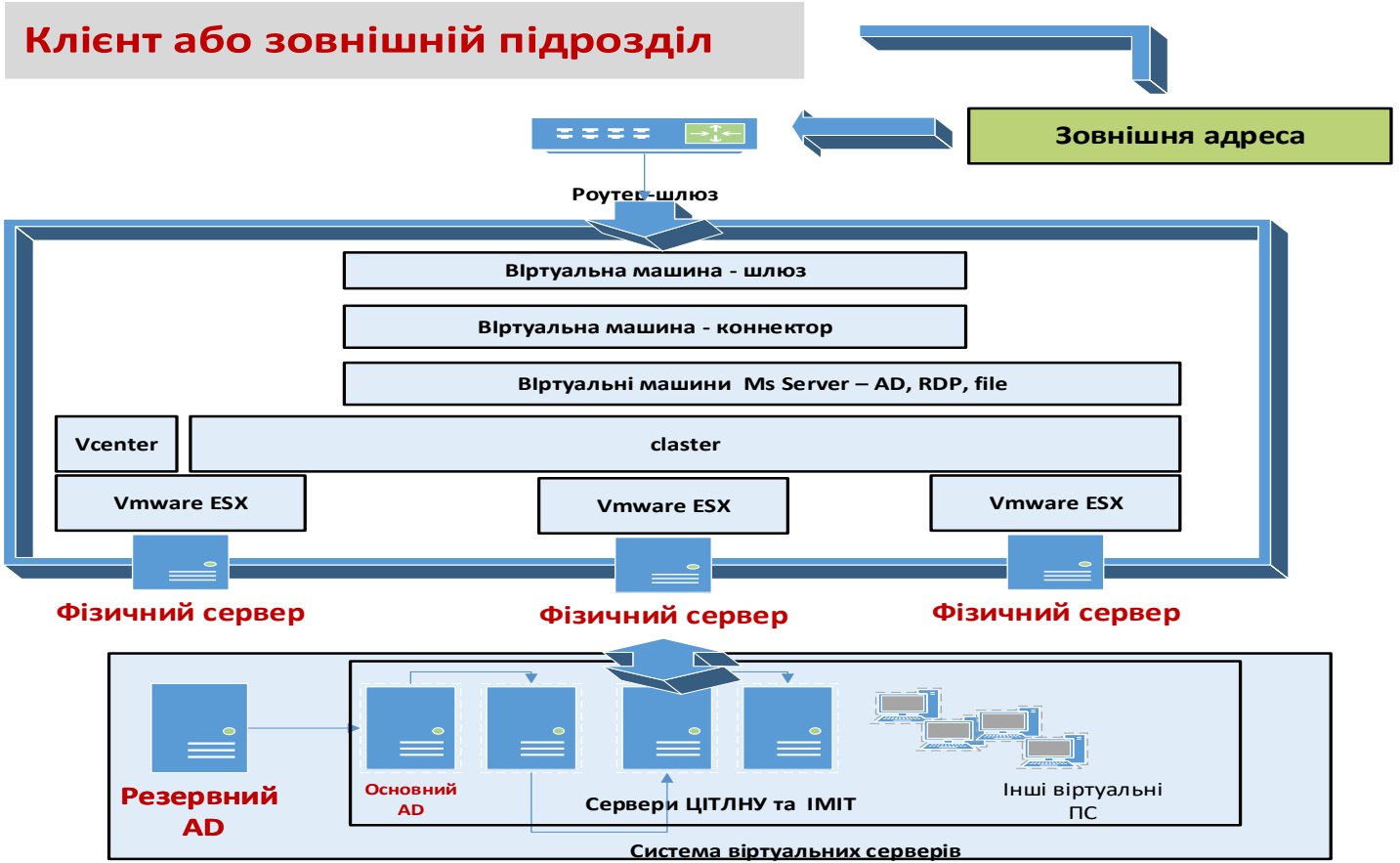


- **Клієнт Vmware Horizon** – немає обмежень – рекомендується для постійної роботи – працює на всіх приладах – потребує завантаження та інсталювання клієнту;
- **Браузер** (бажано Хром) – є обмеження на передавання / обмін файлами – рекомендується для ознайомлення – працює на всіх приладах – не потребує додаткового ПЗ;
- **Додатковий VPN – тип L2TP** – немає обмежень, повний доступ до всіх мережевих приладів – розроблено спеціальний інсталятор

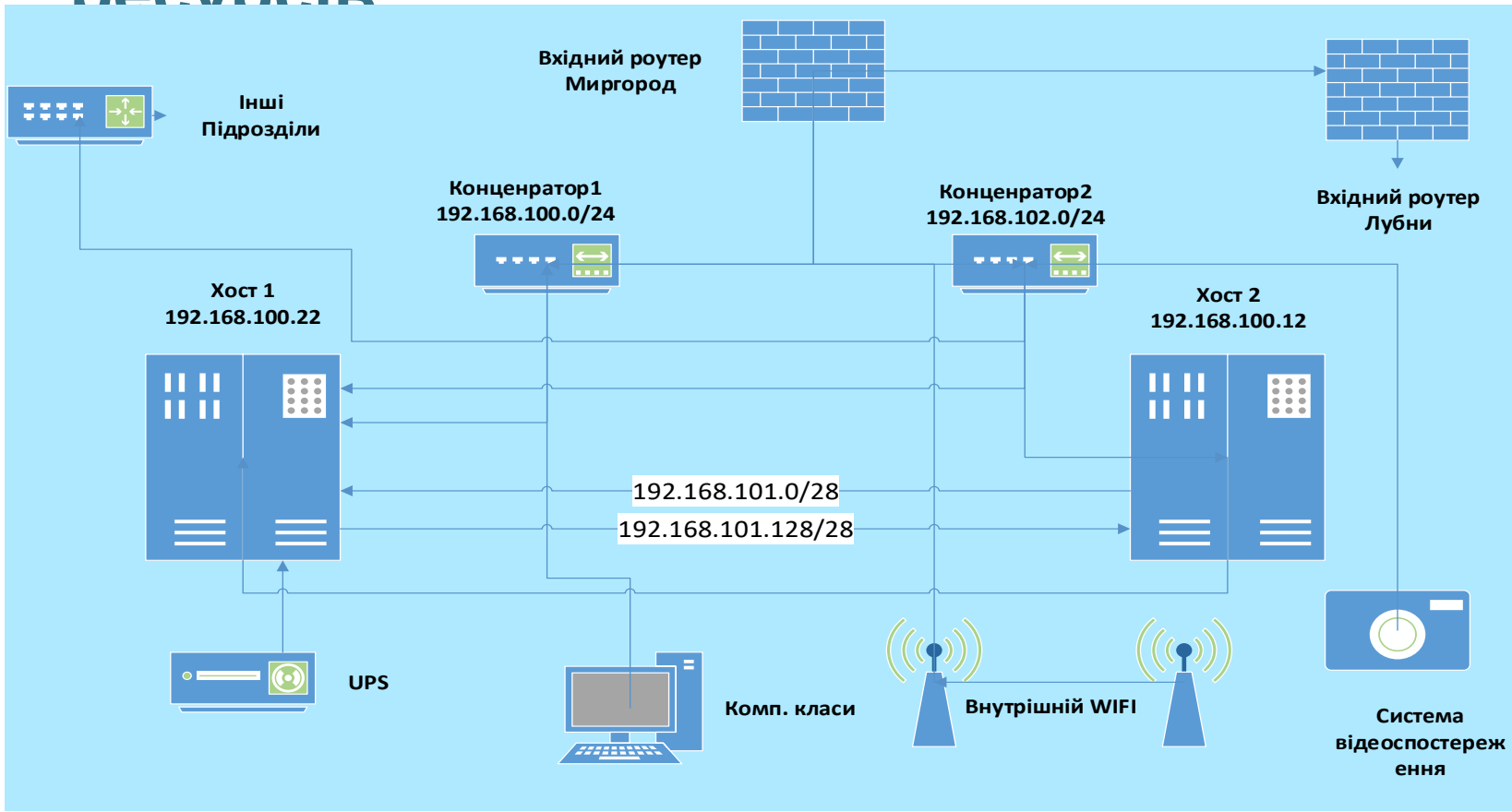
Модель доступу здобувачів



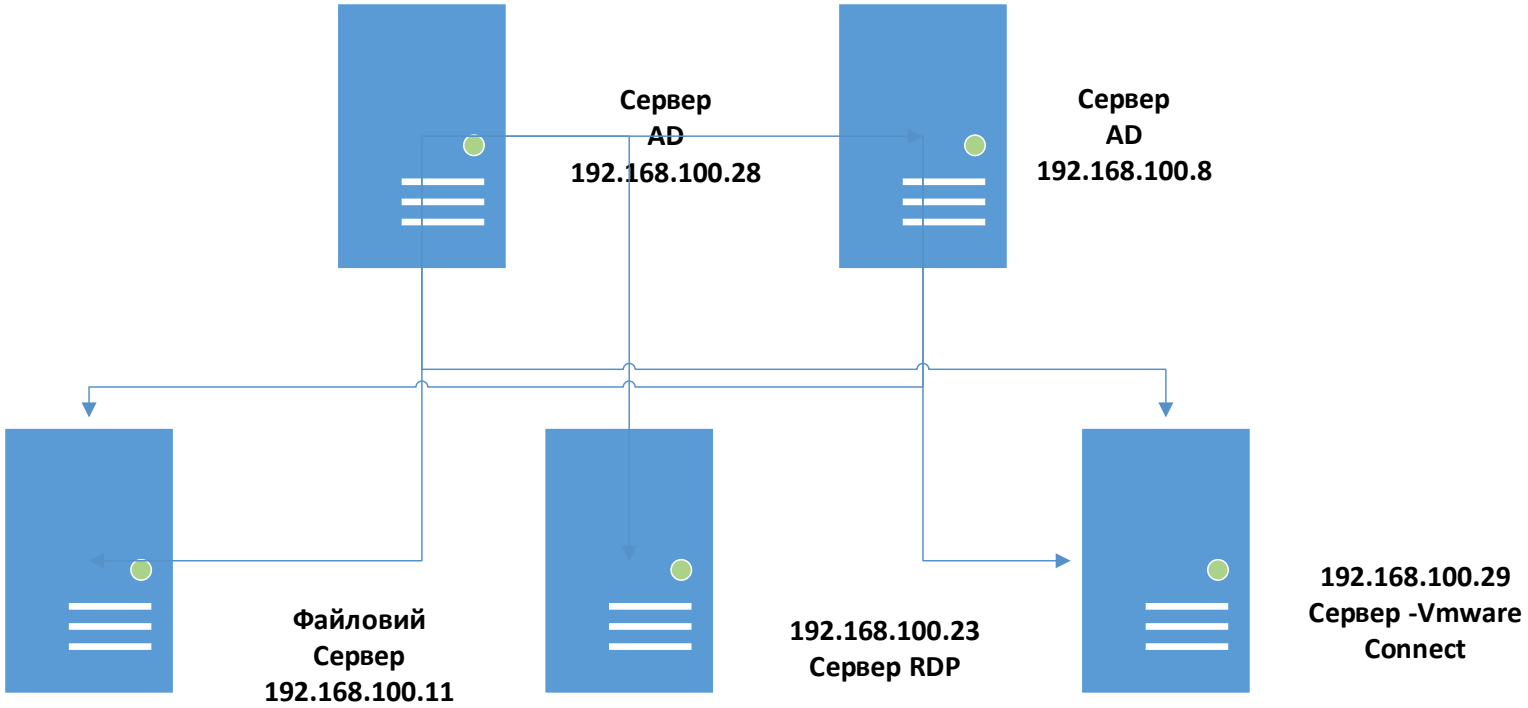
Загальна структура віртуальних ресурсів



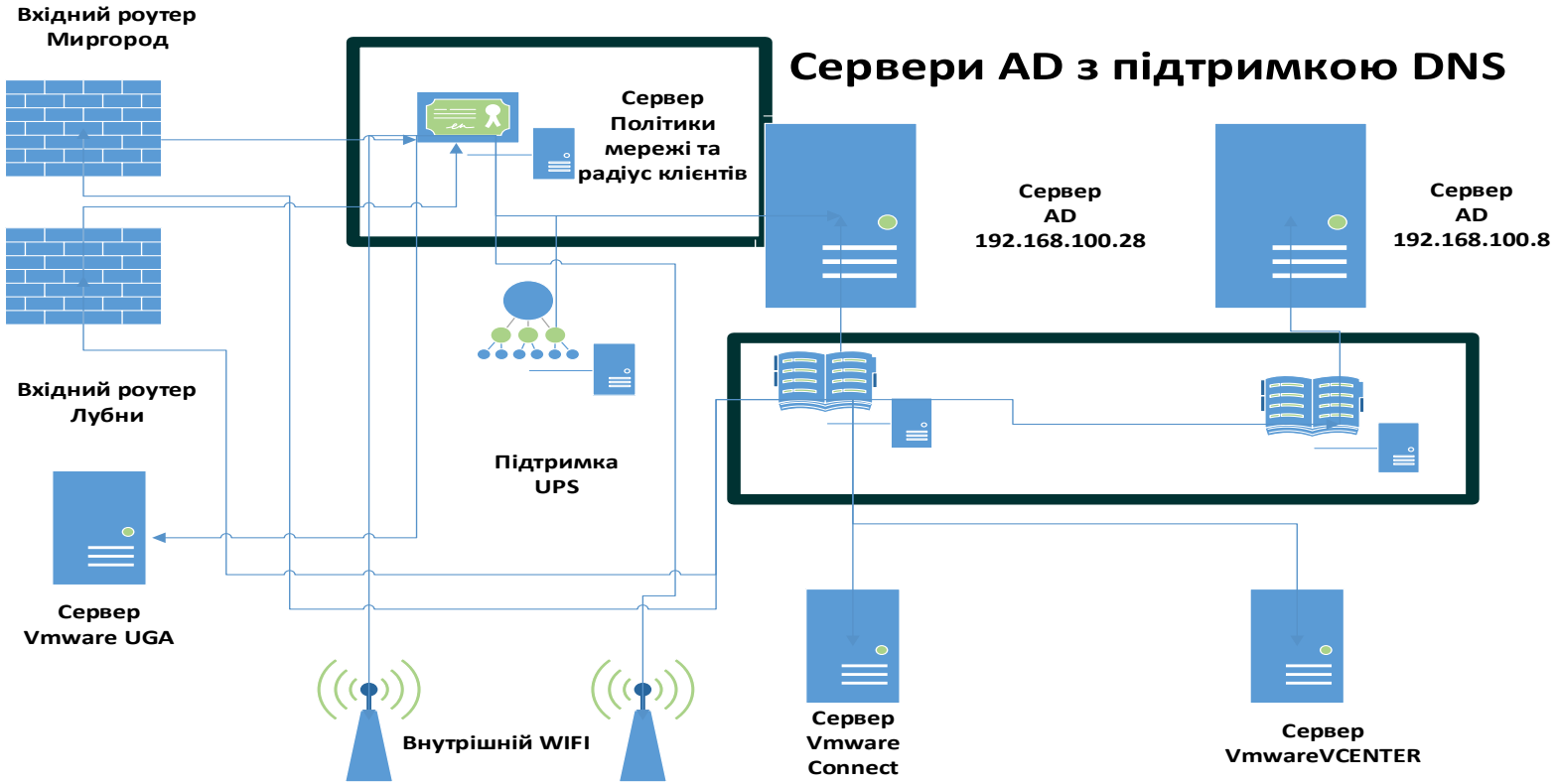
Загальна структура віртуальних ресурсів



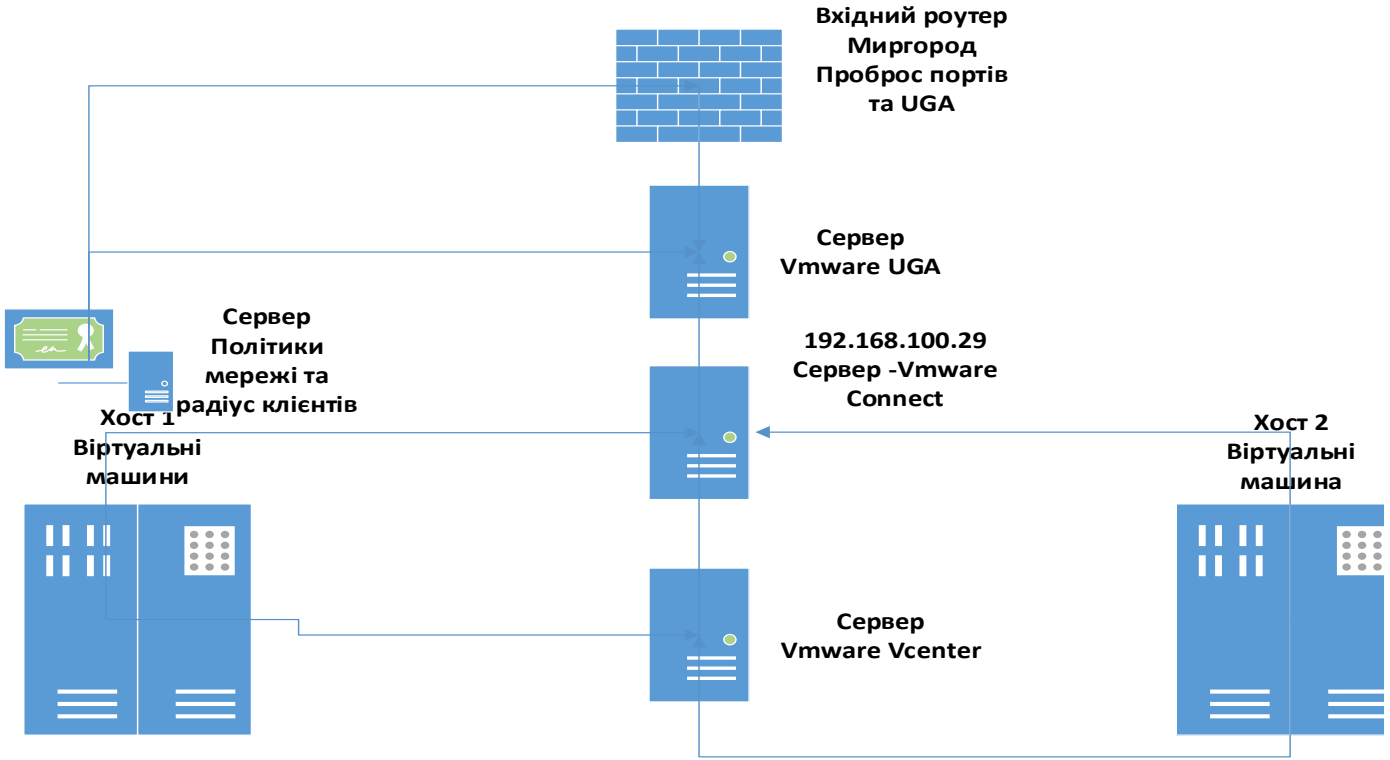
Загальна структура віртуальних WINDOWS



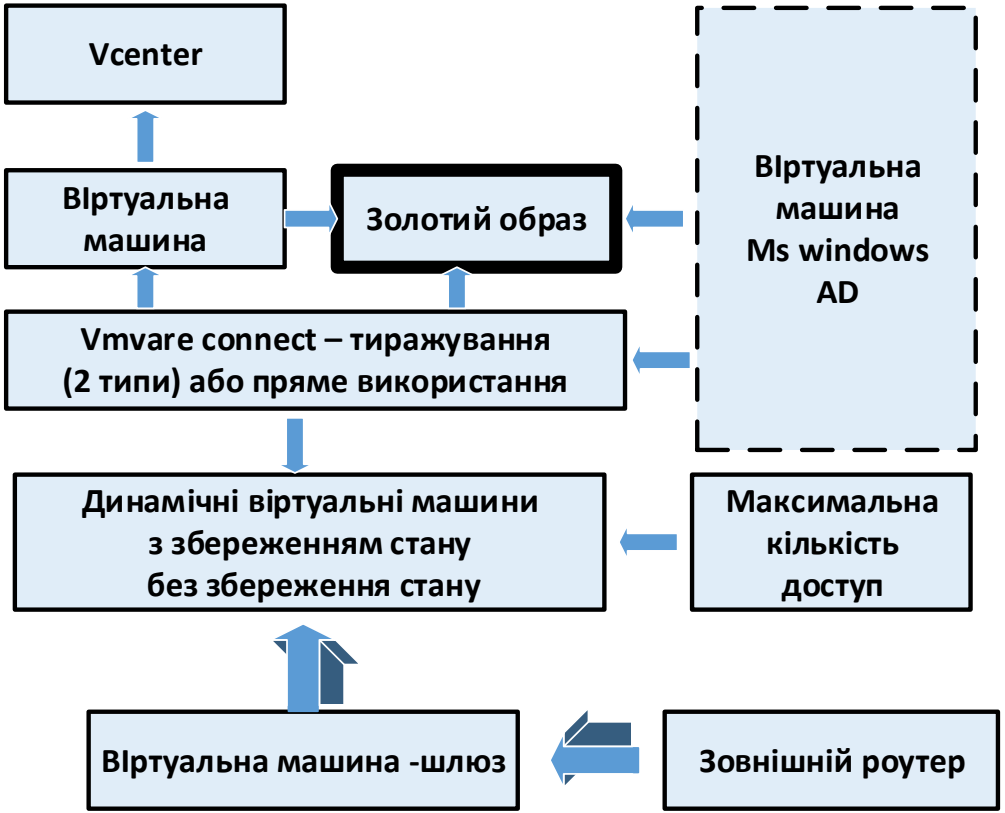
Інтегрована система імен користувачів



Процес підключення до ресурсів



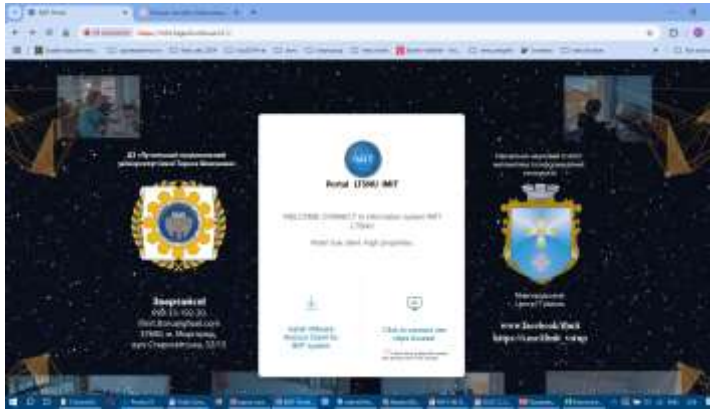
Модель використання в навчальному процесі

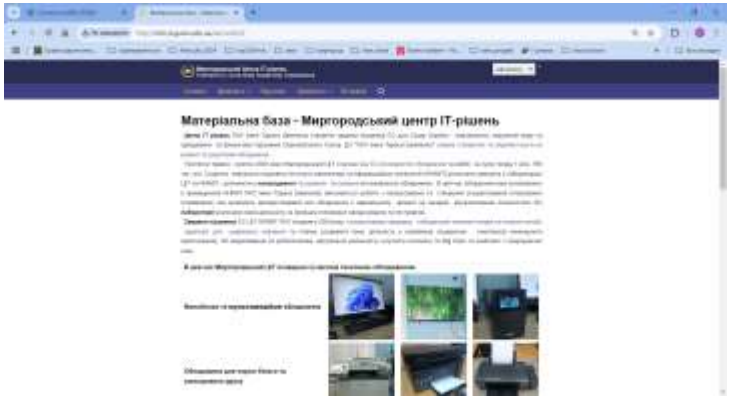


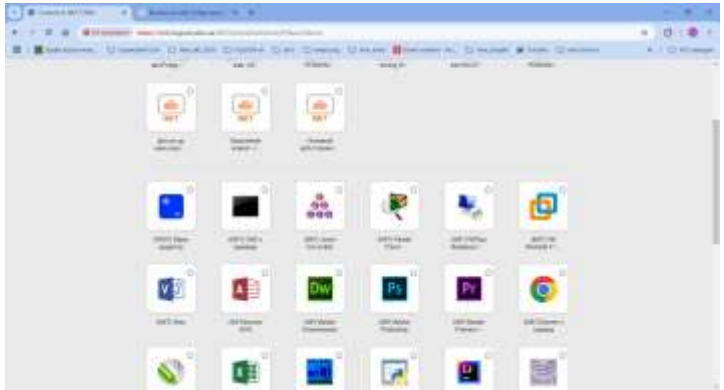
Веб сайт та портал

http://mitc.luguniv.edu.ua

https://mitc.luguniv.edu.ua:4432



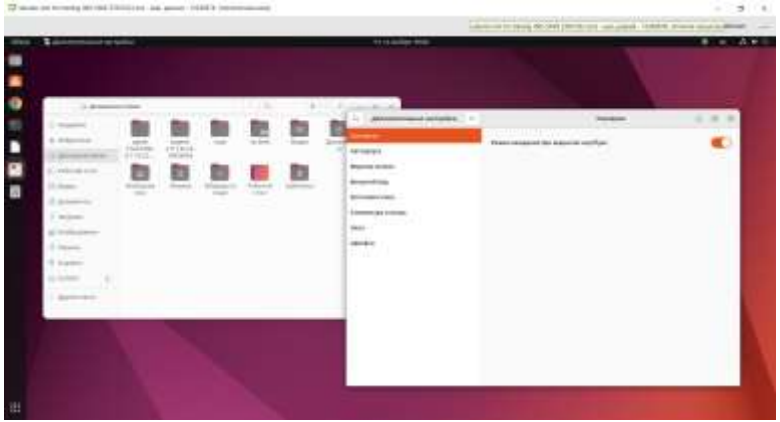




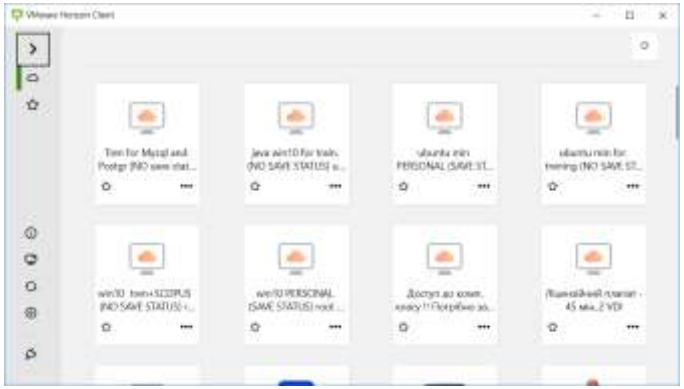
Навчальні віртуальні машини

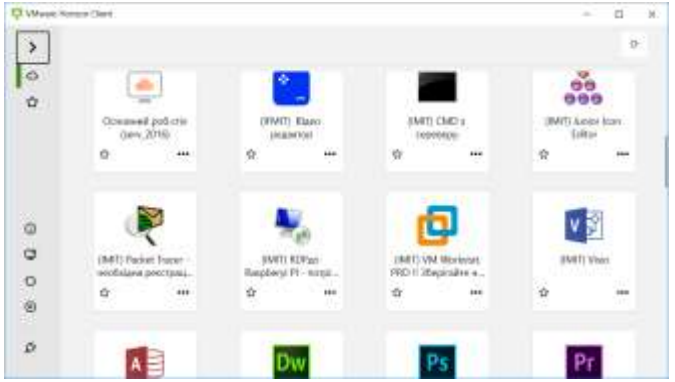
Створено декілька моделей навчальних ресурсів

- Віртуальна машина – для навчання
- Віртуальна машина для роботи
-
-



Перевірка на плагіат





Рівні, протоколи. Топології. Еталонна модель взаємодії відкритих систем OSI

Мета

Мета розділу: Пояснити як мережні протоколи дають змогу пристроям отримувати доступ до локальних і віддалених мережних ресурсів.

Назва теми	Мета вивчення теми
Правила	Описати типи правил, яких необхідно дотримуватися для успішного спілкування.
Протоколи	Пояснити, чому для мережного зв'язку необхідні протоколи.
Стеки протоколів	Пояснити мету дотримання вимог стеків протоколів.
Організації зі стандартизації	Пояснити роль організацій зі стандартизації у створенні протоколів для забезпечення мережної сумісності.
Еталонні моделі	Пояснити як моделі TCP/IP і OSI застосовуються для полегшення стандартизації процесу передавання даних.
Інкапсуляція даних	Пояснити як інкапсуляція забезпечує передавання даних по мережі.
Доступ до даних	Пояснити як локальні вузли одержують доступ до локальних ресурсів мережі.

Правила

Основи комунікацій

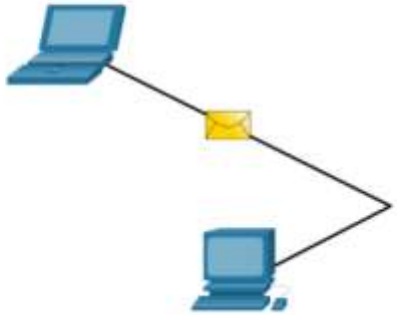
Мережі можуть відрізнятися за розмірами та складністю.
Недостатньо з'єднати пристрої між собою,
вони повинні узгодити правила спілкування.

У будь-якому спілкуванні є три елементи:

- Відправник (Джерело).
- Отримувач (Пункт призначення).
- Канал (Середовище передавання даних), який надає шлях для комунікацій.

Протоколи зв'язку

- Усі комунікації регулюються протоколами.
- Протоколи - це правила, яких необхідно дотримуватися.
- Ці правила, залежно від протоколу, різнитимуться.



Встановлення правил

- Необхідно використовувати встановлені правила або угоди для керування розмовою.
- У першому випадку - повідомлення належно не відформатоване і його важко прочитати. У другому випадку - повідомлення правильно відформатоване

```
humans communication between govern rules. It is verydifficult tounderstand messages that are not
correctly formatted and donot follow the established rules and protocols. A estrutura da
gramatica, da lingua, da pontuacao e do sentence faz a configuracao humana compreensivel por
muitos individuos diferentes.
```

```
Rules govern communication between humans. It is very difficult to understand messages that are
not correctly formatted and do not follow the established rules and protocols. The structure of
the grammar, the language, the punctuation and the sentence make the configuration humanly
understandable for many different individuals.
```

Встановлення правил (Продовж.)

Протоколи повинні відповідати таким вимогам:

- Ідентифіковані відправник та отримувач
- Обрані загальна мова та граматика
- Встановлені швидкість та терміни доставки
- Встановлені вимоги підтвердження отримання повідомлень

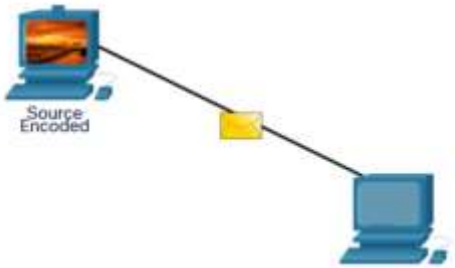
Вимоги до мережного протоколу

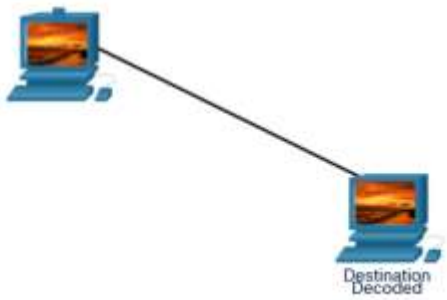
Всі комп'ютерні протоколи повинні бути узгоджені і містити такі вимоги:

- Кодування повідомлень
- Форматування і інкапсуляція повідомлень
- Розмір повідомлення
- Синхронізація повідомлень
- Параметри доставки повідомлень

Кодування повідомлень

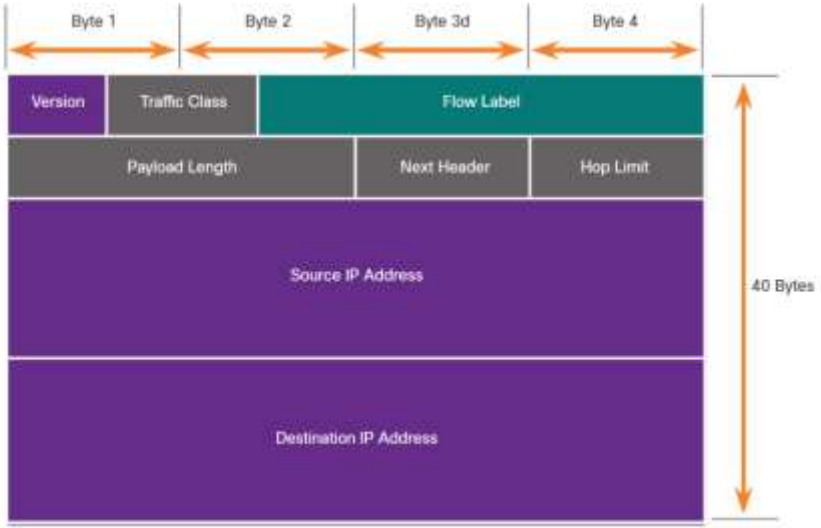
- Кодування - це процес перетворення інформації з однієї форми в іншу, прийнятну для подальшого передавання.
- Декодування - зворотний процес, в результаті якого інформація набуває початкового вигляду.





Форматування та інкапсуляція повідомлень

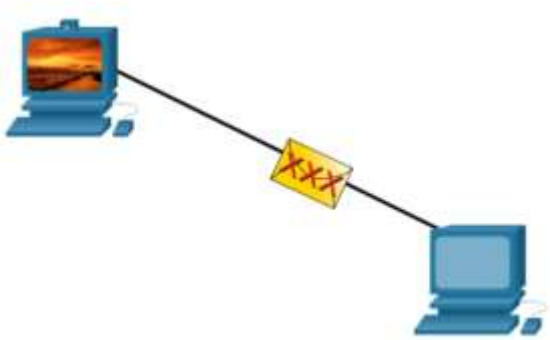
- Для повідомлення, яке надсилається, необхідно використовувати певний формат або структуру.
- Формати повідомлень залежать від типів повідомлень та каналів, що використовується для доставки повідомлень.

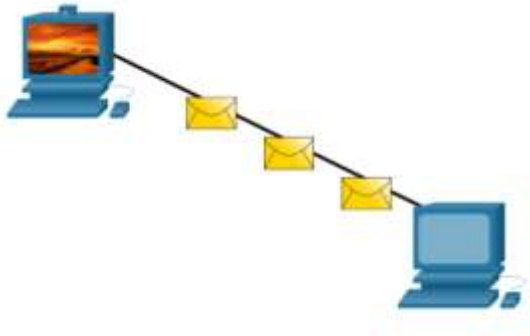


Розмір повідомлення

Кодування для обміну даними між вузлами повинна бути виконане в форматі, що відповідає середовищу.

- Повідомлення, що надсилаються через мережу, перетворюються в біти.
- Біти кодуються світловими, звуковими або електричними імпульсами (сигналами) певної форми.
- Вузол-отримувач повинен декодувати сигнали для інтерпретації повідомлення.





Синхронізація повідомлень

Синхронізація повідомлення включає:

Контроль потоку (Flow Control) – керування швидкістю передавання даних та визначення скільки інформації можна надіслати та з якою швидкістю вона може бути доставлена.

Час очікування відповіді (Response Timeout) – керування тим, як довго очікує пристрій, коли не отримує відповіді від вузла-отримувача.

Метод доступу (Access method) - визначення умов, коли вузол зможе надіслати повідомлення.

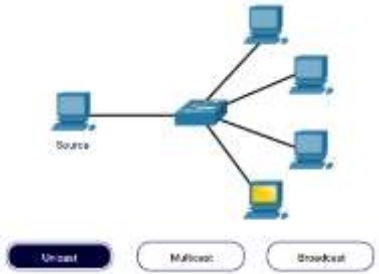
- Можуть існувати різні правила, що регулюють такі питання, як "колізії". Колізія виникає у випадку, коли більше ніж один пристрій одночасно здійснюють передавання трафіку і повідомлення пошкоджуються.
- Деякі протоколи є превентивними та намагаються запобігти колізіям; інші - лише реагують на виниклі колізії і застосовують метод повторної передачі повідомлення після колізії.

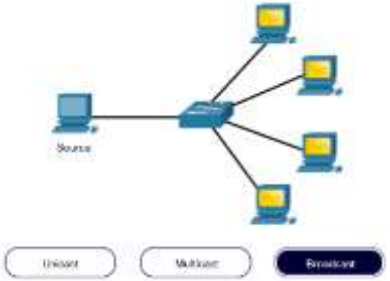
Параметри доставки повідомлень

Доставка повідомлення може здійснюватися одним з таких способів:

- **Одноадресна (Unicast) –** один до одного
- **Багатоадресна (Multicast) –** один до багатьох, зазвичай не до всіх
- **Широкомовна (Broadcast)** – один до всіх у певній мережі

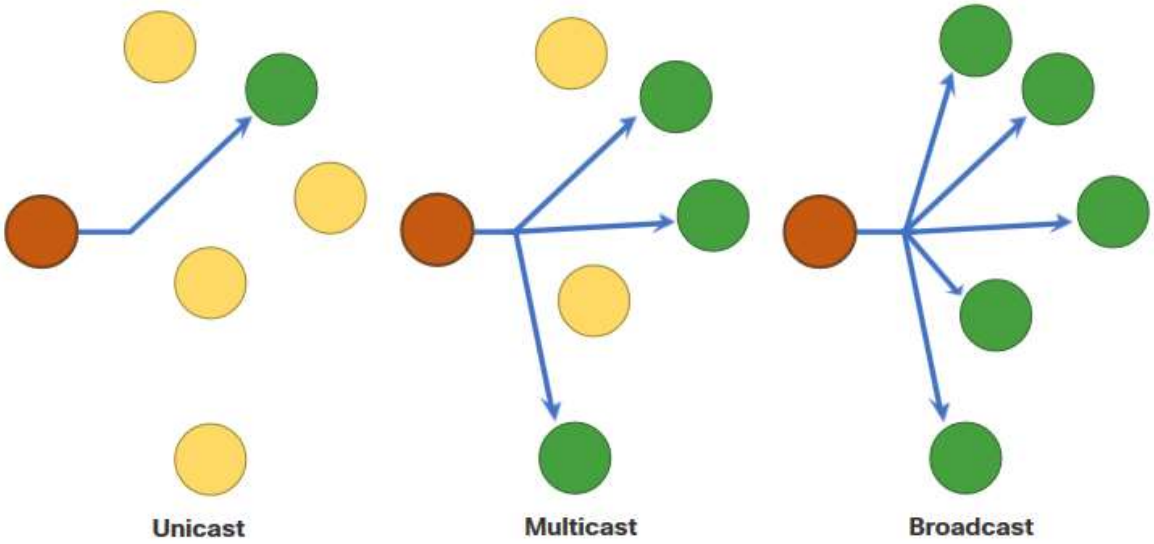
Примітка: Широкомовні розсилки використовуються в мережах IPv4, але не є в IPv6. Пізніше ми також побачимо альтернативну доставку (Anycast), як додатковий варіант доставки для IPv6.





Параметри доставки повідомлень

- У документації можуть використовуватися піктограми вузлів (як правило, кола) для відображення всіх пристроїв.
- На рисунку показано використання піктограм вузлів для різних варіантів доставки.



Протоколи

Огляд мережних протоколів

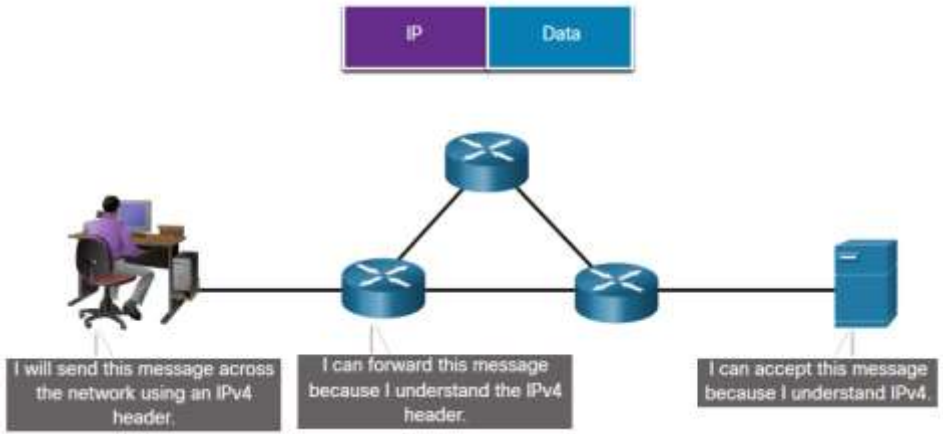
Мережні протоколи визначають загальний набір правил.

- Можуть бути реалізовані на пристроях у:
  - програмно (в ОС чи ПЗ)
  - апаратно (в обладнанні)
  - Програмно-апаратно
- У протоколів є свої:
  - Функції
  - Формати
  - Правила

Тип протоколу	Опис
Мережний зв'язок	дають можливість двом або більше пристроям спілкуватися через одну або кілька мереж
Мережна безпека	надає захист даних, забезпечуючи автентифікацію, цілісність та шифрування даних
Маршрутизація	дозволяє маршрутизаторам обмінюватися маршрутною інформацією, порівнювати записи про маршрути та вибирати найкращий маршрут передавання пакета
Виявлення сервісів	використовується для автоматичного виявлення пристроїв або служб.

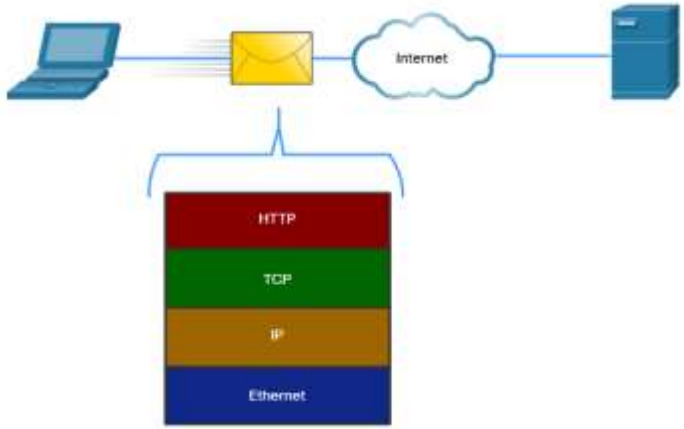
Функції мережного протоколу

- Пристрої використовують узгоджені протоколи для спілкування.
- Протоколи можуть мати одну або більше функцій.



Функція	Опис
Адресація	Ідентифікація відправника та отримувача
Надійність	Забезпечення гарантованої доставки
Керування потоком	Забезпечує ефективні швидкості для потоків даних
Послідовність (Sequencing)	Однозначне позначення (нумерація) кожного переданого сегменту даних
Виявлення помилок	Визначення, чи пошкоджені дані під час передачі
Програмний інтерфейс	Міжпроцесна взаємодія між мережними застосунками

Взаємодія протоколів



- Мережі вимагають використання декількох протоколів.
- Кожен протокол має свої функції та формат.

Протокол	Функція
Протокол передавання гіпертексту (HTTP, Hypertext Transfer Protocol)	▪ Керує взаємодією веб-сервера та веб-клієнта. ▪ Визначає зміст та формат повідомлень
Протокол керування передаванням (TCP, Transmission Control Protocol)	▪ Керує індивідуальними сеансами зв'язку ▪ Забезпечує гарантовану доставку повідомлень ▪ Керує потоком повідомлень
Міжмережний протокол (IP, Internet Protocol)	Забезпечує доставку повідомлення від відправника до отримувача
Ethernet	Доставляє повідомлення від однієї мережної плати/інтерфейсу до іншого в одній і ті й же локальній мережі Ethernet.

Стеки протоколів

Стеки мережних протоколів

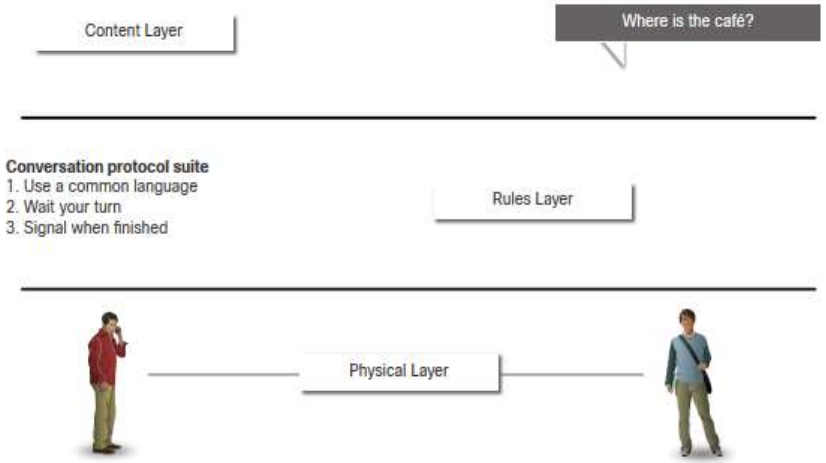
Протоколи повинні мати можливість працювати з іншими протоколами.

Стек протоколів:

- Стек протоколів - це сукупність взаємозалежних протоколів, необхідних для виконання функції зв'язку.
- Набори правил, які використовуються разом для того, щоб допомогти вирішити проблему

Протоколи розглядаються з точки зору рівнів:

- Вищі рівні
- Нижчі рівні- пов'язані з передаванням даних та наданням послуг верхнім рівням

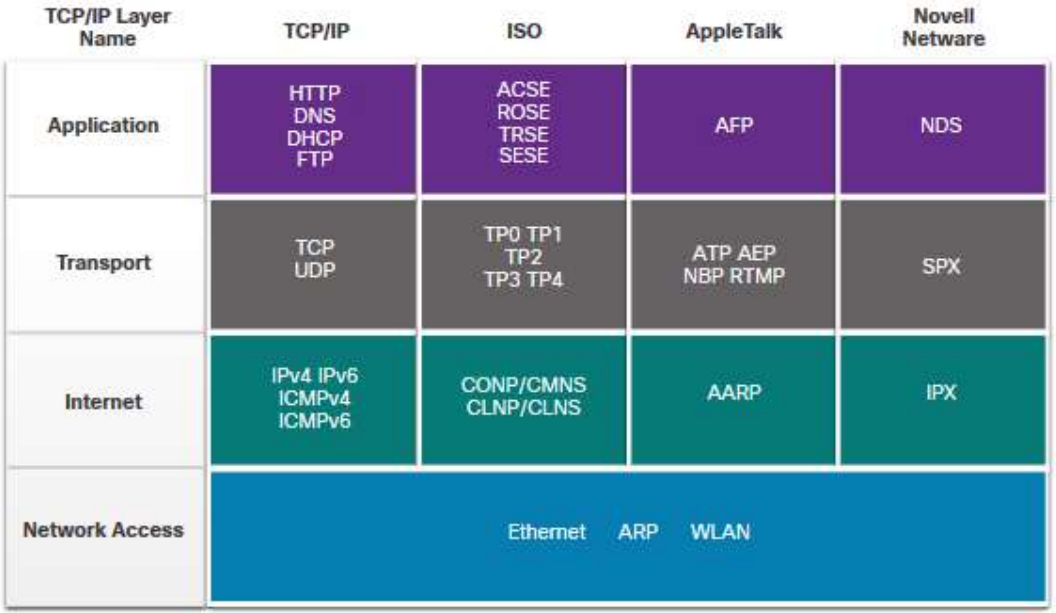


Protocol suites are sets of rules that work together to help solve a problem.

Стеки мережних протоколів

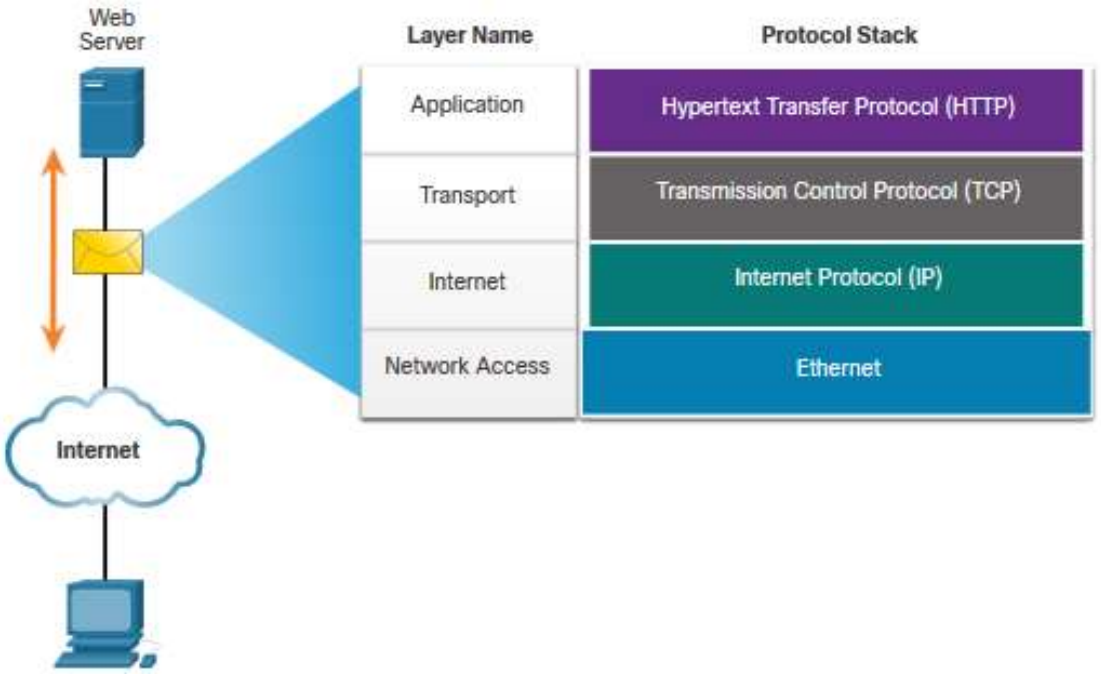
Існує кілька стеків протоколів.

- **Стек Інтернет-протоколів (Internet Protocol Suite) або TCP/IP -** найпоширеніший набір протоколів, який підтримується Інженерною групою з розвитку мережі Інтернет (IETF)
- **Протоколи взаємодії відкритих систем (OSI, Open Systems Interconnection) -** розроблені спільно Міжнародною організацією зі стандартизації (ISO) та Міжнародним союзом телекомунікацій (ITU) в 1977 році.
- **AppleTalk-** Пропрієтарний (фірмовий) стек протоколів від Apple Inc.
- **Novell NetWare-** Пропрієтарний (фірмовий) стек протоколів від Novell Inc.



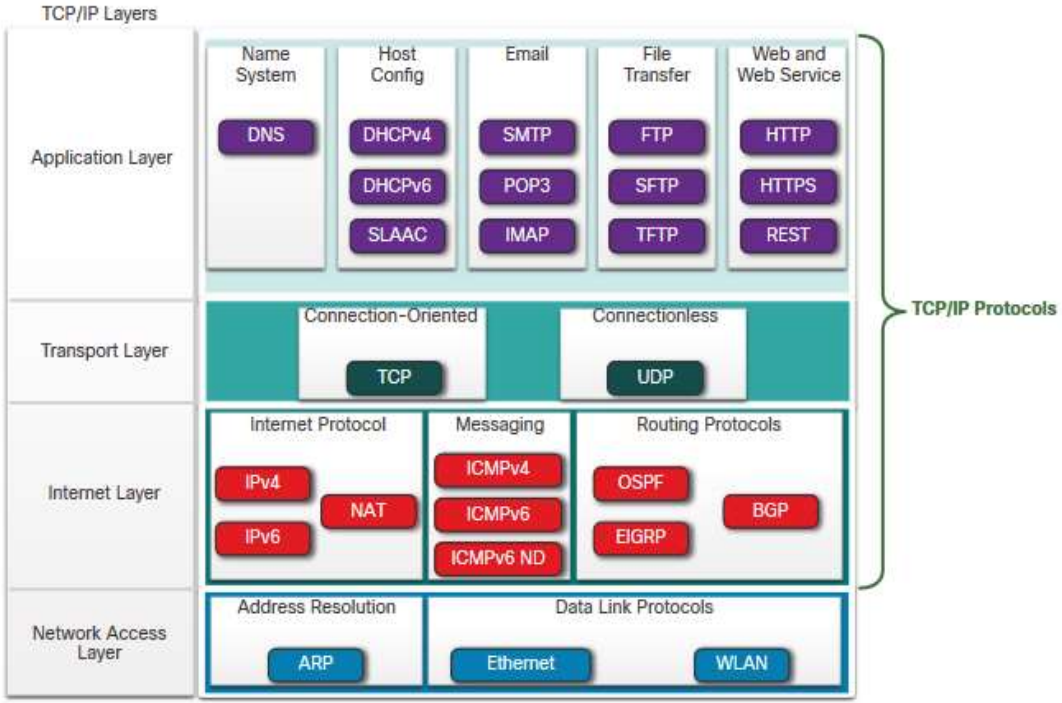
Приклад протоколу TCP/IP

- Протоколи TCP/IP функціонують на прикладному, транспортному та міжмережному рівнях.
- Найпоширенішими протоколами рівня мережного доступу для локальних мереж є Ethernet та WLAN.



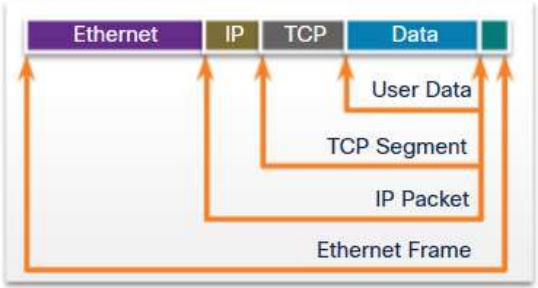
Стек протоколів TCP/IP

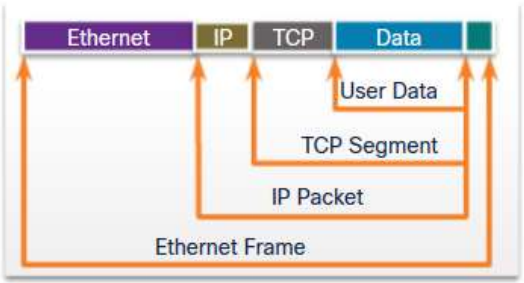
- TCP/IP - це стек протоколів, що використовується для передавання даних в мережі Інтернеті, містить велику кількість протоколів.
- TCP/IP - це:
  - Побудований на відкритих стандартах стек протоколів, який є у вільному доступі для широкого загалу та може вільно використовуватись будь-яким розробником чи виробником обладнання та ПЗ
  - Стек протоколів на основі стандартів, стек, який схвалений мережною індустрією та затверджений організацією зі стандартизації для забезпечення сумісності

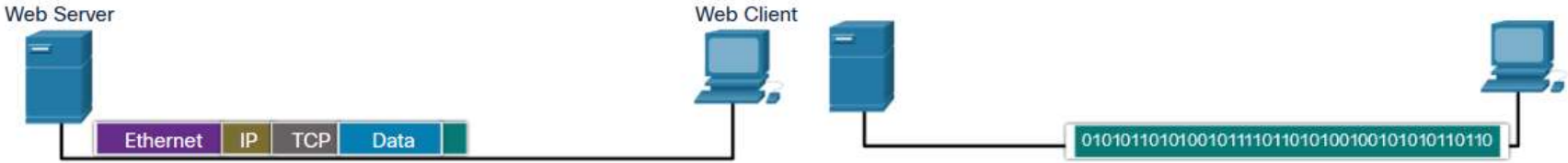


Обмін даними в TCP/IP

- Веб-сервер інкапсулює та відправляє веб-сторінку клієнту.
- Клієнт деінкапсулює веб-сторінку для веб-браузера







Організації зі стандартизації

Відкриті стандарти

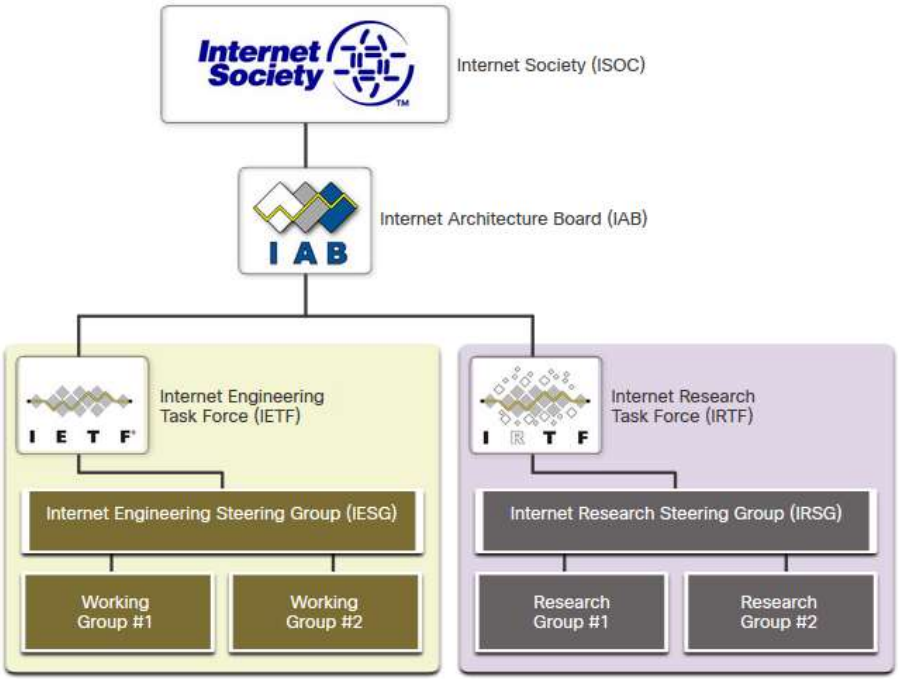
Відкриті стандарти підтримують:

- Функціональну сумісність (interoperability)
- Конкуренцію (competition)
- Інновації(innovation)

Організації зі стандартизації:

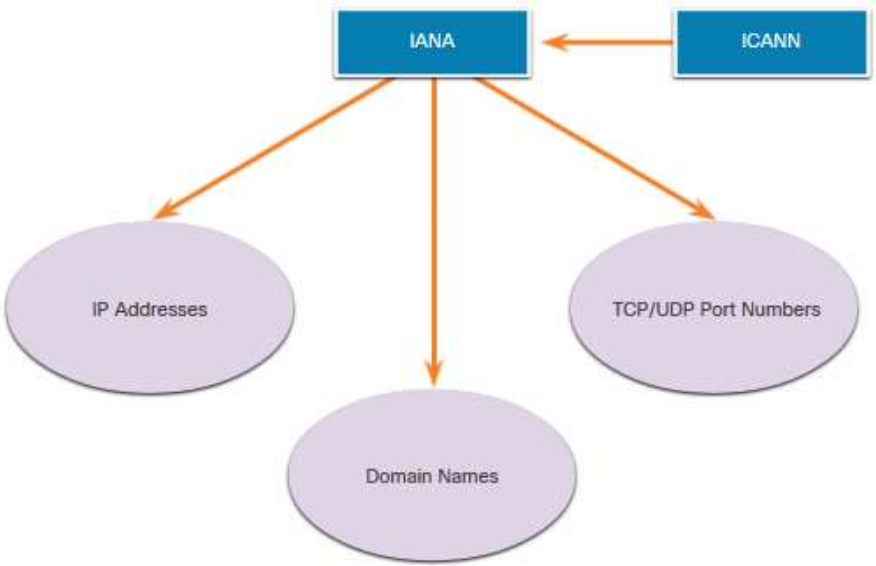
- Незалежні від виробників (vendor-neutral)
- Некомерційні організації (non-profit organizations)
- Створені для розробки та просування концепції відкритих стандартів.

Стандарти Інтернету



- **Інтернет-суспільство (ISOC, Internet Society)** - Сприяє відкритому розвитку та еволюції Інтернету
- **Рада по архітектурі мережі Інтернет (IAB, Internet Architecture Board)** - Відповідає за загальне керівництво і розробку інтернет-стандартів
- **Інженерна група з розвитку мережі Інтернет (IETF, Internet Engineering Task Force)** - Розробляє, оновлює та підтримує технології Інтернету та TCP/IP.
- **Дослідницької групи з розвитку мережі Інтернет (IRTF, Internet Research Task Force)** - Зосереджена на довготривалих дослідженнях, пов’язаних з Інтернетом та протоколами TCP/IP

Стандарти Інтернету (Продовж.)



Організації зі стандартизації, що займаються розробкою та підтримкою стеку TCP/IP:

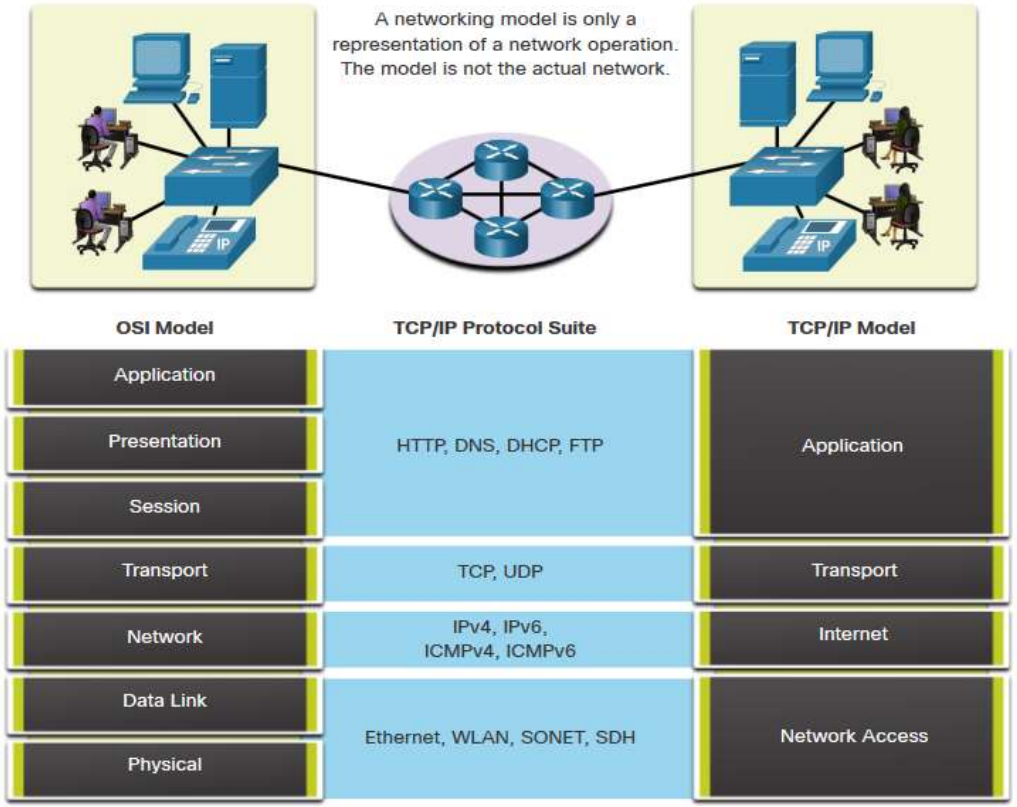
- **Інтернет-корпорація з призначення імен та номерів (ICANN, Internet Corporation for Assigned Names and Numbers** - координує розподіл IP-адрес, керує доменними іменами та надає іншу інформацію, що використовується в протоколах стеку TCP/IP.
- **Адміністрація адресного простору мережі Інтернет (IANA, Internet Assigned Numbers Authority** - Несе відповідальність за контроль і керування розподілом IP-адрес, керує доменними іменами та ідентифікаторами протоколів для ICANN.

Стандартизація електроніки та зв'язку

- **Інститут інженерів з електротехніки та електроніки (IEEE, Institute of Electrical and Electronics Engineers)** - **IEEE** вимовляється “I-triple-E", відповідає за просування технологічних інновацій та створення стандартів у багатьох галузях, зокрема, в енергетиці, охороні здоров'я, телекомунікаціях та мережних технологіях.
- **Альянс галузей електронної промисловості (EIA, Electronic Industries Alliance)** - розробляє стандарти, що стосуються електричної проводки, роз'ємів та 19-дюймових стійок, які використовуються для монтажу мережного обладнання.
- **Асоціація телекомунікаційної промисловості (TIA, Telecommunications Industry Association)** - відповідає за розробку стандартів зв'язку в різних областях, зокрема, стандартів радіотехнічного обладнання, станцій стільникового зв'язку, пристроїв передачі голосу за допомогою протоколу IP (Voice over IP, VoIP), пристроїв супутникового зв’язку тощо.
- **Міжнародний союз електрозв'язку, сектор стандартизації телекомунікацій (ITU-T, International Telecommunications Union-Telecommunication Standardization Sector)**- окреслює стандарти стиснення відео, телебачення на базі протоколу IP (IPTV, InternetProtocol Television) та стандарти широкосмугового зв'язку, наприклад, цифрову абонентську лінію(DSL, Digital Subscriber Line).

Еталонні моделі

Переваги використання багаторівневої моделі



Функціонування мережі є складною концепцією, його досить важко пояснити та зрозуміти. Тому використовується багаторівнева модель.

Нині для опису мережних операцій застосовуються дві багаторівневі моделі:

- Еталонна модель взаємодії відкритих систем (OSI Model, Open Systems Interconnection Reference Model)
- Еталонна модель TCP/IP (TCP/IP Reference Model

Переваги використання багаторівневої моделі (Продовж.)

Переваги використання багаторівневої моделі:

- - Полегшення розробки протоколів, оскільки протоколи, які функціонують на певному рівні, чітко визначають формати оброблюваних даних та мають визначені інтерфейси взаємодії з верхнім та нижнім рівнями.
- - Сприяння конкуренції, оскільки розробки різних виробників можуть працювати разом.
- - Запобігання ситуацій, коли зміна технологій або функціоналу одного рівня впливає на інші рівні (чи вищі, чи нижчі).
- - Надання загальної мови для опису функцій та можливостей мереж.

Еталонні моделі

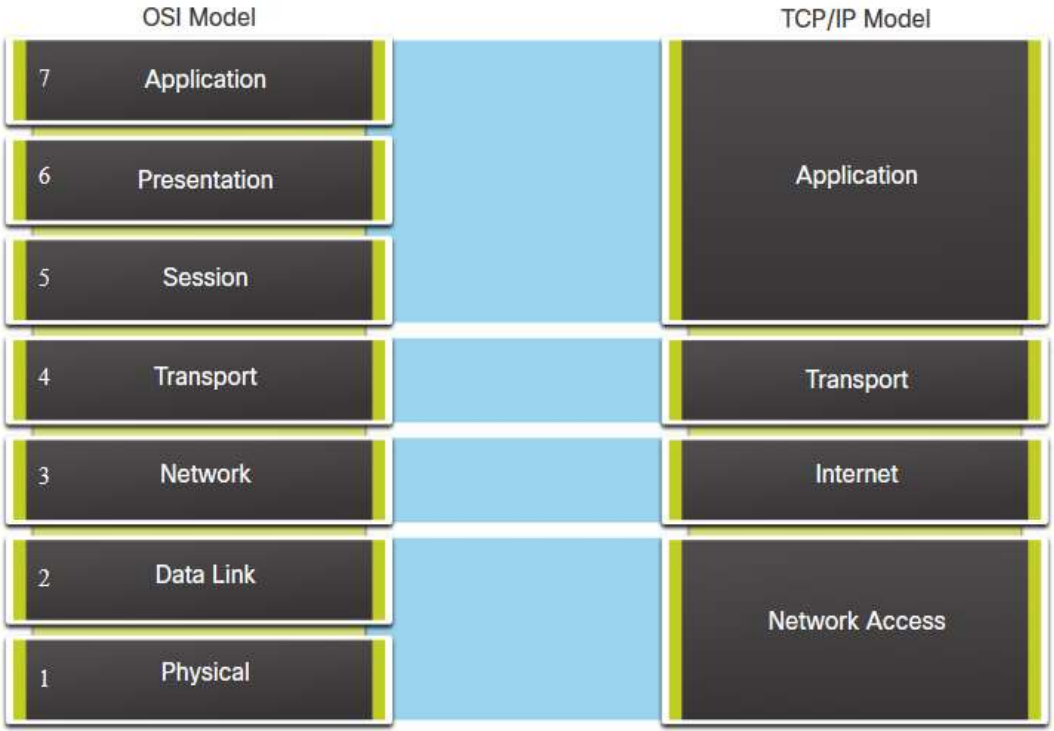
Еталонна модель OSI

Рівень моделі OSI	Опис
7 - Прикладний	Містить протоколи, які використовуються для обміну даними між процесами.
6 - Подання даних	Забезпечує загальне подання даних, що передаються між службами прикладного рівня
5 - Сеансовий	Надає послуги рівню подання та керує обміном даними.
4 - Транспортний	Визначає послуги для сегментації, передачі та десегментації даних для організації індивідуальних сеансів зв'язку.
3 - Мережний	Надає послуги з обміну окремими блоками даних через мережу.
2 - Канальний	Описує методи обміну кадрами даних через загальне середовище передавання інформації.
1 - Фізичний	Описує засоби для активації, підтримки та деактивації фізичних зв’язків.

Еталонна модель TCP/IP

Рівні моделі TCP/IP	Опис
Прикладний рівень	Відображення даних для користувача, а також забезпечення кодування/шифрування та керування сеансами зв'язку.
Транспортний рівень	Підтримка зв’язку між різними пристроями в різних мережах.
Міжмережний рівень	Визначення найкращого маршруту передавання даних через мережу.
Рівень мережного доступу	Керування фізичними пристроями та середовищем передавання даних, з яких складається мережа.

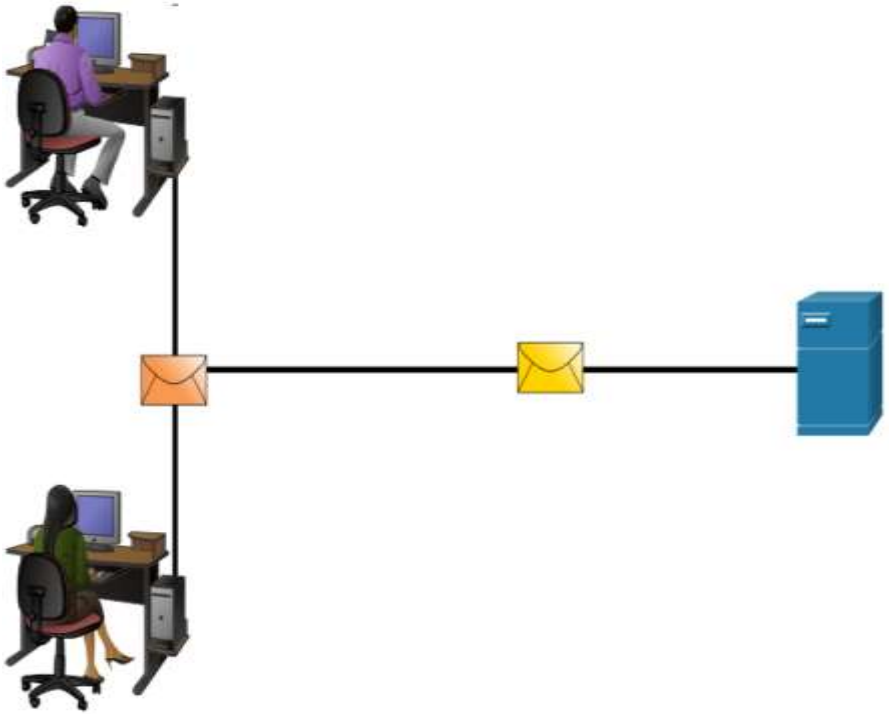
Порівняння моделей OSI і TCP/IP



- Рівень мережного доступу та прикладний рівень моделі TCP/IP для моделі OSI (з метою опису окремих функцій цих рівнів) додатково розділяються.
- На рівні мережного доступу стек протоколів TCP/IP не визначає протоколи, які необхідно використовувати для передавання даних через фізичне середовище.
- Рівні 1 і 2 моделі OSI описують необхідні процедури для доступу до середовища передавання даних та фізичні засоби, необхідні для надсилання даних через мережу.

Інкапсуляція даних

Сегментування повідомлень

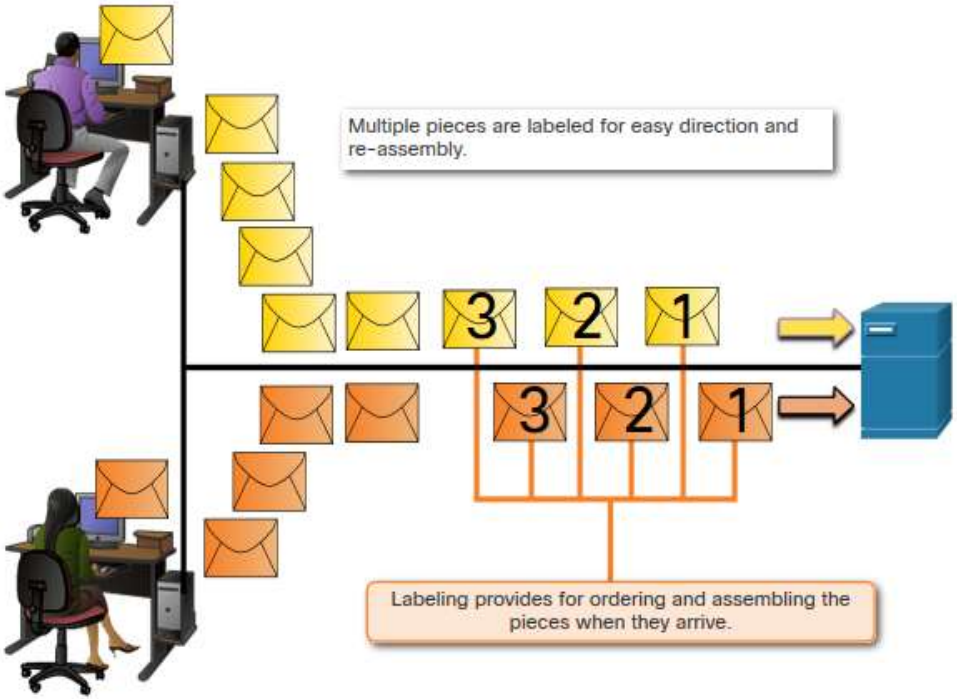


Сегментування - процес поділу потоку даних на менші блоки для передавання через мережу. Мультиплексування - це процеси збору декількох потоків сегментованих даних та їх перемежування.

Сегментування повідомлень надає дві основні переваги:

- **Підвищення швидкості** - Оскільки великий потік даних сегментований на пакети, великі обсяги даних можуть бути надіслані через мережу без прив'язки до каналу зв'язку.
- **Підвищення ефективності** - Якщо один сегмент не може досягти отримувача через мережний збій або перевантаження мережі, необхідно повторно передати тільки цей сегмент замість повторного передавання всього потоку даних .

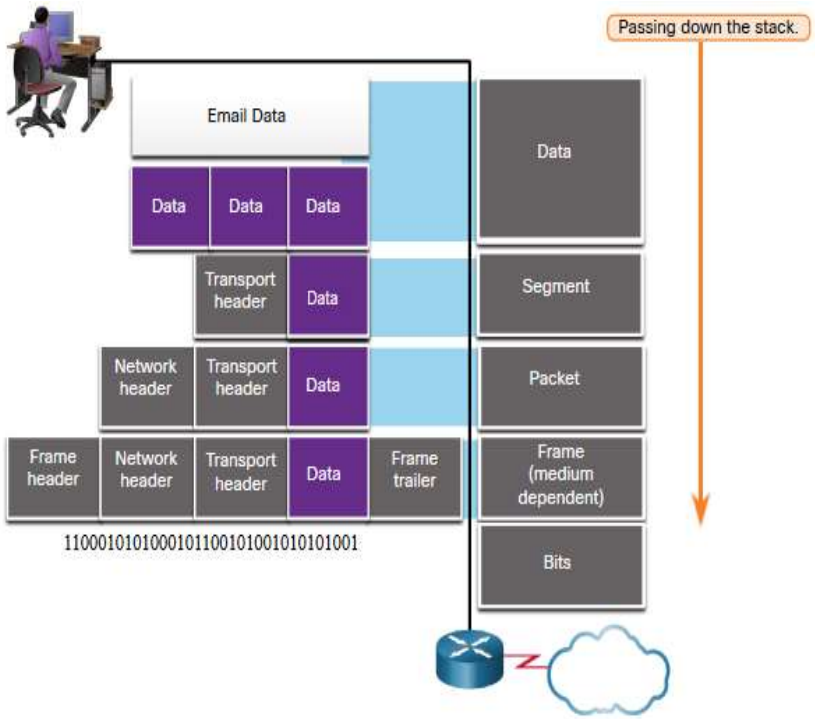
Встановлення послідовності



Встановлення послідовності повідомлень - це процес нумерації сегментів, щоб повідомлення можна було знову зібрати в пункті призначення.

Протокол TCP відповідає за формування послідовностей окремих сегментів.

Протокольний блок даних (PDU)

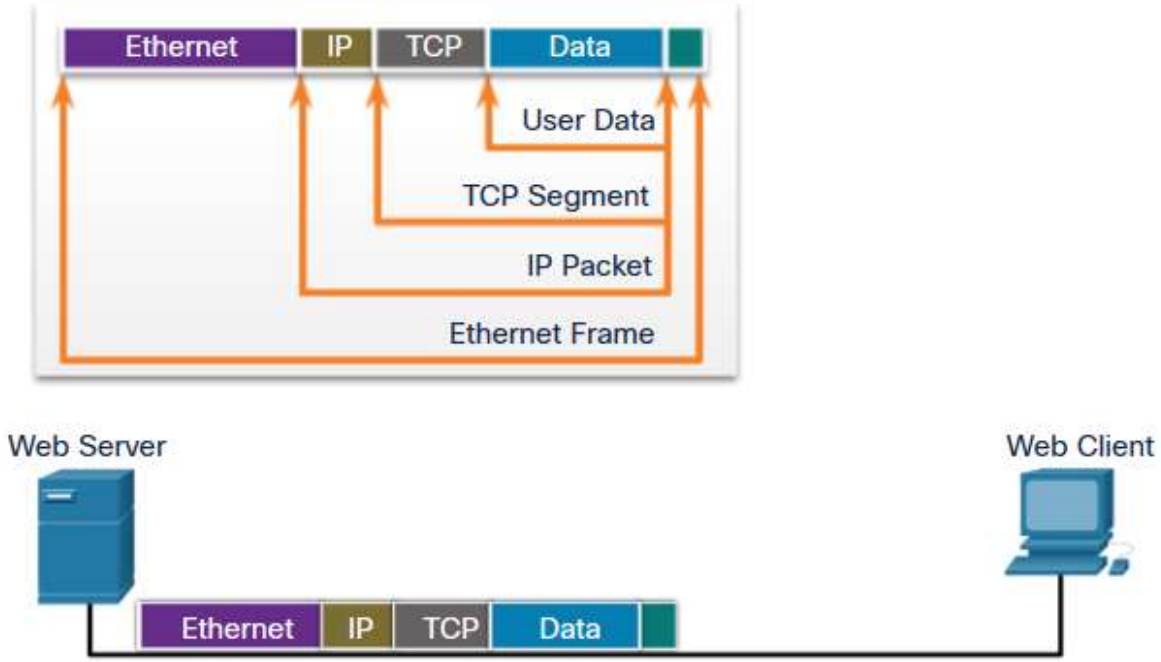


Інкапсуляція - це процес, при якому протоколи додають свою інформацію до даних.

- На кожному етапі цього процесу протокольний блок даних (PDU) має іншу назву, яка відображає його нові функції.
- Зважаючи на відсутність угоди щодо універсальних імен для PDU, в цьому курсі PDU носять назви PDU, які застосовуються у стеці TCP/IP.
- PDU, згідно порядку їх використання від верхнього до нижнього рівнів:
  1. Дані (Потік даних)
  2. Сегмент
  3. Пакет
  4. Кадр
  5. Біти (Потік бітів)

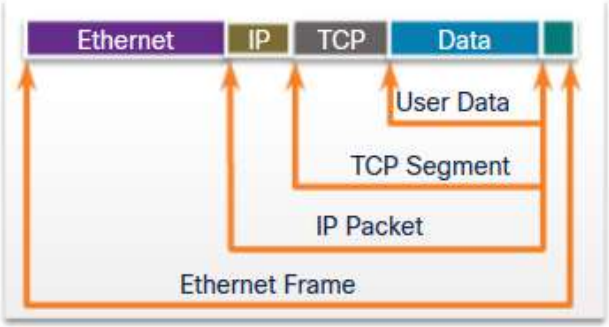
Приклад інкапсуляції

- Інкапсуляція - це низхідний процес.
- Вищий рівень виконує свої операції на даними та передає сформований протокольний блок даних на нижчий рівень. Цей процес повторюється на кожному рівні доти, доки дані не будуть надіслані у середовище як потік бітів.



Приклад деінкапсуляції

- Дані деінкапсулюються під час переміщення догори по стеку
- Коли рівень завершує свої операції, він відкидає заголовок свого протокольного блоку даних, а решту даних передає на вищий рівень. Це повторюється на кожному рівні, поки не отримується потік даних, який може обробити застосунок.
  1. Отримані біти (бітовий потік)
  2. Кадр
  3. Пакет
  4. Сегмент
  5. Дані (Потік даних)



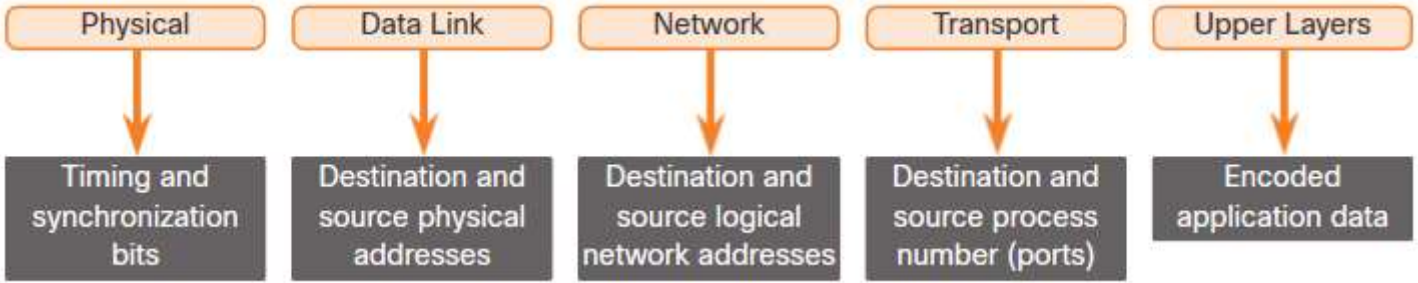
Доступ до даних

Адресація

І канальний, і мережний рівні використовують адресацію для доставки даних від відправника до отримувача.

Адреси відправника та отримувача мережного рівня - адреси, що необхідні для доставки IP-пакета від відправника до отримувача, в тій самій (локальній) або віддаленій мережі.

Адреси відправника та отримувача канального рівня - адреси, що необхідні для доставки кадра від однієї мережної плати до іншої мережної плати в одній і тій же мережі.

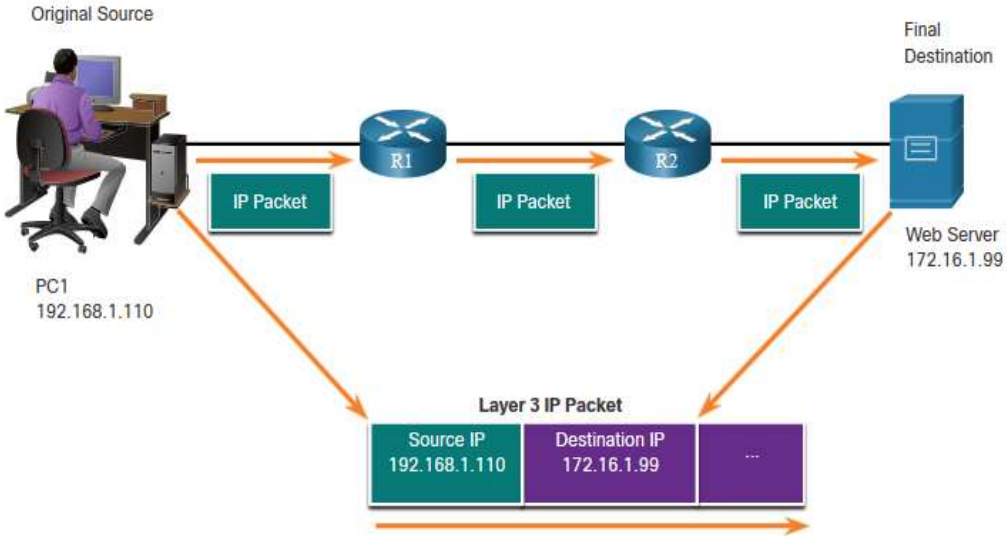


Логічна адреса Рівня 3

IP-пакет містить дві IP адреси:

- **IP-адреса відправника** - IP-адреса пристрою, який формує і надсилає пакет.
- **IP-адреса отримувача** - IP-адреса пристрою, що є кінцевим отримувачем пакету.

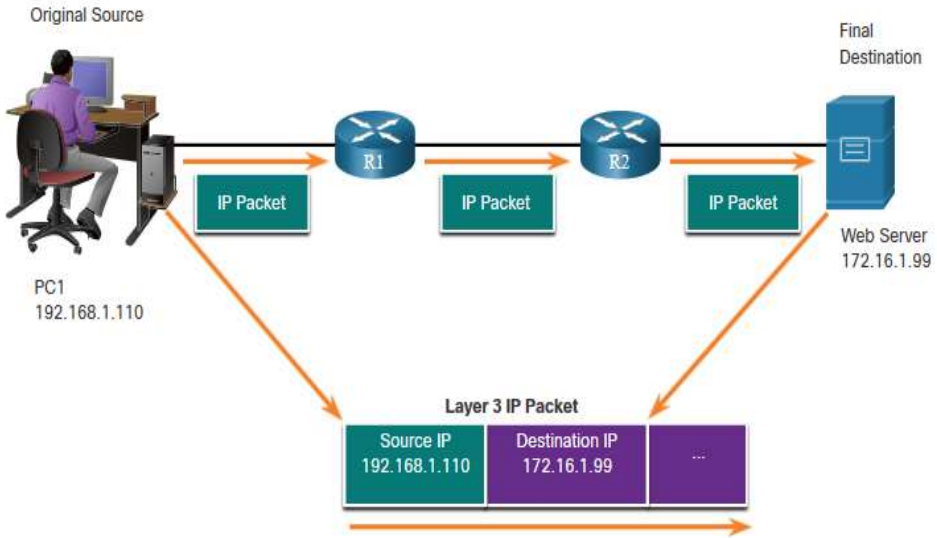
Ці адреси можуть належати як одній мережі, так і різним мережам.



Логічна адреса Рівня 3 (Продовж.)

IP-адреса складається з двох частин:

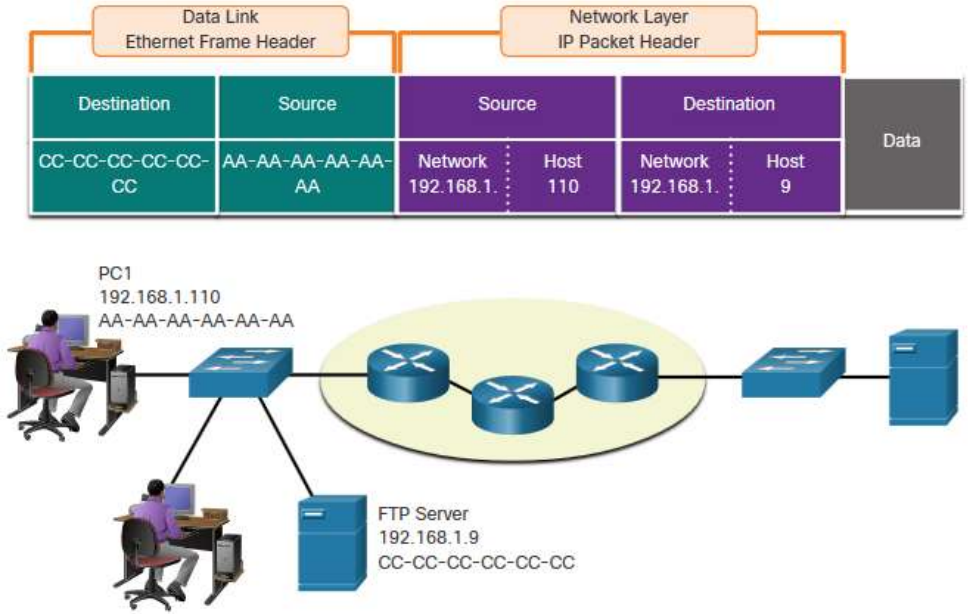
- **Мережна частина (IPv4) або префікс (IPv6)**
  - Частина IP-адреси, яка знаходиться ліворуч, ідентифікує IP-мережу, до якої належить IP-адреса.
  - Кожна локальна або глобальна мережа матиме однакову мережну частину.
- **Вузлова частина (IPv4) або ідентифікатор інтерфейсу (IPv6)**
  - Частина IP-адреси, яка знаходиться праворуч ідентифікує конкретний пристрій у IP-мережі.
  - Ця частина унікальна для кожного пристрою або інтерфейсу в мережі.



Пристрої в одній мережі

Усі пристрої однієї IP-мережі повинні мати однакові мережні частини IP-адрес.

- PC1 – 192.168.1.110
- FTP Server – 192.168.1.9

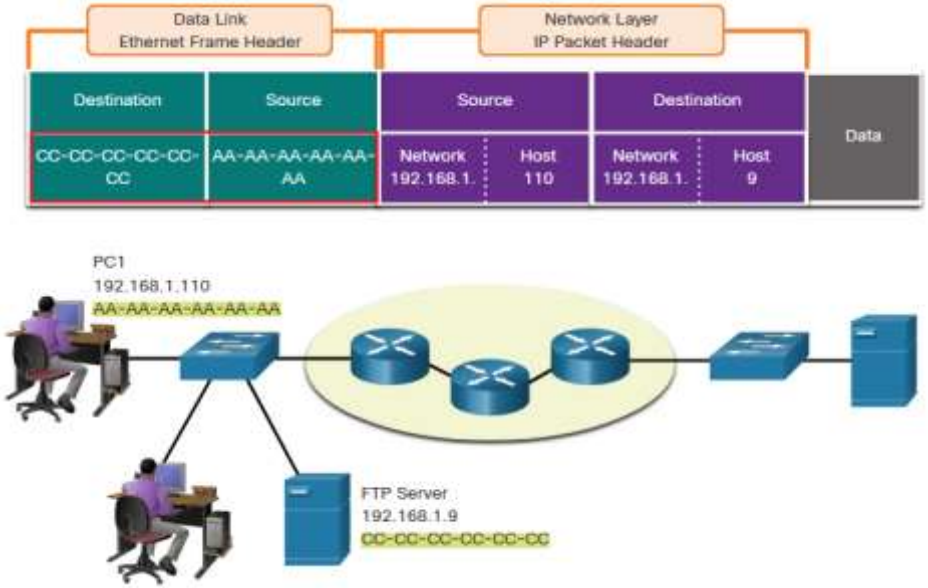


Роль адрес канального рівня даних: та сама IP-мережа

Коли пристрої знаходяться в одній мережі Ethernet, кадр канального рівня використовуватиме реальну MAC-адресу мережної плати отримувача.

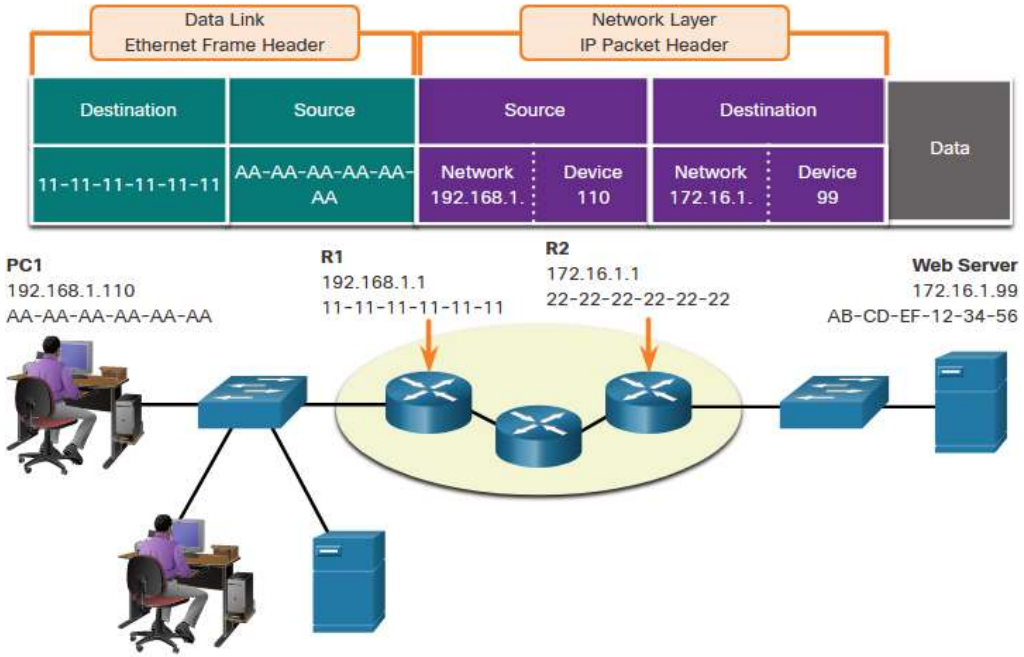
MAC-адреси фізично призначаються виробниками мережних плат/інтерфейсів. Їх також називають локальними, апаратними чи фізичними адресами.

- MAC-адреса відправника - адреса вузла, що підключений до локальної мережі (каналу).
- MAC-адреса отримувача - адреса. яка завжди належатиме вузлові, що підключений до тієї ж мережі (каналу), що і відправник, навіть якщо фактичний отримувач знаходиться у іншій мережі.



Пристрої у віддаленій мережі

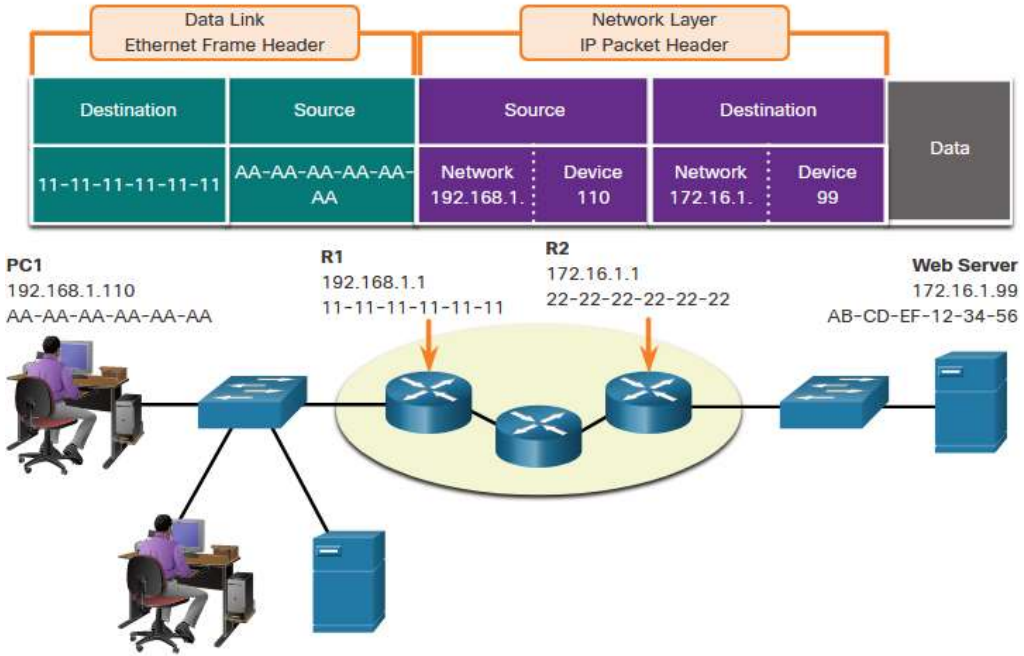
- Постає питання, як здійснюється передавання даних, якщо вузол-відправник і вузол отримувач знаходяться в різних мережах?
- Що відбувається, коли PC1 намагається зв'язатися з Web Server?
- Чи впливає це на канальний та мережний рівні?



Роль адрес мережного рівня

Якщо відправник та отримувач мають різні мережні частини IP-адрес, це означає, що вони знаходяться в різних мережах.

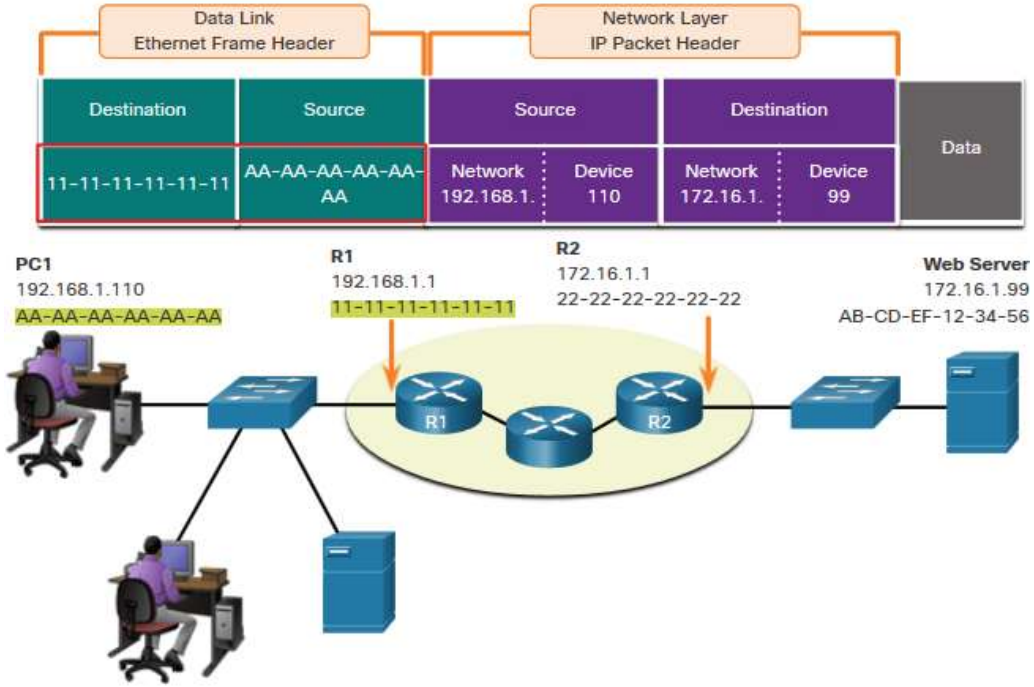
- PC1 – 192.168.1
- Web Server – 172.16.1



Роль адрес канального рівня для різних IP-мереж

Коли отримувач пакету знаходиться у віддаленій мережі, мережний рівень надасть канальному рівню локальну IP-адресу шлюзу за замовчуванням (маршрутизатора).

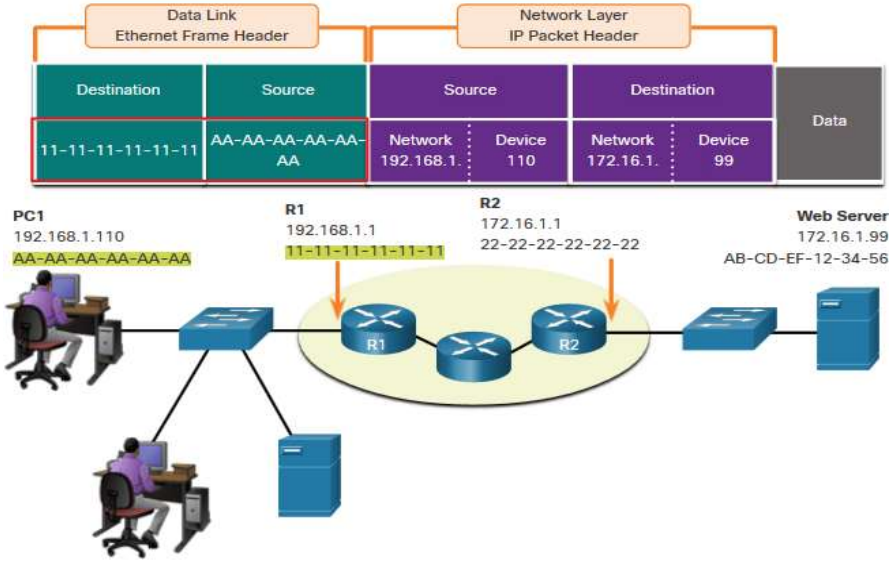
- Шлюз за замовчуванням (DGW, Default GateWay) - це IP-адреса інтерфейсу маршрутизатора, яка належить локальній мережі і буде «вихідними дверима» або «вихідним шлюзом» на шляху до всіх віддалених мереж.
- Усі пристрої локальній мережі повинні знати цю адресу, або їхній трафік буде обмежений лише локальною мережею.
- Після того, як канальний рівень на PC1 доставить пакет до шлюзу за замовчуванням (маршрутизатора), маршрутизатор може розпочати процес маршрутизації для доставки пакету до отримувача.



Роль адрес канального рівня для різних IP-мереж(Продовж.)

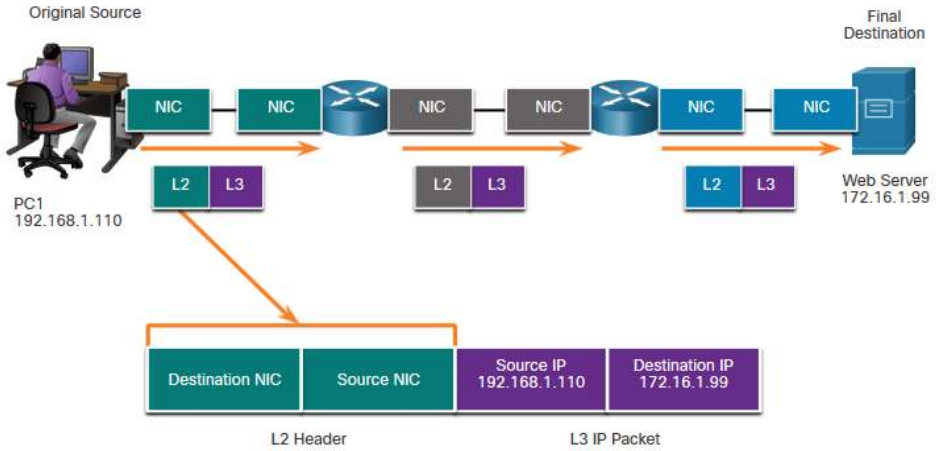
- Адреси канального рівня - це локальна адреси, тому необхідно мати адреси відправника і адреси отримувача для кожного канального сегменту.
- MAC-адреси для першого сегменту:
  - Відправник – AA-AA-AA-AA-AA-AA-AA (PC1) надсилає кадр.
  - Отримувач – 11-11-11-11-11-11 (R1 - MAC-адреса шлюзу за замовчуванням) отримує кадр.

Примітка: Хоча локальні адреси канального рівня змінюватиметься від канального сегменту до канального сегменту чи від переходу до переходу, мережні адреси залишаються незмінними.



Адресація канального рівня

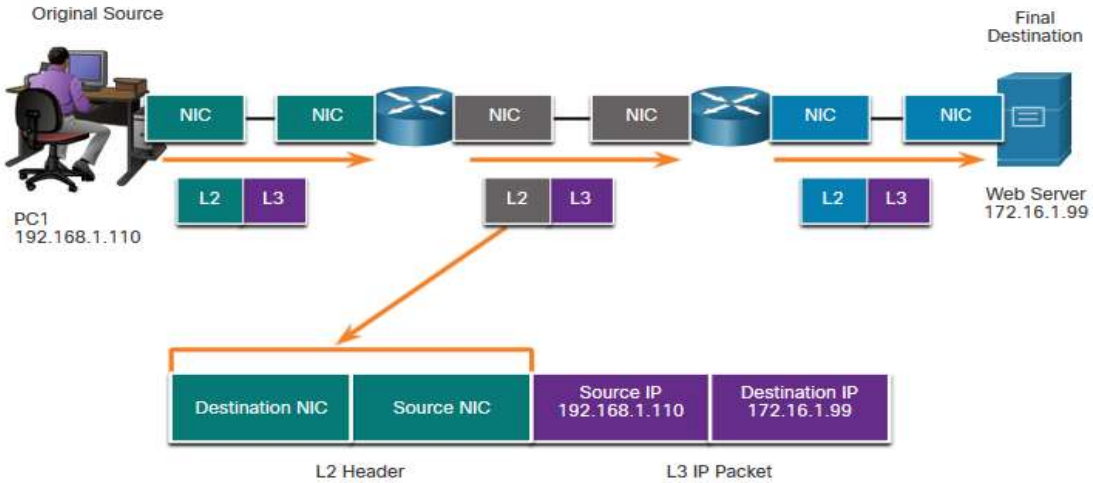
- Оскільки адреси канального рівня є локальними адресами, вони будуть змінюватися для кожного канального сегменту чи переходу на шляху передачі пакету до отриувача.
- MAC-адреси для першого сегменту:
  - Відправник - (мережна плата PC1) надсилає кадр
  - Отримувач - (інтерфейс першого маршрутизатора, DGW) отримує кадр



Адресація Канального рівня (Продовж.)

MAC-адреси для другого переходу:

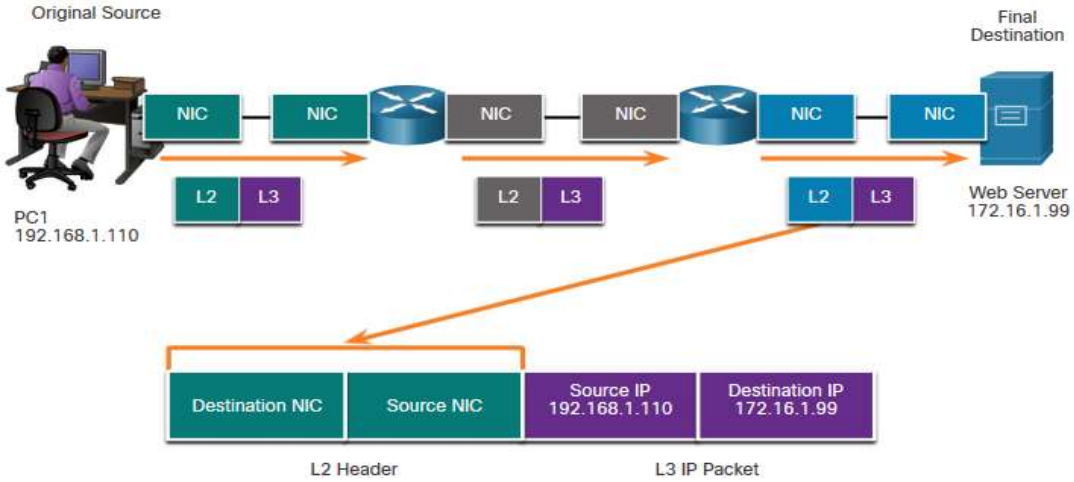
- Відправник - (Перший маршрутизатор - інтерфейс виходу) надсилає кадр
- Отримувач - (Другий маршрутизатор) отримує кадр



Адресація канального рівня (Продовж.)

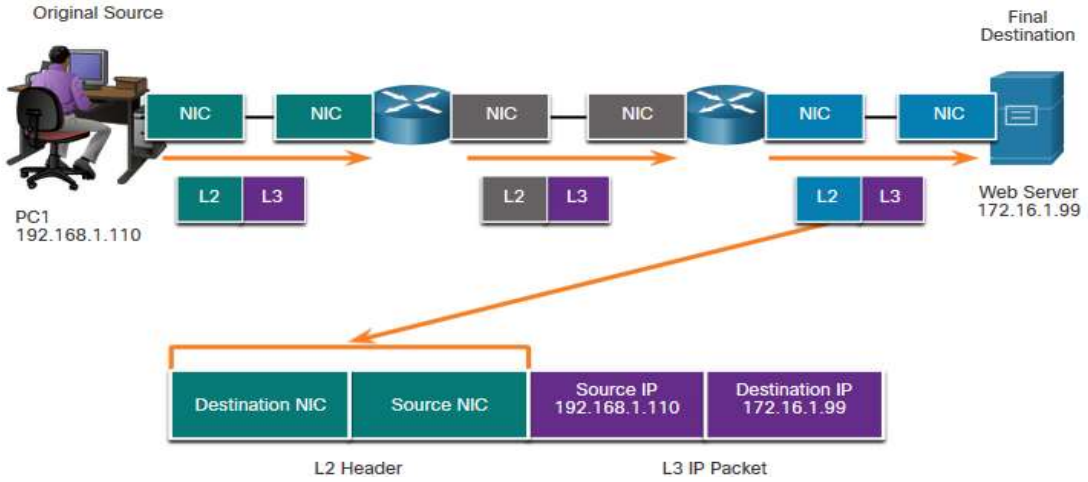
MAC-адреси для останнього сегменту:

- Відправник - (Другий маршрутизатор - інтерфейс вихід) надсилає кадр
- Отримувач - (мережна плата Web Server) отримує кадр



Адресація канального рівня (Продовж.)

- Зауважте, що пакет не модифіковано, але кадр змінено, тому IP-адреси (Рівень 3) не змінюється від сегмента до сегмента так, як MAC-адреси (Рівень 2).
- Адреси залишаються такими ж, оскільки вони є глобальними, а кінцевим вузлом-отримувачем все ще залишається Web Server.



Топології

Фізичні і логічні топології

Топологія мережі - це розташування мережних пристроїв та зв'язки між ними.

Існує два типи топологій, які використовуються при описі мереж:

- **Фізична топологія** — показує фізичні з'єднання між пристроями.
- **Логічна топологія** — визначає віртуальні зв'язки між пристроями, враховуючи інтерфейси пристроїв і схеми IP-адресації.

WAN топології

Існує три поширені фізичні топології WAN:

- **Point-to-Point** - це найпростіша і найбільш поширена WAN топологія. Вона містить постійний канал між двома кінцевими точками.
- **Hub and spoke** – схожа на топологію "зірка", де центральний пристрій з'єднує філіали за допомогою з'єднання точка-точка.
- **Повнозв'язна** – забезпечує високу доступність, але вимагає, щоб кожна кінцева система була з'єднана з кожною іншою кінцевою системою.

WAN топологія точка-точка

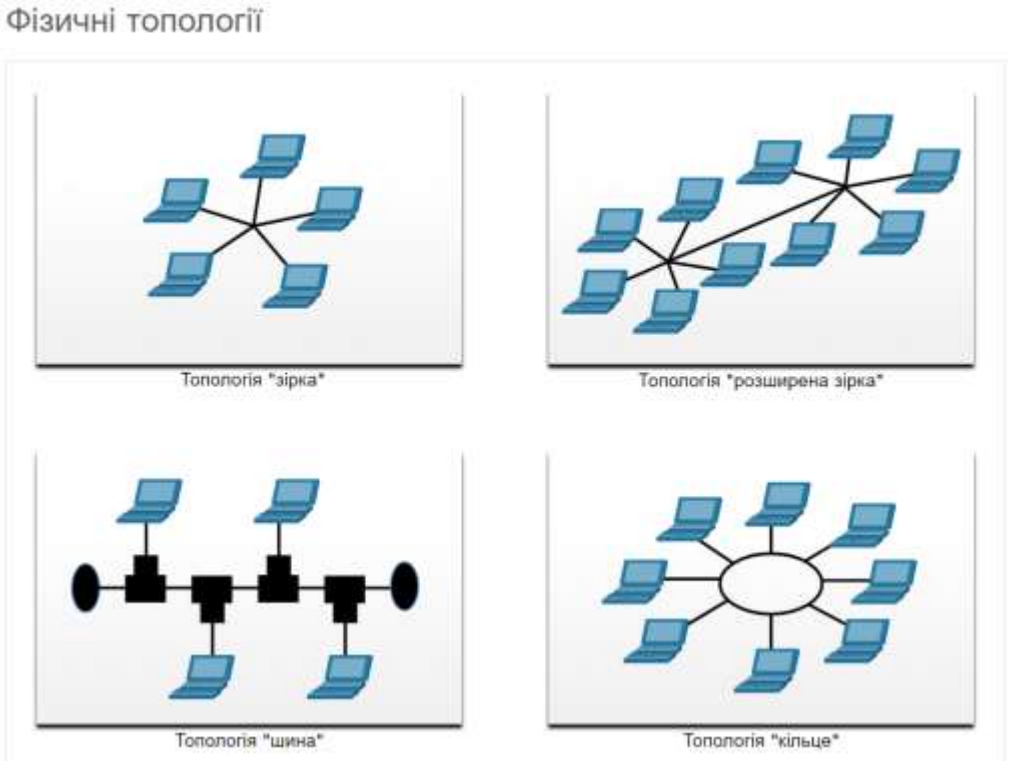
- Фізичні топології точка-точка безпосередньо з'єднують два вузли.
- Вузли можуть не мати спільного доступу до середовища передавання даних з іншими вузлами.
- Оскільки всі кадри в середовищі передавання даних можуть подорожувати лише до або від одного з двох вузлів, Point-to-Point WAN протоколи можуть бути дуже простими.

LAN топології

Кінцеві пристрої в локальних мережах зазвичай взаємозв'язані за топологією "зірка" або "розширена зірка". Топології "зірка" та "розширена зірка" є простими в розгортанні, легко масштабуються і дозволяють легко знайти та усунути несправність.

Технології раннього Ethernet і застарілого Token Ring забезпечували дві додаткові топології:

- **Шина** - Всі кінцеві системи з'єднані одна з одною в ланцюг і на кожному кінці ланцюг завершується у певній формі.
- **Кільце** — Кожна кінцева система з'єднується з відповідними сусідами, щоб сформувати кільце.



Напівдуплексний та повнодуплексний зв'язок

Напівдуплексний зв'язок

- Дозволяє лише одному пристрою надсилати або отримувати дані одночасно в середовищі передавання даних множинного доступу.
- Використовувався на WLAN і застарілих топологіях типу "шина" з концентраторами Ethernet.

Повнодуплексний зв'язок

- Дозволяє обом пристроям одночасно передавати і приймати дані в середовищі передавання даних множинного доступу.
- Комутатори Ethernet працюють в режимі повного дуплексу.

Методи керування доступом

Конкурентний доступ

Всі вузли, які працюють у напівдуплексному режимі, конкурують за використання середовища передавання даних. Приклади:

- Множинний доступ з контролем несучої та виявленням колізій (CSMA/CD) використовується в застарілому Ethernet з топологією "шина".
- Множинний доступ з контролем несучої і униканням колізій (CSMA/CA) використовується в бездротових локальних мережах.

Контрольований доступ

- Детермінований доступ, де кожен вузол має свій час для використання середовища передавання даних.
- Використовується в застарілих мережах, таких як Token Ring і ARCNET.

Конкурентний доступ – CSMA/CD

CSMA/CD

- Використовується застарілими локальними мережами Ethernet.
- Працює у напівдуплексному режимі, коли тільки один пристрій надсилає або отримує одночасно.
- Використовує процес виявлення конфліктів, щоб керувати тим, коли пристрій може надсилати повідомлення, і що відбувається, якщо одночасно надсилають кілька пристроїв.

Процес виявлення конфліктів CSMA/CD:

- Пристрої, що передають одночасно, створюють колізію в середовищі множинного доступу.
- Пристрої виявляють колізії.
- Пристрої очікують впродовж випадкового проміжку часу і ретранслюють дані.

Конкурентний доступ – CSMA/CA

CSMA/CA

- Використовується IEEE 802.11 WLAN.
- Працює у напівдуплексному режимі, коли тільки один пристрій надсилає або отримує одночасно.
- Використовує процес уникнення конфліктів, щоб керувати тим, коли пристрій може надсилати повідомлення, і що відбувається, якщо одночасно надсилають кілька пристроїв.

Процес уникнення конфліктів CSMA/CA:

- Під час передавання пристрої також включають інформацію про тривалість часу, яка для цього необхідна.
- Інші пристрої в середовищі множинного доступу отримують інформацію про тривалість часу передавання і знають, як довго носій буде недоступним.

Що нового я дізнався у цьому розділ?

Правила

- Протоколи повинні мати відправника та отримувача.
- Поширені комп'ютерні протоколи містять вимоги щодо кодування, форматування, інкапсуляції, розміру, синхронізації та варіантів доставки повідомлень.

Протоколи

- Для надсилання повідомлення через мережу потрібно використовувати декілька протоколів.
- Кожен мережний протокол має власні функції, формат та правила зв'язку.

Стеки протоколів

- Стек протоколів - це група взаємопов'язаних протоколів.
- Стек протоколів TCP/IP - це основний сучасний стек протоколів.

Організації зі стандартизації

- Відкриті стандарти заохочують сумісність, конкуренцію та інновації.

Що нового я дізнався у цьому розділ? (Продовж.)

Еталонні моделі

- Дві моделі, що використовуються в сучасних мережах: TCP/IP та OSI.
- Модель TCP/IP має 4 рівні, а модель OSI - 7 рівнів.

Інкапсуляція даних

- Форма, яку фрагмент даних приймає на певному рівні, називається *протокольним блоком даних (PDU, Protocol data unit)*.
- Існує п'ять різних PDU, які використовуються в процесі інкапсуляції даних: дані, сегмент, пакет, кадр та біти

Доступ до даних

- Мережний та канальний рівні забезпечують адресацію для передавання даних через мережу.
- Мережний рівень забезпечить IP-адресацію, а канальний рівень - MAC-адресацію.
- Відповідь на питання, які операції виконують рівні з адресами залежить від того від того, де знаходяться відправник та отримувач (в одній мережі, чи в різних мережах).

Топології

- В мережах LAN і WAN використовуються два типи топологій, фізичні і логічні.
- Три типи фізичних топологій поширені у WAN: точка-точка, hub and spoke та повнозв'язна.
- Напівдуплексні комунікації обмінюються даними в одному напрямку за раз. Повнодуплексний режим дозволяє відправляти і приймати дані одночасно.
- В мережах множинного доступу з конкурентним доступом всі вузли працюють у напівдуплексному режимі.
- Приклади методів конкурентного доступу: CSMA/CD для шинних топологій локальних мереж Ethernet і CSMA/CA для WLAN

Нові терміни та команди

- Кодування (Encoding)
- Протокол (Protocol)
- Канал (Channel)
- Керування потоком (Flow Control)
- Затримка відповіді (Response Timeout)
- Підтвердження (Acknowledgement)
- Одноадресна розсилка (Unicast)
- Багатоадресна розсилка (Multicast)
- Широкомовна розсилка (Broadcast)
- Стек протоколів (Protocol Suite)
- Ethernet
- Стандарт (Standard)
- Пропрієтарний протокол (Proprietary Protocol)
- 802.3 (Ethernet)
- 802.11 (Wi-Fi)
- Сегментація (Segmentation)
- Шлюз за замовчуванням (Default GateWay)
- Протокол передавання гіпертекстових повідомлень (HTTP, HyperText Transfer Protocol)
- Простий протокол електронної пошти (SMTP, Simple Mail Transfer Protocol)
- Поштовий протокол версії 3 (POP3, Post Office Protocol)
- Протокол керування передаванням (TCP, Transmission Control Protocol)
- Транспортний (Transport)
- Канальний (Data Link)
- Мережний доступ (Network Access)

Нові терміни та команди (Продовж.)

- Мережа Агентства передових дослід-ницьких проектів (ARPANET, Advanced Research Projects Agency Network)
- Протокол доступу до Інтернет-повідомлень (IMAP, Internet Message Access Protocol)
- Протокол передавання файлів (FTP, File Transfer Protocol)
- Простий протокол передавання файлів (TFTP, Trivial File Transfer Protocol)
- Протокол користувацьких датаграм (UDP, User Datagram Protocol)
- Технологія трансляції мережних адрес (NAT, Network Address Translation)
- Протокол міжмережних керуючих повідомлень (ICMP, Internet Control Messaging Protocol)
- Протокол знаходження найкоротшого шляху (OSPF, Open Shortest Path First)
- вдосконалений внутрішньошлюзовий протокол маршрутизації (EIGRP, Enhanced Interior Gateway Routing Protocol)
- Протокол визначення адрес (ARP, Address Resolution Protocol)
- Протокол динамічного налаштування вузла (DHCP, Dynamic Host Configuration)
- Інкапсуляція (Encapsulation
- Деінкапсуляція (De-encapsulation)
- Протокольний блок даних (PDU, Protocol Data Unit)
- Сегмент (Segment)
- Пакет (Packet)
- Кадр(Frame)

Базові налаштування комутатора та кінцевого пристрою

Завдання розділу

Назва розділу: Базові налаштування комутатора та кінцевого пристрою

Мета розділу: Виконання початкових налаштувань, зокрема встановлення паролів, IP-адресації і параметрів шлюзу за замовчуванням на мережному комутаторі та кінцевих пристроях.

Назва теми	Мета вивчення теми
Доступ до Cisco IOS	Пояснити як отримати доступ до пристрою під керуванням Cisco IOS з метою налаштування.
Навігація в IOS	Пояснити як орієнтуватися у Cisco IOS для конфігурування мережних пристроїв.
Структура команд	Описати структуру команд програмного забезпечення Cisco IOS.
Базові налаштування пристрою	Налаштування пристрою під керуванням Cisco IOS за допомогою CLI.
Зберігання налаштувань	Використання команд IOS для зберігання поточних налаштувань.
Порти і адреси	Пояснити, як пристрої взаємодіють у мережному середовищі.
Налаштування IP-адресації	Налаштування IP-адреси на кінцевому пристрої.
Перевірка з'єднання	Перевірка з'єднання між двома кінцевими пристроями.

Доступ до Cisco IOS

Призначення ОС

Операційна система ПК дозволяє користувачеві:

- Використовувати мишу для вибору та запуску програм
- Вводити текст та текстові команди
- Переглядати результат на моніторі

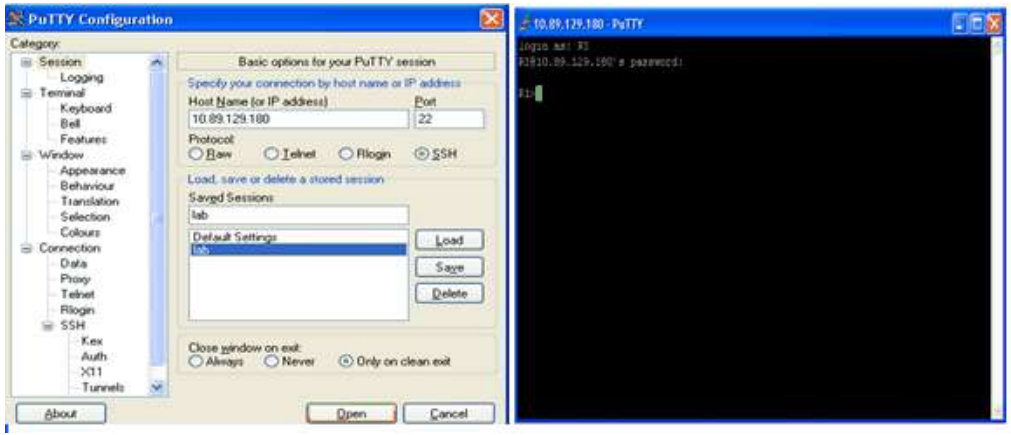
Мережна операційна система на основі CLI дозволяє мережному спеціалісту:

- Використовувати клавіатуру для запуску мережних програм на базі CLI
- Використовувати клавіатуру для введення тексту та текстових команд
- Переглядати результат на моніторі

```
analyst@secOps ~]$ ls
Desktop  Downloads  lab.support.files  second_drive
[analyst@secOps ~]$
```

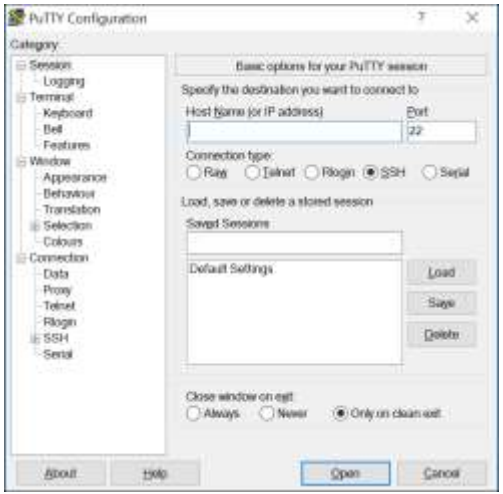
Методи доступу

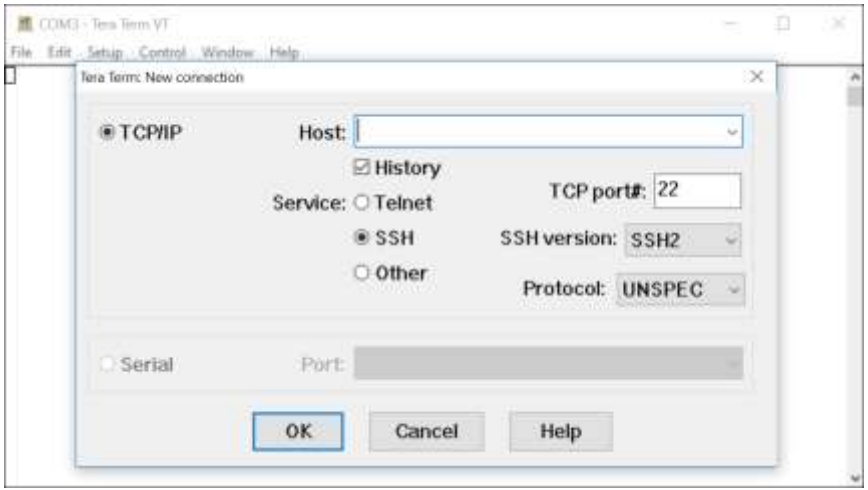
- **Консоль (Console)** – фізичний порт управління, який використовується для доступу до пристрою з метою забезпечення технічного обслуговування, наприклад виконання початкових налаштувань.
- **Безпечна оболонка (SSH - Secure Shell)** – встановлює захищене віддалене з'єднання CLI з пристроєм через віртуальний інтерфейс через мережу. (Примітка. Це рекомендований спосіб дистанційного з'єднання з пристроєм.)
- **Telnet** – встановлює незахищене віддалене під'єднання CLI до пристрою через мережу. (Примітка. Ідентифікація користувача, паролі та команди надсилаються через мережу у вигляді простого тексту.)



Програми емуляції терміналу

- Програми емуляції терміналів використовуються для під'єднання до мережного пристрою або через консольний порт, або через з'єднання SSH/Telnet.
- Існує декілька програм емуляції терміналів, таких як PuTTY, Tera Term та SecureCRT.





Навігація в IOS

Основні командні режими

Користувацький режим EXEC:

- Забезпечує доступ до обмеженої кількості базових команд моніторингу.
- Визначається командним рядком CLI, що закінчується символом >

Привілейований режим EXEC:

- Дозволяє отримати доступ до всіх команд і функцій.
- Визначається командним рядком CLI, що закінчується символом#

Режим конфігурації та підрежими конфігурації

Режим глобальної конфігурації:

- Використовується для доступу до параметрів конфігурації на пристрої

```
Switch(config)#
```

Режим конфігурації лінії:

- Використовується для налаштування доступу до консолі, SSH, Telnet або AUX

```
Switch(config-line)#
```

Режим конфігурації інтерфейсу:

- Використовується для налаштування порту комутатора або інтерфейсу маршрутизатора

```
Switch(config-if)#
```

Навігація між режимами IOS

- **Привілейований режим EXEC:**
  - Щоб перейти з користувацького режиму EXEC в привілейований режим EXEC, використовуйте команду **enable**.

```
Switch> enable
Switch#
```

- **Режим глобальної конфігурації:**
  - Щоб перейти в режим глобальної конфігурації і вийти з нього, використовуйте команду **configure terminal**. Щоб повернутися до привілейованого режиму EXEC використовуйте команду **exit**.

```
Switch(config)#
Switch(config)#exit
Switch#
```

- **Режим конфігурації лінії:**
  - Для входу в режим конфігурації лінії використовуйте команду **line**, а потім тип лінії. Для повернення до режиму глобальної конфігурації використовуйте команду **exit**.

```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```

Навігація між режимами IOS (Продовж.)

Підрежими конфігурації:

- Щоб вийти з будь-якого підрежиму конфігурації та повернутися в режим глобальної конфігурації, використовуйте команду **exit** . Щоб повернутися до привілейованого EXEC режиму використовуйте команду **end** або комбінацію клавіш **Ctrl +Z**.

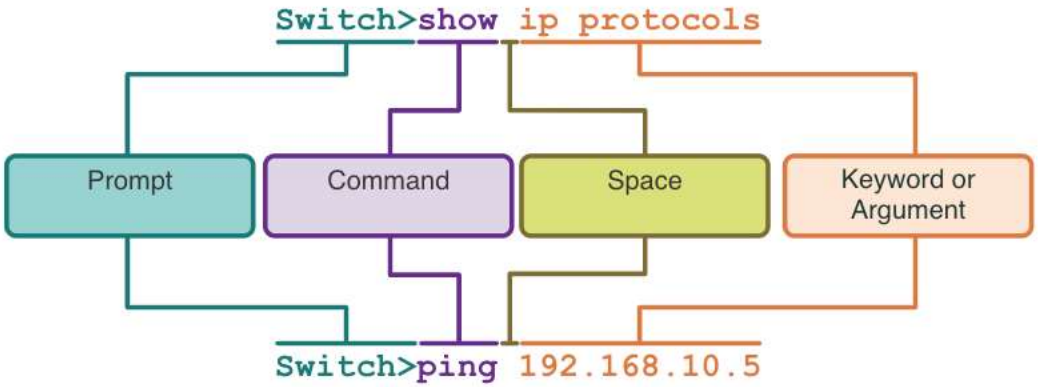
```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

- Щоб перейти безпосередньо з одного підрежиму конфігурації в інший, введіть потрібну команду підрежиму конфігурації. У прикладі, командний рядок змінюється з **(config-line)#** на **(config-if)#**.

```
Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```

Структура команд

Базова структура команд IOS



- **Ключове слово (Keyword)** – це особливий параметр, визначений в операційній системі (на рисунку, **ip protocols**).
- **Аргумент (Argument)** - не заданий заздалегідь, це значення або змінну визначає користувач (на рисунку, **192.168.10.5**).

Перевірка синтаксису команд IOS

Команда може вимагати одного або декількох аргументів. Щоб визначити ключові слова та аргументи, необхідні для команди, зверніться до синтаксису команд.

- Напівжирним шрифтом показано команди та ключові слова, що вводяться.
- Курсивом виділено аргумент, значення якого надає користувач.

Умовне позначення	Опис
напівжирний	Команди і ключові слова, які вводяться, відображаються напівжирним шрифтом, як показано на рисунку.
курсив	Курсивом відображаються аргументи, для яких потрібно вказати значення.
[x]	В квадратних дужках відображаються додаткові елементи (ключове слово або аргумент).
{x}	У фігурних дужках вказується необхідний елемент, такий як ключове слово або аргумент.
[x {y | z }]	Фігурні дужки і вертикальні лінії у квадратних дужках вказують на те, що необхідно обрати додатковий елемент. Пробіли використовуються для чіткого розмежування частин команди.

Перевірка синтаксису команд IOS (Продовж.)

- Командний синтаксис визначає шаблон або формат, який необхідно використовувати при введенні команди.

- Команда - це **ping** , а аргумент, визначений користувачем, IP-адреса вузла призначення *ip-address* . Наприклад, **ping 10.10.10.5**.

```
ping ip-address
```

- Команда - це **traceroute** , а аргумент, визначений користувачем, IP-адреса вузла призначення *ip-address* . Наприклад, **traceroute 192.168.254.254**.

```
traceroute ip-address
```

- Якщо команда складна з декількома аргументами, її можна представити таким чином:

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

Функції довідки IOS

У IOS доступні дві форми допомоги: контекстна довідка та перевірка синтаксису команд.

- Контекстна довідка дозволяє швидко знайти відповіді на такі питання:
  - Які команди доступні в кожному режимі команд?
  - Які команди починаються з конкретних символів або групи символів?
  - Які аргументи та ключові слова доступні для певних команд?

```
Router#ping ?
  WORD  Ping destination address or hostname
  ip    IP echo
  ipv6  IPv6 echo
```

- Перевірка синтаксису команд підтверджує, що користувачем було введено діючу команду.
  - Якщо інтерпретатор не може зрозуміти введену команду, він надасть зворотній зв'язок із описом того, що з командою не так.

```
Switch#interface fastEthernet 0/1
                ^
% Invalid input detected at '^' marker.
```

Гарячі клавіші та ярлики

- CLI в IOS підтримує використання гарячих клавіш та ярликів, які спрощують налаштування, моніторинг та усунення несправностей.
- Команди та ключові слова можна скоротити до мінімальної кількості символів, що ідентифікують унікальний вибір. Наприклад, команду **configure** можна скоротити до **conf** оскільки **configure** є єдиною командою, яка починається з **conf**.

```
Router#con
% Ambiguous command: "con"
Router#con?
configure  connect
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Гарячі клавіші та ярлики (Продовж.)

- У таблиці нижче наведено короткий перелік комбінацій клавіш для вдосконалення редагування командного рядка.

Комбінація клавіш	Опис
Tab	Завершує частковий запис команди.
Backspace	Стирає символ зліва від курсору.
Стрілка ліворуч або **Ctrl+B**	Переміщує курсор на один символ ліворуч.
Стрілка праворуч або **Ctrl+F**	Переміщує курсор на один символ праворуч.
Стрілка вгору або **Ctrl+P**	Повторює команду в буфері історії, починаючи з останніх команд.

Гарячі клавіші та ярлики (Продовж.)

- Коли результат виконання команди повертає більше тексту, ніж можна відобразити у вікні терміналу, IOS відобразить підказку **“--More--”** . У таблиці нижче описано комбінації клавіш, які можна використовувати в такому випадку.

Комбінація клавіш	Опис
Клавіша **Enter**	Показує наступний рядок.
Клавіша **Пробіл**	Відображає наступний екран.
Будь-яка інша клавіша	Закінчує рядок, повертаючись у привілейований режим EXEC.

- У таблиці нижче наведені команди, які можна використовувати для виходу з операції.

Комбінація клавіш	Опис
Ctrl-C	У будь-якому режимі конфігурації завершує цей режим та повертається у привілейований режим EXEC.
Ctrl-Z	У будь-якому режимі конфігурації завершує цей режим та повертається у привілейований режим EXEC.
Ctrl-Shift-6	Універсальна послідовність для переривань, яка використовується для припинення пошуку DNS-каналів, трасування, пінгування, тощо.

Примітка: Щоб побачити більше гарячих клавіш та ярликів, див. 2.3.5.

Гарячі клавіші та ярлики

охоплено наступне:

- Клавіша Tab (завершення клавішею tab)
- Скорочення команд
- Клавіші стрілок вгору і вниз
- CTRL + C
- CTRL + Z
- CTRL + Shift + 6
- CTRL + R

Базові налаштування пристрою

Імена пристроїв

- Першою командою налаштування на будь-якому пристрої має бути присвоєння йому унікального імені вузла.
- За замовчуванням, всім пристроям присвоєне заводське ім'я за замовчуванням. Наприклад, у комутатора Cisco IOS ім'я "Switch.”
- Правило іменування пристроїв:
  - починати імена з літери
  - не використовувати пробіли
  - закінчувати літерою або цифрою
  - використовувати лише літери, цифри і тире
  - мати довжину не більше 64 символів

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Примітка: Щоб повернути комутатору ім'я за замовчуванням, використовуйте команду **no hostname** режиму глобальної конфігурації.

Правила вибору паролів

- Використання слабких або легко вгадуваних паролів шкодить безпеці.
- Усі мережні пристрої повинні обмежувати адміністративний доступ, встановлюючи захищений паролями доступ до привілейованого EXEC та користувацького EXEC режимів, віддаленого доступу до Telnet. Крім того, всі паролі повинні бути зашифровані, та встановлене сповіщення про обмеження доступу.
- Правила вибору паролів:
  - Використовуйте паролі довжиною більше восьми символів.
  - Використовуйте комбінацію великих і малих літер, цифр, спеціальних символів та/або числових послідовностей.
  - Уникайте використання однакового пароля для всіх пристроїв.
  - Не вживайте загальних слів, тому що їх легко вгадати.

Примітка: В більшості лабораторних робіт цього курсу використовують прості паролі, такі як **cisco** чи **class**. Ці паролі вважаються слабкими і легко вгадуваними, тому їх слід уникати у виробничих умовах.

Налаштування паролів

Захист доступу до користувацького режиму EXEC:

- Спочатку увійдіть в режим конфігурації лінії консолі, використовуючи команду **line console 0** в режимі глобальної конфігурації.
- Далі, встановіть пароль користувацького режиму EXEC, використовуючи команду **password** *password* .
- Нарешті, активуйте доступ до користувацького режиму EXEC, використовуючи команду **login** .

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Захист доступу до привілейованого режиму EXEC:

- Спочатку увійдіть до режиму глобальної конфігурації.
- Далі, використовуйте команду **enable secret** *password* .

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Налаштування паролів (Продовж.)

Захист доступу до лінії віртуального терміналу (VTY line):

- Спочатку увійдіть в режим конфігурації лінії віртуального терміналу, використовуючи команду **line vty 0 15** в режимі глобальної конфігурації.
- Далі, встановіть пароль для VTY, використовуючи команду **password** *password* .
- Нарешті, активуйте доступ до VTY, використовуючи команду **login** .

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

- Примітка: лінії віртуального інтерфейсу VTY дозволяють віддалений доступ до пристрою за допомогою Telnet або SSH. Багато комутаторів Cisco підтримують до 16 ліній VTY, які пронумеровані від 0 до 15.

Шифрування паролів

- Файли startup-config та running-config відображають більшість паролів у форматі відкритого тексту.
- Щоб зашифрувати усі відкриті паролі у цих файлах, скористайтеся командою **service password-encryption** в режимі глобальної конфігурації.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

- Використовуйте команду **show running-config** , щоб перевірити, чи зашифровані тепер паролі на пристрої.

```
Sw-Floor-1# show running-config
!

!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```

Банерне повідомлення

- Банерне повідомлення застерігає неуповноважений персонал від спроб отримати доступ до пристрою.
- Щоб створити банерне повідомлення дня на мережному пристрої, використовуйте команду **banner motd** *# the message of the day #* в режимі глобальної конфігурації.

Примітка: Символ"#" у синтаксисі команд називається символом розмежування. Він вводиться до і після повідомлення.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

Банер буде відображатися при спробах доступу до пристрою.

```
Press RETURN to get started.



Authorized Access Only!

User Access Verification

Password:
```

Зберігання налаштувань

Файли конфігурації

- Є два системні файли, в яких зберігаються конфігурації пристрою:
  - **startup-config** - Це файл стартової конфігурації, який зберігається в NVRAM. Він містить усі команди, які будуть використовуватися пристроєм при запуску або перезавантаженні. Флеш-накопичувач не втрачає свого вмісту, коли пристрій вимкнено.
  - **running-config** - Це файл поточної конфігурації, який зберігається в оперативній пам'яті (RAM). В ньому відображена поточна конфігурація. Зміна поточної конфігурації негайно впливає на роботу пристрою Cisco. Оперативна пам'ять (RAM) - енергозалежна пам'ять. Вона втрачає весь свій вміст при вимкненні або перезавантаженні пристрою.
  - Для збереження у файл стартової конфігурації змін, внесених до поточної конфігурації, використовуйте команду **copy running-config startup-config** привілейованого режиму EXEC.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

```
Router#show running-config
Building configuration...

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

Зміна поточної конфігурації

Якщо зміни, внесені до поточної конфігурації, не мають потрібного ефекту, а running-config ще не збережений, ви можете відновити налаштування пристрою до його попередньої конфігурації. Для цього ви можете:

- Видалити змінені команди окремо.
- Перезавантажити пристрій за допомогою команди **reload** у привілейованому режимі EXEC. *Примітка: Це призведе до того, що пристрій ненадовго вийде в режим оффлайн, що призведе до простою мережі.*

```
Router# reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

Якщо небажані зміни були збережені в startup-config, можливо, доведеться очистити всі налаштування, використовуючи команду **erase startup-config** в привілейованому режимі EXEC.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

- Після стирання startup-config перезавантажте пристрій, щоб очистити файл поточної конфігурації в оперативній пам'яті.

Зміна поточної конфігурації

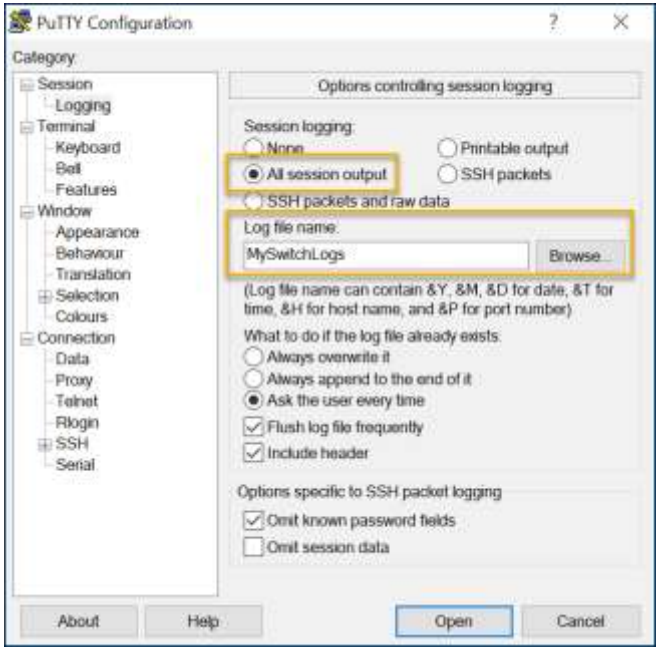
В цьому відео охоплено наступне:

- Копіювання файлу поточної конфігурації running-config у файл стартової конфігурації startup-config
- Перегляд файлів у каталозі flash або NVRAM
- Використання скорочення команд
- Стирання конфігураційного файлу запуску startup-config
- Копіювання файлу стартової конфігурації start-config у файл поточної конфігурації running-config

Захоплення конфігурації у текстовий файл

Файли конфігурації також можна зберігати та архівувати у текстовий документ.

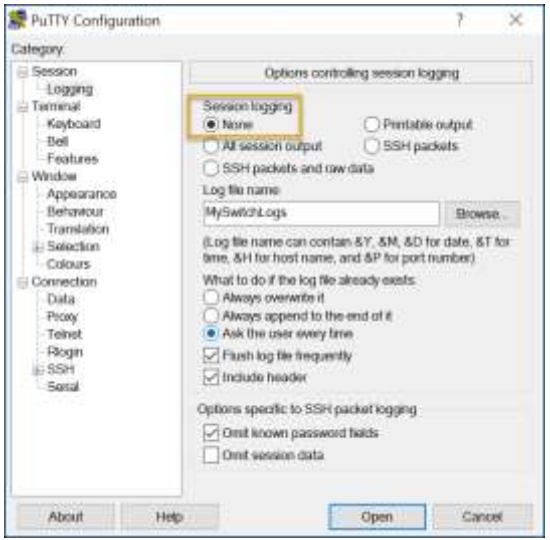
- **Крок 1.** Відкрийте програмне забезпечення для емуляції терміналів, наприклад PuTTY або Tera Term, яке вже підключено до комутатора.
- **Крок 2.** Активуйте ведення журналу терміналу та вкажіть ім’я та місце розташування для збереження файлу журналу (log file). На рисунку показано, що **All session output** буде захоплено у визначений файл (т.з., MySwitchLogs).



Захоплення конфігурації у текстовий файл (Продовж.)

- **Крок 3.** Введіть команду **show running-config** або **show startup-config** в привілейованому режимі EXEC. Текст, що відображається у вікні терміналу, буде розміщений у вибраному файлі.
- **Крок 4.** Відключіть ведення журналу в програмі терміналу. На рисунку показано, як відключити ведення журналу, вибираючи параметр **None**

```
Switch# show running-config
Building configuration...
```

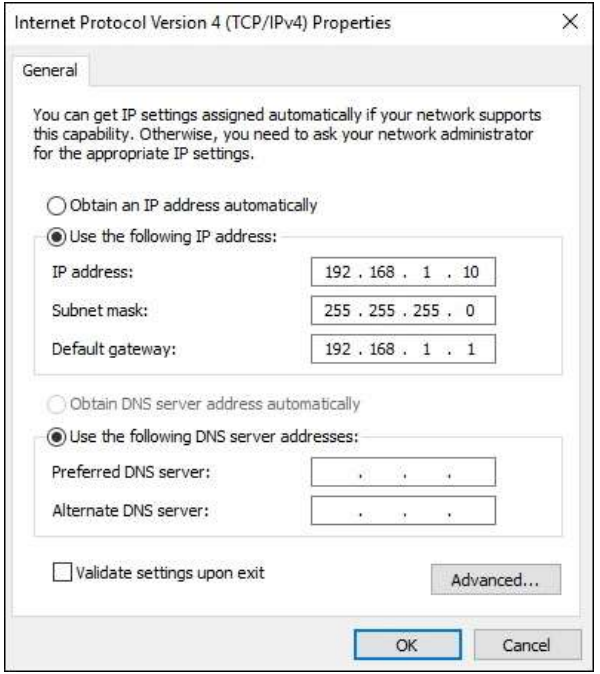


Примітка: Створений текстовий файл може використовуватися як запис про поточне застосування пристрою. Можливо, файл потрібно буде редагувати, перш ніж використовувати для відновлення збереженої конфігурації на пристрої.

Порти і адреси

IP-адреси

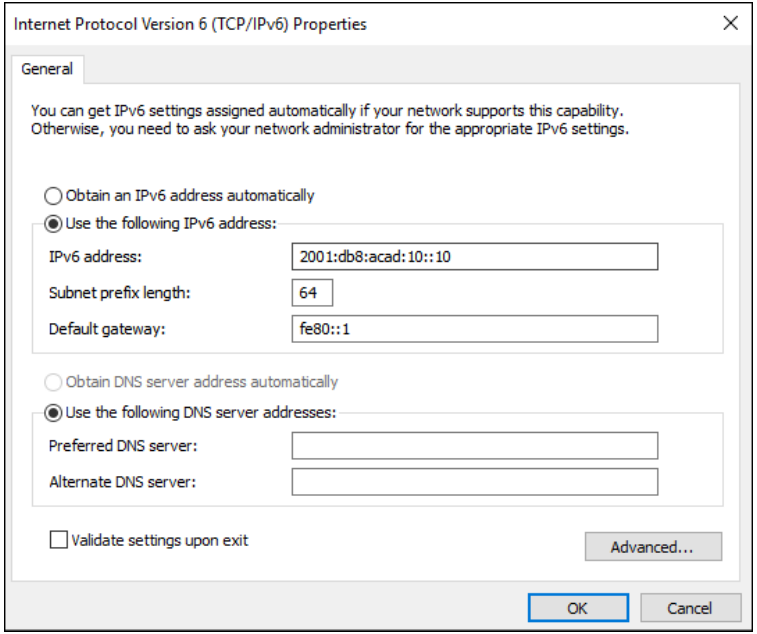
- Використання IP-адрес є основним засобом, що дозволяє пристроям знаходити один одного та встановлювати наскрізне з'єднання в Інтернеті.
- Структура адреси IPv4 називається крапково-десятковим позначенням і представлена чотирма десятковими числами від 0 до 255.
- Маска підмережі IPv4 - це 32-бітове значення, яке відокремлює мережну частину адреси від вузлової частини. У поєднанні з IPv4-адресою маска підмережі визначає, до якої підмережі належить пристрій.
- Адреса шлюзу за замовчуванням - це IP-адреса маршрутизатора, яку вузол використовуватиме для доступу до віддалених мереж, включаючи Інтернет.



IP-адреси (Продовж.)

- Адреси IPv6 мають довжину 128 бітів і записуються у вигляді рядка шістнадцяткових значень. Кожні чотири біти представлені однією шістнадцятковою цифрою; загалом 32 шістнадцяткові цифри. Групи з чотирьох шістнадцяткових цифр розділені двокрапкою “:”.
- IPv6 адреси не чутливі до регістру і можуть бути записані як в нижньому регістрі, так і у верхньому.

Примітка: Термін IP в цьому курсі використовується, коли мова йде про обидва протоколи: IPv4 та IPv6. IPv6 - це найновіша версія IP, яка замінює поширений зараз IPv4.



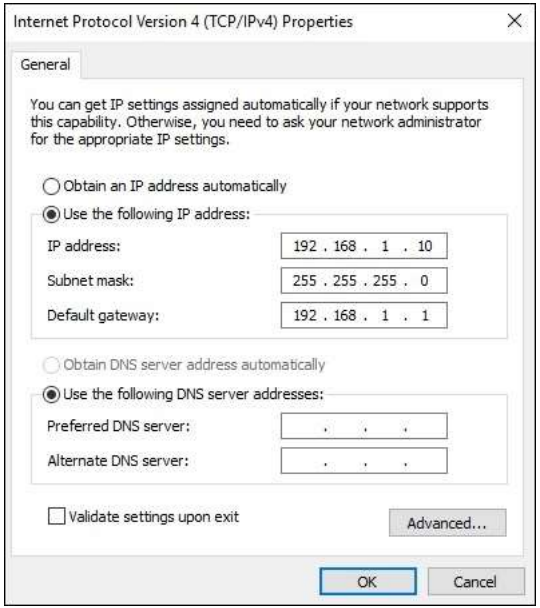
Інтерфейси і порти

- Мережний зв'язок залежить від інтерфейсу пристрою кінцевого користувача, інтерфейсів мережних пристроїв та кабелів, що їх з'єднують.
- Типи мережних носіїв включають кабелі мідної витої пари, волоконно-оптичні кабелі, коаксіальні кабелі або бездротові середовища.
- Різні типи мережних носіїв мають різні особливості та переваги. Деякі з відмінностей між різними видами середовищ передавання включають:
  - Відстань, на яку носій може успішно передавати сигнал
  - Середовище, у якому потрібно прокласти носій
  - Кількість даних і швидкість, з якою їх потрібно передати
  - Вартість носія та його прокладання

Налаштування IP-адресації

Ручне налаштування IP-адресації на кінцевому пристрої

- Кінцеві пристрої для зв'язку з іншими пристроями в мережі потребують IP-адреси.
- Інформацію про адресу IPv4 можна вводити на кінцевих пристроях вручну або автоматично, використовуючи протокол динамічної конфігурації вузла (DHCP - Dynamic Host Configuration Protocol).
  - Щоб вручну налаштувати IPv4-адресу на ПК з Windows, відкрийте вікно панелі управління **Control Panel > Network Sharing Center > Change adapter settings** і виберіть адаптер. Далі натисніть ПКМ і виберіть **Properties** , щоб відкрити вікно властивостей **Local Area Connection Properties**.
  - Далі натисніть **Properties** , щоб відкрити вікно властивостей TCP/IP **Internet Protocol Version 4 (TCP/IPv4) Properties** . Потім налаштуйте інформацію про адресу IPv4, маску підмережі та шлюз за замовчуванням.



Примітка: Для IPv6 адресація та налаштування схожі на IPv4.

Автоматичне налаштування IP-адресації на кінцевому пристрої

- Протокол DHCP робить можливою автоматичну конфігурацію адреси IPv4 для кожного кінцевого пристрою, що підтримує DHCP.
- Кінцеві пристрої зазвичай за замовчуванням використовують DHCP для автоматичного налаштування адреси IPv4.
  - Щоб автоматично налаштувати DHCP на ПК з Windows, відкрийте вікно панелі управління **Control Panel > Network Sharing Center > Change adapter settings** і виберіть адаптер. Далі натисніть ПКМ і виберіть **Properties** , щоб відкрити вікно властивостей **Local Area Connection Properties**.
  - Далі натисніть **Properties** , щоб відкрити вікно властивостей TCP/IP **Internet Protocol Version 4 (TCP/IPv4) Properties** і виберіть **Obtain an IP address automatically** та **Obtain DNS server address automatically**.

Примітка: Для динамічного розподілу адрес IPv6 використовує DHCPv6 та SLAAC (Stateless Address Autoconfiguration).

Налаштування віртуального інтерфейсу комутатора

Щоб отримати віддалений доступ до комутатора, на SVI повинні бути налаштовані IP-адреса та маска підмережі.

Щоб налаштувати SVI на комутаторі потрібно:

- Ввести команду **interface vlan 1** в режимі глобальної конфігурації.
- Далі призначити IPv4 адресу за допомогою команди **ip address** *, що встановлює IP-адресу та маску підмережі.*
- Нарешті, увімкнути віртуальний інтерфейс за допомогою команди **no shutdown**.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

Перевірка з'єднання

Тестування призначень інтерфейсу

охоплено наступне:

- Під'єднання консольного кабелю від ПК до комутатора
- Використання програми емуляції терміналу та прийняття типових параметрів для переходу до командного рядка
- Використання enable для входу в привілейований режим EXEC.
- Введення команди no shutdown в режимі глобальної конфігурації та режимі конфігурації інтерфейсу

Базові налаштування комутатора та кінцевого пристрою

потрібно виконати наступне:

- Налаштувати імена та IP-адреси на двох комутаторах
- Використати команди Cisco IOS для надання або обмеження доступу до конфігурацій пристрою
- Використати команди IOS для зберігання поточних налаштувань
- Налаштувати IP-адреси на двох кінцевих пристроях
- Перевірити зв'язок між двома кінцевими пристроями

Що ми вивчили?

- Усі кінцеві пристрої та мережні пристрої потребують операційної системи (ОС).
- Програмне забезпечення Cisco IOS розділяє доступ до керування на наступні два режими команд: Користувацький режим EXEC та Привілейований режим EXEC.
- Режим глобальної конфігурації доступний перед іншими спеціальними режимами конфігурації. З режиму глобальної конфігурації користувач може перейти в різні підрежими конфігурації.
- Кожна команда IOS має певний формат або синтаксис і може виконуватися лише у відповідному режимі.
- Основні налаштування пристрою - ім'я вузла, пароль, шифрування паролів та банер.
- Є два системні файли, в яких зберігаються конфігурації пристрою: startup-config та running-config.
- IP-адреси дозволяють пристроям знаходити один одного та встановлювати наскрізне з'єднання в Інтернеті. Кожен кінцевий пристрій в мережі повинен бути налаштований з IP-адресою.

Базові налаштування маршрутизатора

Завдання

Мета : Виконання початкових налаштувань на маршрутизаторі та кінцевих пристроях.

Назва теми	Мета вивчення теми
Налаштування початкових параметрів маршрутизатора	Налаштувати початкові параметри на маршрутизаторі під керуванням Cisco IOS
Налаштування інтерфейсів	Налаштувати два активніінтерфейси на маршрутизаторі під керуванням Cisco IOS.
Налаштування шлюзу за замовчуванням	Налаштувати пристрої на використання шлюзу за замовчуванням.

Налаштування початкових параметрів маршрутизатора

Етапи базового налаштування маршрутизатора

- Налаштуйте назву пристрою.
- Захистіть доступ до привілейованого режиму EXEC.
- Захистіть доступ до користувацького режиму EXEC.
- Захистіть віддалений доступ до Telnet / SSH.
- Зашифруйте всі відкриті паролі.
- Налаштуйте попередження і збережіть конфігурацію.

```
Router(config)# hostname hostname
```

```
Router(config)# enable secret password
```

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
```

```
Router(config)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# transport input {ssh | telnet}
```

```
Router(config)# service password encryption
```

```
Router(config)# banner motd # message #
Router(config)# end
Router# copy running-config startup-config
```

Приклад базового налаштування маршрутизатора

- Команди для базового налаштування маршрутизатора R1.
- Конфігурація зберігається в NVRAM.

```
R1(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
**********************************************
WARNING: Unauthorized access is prohibited!
**********************************************
R1(config)# exit
R1# copy running-config startup-config
```

Packet Tracer – Налаштування початкових параметрів маршрутизатора

потрібно виконати:

- Перевірку конфігурації за замовчуванням маршрутизатора.
- Налаштуваня та перевірку початкової конфігурації маршрутизатора.
- Збереження файлу поточної конфігурації.

Налаштування інтерфейсів

Налаштування інтерфейсів маршрутизатора

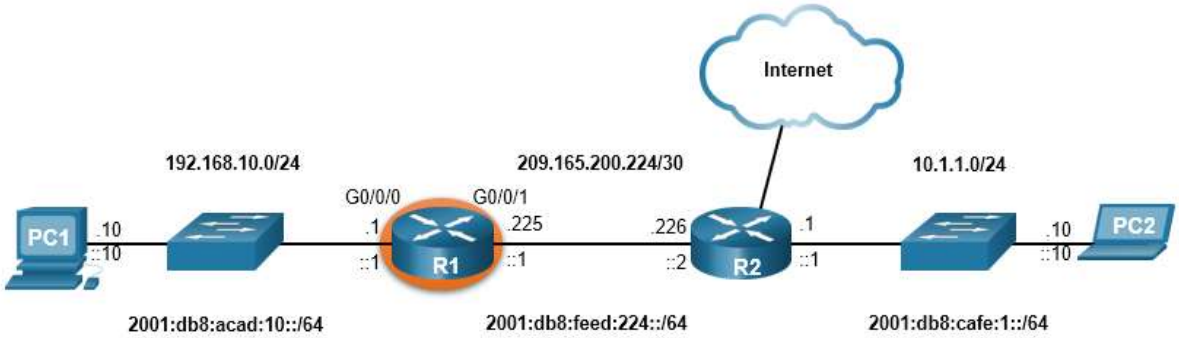
Налаштування інтерфейсу маршрутизатора передбачає введення таких команд:

```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# ipv6 address ipv6-address/prefix-length
Router(config-if)# no shutdown
```

- Гарною практикою вважається використання команди **description** для додавання інформації про мережу, під'єднану до інтерфейсу.
- Команда **no shutdown** активує інтерфейс.

Приклад налаштування інтерфейсів маршрутизатора

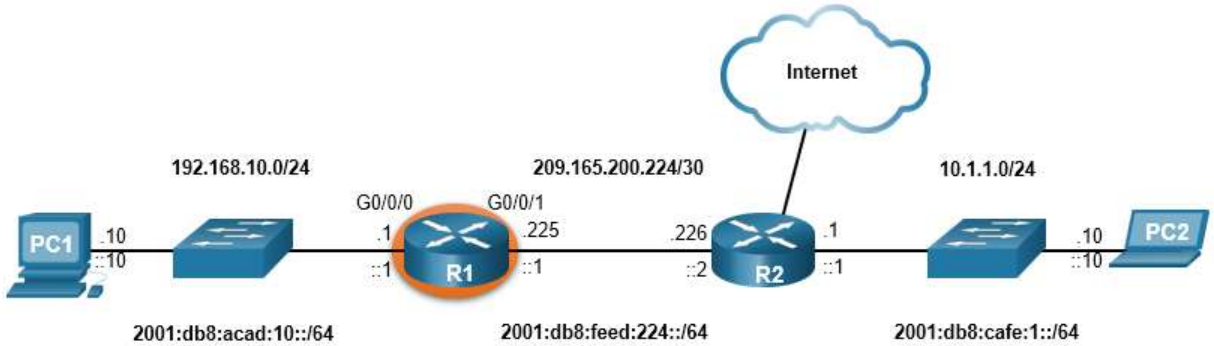
Для налаштування інтерфейсу G0/0/0 на маршрутизаторі R1 слід використати такі команди:




```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:10::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug 1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Aug 1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Aug 1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed
state to up
```

Приклад налаштування інтерфейсів маршрутизатора (Продовж.)

Для налаштування інтерфейсу G0/0/1 на маршрутизаторі R1 слід застосувати такі команди:




```
R1(config)# interface gigabitEthernet 0/0/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:feed:224::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug 1 01:46:29.170: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Aug 1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Aug 1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed
state to up
```

Перевірка налаштувань інтерфейсу

Для перевірки конфігурації інтерфейсу використовуйте команди **show ip interface brief** та **show ipv6 interface brief** , як показано нижче:

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 192.168.10.1 YES manual up up
GigabitEthernet0/0/1 209.165.200.225 YES manual up up
Vlan1 unassigned YES unset administratively down down
```

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1 [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1 [administratively down/down]
    unassigned
R1#
```

Команди для перевірки налаштувань

У таблиці наведено найпоширеніші команди, які використовуються для перевірки конфігурації інтерфейсу.

Команди	Опис
`show ip interface brief` `show ipv6 interface brief`	Відображають усі інтерфейси, їх IP-адреси та поточний стан.
`show ip route` `show ipv6 route`	Відображають вміст таблиць IP-маршрутизації, що зберігаються в оперативній пам'яті RAM.
`show interfaces`	Відображає статистику для всіх інтерфейсів пристрою, а також інформацію про адресацію IPv4.
`show ip interfaces`	Відображає статистику IPv4 для усіх інтерфейсів маршрутизатора.
`show ipv6 interfaces`	Відображає статистику IPv6 для усіх інтерфейсів маршрутизатора.

Команди для перевірки налаштувань (Продовж.)

Приклади застосування команд **show ip interface brief** та **show ipv6 interface brief** для перегляду стану інтерфейсів, подано нижче:

```
R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 192.168.10.1 YES manual up up
GigabitEthernet0/0/1 209.165.200.225 YES manual up up
Vlan1 unassigned YES unset administratively down down
R1#
```

```
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1 [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1 [administratively down/down]
    unassigned
R1#
```

Команди для перевірки налаштувань (Продовж.)

Вивід вмісту таблиць IP-маршрутизації за допомогою команд **show ip route** та **show ipv6 route**, як показано далі:

```
R1# show ip route
< output omitted>
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

```
R1# show ipv6 route
<output omitted>
C 2001:DB8:ACAD:10::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:10::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C 2001:DB8:FEED:224::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L 2001:DB8:FEED:224::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
L FF00::/8 [0/0]
     via Null0, receive
R1#
```

Команди для перевірки налаштувань (Продовж.)

Відображення статистики для усіх інтерфейсів за допомогою команди **show interfaces**:

```
R1# show interfaces gig0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia a0e0.af0d.e140)
  Description: Link to LAN
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:35, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1180 packets input, 109486 bytes, 0 no buffer
     Received 84 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles

<output omitted>

R1#
```

Команди для перевірки налаштувань (Продовж.)

Відображення статистики IPv4 для інтерфейсів маршрутизатора за допомогою команди **show ip interface**:

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled

<output omitted>

R1#
```

Команди для перевірки налаштувань (Продовж.)

Одержання статистики IPv6 для інтерфейсів маршрутизатора за допомогою команди **show ipv6 interface**:

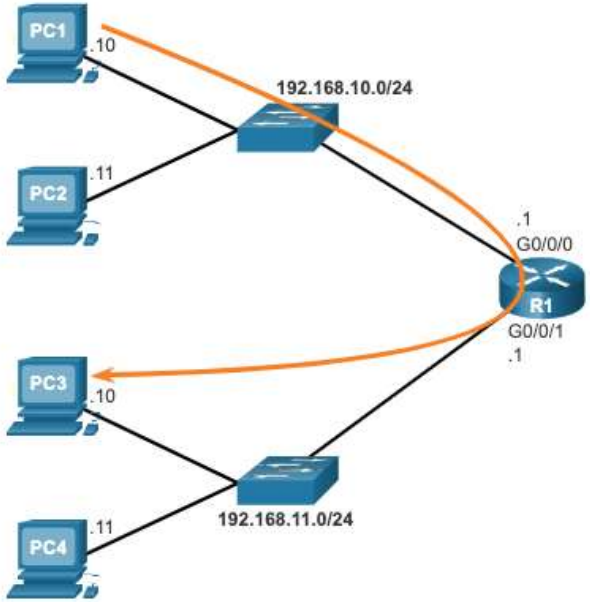
```
R1# show ipv6 interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::868A:8DFF:FE44:49B0
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:10::1, subnet is 2001:DB8:ACAD:10::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF44:49B0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds

R1#
```

Налаштування шлюзу за замовчуванням

Шлюз за замовчуванням на хості

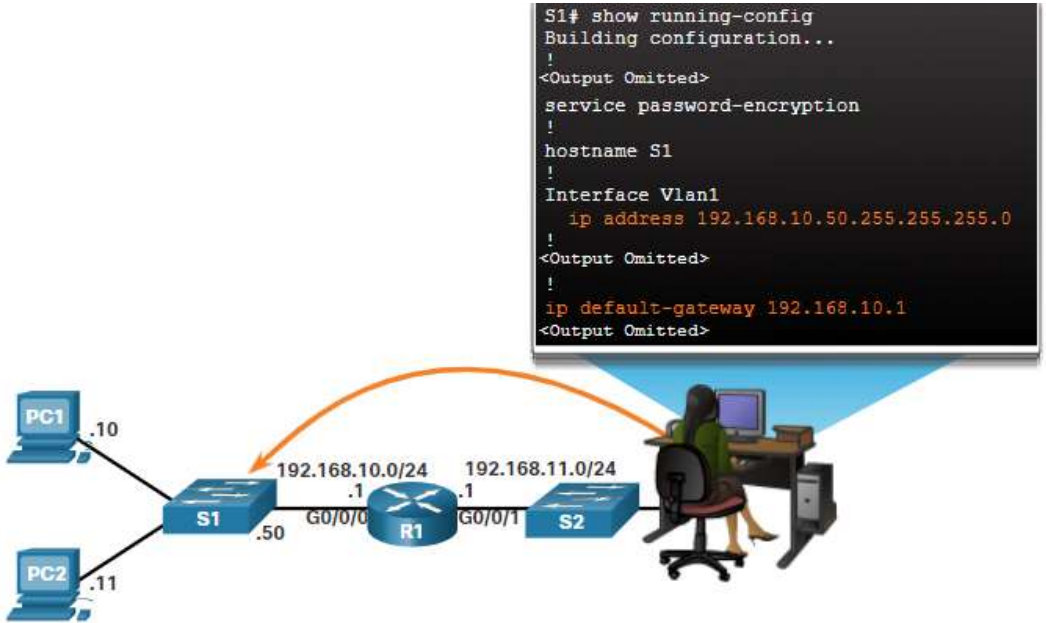
- Шлюз за замовчуванням використовується, коли хост надсилає пакет до пристрою з іншої мережі.
- Адреса шлюзу за замовчуванням - це, як правило, адреса інтерфейсу маршрутизатора, до якого під'єднано локальну мережу хоста.
- Щоб дістатися до PC3, PC1 спрямовує пакет за адресою IPv4 PC3, але пересилає пакет на свій шлюз за замовчуванням - інтерфейс G0/0/0 маршрутизатора R1.



Примітка: IP-адреса хоста та інтерфейс маршрутизатора повинні належати одній мережі.

Шлюз за замовчуванням на комутаторі

- Для віддаленого керування комутатором з іншої мережі на ньому потрібно налаштувати адресу шлюзу за замовчуванням.
- Щоб налаштувати шлюз за замовчуванням IPv4 на комутаторі, використовуйте команду режиму глобальної конфігурації **ip default-gateway** *ip-address*.



Під'єднання маршрутизатора до локальної мережі

виконати наступне:

- Відобразити інформацію про маршрутизатор.
- Налаштувати інтерфейси маршрутизатора.
- Перевірити конфігурацію.

Що ми вивчили?

- Завдання, які слід виконати під час початкового налаштування маршрутизатора.
  - Налаштування назви пристрою.
  - Захист доступу до привілейованого режиму EXEC.
  - Захист доступу до користувацького режиму EXEC.
  - Захист віддаленого доступу до Telnet / SSH.
  - Захист усіх паролів у конфігураційному файлі.
  - Налаштування попередження.
  - Збереження конфігурації.
- Для того, щоб мати доступ до маршрутизаторів, необхідно налаштувати їх інтерфейси.
  - Команда **no shutdown** використовується для активації інтерфейсу. Окрім того, інтерфейс повинен бути під'єднаний до іншого пристрою, наприклад, комутатора або маршрутизатора, для забезпечення активності на фізичному рівні. Існує низка команд, які можуть бути використані для перевірки конфігурації інтерфейсу: **show ip interface brief** та **show ipv6 interface brief**, **show ip route** та **show ipv6 route**, а також **show interfaces**, **show ip interface** та **show ipv6 interface.**

Що ми вивчили (Продовж.)?

- Для того, щоб кінцевий пристрій мав доступ до інших мереж, на ньому потрібно налаштувати шлюз за замовчуванням.
  - IP-адреса хоста та адреса інтерфейсу маршрутизатора повинні перебувати в одній мережі.
- Для віддаленого керування комутатором з іншої мережі на ньому потрібно налаштувати адресу шлюзу за замовчуванням.
  - Щоб налаштувати шлюз за замовчуванням IPv4 на комутаторі, використовуйте команду режиму глобальної конфігурації **ip default-gateway** *ip-address*.

Нові терміни та команди

- **show ip interface brief**
- **show ipv6 interface brief**
- **show ip route**
- **show ipv6 route**
- **show interfaces**
- **show ip interface**
- **show ipv6 interface**
- **ip default-gateway**