Тема3. Протоколи та моделі

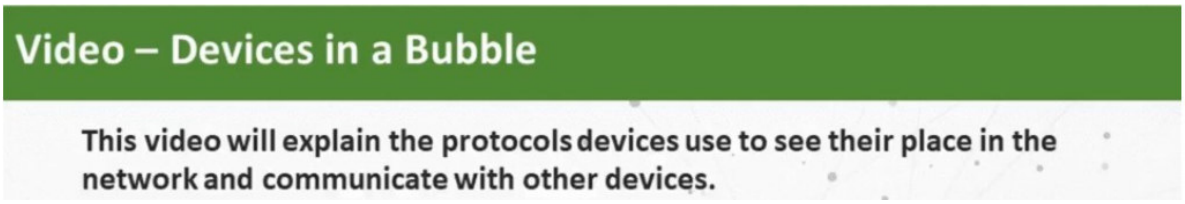
Вам вже знайомі основні компоненти простої мережі, а також процедури їх початкової конфігурації. Але після того, як ви налаштували та підключили ці компоненти, як ви дізнаєтесь, що вони працюватимуть разом? Вам допоможуть протоколи! Протоколи - це сукупності узгоджених правил, створених організаціями зі стандартизації. Але оскільки ви не маєте можливості взяти правило і уважно проаналізувати його, виникає питання: "Як ви справді зрозумієте, чому таке правило існує і що воно повинно робити?" Вам допоможуть моделі! Моделі дають змогу візуалізувати правила та їх місце у вашій мережі. Цей модуль містить огляд мережних протоколів та моделей. Ви маєте можливість набагато глибше зрозуміти, як насправді працюють мережі!

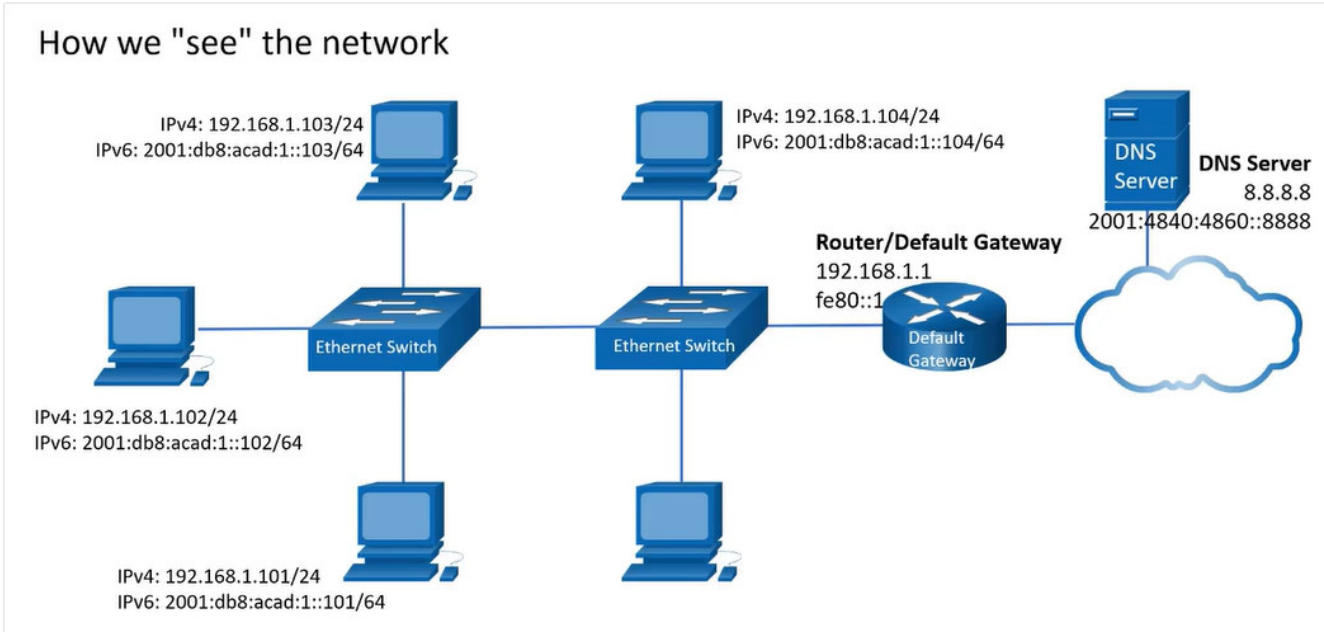
Мета розділу: Пояснити, як мережні протоколи дозволяють пристроям отримувати доступ до локальних і віддалених мережних ресурсів.

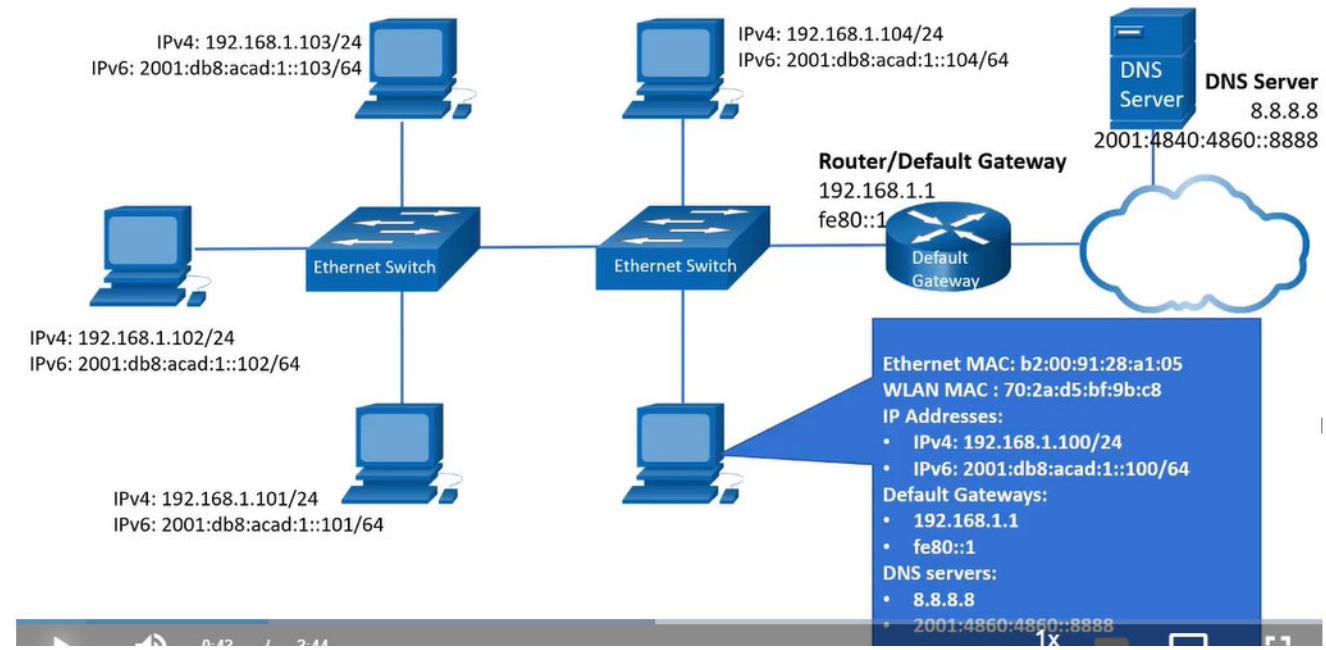
Заголовок таблиці	
Назва теми	**Мета вивчення теми**
3.1. Правила	Описати типи правил, яких необхідно дотримуватися для успішного передавання даних.
3.2. Протоколи	Пояснити, чому для мережної взаємодії потрібні протоколи.
3.3. Стеки протоколів	Пояснити мету дотримання вимог стеку протоколів.
3.4. Організації зі стандартизації	Пояснити роль організацій зі стандартизації при створенні протоколів для забезпечення мережної сумісності.
3.5. Еталонні моделі	Пояснити як моделі TCP/IP і OSI використовуються для полегшення стандартизації процесу передавання даних.
3.6. Інкапсуляція даних	Пояснити як інкапсуляція забезпечує передавання даних по мережі.
3.7. Доступ до даних	Пояснити як локальні хости одержують доступ до локальних ресурсів у мережі.

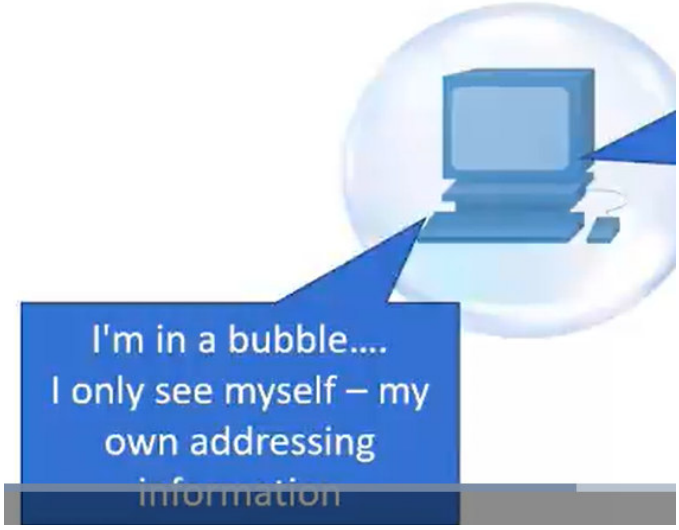
3.1. Правила

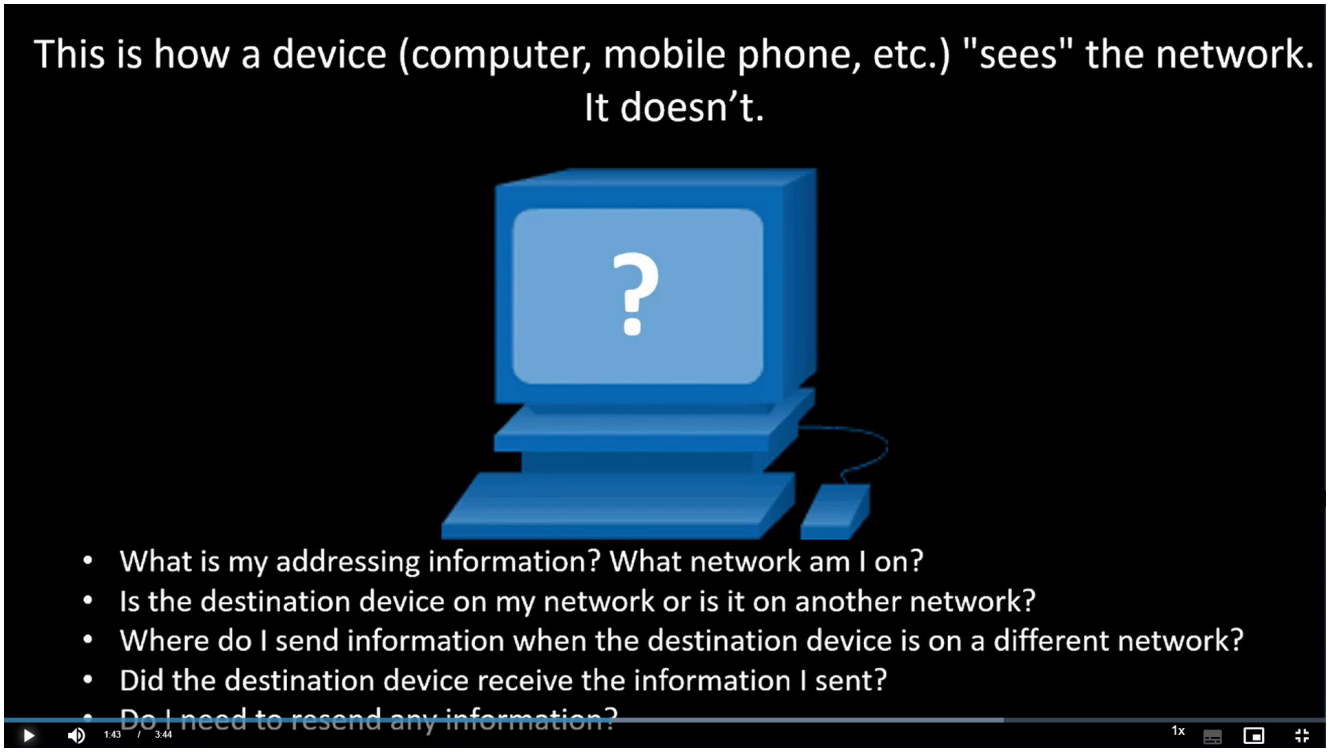
3.1.1. Пристрої в бульбашці

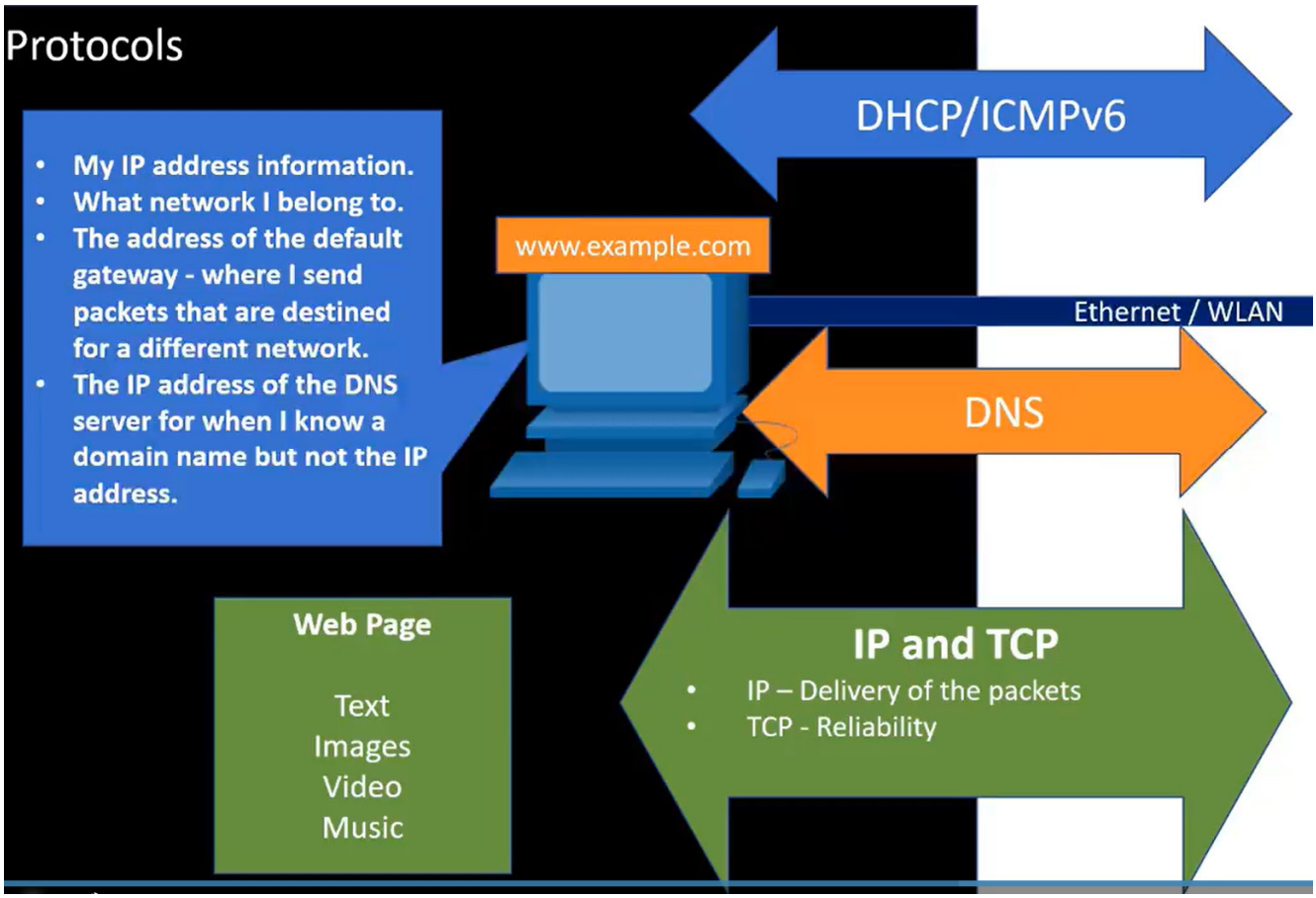


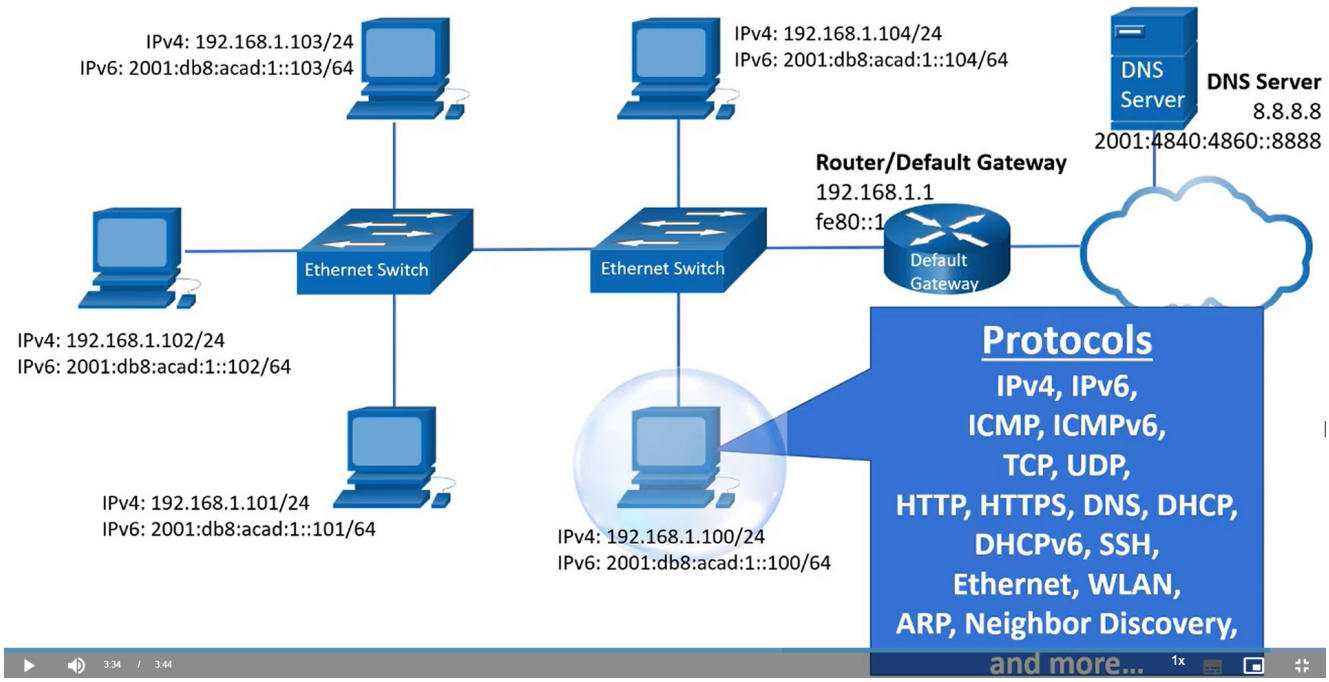

How we "see" the network
IPv4: 192.168.1.103/24
IPv6: 2001:db8:acad:1::103/64
IPv4: 192.168.1.104/24
IPv6: 2001:db8:acad:1::104/64
DNS Server
DNS Server
8.8.8.8
2001:4840:4860::8888
Router/Default Gateway
192.168.1.1
fe80::1
Ethernet Switch
Ethernet Switch
Default Gateway
IPv4: 192.168.1.102/24
IPv6: 2001:db8:acad:1::102/64
IPv4: 192.168.1.101/24
IPv6: 2001:db8:acad:1::101/64


How we "see" the network
IPv4: 192.168.1.103/24
IPv6: 2001:db8:acad:1::103/64
IPv4: 192.168.1.104/24
IPv6: 2001:db8:acad:1::104/64
DNS Server
DNS Server
8.8.8.8
2001:4840:4860::8888
Router/Default Gateway
192.168.1.1
fe80::1
Ethernet Switch
Ethernet Switch
Default Gateway
IPv4: 192.168.1.102/24
IPv6: 2001:db8:acad:1::102/64
IPv4: 192.168.1.101/24
IPv6: 2001:db8:acad:1::101/64
Ethernet MAC: b2:00:91:28:a1:05
WLAN MAC : 70:2a:d5:bf:9b:c8
IP Addresses:
IPv4: 192.168.1.100/24
IPv6: 2001:db8:acad:1::100/64
Default Gateways:
192.168.1.1
fe80::1
DNS servers:
8.8.8.8
2001:4860:4860::8888


I'm in a bubble....
I only see myself – my own addressing information


This is how a device (computer, mobile phone, etc.) "sees" the network. It doesn't.
?
What is my addressing information? What network am I on?
Is the destination device on my network or is it on another network?
Where do I send information when the destination device is on a different network?
Did the destination device receive the information I sent?
Do I need to resend any information?
1:43 / 3:44
1x


Protocols
My IP address information.
What network I belong to.
The address of the default gateway - where I send packets that are destined for a different network.
The IP address of the DNS server for when I know a domain name but not the IP address.
DHCP/ICMPv6
www.example.com
Ethernet / WLAN
DNS
Web Page
Text
Images
Video
Music
IP and TCP
IP – Delivery of the packets
TCP - Reliability



3.1.2. Основи передавання даних

Мережі відрізняються розмірами, формами та функціями. Вони можуть бути як складними (наприклад, пристрої, що взаємодіють один з одним через мережу Інтернет), так і простими (наприклад, два комп'ютери безпосередньо з'єднані один з одним за допомогою кабеля або якогось іншого засобу). Але дротового або бездротового фізичного з'єднання між кінцевими пристроями недостатньо для реалізації зв'язку. Для того, щоб передавання даних здійснювалося, пристрої мають "знати", як взаємодіяти.

Люди обмінюються ідеями, використовуючи безліч різних методів спілкування. Однак усі методи спілкування мають три загальні елементи:

- **Джерело повідомлення (відправник)** - Відправником може бути людина або електронний пристрій, який або якому потрібно надіслати повідомлення іншій людині або пристрою.
- **Отримувач повідомлення (отримувач, адресат)** - отримує і інтерпретує повідомлення.
- **Канал** - Середовище, що забезпечує шлях, яким повідомлення передається від відправника до отримувача.
-

3.1.3. Протоколи передавання даних

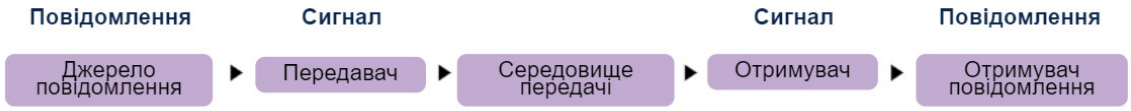
Як особисте спілкування, так і спілкування через мережу, регулюються правилами, які називають протоколами. Ці протоколи специфічні для типу методу передавання даних, що використовується. У нашому повсякденному особистому спілкуванні правила, якими ми користуємось для спілкування через один носій інформації (наприклад, через телефонний дзвінок), не обов'язково збігаються з правилами використання іншого носія (наприклад, через відправлення листа).

Процес надсилання листа схожий на обмін даними, який відбувається в комп'ютерних мережах.

Звичайне спілкування

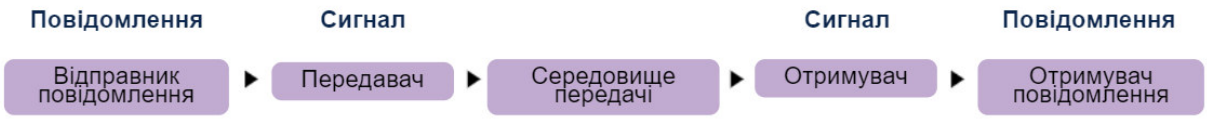
Перед початком спілкуванням вони мають узгодити, яким чином це буде відбуватися. Якщо це спілкування голосом, вони спочатку домовляються про мову. Потім, коли у них є повідомлення для обміну, вони повинні мати можливість форматувати це повідомлення зрозумілим способом.

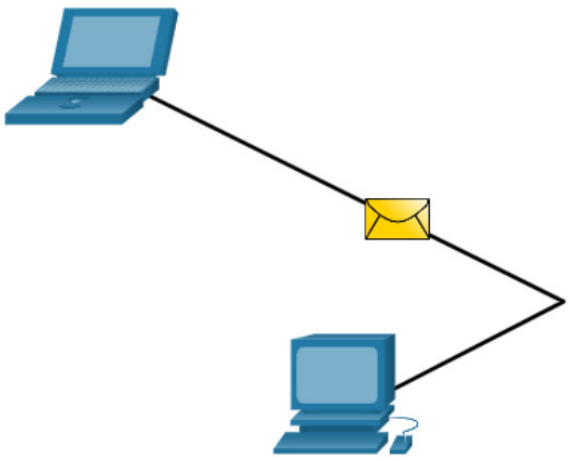
Якщо хтось говорить англійською, але неправильно формує речення, повідомлення може бути незрозумілим. Кожне з цих завдань описує протоколи, які використовуються для зв'язку.



Мережний зв'язок

Як показано в анімації, це справедливо і для комп'ютерного зв’язку. Багато різних правил або протоколів регулюють усі методи спілкування, які існують у світі сьогодні.





3.1.4. Встановлення правил

Перш ніж розпочати спілкування один з одним, ми встановлюємо правила чи домовленості щодо управління розмовою. Розглянемо, наприклад, таке повідомлення:

Правиларегулюютьспілкування міжлюдьми. Дужеважко зрозумітиповідомлення,якінеправильно відформатовані таневідповідаютьвстановленим правилам та протоколам. Використання загальної граматики,правилформування реченьтаправил використаннязнаків пунктуаціїмовидають можливістьлюдям порозумітисяміжсобою.

Зауважте, як важко прочитати повідомлення, оскільки воно не відформатоване належним чином. Воно повинно бути написаним з використанням правил (тобто протоколів), необхідних для ефективної комунікації. Приклад показує повідомлення, яке тепер належним чином відформатоване для мови та граматики.

Правила регулюють спілкування між людьми. Дуже важко зрозуміти повідомлення, які неправильно відформатовані та не відповідають встановленим правилам та протоколам. Використання загальної граматики, правил формування речень та правил використання знаків пунктуації мови дають можливість людям порозумітися між собою.

Протоколи повинні відповідати таким вимогам для успішної доставки повідомлення, яке є зрозумілим для отримувача:

- Ідентифіковані відправник та отримувач
- Загальна мова та граматика
- Швидкість та терміни доставки
- Вимоги щодо підтвердження отримання повідомлення

3.1.5. Вимоги до мережного протоколу

Протоколи, які використовуються в мережному зв'язку, мають багато з цих основних ознак. Окрім визначення відправника та отримувача, комп'ютерні та мережеві протоколи визначають деталі процесу передачі повідомлення через мережу. Поширені комп'ютерні протоколи містять вимоги щодо:

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

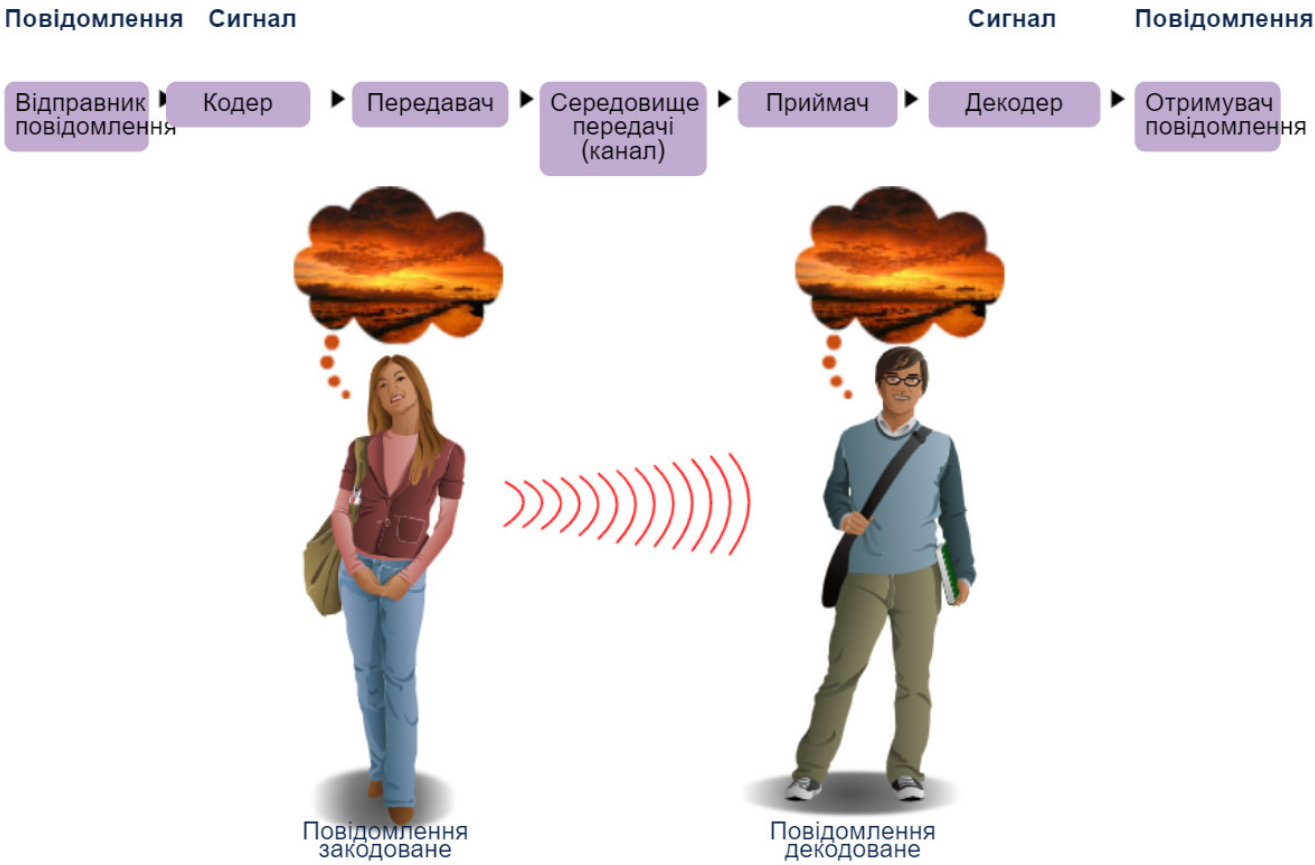
3.1.6. Кодування повідомлень

Одним з перших етапів надсилання повідомлення є етап кодування. **Кодування** - це процес перетворення інформації в форму, прийнятну для передачі. **Декодування** - зворотний процес, в результаті якого інформація перетворюється в початковий вигляд.

Звичайне спілкування

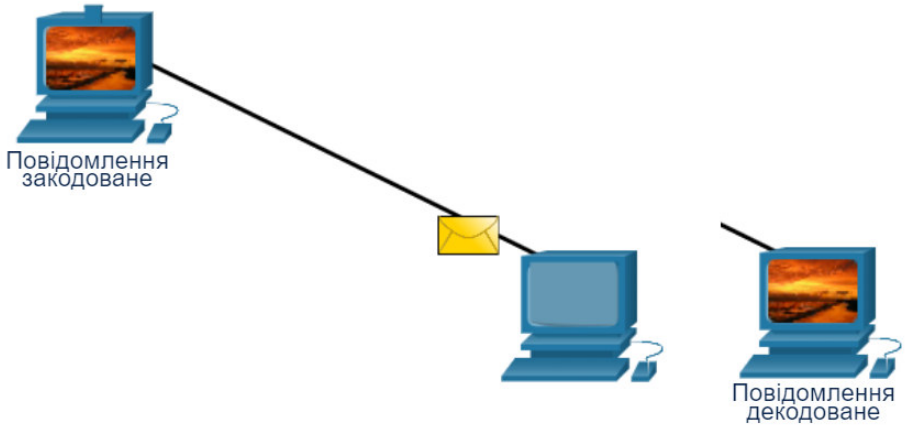
Уявіть, що людина дзвонить другу, щоб обговорити деталі прекрасного заходу сонця.

Для передачі повідомлення людина перетворює свої думки в узгоджену мову. Потім, використовуючи звуки та інтонації розмовної мови, вона вимовляє слова, які передають повідомлення. Її друг слухає і розшифровує звуки, щоб зрозуміти отримане ним повідомлення.



Мережний зв'язок

Кодування для обміну даними між вузлами повинна бути виконане в форматі, що відповідає середовищу. Для здійснення передачі, перш за все, вузол-відправник перетворює повідомлення в біти. Кожен біт кодується відповідним рівнем напруги для мідних дротів, інфрачервоним світлом для оптичних волокон або мікрохвилями для бездротових систем. Вузол-отримувач приймає і декодує сигнали та інтерпретує повідомлення.



3.1.7. *Форматування та інкапсуляція повідомлення*

Для надсилання повідомлення від відправника до отримувача необхідно, щоб воно було сформованим відповідно до певного формату або структури. Формати повідомлень залежать від типів повідомлень та каналів, що використовується для доставки повідомлення.

Звичайне спілкування

Поширений приклад необхідності застосування правильного формату в спілкуванні людини - це надсилання листа. Натисніть Відтворити на рисунку, щоб переглянути анімацію форматування та вкладення листа.

На конверті у належних місцях наявні адреси відправника та отримувача Неправильна адреса отримувача або форматування призведуть до того, що лист не буде доставлений.

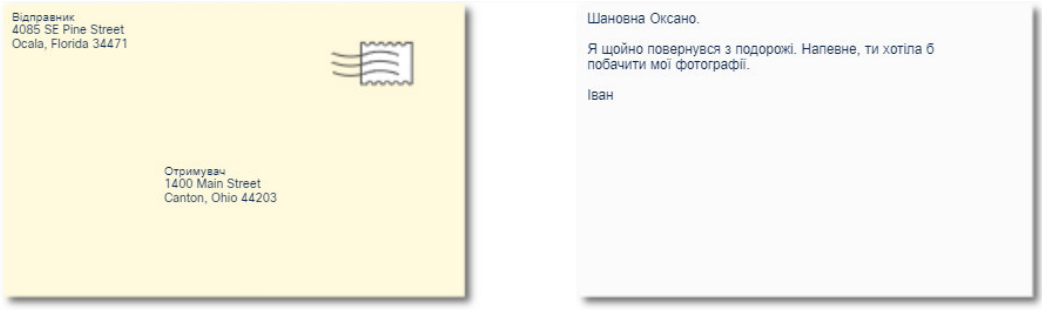
Процес розміщення одного повідомлення (листа) всередині повідомлення іншого формату (конверта) називається інкапсуляцією. Декапсуляція схожа на те, як одержувач виймає листа з конверту.

Мережний зв'язок

За аналогією, для доставки і обробки повідомлення в комп'ютерній мережі необхідно дотримуватися певних правил форматування.

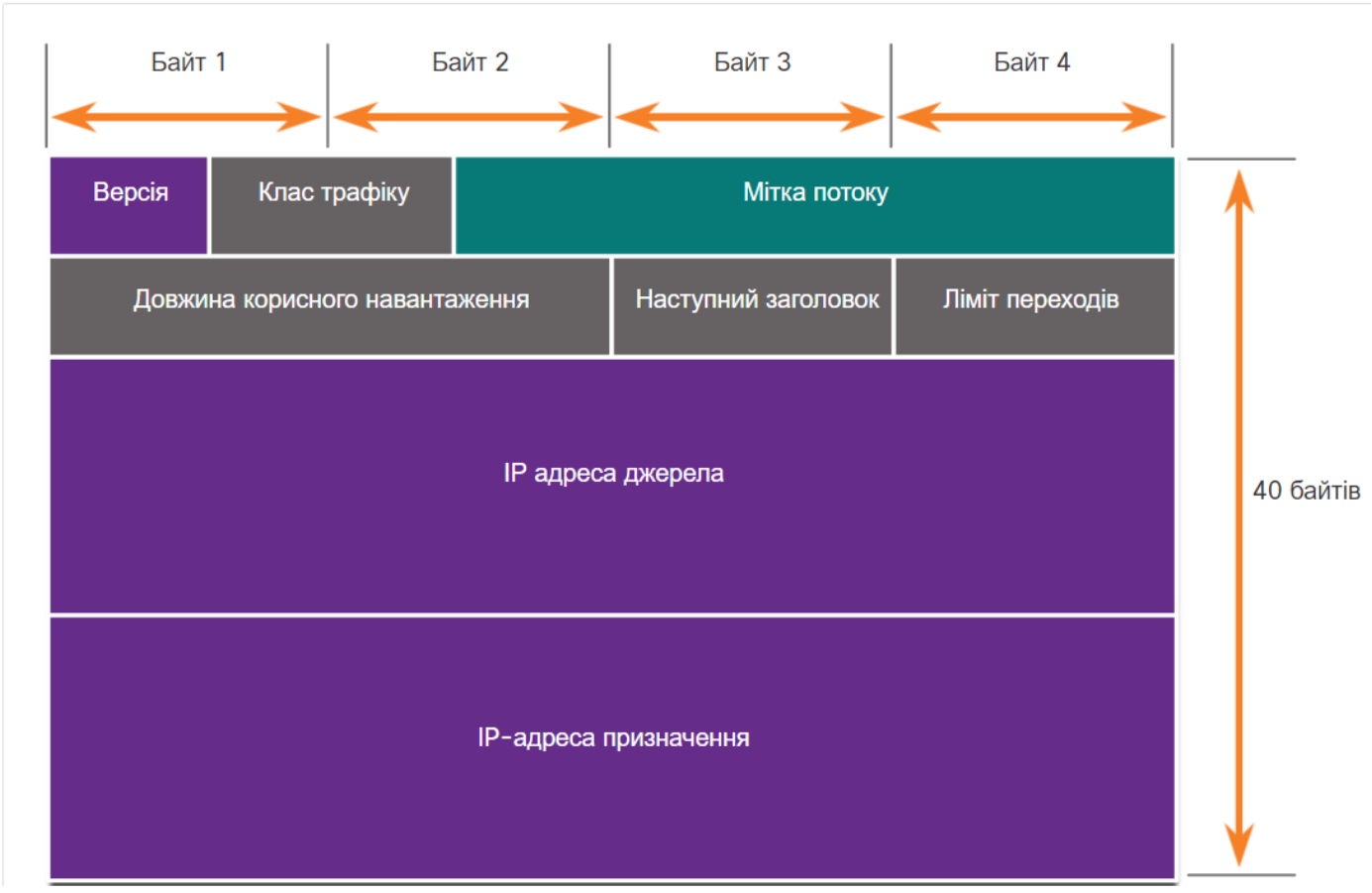
Протокол IP (IP, Internet Protocol) - це протокол, що має функцію, аналогічну прикладу з конвертом. На рисунку поля пакету протоколу IP версії 6 (IPv6, Internet Protocol version 6) ідентифікують відправника та отримувача пакету. IP відповідає за надсилання повідомлення від відправника до отримувача через одну або більше мереж.

Примітка: Поля пакета IPv6 детально розглядаються в іншому модулі.



Адреса місцезнаходження отримувача (адресата)	Адреса місцезнаходження відправника (джерела)	Привітання (індикатор початку повідомлення)	Ідентифікатор одержувача (місця призначення)	Вміст листа (інкапсульовані дані)	Ідентифікатор відправника (джерела)	Кінець фрейму (Індикатор кінця повідомлення)
Адресація на конверті		Інкапсульований лист				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Florida 34471	Шановна	Оксано	Я щойно повернувся з подорожі. Напевне, ти хотіла б побачити мої фотографії.	Іван	

Примітка: Поля пакета IPv6 детально розглядаються в іншому модулі.



3.1.8. Розмір повідомлення

Ще одне правило зв'язку - це розмір повідомлення.

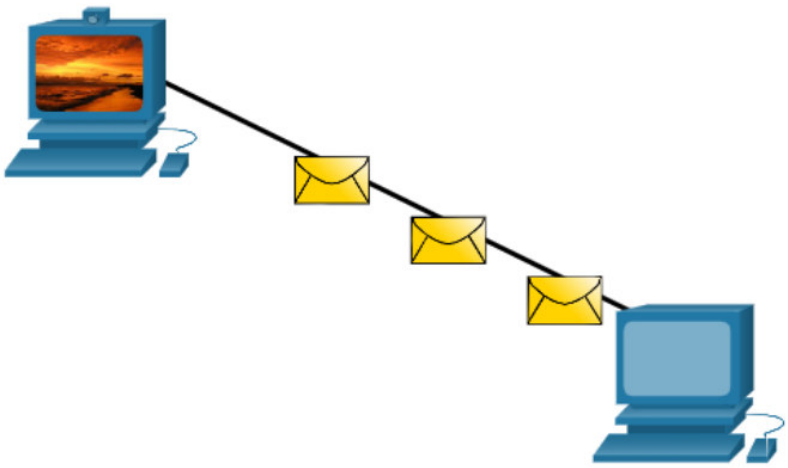
Звичайне спілкування

Коли люди спілкуються один з одним, повідомлення, які вони надсилають, зазвичай розбиваються на менші частини або речення. Ці речення обмежені за розміром так, щоб людина могла їх прийняти і обробити за один раз, як показано на рисунку. Обмеження за розміром також полегшує приймачеві читання та розуміння повідомлення.

Мережний зв'язок

Кодування відбувається також у комп'ютерному зв’язку.

Кодування для обміну даними між вузлами повинна бути виконане в форматі, що відповідає середовищу. Для здійснення передачі, перш за все, вузол-відправник перетворює повідомлення в біти. Кожен біт кодується в набір звуків, світлових хвиль або електричних імпульсів залежно від мережного середовища, через яке передаються біти. Вузол-отримувач приймає і декодує сигнали для інтерпретації повідомлення.



3.1.9. Синхронізація повідомлень

Синхронізація повідомлень також є дуже важливою в мережному зв'язку. Синхронізація повідомлення включає:

- **Управління потоком (Flow Control) -** процес управління швидкістю передачі даних. Контроль потоку визначає, скільки інформації може бути надіслано та швидкість, з якою вона може бути доставлена. Наприклад, якщо одна людина розмовляє занадто швидко, людині-отримувачу може бути важко почути і зрозуміти повідомлення. У мережному зв'язку є мережеві протоколи, які використовуються пристроями-відправниками та пристроями-отримувачами повідомлень для узгодження та управління потоком інформації.
- **Час очікування відповіді (Response Timeout) -** якщо людина ставить запитання і не отримує відповіді протягом прийнятного проміжку часу, вона припускає, що відповіді не надходить і відповідно реагує. Людина може повторити запитання або замість нього може продовжити розмову. Вузли в мережі використовують мережеві протоколи, які вказують, як довго чекати відповіді та які дії потрібно вжити, якщо час очікування відповіді вичерпується.
- **Метод доступу (Access method) -** визначає, коли хтось зможе відправити повідомлення. Натисніть кнопку Відтворити на рисунку для того, щоб побачити анімацію одночасної розмови двох людей, у процесі якої відбувається «зіткнення інформації», і тому потрібно, щоб вони зупинилися і почали розмову знову. Так само, коли пристрій хоче передавати по бездротовій локальній мережі, необхідно, щоб бездротова мережна карта (WLAN NIC) визначила, чи доступне бездротове середовище.

3.1.10. Параметри доставки повідомлень

Повідомлення можна доставити різними способами.

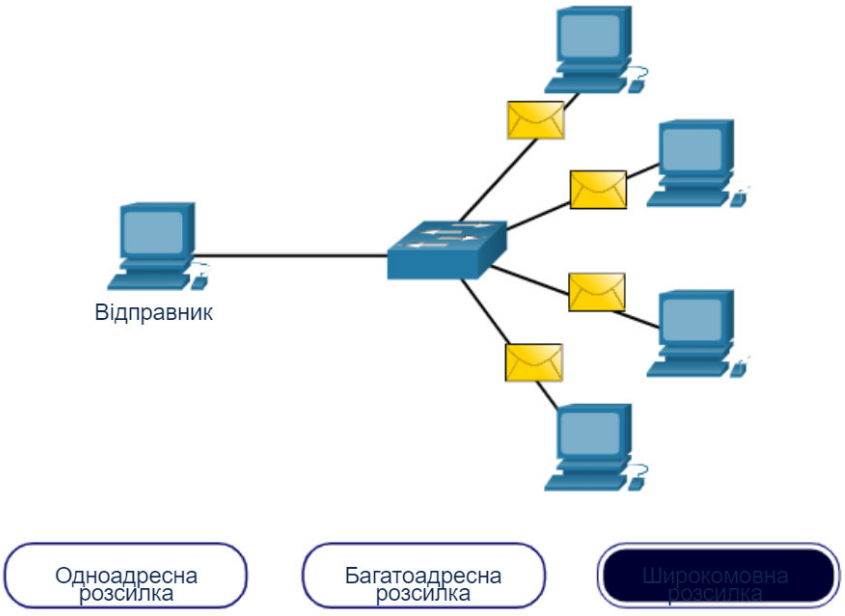
Звичайне спілкування

Іноді людина хоче донести інформацію до іншої індивідуально. Іншого разу у людини виникне необхідність надіслати інформацію одночасно групі людей або навіть усім людям на певній території.

Мережний зв'язок

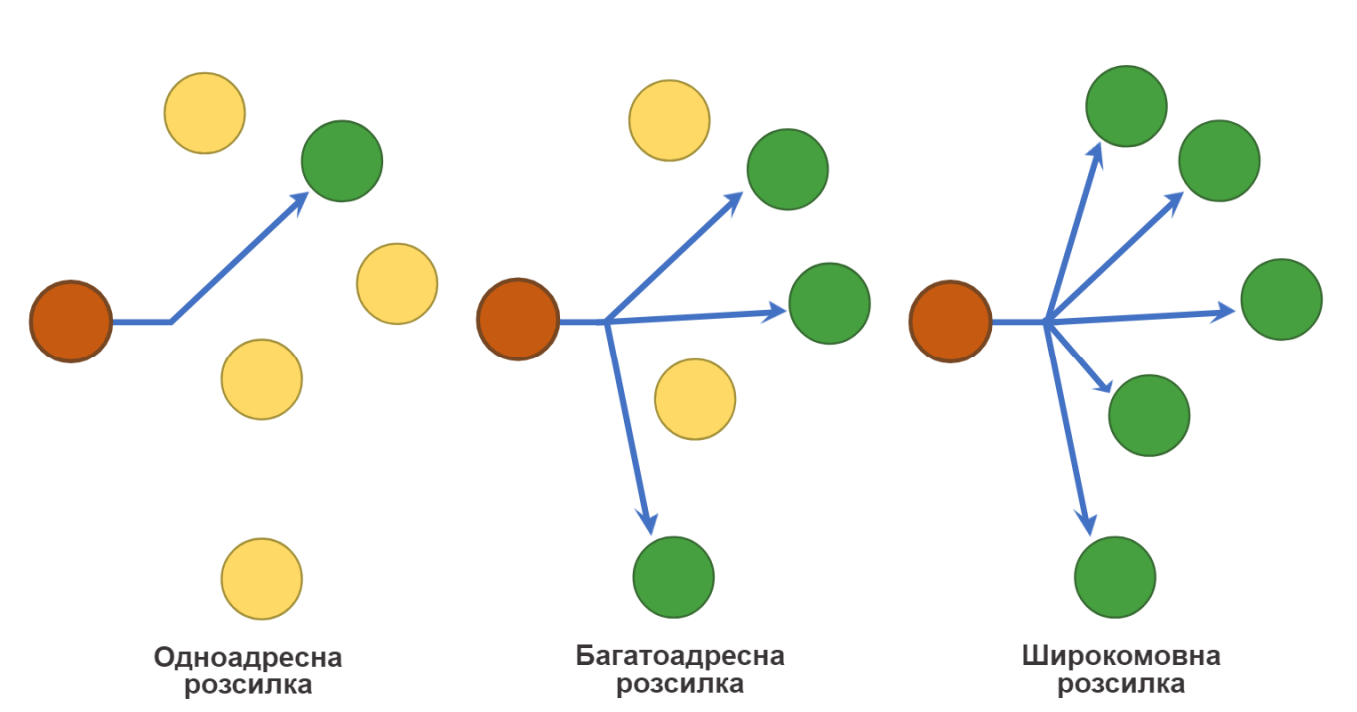
Мережне передавання даних має аналогічні варіанти доставки. Як показано на рисунку, існує три типи передачі даних:

- **Одноадресна розсилка (Unicast)** - інформація передається на один кінцевий пристрій.
- **Багатоадресна розсилка (Multicast)** - інформація передається на один або кілька кінцевих пристроїв.
- **Широкомовна розсилка (Broadcast)** - інформація передається на всі кінцеві пристрої.



3.1.11. Нотатки про піктограму вузла

Мережна документація та мережні топології часто відображають мережеві та кінцеві пристрої за допомогою піктограм вузлів. Вузли зазвичай представлені у вигляді кружків. На рисунку показано порівняння трьох різних варіантів доставки, використовуючи піктограми вузлів замість значків комп'ютерів.



3.1.12. *Питання для самоперевірки - Правила*

1. Як називається процес перетворення інформації у прийнятну для передачі форму?

   - ◯ Форматування
   - ◯ Кодування
   - ◯ Інкапсуляція

2. Який етап процесу зв'язку пов'язаний з належним визначенням адреси відправника та одержувача?

   - ◯ Форматування
   - ◯ Кодування
   - ◯ Інкапсуляція

3. Які три складові синхронізації повідомлення? (Оберіть три.)

   - ☐ Управління потоком
   - ☐ Порядкові номери
   - ☐ Метод доступу
   - ☐ Час повторної передачі
   - ☐ Час очікування відповіді

4. Який спосіб доставки використовується для передачі інформації на один або кілька кінцевих пристроїв, але не на всі пристрої в мережі?

   - ◯ Одноадресна розсилка
   - ◯ Багатоадресна розсилка
   - ◯ Широкомовна розсилка

1. Як називається процес перетворення інформації у прийнятну для передачі форму?

- ○ Форматування
- ◉ Кодування
- ○ Інкапсуляція

2. Який етап процесу зв’язку пов'язаний з належним визначенням адреси відправника та одержувача?

- ◉ Форматування
- ○ Кодування
- ○ Інкапсуляція

3. Які три складові синхронізації повідомлення? (Оберіть три.)

- ☑ Управління потоком
- ☐ Порядкові номери
- ☑ Метод доступу
- ☐ Час повторної передачі
- ☑ Час очікування відповіді

4. Який спосіб доставки використовується для передачі інформації на один або кілька кінцевих пристроїв, але не на всі пристрої в мережі?

- ○ Одноадресна розсилка
- ◉ Багатоадресна розсилка
- ○ Широкомовна розсилка

3.2. Протоколи

3.2.1. Огляд мережних протоколів

Ви знаєте, що для того, щоб кінцеві пристрої могли спілкуватися через мережу, кожен пристрій повинен дотримуватися одного і того ж набору правил. Ці правила називаються протоколами і вони мають багато функцій в мережі. Ця тема містить огляд мережних протоколів.

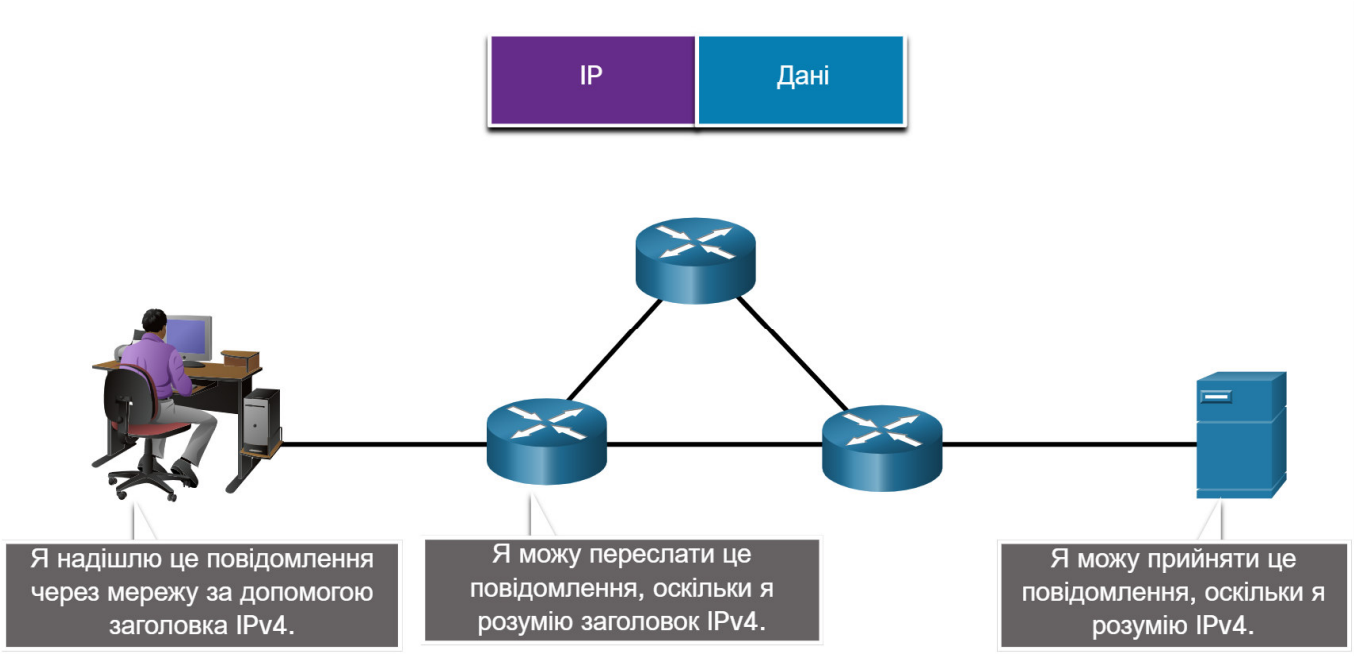
Мережні протоколи визначають загальний формат і набір правил для обміну повідомленнями між пристроями. Протоколи реалізуються кінцевими пристроями та проміжними пристроями програмно, апаратно або програмно-апаратно. Кожен мережний протокол має власну функцію, формат та правила зв'язку.

У таблиці перераховані різні типи протоколів, необхідних для забезпечення зв'язку через одну або кілька мереж.

Заголовок таблиці	
Тип протоколу	**Опис**
Протоколи передавання даних	Протоколи дозволяють двом або більше пристроям спілкуватися через один або більше мереж. Сімейство технологій Ethernet передбачає використання багатьох протоколів, зокрема, протоколу IP, протокол керування передаванням (TCP), протоколу передавання гіпертекстових повідомлень (HTTP) та багатьох інших.
Протоколи мережної безпеки	Протоколи захищають дані забезпечуючи автентифікацію, цілісність та шифрування даних Приклади захищених протоколів включають протокол безпечної оболонки (SSH), протокол рівня захищених сокетів (SSL) та протокол безпеки транспортного рівня (TLS).
Протоколи маршрутизації	Протоколи дозволяють маршрутизаторам обмінюватися інформацією про маршрут, порівнювати маршрутну інформацію, а потім вибрати найкращий шлях до мережі призначення. Приклади протоколів маршрутизації включають протокол пошуку першого найкоротшого шляху (OSPF, Open Shortest Path First) та протокол граничного шлюзу (BGP, Border Gateway Protocol).
Протоколи виявлення служб	Протоколи використовуються для автоматичного виявлення пристроїв або служб. Приклади протоколів виявлення послуг включають протокол динамічного налаштування вузла (DHCP, Dynamic Host Configuration Protocol), який виявляє послуги для призначення IP-адреси та систему доменних імен (DNS, Domain Name System), яка використовується для виконання встановлення відповідностей між назвами та IP-адресами вузлів

3.2.2. Функції мережного протоколу

Протоколи мережного зв'язку відповідають за різні функції, необхідні для передавання даних між кінцевими пристроями. Наприклад, на рисунку показано, як комп'ютер надсилає повідомлення через декілька мережевих пристроїв на сервер

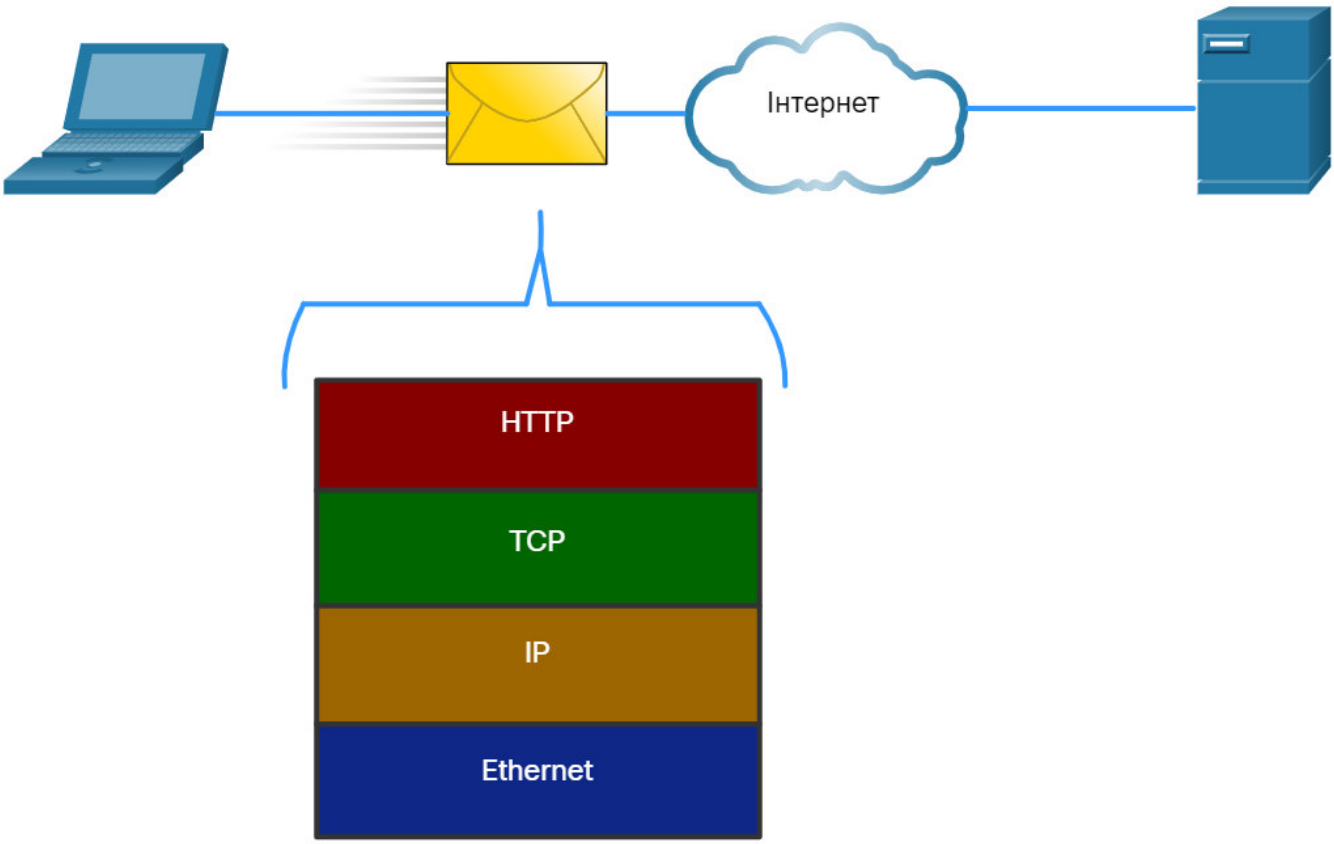


Комп'ютери та мережні пристрої використовують узгоджені протоколи для спілкування. У таблиці перераховані функції цих протоколів.

Заголовок таблиці	
Функція	**Опис**
Адресація	Ця функція ідентифікує відправника та отримувача повідомлення з використанням визначеної схеми адресації. Приклади протоколів, які забезпечують адресацію: Ethernet, IPv4 та IPv6.
Надійність	Ця функція забезпечує механізми гарантованої доставки повідомлення, у випадках якщо повідомлення втрачаються або пошкоджуються під час транспортування. TCP забезпечує гарантовану доставку.
Керування потоком	Ця функція забезпечує якомога ефективніше транспортування потоку даних між двома комунікаційними пристроями. TCP надає служби керування потоком.
Послідовність	Ця функція однозначно позначає кожен переданий сегмент даних. Пристрій-отримувач використовує інформацію про послідовність для правильного збирання інформації. Це корисно, якщо сегменти даних втрачені, отримані з затримкою або не в тому порядку. TCP надає служби послідовності.
Виявлення помилок	Ця функція використовується для визначення, чи були пошкоджені дані під час передачі. До протоколів, що забезпечують виявлення помилок, належать Ethernet, IPv4, IPv6 і TCP.
Програмний інтерфейс	Ця функція містить інформацію, яка використовується для міжпроцесної взаємодії між мережними застосунками. Наприклад, при зверненні до веб-сторінки, протоколи HTTP або HTTPS використовуються для зв'язку між процесами веб-клієнта та веб-сервера.

3.2.3. *Взаємодія протоколів*

Повідомлення, що надсилається через комп'ютерну мережу, зазвичай вимагає використання декількох протоколів, кожен з яких має свої функції та формат. На рисунку показані деякі загальні мережні протоколи, які використовуються у випадку, коли пристрій надсилає запит веб-серверу з метою отримання його веб-сторінки.



Протоколи на рисунку описані так:

- **Протокол передавання гіпертексту (HTTP) –** протокол регулює взаємодію веб-сервера та веб-клієнта. HTTP визначає вміст та формат запитів та відповідей, за допомогою яких здійснюється обмін даними між клієнтом та сервером. Програмне забезпечення і клієнта, і веб-сервера реалізують протокол HTTP як частини своїх застосунків. HTTP покладається на інші протоколи для керування способом передавання повідомлень між клієнтом та сервером.
- **Протокол керування передаванням (TCP, Transmission Control Protocol) –** цей протокол керує окремими сеансами зв'язку. TCP несе відповідальність за гарантовану надійну доставки інформації та керування потоком між кінцевими пристроями.
- **Інтернет-протокол (IP) –** протокол, який відповідає за доставку повідомлень від відправника до отримувача. IP використовується маршрутизаторами для передавання повідомлень через мережі.
- **Ethernet –** цей протокол відповідає за доставку повідомлень від однієї мережної плати до іншої в межах локальної мережі Ethernet.

3.2.4. *Питання для самоперевірки - Протоколи*

1. До якого типу протоколів належать протоколи BGP та OSPF?

- ◯ Протоколи мережного зв'язку
- ◯ Протоколи мережної безпеки
- ◯ Протоколи маршрутизації
- ◯ Протоколи виявлення служб

2. Які два протоколи є протоколами виявлення служб? (Оберіть два.)

- ☐ DNS
- ☐ TCP
- ☐ SSH
- ☐ DHCP

3. З якою метою застосовується функція послідовності в мережному зв’язку?

- ◯ для унікального маркування переданих сегменти даних і подальшого належного відновлення їх порядку передачі отримувачем
- ◯ для визначення пошкоджень даних під час передачі
- ◯ для забезпечення ефективного якнайшвидшого передавання потоків даних між відправником та отримувачем
- ◯ для гарантування доставки даних

4. Зазначте протокол, що відповідає за гарантовану надійну доставку інформації.

- ◯ TCP
- ◯ IP
- ◯ HTTP
- ◯ Ethernet

1. До якого типу протоколів належать протоколи BGP та OSPF?

- ◯ Протоколи мережного зв'язку
- ◯ Протоколи мережної безпеки
- ◉ Протоколи маршрутизації
- ◯ Протоколи виявлення служб

2. Які два протоколи є протоколами виявлення служб? (Оберіть два.)

- ☑ DNS
- ☐ TCP
- ☐ SSH
- ☑ DHCP

3. З якою метою застосовується функція послідовності в мережному зв’язку?

- ◉ для унікального маркування переданих сегменти даних і подальшого належного відновлення їх порядку передачі отримувачем
- ◯ для визначення пошкоджень даних під час передачі
- ◯ для забезпечення ефективного якнайшвидшого передавання потоків даних між відправником та отримувачем
- ◯ для гарантування доставки даних

4. Зазначте протокол, що відповідає за гарантовану надійну доставку інформації.

- ◉ TCP
- ◯ IP
- ◯ HTTP
- ◯ Ethernet

3.3. Стеки протоколів

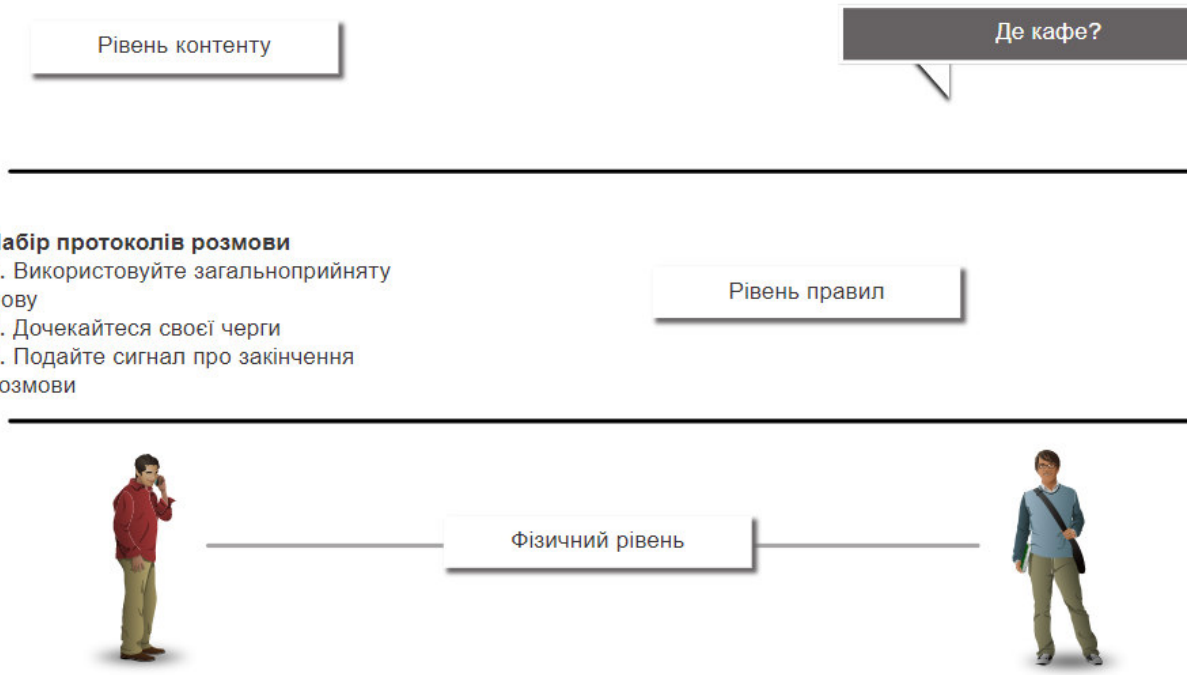
3.3.1. Стеки мережних протоколів

У багатьох випадках протоколи повинні мати можливість працювати з іншими протоколами, щоб надати вам все необхідне для мережного зв'язку. Стеки протоколів розроблені для безперебійної взаємодії пристроїв один з одним.

Стек протоколів - це група взаємозалежних протоколів, необхідних для виконання функції зв'язку.

Один з найкращих способів візуалізації взаємодії протоколів у стеці - це аналіз їх сукупної взаємодії. Стек протоколів показує, як реалізуються окремі протоколи з певного набору. Протоколи розглядаються з точки зору рівнів, кожен сервіс вищого рівня залежить від функціональності, визначеної протоколами нижчих рівнів. Нижні рівні стека відповідають за передавання даних через мережу та надання сервісів верхнім рівням, які відповідають за зміст повідомлень, що передаються.

На рисунку показано, як ми можемо використовувати рівні для опису взаємодії, що відбувається при спілкування віч-на-віч. У нижній частині знаходиться фізичний рівень, на якому двоє людей вимовляють слова вголос. Посередині знаходиться рівень правил, який визначає вимоги до спілкування, включаючи потребу вибору спільної мови. Вгорі знаходиться рівень контенту, і саме тут насправді йдеться про зміст спілкування.

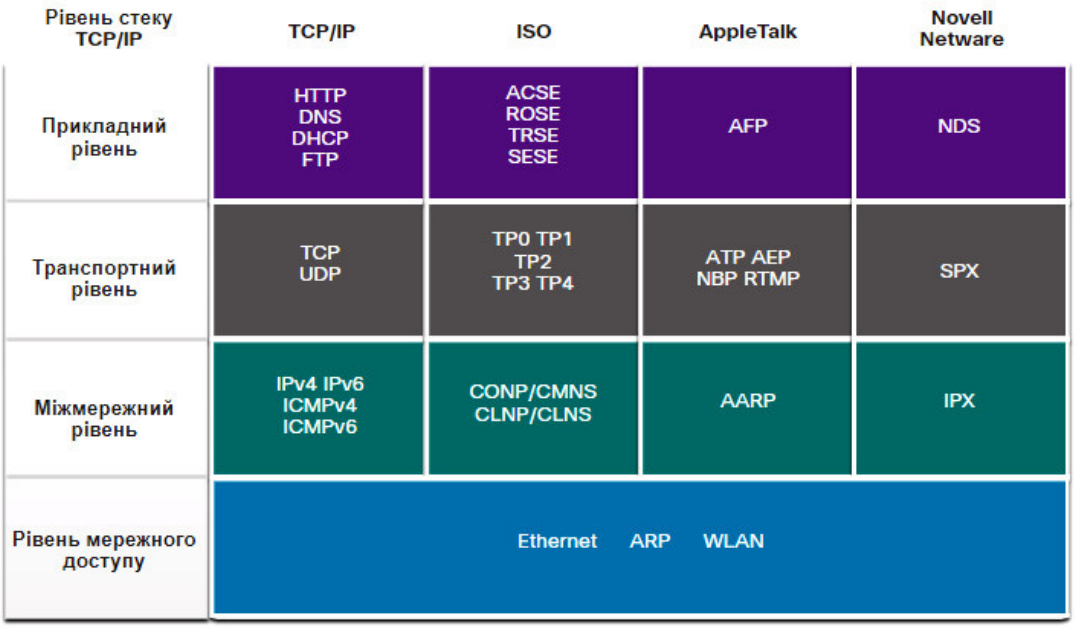


Стеки протоколів – це набори правил, які працюють разом, щоб допомогти вирішити проблему.

3.3.2. Еволюція стеків протоколів

Стек протоколів - це набір протоколів, які працюють разом для забезпечення комунікаційних послуг об'єднаної мережі. Починаючи з 1970-х років існувало декілька різних стеків протоколів, деякі були розроблені організацією зі стандартів, інші розроблені різними постачальниками.

Під час еволюції мережного зв'язку та Інтернету існувало кілька наборів протоколів, що конкурували між собою, як показано на рисунку.



- **Стек інтернет протоколів або стек TCP/IP** - це найпоширеніший і найвживаніший стек протоколів, що застосовується сьогодні. Стек протоколів TCP/IP - це відкритий стандартний набір протоколів, що підтримується Інженерною робочою групою (IETF, Internet Engineering Task Force).
- **Протоколи взаємодії відкритих систем (OSI, Open Systems Interconnection)** - це сімейство протоколів, розроблених спільно в 1977 році Міжнародною організацією зі стандартизації (ISO, International Organization for Standardization) та Міжнародним союзом телекомунікацій (ITU, International Telecommunications Union). Протокол OSI також включав семирівневу модель, що називається еталонною моделлю OSI. Еталонна модель OSI визначає функції своїх протоколів. Сьогодні OSI в основному відома своїми сімома рівнями. Протоколи OSI значною мірою були замінені протоколами TCP/IP.
- **AppleTalk** - застарілий патентований стек протоколів, випущений Apple Inc. в 1985 році для пристроїв Apple. У 1995 році Apple впровадила стек TCP/IP як заміну стеку AppleTalk.
- **Novell NetWare** - застарілий патентований стек протоколів та мережна операційна система, розроблена Novell Inc. в 1983 році, яка використовувала мережний протокол IPX. У 1995 році Novell впровадила стек TCP/IP як заміну стеку IPX.

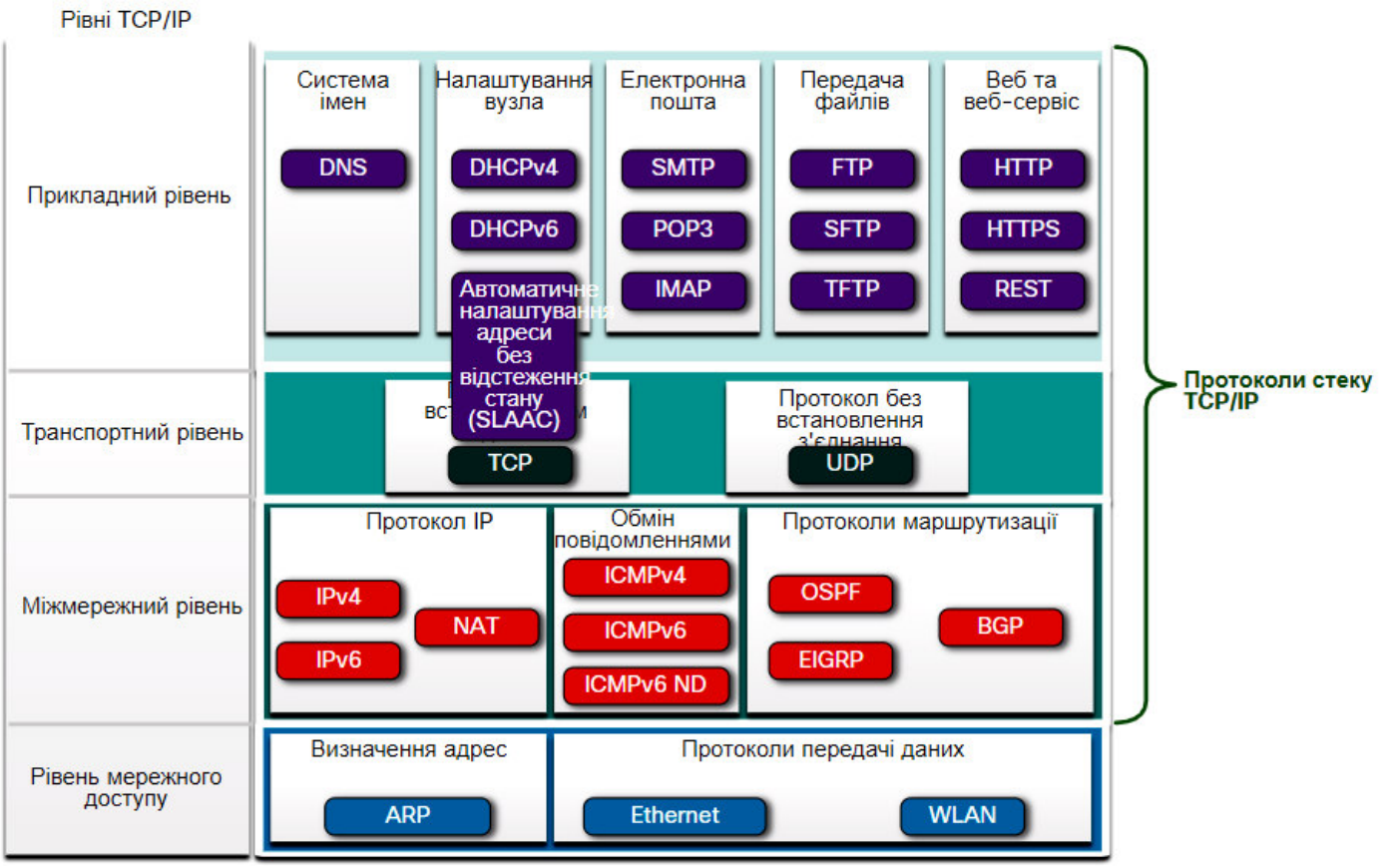
3.3.3. Приклад використання протоколів TCP/IP

Протоколи TCP/IP функціонують на прикладному, транспортному та міжмережному рівнях. На рівні мережного доступу протоколи стеку TCP/IP відсутні. Найпоширенішими протоколами рівня мережного доступу є протоколи технологій Ethernet та бездротових локальних мереж (WLAN). Протоколи рівня мережного доступу відповідають за доставку IP-пакету через фізичне середовище.

На рисунку наведений приклад застосування трьох протоколів TCP/IP для надсилання пакетів між веб-браузером та веб-сервером. HTTP, TCP і IP - це використовувані протоколи TCP/IP. На рівні мережного доступу у прикладі використовується Ethernet. Однак, також може бути використаний бездротовий (WLAN) або стільниковий зв'язок.

3.3.4. *Стек протоколів TCP/IP*

Сьогодні набір протоколів TCP/IP містить багато протоколів і продовжує розвиватися для підтримки нових інформаційних послуг. Деякі з найбільш вживаних протоколів зображені на рисунку.



TCP/IP – це стек протоколів, що використовується в сучасних мережах та мережі Інтернет. TCP/IP має два важливих аспекти для постачальників та виробників:

- **Відкритий стандартний набір протоколів** – це означає, що він знаходиться у вільному доступі для громадськості і може бути використаний будь-яким постачальником на власному обладнанні або у власному програмному забезпеченні.
- **Набір протоколів на основі стандартів** – це означає, що він був схвалений мережевий індустрією і схвалений організацією зі стандартизації. Це гарантує, що продукти від різних виробників будуть успішно взаємодіяти між собою.

Прикладний рівень

Система імен

- **DNS, Domain Name System** - доменна система імен. Визначає IP-адреси, що відповідають доменним іменам (наприклад, IP-адреси для сайту cisco.com).

Протоколи налаштування вузла

- **DHCPv4б Dynamic Host Configuration Protocol for IPv4** - протокол динамічного налаштування вузла для IPv4. Сервер DHCPv4 динамічно надає інформацію про адресацію IPv4 клієнтам DHCPv4 при запуску і дозволяє повторно використовувати адреси, коли вони більше не потрібні.
- **DHCPv6, Dynamic Host Configuration Protocol for IPv6** - протокол динамічного налаштування вузла для IPv6. DHCPv6 подібний на DHCPv4. Сервер DHCPv6 динамічно надає інформацію про адресацію IPv6 клієнтам DHCPv6 при запуску.
- **SLAACб Stateless Address Autoconfiguration** - автоматичне налаштування адреси без відстеження стану. Метод, який дозволяє пристрою отримувати адресну інформацію IPv6 без використання сервера DHCPv6.

Протоколи електронної пошти

- **SMTP, Simple Mail Transfer Protocol** - простий протокол електронної пошти. Дозволяє клієнтам надсилати email-повідомлення на поштовий сервер, а серверам - на інші сервери.
- **POP3, Post Office Protocol version 3** - поштовий протокол версії 3. Дозволяє клієнтам отримувати електронну пошту з поштового сервера та завантажувати електронну пошту до локальної поштової програми клієнта.
- **IMAP, Internet Message Access Protocol** - протокол доступу до інтернет-повідомлень. Дозволяє клієнтам отримувати доступ до електронної пошти, що зберігається на поштовому сервері, а також зберігати електронну пошту на сервері.

Протоколи передавання файлів

- **FTP, File Transfer Protocol** - протокол передавання файлів. Встановлює правила, які дозволяють користувачу одного хоста мати доступ до файлів та передавати файли з іншого хоста через мережу FTP - надійний, орієнтований на з'єднання протокол гарантованої доставки файлів
- **SFTP, Secure Shell FTP** - безпечний протокол передавання файлів. Протокол SFTP є розширенням протоколу SSH та може застосовується для організації безпечного сеансу передавання файлів. SSH - метод безпечного віддаленого входу, який зазвичай використовується для доступу до командного рядка пристрою.
- **TFTP, Trivial FTP** - простий протокол передавання файлів. TFTP - це простий протокол передавання файлів без встановлення з'єднання, який докладає зусиль для доставки, але її не гарантує. У порівнянні з FTP має менші накладні витрати.

Протоколи Веб та веб-сервісів

- **HTTP, Hypertext Transfer Protocol** - протокол передавання гіпертекстових повідомлень. Набір правил для обміну текстом, графічними зображеннями, аудіо, відео та іншими мультимедійними файлами у всесвітній мережі.
- **HTTPS, HTTP Secure** - Захищений HTTP. Безпечний варіант HTTP, що шифрує дані, якими обмінюються вузли через всесвітню мережу (WWW, World Wide Web).
- **REST, Representational State Transfer** - передавання репрезентативного стану. Веб-сервіс, який використовує інтерфейси прикладного програмування (APIs, Application Programming Interfaces) та HTTP-запити для створення веб-застосунків.

Транспортний рівень

Connection-Oriented Protocols, протоколи з встановленням з'єднання

- **TCP, Transmission Control Protocol** - протокол керування передаванням. Забезпечує надійний зв'язок між процесами, що виконуються на окремих вузлах, за рахунок передачі повідомлень, які підтверджують успішну доставку.

Connectionless Protocols, Протоколи без встановлення з'єднання

- **UDP, User Datagram Protocol** - протокол дейтаграм користувача. Дозволяє процесу, який виконується на одному хості, відправляти пакети процесу, який виконується на іншому хості Проте, протокол UDP Не підтверджує успішне передавання дейтаграм.

Internet Layer (Міжмережний рівень)

Протоколи Інтернет (Internet Protocol, IP)

- **IPv4, Internet Protocol version 4** - Інтернет-протокол версії 4. Отримує повідомлення-сегменти з транспортного рівня, вкладає ці повідомлення в пакети і спрямовує сформовані пакети на рівень мережного доступу для наскрізної доставки через мережу. IPv4 використовує 32-бітні адреси.
- **IPv6, Internet Protocol version 6** - Інтернет-протокол версії 6. Схожий на IPv4, але використовує 128-бітні адреси.
- **NAT, Мережний зв'язок Address Translation** - технологія трансляції (перетворення, заміни) мережних адрес. Замінює (транслює) приватні IP-адреси на глобальні унікальні публічні IP-адреси.

Протоколи обміну службовими повідомленнями

- **ICMPv4, Internet Control Message Protocol for IPv4** - протокол міжмережних керуючих повідомлень. Забезпечує зворотний зв'язок від вузла призначення до вихідного вузла, щоб повідомляти про помилки доставки пакетів.
- **ICMPv6, Internet Control Message Protocol for IPv6** - протокол міжмережних керуючих повідомлень для IPv6. Функціонал протоколу схожий на ICMPv4, але використовується для IPv6.
- **ICMPv6 Neighbor Discovery** - протокол виявлення сусідів. Містить чотири повідомлення протоколу ICMPv6, які використовуються для визначення адрес і виявлення адрес, що повторюються.

Протоколи маршрутизації

- **OSPF, Open Shortest Path First** - протокол знаходження найкоротшого шляху. Протокол маршрутизації з врахуванням стану каналу зв'язку, який використовує ієрархічний дизайн на основі областей. OSPF - відкритий внутрішньошлюзовий протокол маршрутизації.

- **EIGRP, Enhanced Interior Gateway Routing Protocol.** вдосконалений внутрішньошлюзовий протокол маршрутизації. Власний протокол маршрутизації Cisco, що використовує комплексну метрику, до якої входять пропускна здатність, затримка, навантаження та надійність.
- **BGP, Border Gateway Protocol** - Протокол граничного шлюзу. Відкритий зовнішньошлюзовий протокол маршрутизації, що використовується для передавання даних між постачальниками послуг Інтернету (ISP, Internet Service Providers). BGP також використовується для обміну маршрутною інформацією між Інтернет-провайдерами та їх великими приватними клієнтами.

Рівень мережного доступу

Визначення адрес

- **ARP, Address Resolution Protocol** - протокол визначення адрес. Забезпечує динамічне співставлення IPv4-адресою та апаратною адресою.

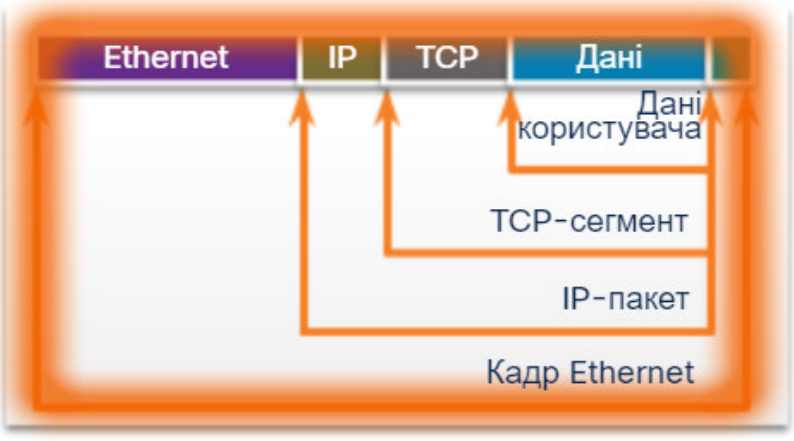
Протоколи канального рівня

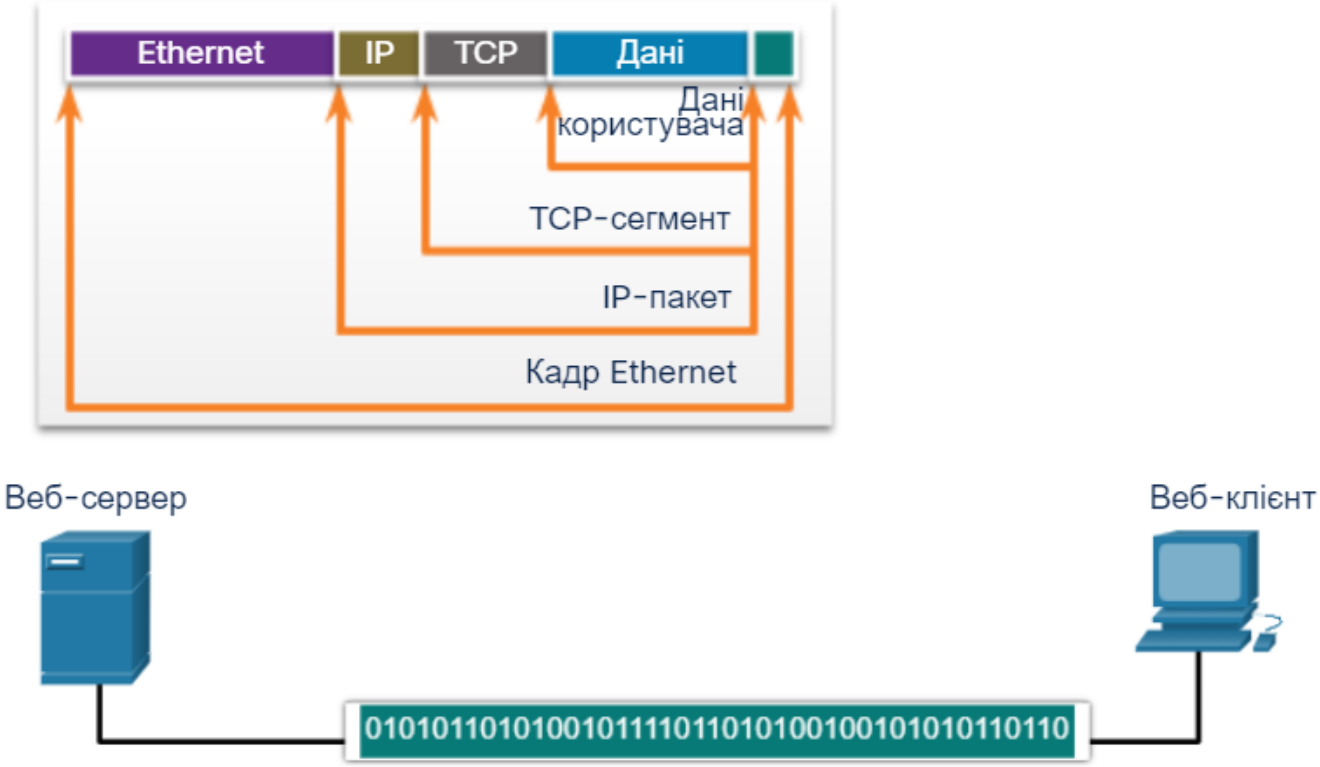
- **Ethernet** - визначає правила для стандартів кабельної інфраструктури та стандартів передачі сигналів на рівні мережного доступу.
- **WLAN, Wireless Local Area Мережний зв'язок** - бездротова локальна мережа. Визначає правила бездротової передачі сигналів на радіочастотах 2,4 ГГц і 5 ГГц.

3.3.5. Передавання даних в стеці TCP/IP

Анімації на рисунках демонструють повний процес зв'язку на прикладі передачі даних від веб-сервера до веб-клієнта.

Натисніть кнопку Відтворити , щоб побачити, як відбувається процес інкапсуляції у випадку, коли веб-сервер відправляє веб-сторінку веб-клієнтові.





Натисніть кнопку Відтворити на наступному рисунку, щоб переглянути анімацію процесу отримання даних та процесу деінкапсуляції веб-сторінки клієнтом для подальшого відображення у веб-браузері.

3.3.6. Питання для самоперевірки - Стек протоколів

1. Зазначте рівень стеку TCP/IP, до якого належать протоколи UDP та TCP.

- ◯ Прикладний
- ◯ Транспортний
- ◯ Міжмережний
- ◯ Мережного доступу

2. Які два протоколи належать до прикладного рівня моделі TCP/IP? (Оберіть два.)

- ☐ EIGRP
- ☐ DNS
- ☐ OSPF
- ☐ ICMP
- ☐ DHCP

3. Який протокол функціонує на рівні мережного доступу моделі TCP/IP?

- ◯ HTTP
- ◯ IP
- ◯ DNS
- ◯ Ethernet

4. Який з наведених протоколів забезпечує зворотній зв'язок від вузла-отримувача до вузла-відправника, щодо помилок при доставці пакетів? (Оберіть два.)

- [ ] IPv4
- [ ] TCP
- [ ] ICMPv4
- [ ] IPv6
- [ ] UDP
- [ ] ICMPv6

5. Пристрій отримує кадр канального рівня з даними, опрацьовує і видаляє дані Ethernet. Які наступні дані будуть опрацьовані пристроєм-отримувачем?

- ◯ дані протоколу HTTP на прикладному рівні
- ◯ HTML-дані на прикладному рівні
- ◯ дані протоколу IP на міжмережному рівні
- ◯ дані протоколу UDP на міжмережному рівні
- ◯ дані протоколів TCP та UDP на транспортному рівні

6. Які послуги надає міжмережний рівень стеку TCP/IP? (Оберіть три.)

- [ ] Передавання файлів
- [ ] Визначення адрес
- [ ] Протоколи маршрутизації
- [ ] Обмін повідомленнями
- [ ] Ethernet
- [ ] Протокол IP

1. Зазначте рівень стеку TCP/IP, до якого належать протоколи UDP та TCP.

- ○ Прикладний
- ◉ Транспортний
- ○ Міжмережний
- ○ Мережного доступу

2. Які два протоколи належать до прикладного рівня моделі TCP/IP? (Оберіть два.)

- ☐ EIGRP
- ☑ DNS
- ☐ OSPF
- ☐ ICMP
- ☑ DHCP

3. Який протокол функціонує на рівні мережного доступу моделі TCP/IP?

- ○ HTTP
- ○ IP
- ○ DNS
- ◉ Ethernet

4. Який з наведених протоколів забезпечує зворотній зв'язок від вузла-отримувача до вузла-відправника, щодо помилок при доставці пакетів? (Оберіть два.)

- [ ] IPv4
- [ ] TCP
- [x] ICMPv4
- [ ] IPv6
- [ ] UDP
- [x] ICMPv6

5. Пристрій отримує кадр канального рівня з даними, опрацьовує і видаляє дані Ethernet. Які наступні дані будуть опрацьовані пристроєм-отримувачем?

- ( ) дані протоколу HTTP на прикладному рівні
- ( ) HTML-дані на прикладному рівні
- (•) дані протоколу IP на міжмережному рівні
- ( ) дані протоколу UDP на міжмережному рівні
- ( ) дані протоколів TCP та UDP на транспортному рівні

6. Які послуги надає міжмережний рівень стеку TCP/IP? (Оберіть три.)

- [ ] Передавання файлів
- [ ] Визначення адрес
- [x] Протоколи маршрутизації
- [x] Обмін повідомленнями
- [ ] Ethernet
- [x] Протокол IP

3.4. Організації зі стандартизації

3.4.1. Відкриті стандарти

При купівлі нових автомобільних шин перед нами стоїть проблема вибору серед продукції багатьох виробників. Кожен з них буде мати, як мінімум, один тип шин, що підходитимуть вашому автомобілю. Це наслідок того, що автоіндустрія використовує певні стандарти при розробці автомобілів. Те ж саме відбувається і з протоколами. Існує велика кількість виробників мережних компонентів і вони всі повинні використовувати єдині стандарти. У сфері мереж стандарти розробляються міжнародними організаціями зі стандартизації.

Відкриті стандарти заохочують сумісність, конкуренцію та інновації. Вони також гарантують, що товар жодної з компаній не може монополізувати ринок або отримати несправедливу перевагу над своїми конкурентами.

Чудовим прикладом цього є придбання домашнього безпровідного маршрутизатора. Є багато різних варіантів маршрутизаторів від різних виробників і кожен з них підтримує стандартні протоколи, такі як IPv4, IPv6, DHCP, SLAAC, Ethernet та 802.11. Відкриті стандарти також дають можливість клієнтові з операційною системою Apple OS X завантажити веб-сторінку з веб-сервера, яким керує операційна система Linux. Це відбувається через те, що обидві операційні системи використовують відкриті стандартні протоколи стандартів, наприклад з стеку протоколів TCP/IP.

Зазвичай, організації зі стандартизації є незалежними від виробників некомерційними організаціями, що створені для розробки та сприяння впровадженню концепцій відкритих стандартів. Важливою є роль цих організації щодо підтримки відкритого Інтернету з вільно доступними специфікаціями та протоколами, що можуть бути реалізовані будь яким виробником.

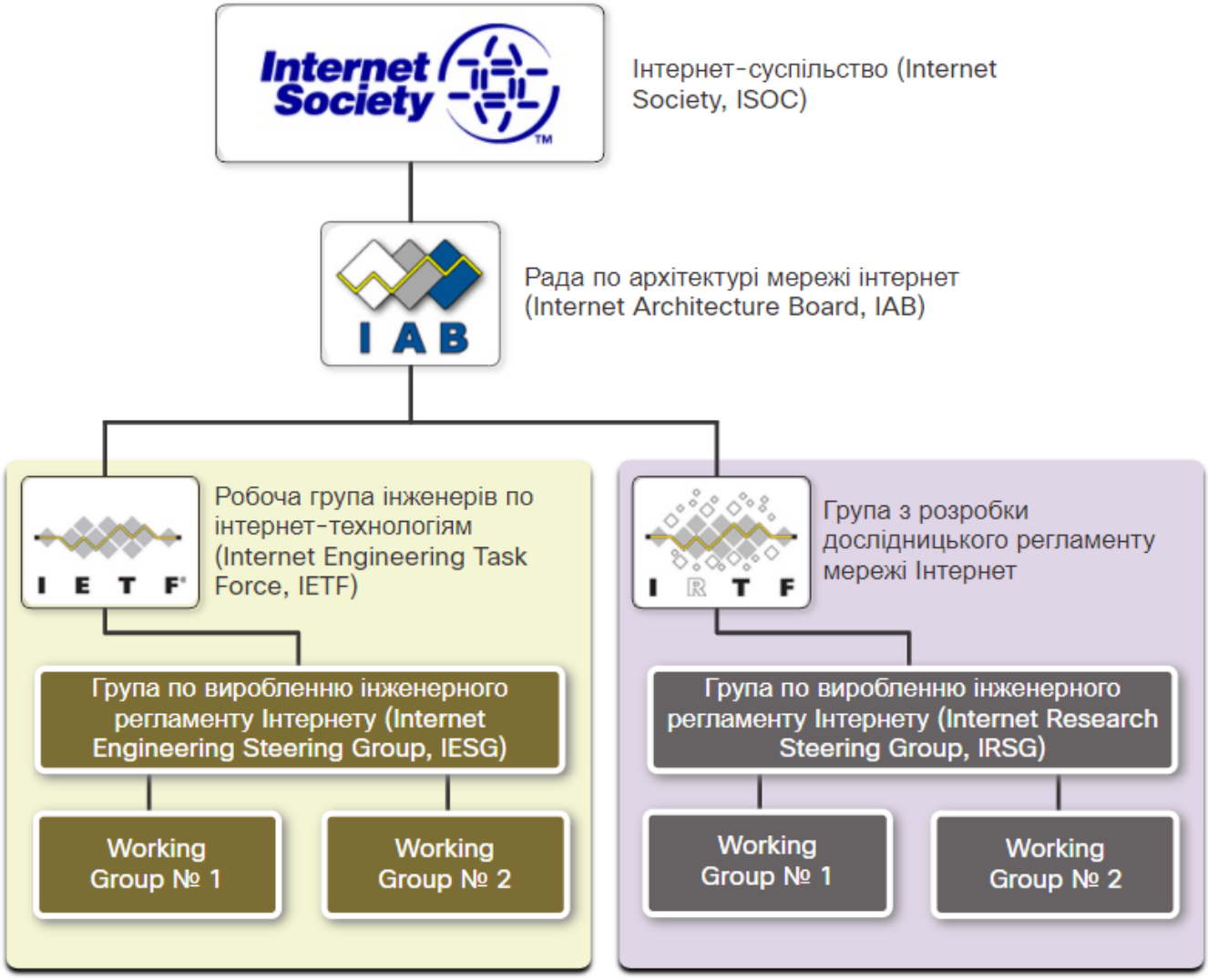
Організації зі стандартизації можуть розробляти набори правил самостійно або обрати певний фірмовий протокол як основу стандарту. Якщо використовується фірмовий протокол певного виробника, то розробка стандарту, зазвичай, відбувається за участі розробника цього протоколу.

На рисунку наведені логотипи організацій зі стандартизації.

3.4.2. Стандарти Інтернету

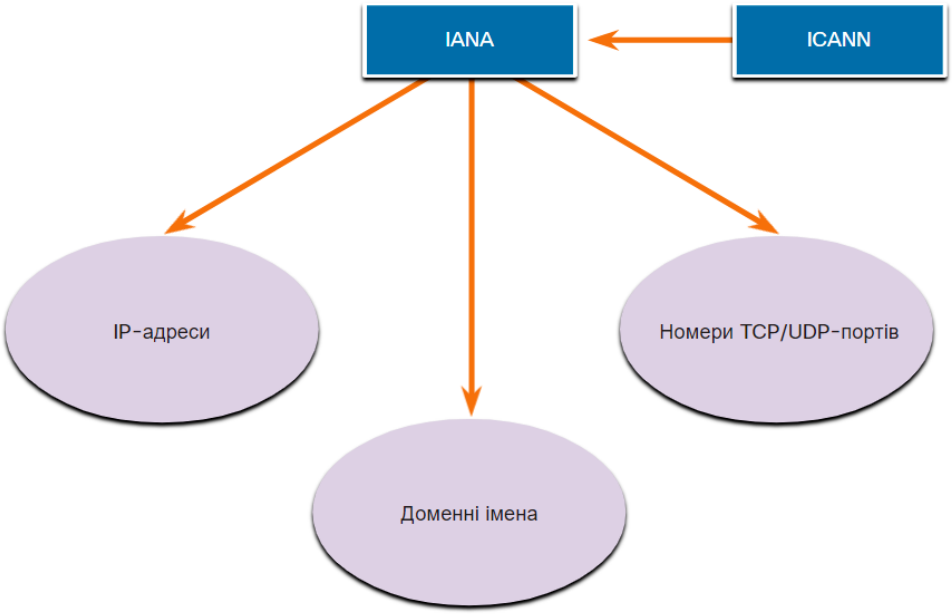
Кожна організація має свої обов'язки з створення та сприяння впровадженню стандартів Інтернету та протоколів стеку TCP/IP.

На рисунку наведений перелік організацій зі стандартизації, які займаються розробкою і підтримкою мережі Інтернет.



- **ISOC, Internet Society** – Інтернет-суспільство. ISOC відповідає за сприяння відкритій розробці і розширенню використання інтернету в усьому світі.
- **IAB, Internet Architecture Board** – Рада з архітектури мережі Інтернет. Відповідає за загальне керівництво і розробку інтернет-стандартів.
- **IETF, Internet Engineering Task Force** – Інженерна групи з розвитку мережі Інтернет. Розроблює, оновлює та підтримує технології мережі Інтернету та стеку TCP/IP. Також вона випускає документи для розробки нових та оновлення вже існуючих протоколів, відомі як "Робочі пропозиції" (RFC).
- **IRTF, Internet Research Task Force** – Група з розробки дослідницького регламенту мережі Інтернет. Зосереджується на довгострокових дослідженнях протоколів Інтернету та стеку TCP/IP, містить групу з досліджень захисту від спаму (ASRG, Anti-Spam Research Group), групу з досліджень криптографічного захисту (CFRG, Crypto Forum Research Group) та групу з досліджень одноранговых мереж (P2PRG, Peer-to-Peer Research Group).

На наступному рисунку наведені організацій зі стандартизації, які залучені до розробки і підтримки стеку TCP/IP, зокрема IANA та ICANN.



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

3.4.3. Організації з стандартизації електроніки та зв'язку

Інші організації зі стандартів несуть відповідальність за розробку проектів та створення стандартів з електроніки та зв'язку, які використовуються для доставки IP-пакетів у вигляді відповідних сигналів по дротових або бездротових середовищах.

До таких організацій зі стандартизації належать:

- **IEEE, Institute of Electrical and Electronics Engineers** (- Інститут інженерів з електротехніки та електроніки (**IEEE** вимовляється англійською мовою як "ай тріпл і"). Ця організація відповідає за просування технологічних інновацій та створення стандартів у багатьох галузях, зокрема, у енергетиці, охороні здоров'я, телекомунікаціях та мережних технологіях. Найважливішими мережними стандартами IEEE є стандарти 802.3 Ethernet та 802.11 WLAN. В мережі Інтернеті можна знайти інформацію й про інші мережні стандарти IEEE.
- **EIA, Electronic Industries Alliance** - Альянс галузей електронної промисловості. Ця організація відома своїми стандартами, що стосуються електричної проводки, роз'ємів та 19-дюймових стійок, які використовуються для монтажу мережного обладнання.
- **TIA, Telecommunications Industry Association** - Асоціація телекомунікаційної промисловості. Ця організація 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. На рисунку показаний приклад сертифікованого кабелю Ethernet, який був розроблений спільно TIA та EIA.
- **ITU-T, International Telecommunications Union-Telecommunication Standardization Sector** - Міжнародний союз електрозв'язку, сектор стандартизації телекомунікацій. Одна з найбільших і найстаріших організацій зі стандартів зв'язку. ITU-T окреслює стандарти стиснення відео, телебачення на базі протоколу IP (IPTV, Internet Protocol Television) та стандарти широкосмугового зв'язку, наприклад, цифрову абонентську лінію (DSL, Digital Subscriber Line).

3.4.5. *Питання для самоперевірки - Організації зі стандартизації*

1. Правда чи Неправда? Організації зі стандартизації, як правило, нейтральні з точки зору виробників.

- ◯ Правда
- ◯ Неправда

2. Ця організація зі стандартизації працює з документами RFC, які описують нові протоколи та оновлюють існуючі.

- ◯ Інтернет-суспільство (Internet Society, ISOC)
- ◯ Робоча група інженерів з інтернет-технологій (IETF)
- ◯ (Internet Architecture Board, IAB)
- ◯ Дослідницька група інтернет-технологій (IRTF)

3. Ця організація відповідає за розподіл IP-адрес та керування доменними іменами.

- ◯ Інтернет-суспільство (ISOC)
- ◯ Робоча група інженерів з інтернет-технологій (IETF)
- ◯ Рада з архітектури мережі інтернет (IAB)
- ◯ Адміністрація адресного простору Інтернет (IANA)

4. Які типи стандартів розроблені Альянсом електронної промисловості (EIA)?

- ◯ електрична проводка та роз'єми
- ◯ радіотехнічне обладнання та станції стільникового зв'язку
- ◯ стиснення відео та широкосмуговий зв’язок
- ◯ голосовий зв’язок через IP (VoIP) та супутниковий зв’язок

1. Правда чи Неправда? Організації зі стандартизації, як правило, нейтральні з точки зору виробників.

- (•) Правда
- ( ) Неправда

2. Ця організація зі стандартизації працює з документами RFC, які описують нові протоколи та оновлюють існуючі.

- ( ) Інтернет-суспільство (Internet Society, ISOC)
- (•) Робоча група інженерів з інтернет-технологій (IETF)
- ( ) (Internet Architecture Board, IAB)
- ( ) Дослідницька група інтернет-технологій (IRTF)

3. Ця організація відповідає за розподіл IP-адрес та керування доменними іменами.

- ( ) Інтернет-суспільство (ISOC)
- ( ) Робоча група інженерів з інтернет-технологій (IETF)
- ( ) Рада з архітектури мережі інтернет (IAB)
- (•) Адміністрація адресного простору Інтернет (IANA)

4. Які типи стандартів розроблені Альянсом електронної промисловості (EIA)?

- (•) електрична проводка та роз'єми
- ( ) радіотехнічне обладнання та станції стільникового зв'язку
- ( ) стиснення відео та широкосмуговий зв'язок
- ( ) голосовий зв'язок через IP (VoIP) та супутниковий зв'язок

3.5. Еталонні моделі

3.5.1. *Переваги використання багаторівневої моделі:*

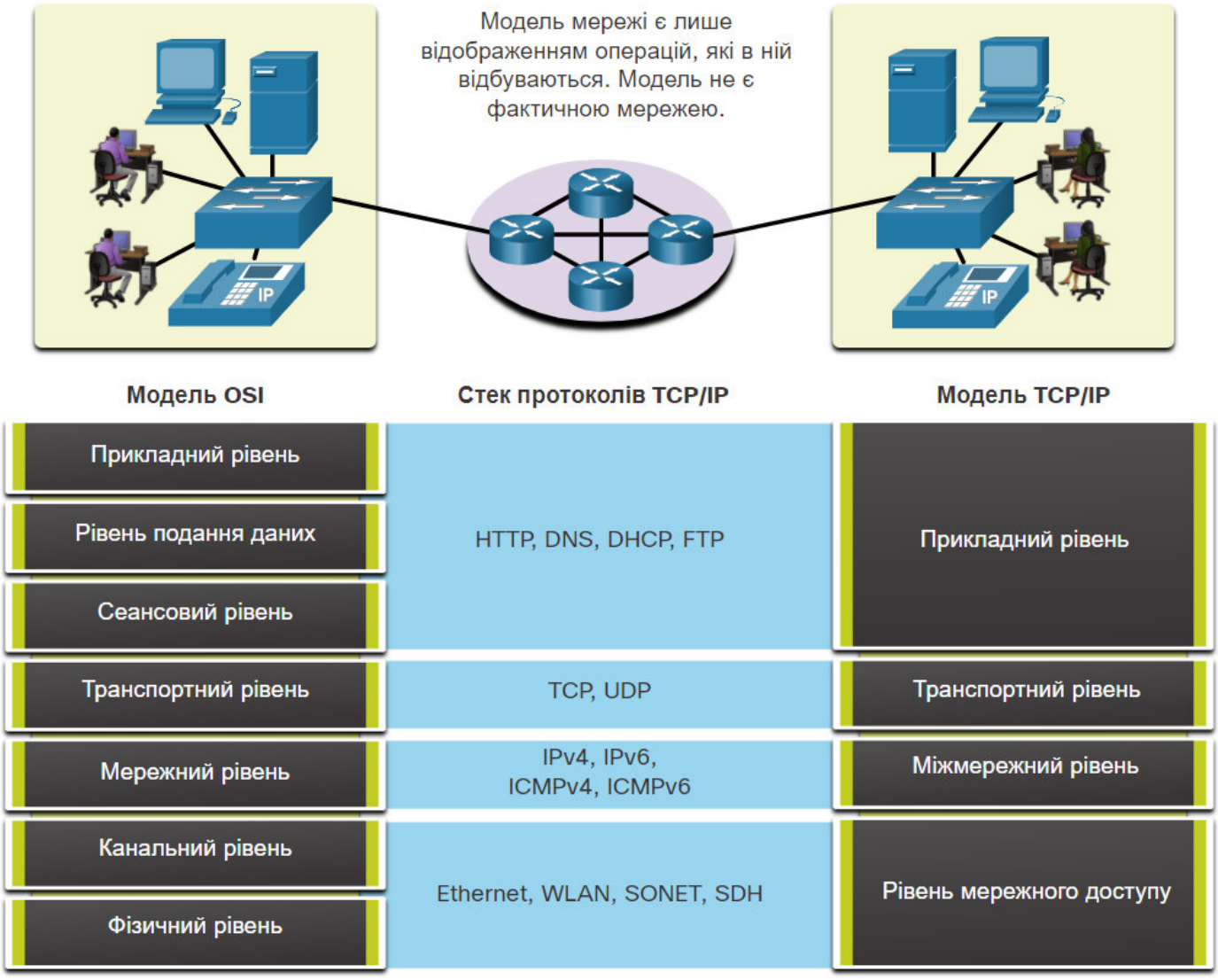
В реальному житті ви не можете спостерігати процес передачі повідомлення через реальну мережі так, як ви можете спостерігати процес збирання автомобіля на конвеєрі. Така ситуація змушує нас уявляти процес передачі. І в цьому випадку буде корисним використання моделі.

Функціонування мережі є складною концепцією, його досить важко пояснити та зрозуміти. З цієї причини для групування мережних операцій по керованих рівнях використовується багаторівнева модель.

Перевагами використання багаторівневої моделі для опису мережних протоколів і операцій є:

- 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.

На рисунку показано, що 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)



3.5.2. *Еталонна модель OSI*

Еталонна модель OSI надає великий перелік функцій і сервісів, які можуть бути присутніми на кожному рівні. Модель цього типу забезпечує узгодженість усіх типів мережних протоколів та

служб, описуючи, що необхідно зробити на певному рівні, але не визначаючи, як це потрібно виконати.

Ця модель також описує взаємодію кожного рівня з рівнями, які розташовані безпосередньо зверху та знизу. Протоколи TCP/IP, що розглядаються у цьому курсі, пов'язані як з моделлю OSI, так і моделлю TCP/IP. У таблиці наведена детальна інформація про рівні моделі OSI. Функціональність кожного рівня та взаємозв'язок між рівнями стануть більш очевидними протягом цього курсу, оскільки протоколи будуть розглянуті більш детально.

Рівні моделі OSI	Опис
7 - Прикладний рівень	Прикладний рівень містить протоколи, які використовуються для обміну даними між процесами
6 - Рівень подання даних	Рівень подання даних забезпечує загальне подання даних, які передається між службами прикладного рівня.
5 - Сеансовий рівень	Сеансовий рівень надає послуги для рівню подання даних для організації діалогу та організації діалогу та керування обміном даними.
4 - Транспортний рівень	Транспортний рівень визначає послуги сегментування, передачі та відновлення послідовності даних для індивідуального зв'язку а відновлення послідовності даних для індивідуального зв'язку між кінцевими пристроями.
3 - Мережний рівень	Мережний рівень надає послуги для обміну окремими блоками даних через мережу між визначеними кінцевими пристроями
2 - Канальний рівень	Протоколи канального рівня описують методи обміну кадрами даних між пристроями через загальне середовище передавання даних.
1 - Фізичний рівень	Протоколи фізичного рівня описують механічні, електричні, функціональні і процедурні засоби для активації, підтримки та деактивації фізичних з'єднань для передачі бітів пристроєм до мережі та прийняття бітів пристроєм з мережі.

Примітка: Варто відмітити, що для зазначення рівнів моделі TCP/IP, як правило, використовуються назви рівнів, а для зазначення рівнів моделі OSI частіше використовуються номери рівнів, ніж їх назви. Наприклад, фізичний рівень зазначається як перший рівень моделі OSI, канальний рівень - як другий рівень моделі OSI тощо.

3.5.3. Протокольна модель TCP/IP

Протокольна модель TCP/IP, як модель для міжмережного зв'язку була створена на початку 1970-х років. Іноді її називають моделлю мережі Інтернет. Модель цього типу тісно пов'язана зі структурою відповідного стеку протоколів. TCP/IP - протокольна модель, оскільки вона описує функції, які виконуються на кожному рівні стеку TCP/IP. TCP/IP також використовується як еталонна модель. У таблиці наведена детальна інформація про рівні моделі OSI.

Рівні моделі TCP/IP	Опис
4 - Прикладний	Відображення даних для користувача, а також забезпечення шифрування та керування сеансами зв'язку.

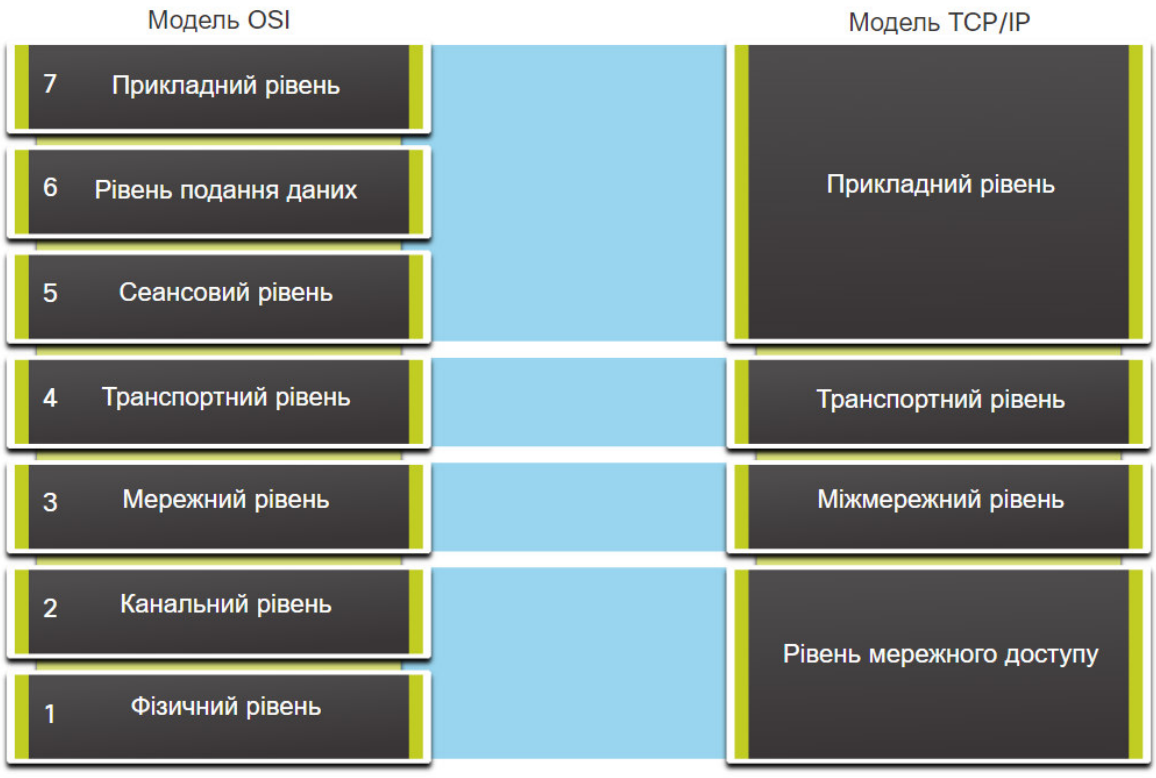
Рівні моделі TCP/IP	Опис
рівень	
3 - Транспортний рівень	Підтримка зв’язку між різними пристроями в різних мережах.
2 - Міжмережний рівень	Визначення найкращого маршруту передавання даних через мережу.
1 - Рівень мережного доступу	Керування фізичними пристроями та середовищем передавання даних, з яких складається мережа.

Визначення стандарту та протоколів TCP/IP обговорені на загальнодоступному форумі та описані в загальнодоступному набір документів RFC, виданих IETF. RFC створюються мережними інженерами і надсилаються іншим членам IETF для обговорення.

3.5.4. Порівняння моделей OSI і TCP/IP

Протоколи, що формують стек TCP/IP можуть бути описані з точки зору еталонної моделі OSI. 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. Він описує лише передавання з мережного рівня на фізичний рівень (для відповідних мережних протоколів). Рівні 1 і 2 моделі OSI описують необхідні процедури для доступу до середовища передавання даних та фізичні засоби, необхідні для надсилання даних через мережу.



Є велика схожість між транспортним і мережним рівнями. Однак дві моделі відрізняються тим, як ці рівні взаємодіють з вищим та нижчим прилеглими рівнями.

- Рівень 3 OSI (мережний рівень) повністю відповідає міжмережному рівню TCP/IP. Цей рівень використовується для опису протоколів, які адресують повідомлення та визначають маршрути передачі повідомлень між мережами.
- Рівень 4 OSI (транспортний рівень) повністю відповідає транспортному рівню TCP/IP. Цей рівень описує загальні служби та функції, які забезпечують впорядковану і надійну доставку даних між вузлом-відправником та вузлом-отримувачем.
- Прикладний рівень TCP/IP містить декілька протоколів, які забезпечують певні функціональні можливості для різних застосунків кінцевого користувача. Рівні 5, 6 і 7 моделі OSI є основою для розробників прикладного програмного забезпечення і постачальників у процесі створення програм, які працюють у мережах.
- Зазвичай, і модель TCP/IP, і модель OSI використовують при посиланні на протоколи різних рівнів. Оскільки модель OSI відокремлює канальний і фізичний рівні, її зазвичай використовують при посиланні на ці нижні рівні.

3.5.5. *Packet Tracer - Дослідження моделей TCP/IP і OSI*

Це завдання з моделювання є першим кроком на шляху до розуміння принципів роботи стеку TCP/IP і його взаємозв'язку з моделлю OSI. Режим симуляції дозволяє переглядати вміст повідомлень на кожному з рівнів при передаванні даних через мережу.

Під час передавання через мережу дані розбиваються на менші частини та ідентифікуються. Ці дії виконуються з метою відновлення порядку частин даних при надходженні до отримувача. Кожному блоку, відповідно до певних рівнів моделей TCP/IP та OSI, призначена власна назва. Як загальна назва блоку даних певного рівня застосовується термін Протокольний блок даних (Protocol data unit, PDU). Режим моделювання Packet Tracer дає можливість переглядати кожен рівень і пов'язані з ним PDU. Наступні кроки познайомлять користувача з процесом запиту веб-сторінки з веб-сервера за допомогою браузера на клієнтському ПК.

Незважаючи на те, що більшість поданої інформації детально розглядатиметься пізніше, це завдання дає можливість вивчити функціональність Packet Tracer і відтворити процес інкапсуляції.

Цілі та задачі

Частина 1: Вивчення веб-трафіку HTTP

Частина 2: Відображення складових стеку протоколів TCP/IP

Довідкова інформація

Це завдання з моделювання покликане сформувати засади для розуміння стеку протоколів TCP/IP і його взаємозв'язку з моделлю OSI. Режим симуляції дозволяє переглядати вміст даних на кожному рівні в процесі надсилання мережею.

Під час передавання по мережі дані розбиваються на менші частини та ідентифікуються з метою повторного збирання при надходженні до пункту призначення. Кожному блоку, відповідно до певних рівнів моделей TCP/IP та OSI, призначена власна назва. Режим моделювання Packet Tracer дає можливість переглядати кожен рівень і пов'язані з ним PDU. Наступні кроки познайомлять користувача з процесом запиту веб-сторінки з веб-сервера за допомогою браузера на клієнтському ПК.

Не зважаючи на те, що більшість поданої інформації детально розглядатиметься пізніше, це завдання дає можливість вивчити функціональність Packet Tracer і відтворити процес інкапсуляції.

Інструкції

Частина 1: Дослідження веб-трафіку протоколу HTTP

У Частині 1 цього завдання Ви використаєте Режим моделювання (Simulation mode) Packet Tracer (PT) для створення веб-трафіку та вивчення HTTP.

Крок 1: Перехід з режиму реального часу (Realtime) до режиму моделювання (Simulation mode).

У нижньому правому куті інтерфейсу Packet Tracer розміщені кнопки перемикання між режимами **Realtime** і **Simulation**. PT завжди запускається у режимі **Realtime**, у якому мережні протоколи оперують у реальних часових проміжках. Проте, можливості Packet Tracer дозволяють користувачеві "зупинити час" за допомогою перемикання до режиму моделювання. У цьому режимі пакети відображаються у вигляді конвертів, час керується подіями, а користувач може покроково проходити по мережних подіях.

a. Натисніть на піктограмі **Simulation** аби перемкнутися з режиму реального часу **Realtime** до режиму моделювання **Simulation**.

b. Оберіть **HTTP** у фільтрах переліку подій **(Event List Filters)**.

1) HTTP може бути єдиною подією, яка відображається. Якщо потрібно, натисніть на кнопку **Edit Filters** (Редагувати фільтри), яка знаходиться нижче панелі моделювання для відображення подій, доступних для перегляду. Додайте позначку для **Show All/None** (Показати все/Нічого) і зауважте, як перемикаються прапорці з позначеного на непозначений і навпаки, залежно від поточного стану.

2) Натискайте на прапорці **Show All/None** допоки не звільняться усі опції, і після цього оберіть **HTTP** у вкладці Misc (Різне) у вікні редагування фільтрів. Натисніть на X у верхньому правому куті для закриття вікна **Edit Filters**. У видимих подіях (Visible Events) зараз повинен відображатися тільки протокол HTTP.

3.6. Інкапсуляція даних

3.6.1. Сегментація повідомлень

Знання еталонної моделі OSI та моделі TCP/IP стане у нагоді, коли ви вивчатимете, як дані інкапсулюються під час їх передачі через мережу. Цей процес не такий простий як надсилання звичайного поштового листа.

Теоретично одне повідомлення (наприклад відеокліп або електронний поштовий лист), може бути надіслане через мережу від відправника до отримувача як один великий безперервний потік бітів. Але це створить проблеми для інших пристроїв, яким необхідно використовувати ті ж канали зв'язку. Великі потоки даних призводять до значних затримок. Крім того, якщо під час передавання повідомлення, будь-яка ланка в мереженої інфраструктури вийде з ладу, все повідомлення буде втрачено і його доведеться повністю повторно передавати.

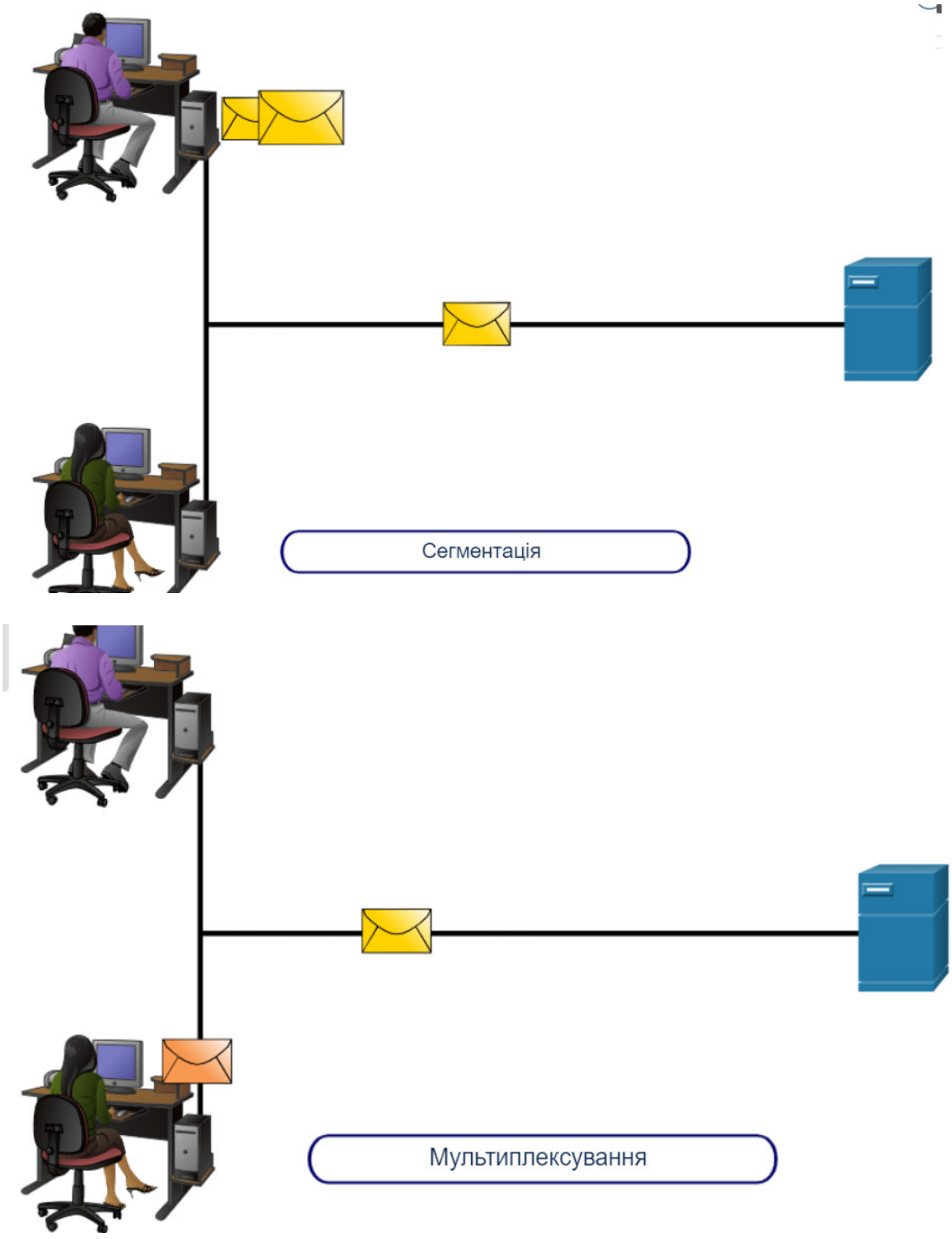
Кращим підходом для передавання даних через мережу є їх поділ на менші, керованіші частини. Сегментація - це процес поділу потоку даних на менші блоки для передавання через мережу. Сегментація необхідна, оскільки в мережах. побудованих на основі стеку TCP/IP, для передачі даних використовують окремі IP-пакети. Кожен пакет надсилається окремо, аналогічно до надсилання довгого листа як серії окремих листівок. Пакети, що містять сегменти для одного і того ж отримувача, можуть надсилатися різними шляхами.

Сегментація повідомлень надає дві головні 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. Це також дозволяє узгоджувати велику кількість різних обмінів даними у мережі - виконувати мультиплексування.

- **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.

Можна переглянути анімацію процесів сегментації та мультиплексування.



3.6.2. *Послідовність*

Використання сегментації та мультиплексування для передачі повідомлень через мережу підвищує рівень складності процесу передачі. Уявіть, якби вам довелося надіслати лист на 100 сторінок, але кожен конверт міг містити лише одну сторінку. Потрібно буде мати 100 конвертів, і кожен конверт доведеться підписувати окремо. Цілком можливо, що лист на 100 сторінок у 100 різних конвертах надійде адресатові в порядку відмінному від порядку відправлення. Тому інформація у

конверті повинна містити порядковий номер. Номери нададуть змогу отримувачеві зібрати сторінки в належному порядку.

В мережному зв'язку кожен сегмент повідомлення повинен бути опрацьованим аналогічно. Це дасть змогу переконатися, що він потрапить до правильного отримувача та отримувач зможе відновити вміст вихідного повідомлення, як показано на рисунку. Протокол TCP відповідає за формування послідовностей окремих сегментів.

3.6.3. Протокольні блоки даних

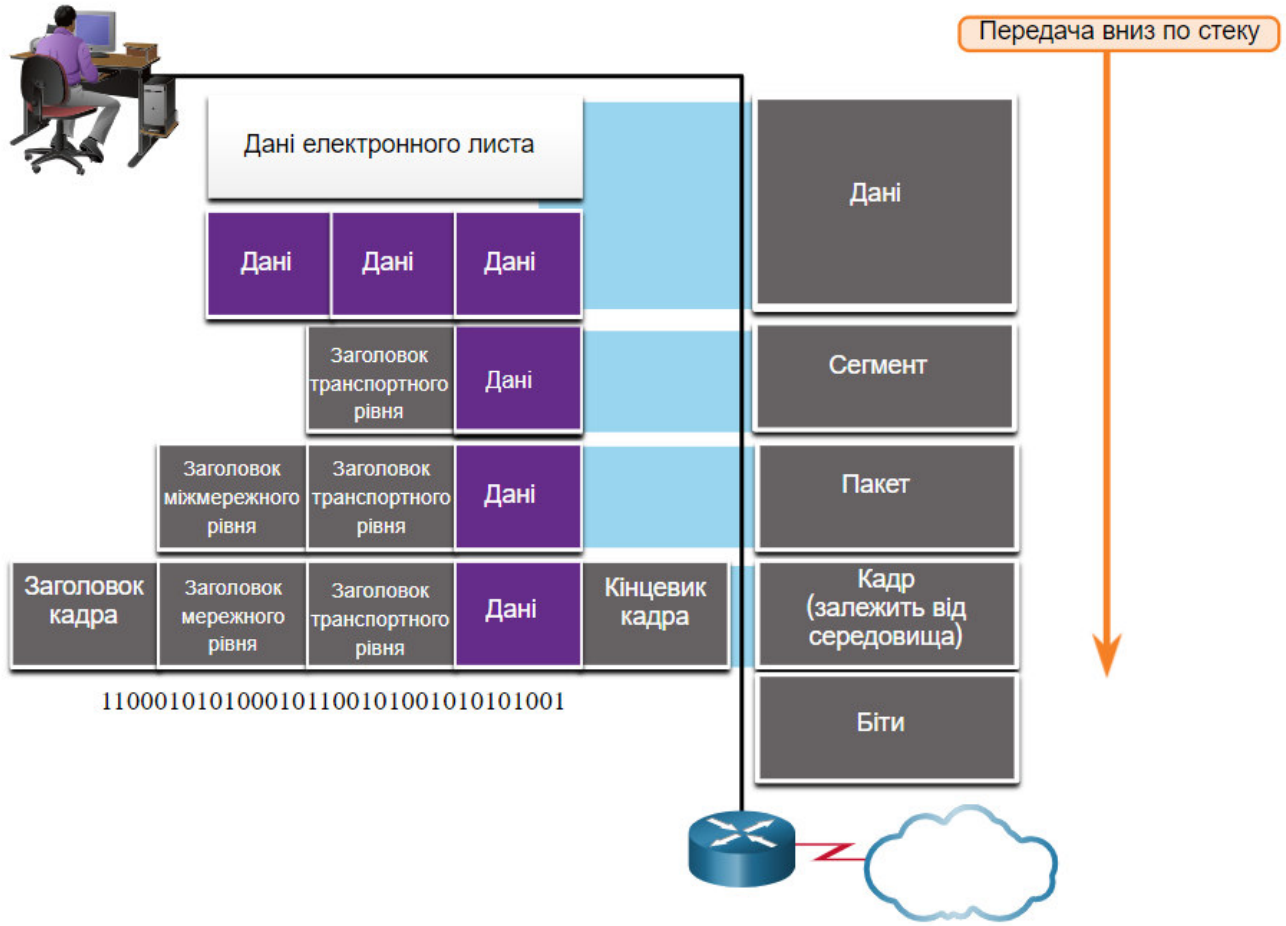
У міру того як дані додатків передаються по стеку протоколів для передавання через мережне середовище, на кожному з рівнів різні протоколи додають до них свою службову інформацію. Цей процес називається інкапсуляцією.

Примітка: Примітка: Хоча блок даних протоколу UDP називають дейтаграмою, IP-пакети іноді також називають IP-дейтаграмами.

Фрагмент даних з доданою службовою інформацією певного рівня називають Блоком даних протоколу (PDU, Protocol Data Unit). Під час інкапсуляції кожен рівень інкапсулює PDU, отриманий від вищого рівня, за правилами протоколу, що використовується на даному рівні. На кожному етапі цього процесу 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 для кожної форми даних наведені на рисунку.

На рисунку наведені протокольні блоки даних, що відповідають різним рівням моделі OSI. У верхній частині рисунку зображений користувач комп'ютера, який надсилає електронну пошту. Дані проходять зверху донизу по стеку TCP/IP і інкапсулюються в новий PDU на кожному рівні. Спочатку дані електронного листа поділяються на менші блоки. На наступному кроці перед заголовком даних додається заголовок транспортного рівня, і блок даних стає сегментом. Потім, перед заголовком транспортного рівня, додається заголовок міжмережного рівня і блок даних стає пакетом. Ще нижче додається заголовок кадру перед заголовком міжмережного рівня, за даними додається кінцевик кадру, і блок даних стає кадром (залежно від середовища). Кадр показаний як потік бітів, що отримується маршрутизатором, який підключений до хмари. Текст внизу читається як: Дані - Загальний термін для PDU, що використовується на прикладному рівні; Сегмент - PDU транспортного рівня; Пакет - PDU міжмережного рівня; Кадр- PDU канального рівня; Біти - PDU

фізичного рівня, що використовується для фізичного передавання даних через середовище. Примітка. Якщо заголовком PDU транспортного рівня є заголовок протоколу TCP, то це сегмент. Якщо заголовком PDU транспортного рівня є заголовок протоколу UDP, то це дейтаграма.



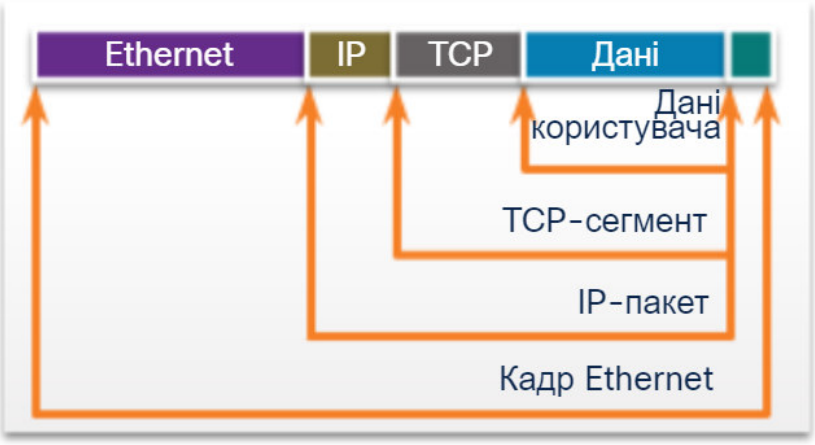
- Дані - загальний термін для PDU, який використовується на прикладному рівні.
- Сегмент - PDU транспортного рівня
- Пакет - PDU міжмережного рівня
- Кадр - PDU канального рівня
- Біти - це PDU фізичного рівня, який використовується під час фізичного передавання даних через середовище

Примітка: Примітка. Якщо заголовком PDU транспортного рівня є заголовок протоколу TCP, то це сегмент. Якщо заголовком PDU транспортного рівня є заголовок протоколу UDP, то це дейтаграма.

3.6.4. *Приклад інкапсуляції*

Коли повідомлення надсилається до мережі, процес інкапсуляції здійснюється від верху до низу. На кожному рівні інформація верхнього рівня розглядається як дані всередині PDU протоколу, який інкапсулює. Наприклад, TCP-сегмент вважається даними всередині IP-пакета.

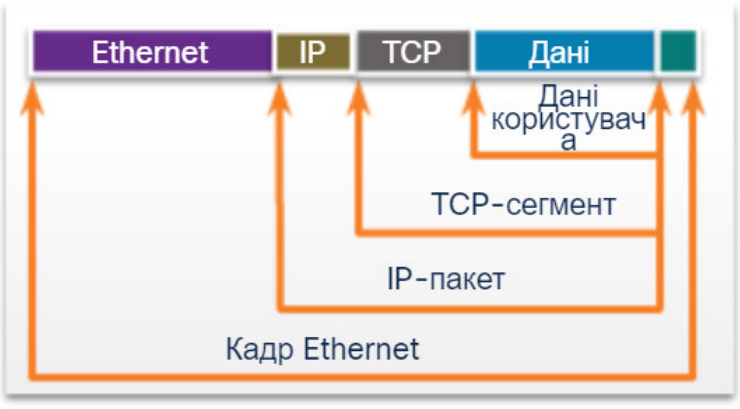
Попередньо ви вже бачили дану анімацію в цьому модулі. Натисніть Програвати, щоб побачити процес інкапсуляції для випадку, коли веб-сервер надсилає веб-сторінку веб-клієнту.

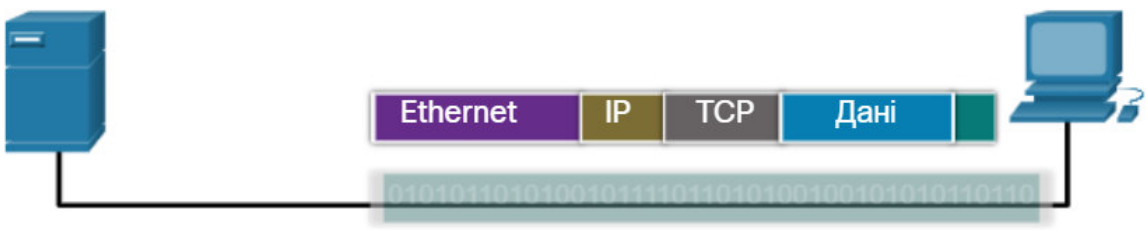


3.6.5. *Приклад деінкапсуляції*

На вузлі-отримувачі відбувається процес зворотний до інкапсуляції. Цей процес називають деінкапсуляцією. Деінкапсуляція - це процес видалення одного або декількох заголовків PDU, що виконується вузлом-отримувачем. Дані декапсулюються, переміщуючись догори по стеку до застосунку кінцевого користувача.

Попередньо ви вже бачили дану анімацію в цьому модулі. Натисніть "Програвати" та зосередьтесь на процесі де-інкапсуляції.





3.6.6. *Питання для самоперевірки - Інкапсуляція даних*

1. Як називається процес поділу великого потоку даних на менші частини перед відправкою?

- ◯ Послідовність
- ◯ Дуплексування
- ◯ Мультиплексування
- ◯ Сегментація

2. Який PDU є PDU транспортного рівня?

- ◯ Сегмент
- ◯ Пакет
- ◯ Біти
- ◯ Кадр

3. Який рівень стеку протоколів виконує інкапсуляцію даних у кадри?

- ◯ Канальний
- ◯ Транспортний
- ◯ Міжмережний
- ◯ Прикладний

4. Як називається процес додавання службової інформації протоколу до даних у процесі їх переміщення вниз по стеку протоколів?

- ◯ Деінкапсуляція
- ◯ Послідовність
- ◯ Сегментація
- ◯ Інкапсуляція

1. Як називається процес поділу великого потоку даних на менші частини перед відправкою?

- ◯ Послідовність
- ◯ Дуплексування
- ◯ Мультиплексування
- ◉ Сегментація

2. Який PDU є PDU транспортного рівня?

- ◉ Сегмент
- ◯ Пакет
- ◯ Біти
- ◯ Кадр

3. Який рівень стеку протоколів виконує інкапсуляцію даних у кадри?

- ◉ Канальний
- ◯ Транспортний
- ◯ Міжмережний
- ◯ Прикладний

4. Як називається процес додавання службової інформації протоколу до даних у процесі їх переміщення вниз по стеку протоколів?

- ◯ Деінкапсуляція
- ◯ Послідовність
- ◯ Сегментація
- ◉ Інкапсуляція

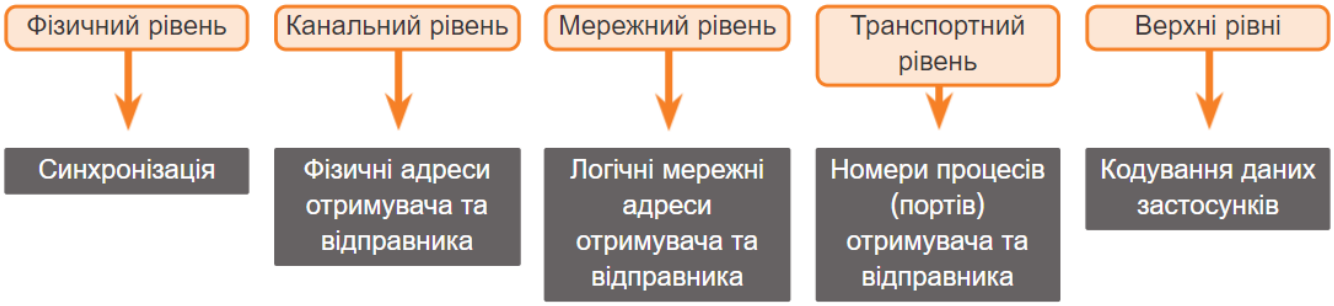
3.7. Доступ до даних

3.7.1. Адреси

Як ви вже знаєте, для передавання повідомлень через мережу необхідно виконувати їх сегментацію. Проте ці сегментовані повідомлення нікуди не потраплять, якщо ви виконати їх належну адресацію. Ця тема містить огляд мережних адрес. Також ви отримаєте можливість використати програму Wireshark, яка допоможе вам переглядати мережний трафік.

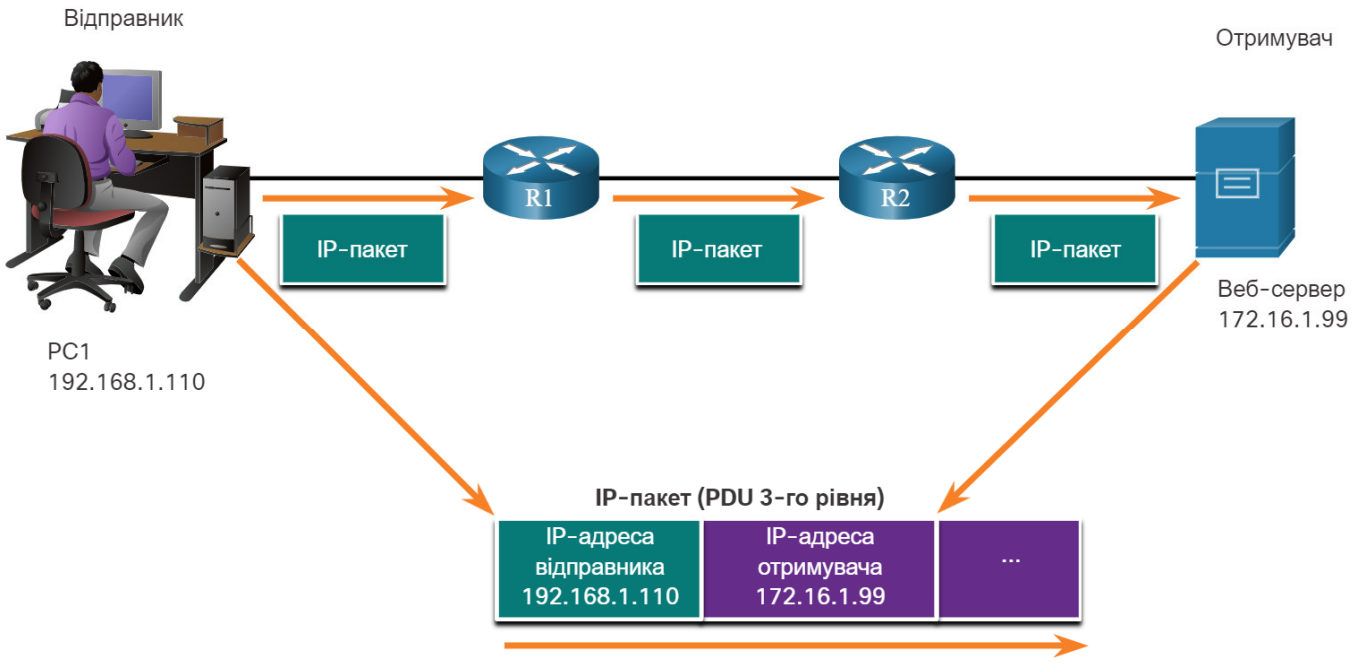
Мережний та канальний рівні відповідають за доставку даних від пристрою-відправника до пристрою- отримувача. На рисунку показано, що протоколи обох рівнів мають адреси відправника та отримувача, але ці адреси мають різне призначення.

- **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.



3.7.2. Логічна адреса 3-го рівня

IP-адреса - це логічна адреса мережного рівня (рівня 3) моделі OSI, що необхідна для доставки IP-пакета від відправника до отримувача, як показано на рисунку.



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.

IP-адреси однозначно ідентифікують відправника та отримувача пакета. Це твердження справедливе і для випадку, коли відправник і отримувач знаходяться в одній IP-мережі, і для випадку, коли відправник і отримувач знаходяться в різних IP-мережах.

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. Усі пристрої однієї IP-мережі повинні мати однакові мережні частини IP-адрес.
- **Вузлова частина (IPv4) або ідентифікатор інтерфейсу (IPv6)**- частина IP-адреси, яка знаходиться праворуч, яка ідентифікує конкретний пристрій у IP-мережі. Ця частина унікальна для кожного пристрою або інтерфейсу в мережі.

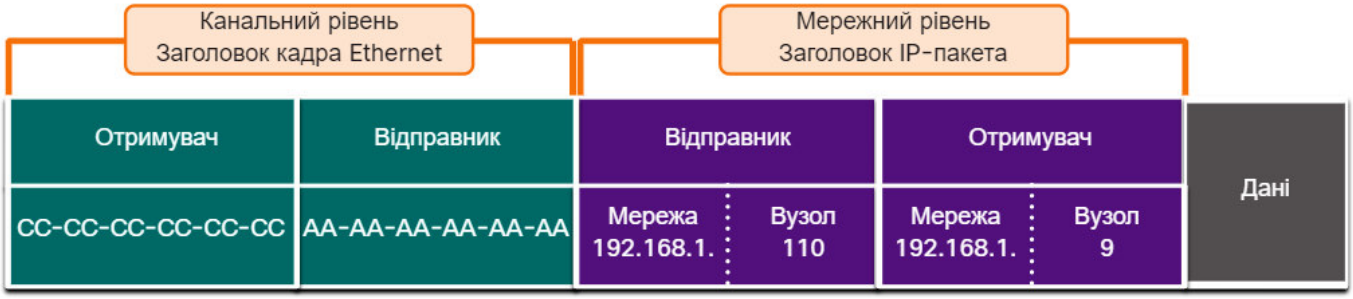
Примітка: Маска підмережі (IPv4) або префікс (IPv6) використовуються для ідентифікації мережної та вузлових частин IP-адреси.

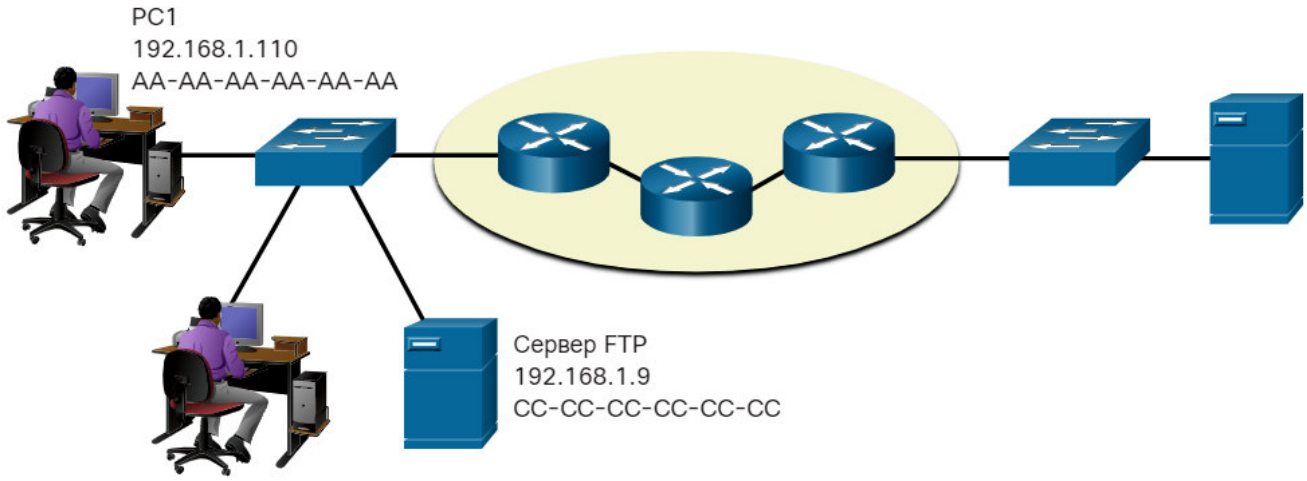
3.7.3. *Пристрої в одній мережі*

Прикладі містить клієнтський комп'ютер PC1, який спілкується з FTP-сервером у одній IP-мережі.

- **Source IPv4 address** - The IPv4 address of the sending device, the client computer PC1: 192.168.1.110
- **Destination IPv4 address** - The IPv4 address of the receiving device, FTP server: 192.168.1.9.

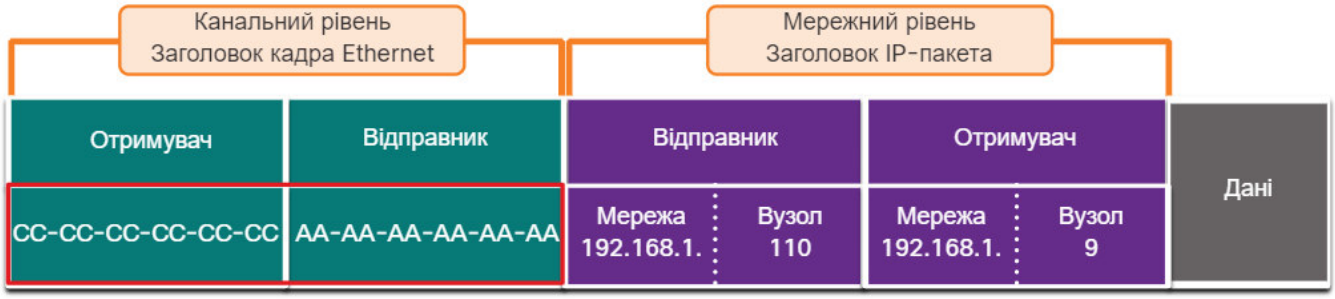
Зверніть увагу, що мережна частина IPv4-адреси відправника, та мережна частина IPv4-адреси отримувача належать одній мережі. Зверніть увагу, що мережна частина IPv4-адреси відправника, та мережна частина IPv4-адреси отримувача однакові, тому можна зробити висновок, що відправник та отримувач належать одній мережі

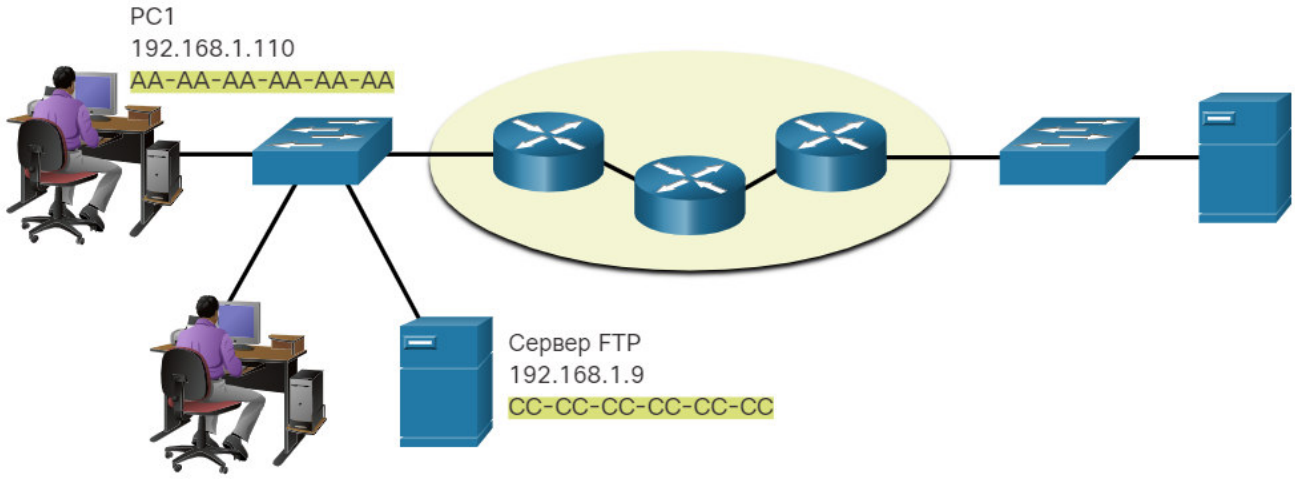




3.7.4. Роль адрес канального рівня для однієї IP-мережі

Коли відправник і отримувач IP-пакета знаходяться в одній мережі, кадр канального рівня передається безпосередньо на отримувачеві. У мережах Ethernet адреси канального рівня називають MAC-адресами (MAC, Media Access Control). Ці адреси на рисунку виділені кольором.





MAC-адреси також називають апаратними або фізичними адресами. Ці адреси фізично призначаються виробниками мережним платам (NIC, Мережний зв'язок Interface Card) Ethernet.

- **MAC-адреса відправника - адреса канального рівня або MAC-адреса Ethernet-пристрою, який надсилає кадр канального рівня із інкапсульованим IP-пакетом. MAC-адреса мережної плати Ethernet PC1 - AA-AA-AA-AA-AA-AA-AA, для запису використано шістнадцятковий формат.
- **Destination MAC address** - When the receiving device is on the same Мережний зв'язок as the sending device, this is the data link address of the receiving device. In this example, the destination MAC address is the MAC address of the FTP server: CC-CC-CC-CC-CC-CC, для запису використано шістнадцятковий формат.

Кадр з інкапсульованим IP-пакетом тепер може передаватися з PC1 безпосередньо до FTP-сервера.

3.7.5. Пристрої у віддаленій мережі

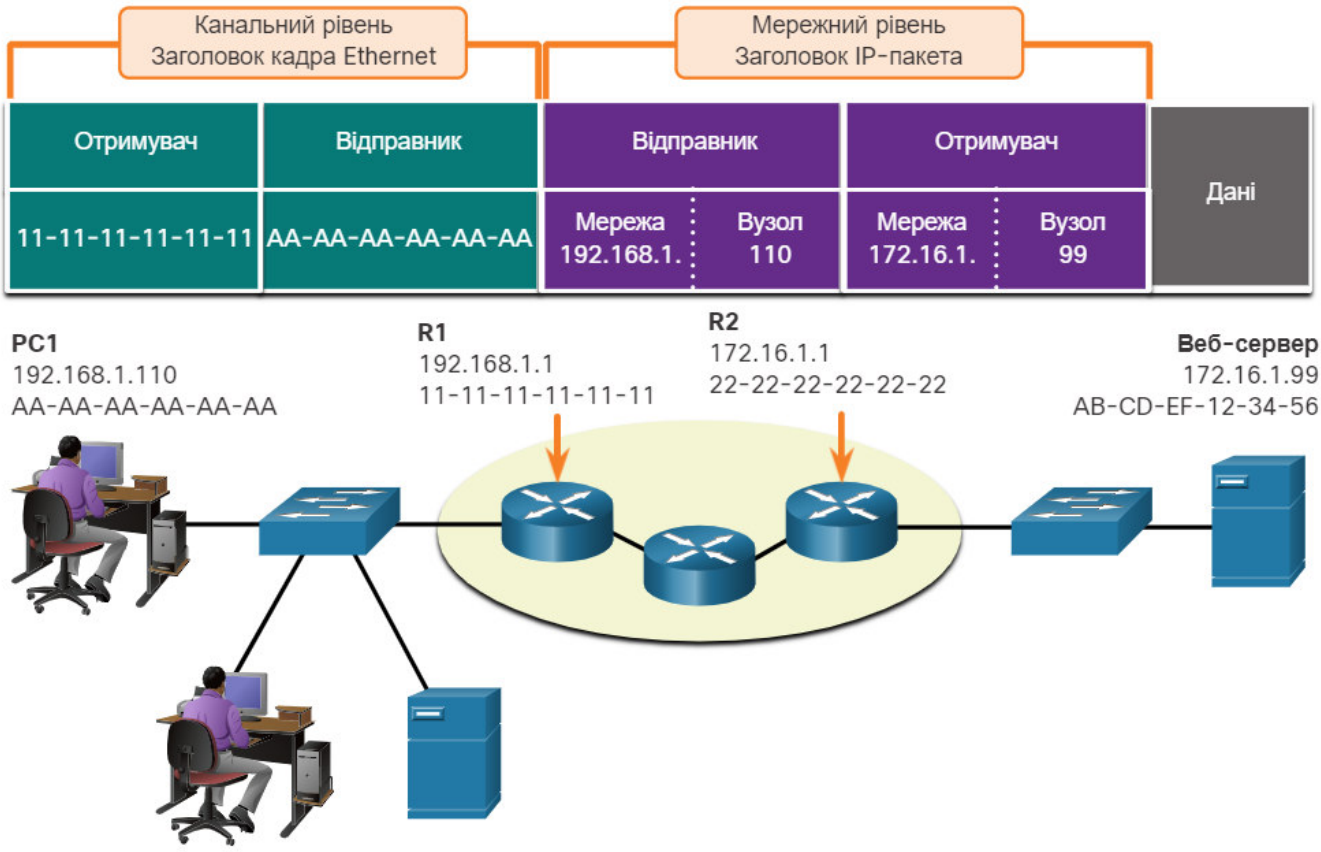
Постає питання, якими є ролі адрес мережного та канального рівнів, коли відбувається взаємодія пристрою локальної мережі з пристроєм віддаленої мережі? У цьому прикладі розглядається взаємодія клієнтського комп'ютера PC1 з сервером Web Server, який розміщений в іншій IP-мережі.

3.7.6. Роль адрес мережного рівня

Коли відправник пакета знаходиться в іншій мережі ніж отримувач, IP-адреси відправника та отримувача будуть представляти вузли у різних мережах. Це показуватиме мережна частина IP-адреси вузла-отримувача.

- **Source IPv4 address** - The IPv4 address of the sending device, the client computer PC1: 192.168.1.110
- **Destination IPv4 address** - The IPv4 address of the receiving device, the server, Web Server: 172.16.1.99.

Зверніть увагу, що мережна частина IPv4-адреси відправника, та мережна частина IPv4-адреси отримувача належать різним мережам.

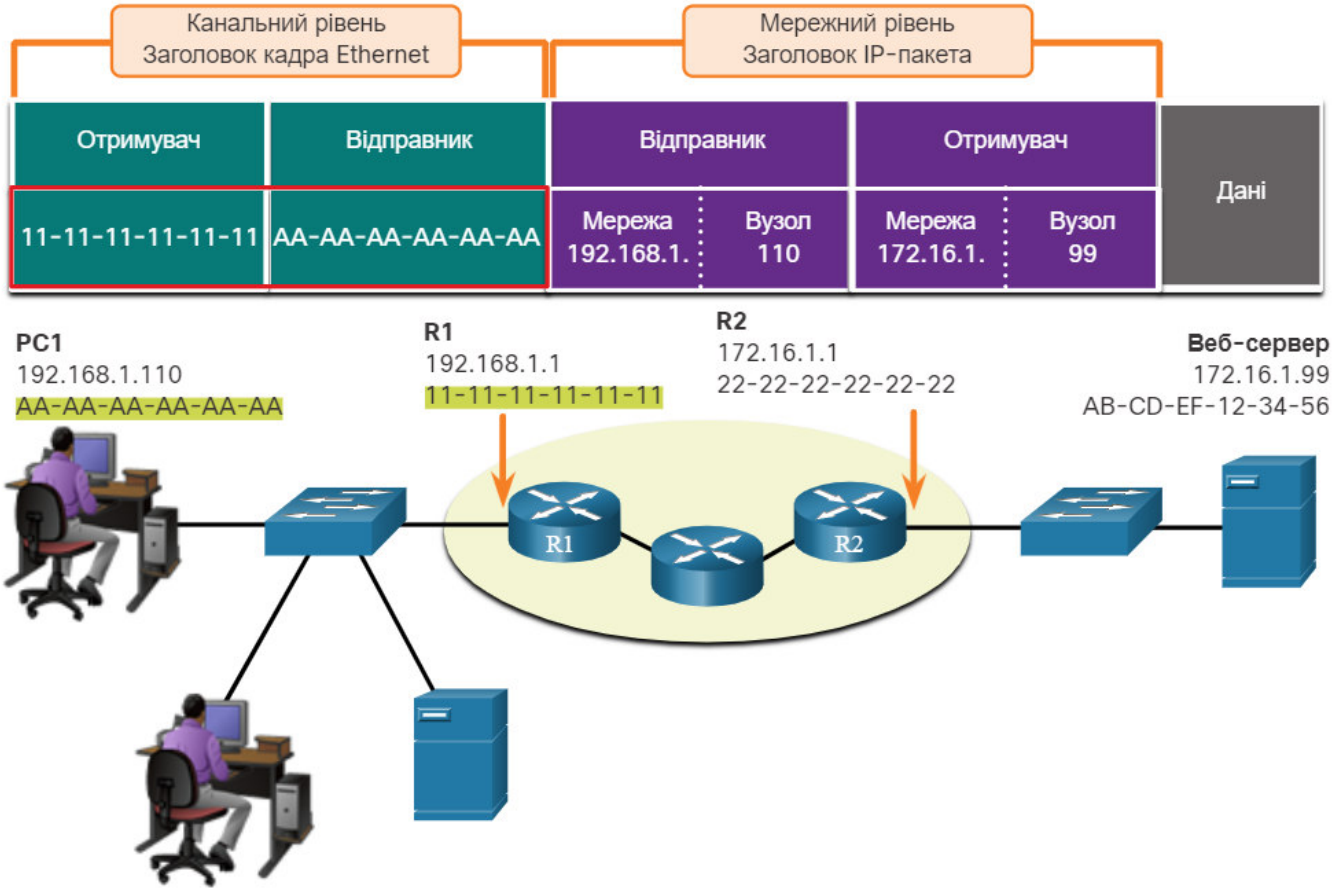


3.7.7. Роль адрес канального рівня для різних IP-мереж

Коли відправник і отримувач IP-пакету знаходяться в різних мережах, кадр канального рівня - кадр Ethernet не може бути надісланий безпосередньо до вузла-отримувача, оскільки вузол-отримувач безпосередньо недоступний у мережі вузла-відправника. Кадр Ethernet має бути надісланий на інший пристрій - маршрутизатор (шлюз за замовчуванням). Для цього прикладу шлюзом за замовчуванням є маршрутизатор R1. R1 має канальну адресу Ethernet і належить до тієї ж мережі, що і PC1. Це дозволяє PC1 безпосередньо взаємодіяти з цим маршрутизатором.

- **MAC-адреса відправника** - MAC-адреса мережної плати/мережного адаптера Ethernet вузла-відправника. MAC-адреса мережної плати Ethernet PC1 - AA-AA-AA-AA-AA-AA-AA.
- **MAC-адреса отримувача** - Якщо IP-адреса вузла-отримувача належить IP-мережі, відмінній від IP-мережі вузла відправника, то як MAC-адреса отримувача використовується MAC-адреса шлюзу за замовчування (маршрутизатора). У прикладі MAC-адреса призначення - це MAC-

адреса інтерфейсу Ethernet маршрутизатора R1 - 11-11-11-11-11-11. Це інтерфейс маршрутизатор, який підключений до тієї ж мережі, що і мережна плата PC1, як показано на рисунку.



Кадр Ethernet з інкапсульованим IP-пакетом тепер може бути переданий до маршрутизатора R1. R1 пересилає пакет до отримувача - сервера Web Server. Це може означати, що маршрутизатор R1 пересилає пакет на інший маршрутизатор або безпосередньо на веб-сервер, якщо отримувач знаходиться в мережі, підключеній до маршрутизатора R1.

Важливо, щоб IP-адреса шлюзу за замовчуванням була налаштована на кожному вузлі локальної мережі. Усі пакети для отримувачів, що розташовані у віддалених мережах, надсилаються до шлюзу за замовчуванням. Питання MAC-адрес Ethernet та шлюз за замовчуванням детальніше обговорюються в інших модулях.

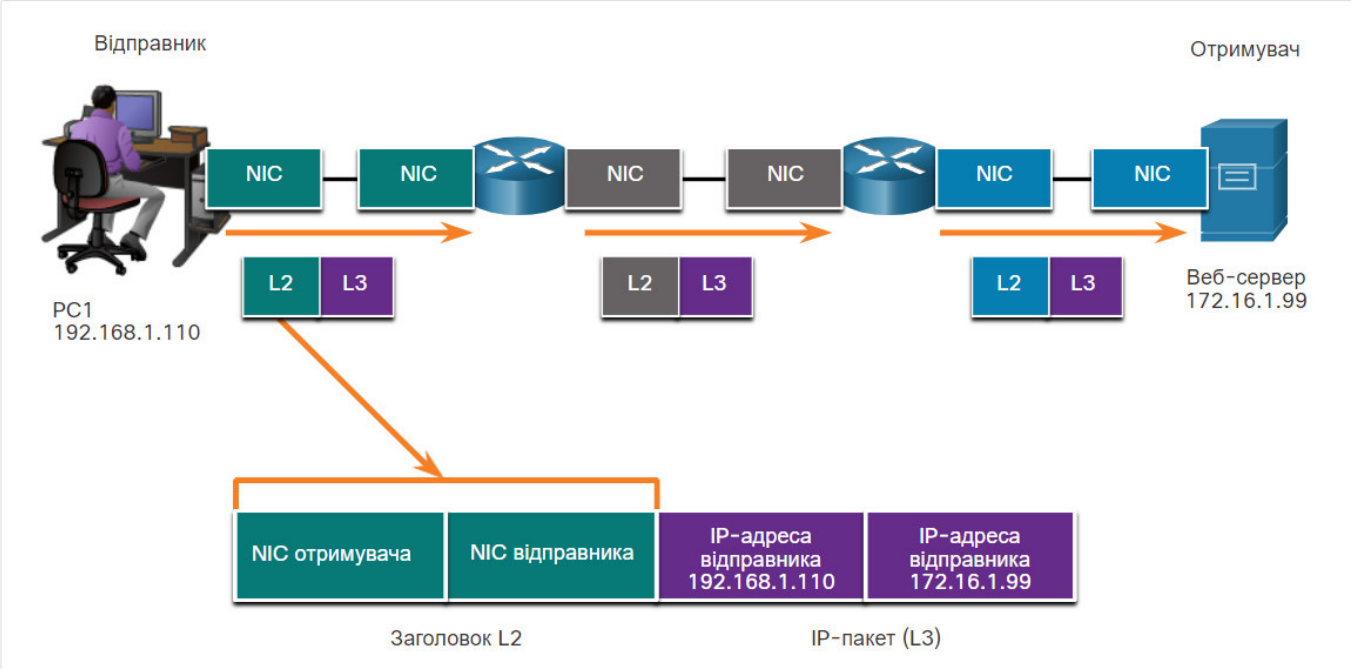
3.7.8. Канальні адреси

Канальні адреси (адреси рівня 2 моделі OSI), також називають фізичними або апаратними адресами. Вони мають різне застосування, залежно від конкретного випадку. Канальні адреси застосовуються з метою забезпечення передавання кадру з одного мережного інтерфейсу до іншого в одній і тій же мережі.

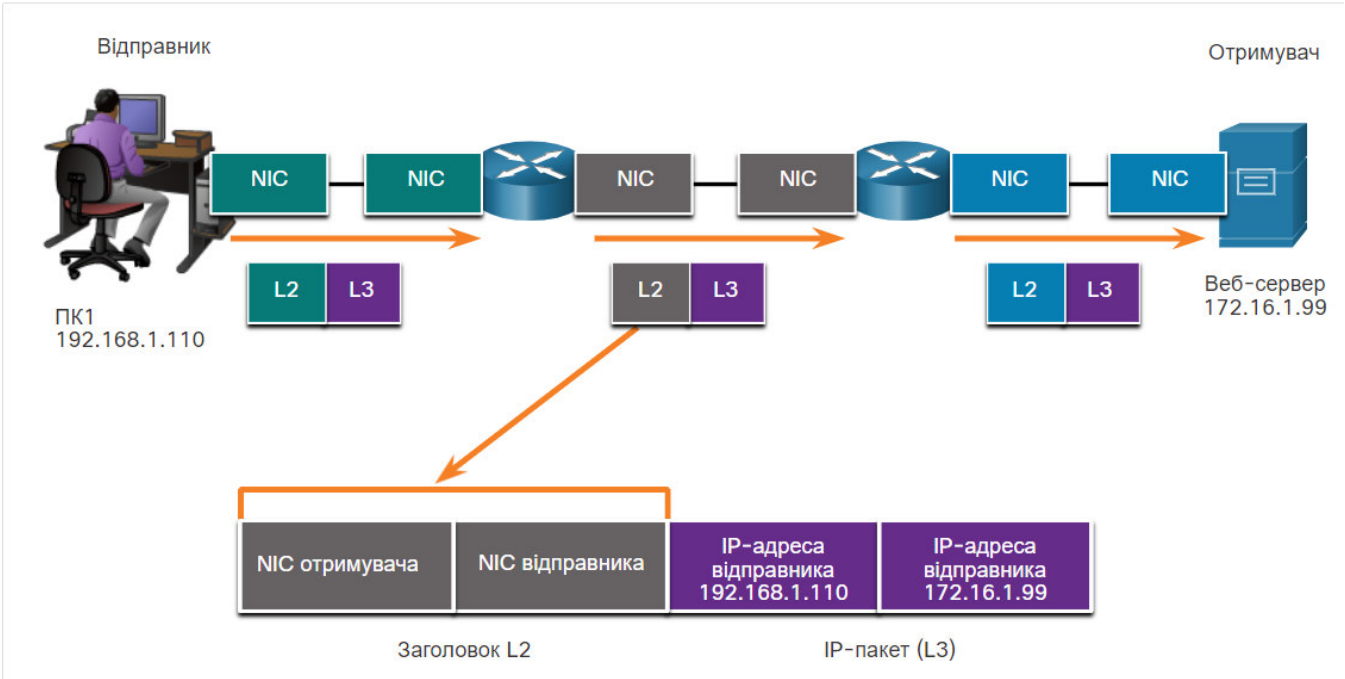
Перш ніж IP-пакет буде надіслано через дротову або бездротову мережу, його необхідно інкапсулювати у кадр канального рівня, щоб передати через фізичне середовище.

Натисніть на кожну кнопку, щоб переглянути ілюстрацію процесу змін канальних адрес на кожній ділянці маршруту від відправника до отримувача

Вузол - Маршрутизатор



Маршрутизатор - Маршрутизатор

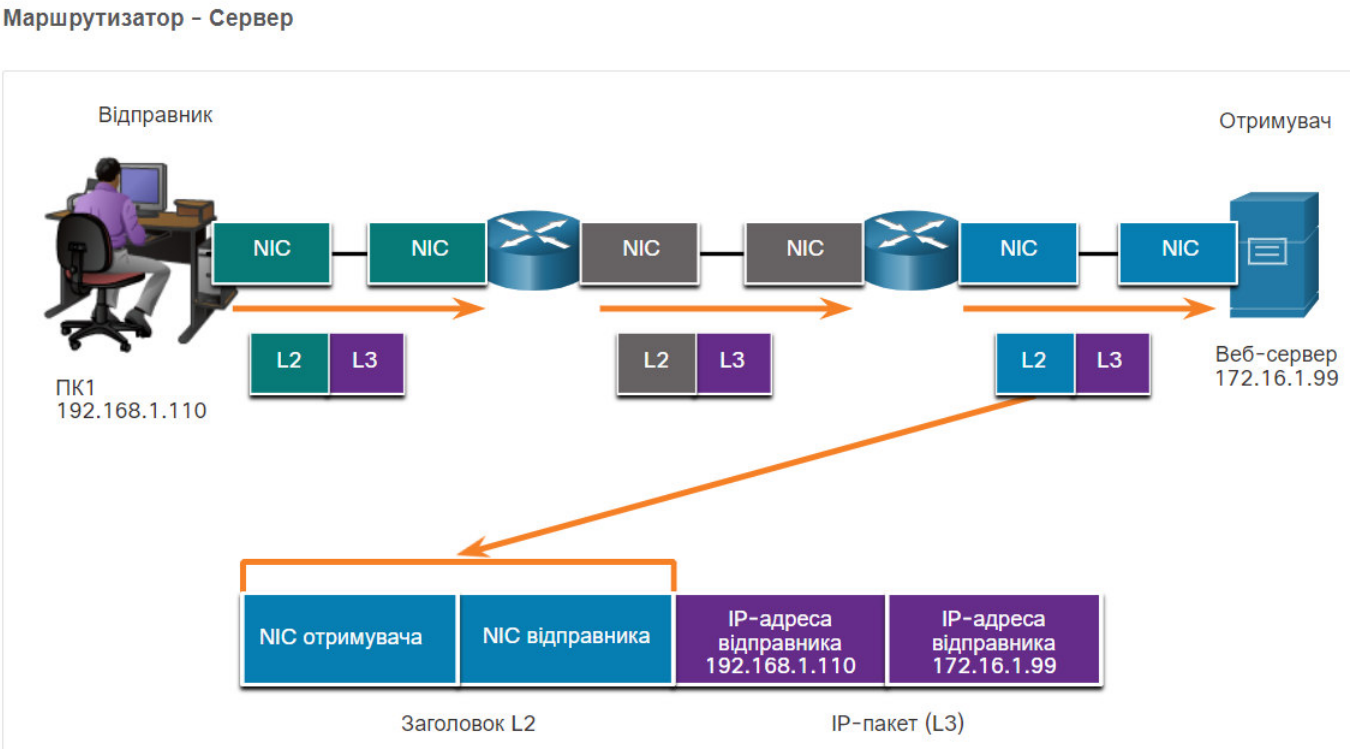


Передача IP-пакета здійснюється через ділянки комп'ютер-маршрутизатор, маршрутизатор-маршрутизатор, маршрутизатор- сервер, і в кожній точці на цьому шляху IP-пакет інкапсулюється до нового кадру. Кожен кадр містить адресу канального рівня мережної плати/інтерфейсу, що надсилає кадр, та адресу канального рівня мережної плати/інтерфейсу, що приймає кадр.

Протокол канального рівня (L2) застосовується для доставки пакету з однієї мережної плати/інтерфейсу до іншої в межах одній мережі. Маршрутизатор видаляє інформацію канального рівня (L2) при отриманні однією мережною платою/інтерфейсом, і додає нову інформацію канального рівня, перш ніж виконати пересилку з іншої мережної плати/інтерфейсу по маршруту до мережі призначення.

Кадр, що якого інкапсульовано IP-пакет, який містить такі дані канального рівня:

- **Адреса канального рівня вузла-відправника**- фізична адреса мережної плати/інтерфейсу пристрою, що надсилає кадр.
- **Адреса канального рівня вузла-отримуача**- фізична адреса мережної плати/інтерфейсу пристрою, який отримує кадр. Це може бути або адреса найближчого транзитного маршрутизатора або вузла-отримувача.



3.7.11. *Питання для самоперевірки - Доступ до даних*

Перевірте своє розуміння інкапсуляції даних, обравши НАЙКРАЩІ відповіді на наступні запитання.

1. Правда чи Неправда? Кадри, якими обмінюються пристрої, що належать до різних IP-мереж, повинні бути спрямовані до шлюзу за замовчуванням.

- ◯ Правда
- ◯ Неправда

2. Правда чи Неправда? Права частина IP-адреси використовується для ідентифікації мережі, до якої належить пристрій?

- ◯ Правда
- ◯ Неправда

3. Що використовується для визначення мережної частини IPv4-адреси?

- ◯ Маска підмережі
- ◯ MAC-адреса
- ◯ Права частина IP-адреси
- ◯ Ліва частина MAC-адреси

4. Які з перелічених нижче тверджень стосуються адрес мереженого та канального рівнів? (Оберіть три.)

- ☐ Адреси канального рівня це логічні адреси, а адреси мережного рівня це фізичні адреси.
- ☐ Адреси мережного рівня записуються за допомогою 12 шістнадцяткових цифр, а адреси канального рівня - десяткових.
- ☐ Адреси мережного рівня є логічними, а адреси канального записуються за допомогою 12 шістнадцяткових цифр.
- ☐ Адреси канального рівня це фізичні адреси, а адреси мережного рівня це логічні адреси.
- ☐ Адреси мережного рівня мають довжину 32 біти або 128 бітів.
- ☐ Адреси канального рівня мають довжину 32 біти.

5. Який порядок запису двох адрес у кадрі канального рівня?

- ◯ MAC-адреса відправника, MAC-адреса отримувача
- ◯ MAC-адреса отримувача, IP-адреса відправника
- ◯ IP-адреса отримувача, IP-адреса відправника
- ◯ MAC-адреса отримувача, MAC-адреса відправника
- ◯ IP-адреса отримувача, IP-адреса відправника

6. Правда чи Неправда? Адреси канального рівня це фізичні адреси, тому вони ніколи не змінюються при передаванні кадру від відправника до отримувача.

- ◯ Правда
- ◯ Неправда

---

1. Правда чи Неправда? Кадри, якими обмінюються пристрої, що належать до різних IP-мереж, повинні бути спрямовані до шлюзу за замовчуванням.

- ◉ Правда
- ◯ Неправда

2. Правда чи Неправда? Права частина IP-адреси використовується для ідентифікації мережі, до якої належить пристрій?

- ◯ Правда
- ◉ Неправда

3. Що використовується для визначення мережної частини IPv4-адреси?

- ◉ Маска підмережі
- ◯ MAC-адреса
- ◯ Права частина IP-адреси
- ◯ Ліва частина MAC-адреси

4. Які з перелічених нижче тверджень стосуються адрес мереженого та канального рівнів? (Оберіть три.)

- [ ] Адреси канального рівня це логічні адреси, а адреси мережного рівня це фізичні адреси.
- [ ] Адреси мережного рівня записуються за допомогою 12 шістнадцяткових цифр, а адреси канального рівня - десяткових.
- [x] Адреси мережного рівня є логічними, а адреси канального записуються за допомогою 12 шістнадцяткових цифр.
- [x] Адреси канального рівня це фізичні адреси, а адреси мережного рівня це логічні адреси.
- [x] Адреси мережного рівня мають довжину 32 біти або 128 бітів.
- [ ] Адреси канального рівня мають довжину 32 біти

- [ ] Адреси канального рівня мають довжину 32 біти.

5. Який порядок запису двох адрес у кадрі канального рівня?

- ( ) MAC-адреса відправника, MAC-адреса отримувача
- ( ) MAC-адреса отримувача, IP-адреса відправника
- ( ) IP-адреса отримувача, IP-адреса відправника
- (•) MAC-адреса отримувача, MAC-адреса відправника
- ( ) IP-адреса отримувача, IP-адреса відправника

6. Правда чи Неправда? Адреси канального рівня це фізичні адреси, тому вони ніколи не змінюються при передаванні кадру від відправника до отримувача.

- ( ) Правда
- (•) Неправда

3.8. Контрольна робота

3.8.1. Огляд розділу

Правила

Усі методи зв’язку мають три елементи: джерело повідомлення (відправник), призначення повідомлення (отримувач) та канал. Надсилання повідомлення регулюється правилами, які називаються *протоколами*. Протоколи повинні включати: ідентифікованого відправника та отримувача, загальну мову та граматику, швидкість та терміни доставки та вимоги щодо підтвердження чи підтвердження доставки повідомлення. Поширені комп'ютерні протоколи містять вимоги щодо кодування повідомлень, форматування та інкапсуляції, розміру, синхронізації та варіантів доставки. Кодування - це процес перетворення інформації в іншу прийнятну форму для передачі. Декодування - зворотний процес, в результаті якого інформація перетворюється в початковий вигляд. Формати повідомлень залежать від типу повідомлення та каналу, який використовується для доставки повідомлення. Синхронізація повідомлення включає в себе контроль потоку, час очікування відповіді та спосіб доступу. Варіанти доставки повідомлень включають одноадресні, багатоадресні та широкомовні розсилки.

Протоколи

Протоколи реалізуються кінцевими та проміжними пристроями програмно, апаратно або програмно- апаратно. Повідомлення, що надсилається через комп'ютерну мережу, зазвичай вимагає використання декількох протоколів, кожен з яких має свої функції та формат. Кожен мережний протокол має власну функції, формат повідомлення та правила зв'язку. Сімейство протоколів Ethernet включає IP, TCP, HTTP та багато інших. Протоколи, які захищають дані забезпечуючи автентифікацію, цілісність та шифрування даних: SSH, SSL та TLS. Протоколи, які дозволяють маршрутизаторам обмінюватися маршрутною інформацією, порівнювати інформацію записи про маршрути, а потім обирати найкращий маршрут до цільової мережі: OSPF та BGP. Протоколи, які використовуються для автоматичного виявлення пристроїв або служб: DHCP та DNS. Комп'ютери та мережні пристрої використовують узгоджені протоколи, які забезпечують такі функції: адресація, надійність, контроль потоку, послідовність, виявлення помилок та програмний інтерфейс.

Стеки протоколыв

Стек протоколів - це сукупність взаємозалежних протоколів, необхідних для виконання функції зв'язку. Стек протоколів показує, як реалізуються окремі протоколи з певного набору. Починаючи з 1970-х років існувало декілька різних наборів протоколів, деякі розроблені організаціями зі стандартизації, а інші розроблені різними виробниками обладнання та програмного забезпечення. Протоколи TCP/IP функціонують на прикладному, транспортному та міжмережному рівнях. TCP/IP - це набір протоколів, на базі якого побудовані сучасні комп'ютерні мережі та мережа Інтернет. TCP/IP пропонує два важливих аспекти для постачальників і виробників: відкритість та стандартизацію протоколів. Процес зв'язку за допомогою протоколів TCP/IP забезпечує наступне: веб-сервер інкапсулює та відправляє веб-сторінку клієнту, а також клієнт деінкапсулює веб-сторінку для відображення у веб-браузері.

Організації зі стандартизації

Відкриті стандарти сприяють сумісності, конкуренції та інноваціям. Організації зі стандартизації - це, зазвичай, незалежні некомерційні організацій, які створені для розробки і впровадження концепцій відкритих стандартів. Існує кілька організації, які виконують різні обов'язки щодо

просування та створення стандартів для Інтернету. До них належать: ISOC, IAB, IETF та IRTF. Організації зі стандартів, які розробляють та підтримують стек TCP/IP: ICANN та IANA. Організації, які розробляють та впроваджуються стандарти з електроніки та зв'язку: IEEE, EIA, TIA та ITU-T.

Еталонні моделі

Дві еталонні моделі, які використовуються для опису мережних операцій: OSI і TCP/IP. Модель OSI має сім рівнів:

7 - Прикладний рівень
6 - Рівень подання даних
5 - Сеансовий рівень
4 - Транспортний рівень
3 - Мережний рівень
2 - Канальний рівень
1 - Фізичний рівень

Модель TCP/IP має чотири рівні:

4 - Прикладний рівень
3 - Транспортний рівень
2 - Міжмережевий рівень
1 - Рівень мережного доступу

Інкапсуляція даних

Сегментація повідомлень надає дві основні переваги:

- Багато різних процесів передавання можуть чергуватися в мережі завдяки надсиланню менших окремих фрагментів від відправника до отримувача. Цей процес називається *мультиплексуванням*.
- Сегментація може підвищити ефективність мережних комунікацій. Якщо під час передачі великого повідомлення втрачено лише його частини, не потрібно повторно передавати все повідомлення, достатньо передати лише втрачені частини.

Протокол TCP відповідає за формування послідовностей окремих сегментів. Форма, яку фрагмент даних приймає на будь-якому рівні, називається *Протокольним блоком даних (PDU)*. Під час інкапсуляції кожен рівень інкапсулює PDU, отриманий від вищого рівня, за правилами протоколу, що використовується на даному рівні. Під час надсилання повідомлень у мережу процес інкапсуляції працює зверху вниз. На вузлі-отримувачі відбувається процес зворотний до інкапсуляції. Цей процес носить назву*деінкапсуляція*. Деінкапсуляція - це процес видалення одного або декількох заголовків PDU, що виконується вузлом-отримувачем. Дані декапсулюються, переміщуючись догори по стеку до застосунку кінцевого користувача.

Доступ до даних

Мережний та канальний рівні відповідають за доставку даних від пристрою-відправника до пристрою- отримувача. Протоколи обох рівнів мають адреси відправника та отримувача, але ці адреси мають різне призначення

- **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.

IP-адреси однозначно ідентифікують відправника та отримувача IP-пакета. IP-адреса містить дві частини: мережну частину (IPv4) або префікс (IPv6) та вузлову частину (IPv4) або ідентифікатор інтерфейсу (IPv6). Коли відправник і отримувач IP-пакету знаходяться в одній мережі, кадр канального ррівня передається безпосередньо до отримувача. У мережах Ethernet адреси канального рівня носять назву MAC-адреси (MAC, Media Access Control). Коли відправник і отримувач пакета знаходиться в різних мережах, то IP-адреса відправника та IP-адреси отримувача є адресами вузлів в цих мережах. Кадр Ethernet має бути надісланий на інший пристрій, відомий як маршрутизатор або шлюз за замовчуванням.

3.8.2. *Контрольна робота з розділу Протоколи та моделі*

1. Які три абревіатури є абревіатурами організації зі стандартизації? (Оберіть три.)

- [ ] IANA
- [ ] TCP/IP
- [ ] IETF
- [ ] MAC
- [ ] IEEE
- [ ] OSI

2. Який вид розсилки необхідно використати для передавання повідомлення всім пристроям локальної мережі?

- ◯ Широкомовна розсилка (broadcast)
- ◯ Одноадресна розсилка (unicast)
- ◯ Всеосяжна розсилка (Allcast)
- ◯ Багатоадресна розсилка (multicast)

3. З якою метою у комп'ютерному зв'язку застосовується кодування повідомлень?

- ◯ Для інтерпретації інформації
- ◯ Для поділу великих повідомлень на менші за розміром кадри
- ◯ Для переговорів про коректну синхронізацію з метою успішного спілкування
- ◯ Для перетворення інформації у відповідну форму для передачі

4. Який варіант доставки повідомлень використовується, щоб усі пристрої одночасно отримували однакове повідомлення?

- ◯ Широкомовна розсилка (Broadcast)
- ◯ Багатоадресна розсилка (Multicast)
- ◯ Дуплексна передача (Duplex)
- ◯ Одноадресна розсилка (Unicast)

5. Зазначте дві переваги використання багаторівневої мережної моделі. (Оберіть два.)

- ☐ Прискорення доставку пакетів.
- ☐ Допомога в розробці протоколів.
- ☐ Гарантія того, що пристрій одного рівня може функціонувати на наступному більш високому рівні.
- ☐ Перепони для розробників у створенні власних моделей.
- ☐ Запобігання впливу технологій одного рівні на інші рівні.

6. Для чого необхідні протоколи при передаванні даних?

- ◯ Зазначення пропускної здатності каналу або середовища для кожного типу зв'язку
- ◯ Надання правил, необхідних для певного типу зв'язку
- ◯ Диктування вмісту повідомлення, надісланого під час зв'язку
- ◯ Зазначення операційної системи пристрою, яка буде підтримувати зв'язок

7. Який логічна адреса використовується для доставки даних у віддалену мережу?

- ◯ MAC-адреса отримувача
- ◯ Номер порту отримувача
- ◯ IP-адреса відправника
- ◯ MAC-адреса відправника
- ◯ IP-адреса отримувача

8. Який загальний термін використовується для опису фрагмента даних на будь-якому рівні мережної моделі?

- ◯ Пакет (Packet)
- ◯ Протокольний блок даних (Protocol Data Unit)
- ◯ Сегмент (Segment)
- ◯ Кадр (Frame)

9. Які два протоколи функціонують на міжмережному рівні? (Оберіть дві.)

- ☐ POP
- ☐ BOOTP
- ☐ IP
- ☐ PPP
- ☐ ICMP

10. Який рівень моделі OSI визначає сервіси для сегментування і десегментування даних у процесі індивідуальної зв'язку між кінцевими пристроями?

- ◯ Мережний (Мережний зв'язок)
- ◯ Сеансовий (Session)
- ◯ Подання даних (Presentation)
- ◯ Транспортний (Transport)
- ◯ Прикладний (Application)

11. Який тип зв'язку застосовується для одночасного надсилання повідомлення групі вузлів?

- ◯ Групова розсилка (Anycast)
- ◯ Одноадресна розсилка (Unicast)
- ◯ Багатоадресна розсилка (Multicast)
- ◯ Широкомовна розсилка (Broadcast)

12. Який процес використовується для отримання переданих даних та перетворення їх у читабельне повідомлення?

- ◯ Керування потоком
- ◯ Декодування
- ◯ Інкапсуляція
- ◯ Контроль доступу

13. Які дії виконуються з IP-пакетом перед його передачею через фізичне середовище?

- ◯ До нього додається інформація, що гарантує надійну доставку.
- ◯ Він інкапсулюється в кадр канального рівня.
- ◯ Він інкапсулюється в TCP-сегмент.
- ◯ Він сегментується на дрібніші частини.

14. Який процес використовується для розміщення одного повідомлення всередині іншого повідомлення для подальшого передавання від відправника до отримувача?

- ◯ Контроль доступу
- ◯ Декодування
- ◯ Керування потоком
- ◯ Інкапсуляція

15. Веб-клієнт надсилає запит на веб-сторінку до веб-сервера. Яким є правильний порядок стеку протоколів (з точки зору клієнта), що використовується для підготовки запиту на передавання?

- ◯ Ethernet, TCP, IP, HTTP
- ◯ Ethernet, IP, TCP, HTTP
- ◯ HTTP, TCP, IP, Ethernet
- ◯ HTTP, IP, TCP, Ethernet