Тема. Модель ISO/OSI и стек протоколів TCP/IP як стандарт побудови корпоративних комп'ютерних мереж

1.1. Еталонна модель взаємодії відкритих систем OSI

Еталонна модель взаємодії відкритих систем OSI (Open System Interconnect Reference Model,) - це універсальний стандарт, який описує взаємодію комп'ютерів через комп'ютерну мережу (КМ). За допомогою цієї моделі складна і багатогранна задача взаємодії віддалених робочих станцій КМ представляється сукупністю простіших підзадач, кожна з яких вирішується своїм модулем (програмним або апаратним ресурсом).

Модель складається з 7-ми рівнів, кожен з яких виконує строго визначені функції, і може взаємодіяти тільки зі своїми сусідами й виконувати відведені тільки йому функції (рис. 1.1). Зауважимо, що це є саме еталонна модель, з якою порівнюються стеки протоколів будь-яких сучасних комп'ютерних мереж, які мають на теперішній момент від 4 до 7 рівнів (модулів), реалізованих програмним або апаратним чином.

Прикладний рівень (Application layer)

Верхній прикладний рівень моделі забезпечує взаємодію мережі і користувача. Рівень дозволяє додаткам користувача, таким як обробник запитів до баз даних, доступ до файлів, пересилку повідомлень електронної пошти, доступ до мережевих служб. Також він відповідає за передачу службової інформації, надає додаткам інформацію про помилки і формує запити до рівня представлення.

Представницький рівень (Presentation layer)

Цей рівень відповідає за перетворення форматів даних і кодування/декодування даних. Запити програм, отримані із прикладного рівня, він перетворює в стандартний формат повідомлення для передачі мережею, а отримані з мережі дані перетворює у формат, зрозумілий відповідному сервісу програм. На цьому рівні може здійснюватися стиснення/розпакування або кодування/декодування даних, а також перенаправлення запитів іншому мережевому ресурсу, якщо вони не можуть бути оброблені локально.

Рисунок 1.1 - Рівні моделі OSI

Сеансовий рівень (Session layer)

Цей рівень відповідає за підтримку сеансу зв'язку, дозволяючи застосуванням взаємодіяти між собою тривалий час. Рівень керує створенням/завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу в періоди неактивності застосувань. Синхронізація передачі забезпечується розміщенням у потоці даних контрольних точок, починаючи з яких відновлюється процес при порушенні взаємодії.

Транспортний рівень (Transport layer)

Транспортний рівень призначений для доставки даних без помилок, втрат і дублювання в тій послідовності, в якій вони були передані. При цьому немає значення, які дані передаються, звідки й куди, тобто він визначає сам механізм передачі. Блоки даних повідомлення він розділяє на сегменти, розмір яких залежить від протоколу, що використовується, або налаштуваннями каналу. Крім того, при прийомі даних з мережі пакети об’єднуються в єдине повідомлення, яке і передається через порти на вищі рівні. Протоколи цього рівня призначені для взаємодії типу point-to-point.

Мережевий рівень (Network layer)

Мережевий рівень моделі OSI, призначений для визначення маршруту передачі даних через комунікаційне середовище мережі. Відповідає за трансляцію логічних адрес і імен у фізичні, визначення найкоротших маршрутів, комутацію і маршрутизацію пакетів, відстеження проблем і перевантажень у мережі. На цьому рівні працює такий мережевий пристрій, як маршрутизатор.

Канальний рівень (Data Link layer)

Цей рівень призначений для забезпечення взаємодії мереж на фізичному рівні і контролю за помилками, які можуть виникнути. Отримані із фізичного рівня дані він упаковує в кадри даних, перевіряє на цілісність, якщо потрібно,

виправляє помилки і відправляє на мережевий рівень. Канальний рівень може взаємодіяти з одним або декількома фізичними рівнями, контролюючи і керуючи цією взаємодією. Для локальних мереж цей рівень представлено 2 підрівнями - MAC (Media Access Control), який регулює доступ до розподіленого фізичного середовища, та LLC (Logical Link Control), який забезпечує управління передачею між модулями. На цьому рівні працюють комутатори, мости і мережеві адаптери.

MAC-підрівень забезпечує коректне спільне використання загального середовища, надаючи його в розпорядження тієї або іншої станції мережі. Також він додає адресну інформацію до фрейму, позначає початок і кінець фрейму.

Рівень LLC відповідає за достовірну передачу кадрів даних між вузлами, а також реалізує функції інтерфейсу з мережевим рівнем. Також він здійснює ідентифікування протоколу мережевого рівня.

У програмуванні цей рівень представляє драйвер мережевої карти, в операційних системах є програмний інтерфейс взаємодії канального і мережевого рівнів між собою, це не новий рівень, а просто реалізація моделі для конкретної ОС. Приклади таких інтерфейсів: NDIS, ODI.

Фізичний рівень (Physical layer)

Найнижчий рівень моделі призначений безпосередньо для передачі потоку даних. Здійснює передачу електричних або оптичних сигналів у кабель і відповідно їх приймання і перетворення в біти даних відповідно до методів кодування цифрових сигналів, тобто здійснює інтерфейс між мережевим носієм і мережевим пристроєм. На цьому рівні працюють концентратори і повторювачі (ретранслятори) сигналу. Фізичний рівень визначає електричні, механічні, процедурні і функціональні специфікації для середовища передачі даних, у тому числі роз'єми, розпаювання і призначення контактів, рівні напруги, синхронізацію зміни напруги, кодування сигналу.

Цей рівень приймає кадр даних від канального рівня, представляє його в тій послідовності сигналів, які потім передаються в лінію зв'язку. Передача кадру даних через лінію зв'язку вимагає від фізичного рівня визначення таких елементів: тип середовища передачі (проводовий або безпроводовий, мідний кабель або оптичне волокно) і відповідних конекторів; як повинні бути представлені біти даних у середовищі передачі; як кодувати дані; якими повинні бути схеми приймача і передавача.

В сучасних мережах використовуються три основних типи середовища передачі: мідний кабель (copper), оптичне волокно (fiber) та бездротове середовище передачі (wireless). Тип сигналу, за допомогою якого здійснюється передача даних, залежить від типу середовища передачі. Для мідного кабелю сигнали, що представляють біти даних, є електричними імпульсами, для оптичного волокна - імпульсами світла. У випадку використання безпроводових з'єднань сигнали є радіохвилями (електромагнітними хвилями).

Коли пристрій, що працює на фізичному рівні, кодує біти кадру в сигнали для конкретного середовища передачі, він має розрізняти кадри. Тобто позначати, де закінчується один кадр і починається інший. Інакше мережеві пристрої, що здійснюють прийом сигналів, не зможуть визначити, коли кадр буде отриманий

повністю. Відомо, що початок і кінець кадру позначається на канальному рівні, але в багатьох технологіях фізичний рівень також може додати спеціальні сигнали, що використовуються тільки для позначення початку і кінця кадру даних.

Технології фізичного рівня визначаються стандартами, що розробляються такими організаціями: The International Organization for Standardization (ISO), The Institute of Electrical and Electronics Engineers (IEEE), The American National Standards Institute (ANSI), The International Telecommunication Union (ITU), The Electronics Industry Alliance/Telecommunications Industry Association (EIA/TIA), тощо. Дані стандарти охоплюють чотири області, що належать фізичному рівню: фізичні та електричні властивості середовища передачі, механічні властивості (матеріали, розміри, розпайка контактів конекторів), кодування (представлення бітів сигналами), визначення сигналів для керування інформацією. Всі компоненти апаратного забезпечення, такі, як мережеві карти (Network interface card, NIC), інтерфейси і конектори, матеріали кабелів та їх конструкція визначаються стандартами фізичного рівня. Слід зазначити, що функції фізичного рівня вбудовані в мережеве обладнання (hardware).

Основними функціями фізичного рівня є: фізичні компоненти, кодування даних, передача даних. Фізичні компоненти — електронне обладнання, середовище передачі і конектори, через які передаються сигнали, що представляють біти даних.

Кожний з описаних рівнів визначається сервісом, який він надає розташованому вище рівню, і протоколом - набором правил і форматів даних для взаємодії між собою об’єктів одного рівня, що працюють на різних комп’ютерах (рис. 1.2).

Дані, які обробляються на кожному рівні, мають різний формат і називаються протокольними блоками даних PDU (Protocol Data Unit).

При передачі кожний рівень приєднує до PDU, що надходить з верхнього рівня, службову інформацію у вигляді заголовку певної структури. Цей процес називається інкапсуляцією. Процес продовжується до досягнення самого нижнього рівня (фізичного рівня або рівня доступу до мережі), з якого дані передаються на мережевий пристрій. У пристрої одержувача відбувається зворотній процес, деінкапсуляція даних на кожному рівні. Потім додаток, нарешті, використовує дані. Процес продовжується, поки всі дані не будуть передані і отримані.

Вся складна процедура мережевої взаємодії може бути поділена на деяку кількість простіших процедур, що послідовно виконуються об’єктами певних рівнів моделі. Модель побудована таким чином, що об’єкти одного рівня двох

взаємодіючих комп’ютерів взаємодіють безпосередньо один з одним за допомогою відповідних протоколів, не знаючи, які рівні розташовані нижче і які функції вони виконують. Задача кожного з рівнів полягає в наданні через стандартизований інтерфейс певного сервісу модулю розташованого вище рівня, скориставшись, в разі необхідності, сервісом, який надає даному об’єкту нижче розташований рівень.

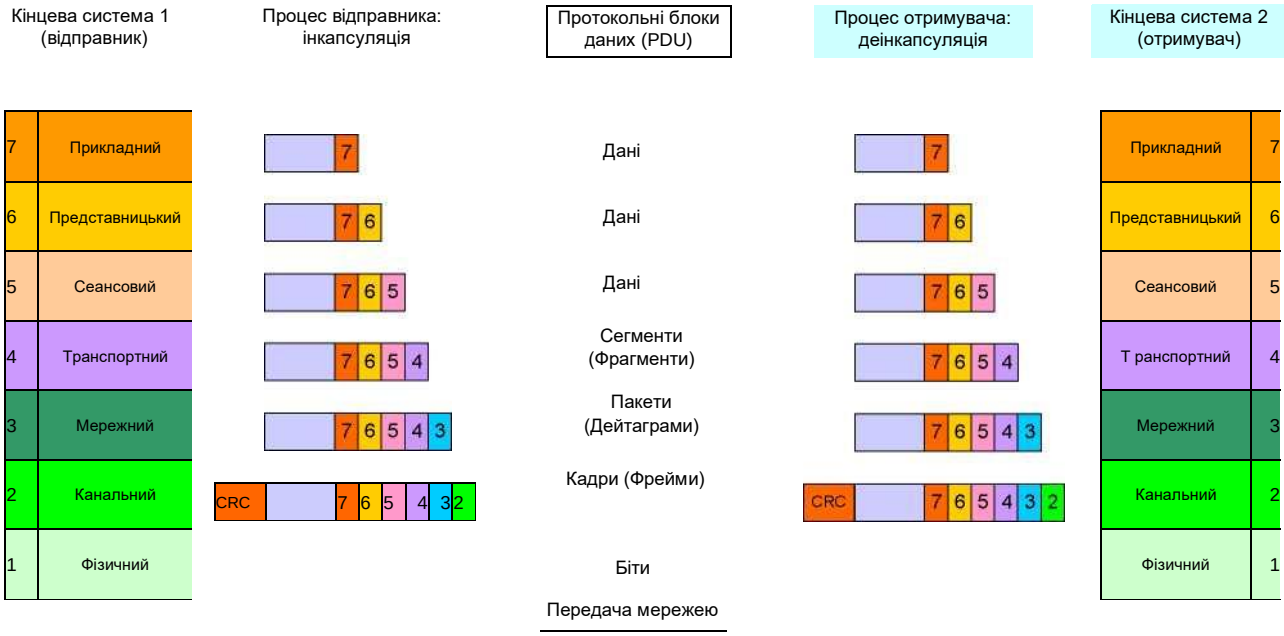

Рисунок 1.2 - Потоки даних від верхніх рівнів до нижніх. Інкапсуляція і деінкапсуляція

Наприклад, деякий процес відправляє дані через мережу процесу, що знаходиться на іншому комп'ютері. Через стандартизований інтерфейс процес- відправник передає дані нижньому рівню, який надає процесу сервіс для пересилки даних, а процес-отримувач через такий же стандартизований інтерфейс отримує ці дані від нижнього рівня. При цьому ні один із процесів не знає, як саме здійснює передачу даних протокол нижнього рівня, скільки ще рівнів знаходиться під ним, яке фізичне середовище передачі даних і яким шляхом дані передаються.

Ці процеси, з іншого боку, можуть знаходитися не на самому верхньому рівні моделі. Припустимо, що вони через стандартний інтерфейс взаємодіють із застосуваннями вище розташованого рівня і їхня задача (сервіс, що надається)- перетворення даних, а саме фрагментація і збирання великих блоків даних, які вище розташовані застосування відправляють один одному. При цьому сутність цих даних і їх інтерпретація для процесів, що розглядаються, абсолютно не важливі.

Можлива також взаємозаміна об'єктів одного рівня (наприклад, при зміні способу реалізації сервісу) таким чином, що об'єкт вище розташованого рівня не помітить заміни.

Об'єкти, які виконують функції рівнів, можуть бути реалізовані в програмному, програмно-апаратному або апаратному вигляді. Як правило, чим нижче рівень, тим більша частка апаратної частини в його реалізації.

Модулі усіх рівнів, що функціонують в одній технічній системі, взаємодіють за допомогою інтерфейсів, а однойменні модулі, що функціонують у різних технічних системах, взаємодіють за допомогою протоколів(рис. 1.3).

Мережнонезалежні протоколи

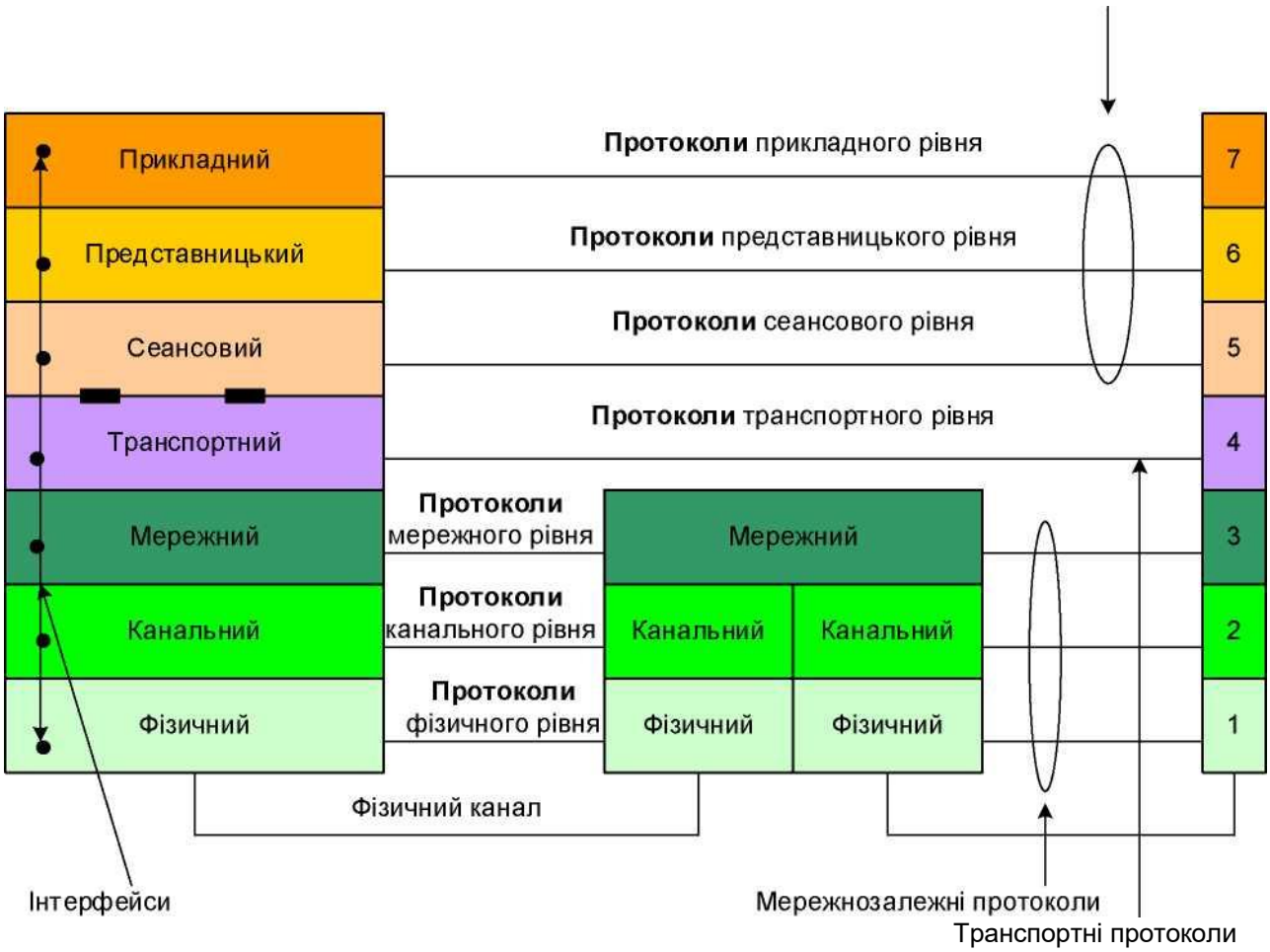

Рисунок 1.3 - Інтерфейси і протоколи

1.2. Інкапсуляція і обробка пакетів

При передачі повідомлення від прикладного рівня до фізичного для введення в мережу модуль кожного рівня додає до блоку даних, отриманого з сусіднього, верхнього рівня, свою службову інформацію у вигляді відповідного заголовку і, в разі необхідності, кінцевика (CRC), який додається в кінець блоку. Ця операція називається інкапсуляцією даних і відбувається на модулях кожного рівня стеку протоколів. Службова інформація призначається для об’єкту однойменного рівня на віддаленій робочій станції,; її формат і інтерпретація визначаються протоколом даного рівня.

Зрозуміло, що блоки, які надходять з сусіднього верхнього рівня, можуть містити службову інформацію більш високих рівнів, тобто вже бути інкапсуль ованими.

Процедура інкапсуляції в комп’ютерних мережах — це метод побудови модульних мережевих протоколів, коли логічно незалежні функції мережі абстрагуються від нижче розташованих механізмів шляхом включення цих механізмів у вище розташовані об’єкти.

Загальна процедура інкапсуляції представлена на рис. 1.4.

В ряді випадків, блок даних може не передаватись на самий верхній прикладний рівень, оскільки даний модуль є не модулем кінцевої обробки, а

тільки проміжним (комунікаційним вузлом на маршруті між відправником і отримувачем. У цьому випадку протокол відповідного рівня при аналізі службової інформації виявить, що блок даних на цьому рівні адресований не йому (хоча з точки зору нижніх рівнів він був адресований саме цьому комп'ютеру). Тоді протокол виконає необхідні дії для перенаправлення пакету до місця призначення або поверне відправнику з повідомленням про помилку, але в будь-якому випадку він не буде передавати дані на верхній рівень.

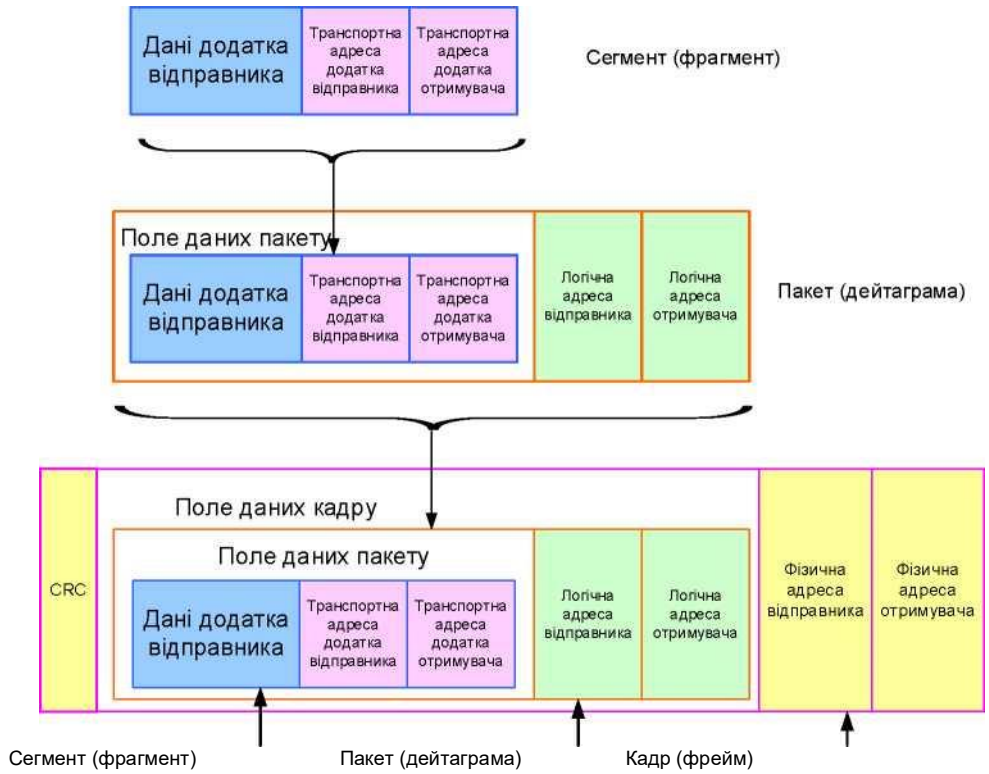

Рисунок 1.4 - Загальна процедура інкапсуляції

1.3. Стек протоколів TCP/IP

На відміну від еталонної моделі OSI, модель TCP/IP або модель DOD (Department of Defense) значною мірою більше орієнтується на забезпечення мережевої взаємодії, ніж на жорстке розділення функціональних рівнів.

Реалізація стеку протоколів TCP/IP фірми Microsoft відповідає чотирирівневій моделі замість семирівневої моделі, як показано на рисунку 1.5. При цьому прикладний рівень, який і реалізує відповідний прикладний сервіс, виконує сукупність функцій, а саме: формування повідомлення, представлення його в необхідному форматі, активізацію або створення необхідних портів процесів та підтримку їх (в разі необхідності) в активному стані протягом всього сеансу зв'язку. Кожен модуль моделі TCP/IP виконує більшу кількість функцій порівняно з моделлю OSI, внаслідок чого і зменшується кількість рівнів до чотирьох.

Рисунок 1.5 - Стек протоколів TCP/IP

Особливості TCP/IP:

- відкриті стандарти протоколів, що розробляються незалежно від програмного та апаратного забезпечення;
- незалежність від фізичного середовища передачі;
- унікальна система адресації;
- стандартизовані протоколи високого рівня для реалізації сервісів користувача.

Терміни, що використовуються для визначення блоків даних, які передаються, різні при використанні різних протоколів транспортного рівня - TCP і UDP (рис. 1.6).

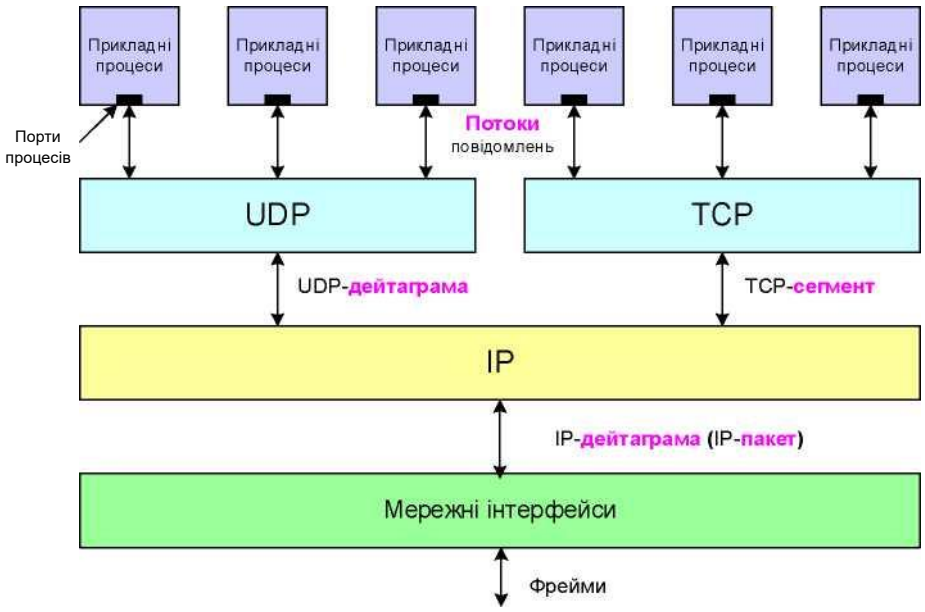

Рисунок 1.6 - Назви блоків даних, що обробляються протоколами різних рівнів

Обробка повідомлення, сформованого прикладним сервісом, при передачі в канал через стек протоколів TCP/IP принципово не відрізняється від такої ж обробки в еталонній моделі OSI. Особливості передачі повідомлення стосуються тільки протоколів, які оброблюють прийняту з більш високого рівня блоку даних та формату службової інформації (заголовку), з якою працює відповідний ресурс.

В мережі Інтернет використовуються три типи адрес, кожна з яких застосовуються відповідними модулями стеку протоколів. Кожна технічна система в мережі TCP/IP визначається адресами (ідентифікаторами) трьох типів, які використовуються модулями різних рівнів.

- **Символьний ідентифікатор-ім'я (символьна адреса)**, що призначається адміністратором і складається з декількох частин: ідентифікатора станції, імені організації, ідентифікатора домену. Це ім'я, яке також називають ***доменним*** іменем або ***DNS-іменем***, використовується на прикладному рівні, наприклад, у протоколах FTP, telnet та інших. Прикладами символьних адрес можуть служити microsoft.com, g.com.ua тощо.
- **Логічна адреса - IP-адреса** призначається адміністратором у момент підключення до мережі та конфігурування комп'ютерів і маршрутизаторів. IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання. Логічна адреса є адресою **програмного** забезпечення і використовується для передачі потоку повідомлень мережею.
- **Фізична (локальна) адреса** вузла залежить від технології, за допомогою якої побудована окрема мережа чи її сегмент, в яку входить даний вузол. Для вузлів, що входять у локальні мережі, - це **MAC-адреса** (Medium Access Control або Media Access Control) мережного адаптера або порту маршрутизатора або іншого технічного вузла,

наприклад, 11:AO:17:3D:BC:O1. Фізична адреса є адресою **апаратного** забезпечення конкретного вузла, яка використовується при прийомі даних

(або їх передачі) з каналу передачі в конкретну технічну систему (або видачі підготовлених даних з вихідного інтерфейсу системи в канал).

Загальна структура інкапсуляції, представлена на рис. 1.4 для стеку протоколів TCP/IP, відрізняється тільки форматами службової частини (заголовком) блоків даних кожного рівня, які залежать від типу протоколу, що використовується в конкретному випадку.

Наприклад, в якості транспортної адреси відправника та отримувача використовуються порти процесів (з додатковими параметрами передачі в разі обробки за допомогою протоколу TCP або без таких параметрів при використанні протоколу UDP). На мережевому рівні при формуванні пакету (дейтаграми) в якості логічної адреси використовується IP-адреса відправника та отримувача (32-бітної в разі застосування протоколу IPv4 або 128-бітної в разі застосування протоколу IPv6). На рівні канальних інтерфейсів в якості фізичної адреси кадру (фрейму) зазвичай використовується 48-бітна MAC-адреса, що застосовується в багатьох протоколах Ethernet (стандарти IEEE 802.2 та IEEE 802.3), Token Ring, FDDI, WI-FI (стандарт IEEE 802.11) та інших, структура якої наведена на рис. 1.7. Унікальний 24-бітний ідентифікатор OUI (Organizationally Unique Identifier) надається реєстраційним підрозділом IEEE (Registration Authority Committee), а 24-бітна адреса NIC визначає ідентифікатор даного модуля у виробника.

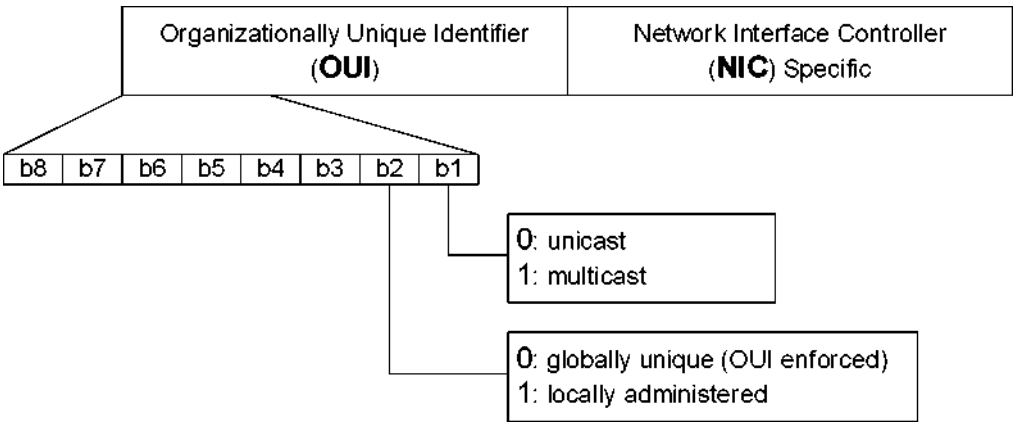

Рисунок 1.7 - Структура MAC-адреси

На сьогодні більшість мережевих протоколів канального рівня використовують один з трьох просторів MAC-адрес, які управляються IEEE: MAC-48, EUI-48 та EUI-64. Розширений ідентифікатор EUI-48 (Extended Unique Identifier) використовується для інших типів апаратного та програмного забезпечення (наприклад, мережевих протоколів). Інститут IEEE вважає термін MAC-48 застарілим і розглядається як окремий випадок використання ідентифікатора EUI-48 для стандартів IEEE 802.x та інших.

В подальшому виробники та інші організації повинні використовувати визначення EUI-48. Ідентифікатори MAC-48 і EUI-48 ідентичні при самостійному використанні, але є деякі особливості при їх інкапсуляції в EUI-

64.

Розширений ідентифікатор EUI-64 використовується в мережах FireWire, а також у протоколі IPv6 в якості молодших 64 біт у мережевій адресі вузла.

Ідентифікатор інтерфейсу в форматі EUI-64 складається з трьох частин:

• 24-бітний OUI на основі MAC-адреси клієнта, в якому сьомий біт є зворотним, тобто якщо 7-й біт має значення 0, він стає 1, і навпаки;

• в середину вставляється 16-бітне значення:

- FFFE (в шістнадцятковій системі числення) для OUI-48;
- FFFF для MAC-48;

• 24-бітний ідентифікатор пристрою на основі MAC-адреси клієнта.