

Модель OSI та TCP/IP

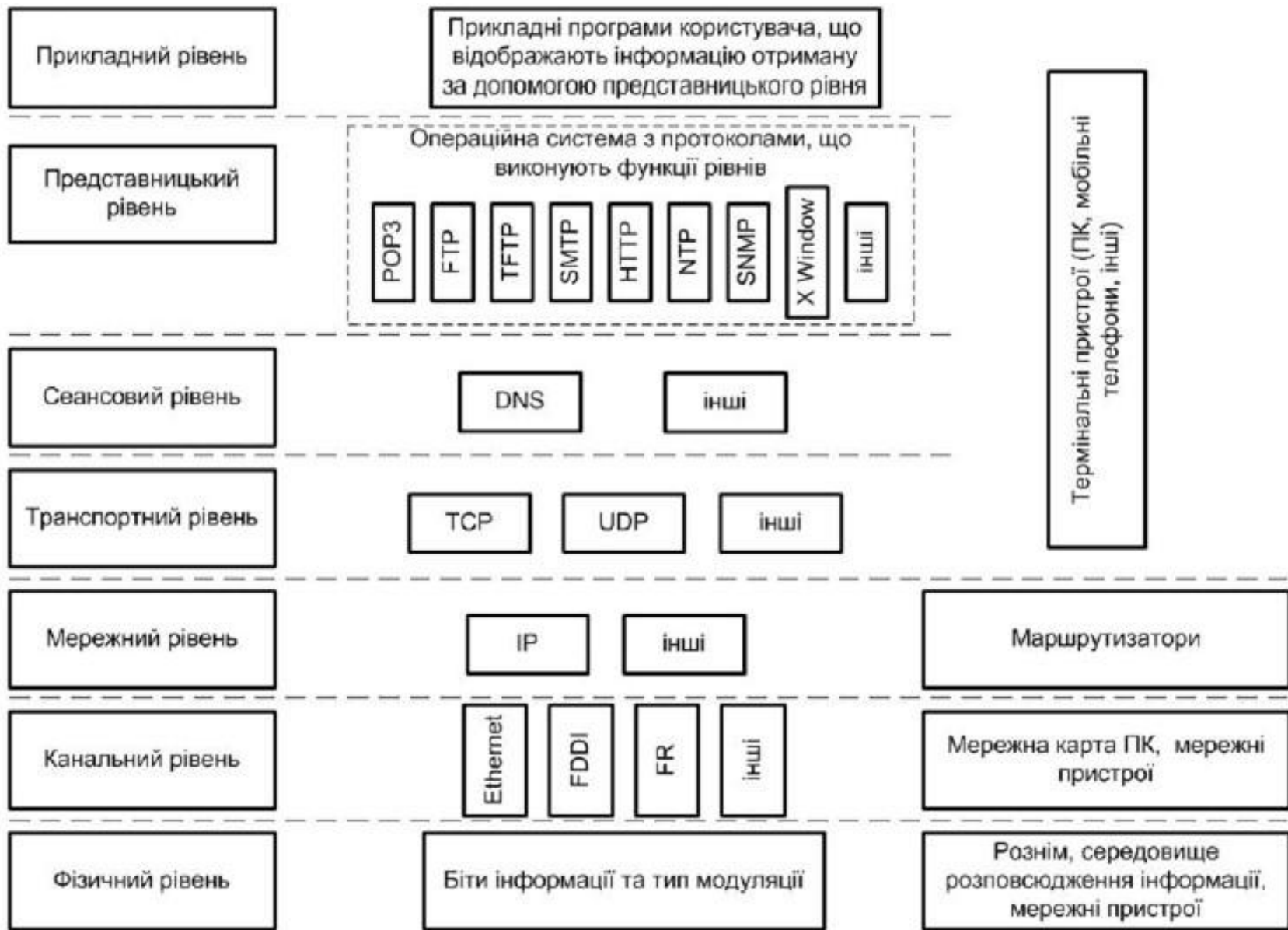
Лекція 23

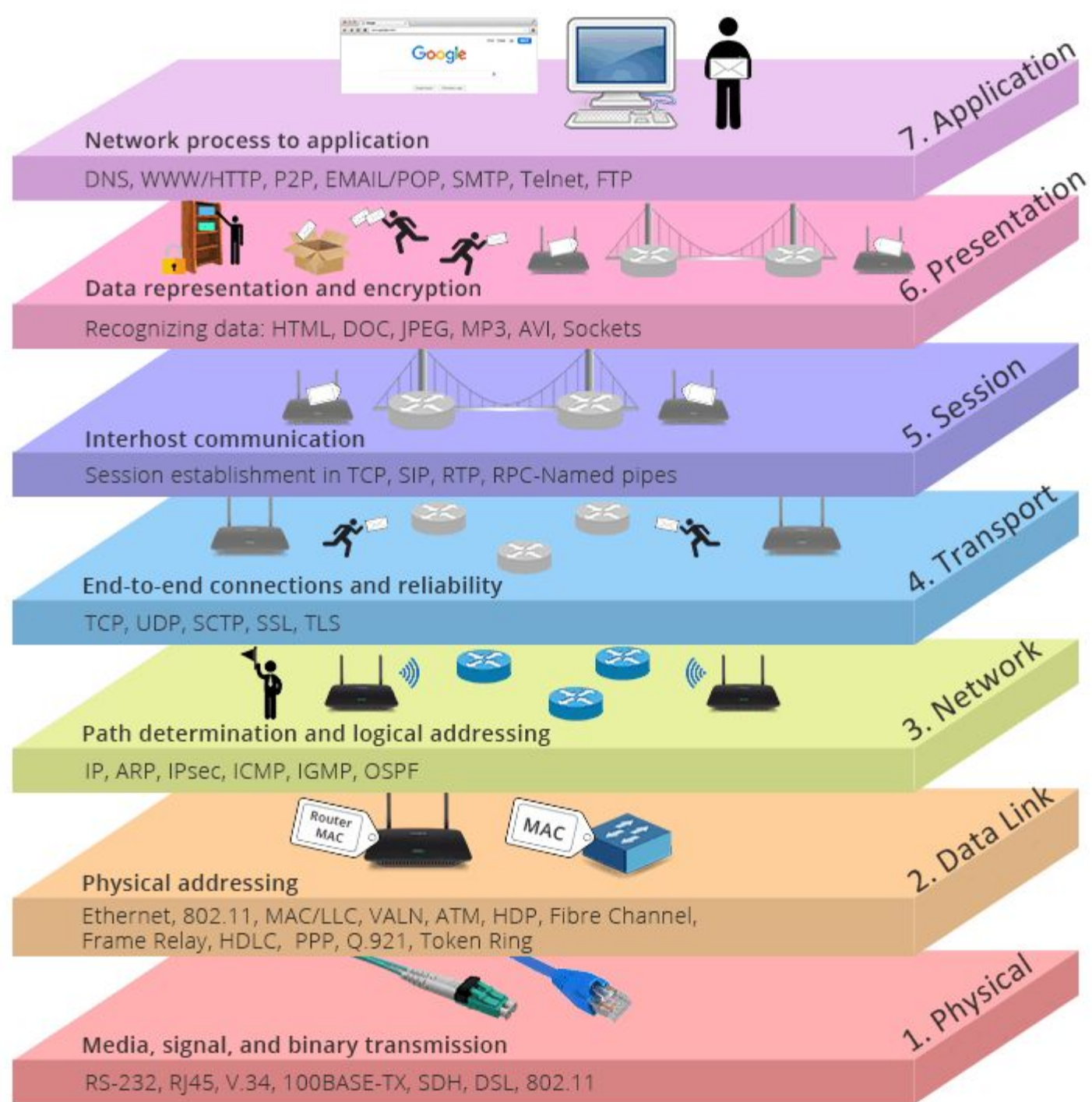
Модель взаємодії відкритих систем (Open Systems Interconnection (OSI)).

Це сімерівнева модель, кожен рівень котрої виконує певні функції. Кожен нижчий рівень в моделі надає вищому рівню певні послуги для передавання інформації. При цьому важливою є взаємодія однакових рівнів приймача та передавача, котра забезпечує передавання інформації між абонентами.

Модель OSI

Дані	7 прикладний application	Доступ до мережевих служб
	6 представлень presentation	Представлення і кодування даних
	5 сеансовий session	Управління сеансом зв'язку
Сегменти	4 транспортний transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережевий network	Визначення маршруту і логічна адресація
Кадри	2 канальний data link	Фізична адресація
Біти	1 фізичний physical	Робота з середовищем передачі, сигналами і двійковими даними





Фізичний рівень

Фізичний рівень (*Physical layer*) має справи з передачею бітів по фізичних каналах зв'язку, таким, як коаксіальний кабель, кручена пара, оптоволоконний кабель або цифровий територіальний канал.

До цього рівня мають відношення характеристики фізичних середовищ передачі даних, такі як смуга пропускання, перешкодозахищеність, хвильовий опір і інші.

На цьому ж рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію, таку як крутість фронтів імпульсів, рівні напруги або струму переданого сигналу, тип кодування, швидкість передачі сигналів.

Крім того, тут стандартизуються типи роз'ємів і призначення кожного контакту.

Функції фізичного рівня:

- передача бітів по фізичних каналах;
- формування електричних сигналів;
- кодування інформації;
- синхронізація;
- модуляція.

Реалізується апаратно.

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

Прикладом протоколу фізичного рівня може служити специфікація *100Base-TX* технології Ethernet, що визначає в якості середовища передачі даних неекрановану кручену пару категорії 5 із хвильовим опором 100 Ом, роз'єм *RJ-45*, максимальну довжину фізичного сегмента 100 метрів, а також деякі інші характеристики середовища й електричних сигналів.

Канальний рівень

На фізичному рівні просто пересилаються біти. При цьому не враховується, що в тих мережах, у яких лінії зв'язку використовуються (розділяються) поперемінно декількома парами взаємодіючих комп'ютерів, фізичне середовище передачі може бути зайняте.

Тому одне із завдань канального рівня (Data Link layer) є перевірка доступності середовища передачі. Інше завдання канального рівня - реалізація механізмів виявлення й корекції помилок. Для цього на канальному рівні біти групуються в набори, називані кадрами (frames).

Канальний рівень забезпечує коректність передачі кожного кадру поміщаючи спеціальну послідовність біт у початок і кінець кожного кадру, для його виділення, а також обчислює контрольну суму, обробляючи всі байти кадру певним способом, і додає контрольну суму до кадру. Канальний рівень може не тільки виявляти помилки, але й виправляти їх за рахунок повторної передачі ушкоджених кадрів. Необхідно відзначити, що функція виправлення помилок для канального рівня не є обов'язковою, тому в деяких протоколах цього рівня вона відсутня, наприклад в *Ethernet* і *Frame Relay*. Реалізується апаратно.

Мережний рівень

Мережний рівень (*Network layer*) служить для утворення єдиної транспортної системи, що поєднує кілька мереж, причому ці мережі можуть використовувати зовсім різні принципи передачі повідомлень між кінцевими вузлами й мати довільну структуру зв'язків. Функції мережного рівня досить різноманітні.

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

Повідомлення мережного рівня прийнято називати **пакетаму (*packets*)**. При організації доставки пакетів на мережному рівні використовується поняття «номер мережі». У цьому випадку адреса одержувача складається зі старшої частини - номера мережі й молодшої - номера вузла в цій мережі. Всі вузли однієї мережі повинні мати ту саму старшу частину адреси, тому терміну «мережа» на мережному рівні можна дати й інше, більше формальне визначення: мережа - це сукупність вузлів, мережна адреса яких містить той самий номер мережі.

На мережному рівні визначаються два види протоколів:

1. **мережні протоколи (*routed protocols*)** - реалізують просування пакетів через мережу. Саме ці протоколи звичайно мають на увазі, коли говорять про протоколи мережного рівня. Однак часто до мережного рівня відносять і інший вид протоколів, названих протоколами обміну маршрутною інформацією або просто *протоколами маршрутизації (routing protocols)*.

2. **протоколи вирішення адрес** - *Address Resolution Protocol, ARP*, які відповідають за відображення адреси вузла, використовуваного на мережному рівні, у локальну адресу мережі.

Прикладами протоколів мережного рівня є протокол міжмережної взаємодії *IP* стека *TCP/IP* і протокол обміну пакетами *IPX* стека *Novell*.

Транспортний рівень

Транспортний рівень (Transport layer) забезпечує додаткам або верхнім рівням стека - прикладному й сеансовому - передачу даних з тим ступенем надійності, що їм потрібно. Модель OSI визначає п'ять класів сервісу, надаваних транспортним рівнем. Ці види сервісу відрізняються якістю надаваних послуг: терміновістю, можливістю відновлення перерваного зв'язку, наявністю засобів націлити декількох з'єднань між різними прикладними протоколами через загальний транспортний протокол, а головне - здатністю до виявлення й виправлення помилок передачі, таких як перекручування, втрата й дублювання пакетів.

Основні завдання транспортного рівня:

- 1.розбивка повідомлення сеансового рівня на пакети, їхня нумерація;
- 2.буферизація прийнятих пакетів;
- 3.впорядочення пакетів, що прибувають;
- 4.адресація прикладних процесів;
- 5.керування потоком.

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

Сеансовий рівень

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

Основні завдання сеансового рівня:

1. встановлення способу обміну повідомленнями (дуплексний або напівдуплексний);
2. синхронізація обміну повідомленнями;
3. організація "контрольних точок" діалогу.

Представницький рівень

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

Основні завдання представницького рівня:

1. перетворення даних із зовнішнього формату у внутрішній;
2. шифрування й розшифровка даних.

Прикладний рівень

Прикладний рівень (*Application layer*) - це в дійсності просто набір різноманітних протоколів, за допомогою яких користувачі мережі одержують доступ ресурсів, що розділяються, таким як файли, принтери або гіпертекстові Web-сторінки, а також організують свою спільну роботу, наприклад, за допомогою протоколу електронної пошти. Одиниця даних, який оперує прикладний рівень, звичайно називається повідомленням (*message*).

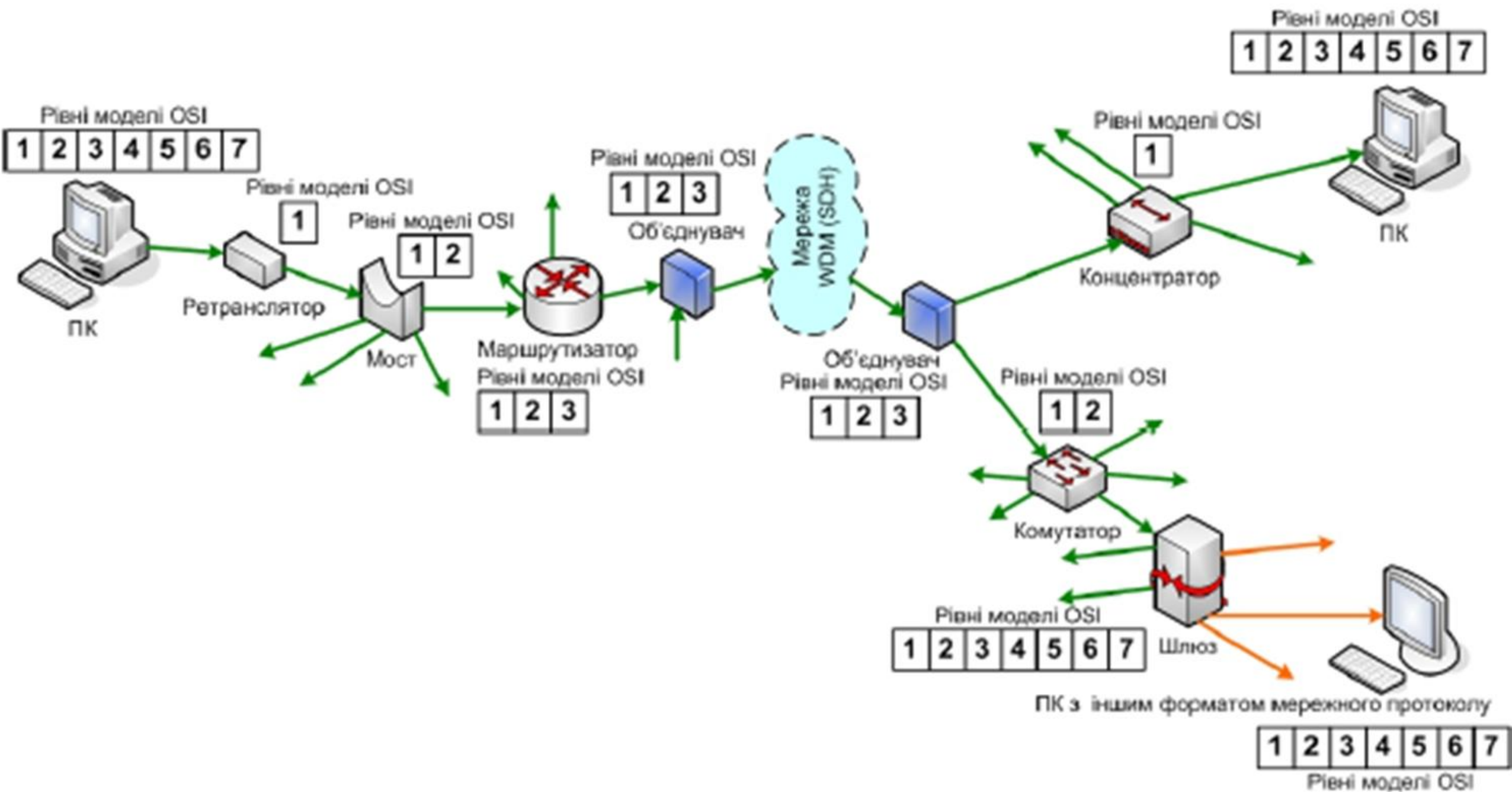
Основні завдання прикладного рівня:

1. ідентифікація, перевірка прав доступу;
2. принт- і файл-сервіс, пошта, вилучений доступ і т.д.

Крім моделі *OSI*, існує також модель **IEEE Project 802**, яку можна розглядати як модифікацію, розвиток, уточнення моделі *OSI*. Стандарти, обумовлені цією моделлю (так звані 802-специфікації), діляться на дванадцять категорій:

- 802.1 - об'єднання мереж.
- 802.2 - керування логічним зв'язком.
- 802.3 - локальна мережа з методом доступу *CSMA/CD* і топологією «шина» (*Ethernet*).
- 802.4 - локальна мережа з топологією «шина» і маркерним доступом.
- 802.5 - локальна мережа з топологією «кільце» і маркерним доступом.
- 802.6 - міська мережа (*Metropolitan Area Network, MAN*).
- 802.7 - широкомовна технологія.
- 802.8 - оптоволоконна технологія.
- 802.9 - інтегровані мережі з можливістю передачі мови й даних.
- 802.10 - безпека мереж.
- 802.11 - бездротова мережа.
- 802.12 - локальна мережа із централізованим керуванням доступом по пріоритетах запитів і топологією «зірка» (*100VG-AnyLAN*).

Стандарти 802.3, 802.4, 802.5, 802.12 прямо ставляться до підрівню *MAC* другого (канального) рівня еталонної моделі *OSI*. Інші 802-специфікації вирішують загальні питання мереж.



Роль моделі OSI при побудові мереж

Модель OSI служить інструментом при діагностиці мереж. Якщо в мережі щось не працює, то набагато простіше визначити рівень, на якому сталася неполадка, ніж намагатися перебудувати всю мережу заново.

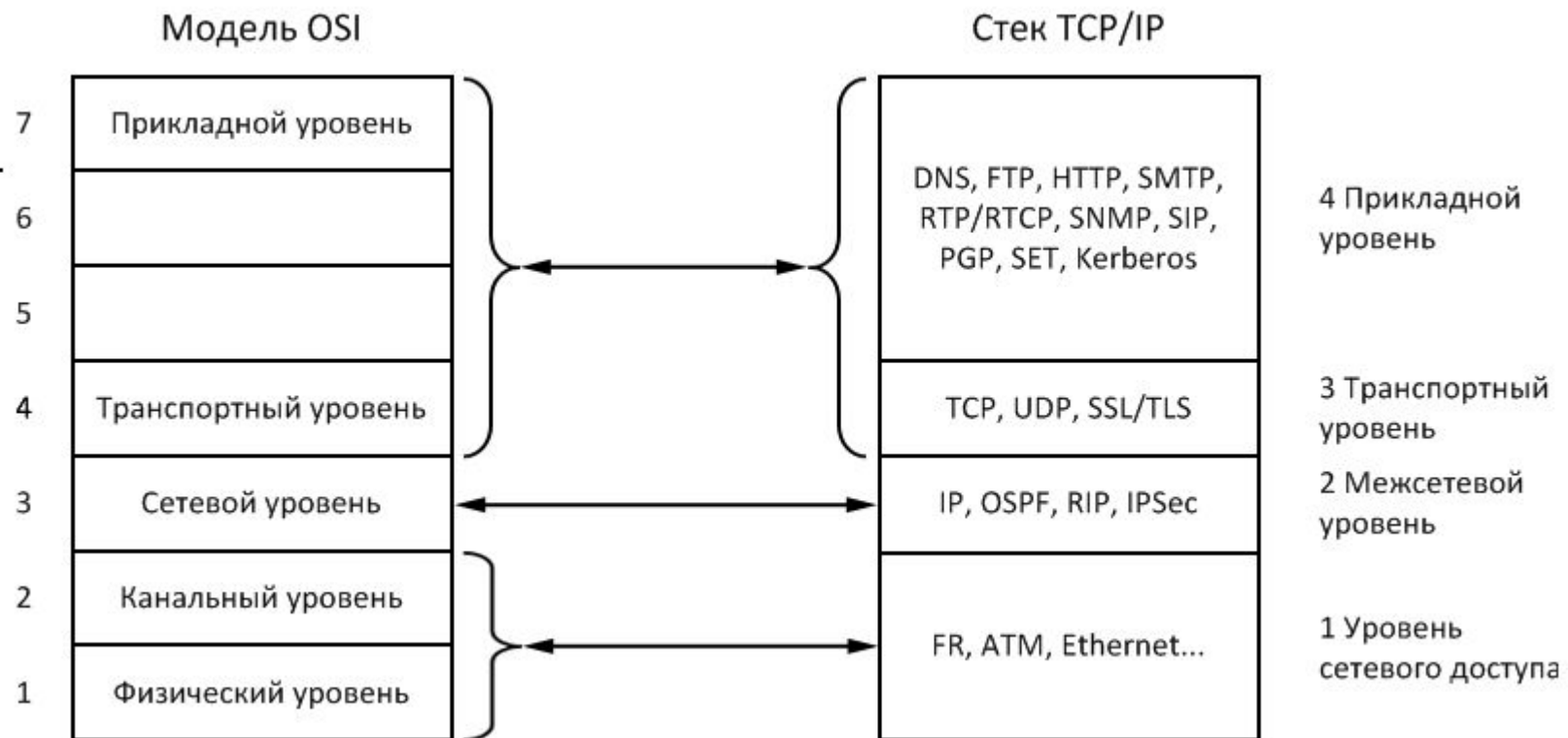
Знаючи архітектуру мережі, набагато простіше її будувати і діагностувати. Як можна побудувати будинок, не знаючи його архітектури, так неможливо побудувати мережу, не знаючи моделі OSI.

При проектуванні важливо враховувати всі. Важливо врахувати взаємодію кожного рівня з іншими, наскільки забезпечується безпека, шифрування даних усередині мережі, який приріст користувачів витримає мережу без обвалення, чи буде можливо перенести мережу на іншу машину і т.д. Кожен з перелічених критеріїв укладається в функції одного з семи рівнів.

Мережева модель ТСП / IP



Модель TCP / IP також є багаторівневою мережевою моделлю, але це чотирирівнева модель. Він широко відомий як TCP / IP, оскільки основними протоколами є TCP і IP, але в цій моделі використовуються не тільки ці два протоколи.



Модель TCP / IP і модель OSI є концептуальними моделями, що використовуються для опису всіх мережевих комунікацій, в той час як TCP / IP сама по собі також є важливим протоколом, використовуваним у всіх операціях Інтернету.

Як правило, коли ми говоримо про рівень 2, рівні 3 або рівні 7, в якому працює мережевий пристрій, ми маємо на увазі модель OSI.

Моделі TCP / IP використовується як для моделювання поточної архітектури Інтернету і забезпечують набір правил, яких дотримуються всі форми передачі по мережі.

IPv4

223.135.100.7

2^{32} шт.

IPv6

2DAB:FFFF:0000:0000:01AA:00FF:DD72:2C4A

2^{128} шт.

Транспортний рівень

Транспортний рівень, також відомий як транспортний рівень хост-хост, відповідає за надання прикладного рівня сервісами зв'язку сеансу і датаграмм.

Основними протоколами цього рівня є TCP і UDP.

TCP (протокол управління передачею) - надійний, він забезпечує передачу інформації, перевіряючи чи дійшла вона, наскільки повним є обсяг отриманої інформації і т.д. TCP дає можливість двом хостам проводити обмін пакетами через установку з'єднання. Він надає послугу для додатків, повторно запитує втрачену інформацію, усуває дублюючі пакети, регулюючи завантаженість мережі. TCP гарантує отримання і складання інформації у адресата в правильному порядку.

UDP (протокол призначених для користувача датаграм) - ненадійний, він займається передачею автономних датаграмм. UDP не гарантує, що всіх датаграми дійдуть до одержувача. Датаграми вже містять всю необхідну інформацію, щоб дійти до одержувача, але вони все одно можуть бути втрачені або доставлені в порядку відмінному від порядку при відправленні.

Мережевий рівень

Мережевий рівень відповідає за адресацію хостів, упаковку і функції маршрутизації.

1. Основними протоколами мережевого рівня є:
 - IP,
2. протокол дозволу адрес (ARP),
3. протокол керуючих повідомлень Інтернету (ICMP),
4. протокол управління групами Інтернету (IGMP).

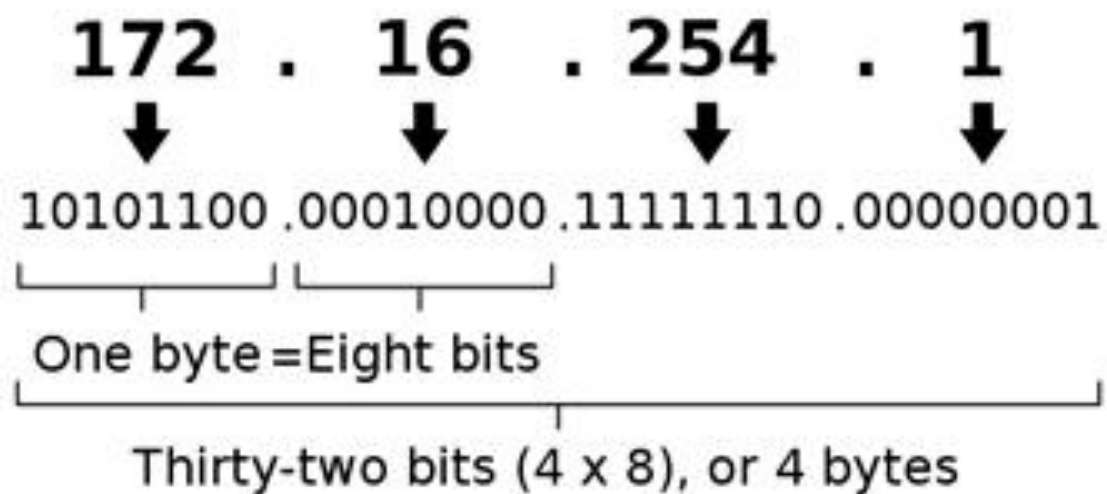
IP - це протокол маршрутизації, який відповідає за IP-адресацію, маршрутизацію і фрагментацію і повторне складання пакетів.

ARP відповідає за виявлення адреси рівня мережевого доступу, такого як адреса апаратних засобів, пов'язаний з даними доступом до Інтернет-рівня.

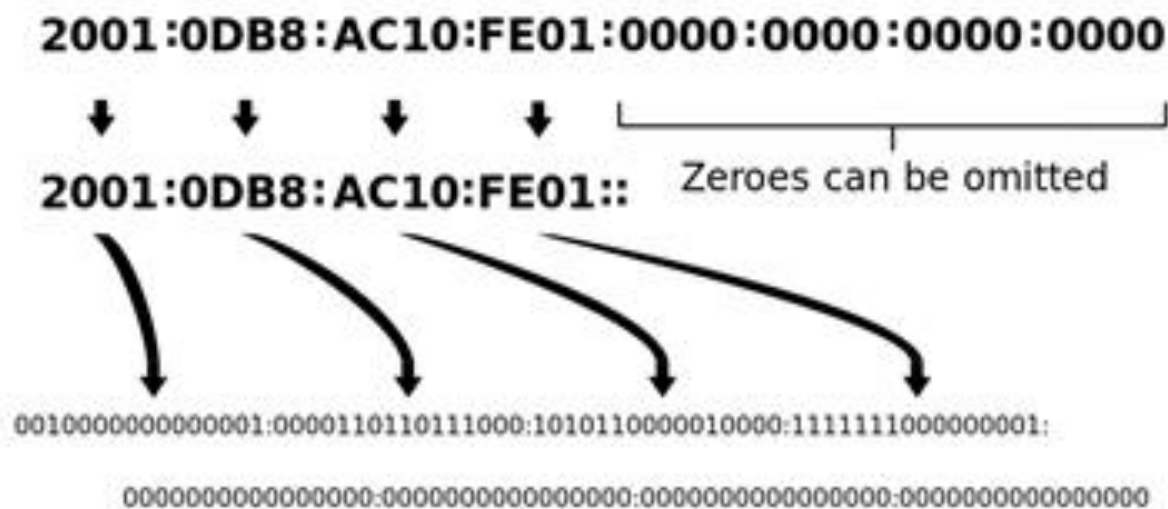
ICMP відповідає за надання діагностичних функцій і звітів про помилки через невдалу доставки IP-пакетів. IGMP відповідає за управління багатоадресними групами IP. На цьому рівні IP додає заголовки до пакетів, який відомий як IP-адреса.

Зараз є IPv4 (32-бітний) адреса і IPv6 (128-бітний) адреса.

An IPv4 address (dotted-decimal notation)



An IPv6 address (in hexadecimal)



Канальний рівень

Канальний рівень (Link layer) описує, яким чином передаються пакети даних через фізичний рівень, включаючи кодування (тобто спеціальні послідовності біт, що визначають початок і кінець пакету даних).

Канальний рівень іноді поділяють на 2 підрівні - LLC і MAC.

- MAC (Media Access Control) - рівень управління доступом до фізичної середовищі;
- LLC (Logical Link Control) - рівень логічної передачі даних.

Крім того, канальний рівень описує середовище передачі даних (будь то коаксіальний кабель, кручена пара, оптичне волокно або радіоканал), фізичні характеристики такого середовища і принцип передачі даних (поділ каналів, модуляцію, амплітуду сигналів, частоту сигналів, спосіб синхронізації передачі, час очікування відповіді і максимальна відстань).

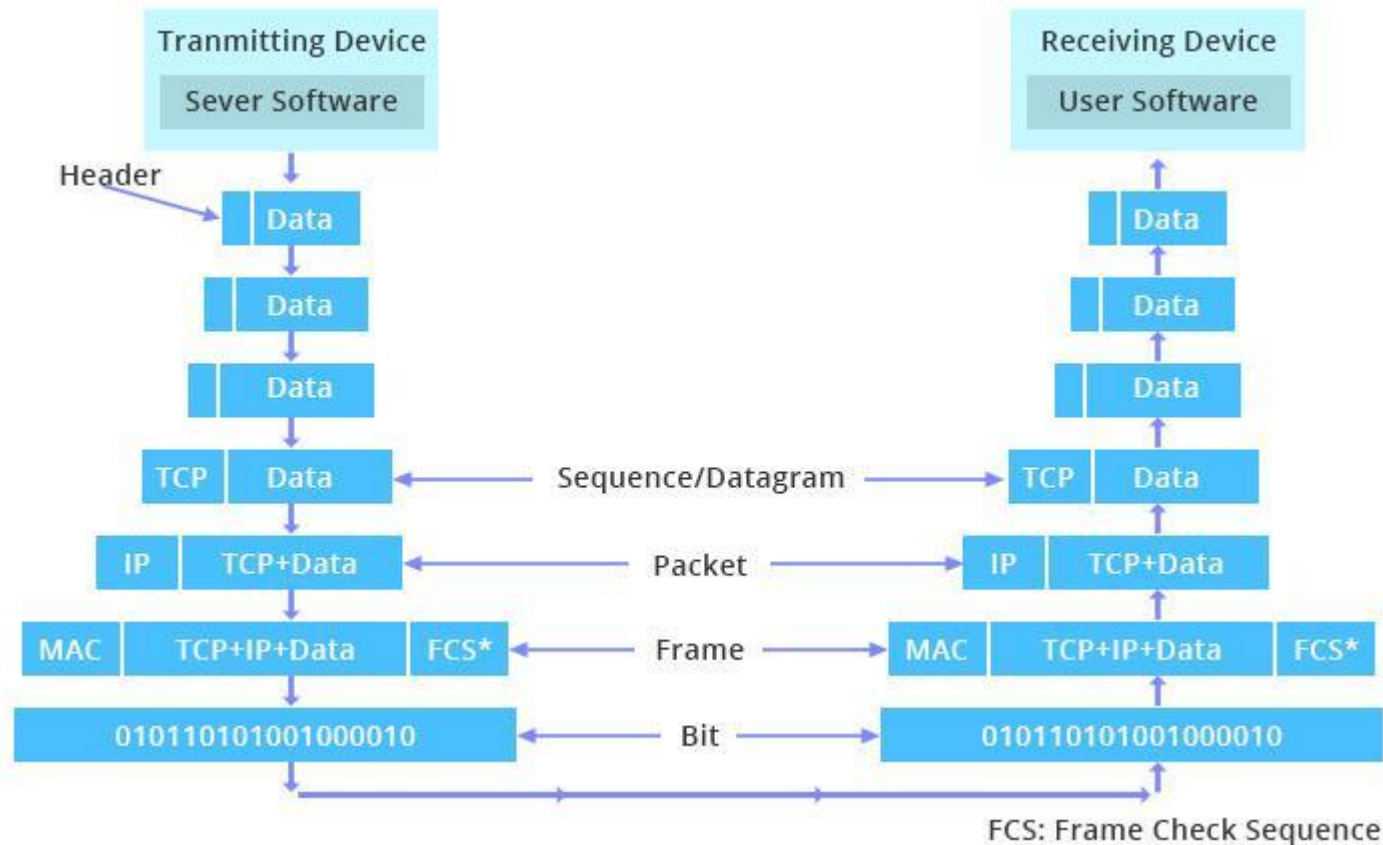
Як обробляються дані під час передачі?

У багаторівневій системі, пристрої рівня обмінюються даними в іншому форматі, який відомий як protocol data unit (PDU). У таблиці нижче показані PDU на різних рівнях.

Таблиця: protocol data unit (PDU), що обробляється на різних рівнях.

Тип моделі	Уровни OSI	Protocol Data Unit (PDU)	Уровни TCP/IP
Уровни хоста	Прикладной уровень	Данные	Прикладной уровень
	Уровень представления		Сеансовый уровень
	Сеансовый уровень		Применение
	Транспортный уровень	Segment (TCP) / Datagram (UDP)	Транспортный уровень
Уровни медиа	Сетевой уровень	Пакет	Сетевой уровень
	Канальный уровень	Кадр	Канальный уровень
	Физический уровень	Бит	

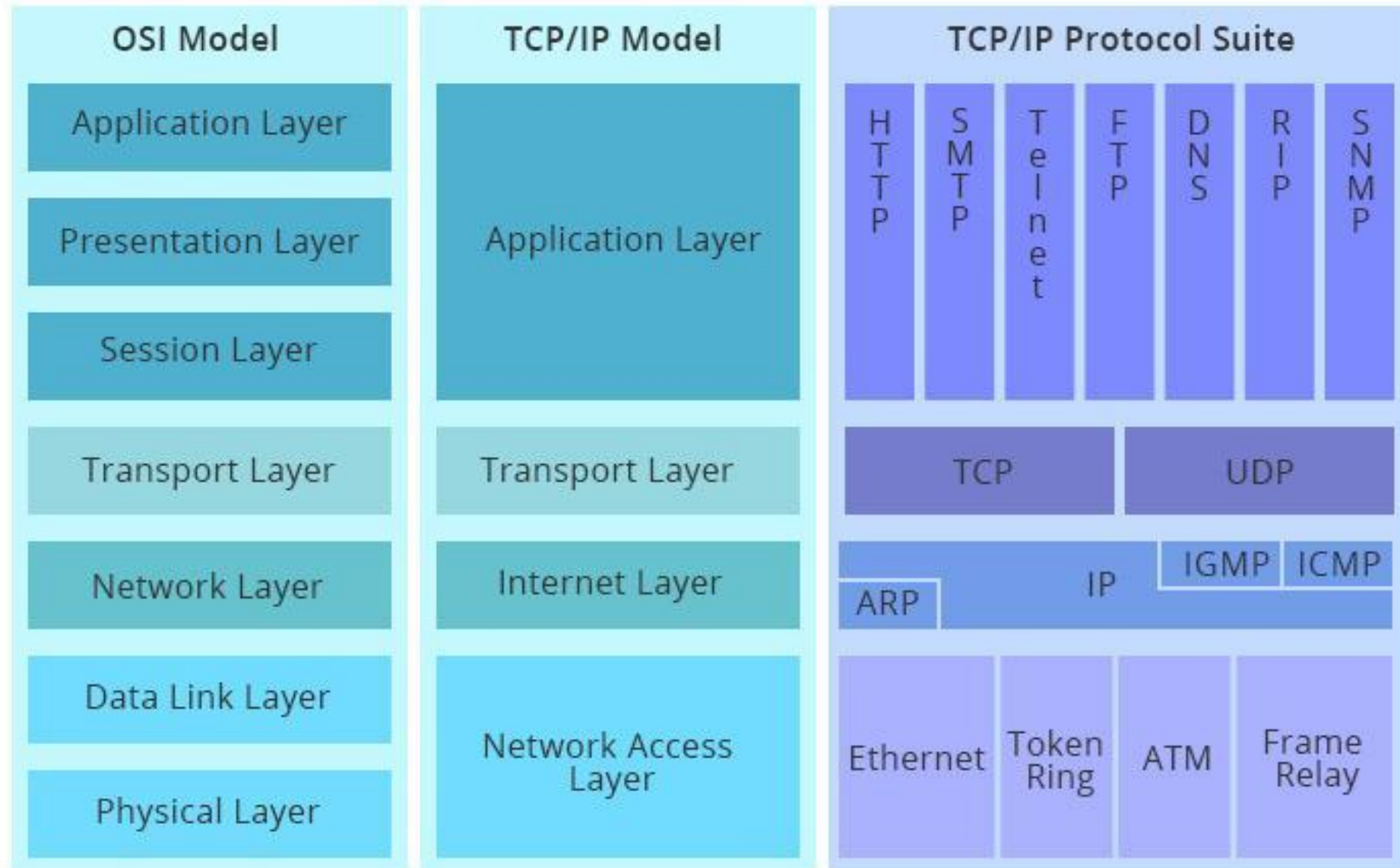
Наприклад, коли користувач запитує перегляд веб-сайту на комп'ютері, програмне забезпечення віддаленого сервера спочатку передає запитані дані на прикладний рівень, де вони обробляються від рівня до рівня, при цьому кожен рівень виконує свої призначені функції. Потім дані передаються по фізичному рівню мережі до тих пір, поки їх не отримає кінцевий сервер або інший пристрій. На цьому етапі дані знову передаються вгору по рівнях, кожен рівень виконує призначені йому операції, поки дані не будуть використані приймають програмним забезпеченням.



Під час передачі кожен шар додає верхній або нижній колонтитул або обидва до PDU, що надходить з верхнього рівня, який направляє і ідентифікує пакет. Цей процес називається інкапсуляцією. Верхній (і Нижній колонтитули) і дані разом утворюють PDU для наступного рівня.

Процес триває до досягнення найнижчого рівня (фізичного рівня або рівня доступу до мережі), з якого дані передаються на приймаючий пристрій. У приймальному пристрої відбувається зворотний процес, де-інкапсуляції даних на кожному рівні. верхні і нижні колонтитули направляють операції.

Потім додаток, нарешті, використовує дані. Процес триває до тих пір, поки всі дані не будуть передані і отримані.



Значення TCP / IP і OSI для усунення неполадок

Зі знанням поділу рівнів, ми можемо діагностувати, де знаходиться проблема, коли з'єднання пропадає. Принцип полягає в тому, щоб перевірити з найнижчого рівня, а не з самого високого рівня.

Тому що кожен рівень служить для рівня вище, і буде легше впоратися з проблемами нижнього шару.

Наприклад, якщо ваш комп'ютер не може підключитися до Інтернету, по-перше ви повинні перевірити, чи підключений мережевий кабель до вашого комп'ютера, або якщо до комутатора підключений з точкою бездротового доступу (WAP), або якщо штирі роз'ємів RJ45 знаходяться в хорошому стані.

Протокол інтернету - IP (Internet Protocol) використовується маршрутизатором, щоб визначити, до якої підмережі належить одержувач. Свій унікальний IP-адреса є у кожного мережевого пристрою, при цьому в глобальній мережі не може існувати два пристрої з однаковим IP. Він має два підвиди, першим був прийнятий IPv4 (IP version 4, версії 4) в 1983 році.

IPv4 передбачає призначення кожному пристрою 32-бітного IP-адреси, що обмежувало максимально можливе число унікальних адрес 4 мільярдами (2^{32}). У більш звичному для людини десятковому вигляді IPv4 виглядає як чотири блоки (октету) чисел від 0 до 255, розділених трьома точками. Перший октет IP-адреси означає його клас, класів всього 4: A, B, C, D. Розглянемо, наприклад, IPv4 адреса класу C 223.135.100.7. Перші два октету 223.135 визначають клас, третій - .100 - це номер підмережі, а останній означає номер мережевого обладнання. Наприклад, якщо необхідно відправити інформацію з комп'ютера номер 7 з IPv4 адресою 223.135.100.7 на комп'ютер номер 10 в тій же підмережі, то адреса комп'ютера одержувача буде наступний: 223.135.100.10.

У зв'язку з швидким зростанням мережі інтернет гостро поставала необхідність збільшення числа можливих IP-адрес. У 1998 вперше був описаний IPv6 (IP version 6, версії 6), який використовує 128-бітові адреси, і дозволяє призначити унікальні адреси для 2¹²⁸ пристроїв.

Такої кількості IPv6 адрес буде достатньо, щоб призначити унікальну адресу для кожного атома на планеті. IPv6 має вигляд восьми блоків по чотири шістнадцяткові значення, а кожен блок розділяється двокрапкою. IPv6 виглядає наступним чином: 2DAB: FFFF: 0000: 0000: 01AA: 00FF: DD72: 2C4A.

Так як IPv6 адреси довгі, їх дозволяється скорочувати за такими правилами: провідні нулі допускається опускати, наприклад в адресі вище: 00FF: дозволяється записувати як: FF :, групи нулів, що йдуть підряд теж допустимо скорочувати і замінювати на подвійне двокрапка, наприклад, 2DAB: FFFF :: 01AA: 00FF: DD72: 2C4A. Допускається робити не більше одного подібного скорочення в адресі IPv6

IP призначений для визначення адресата і доставки йому інформації, він надає послугу для вищих рівнів, але не гарантує цілісність доставляється інформації.

IP здатний інкапсулювати інші протоколи, надавати місце, куди вони можуть бути вбудовані. Як було сказано вище, IP - це 32 біта інформації, перші 8 біт в заголовку IP - поля для зазначення номера інкапсулюемого протоколу.

Для IPv4 перші 8 біт - поле «протокол», для IPv6 - поле «наступний заголовок».

Наприклад, ICMP (міжмережевий протокол керуючих повідомлень) буде позначений числом 1, а IGMP (міжмережевий протокол групового управління) буде позначений числом 2.

Мережеві пристрої об'єднуються в групи за допомогою IGMP, який використовується хостами і роутерами в IPv4 мережах. IGMP організовує multicast-передачу інформації, що дозволяє мережам направляти інформацію тільки хостам, що запросив її. Це зручно для онлайн-ігор або потокової передачі мультимедіа. IGMP використовується тільки в IPv4 мережах, в мережах IPv6 використовується MLD (Multicast Listener Discovery, протокол пошуку групових слухачів), інкапсульований в ICMPv6.

ICMP використовується в якості підтримки маршрутизаторами і іншими мережевими пристроями. Усередині мережі він служить для доставки повідомлень про помилки і операційної інформації, що повідомляє про успіх або помилку при зв'язку з іншим IP. Наприклад, в ситуаціях, коли необхідний сервіс не може бути запитаний, чи коли не було отримано відповіді від маршрутизатора або хоста.

ICMP ніколи не викликається мережевими додатками користувача, крім випадків діагностики мережі, наприклад, пінг (ping) або traceroute (tracert). ICMP не передає дані, це відрізняє його від транспортних TCP і UDP, розташованих на L3, які переносять будь-які дані. ICMP працює тільки з IP четвертої версії, з IPv6 взаємодіє ICMPv6.

ICMP



Навіщо потрібен порт і що означає термін сокет

Додатки прикладного рівня, спілкуються також з попереднім, транспортним, але вони бачать його протоколи як «чорні ящики».

Для прийому-передачі інформації вони можуть працювати з TCP або UDP, але розуміють тільки кінцевий адресу у вигляді IP і порту, а не принцип їх роботи. IP присвоюється кожному комп'ютеру міжмережєвих рівнем, але обмін даними відбувається не між комп'ютерами, а між додатками, встановленими на них. Щоб отримати доступ до тієї чи іншої мережному додатку недостатньо тільки IP, для ідентифікації додатків застосовують порти.

Комбінація IP-адреси і порту називається сокетом або гніздом (socket). Тому обмін інформацією відбувається між сокетами.

Нерідко слово сокет вживають як синонім для хоста або користувача, також сокетом називають гніздо підключення процесора. З привілеїв у додатків на прикладному рівні можна виділити наявність власних протоколів для обміну даними, а також фіксований номер порту для звернення до мережі.

Адміністрація адресного простору інтернет (IANA), що займається виділенням діапазонів IP-адрес, відповідає ще за призначення мережєвим додаткам портів.

Так поштові додатки, які спілкуються по SMTP-протоколу, прослуховують порт 25, пошта через POP3 приходить на 110-й, по HTTP приймають повідомлення веб-сервера - це порт 80, 21-й зарезервованій за FTP. Порт завжди записується після IP і відділяється від нього двокрапкою, виглядає це, наприклад, так: 192.168.1.1:80.

Щоб не запам'ятовувати числові адреси інтернет-серверів була створена DNS - служба доменних імен. DNS завжди слухає на 53 порту і перетворює літерні імена мережевих доменів в числові IP-адреси і навпаки. Служба DNS дозволяє не запам'ятовувати IP - комп'ютер самостійно надсилає запит «який IP у selectel.ru?» на 53 порт DNS-сервера, отриманого від постачальника послуг інтернет.

DNS-сервер дає комп'ютера відповідь «IP для selectel.ru - XXX.XXX.XXX.XXX». Потім, комп'ютер встановлює з'єднання з веб-сервером отриманого IP, який слухає на порту 80 для HTTP-протоколу і на порту 443 для HTTPS. У браузері порт не відображається в адресному рядку, а використовується за умовчанням, але, по суті, повна адреса сайту Selectel виглядає ось так: <https://selectel.ru:443>.

Процес, кодування даних на прикладному рівні, передача їх на транспортному, а потім на межсетевом і, нарешті, на каналному рівні називається інкапсуляцією даних. Зворотній передача бітів інформації за ієрархією, з каналного на прикладної рівні, називають декапсуляції. Обидва процеси здійснюються на комп'ютерах одержувача і відправника даних поперемінно, це дозволяє довго не утримувати одну сторону каналу зайнятої, залишаючи час на передачу інформації іншого комп'ютера.



Стек протоколів(каналний рівень)

Більшості користувачів використовує протокол Ethernet. У мережі, за стандартом Ethernet, пристрої відправника і адресата мають певну MAC-адресу - ідентифікатор «заліза».

MAC-адресу інкапсулюється в Ethernet разом з типом даних, що передаються і самими даними. Фрагмент даних, складених відповідно до Ethernet називається фреймом або кадром (frame). MAC-адресу кожного пристрою унікальний і двох «залізяк» з однаковою адресою не повинно існувати, хоча деколи таке трапляється, що призводить до мережеских проблем. Таким чином, при отриманні мережеского адаптера займається вилученням отриманої інформації з кадру і її подальшою обробкою.

Після ознайомлення з рівневою структурою моделі стає зрозуміло, що інформація не може передаватися між двома комп'ютерами безпосередньо. Спочатку кадри передаються на міжмережеский рівень, де комп'ютера відправника і комп'ютера одержувача призначається унікальний IP. Після чого, на транспортному рівні, інформація передається у вигляді TCP-фреймів або UDP-датаграм.

На кожному етапі, подібно снігової грудки, до вже наявної інформації додається службова інформація, наприклад, порт на прикладному рівні, необхідний для ідентифікації мережеского додатку. Додавання службової інформації до основної забезпечують різні протоколи - спочатку Ethernet, поверх нього IP, ще вище TCP, над ним порт, що означає додаток з делегованим йому протоколом. Така вкладеність називається стеком, названим TCP / IP за двома головними протоколами моделі.

Модель TCP/IP		
4	Прикладной уровень (application layer)	DHCP DNS FTP HTTP HTTPS SMTP POP
3	Транспортный уровень (transport layer)	TCP UDP RSVP
2	Межсетевой уровень (internet layer)	IPv4 IPv6 ICMP ICMPv6 IGMP MLD
1	Канальный уровень (link layer)	MAC Ethernet Wi-Fi DSL PPP SLIP



Дякую за увагу!