Л. М. Петречук, Ю. С. Іващенко, К. Д. Підгорна

КОМП'ЮТЕРНІ МЕРЕЖІ та ТЕЛЕКОМУНІКАЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ

Л. М. Петречук, Ю. С. Іващенко, К. Д. Підгорна

Комп’ютерні мережі та телекомунікації

НАВЧАЛЬНИЙ ПОСІБНИК

ДНІПРО
2025

УДК 004.7:621.39(075.8)
П 30

Авторський колектив:
Петречук Л. М., Іващенко Ю. С., Підгорна К. Д.

Рекомендовано Радою якості освітньої діяльності УДУНТ
Протокол № 1 від «16» вересня 2025 р.

П 30 **Петречук, Л. М.** Комп’ютерні мережі та телекомунікації : навч. посіб. / Л. М. Петречук, Ю. С. Іващенко, К. Д. Підгорна ; Укр. держ. ун-т науки і технологій. – Електрон. вид. – Дніпро : УДУНТ, 2025. – 202 с.

ISBN 978-617-8314-78-1 (PDF)

Навчальний посібник призначений для використання студентами денної та заочної форм навчання спеціальності F6 «Інформаційні системи і технології» (бакалаврський рівень) під час вивчення дисципліни «Комп’ютерні мережі та телекомунікації».

Містить матеріал для формування систематизованих знань про основні принципи організації комп’ютерних мереж та технології телекомунікаційних систем: типи комп’ютерних мереж та їх забезпечення, мережеві моделі і протоколи передачі даних, служби глобальної мережі, аспекти безпеки та захисту мереж.

Іл. 54, табл. 8, бібліогр. 22 назв.

УДК 004.7:621.39(075.8)

ISBN 978-617-8314-78-1 (PDF)
DOI 10.15802/978-617-8314-78-1

ЗМІСТ

ВСТУП

Наше сьогодення базується на постійному обміні інформацією, підставою для якого є інформаційні технології, комп'ютерні мережі та телекомунікації. Вони становлять фундамент цифрової інфраструктури і забезпечують обмін даними і взаємодію між користувачами, організаціями і всесвітом взагалі. Особливо це вагомо під час спілкування в режимі реального часу. Без ефективно побудованих і налаштованих мереж неможливо уявити будь-які сфери нашого життя.

Дисципліна «Комп'ютерні мережі та телекомунікації» надає студентам теоретичні знання та практичні навички, необхідні для розуміння принципів побудови мереж, роботи телекомунікаційних систем, їх проєктування, адміністрування та забезпечення безпеки. Це важлива галузь знань, що лежить в основі сучасних інформаційних технологій і комунікаційних сервісів.

Розвиток комп'ютерних мереж і телекомунікаційних технологій органічно поєднані та доповнюють один одного, забезпечуючи високошвидкісний обмін інформацією. Навчальний посібник створений для студентів, які вивчають інформаційні технології та застосування комп'ютерних наук в бізнесі. У ньому систематизовано основні поняття, стандарти, протоколи і технології, що лежать в основі комп'ютерних мереж і телекомунікаційних систем.

Поданий матеріал містить такі теми, як архітектура мереж та конфігурування мережевого обладнання, моделі взаємодії та технології доступу, телекомунікаційні канали, бездротові мережі, робота мережевих сервісів та аспекти безпеки в мережах. Посібник надає студентам можливості не лише отримати теоретичні знання, а й придбати досвід у розв'язанні практичних задач реального життя, набути необхідних навичок і уміння, які передбачені програмою навчальної дисципліни:

ОРН1. Знати базові поняття комп’ютерних технологій, сучасний стан і напрямки розвитку мережних технологій, особливості організації і принципи роботи комп’ютерних мереж, базові принципи організації комп’ютерних мереж.

ОРН2. Розуміти доцільність застосування певної технології та обладнання при побудови мережі. Вміти здійснювати пошук інформації в різних джерелах, застосовувати творчі здібності для розв’язання поставлених задач.

ОРН3. Використовувати комунікативні технології для ефективного спілкування на професійному, науковому та соціальному рівнях. Вміти застосовувати технології електронних інформаційних ресурсів та сервісів, базові технології роботи з даними в інформаційних системах з використанням комп’ютерних мереж.

Оволодіння знаннями з комп’ютерних мереж та телекомунікацій полегшує шлях подальшого навчання. Матеріал, викладений у навчальному посібнику, допоможе студентам здобути необхідні компетенції, сприятиме розвитку критичного мислення та навичок самостійної роботи, зорієнтує у використанні простору комп’ютерних комунікацій.

РОЗДІЛ І. ОСНОВИ КОМП'ЮТЕРНИХ МЕРЕЖ І ТЕЛЕКОМУНІКАЦІЙ

Тема 1. Базові поняття та визначення. Розвиток комп'ютерних мереж.

1.1 Основні поняття телекомунікацій

Створенню сучасних комп'ютерних мереж (КМ) передувало багато подій та винаходів. Наше суспільство характеризується створенням глобального інформаційного простору, який забезпечує інформаційну взаємодію людей, доступ до світових інформаційних ресурсів і задоволення потреб щодо інформаційних продуктів і послуг. Історія людської цивілізації – це історія *інформаційних революцій*, кожна з яких є якісним стрибком у технологіях комунікацій: збирання, збереження та передачі інформації.

Термін *телекомунікація* складається з грецького префіксу *теле* (τηλε – далекий), та латинського *комунікація* (communicare – ділитись). Телекомунікація виникає при обміні інформацією між учасниками з використанням спеціальних технологій. Існує багато різних технологій і систем, тому термін часто використовують у множині, тобто *телекомунікації*.

Телекомунікації (Telecommunications) – це процес передачі, отримання та обробки інформації (знаків, сигналів, письмового тексту, зображень, звуків, повідомлень будь-якого роду) з використанням електронних, електромагнітних, мережевих, комп'ютерних та інформаційних технологій (дротовими, радіо, оптичними або іншими електромагнітними системами).

До телекомунікацій відносяться: радіозв'язок, телебачення, комп'ютерні мережі, соціальні мережі, мобільний та супутниковий зв'язок, системи глобального позиціонування, електронна комерція (інтернет-магазини, аукціони).

Серед телекомунікаційних підприємств виділяють підкатегорії:

– інтернет-провайдери (Датагруп, Київстар, Ланет, Укртелеком, Lifecell,

Triolan);

– мобільні оператори (Київстар, Lifecell, PEOPLEnet, Vodafone Україна);

– провайдери DBS-послуг (НТВ-Плюс Україна, Укркосмос, MYtv (Україна), Viasat Україна, Xtra TV).

DBS (Delivery by Seller) – модель співпраці/продажу на маркетплейсі.

Маркетплейс (електронний/віртуальний торговий майданчик) – платформа електронної комерції.

Історія телекомунікацій розпочалась з винаходу телеграфу. Телеграф став першим кроком у формуванні сучасної телекомунікаційної системи.

Телеграф, як вид зв'язку, виник у XIX столітті, коли люди навчилися передавати по дротах повідомлення (у вигляді сигналів) на далеку відстань. Перший працездатний електричний телеграф був створений англійцем Френсісом Рональдсом у 1816 році, але його проєкт Британське адміралтейство відкинуло. 4 серпня 1837 року американець Самюель Морзе представив електромагнітний телеграф, розробивши до нього код, відомий як код Морзе – апарат перетворював мову в електричні сигнали.

Телефонний зв'язок – вид технічного електрозв'язку, що дає змогу приймати і передавати мовлення на відстань за допомогою електричних або радіо- сигналів. Телефон працює на основі принципу перетворення звукових коливань у електричні сигнали та їх подальшої передачі. Датою народження першого електричного телефону вважається 14 лютого 1876 року і пов’язано з іменем американського вченого – Александер Грем Белл.

Винахід телефону (як і телеграфу) є результатом праці багатьох людей і його авторство не можна приписати одній конкретній особі. На першість у винаході телефону, окрім Белла, претендувало близько трьох десятків вчених.

Радіозв'язок. На початку XX століття почався бурхливий розвиток радіозв'язку. Теоретичні засади радіо були сформульовані англійським вченим

Джеймсом Кларком Максвеллом у 1878 році. Практичне підтвердження теорії Максвела у 1886 року здійснив німецький вчений Генріх Герц, який побудував *передавач* і *приймач* радіохвиль. Винахідником радіо вважається італієць Гульєльмо Марконі, він першим отримав відповідний патент (2 червня 1896 року).

Телебачення – загальний термін, що охоплює всі аспекти технологій та практичної діяльності, пов'язаних з передачею *рухомих* зображень зі *звуковим* супроводом у реальному часі.

Концепція передачі рухомих телевізійних зображень за допомогою електрики з'явилася у 1878 році, невдовзі після винаходу телефону. Родоначальниками телебачення вважають німецьких вчених – у 1884 році Пауль Ніпков винайшов, а у 1885 році запатентував перший механічний пристрій, який дозволяв розкладати зображення на лінії (диск Ніпкова). У грубій експериментальній формі телебачення стало доступним наприкінці 20-х років минулого століття.

Епоха телебачення розпочалася у 1934 році, коли німецька компанія Telefunken вперше розпочала серійний випуск *кінескопних* телевізорів (екрани з електронно-променевою трубкою). До середини 90-х років використовувалися пристрої (телевізори та монітори) виключно на основі кінескопу.

У 2008 році випуск кінескопних (лампових) телевізорів було припинено, їх витіснили тонкі LCD (рідкокристалічний, liquid crystal display) та LED (світлодіо́д, light-emitting diode) пристрої. Сучасний ринок пропонує телевізори (панелі), виготовлені за технологіями OLED, QLED та похідними від них (microLED, NanoCell тощо). Завдяки інтернету звичайні телевізори поступово перетворилися на смартмонітори.

Комп'ютерні мережі. У 1954 році було затверджено втілення програми SAGE (Semi Automatic Ground Environmen) – американської системи

напівавтоматичної координації дій перехоплювачів шляхом програмування їх автопілотів по радіо через комп'ютери, які знаходяться на землі. Прийнята на озброєння у 1963 році, система SAGE була однією з перших великомасштабних глобальних комп'ютерних мереж. Фірмою IBM спільно з Масачусетським технологічним інститутом для системи було розроблено комп'ютер IBM AN/FSQ-7, який важив 250 тон, займав площу близько 7 тис. кв. метрів. Проєкт SAGE заклав важливу технічну основу для майбутніх комп'ютерних мереж.

1958 року у відповідь на запуск радянського штучного супутника землі було створено Агентство передових дослідницьких проєктів Міністерства оборони США (DARPA, Defense Advanced Research Projects Agency). Зусилля організації були спрямовані на збереження технологічної переваги збройних сил країни та дослідження у галузі комп'ютерних технологій, створення надійної системи передачі інформації у вигляді комп’ютерної мережі. При DARPA був створений Офіс методів обробки інформації (Information Processing Techniques Office, IPTO) і до розробки такої мережі були долучені Каліфорнійський університет в Лос-Анджелесі, Стенфордський дослідний центр, Університет Юти та Каліфорнійський університет в Санта-Барбарі. У 1969 році комп'ютерна мережа, що об'єднала ці чотири наукові установи, отримала назву ARPANET (Advanced Research Projects Agency Network) і стала попередником сучасного Інтернету. Термін «Інтернет» закріпився за мережею ARPANET приблизно з 1983 року.

Смарт-технології – це технологічні рішення, які використовуються для автоматизації, оптимізації, поліпшення різних аспектів життя людини та функціонування різних систем. Ці технології зазвичай використовують сенсори, зв'язок мереж, штучний інтелект та аналітику даних для забезпечення зв'язку, збору та обробки інформації, що дозволяє реагувати на змінні умови навколишнього середовища або потреби користувача. Серед таких технологій

можуть бути розумний дім, розумне місто, розумний транспорт, розумні медичні системи. Вони сприяють підвищенню комфорту, ефективності, безпеки та сталості в різних сферах життя [5].

Мобільний зв'язок (рухомий зв'язок) – зв'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщуватися в межах телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції.

Уперше мобільний телефонний зв'язок використала поліція Детройта у 1921 році, це був односторонній зв'язок у діапазоні 2 МГц. Через 20 років поліцейські Нью-Йорка почали застосовувати і двосторонній.

Перший споживчий мобільний радіотелефон (частота – 150 МГц) був розроблений Bell Labs у 1946 році.

1973 року був випущений перший прототип *портативного* стільникового телефону – Motorola DynaTAC.

9 січня 2007 року на щорічній конференції «Macworld» в Сан-Франциско Стів Джобс представив перший iPhone компанії Apple, мультимедійний пристрій, що суміщав у собі можливості телефона, плеєра та інтернет-планшета, мав сенсорний екран і віртуальну клавіатуру.

Розрізняють наземні та супутникові системи мобільного радіозв'язку.

Наземні: системи персонального радіовиклику; стільникові; транкінгова система мобільного радіозв'язку – невелика кількість радіоканалів динамічно розподіляється між великою кількістю користувачів, користувачі отримують доступ до каналу лише на час сеансу зв'язку.

Супутникові: геостаціонарні (супутник перебуває на геостаціонарній орбіті, висота близько 36 тисяч км.); середньоорбітальні; низькоорбітальні; високоеліптичні (робота супутника здійснюється при його знаходженні в апогеї).

Мобільний (стільниковий) телефон працює завдяки електромагнітним хвилям. *Електромагнітна хвиля* являє собою процес розповсюдження електромагнітної взаємодії в просторі у вигляді змінних, зв'язаних між собою, електричного та магнітного полів. Найважливішими її характеристиками є частота і довжина.

Стільниковий зв'язок (СЗ) – один із видів мобільного радіозв'язку, в основі якого лежить стільникова мережа. Загальна зона покриття ділиться на «стільники», що визначається зонами покриття окремих базових станцій. Стільники частково перекриваються й разом утворюють мережу. СЗ є найпоширенішим з усіх видів мобільного радіозв'язку, тому зазвичай «мобільним телефоном» називають саме стільниковий телефон, хоча мобільними телефонами крім стільникових є також супутникові телефони, радіотелефони, апарати магістрального зв'язку.

Супутниковий зв'язок – один з видів космічного радіозв'язку, що базується на використанні штучних супутників Землі, на яких змонтовані ретранслятори. Супутниковий зв'язок здійснюється між земними станціями, які можуть бути як стаціонарними, так і мобільними.

Соціальна мере́жа (суспі́льна мере́жа) – соціальна структура, утворена індивідами або організаціями. Служба соціальної мережі дозволяє користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок та переглядати власний список зв'язків і списки інших користувачів.

Однією з найперших соціальних мереж, що з'явилися в Інтернеті. була американська мережа *classmates.com,* заснована у 1995 році. 2004 року була створена найбільша на сьогодні соціальна мережа світу – Facebook.

Лідерами за відвідуваністю є: соцмережі Facebook та Instagram, відеохостинг YouTube, месенджер WhatsApp.

Системи глобального позиціонування GPS. GPS (Global Positioning System) – це мережа супутників та радіоелектронних засобів, яка дозволяє будь-кому знайти місцезнаходження будь-якої адреси на Землі в будь-який час доби, визначати положення та швидкість руху об'єкта на поверхні Землі або в атмосфері (рис. 1).

Положення об'єкта обчислюється завдяки використанню розміщеного на ньому GPS-приймача, який приймає та обробляє сигнали супутників космічного сегменту GPS-системи. Для керування та визначення точних параметрів орбіт супутників GPS-система має в своєму складі наземні центри управління.

Рисунок 1 – Принцип функціонування навігаційної системи GPS [6]

Коли мова йде про GPS, найчастіше мається на увазі система NAVSTAR (початок розробки 1973 р.), розроблена на замовлення Міністерства оборони США, але існують / розробляються також інші системи глобального позиціонування.

Глобальна система позиціонування NAVSTAR є сузір'ям супутників, розроблених, запущених та обслуговуваних військово-повітряними силами США, які надають сигнали позиціонування, часу та навігації як військовим, так і цивільним користувачам по всьому світу. Припинення роботи GPS може

призвести до збоїв у роботі систем енергопостачання, мобільних телефонів, банків, серйозно ускладнить використання високоточних озброєнь [6].

Системи електронної комерції. Перші системи електронної комерції у своїй найпростішій формі з'явилися у 1960-х роках в США та використовувались головним чином у транспортних компаніях для замовлення квитків та обміну інформацією між транспортними службами перед підготовкою до рейсів.

Концепція електронного бізнесу (е-бізнесу) виникла в США у 80-х роках XX ст. і стала результатом розвитку ідеї глобальної інформаційної економіки, яка базується на використанні локальних і глобальних мереж з поєднанням відповідних інформаційно-комунікаційних технологій.

Торговий інтернет-майданчик являє собою спеціальний ресурс, на якому укладають між собою угоди купівлі-продажу продавці і покупці. Також тут можуть проводитися аукціони, конкурси, рекламні кампанії та інші торгові заходи.

Портали електронної комерції – це масштабні платформи, які об'єднують велику кількість продавців і покупців. Серед відомих прикладів: Amazon, Alibaba, eBay, OLX, Rozetka, Prom.ua.

Отже, з появою комп’ютерів та цифрових технологій телекомунікації зазнали революційних змін. Інтернет став ключовим інструментом спілкування та обміну інформацією, невід’ємною частиною життя багатьох людей.

1.2 Виникнення та розвиток комп’ютерних мереж

Перші комп’ютери 50-х років XX століття були громіздкими, дорогими, займали цілі будівлі, призначалися для обмеженого кола користувачів і не передбачали можливість інтерактивної роботи. Електронні обчислювальні машини обробляли дані на перфокартах. Програма передавалась на обрахунок,

як набір перфокарт, які приносили та вставлялися в порядку черги в ЕОМ, що працювала цілодобово. Аналогічно приходили і забирали результати, оскільки віддаленого спілкування з ЕОМ не було.

На початку 60-х років двадцятого століття почали розвиватися інтерактивні багатотермінальні системи розподілу часу. У таких системах потужний центральний комп'ютер (мейнфрейм) обслуговував певну кількість користувачів, кожен з яких мав у своєму розпорядження термінал (монітор з клавіатурою без системного блоку), за допомогою якого відбувався діалог з комп'ютером. Мейнфрейм по черзі обробляв програми і дані, що надходили з кожного терміналу (рис. 2; фотографом зображення є Schaack, Lothar; джерелом є Німецький федеральний архів).

Рисунок 2 – IBM System/360

У кінці 60-х – на початку 70-х років з’явилися перші глобальні мережі, які будувалися між ЕОМ. Передача даних (з маленькою швидкістю) між комп’ютерами різних організацій відбувалася на базі існуючих телефонних мереж.

Історично перші комп'ютерні мережі були створені агентством ARPA за завданням військового відомства США. У 1964 році була розроблена концепція та архітектура першої комп'ютерної мережі ARPANET, в 1967 вперше було введено поняття протоколу комп'ютерної мережі. У вересні 1969 року стався сеанс першого комп'ютерного сполучення між комп'ютерними вузлами

Каліфорнійського і Стенфордського університетів. У 1977 році мережа ARPANET налічувала вже 111 вузлів, а в 1983 – 4000. Мережа ARPANET припинила своє існування в 1989 році, не витримавши конкуренції з мережею Інтернет.

На початку 70-х років XX століття, завдяки розвитку мікроелектроніки, були створені *міні*-комп'ютери (рис. 3), які стали реальними конкурентами мейнфреймів. Кілька десятків міні-комп'ютерів виконували завдання швидше за один мейнфрейм і при цьому всі разом коштували дешевше. Навіть невеликі підрозділи підприємств отримали можливість купувати для себе комп'ютери.

DEC PDP-8, 1965 р.

8-розрядний міні-комп'ютер MERA 302, 1974 р.

Рисунок 3 – Міні-комп’ютери

Міні-комп'ютери стали широко використовуватися в управлінні технологічними процесами, складами, в бухгалтерському обліку. В результаті йшов інтенсивний процес розподілу обчислювальних ресурсів по всьому підприємству, що, однак, через деякий час призвело до необхідності зворотного об'єднання всіх обчислювальних ресурсів в одну систему. Тепер це об'єднання відбувалося вже на базі не одного комп'ютера, а шляхом підключення до мережі окремих розподілених комп'ютерів.

Наприкінці 80-х, початку 90-х років минулого сторіччя розпочинається бурхливий розвиток комп’ютерних комунікацій, який супроводжувався наступними подіями:

– комерційне використання Internet;

– серед технологій локальних мереж лідером стає Ethernet;

– відбувається розвиток стандартів, оновлення мереж передачі даних; винайдені URL, HTTP, HTML;

– поява всесвітнього павутиння (WWW); починає роботу консорціум W3C (World Wide Web Consortium – організація, що розробляє та впроваджує технологічні стандарти для мережі Інтернет, 1994 р.);

– телекомунікаційні мережі об'єднуються з комп'ютерними мережами;

– зменшуються відмінності між локальними (LAN) та глобальними (WAN) мережами, швидкість передачі даних значно росте (оптоволоконний бум) та перестає бути вузьким місцем.

1.3 Класифікація та архітектура комп'ютерних мереж

Комп'ютерна мережа являє собою сукупність взаємопов'язаних пристроїв/вузлів, з'єднаних комунікаційними каналами та призначених для обміну даними, інформацією і ресурсами один з одним. Пристроями можуть бути як звичайні комп'ютери, смартфони, так і складніше обладнання – сервери, маршрутизатори, комутатори тощо. Мета мережі – забезпечити безперебійний потік даних між різними пристроями, дозволяючи користувачам отримувати доступ до спільних ресурсів.

Існує величезна кількість мереж різного призначення, побудованих на основі різних комп'ютерних і комунікаційних технологій, обумовлених використанням певної мережевої архітектури.

Мережева архітектура – це сукупність мережевих апаратних і програмних рішень, методів доступу та протоколів обміну інформацією.

Мережева технологія – це узгоджений набір програмних і апаратних засобів (драйверів, мережевих адаптерів, кабелів, роз'ємів) і механізмів передачі

даних лініями/каналами зв’язку, достатніх для побудови обчислювальної мережі.

Розмір/масштаб та мета мережі визначають її дизайн (конфігурацію). Будь-яка класифікація мереж є доволі умовною, оскільки реальні конфігурації здебільшого охоплюють одразу декілька класифікаційних груп. Для класифікації комп'ютерних мереж використовуються різні ознаки, згідно з якими мережі ділять на типи:

– за територіальною ознакою (за областю дії);

– за середовищем передавання даних;

– за топологією;

– за рівнем доступу.

Класифікація за областю дії

Класифікація комунікаційних мереж за областю дії враховує географічний район, охоплений мережею та, в меншому ступені, розмір мережі. Виділяють мережі:

– персональні (Personal Area Networks - PAN);

– локальні (Local Area Networks - LAN);

– кампусні/корпоративні (Campus Area Network);

– міські (MAN, Metropolitan Area Network);

– глобальні (Wide Area Networks - WAN).

Персональна мережа (Personal Area Network, PAN) є найменшим і найпростішим типом мережі. PAN – це комп'ютерна мережа, організована навколо окремої людини і налаштовується лише для особистого використання, такі мережі покликані об'єднувати усе персональне електронне обладнання користувача. Зазвичай такі мережі включають комп'ютер, ноутбук, телефон, кишенькові комп’ютерні пристрої, гарнітури та інше

персональне обладнання для передачі даних різного формату: файлів, електронних повідомлень, фотографій, музики тощо [2].

Особисті мережі можуть бути як бездротовими (WPAN, Wireless personal area network), так і кабельними. Кабелі USB з'єднують провідну PAN, в той час як WPAN зазвичай використовують Bluetooth або інфрачервоні з'єднання. Приклади організації PAN: бездротові клавіатура і миша; смарт-годинник; чіп, вставлений під шкірою пальця, який зберігає медичні дані і може підключатися до пристрою для передачі інформації лікарю; хірургічний кабінеті лікарні може мати персональну мережу, щоб хірург мав можливість спілкуватися з іншими членами команди в межах однієї кімнати.

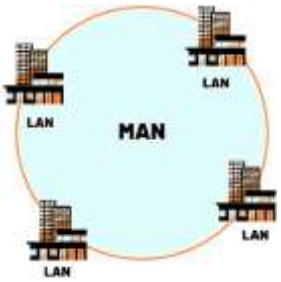
USB-кабель – це кабель, який використовується для підключення пристроїв за допомогою стандарту USB (Universal Serial Bus).

Локальні мережі звичайно займають обсяг одного чи декількох поряд розміщених будинків. Загальною практикою є розподілення великих локальних обчислювальних мереж (ЛОМ) на робочі групи. Малі локальні мережі можуть утворювати єдину робочу групу.

Кампусна мережа (Campus Area Network) – це група локальних мереж, розгорнутих на компактній території (кампусі) певної установи та обслуговуючих цю установу: університет, промислове підприємство, порт, оптовий склад. При цьому мережеве обладнання (комутатори, маршрутизатори, тощо) та середовище передачі даних (оптичне волокно, мідні кабелі) належить орендарю чи власнику підприємства, університету, уряду.

Кампусна мережа – це велика багатосегментна локальна мережа на території до кількох кілометрів у поперечнику, що об'єднує локальні мережі близько розташованих будівель. Кампусні види мереж розвинені у коледжах та університетах, об'єднуючи: адміністративні будинки, навчальні корпуси,

бібліотеки, гуртожитки та інші споруди.



Міська мережа (MAN, Metropolitan Area Network) – це комунікаційна мережа, яка охоплює простір міста включно з передмістями, областями. Як і локальні мережі, MAN використовують різні дротові чи бездротові варіанти підключення, такі як оптоволокно, кабелі Ethernet, Wi-Fi або мобільний зв'язок. MAN забезпечують доступ до однієї мережі в декількох місцях. У LAN користувачі можуть отримати доступ до мережі лише в одному місці.

Глобальні мережі розміщуються на великих географічних просторах. Практично для глобальних мереж не існує обмежень на обсяг. Глобальні мережі об'єднують велику кількість локальних, кампусних, міських мереж. Суттєвою їх рисою є відсутність єдиної адміністративної підпорядкованості. Прикладом глобальної мережі є Інтернет.

Існують комп'ютерні мережі, переважно в сфері бізнесу, які використовують технології Інтернет, але мають обмеження при з'єднуванні, наданні та отриманні таких послуг, як передавання файлів та дистанційне входження в систему. Такі мережі відомі під назвою Інтранет (Intranet).

Класифікація за середовищем передавання даних

Передати інформацію можна за допомогою фізичних сигналів різної природи. Це можуть бути електричні сигнали, електромагнітне випромінювання, оптичні сигнали. Залежно від виду сигналу використовують різні середовища передавання:

– провідні: спеціальні мережеві кабелі (вита пара, волоконно-оптичний, коаксіальний);

– безпровідні/бездротові: радіохвилі, світлові сигнали.

Бездротовою називають мережу, яка використовує бездротове з'єднання для передачі даних й підключення до мережевих вузлів. За дальністю дії розрізняють бездротові мережі:

– персональні (WPAN, Wireless Personal Area Networks), технологія Bluetooth;

– локальні (WLAN, Wireless Local Area Networks), технологія Wi-Fi;

– масштабу міста (WMAN, бездротовий Metropolitan Area Networks), технологія WiMAX;

– глобальні (WWAN, бездротова глобальна мережа), технологіЇ CSD, GPRS, EDGE, EV-DO, HSPA, LTE.

Класифікація за топологією

Зазвичай, коли мова йде про топологію комп’ютерної мережі, мають на увазі *логічну* або *фізичну* топології.

Фізична топологія мережі – це її геометрична форма або фізичне розташування вузлів по відношенню один до одного (до вузлів відносять комп'ютери, маршрутизатори, точки доступу тощо) й спосіб їх з'єднання лініями зв'язку.

Логічна (сигнальна) топологія – описує ходіння сигналу у межах фізичної топології, це концепція, яка визначає архітектуру механізму зв'язку для всіх вузлів мережі. Використовуючи мережеве обладнання, таке як маршрутизатори та комутатори, логічну топологію мережі можна динамічно підтримувати та конфігурувати. Логічна топологія мережі визначає реальні шляхи руху сигналів при передачі даних фізичними лініями зв'язку, тобто, як дані повинні передаватися.

Поняття топології ставиться, насамперед, до локальних мереж, у яких

структуру зв’язків можна легко простежити. У глобальних мережах структура зв’язків схована від користувачів і не так важлива, тому що кожний сеанс зв’язку може виконуватися по своєму власному шляху.

Від топології залежать характеристики мережі. Топологія визначає вимоги до устаткування, тип кабелю, який використовується, можливі й найбільш зручні методи керування обміном, надійність роботи, можливості розширення мережі. На рисунку 4 зображено схеми трьох базових топології: а) зірка (star), б) кільце (ring), в) шина (bus).

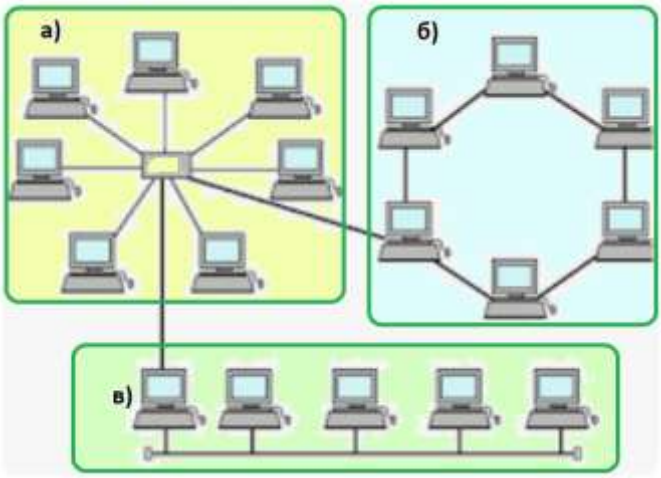


Рисунок 4 – Схеми базових фізичних топологій

Мережева архітектура

Архітектура – це концепція, що описує взаємозв'язок між елементами системи. Мережева архітектура є набором стандартів і правил (протоколів) для створення якісної мережі. Усі елементи комп'ютерної мережі мають бути сумісні між собою. Швидкісні характеристики мережі та надійність залежать від вибору її архітектури.

Мережева архітектура визначає структуровану взаємодію між мережевими службами, пристроями та клієнтами для задоволення їх вимог до підключення. Вона закладає основу того, як пристрої та служби взаємодіють у межах *конкретної мережі*, тоді як архітектура Інтернету забезпечує правила та

протоколи, які дозволяють цим окремим мережам взаємодіяти та формувати глобальний інтернет.

Мережева архітектура та архітектура інтернету – це дві пов'язані, але різні концепції. Архітектура інтернету не займається окремими мережами, а розглядає, як усі мережі взаємодіють, формуючи Інтернет. Вона описує структуру та протоколи, які змушують функціонувати глобальну мережу.

Виділяють мережеву архітектуру таких видів:

– архітектура термінал-головний комп'ютер;

– однорангова архітектура;

– архітектура клієнт-сервер.

Архітектура термінал-головний комп'ютер – це концепція інформаційної мережі, де вся обробка даних здійснюється одним чи групою головних комп'ютерів і передбачає два типи обладнання:

– головний комп'ютер, де здійснюється керування мережею, зберігання та обробка даних;

– термінали, призначені для передачі головному комп'ютеру команд на організацію сеансів, введення даних для виконання завдань та отримання результатів.

Прикладом архітектури мережі із головними комп'ютерами є системна мережева архітектура (System Network Architecture – SNA).

Однорангова архітектура **(**Peer-to-peer, P2P, рівний до рівного) – варіант архітектури системи, в основі якої стоїть мережа рівноправних вузлів. До однорангових мереж відносяться невеликі мережі, де кожна робоча станція може виконувати одночасно функції файлового сервера та робочої станції, дисковий простір та файли на будь-якому комп'ютері можуть бути спільними. При з'єднанні комп'ютерів користувачі можуть надавати ресурси та інформацію у спільне користування. Залежно від налаштування захисту даних інші

користувачі зможуть користуватися файлами відразу після створення такої мережі.

Переваги: мережі легко налаштовуються, окремі персональні комп’ютери (ПК) не залежать від виділеного сервера, мінімум обладнання та програмного забезпечення, відсутня потреба в адміністраторі.

Недоліки: при відключенні комп'ютерів від мережі, зникають сервіси, які вони надавали; безпеку мережі одночасно можна застосувати лише до одного ресурсу, і користувач повинен пам'ятати стільки паролів, скільки є мережевих ресурсів; падіння продуктивності роботи комп'ютера при доступу до ресурсу, що розділяється; відсутність централізованого адміністрування.

Архітектура клієнт-сервер – обчислювальна чи мережева архітектура, у якій завдання чи мережне навантаження розподілені між постачальниками послуг (*серверами*), та замовниками послуг (*клієнтами*).

Фактично *клієнт* та *сервер* – це програмне забезпечення. Зазвичай програми розташовані на різних обчислювальних машинах і взаємодіють між собою через обчислювальну мережу за допомогою мережевих протоколів, але можуть бути розташовані також і на одній машині. *Програми-сервери* очікують від *клієнтських програм* запити та надають їм свої ресурси у вигляді даних (наприклад, передача файлів за допомогою HTTP, FTP, BitTorrent, потокове мультимедіа або робота з базами даних) або у вигляді сервісних функцій (наприклад, робота з електронною поштою, спілкування за допомогою систем миттєвого обміну повідомленнями або перегляду веб-сторінок у всесвітній павутині). Оскільки одна *програма-сервер* може обробляти і виконувати запити від багатьох *програм-клієнтів*, її розміщують на спеціально виділеній обчислювальній машині, налаштованій особливим чином, як правило, спільно з іншими програмами-серверами, тому продуктивність цієї машини повинна бути високою. Через особливу роль такої машини в мережі, специфіки її обладнання

та програмного забезпечення її також називають *сервером*, а машини, що виконують клієнтські програми, відповідно, *клієнтами*.

У клієнт-серверній архітектурі виділяється чотири групи об'єктів: клієнти, сервери, дані та мережеві служби. Клієнти розміщуються у системах на робочих місцях користувачів. Дані переважно зберігаються на серверах. Мережеві служби є спільно використовуваними серверами та даними. Крім того, служби керують процедурами обробки даних.

Багаторівнева архітектура клієнт-сервер – різновид архітектури клієнт-сервер, в якій функція обробки даних винесена на кілька окремих серверів. Це дозволяє розділити функції зберігання, обробки та подання даних для більш ефективного використання можливостей серверів та клієнтів. Приватний випадок багаторівневої архітектури – трирівнева архітектура.

Мережа з виділеним сервером (client/server network) – це локальна обчислювальна мережа (LAN), в якій мережеві пристрої *централізовані* та керуються одним або декількома серверами. Індивідуальні робочі станції або клієнти (наприклад, персональний комп'ютер) повинні звертатися до ресурсів мережі через сервер/сервери.

Переваги мережі клієнт-серверної архітектури: мережі із великою кількістю робочих станцій; централізоване управління обліковими записами користувачів, безпекою та доступом, що спрощує мережеве адміністрування; швидкий доступ до мережевих ресурсів; користувачеві потрібен один пароль для входу в мережу та для доступу до всіх ресурсів, на які поширюються права користувача.

Недоліки: несправність сервера робить мережу непрацездатною, можливість втрати мережевих ресурсів; потреба у кваліфікованому персоналі для адміністрування; більш висока вартість мереж та мережевого обладнання.

Архітектура на основі хмари. Хмарні мережі пропонують послуги та

сховище через Інтернет. Користувачам не потрібно підтримувати своє обладнання та програмне забезпечення; натомість вони можуть отримувати доступ до програм та сховищ, наданих постачальниками хмарних послуг. Така гнучкість забезпечує легке масштабування та глобальну доступність.

Тема 2. Апаратне та програмне забезпечення комп'ютерних мереж

Комп'ютерна мережа (КМ) – це комплекс взаємопов'язаних, узгоджено функціонуючих *апаратних* і *програмних* компонентів, її роботу забезпечують технічні (апаратні), програмні, інформаційні та організаційні ресурси.

2.1 Апаратне забезпечення комп'ютерних мереж

Апаратні ресурси мережі, або апаратне забезпечення – це фізичні пристрої, які забезпечують підключення, передачу даних і управління мережею. До основних компонентів апаратного забезпечення належать: комп'ютери, сервери, канали передавання даних (канали зв'язку/кабельні системи), мережеве обладнання (активне та пасивне).

Активне мережеве обладнання – це «інтелектуальні» пристрої, необхідні для передачі і прийому даних (мережевий адаптер, комутатор, маршрутизатор тощо). Таке обладнання не тільки отримує і передає *сигнал*, але і обробляє цю технічну інформацію, перенаправляючи і розподіляючи вхідні потоки відповідно з вбудованими в пам'ять пристрою алгоритмами. Для роботи активного обладнання потрібне живлення (від електричної мережі або інших джерел), воно містить електронні схеми, виконує функції посилення, перетворення сигналів.

Під пасивним мережним устаткуванням маються на увазі компоненти, не наділені «інтелектуальними» особливостями, які не потребують живлення та не обробляють сигнали, а лише забезпечують фізичне з'єднання між пристроями. Вони не аналізують, не змінюють і не маршрутизують трафік.

Мережеві пристрої

Мережева плата /мережева карта /мережевий адаптер, NIC (network interface controller) – це периферійний пристрій, що дозволяє комп'ютеру взаємодіяти з іншими пристроями мережі (рис. 5).

Рисунок 5 – Мережева карта / адаптер

Повторювач, ретранслятор або репі́тер (repeater) – це мережеве обладнання для підсилювання сигналу (рис. 6). Призначений для збільшення відстані мережного з'єднання шляхом повторення електричного сигналу.

Рисунок 6 – Підсилювачі / ретранслятори сигналу

Мережевий комутатор (network switch) або світч (switch, «перемикач») – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента (рис. 7). Комутатор передає дані лише безпосередньо отримувачу. Це підвищує продуктивність і безпеку мережі, рятуючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися.

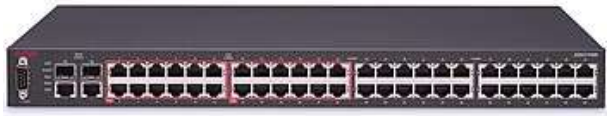


Рисунок 7 – Комутатор

Маршрутизатор/*роутер* (router) – визначає маршрути передавання даних; розподіляє дані на такі, що залишаються в межах однієї мережі, і такі, що повинні бути передані до іншої мережі, та пересилає дані; може здійснювати трансляцію адреси відправника й одержувача; фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу; шифрування/дешифрування даних тощо (рис. 8).

Рисунок 8 – Маршрутизатори

Точка доступу / *точка бездротового доступу* (wireless access point, WAP) – пристрій, що дозволяє бездротовим пристроям підключатися до провідної мережі за допомогою Wi-Fi, Bluetooth або інших бездротових підключень. Служить центральним вузлом для бездротової комунікації, дозволяючи пристроям приєднуватися до мережі та отримувати доступ до інтернету та інших ресурсів (рис. 9).

Рисунок 9 – Точки доступу

Мережа Internet складається з безлічі мереж, які мають різне апаратне та програмне забезпечення. Шлюзи та мости дозволяють з'єднувати такі мережі між собою.

Мережевий міст (бридж, bridge) – пристрій, основним призначенням якого є об'єднання сегментів комп'ютерної мережі (іноді різних топологій та архітектури), з'єднує дві окремі комп'ютерні мережі, щоб забезпечити зв'язок між ними та дозволити їм працювати як єдина мережа, знижує навантаження в мережі, виконуючи фільтрацію трафіку (рис. 10). Мости використовують виключно в локальних мережах. Наприклад, точка доступу уможливлює з'єднання дротового і бездротового сегментів мережі (виконує функції моста між ними). Типи мережевих мостів: простий міст (з'єднує два сегменти); многопортовий міст – схожий на комутатор (switch); програмний міст (наприклад, у Windows можна створити «мережевий міст» між адаптерами); Wi-Fi міст (з'єднання двох мереж через бездротове з'єднання).

Рисунок 10 – Пристрої з функціями мережевих мостів

Мереже́вий шлюз (gateway) – апаратний маршрутизатор або програмне забезпечення для сполучення комп'ютерних мереж, що використовують різні протоколи (наприклад, локальної та глобальної мереж). Мережевий шлюз конвертує протоколи одного фізичного середовища у протоколи іншого фізичного середовища (при з'єднанні локального комп'ютера з Інтернетом зазвичай використовується мережевий шлюз). Мережевий шлюз – це точка мережі, яка є виходом в іншу мережу. Роутери є одним із прикладів апаратних мережевих шлюзів, або сервер, що контролює трафік між локальною мережею компанії та мережею Інтернет – це мережевий шлюз.

Пасивне мережеве устаткування

Кабелі – служать для передачі сигналів (вита/кручена пара, оптоволоконні або коаксіальні).

Коннектори (роз'єми) – використовуються для з'єднання кабелів з портами пристроїв (RJ-45, SC, LC тощо)

Патч-корди – готові до використання, заторцьовані на кінцях кабелі з конекторами для з'єднання пристроїв у мережі.

Патч-панелі – панелі для організованого підключення кабелів у серверних або телекомунікаційних шафах.

Кросові панелі – елементи для з'єднання і зміни кабельних трас у розподільчих шафах.

Мережеві розетки – стаціонарні точки підключення мережі на стінах офісу або приміщення.

Кабель-менеджери – органайзери для охайного укладання кабелів у шафах або вздовж стін.

Шафи та стійки – серверні або телекомунікаційні шафи для розміщення активного і пасивного обладнання.

Перехідники, муфти, з'єднувачі – використовуються для з’єднання або подовження кабелів.

Мережевий кабель

При побудові дротових каналів передачі даних використовують три типи кабелів: вита пара, оптоволоконний і коаксіальний кабелі.

Вита (кручена) пара – вид мережевого кабелю з однією або декількома парами ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини) для зменшення взаємних наведень при передачі сигналу і покритих пластиковою оболонкою (рис. 11). Використовується для

побудови мереж у багатьох технологіях, наприклад, Ethernet, ARCNet, Token ring. Поки ще вита пара є найпоширенішою для побудови локальних мереж.

Рисунок 11 – Кабель «вита пара»

Для захисту від електричних завад при використанні високочастотних сигналів, в кабелях використовується екранування. Залежно від наявності захисту – електрично заземленої мідної сітки або алюмінієвої фольги навколо скручених пар, визначають різновиди цієї технології:

– неекранована вита пара (UTP);

– екранована вита пара (STP);

– фольгована вита пара (FTP);

– фольгована екранована вита пара (SFTP).

Існує декілька категорій кабелю вита пара, які нумеруються від *Cat 1* до *Cat 8* (Cat від «Category»). Кабель вищої категорії зазвичай містить більше пар дротів і кожна пара має більше витків на одиницю довжини.

Основні характеристики кабелю «вита пара» надано в таблиці 1.

Якщо порівняти кабелі *Cat 5* та *Cat 6* – обидві категорії можуть працювати зі швидкістю до 1000 Мбіт/с (1 гігабіт за секунду), підтримують передачу сигналу без спотворення на відстань до 100 метрів. Головна різниця між цими проводами полягає у пропускній здатності. Кабелі *Cat 6* розраховані на робочі частоти до 250 МГц, а *Cat 5e* лише до 100 МГц.

Таблиця 1 – Характеристики кабелю «вита пара»

Категорія	Максимальна швидкість	Частота	Типова довжина	Опис
Cat 5e	до 1 Гбіт/с	100 МГц	до 100 м	Стандарт для домашніх мереж
Cat 6	до 10 Гбіт/с (до 55 м)	250 МГц	до 100 м	Краща ізоляція, рекомендований для нових мереж
Cat 6a	до 10 Гбіт/с (до 100 м)	500 МГц	до 100 м	Посилене екранування
Cat 7 / 8	10-40 Гбіт/с	600–2000 МГц	до 100 м	Використовується в дата-центрах

Оптоволоконний кабель – це кабель на основі *волоконних світловодів*, який призначений для передачі оптичних сигналів у вигляді *фотонів*. Він є основою магістральних (backbone) мереж Інтернету, міжконтинентальних з'єднань і високошвидкісних каналів зв’язку. Головним елементом такого кабелю є прозоре скловолокно, інформація в ньому передається не *електричним* сигналом, а *світловим*. Головна перевага даного кабелю полягає у високому рівні захищеності і відсутності випромінювання, він забезпечує не тільки високу швидкість передачі інформації, але і захист від несанкціонованого доступу.

Оптоволоконний кабель має виняткові характеристики стосовно перешкодозахищеності і секретності інформації, яка передається. Ніякі зовнішні електромагнітні перешкоди не здатні спотворити світловий сигнал, який в свою чергу не породжує зовнішні електромагнітні випромінювання.

Волоконно-оптичні лінії зв'язку (ВОЛЗ) дозволяють передавати аналогові та цифрові сигнали на далекі відстані (до 100 км без підсилювачів), мають великі пропускні показники – понад 10 Гбіт/с (що дорівнює 10 мільярдам біт на секунду), які значно перевищують можливості мідної сировини. Швидкість потоку інформації залежить від типу оптичного дроту (одномодовий,

багатомодовий). Для передачі на великі відстані (понад 100 км), використовують одномодовий кабель. Багатомодовий кабель зазвичай використовується для менших відстаней, наприклад, до 550 метрів при швидкості 10 Гбіт/с.

Переваги оптики: це імунітет до шумів та перешкод, малий діаметр кабелів при величезній пропускній здатності, стійкість до злому та перехоплення інформації, відсутність потреби в ретрансляторах та підсилювачах тощо.

Конструкція кабелів оптоволокна (рис. 12) може бути досить різноманітною, але загальними є такі компоненти: оптичне волокно (світловод/серцевина/ядро), буферна оболонка, силовий елемент, зовнішня оболонка. Серцевина оптичного волокна – це центральна частина волоконно-оптичного кабелю, якою поширюється світло.

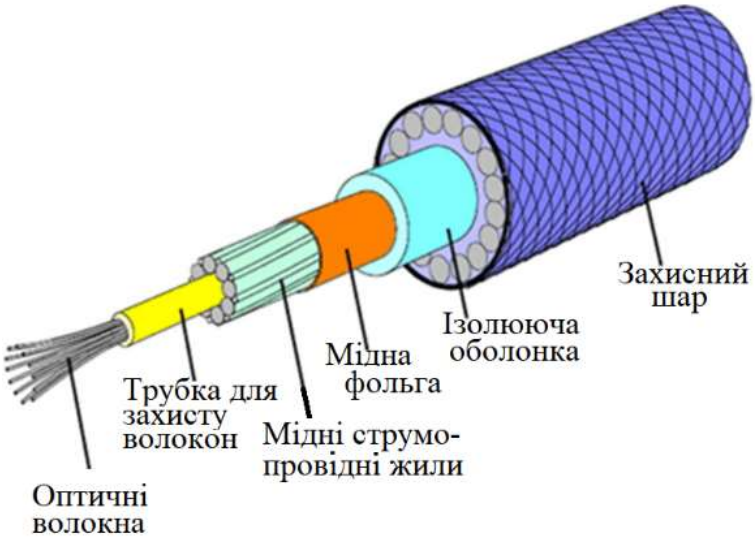


Рисунок 12 – Схематична структура оптоволоконного кабелю

Оптоволоконний кабель ділиться на два типи: одномодовий (single-mode, SM/OS1/OS2) і багатомодовий (multi-mode, OM1–OM5). Основні відмінності між цими типами пов'язані з різними режимами проходження світлових променів у кабелі (табл. 2).

Таблиця 2 – Типи оптоволоконних кабелів

Тип кабелю	**Тип світловоду**	**Застосування**	**Особливості**
Single-mode (SM)	Один вузький промінь	Глобальні мережі, магістралі, зовні і всередині будинків	Довгі відстані, висока пропускна здатність
Multi-mode (MM)	Кілька променів	Локальні мережі, дата-центри	Коротка відстань (до 2 км), обладнання більш дешевше

Одномодовий оптоволоконний кабель – оптоволоконний кабель, по якому передається світлова хвиля однієї частоти (одна мода). Завдяки малому діаметру серцевини оптичне випромінювання поширюється по волокну в одній моді, що сприяє відсутності межмодової дисперсії. Одномодовий кабель (рис. 13-а, б) має джерело лазерного випромінювання – лазерний приймач, використовує світло виключно з необхідною довжиною хвилі. Практично всі промені, що утворюються, проходять один і той же шлях, завдяки чому доходять до приймача одночасно. Форма сигналу майже не спотворюється. Саме цей кабель є пріоритетним у здійсненні комунікацій на великих відстанях.

Багатомодовий кабель для передачі сигналу використовує звичайний, не лазерний світлодіод. Від передавача світлові промені йдуть трохи хаотично, їх траєкторії мають помітний розкид, у результаті форма сигналу на приймальному кінці кабелю спотворюється (рис. 13-в).

Діаметр світловоду у волоконно-оптичних лініях, як правило, становить близбко 9 мікрометрів для одномодового волокна, і 50 або 62,5 мікрометрів для багатомодового волокна. Розмір оболонки, яка оточує серцевину, зазвичай становить 125 мікрометрів для обох типів волокон. Світловоди виготовляються з двох основних матеріалів: скла (найчастіше кварцового) та пластику. Скловолокно використовується для передачі даних на великі відстані,

пластикове волокно частіше застосовується для ближнього зв'язку та в деяких спеціальних застосуваннях.

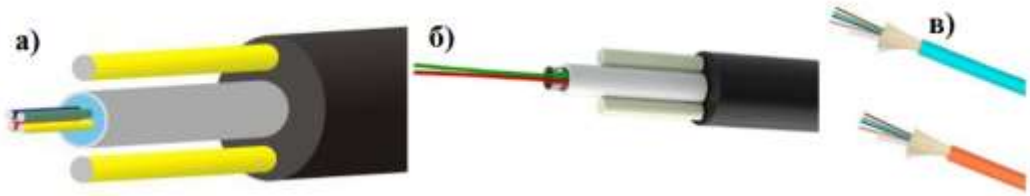


Рисунок 13 – Оптоволоконний кабель

Коаксіальний кабель. У сучасних комп'ютерних мережах для підключення антен зазвичай використовують коаксіальний кабель (рис. 14). Він добре підходить для передачі високочастотних сигналів. В основі *коаксіального кабелю* використовується мідний дріт, який, в свою чергу оточений шаром ізольованого матеріалу. Виділяють два типи коаксіального кабелю: тонкий (діаметром до 5 мм) і товстий (діаметром до 10 мм). Механічні, температурні та електричні характеристики дозволяють використовувати коаксіальний кабель в кабельних трасах з несприятливими умовами експлуатації (підземні траси, повітряні лінії).

Рисунок 14 – Коаксіальний кабель

Конектори

Конектор – це роз'єм, який використовується для підключення мережевого кабелю до мережевого обладнання (рис. 15).

Найпоширеніший тип коннектора для мережевого кабелю – це RJ-45 (скорочення від Registered Jack 45). Його використовують для підключення

кабелів типу «вита пара» (Ethernet, UTP/STP) у локальних мережах. RJ45 зареєстрований стандарт роз'єму, який був розроблений у США для мережевих кабелів.

RJ-45 має 8 контактів (8P8C), якими передаються сигнали. Кабель вставляється в конектор і обжимається спеціальним інструментом – *кримпером*, забезпечуючи надійне фізичне та електричне з'єднання.

Рисунок 15 – Конектор RJ-45

Існують інші типи конекторів (рис. 16) для інших типів кабелів – оптоволоконні конектори (SC, LC, ST, FC).

Рисунок 16 – Конектори для оптоволоконного кабелю

SC (Subscriber Connector) – конектор прямокутний, пластиковий корпус з фіксуючою засувкою, діаметр ферули 2,5 мм. Забезпечує швидке з'єднання завдяки механізму «push-pull» (вставити-витягнути), використовується в телекомунікаційних мережах та центрах обробки даних.

LC (Lucent Connector) – компактний роз'єм з фіксуючою засувкою, діаметр ферули 1,25 мм. Завдяки меншому розміру, LC-конектори дозволяють розмістити більше портів на одному пристрої, зручні для високощільних мережевих підключень, таких як комутатори та маршрутизатори.

ST (Straight Tip) – конектор має циліндричний металевий корпус з байонетним замком (поворотне з'єднання), діаметр ферули 2,5 мм з надійним з'єднанням, стійким до вібрацій. Використовується в промислових мережах та деяких старих мережевих інфраструктурах.

FC/UPC – тип оптоволоконного з'єднувального кабелю, який має конектори типу *FC* з поліруванням *UPC (Ultra Physical Contact)* на обох або одному кінці.

SC, LC, ST конектори можуть бути використані як з одномодовими (single-mode), так і з багатомодовими (multi-mode) оптоволоконними кабелями, залежно від специфікації.

Патч-корд

Патч-корд – це короткий з’єднувальний кабель із конекторами на обох кінцях для підключення мережевого обладнання. Є *мідні* Ethernet (рис. 17) і *оптоволоконні* (рис. 18) патч-корди.

Рисунок 17 – Мідний патч-корд. а) UTP-Cat.5e; б) S/FTP- Cat.6A

Рисунок 18 – Оптичні патч-корд: а) звичайний, комбінований FC/UPC-SC/UPC б) мультимодовий MM OM4 LC-LC.

Патч-панелі

Патч-панель – це комутаційний пристрій для налаштування з’єднання кабелів у телекомунікаційних шафах. Вона виконує роль *централізованого з’єднувального вузла* між різними мережевими пристроями, комутаторами або кросами.

Патч-панель – це *інтерфейсна* панель, до якої можна легко підключати та відключати пристрої через патч-корди. Ці панелі забезпечують швидку та зручну комутацію мережевих з'єднань, переважно задіяні для користувачів, IT-адміністраторів.

Крос – це спеціальне місце або пристрій для організації, з’єднання та комутації кабелів зв'язку, переважно у структурованих кабельних системах (СКС), телефонних або оптоволоконних мережах. Крос – це «точка збору» всіх кабелів, в якій їх зручно підключати, перемикати або тестувати

Мідні патч-панелі (Ethernet) – використовуються з кабелями Cat 5e, Cat 6, Cat 6a, мають порти *RJ-45*, кожен порт ззаду має клеми типу IDC, куди підключається витапарний кабель, застосовуються у локальних мережах, офісах, дата-центрах (рис. 19).

Рисунок 19 – Мідні патч-панелі

Оптоволоконні патч-панелі призначені для організації оптоволоконних з’єднань, мають порти під SC, LC, ST, FC, можуть бути з касетами для зварювання, адаптерами та кабельними лотками для зручного укладання волокна, застосовуються у магістральних мережах, FTTH, дата-центри (рис. 20).

Рисунок 20 – Оптоволоконні патч-панелі: а) SC/UPC, б)FC/UPC, в) LC-Duplex

FTTH (Fiber To The Home) – технологія підключення інтернету, при якій оптичне волокно прокладається безпосередньо до оселі абонента (будинку, квартири, офісу).

Кросові панелі

Патч-панелі та кросові панелі (кроси) часто використовуються в одних і тих самих мережевих середовищах, але вони мають різне призначення, конструкцію та спосіб підключення.

Крос панель – це постійний *розподільний вузол*, де кабелі підключаються безпосередньо і стаціонарно, зручно використовувати для довготривалих та стабільних з'єднань (рис. 21). Застосовується частіше у магістралях, вузлах зв'язку, оптоволокні, для телеком-операторів.

Рисунок 21 – Кросові панелі

Мережеві розетки

Мережеві розетки – це елементи структурованої кабельної системи, призначені для з'єднання кінцевих пристроїв (наприклад, комп’ютерів, IP-телефонів, принтерів) з локальною мережею (рис. 22).

Основними характеристиками мережевих розеток є:

– тип інтерфейсу (для Ethernet найпоширеніший RJ-45);

– категорія (Cat.5e, Cat.6, Cat.6a, Cat.7 – залежить від швидкості мережі);

– кількість портів (одинарні, подвійні тощо);

– тип монтажу (вбудовуються в стіну або накладні);

– екранізація (UTP – неекрановані, STP/FTP – екрановані);

– сумісність (підключення до патч-панелей, комутаторів, роутерів тощо).

Рисунок 22 – Мережеві розетки: а_б - для Ethernet, в – для оптоволокна

Кабель-менеджери (кабель-менеджмент)

Для забезпечення порядку у приміщеннях із високими вимогами до організації простору використовуються принципи кабель-менеджменту. У зв’язку з цим застосовуються спеціальні аксесуари: затискачі, кабель-канали, кабельні органайзери, стяжки та хомути, кабельні гребінці (рис. 23). Кабель-менеджмент є основним принципом для створення організованої та завершеної сукупності телекомунікаційного обладнання та кабелів зв'язку. Ця система розроблена для правильної маршрутизації кабелів, спрощення їх обслуговування та оперативного внесення змін до початкової структури.

Рисунок 23 – Елементи кабель-менеджменту

Серверні / телекомунікаційні шафи

Шафи та стійки – це сховища для дорогого високотехнологічного обладнання (рис. 24). Якісним матеріалом для яких вважається сталь 1,5 мм товщиною. Функціонал серверних шаф значно широкий і потребує можливості установки хорошої системи охолодження всього внутрішнього простору, додаткових нестандартних пристроїв, різних кабельних організаторів та інших пристроїв .

Обладнання, що розміщується у шафах для серверів, живиться від електромережі. Тому обов’язково має бути передбачено заземлення серверної шафи, а живлення має подаватися в достатній кількості для всіх пристроїв, розміщених усередині.

Рисунок 24 – Серверні шафи та стійки

Перехідники, муфти, з'єднувачі

Перехідники, муфти та з’єднувачі для кабелів Ethernet використовуються для з'єднання, подовження або зміни типу підключення мережевих кабелів.

Для Ethernet

Перехідники Ethernet (адаптери) змінюють тип роз'єму (наприклад, з RJ-45 на USB або з RJ-45 на оптоволоконний порт), дозволяють підключати кабелі до пристроїв з різними портами (рис. 25).

З’єднувачі (куплери) Ethernet RJ-45 потрібні для: подовження кабелю без заміни всієї лінії; виправлення пошкоджень, без перетягування нового кабелю; забезпечення гнучкості у монтажі, особливо у важкодоступних місцях: заміни типу з’єднання для адаптації до різного обладнання.

Рисунок 25 – Перехідник та з'єднувач (Ethernet)

Перехідники, муфти та з’єднувачі для оптоволокна є ключовими елементами у побудові надійних волоконно-оптичних мереж.

Для оптоволокна

Оптоволоконні перехідники (адаптери): з'єднують два оптичні роз'єми одного або різного типу; забезпечують точне вирівнювання волокон для мінімізації втрат сигналу (рис. 26). Бувають одинарні (simplex) та подвійні (duplex). За типом адаптери бувають:

– однотипні: *SC-SC, LC-LC, ST-ST*;

– міжтипові: *SC-LC, SC-ST*.

– існують варіанти: *single-mode (SM)* та *multi-mode (MM).*

Оптичні з’єднувачі (механічні або швидкого монтажу): забезпечують тимчасове або постійне з’єднання двох оптичних волокон без зварювання; особливо доречні для польових умов або ремонтів. За типом розрізняють:

– механічний з’єднувач (Mechanical Splice): склеювання/вирівнювання волокон у пластиковій капсулі;

– Fast Connector: з’єднання волокна з конектором (1-2 хвилини).

Оптичні муфти (зварні муфти): захищають точку зварювання або з'єднання кількох волокон у мережі; використовуються для підземного, повітряного або настінного монтажу. За типом бувають:

– магістральні муфти (для з'єднання великої кількості волокон – до 96 і більше).

– купольні (куполоподібні): герметичні, для вуличного монтажу.

– касетні: з роз'ємами всередині для легкого доступу до зварок.

З'єднання оптоволокна вимагає точного вирівнювання серцевини волокна, тому якість муфт і перехідників критично впливає на втрати сигналу. У випадку *single-mode* волокон вимоги до точності з'єднання вищі, ніж у *multi-mode*.

Рисунок 26 – Адаптер, з'єднувач, зварна муфта (оптоволокно)

2.2 Програмне забезпечення мереж

Мережеве програмне забезпечення – це загальний термін, що використовується для опису широкого спектру програмного забезпечення, яке оптимізує роботу комп'ютерних мереж, дозволяє їх проєктування, моніторинг, організацію. Програмне забезпечення мережі включає в себе операційні системи, спеціалізовані мережеві програми для забезпечення функціонування, керування та безпеки мереж.

Обмін даними між комп'ютерами мережі уможливлюють кілька видів програмного забезпечення: мережні компоненти операційної системи; драйвери пристроїв; прикладні програми.

Операційні системи

Операційні системи для серверів забезпечують їх основні функції: управління файлами, користувачами, додатками, мережею. Прикладами таких операційних систем є Microsoft Windows Server, Linux (Ubuntu Server, CentOS Server), MacOS Server.

Операційні системи для клієнтів: сьогодні практично всі операційні системи мають вбудовані мережеві функції, тому взаємодія певного комп'ютера з іншими пристроями в мережі звичайна справа (Windows, Linux, macOS або мобільні операційні системи Android та iOS).

Операційні системи для мережевих пристроїв, таких як комутатор, маршрутизатор, фаєрвол (Cisco IOS, RouterOS, OpenWrt) з можливостями для роботи в комп'ютерних мережах.

Спеціалізовані мережеві програми

Діагностику мережного з’єднання та перевірку працездатності віддаленого вузла можна виконати вбудованими засобами Windows – утиліти Ping та Tracert (ОС Windows має кілька утиліт для діагностики стану мережі, але найчастіше використовуються Ping та Tracert).

Програма Ping відправляє запит зазначеному вузлу мережі і фіксує час між відправкою запиту та отриманням відповіді (RTT, Round Trip Time), дана утиліта дозволяє визначити час відгуку сервера, який цікавить.

Програма Tracert виконує надсилання тестового пакета вказаному вузлу мережі, відображаючи інформацію про всі проміжні маршрутизатори, через які пройшов пакет на шляху до запитаного вузла, а також мінімальний, максимальний та середній час відгуку кожного з них. Це дозволяє оцінити, наскільки «довгий» шлях пройшов пакет і на якій ділянці виникають найбільші затримки, пов’язані з передачею даних.

Програми для сканування локальної мережі дозволяють швидко визначити логічну схему ЛОМ та провести інвентаризацію комп'ютерів, периферійного та мережевого обладнання (Lansweeper, Spiceworks, Total Network Inventory, Zoho Creator тощо).

Lansweeper (Бельгія, платне ПЗ) надає можливість мережевим адміністраторам збирати докладну інформацію про мережні пристрої (принтери, комутатори, маршрутизатори), використовуючи можливості мережевого сканування SNMP (Simple Network Management Protocol – протокол керування мережею).

Spiceworks (США, безкоштовне ПЗ) – система, що дозволяє зібрати та структурувати інформацію про мережу: встановлене програмне забезпечення (ПЗ), журнали подій, інвентаризація мережного обладнання, навіть витрати картриджів у мережевих принтерах.

Для тестування і аналізу мережевого трафіку використовуються інструменти, які мають загальну назву сніфери (sniffer) або перехоплювачі (interceptor), які по суті виконують функцію проксі-сервера. Сніфер підключається у канал зв’язку між клієнтом (додатком, аплікацією) та сервером, й пропускає через себе їх мережевий трафік, відповідно має можливість його відстежувати.

Мережеві інтерфейси

Інтерфейс – це сукупність засобів, методів і правил взаємодії між елементами системи. Мережеві інтерфейси (Network Interfaces) – це апаратні або програмні компоненти, що забезпечують зв’язок між пристроєм/користувачем та мережею. Мережевий інтерфейс може бути представлений у вигляді фізичного апаратного забезпечення, такого як мережева карта, або програмного компонента, такого як віртуальний мережевий інтерфейс. Також, це програми,

що забезпечують взаємодію між користувачем і мережею (браузери, поштові клієнти, програмне забезпечення для доступу до віддалених серверів тощо). Мережеві інтерфейси є ключовими компонентами для взаємодії пристроїв у мережах.

Фізичні мережеві інтерфейси

Мережева карта (NIC, Network Interface Card):

– Ethernet-підключення через мідні або оптичні кабелі (має ім'я eth0, enp3s0);

– Wi-Fi, бездротове підключення до мережі через радіочастотний сигнал (wlan0, wlp2s0);

– Fiber Optic, оптоволокно, підключення для високошвидкісного обміну даними.

Віртуальні інтерфейси

– VLAN, віртуальні локальні мережі, що дозволяють створювати кілька логічних мереж на одному фізичному інтерфейсі.

– VPN, віртуальна приватна мережа, що забезпечує захищене з'єднання через публічні мережі.

– Loopback, спеціальний тип мережевого інтерфейсу, що використовується для тестування і діагностики мережевих програм на локальному пристрої (ім'я – lo; localhost, адреса інтерфейсу – 127.0.0.1).

Приклади використання мережевих інтерфейсів:

– комп'ютер з мережею (мережевий інтерфейс використовується для підключення до інтернету через Ethernet або Wi-Fi);

– віртуалізація (віртуальні машини використовують віртуальні мережеві інтерфейси для комунікації з хостом або іншими віртуальними машинами).

Мережеві протоколи

Все програмне забезпечення засобів зв'язку засноване на *протоколах*, які являють собою *набори* семантичних і синтаксичних правил, що визначають, яким чином повинні діяти різні пристрої для встановлення з'єднання. Існує близько 7 тисяч різних мережевих протоколів, але всі вони виконують одну з трьох основних дій: *комунікація*, *управління мережею*, *безпека*.

- *TCP/IP* (набір протоколів мережі Інтернет);
- *HTTP/HTTPS* (протоколи, для передачі даних через веб-браузери);
- *FTP* (протокол передачі файлів між пристроями в мережі);
- *SMTP*(комунікаційний протокол для пересилання електронної пошти);
- *POP3* (протокол прийому електронних повідомлень).

Безпека мережі

Забезпечення інформаційної безпеки комп'ютерної мережі та її ресурсів є комплексним питанням. Серед апаратних і програмних засобів, що застосовуються для цієї мети виділяють: міжмережеві екрани (фаєрволи, Firewalls), антивірусні програми, засоби моніторингу мережі, засоби виявлення спроб несанкціонованого доступу (вторгнення), проксі-сервери та сервери аутентифікації, які забезпечують мережну безпеку, контролюють вхідний та вихідний інтернет-трафік, контролюють мережеву активність програм, захищають від хакерів, завантаження шкідливого програмного забезпечення. Особливу цінність становлять методи інтелектуального захисту у вигляді нейронних мереж.

Тема 3. Стандарти і протоколи комп’ютерних мереж. Еталонна модель OSI.

3.1 Мережеві стандарти

Сучасний глобалізований світ не може існувати без стандартів, які підтримують співпрацю пов'язаних між собою об'єктів. Мережеві стандарти є нормативною документацією, що встановлює комплекс норм, правил, вимог до об'єктів мережі. Стандарти розробляються науковими та інтернет-організаціями (наприклад: IETF, консорціуми W3C та Юнікод).

Документація RFC

Майже всі стандарти Глобальної мережі існують у вигляді опублікованих заявок RFC (Request for Comments). Як документи RFC виходять не лише *стандарти*, але й концепції, введення в нові напрямки у дослідженнях, результати експериментів, посібники з впровадження технологій, пропозиції та рекомендації щодо розвитку вже існуючих стандартів інформаційних технологій.

RFC – це серія пронумерованих документів, які визначають стандарти, протоколи, методології та інновації, пов'язані з роботою Інтернету. Вони розробляються та публікуються Інженерною радою Інтернету (IETF) або іншими організаціями. Ці документи описують технічні специфікації, що забезпечують сумісність між різними системами, протоколами та додатками, а також регулюють способи передачі даних та взаємодію мережевих технологій.

До уваги: RFC є документом, який описує специфікації для технології, що рекомендується. Якщо специфікація ратифікована, вона стає документом стандартів. Не всі RFC стають стандартами; деякі з них позначені на невизначений термін із інформаційним чи експериментальним статусом.

Приклади: RFC 1256 – виявлення маршрутизатора в мережі; RFC 1591 – структура доменних імен; RFC 2525 – проблеми TCP.

Стандарти IEEE («ай-трипл-і»)

Інститут інженерів з електротехніки та електроніки (IEEE, Institute of Electrical and Electronics Engineers) – міжнародна організація інженерів у галузі електротехніки, радіоелектроніки та радіоелектронної промисловості. Світовий лідер в галузі розроблення *стандартів* з електроніки та електротехніки. Штаб-квартира організації розташована в Піскатавей, Нью-Джерсі (США). Організація була утворена в 1963 році внаслідок злиття американських співтовариств IAEE (American Institute of Electrical Engineers) та IRE (Institute of Radio Engineers).

Організація IEEE [7] описує себе як «найбільше у світі технічне професійне суспільство, що сприяє розвитку та застосуванню електротехнологій та суміжних наук на благо людства, розвитку професії та благополуччя людства». Має в своєму складі багато груп, кожна з яких відповідає за свій напрямок.

IEEE 802 – група стандартів сімейства IEEE, що стосуються локальних обчислювальних мереж (LAN) та мереж мегаполісів (MAN). Зокрема стандарти IEEE 802 обмежені мережами з пакетами змінної довжини.

IEEE 802.3 – стандарти сімейства IEEE, групи IEEE 802: відносяться до функціонування комп'ютерних мереж. Роди́ну (сімейство) цих протоколів також називають Ethernet.

IEEE 802.11 – набір стандартів бездротового зв'язку з використанням радіохвиль (частотні діапазони 0,9; 2,4; 3,6; 5; 6 та 60 ГГц) та видимого світла (так званий Li-Fi), призначений для створення комп'ютерних мереж (більш відомий за назвою Wi-Fi).

IEEE 802.15.1 – стандарт, що описує побудову персональних бездротових мереж (Wireless Personal Area Network, WPAN/Bluetooth).

На сьогодні загальноприйнятою технологією, яка використовується для обміну даними в комп'ютерних мережах є Ethernet. Технологія Ethernet

переважно описується стандартами IEEE групи 802.3 і є однією з найпоширеніших технологій ЛОМ ще з середини 1990-х років.

3.2 Протоколи комп’ютерних мереж

Вся робота комп'ютерів у мережі, незалежно від її призначення та розмірів, зводиться лише до одного – обміну інформацією. Необхідною умовою для узгодженої взаємодії всіх учасників процесу обміну даними є дотримання певних правил, які називаються мережевими (комунікаційними) протоколами.

Мережевий протокол – це встановлений набір правил, що визначають, як дані передаються між різними пристроями однієї мережі, він дозволяє підключеним пристроям спілкуватися один з одним, незалежно від будь-яких відмінностей у їхніх внутрішніх процесах, структурі чи дизайні. Протоколи забезпечують та визначають формат обміну інформацією між учасниками комп'ютерних мереж.

Мережеві протоколи зазвичай створюються відповідно до галузевих стандартів різними мережевими або інформаційними організаціями. Наступні групи визначили та опублікували різні мережеві протоколи:

– інститут інженерів з електротехніки та електроніки (IEEE, Institute of Electrical and Electronics Engineers);

– цільова група з інжинірингу Інтернету (IETF, Internet Engineering Task Force);

– міжнародна організація зі стандартизації (ISO, International Organization for Standardization);

– міжнародна спілка електрозв'язку (MCE, ITU – International Telecommunication Union);

– консорціум Всесвітньої павутини (W3C, World Wide Web Consortium).

Протокол в певному сенсі вважається мовою, необхідною машинам для взаємодії. Серед його ключових особливостей – *структурованість* і *стандартизація*. У роботі мереж задіяна велика кількість протоколів. Наприклад, завантаження сторінки в браузері – це результат роботи, організованої за кількома протоколами:

– за протоколом HTTP/ HTTPs браузер формує повідомлення для сервера;

– згідно DNS браузер дізнається IP-адресу сайту за його доменним ім'ям;

– за протоколом TCP встановлюється з'єднання та гарантується цілісність передачі даних, а за протоколом IP здійснюється адресація в мережі.

Безліч протоколів можна класифікувати за мережевими рівнями, де вони працюють. Найбільш поширені *мережеві моделі* – це OSI та TCP/IP. Модель OSI є широко прийнятою структурою, що описує, як різні мережеві протоколи взаємодіють для надання мережевих послуг.

3.3 Еталонна модель OSI

На момент зародження комп'ютерних мереж не існувало моделей, які визначали б загальні стандарти роботи мереж та підходи до їх проєктування. Окремі компанії, що працювали над створенням мереж, реалізовували власні задуми, які не стикувалися з рішеннями інших розробників комп'ютерних мереж. Через архітектурні відмінності, мережі, які мали об'єднувати комп'ютери, створювали перепони для розширення. Однією з організацій, що займалася вирішенням проблем несумісностей у мережах, була міжнародна організація зі стандартизації ISO (International Organization for Standardization), яка у 1984 році представила модель OSI (Open Systems Interconnection/Взаємодія відкритих систем).

Модель OSI складалася з двох основних компонентів:

– абстрактної моделі мережі (яка називається *базовою еталонною моделлю* або семирівневою моделлю);

– набору мережевих протоколів.

Еталонна модель OSI вважається великим досягненням у *стандартизації* концепцій мережевої взаємодії. Модель складається з 7 мережевих рівнів, кожному з яких відведена своя роль та функції (рис.27).

Рисунок 27 – Еталонна модель OSI

У процесі передачі даних завжди беруть участь пристрій-*відправник*, пристрій-*одержувач* та самі *дані*, які мають бути передані та отримані. Все, що відбувається при надсиланні та прийомі даних, описує семирівнева модель OSI.

Кожен рівень комп'ютера-відправника взаємодіє з таким же рівнем комп'ютера-одержувача, ніби вони пов'язані безпосередньо. Такий зв'язок називається *логічним* або *віртуальним* зв'язком.

Приклад: користувач *А* має намір відправити по мережі *картинку*. На сьомому рівні моделі OSI вона є *даними*. І ось ці дані необхідно так упакувати, щоб вони могли дістатися до пункту призначення *Б*, і щоб отримувач зміг їх

розпізнати/прочитати. Для цього дані повинні пройти обробку протоколами всіх семи рівнів – від сьомого до першого: *дані* → *біти* (процес *упаковки* даних для їх передачі через мережу називається *інкапсуляцією*), а потім у вигляді сигналів через певне середовище доставлені до одержувача. Комп'ютер-одержувач користувача *Б* приймає сигнали, перетворює їх у цифрові (біти), які надалі мають стати даними (цей зворотний процес розпаковки називається *декапсуляцією*).

На кожному із семи рівнів інформація подається у вигляді *фрагментів даних* протоколу PDU (таблиця 3).

PDU (Protocol Data Unit) – узагальнена назва/одиниця *даних*, яка передається або обробляється, на різних рівнях моделі OSI: кадр Ethernet, IP-пакет, UDP-датаграма, TCP-сегмент.

Таблиця 3 – Узагальнена назва даних відповідно до рівня моделі OSI

<table>
<tr><th colspan="2">Семирівнева модель OSI</th><th>PDU</th><th colspan="3">Стан</th></tr>
<tr><td>7</td><td>Прикладний (application layer)
взаємодія з користувачем і додатками</td><td rowspan="3">Дані</td><td rowspan="4">Host layers</td><td rowspan="6">↓ Інкапсуляція</td><td rowspan="6">↑Декапсуляція</td></tr>
<tr><td>6</td><td>Представницький (presentation layer, L6)
форматування даних, кодування /декодування/ шифрування</td></tr>
<tr><td>5</td><td>Сеансовий (session layer, L5)
керування сеансом зв’язку</td></tr>
<tr><td>4</td><td>Транспортний (transport layer, L4)
надійна передача даних між кінцевими точками</td><td>Сегмент. Датаграма. Блоки</td></tr>
<tr><td>3</td><td>Мережевий (network layer, L3)
Визначення маршруту; IP-адресація</td><td>Пакет</td><td rowspan="3">Media layers</td></tr>
<tr><td>2</td><td>Канальний (data link layer, L2)
керування доступом до середовища</td><td>Кадр</td></tr>
<tr><td>1</td><td>Фізичний (physical layer, L1)
передача сигналів по фізичному середовищу</td><td>Біт</td></tr>
</table>

У горизонтальній моделі OSI потрібен *загальний протокол* для обміну даними. У вертикальної моделі сусідні рівні обмінюються даними з використанням інтерфейсів прикладних програм API (Application Programming Interface).

Перший рівень, фізичний (physical layer, L1)

Найнижчий рівень відповідає за фізичну передачу даних між пристроями (обмін фізичними сигналами між фізичними пристроями) – здійснення передавання сигналів через кабель або радіоефір і, відповідно, їх прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів. На цьому рівні вирішуються питання, пов'язані із фізичними аспектами передачі даних: метод передачі даних, характеристики мережного середовища, модуляція сигналу.

Пристрої фізичного рівня оперують бітами. На цьому рівні працюють повторювачі сигналу, медіаконвертери.

При обміні даними каналами зв'язку використовуються три методи передачі:

- симплексна (односпрямована): TV, радіо;
- напівдуплексна: прийом та передача даних здійснюються по черзі;
- дуплексна (двонаправлена): кожна станція одночасно передає та приймає дані.

Другий рівень, канальний (data link layer, L2)

Канальний рівень працює у межах локальної мережі. Він формує отримані від фізичного рівня дані (потік бітів) у новий формат – кадр, знаходить початок та кінець повідомлення. Задача рівня – сформувати кадри (фрейми) з MAC-адресою пристрою-відправника та пристрою-одержувача, після чого відправити їх по мережі. На цьому рівні вирішуються завдання: адресація

всередині локальної мережі, пошук помилок, перевірка цілісності даних. Основні мережеві протоколи: PPP та стандарт Ethernet.

Пристрої: комутатор, мережевий міст (bridge). Їхня переважна відмінність від пристроїв фізичного рівня – ведення таблиць MAC-адрес по своїх портах і розсилка/фільтрація трафіку вже тільки за необхідними напрямками.

Третій рівень, мережевий (network layer, L3)

На третьому рівні з'являється нове поняття – маршрутизація. Одиниця інформації – пакети. Мережевий рівень призначений для визначення шляху передачі даних, вирішує глобальні логістичні задачі передавання даних між різними сегментами великих мереж:

– маршрутизація (визначення оптимальних шляхів між мережами);

– фільтрація, оптимізація (відстеження неполадок/заторів у мережі), контроль якості;

– логічна адресація (присвоєння та керування IP-адресами);

– фрагментація (розділення великих пакетів даних на менші фрагменти передачі);

– перенаправлення (забезпечення передачі даних через проміжні вузли).

На мережному рівні використовується протокол ARP (Address Resolution Protocol, протокол визначення адреси), який перетворює IP-адреси пристроїв у їх відповідні MAC-адреси.

На третьому рівні задіяні символьні імена вузлів, за відповідність яких IP-адресам відповідають протоколи мережного рівня.

Пристрої, що працюють на цьому рівні – маршрутизатори, шлюзи. Реалізуючи у собі три перших рівня стека протоколів, вони об'єднують собою різні мережі, перенаправляють пакети з однієї в іншу, вибираючи за певними правилами їх маршрут, ведуть статистику передачі, забезпечують безпеку за рахунок таблиць фільтрації. Маршрутизатори отримують MAC-адресу від

комутаторів з попереднього рівня та займаються побудовою маршруту від одного пристрою до іншого з урахуванням усіх потенційних несправностей у мережі.

Протоколи мережевого рівня: IP/IPv4/IPv6 (Internet Protocol), IPX (Internetwork Packet Exchange, протокол міжмережевого обміну), X.25 (частково цей протокол реалізований на рівні 2), CLNP (мережевий протокол без організації з'єднань), IPsec (Internet Protocol Security). Протоколи маршрутизації - RIP (Routing Information Protocol), OSPF (Open Shortest Path First).

Четвертий рівень, транспортний (transport layer, L4)

Рівень наскрізної передачі даних, він надає сам механізм передачі. Протоколи транспортного рівня забезпечують двосторонній зв'язок комунікаційних сервісів. Підтримує сегментацію та мультиплексування. Блоки даних він розділяє на фрагменти, розмір яких залежить від протоколу, короткі поєднує в один, довгі розбиває.

Основні завдання транспортного рівня:

– розбивка повідомлень сеансового рівня на пакети, їхня нумерація;

– буферизація прийнятих пакетів;

– впорядочення пакетів, що прибувають;

– адресація прикладних процесів (дані потрапляють до конкретного адресата, на конкретний порт; порти потрібні для того, щоб дані були отримані саме тією службою або процесом, які їх запитували);

– керування потоком.

На цьому рівні працюють два основних протоколи TCP та UDP, які здійснюють зв'язок між кінцевими системами (машиною-відправником пакетів і машиною-адресатом пакетів) для додатків верхнього рівня і забезпечують різний сервіс:

– *UDP* (User Datagram Protocol): протокол реалізує негарантовану доставку даних;

– TCP (Transmission Control Protocol): протокол реалізує гарантовану доставку даних.

TCP забезпечує надійну передачу даних між двома хостами. Він дозволяє клієнту і серверу додатка встановлювати між собою логічне з'єднання і потім використовувати його для передачі великих масивів даних, ніби між ними існує пряме фізичне з'єднання. Протокол дозволяє здійснювати дроблення потоку даних, підтверджувати одержання пакетів даних, задавати тайм-аути, організовувати повторну передачу у випадку втрати даних.

Протокол UDP реалізує набагато більш простий алгоритм передачі, забезпечуючи ненадійну доставку даних без установлення логічного з'єднання, не гарантує послідовність, відсутність втрат та дублювання, але завдяки відсутності цих можливостей не має так званого «службового» трафіку. Він просто посилає пакети даних (дейтаграми), з однієї машини на іншу, але не надає жодних гарантій їхньої доставки.

Транспортний рівень в залежності від доступної йому мережевої служби (або служб) визначає можливість надання потрібного сервісу. До основних параметрів якості обслуговування транспортного рівня відносяться: затримка встановлення з’єднання, ймовірність невдалого встановлення з’єднання, пропускна здатність, затримка доставки, залишкова доля помилок, захист, пріоритет, стійкість з’єднання.

Затримка встановлення з’єднання являє собою проміжок часу між запитом транспортного з’єднання і отриманням підтвердження. Цей параметр включає в себе час обробки запиту віддаленим транспортним об’єктом.

Ймовірність невдалого встановлення з'єднання означає ймовірність того, що з'єднання не буде встановлено за максимальний час затримки встановлення з'єднання, наприклад, через перенавантаження мережі.

Пропускна здатність визначає кількість переданих байтів даних за секунду. Пропускна здатність визначається окремо у кожну сторону.

Затримка доставки показує час від моменту відправки повідомлення користувачем транспортного рівня комп'ютером-відправником до його отримання користувачем транспортного рівня комп'ютером-одержувачем. Як і пропускна здатність, затримка доставки вимірюється у кожну сторону окремо.

Залишкова доля помилок визначає відношення втрачених або пошкоджених повідомлень до загальної кількості повідомлень. Теоретично залишкова доля помилок повинна дорівнювати нулю, так як компенсація всіх помилок, які з'являються на мережевому рівні, складає задачу транспортного рівня.

Параметр захисту дозволяє користувачеві транспортного рівня виявити свою зацікавленість у наданні транспортним рівнем захисту від несанкціонованого доступу сторонніх осіб до даних, що передаються.

Значення пріоритету дозволяє користувачеві транспортного рівня вказати, що деякі його з'єднання є більш важливими, ніж інші. У випадку перевантаження мережі з'єднання з більш високим пріоритетом будуть обслуговуватися у першу чергу.

Адреса на транспортному рівні називається *портом*: число від 1 до 65535. Кожний мережний застосунок на вузлу має свій порт. Номери портів у застосунках не повторюються. Приклад форми запису: 10.18.49.20:80 (IP-адреса: порт).

Мережевий порт – це ідентифікуємий номером системний ресурс, що виділяється додатку на деякому мережевому хості, для зв'язку з додатками, що

виконуються на інших мережевих хостах (у тому числі з іншими додатками на цьому ж хості).

Для кожного з протоколів TCP і UDP стандарт визначає можливість одночасного виділення на хості до 65536 унікальних портів, що ідентифікуються номерами від 0 до 65535. При передаванні по мережі номер порту зазначається в заголовку пакета і використовується (разом з IP-адресою хоста) для адресації конкретної програми (і конкретного мережевого з'єднання).

Усі порти поділені на три діапазони: загальновідомі (системні, 0–1023), зареєстровані (користувальницькі, 1024–49151) та динамічні (приватні, 49152–65535). Деякі загальновідомі порти:

– порт 80: HTTP; порт 443: HTTPS (веб-трафік, зв'язок між веб-браузером та веб-сервером);

– порт 22: SSH (криптографічний мережевий протокол для безпечної передачі даних, Secure Shell);

– порт 25: SMTP (передача електронних листів між поштовими серверами);

– порт 53: DNS (канал, який поєднує *запити* та *відповіді* DNS, сприяє у перетворенні доменних імен на IP-адреси).

Перші чотири рівні моделі – спеціалізація мережевих інженерів (системних адміністраторі), з останніми трьома вони не так часто стикаються, бо п'ятим, шостим та сьомим займаються розробники програмного забезпечення.

П'ятий рівень, сеансовий (session layer, L5)

Сеансовий рівень відповідає за підтримку сеансу чи сесії зв'язку, обмежує час з'єднання (сесії) одного вузла з іншим; контролює права доступу; синхронізує початок, кінець обміну; керує взаємодією між програмами, обміном інформацією. Сеансовий рівень дозволяє взаємодіяти мережевим програмам тривалий час і має вирішувати таке:

– створювати сеанс зв'язку;

– завершувати сеанс зв'язку;

– підтримувати обмін інформацією між програмами;

– здійснювати синхронізацію між приймальним та передавальним пристроєм;

– підтримувати сеанс зв'язку, коли передавання даних не ведеться.

Служби сеансового рівня найчастіше застосовуються серед додатків, які потребують віддаленого виклику процедур, тобто вимагають виконання дій на віддалених комп'ютерах або незалежних системах на одному пристрої (за наявності кількох ОС).

Прикладом роботи п'ятого рівня може бути відеодзвінок по мережі. Під час відеозв'язку необхідно, щоб два потоки даних (аудіо та відео) йшли синхронно. Коли до розмови двох людей під'єднається третя – вийде вже конференція. Завдання п'ятого рівня зробити так, щоб співрозмовники могли зрозуміти, хто зараз говорить.

Шостий рівень, представницький/подання даних (presentation layer, L6)

Завданням представницького рівня є представлення даних у зрозумілому для відправника та одержувача вигляді, представляє дані (які все ще є PDU) у зрозумілому для людини та машини вигляді, відповідає за можливість діалогу між програмами на різних машинах. Він забезпечує перетворення (кодування, компресію/стиснення) даних прикладного рівня у потік даних для транспортного рівня. Наприклад, коли один пристрій вміє відображати текст тільки в кодуванні ASCII, а інший тільки в UTF-8, перетворення тексту з одного кодування в інше відбувається на шостому рівні. До представницького рівня можна віднести різні варіанти подання даних: шифрування та дешифрування, кодування тексту за допомогою ASCII або UTF-8, специфікації HTML, графічні формати JPEG, PNG, GIF.

Сьомий рівень, прикладний (application layer)

Рівень програм, з якими працюють кінцеві користувачі, забезпечує взаємодію мережі й користувача. На цьому рівні працюють всі прикладні програми, які використовують доступ до мережі: оглядачі веб-сторінок (браузери), електронна пошта, віддалений доступ до файлів, програми для відео та аудіо- зв'язку тощо.

3.4 Модель TCP/IP

Модель TCP/IP була розроблена в 1970-х роках в рамках проєкту ARPANET і стала стандартом для мережі Інтернет та комп'ютерних мереж загалом.

TCP/IP (Transmission Control Protocol / Internet Protocol) – це набір мережевих протоколів, що використовується для організації зв’язку в Інтернеті. Модель TCP/IP описує, як дані передаються від одного комп'ютера до іншого через мережу. Модель базується на наборі протоколів, де головними є *IP* (Internet Protocol), який забезпечує адресацію і маршрутизацію пакетів та *TCP* (Transmission Control Protocol) – відповідає за надійну передачу даних.

Структура моделі TCP/IP

Модель TCP/IP поділяється на чотири рівні – прикладний (application), транспортний (transport), міжмережевий (internet) та рівень доступу до середовища передачі (рис. 28). Основні принципи роботи:

– *прикладний рівень* (Application layer) забезпечує інтерфейс для користувачів та програм, взаємодію між додатками та визначає формат переданих даних.

– *транспортний рівень* (Transport Layer) здійснює надійну передачу даних між додатками, при цьому дані поділяються на пакети.

– *мережевий рівень* (Internet Layer) займається маршрутизацією даних між різними мережами, визначаючи оптимальний шлях передавання даних.

– *рівень мережевих інтерфейсів* (Network Interface Layer) або *канальний рівень* (Link Layer): надаючи доступ до фізичного середовища передавання даних, він визначає метод передавання даних цим середовищем.

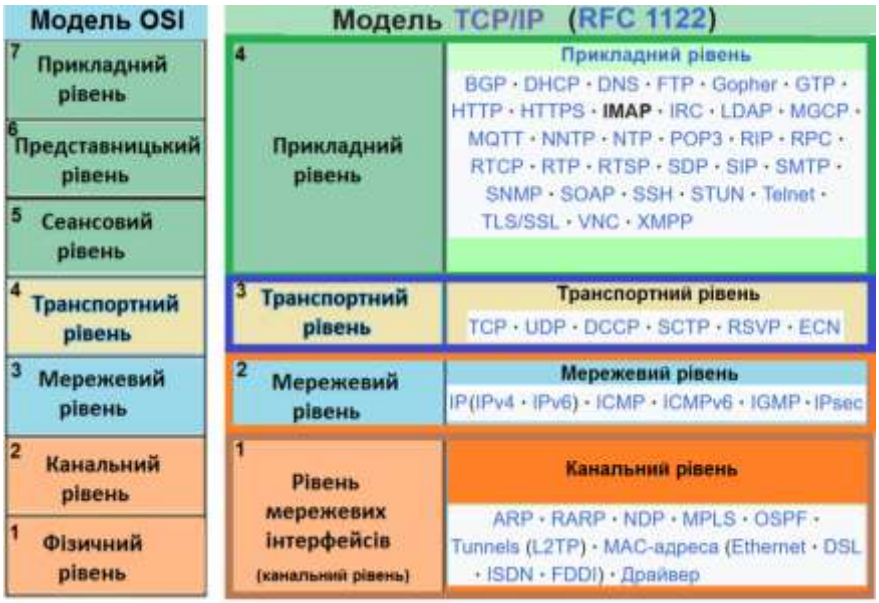


Рисунок 28 – Порівняння моделей OSI та TCP/IP

Ключові функції стеку протоколів TCP/IP наступні:

– адресація: використовує IP-адреси для ідентифікації пристроїв у мережі;

– пакування: розділяє дані на пакети для передавання мережею, кожен із заголовком;

– маршрутизація: визначає шлях для надсилання даних від одного комп’ютера до іншого;

– повторне передавання: забезпечує надійне доставлення даних із використанням повторного передавання пакетів;

– шифрування: надає механізми для захисту даних з використанням шифрування.

Протоколи стеку TCP/IP

IP (Internet Protocol) – забезпечує маршрутизацію/доставку пакетів даних від відправника до отримувача, використовує IP-адреси для зазначення місця розташування пристроїв у мережі.

TCP (Transmission Control Protocol) – протокол з підключенням та гарантованою доставкою пакетів. Спочатку проводиться обмін спеціальними пакетами для встановлення з'єднання, далі по цьому з'єднанню посилаються пакети TCP (процес TCP-рукостискання) з перевіркою, чи пакет дійшов до одержувача.

UDP (User Datagram Protocol) – протокол без підключення та з негарантованою доставкою пакетів, сконцентрований на швидкій передачі даних. Надає швидкий, але менш надійний спосіб передавання даних.

ICMP (Internet Control Message Protocol) – відповідає за управління мережею та обробку помилок, виявляє помилки та допомагає усунути проблеми в мережі (наприклад, запитувана послуга недоступна, хост/маршрутизатор не відповідають).

DHCP (Dynamic Host Configuration Protocol) протокол автоматичної конфігурації в IP-мережах, спрощує процес підключення до мережі, надаючи клієнту IP-адресу, повідомляє IP-адресу DNS-сервера та IP-адресу шлюзу за замовчуванням.

DNS (Domain Name System) – виконує роль довідника в інтернеті, перетворює доменні імена в IP-адреси.

HTTP (Hypertext Transfer Protocol) / *HTTPS* (Hypertext Transfer Protocol Secure) – забезпечують зв’язок між браузерами і серверами. HTTP – для звичайних з’єднань, HTTPS – для безпечних транзакцій із шифруванням.

RIP (Routing Information Protocol), OSPF (Open Shortest Path First) – протоколи маршрутизації, що займаються вивченням топології мережі, визначенням маршрутів, і складанням таблиць маршрутизації, на основі яких протокол IP переміщає пакети в потрібному напрямку.

ICMP (Internet Control Message Protocol) використовується для передачі повідомлень про помилки та інші виняткові ситуації, що виникли під час передачі даних (наприклад, запитувана послуга недоступна, хост/маршрутизатор не відповідають).

ARP (*Address Resolution Protocol*) – протокол визначення адреси, в локальних мережах протокол ARP використовує широкомовні кадри протоколу канального рівня для пошуку в мережі вузла із заданою IP-адресою (визначає MAC-адресу цільового комп'ютера за його IP-адресою).

У сімействі протоколів IPv6 протокол ARP відсутній, його функції покладено на протокол ICMPv6 (ICMPv6 – невід'ємна частина протоколу IPv6, визначений у RFC 4443).

Тристороннє рукостискання TCP (TCP handshake)

TCP-рукостискання (three-way handshake) є процедурою взаємодії між двома пристроями (комп'ютерами, клієнтом та сервером) в мережі для встановлення з'єднання, яка відбувається на транспортному рівні протоколу TCP. Процес включає обмін спеціальними пакетами даних, які підтверджують готовність обох сторін передачі інформації і складається з трьох етапів: SYN, SYN-ACK та ACK. Він гарантує, що обидві сторони готові до передачі даних та погоджуються на параметри з'єднання.

Етапи процесу Three-Way Handshake:

1. *SYN* (synchronize) – ініціатор з’єднання відправляє пакет із прапором SYN, повідомляючи про потребу встановлення зв’язку і вказуючи початковий номер послідовності.
2. *SYN-ACK* (synchronize-acknowledge) – отримувач відповідає пакетом із прапорами SYN і ACK, підтверджуючи отримання запиту і відправляючи свій початковий номер послідовності.
3. *ACK* (acknowledge) – ініціатор відправляє підтвердження ACK отримання пакету від відповідача.

По завершенню трьох етапів TCP-рукостискання з’єднання встановлене і можливе передавання даних.

Набір протоколів TCP/IP є основою Інтернету, дозволяючи різним комп’ютерам і мережам взаємодіяти незалежно від обладнання та операційних систем, забезпечує гнучкість і масштабованість мереж.

ЗАПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ ДО РОЗДІЛУ 1

1. Поняття телекомунікації. Що становить сучасні телекомунікації? Розташуйте надані поняття в хронологічному порядку їх виникнення: системи електронної комерції, телебачення, телеграф, радіозв’язок, телефонний зв’язок, системи глобального позиціонування, комп’ютерні мережі.
2. Яку мережу вважають родоначальницею сучасних комп’ютерних мереж? Коли розпочався бурхливий розвиток комп’ютерних мереж? Основні причини.
3. Дайте визначення поняття комп'ютерна мережа. За якими ознаками класифікують комп'ютерні мережі?
4. Що таке топологія комп’ютерної мережі? Види топологій.
5. Яка мережна топологія характеризується підключенням усіх вузлів до одного центрального пристрою:
    a. шина
    b. зірка
    c. кільце
6. Що таке мережева архітектура?
7. Апаратне забезпечення комп’ютерної мережі, основні характеристики.
8. Призначення мережевого адаптера (NIC), основні характеристики та параметри мережевих карт.
9. Поясніть принцип роботи комутатора (switch) у мережі.
10. Яка основна функція маршрутизатора:
    a. зберігання даних
    b. пересилання пакетів між мережами

c. шифрування даних

d. визначення MAC-адреси

11. В чому різниця між комутатором і маршрутизатором?

12. Призначення і основні властивості точки доступу (Access Point).

13. Середовища передачі даних у комп'ютерних мережах, основні властивості.

14. Основні типи кабелів для підключення мережевого обладнання та їхні характеристики.

15. Чим відрізняється кручена пара від оптоволоконного кабелю?

16. Поясніть різницю між крученою парою категорії 5 і категорії 6.

17. Які стандарти Ethernet існують і чим вони відрізняються?

18. Що таке MAC-адреса і яке її значення в мережі? Чи може один пристрій мати декілька MAC-адрес.

19. Які типи мережевого обладнання можна віднести до активного, а які – до пасивного?

20. Що таке шлюз (gateway) і яка його роль у мережі?

21. Поясніть принцип роботи оптичних трансиверів.

22. Яке апаратне забезпечення використовується для побудови бездротових мереж?

23. Що таке мережеве програмне забезпечення і які його основні види?

24. Що таке мережевий протокол? Наведіть приклади основних мережних протоколів.

25. Що таке мережевий моніторинг і які інструменти для нього існують?

26. Модель OSI: назвіть та коротко охарактеризуйте кожен рівень.

27. Яка різниця між моделлю OSI і моделлю TCP/IP?

28. Що таке порт у контексті мережі?

29. Який порт використовується за замовчуванням для HTTPS?

a. 21

b. 80
c. 443
d. 25

30. Що таке тристороннє рукостискання (three-way handshake):
    a. спосіб з’єднання в UDP
    b. механізм встановлення TCP-з’єднання
    c. метод шифрування
    d. тип маршрутизації
31. Що таке маршрутизація? Основні протоколи маршрутизації.
32. Який протокол дозволяє транслювати імена доменів у IP-адреси:
    a. FTP
    b. DNS
    c. HTTP
    d. SMTP
33. Який з наведених протоколів працює на транспортному рівні?
    a. IP
    b. TCP
    c. Ethernet
    d. ARP
34. Що таке NAT і навіщо він потрібен?
35. Поясніть різницю між IPv4 та IPv6.
36. Яка максимальна довжина IPv4-адреси:
    a. 32 біти
    b. 64 біти
    c. 128 біт
    d. 256 біт
37. Що таке URL. Яка різниця між доменним ім'ям сайту та його URL?

РОЗДІЛ ІІ. ТЕХНОЛОГІЇ КОМП’ЮТЕРНИХ МЕРЕЖ

Тема 4. Поняття та визначення локальних мереж

Локальна мережа **(LAN)** – це інформаційне середовище, яке об'єднує в єдине ціле комп'ютери, сервери, пристрої зберігання даних, мережеве обладнання та програмне забезпечення. У локальній мережі може бути всього кілька комп'ютерів, а можуть бути тисячі робочих станцій в межах однієї організації.

Локальна мережа складається з кабелів, точок доступу, комутаторів, маршрутизаторів та інших компонентів (рис. 29), які дозволяють пристроям підключатися до внутрішніх серверів, веб-серверів або інших локальних мереж, через глобальні. Пристрої можуть використовувати єдине підключення до Інтернету, обмінюватися файлами один з одним, друкувати на спільних принтерах.

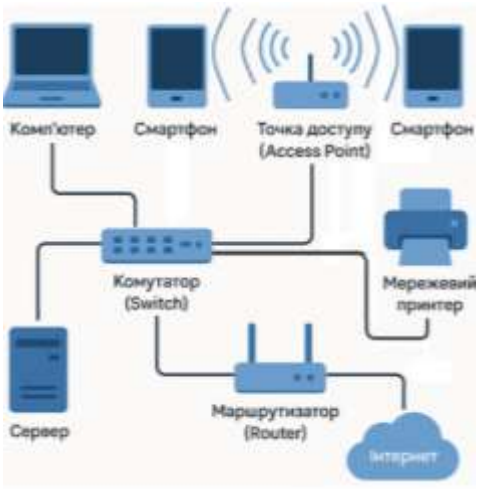


Рисунок 29 – Типова схема локальної мережі

Хронологічно першими з'явилися глобальні мережі, які об'єднували територіально розосереджені комп'ютери. В 1969 році міністерство оборони США ініціювало роботи по об’єднанню в єдину *мережу* суперкомп’ютерів захисних та науково-дослідних центрів. Ця мережа, яка отримала назву

ARPANET, стала відправною точкою для створення першої і самої відомої глобальної мережі світового масштабу – Internet.

Винахід великих інтегральних схем на початку 70-х років призвів до створення міні-комп'ютерів, цінова політика яких влаштовувала багато підприємств і давала їм можливість придбання власних комп'ютерів навіть для невеликих своїх підрозділів. Таким чином з'явилася концепція розподілення комп'ютерних ресурсів по всьому підприємству, однак при цьому всі комп'ютери однієї організації працювали автономно. Потреба обміну електронними даними з користувачами інших підрозділів в автоматичному режимі призвела до розгляду можливостей об'єднання розрізнених комп'ютерів між собою в єдину локальну мережу.

Спочатку для з'єднання комп'ютерів один з одним застосовувалися нестандартні мережеві технології. Тобто набір програмних і апаратних засобів та механізми передавання даних не були єдиними, узгодженими між собою.

У середині 1970-х років наукові установи та компанії почали використовувати мережі з кількох комп'ютерів, які потребували:

– спільного доступу до ресурсів (принтерів, дискових накопичувачів, терміналів);

– передачі файлів між машинами.

На той момент існували окремі, малоефективні способи зв'язку:

– послідовні з'єднання: RS-232 (повільні, для пари пристроїв);

– шинні топології без управління (конфлікти і повільна передача).

Із зростанням обсягів даних зростала необхідність передавати їх швидше, ніж дозволяли існуючі інтерфейси. Початковою технологією, придатною для повноцінної роботи комп'ютерної мережі став Ethernet (зі швидкістю 2,94 Мбіт/с).

Ethernet був розроблений у 1973 році інженером Робертом Меткалфом в дослідницькому центрі Xerox PARC (Palo Alto Research Center).

Офіційно технологію Ethernet було стандартизовано у 1980 році в рамках першого специфікаційного документа DIX (Digital, Intel, Xerox), а перший офіційний стандарт IEEE 802.3 вийшов у 1983 році. Це був ключовий момент в історії комп'ютерних мереж, який зробив можливим створення сучасних локальних мереж (LAN) і став основою для більшості сучасних мережевих технологій.

В середині 80-х років стан справ у локальних мережах кардинально змінився. Були винайдені і затверджені стандартні мережеві технології об’єднання комп’ютерів у мережу – Ethernet, Arcnet, Token Ring, Token Bus, FDDI. Починаючи з кінця 90-х років явним лідером серед технологій локальних мереж є родина Ethernet. Отже Ethernet (IEEE 802.3) – основна технологія дротових локальних мереж до якої відносяться:

– *Ethernet*, класична технологія (стандарт IEEE 802.3) – швидкість передачі 10 Мбіт/с;

– *Fast Ethernet* (IEEE 802.3u) – 100 Мбіт/с;

– Gigabit Ethernet, 1G (IEEE 802.3ab, 802.3z) – 1 Гбіт/с;

– сучасні стандарти (IEEE 802.3ae, 802.3ba та ін.):

- 10-Gigabit Ethernet (10G) – 10 Гбіт/с і вище;
- 40G, 100G, 400G Ethernet (для дата-центрів).

Технології локальних мереж також становлять:

– *PoE* (Power over Ethernet) – передача живлення по мережевому кабелю (камери, точки доступу);

– *Wi-Fi* (IEEE 802.11) – бездротовий доступ:

– *VLAN* (Virtual LAN) – логічне поділення фізичної мережі на окремі віртуальні сегменти для ізоляції трафіку, підвищення безпеки та керованості. Сучасні реалії сприяють зростанню популярності віртуальних локальних мереж.

4.1 Технологія Ethernet

Технологія Ethernet є монополістом, виштовхнувши спочатку всі інші технології канального рівня з локальних мереж, а після зробила теж саме в області глобальних мереж. До середини 2000-х років Ethernet застосовувалася виключно в локальних мережах.

Практично всі технології 80-х років (Ethernet також) використовували середовище, що розділяється (розподілене середовище). З середини 90-х в локальних мережах почали застосовувати комутовані версії технологій. Відмова від середовища, що розділяється дозволила збільшити пропускну здатність і масштабованість локальних мереж. Перевагою комутованих локальних мереж є можливість логічної структуризації мережі з подальшим її розподілом на окремі сегменти – VLAN.

Розподіл середовища означає, що всі вузли мережі користуються ним, але по черзі і в будь-який момент часу по цьому середовищу передається кадр тільки одного вузла.

Ethernet традиційно використовується для локальних мереж, сучасні технології розширили його можливості, дозволяючи застосовувати Ethernet і в глобальних мережах. Завдяки розвитку технологій оператори зв’язку можуть надавати Ethernet-послуги на великі відстані, включаючи міжміські, міжнародні та міжконтинентальні з’єднання.

Основні характеристики Ethernet

Ранні технології Ethernet (сімейство стандартів 10M Ethernet, швидкість 10 Мбіт/с) тривалий час задовольняли потреби користувачів локальних мереж.

Історично, топологією Ethernet була шинна топологія – усі комп'ютери під'єднані до одного коаксіального кабелю, що виконує роль «магістралі», по якій передаються всі дані. Якщо два пристрої передають одночасно, виникає колізія (накладання сигналів). Для її запобігання використовується метод доступу до середовища CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – механізм виявлення колізій (застарілі версії із коаксіальним кабелем та хабами).

Сучасна топологія Ethernet – зірка, з використанням комутаторів та маршрутизаторів. Середовище, що розділяється, майже витіснене комутованими мережами, де кожен пристрій має свій окремий канал до комутатора (switch), і передача відбувається без колізій (повнодуплексно).

Типи кабелів. Вита пара (Cat5e, Cat6, Cat6a, Cat7). Оптоволоконні кабелі (для довгих та високошвидкісних з'єднань). Коаксіальні кабелі (старі версії).

Роз'єми. RJ-45 - найпоширеніший для кручений пари. LC, SC та ін. - для оптоволоконних з'єднань.

Максимальна довжина сегмента. До 100 м для крученої пари без повторювачів. До кількох кілометрів для оптоволокна (залежно від стандарту).

Кадри Ethernet. Розмір: від 64 до 1518 байт (без урахування тегів VLAN). Містять адреси відправника та одержувача (MAC-адреси), тип даних, дані та контрольну суму.

MAC-адресація. Унікальні 48-бітові адреси, які присвоюються мережевим інтерфейсам.

Рівні Ethernet

Відповідно до сімейства стандартів IEEE 802.x у протоколах локальних мереж виділено три функціональні рівні:

– фізичний;

– рівень доступу до середовища (Media Access Control, MAC);

– рівень управління логічним каналом (Logical Link Control, LLC).

Визначення фізичного рівня стандарту IEEE 802 повністю відповідає визначенню фізичного рівня моделі OSI, який містить опис характеристик технології: типи фізичного середовища, методи кодування, типи з'єднувальних роз'ємів тощо. Функції канального рівня моделі OSI у стандартах IEEE 802 представлені двома рівнями – MAC та LLC.

Виділення функцій доступу до середовища в окремий рівень відображає їх важливість при використанні середовища.

Рівень MAC виконує такі основні функції: надає вузлу доступ до середовища з подальшою доставкою кадру від вузла джерела до вузла призначення відповідно до його адреси. Рівень MAC дав назву адресам локальних мереж, назви MAC-адреси та адреси Ethernet використовуються як рівноправні.

Хоча рівень MAC відповідає за доставку кадру вузлу призначення, він не забезпечує його надійну доставку. Цю функцію реалізує рівень LLC, призначення якого можна порівняти з призначенням транспортного рівня моделі OSI, саме протоколів TCP і UDP.

Логічний рівень визначає три типи послуг:

– послуга LLC1 (послуга без встановлення з'єднання та без підтвердження отримання даних);

– послуга LLC2 (послуга, яка дозволяє користувачеві встановити логічне з'єднання перед початком передачі будь-якого блоку даних і при необхідності виконати процедури відновлення після помилок та впорядкування потоку блоків у рамках встановленого з'єднання);

– послуга LLC3 (послуга без встановлення з'єднання, але з підтвердженням отримання даних).

Який із трьох режимів роботи рівня LLC буде використаний залежить від вимог протоколу верхнього рівня.

Технологія Ethernet спочатку функціонувала в дейтаграмному режимі (він найпростіший), обладнання Ethernet і після опублікування стандарту IEEE 802.2 продовжувало підтримувати лише цей режим роботи, який формально є режимом LLC1.

Кадри технології Ethernet

Ethernet кадр (фрейм) – це структура даних, яка використовується для передачі інформації по мережі Ethernet. Він містить кілька ключових полів, кожне з яких має свою функцію (рис. 30). Вони забезпечують ефективний і надійний спосіб передачі інформації між пристроями в локальних мережах.

Існує декілька типів формату Ethernet-кадрів:

– Ethernet II (DIX): найпоширеніший формат, використовується для мереж TCP/IP (рис. 30);

– IEEE 802.3: має дещо іншу структуру, де поле Length замінює EtherType;

– Ethernet SNAP: розширена версія IEEE 802.3 з підтримкою більшої кількості протоколів.

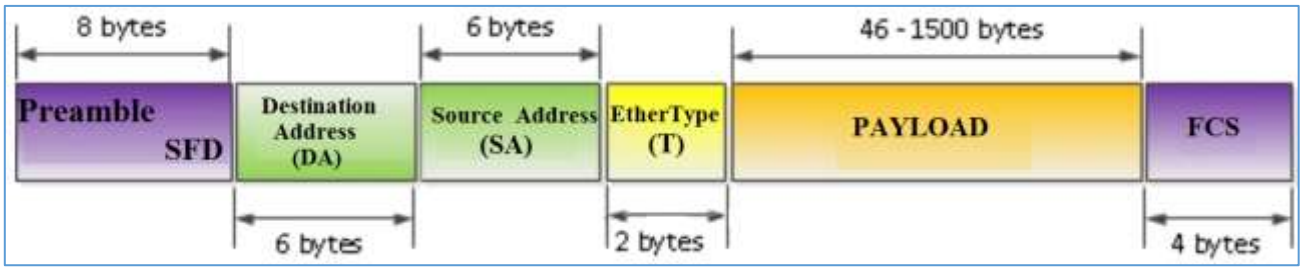


Рисунок 30 – Формату Ethernet-кадру

Основні компоненти кадру Ethernet:

– Preamble (Преамбула, 7 байт). Служить для синхронізації приймача і передавача, складається з чередування 1 і 0.

– Start Frame Delimiter (SFD, 1 байт). Позначає початок кадру, послідовність бітів: 10101011.

– Destination Address (MAC-адреса отримувача, 6 байт). Унікальна апаратна адреса пристрою, для якого призначені дані.

– Source Address (MAC-адреса відправника, 6 байт). Унікальна апаратна адреса пристрою, який відправляє кадр.

– EtherType/Length (2 байти). Визначає тип даних, що передаються (наприклад, IPv4, IPv6) або довжину корисного навантаження.

– Payload (дані, 46-1500 байт). Основна частина кадру, яка містить корисні дані. Може бути від 46 до 1500 байт, залежно від типу Ethernet.

– Frame Check Sequence (FCS, 4 байти). Поле для перевірки помилок, яке містить контрольну суму (CRC).

MAC-адреса

На рівні MAC використовуються регламентовані стандартом IEEE 802.3 унікальні 6-байтові адреси. Зазвичай MAC-адреса записується у вигляді шести пар шістнадцяткових цифр (наприклад, 11-A0-16-3C-BC-15).

Формат запису:

– шістнадцятковий формат: 00:1A:2B:AC:34:76;

– без роздільників: 001A2BAC3476;

– через тире: 00-1A-2B-AC-34-76;

– через крапки: 001a.2bac.3476 (використовується в деяких пристроях Cisco).

Кожен мережевий адаптер має принаймні одну MAC-адресу. Крім окремих інтерфейсів, MAC-адреса може визначати групу інтерфейсів і навіть усі інтерфейси мережі. Перший (молодший) біт старшого байта адреси призначення визначає, чи є адреса індивідуальною або груповою. Якщо він дорівнює 0, то

адреса є індивідуальною, тобто ідентифікує один мережевий інтерфейс, а якщо 1, то груповим.

У випадку, коли мережевий інтерфейс включено до групи, то разом із унікальною MAC-адресою, із нею асоціюється ще одна адреса – групова. Групова адреса пов'язана лише з інтерфейсами, сконфігурованими (вручну або за автоматичним запитом вищого рівня) як для членів групи, номер якої вказаний у груповій адресі. Коли групова адреса складається з усіх одиниць (у шістнадцятковому поданні це 0xFFFFFFFFFFFF), вона ідентифікує всі вузли мережі і називається широкомовною.

Спеціальні біти:

– Універсальний/локальний біт (U/L bit, 7-й біт першого байта):

- 0 – універсально призначена адреса (OUI).
- 1 – локально адмініструєма адреса (може бути задана вручну).

– Груповий/Унікальний біт (I/G bit, 8-й біт першого байта):

- 0 – унікальна (Unicast) адреса.
- 1 – групова (Multicast) адреса.

Другий біт старшого байта MAC-адреси визначає спосіб призначення адреси – централізований чи локальний. Якщо цей біт дорівнює 0 (що буває завжди в стандартній апаратурі Ethernet), це говорить про те, що адреса призначена централізовано за правилами IEEE 802.

Комітет IEEE розподіляє між виробниками обладнання організаційно-унікальні ідентифікатори (Organizationally Unique Identifiers, OUI) – це унікальні 24-бітові префікси, що привласнюються кожній організації (зазвичай виробнику мережного обладнання) для ідентифікації їх пристроїв у мережах. OUI використовується як частина MAC-адреси.

Основні характеристики OUI

1. Структура MAC-адреси:

– перші 24 біти (3 октети) - OUI, належать конкретному виробнику.

– останні 24 біти – унікальний серійний номер пристрою, який визначається виробником.

Приклад MAC-адреси: 00:1A:2B:4C:12:E2, де 00:1A:2B – це OUI.

2. Реєстрація:

– керується міжнародною організацією IEEE (Institute of Electrical and Electronics Engineers);

– кожне OUI унікальне для кожної компанії та зареєстроване у публічній базі даних.

3. Використання:

– застосовується для ідентифікації виробників у мережах Ethernet, Wi-Fi, Bluetooth, інших технологій;

– дозволяє відстежувати виробника пристрою та діагностувати мережеві проблеми.

4. Безпека: може використовуватися для фільтрації пристроїв виробника або блокування небажаних пристроїв.

Основні функції MAC-адреси

Ідентифікація пристроїв: MAC-адреса дозволяє унікально ідентифікувати кожен пристрій у мережі; зазвичай вона прошита у мережній карті (NIC) виробником і є унікальною для кожного пристрою; може бути змінена програмно в деяких випадках (MAC spoofing).

Маршрутизація даних: використовується для доставки кадрів (frames) всередині однієї локальної мережі; на відміну від IP-адреси, яка працює на

мережному рівні (Layer 3), MAC-адреса не використовується для маршрутизації через інтернет.

Формування кадру: кожен Ethernet-кадр містить MAC-адресу відправника (source MAC) та одержувача (destination MAC); ці адреси необхідні для передачі даних від одного пристрою до іншого.

Комутований Ethernet

У комутованих локальних мережах проблема забезпечення їх надійності пов'язані з базовим алгоритмом прозорого мосту, коректність роботи якого можлива лише у мережі з деревоподібної топологією, тобто такої мережі, між будь-якими двома вузлами якої існує єдиний маршрут.

Прозорий міст, також відомий як мережевий міст, є апаратним або програмним компонентом, що забезпечує стійке з'єднання між двома або більше сегментами мережі. Цей міст працює на канальному рівні моделі OSI та сприяє фільтрації та пересиланню мережевого трафіку на основі MAC-адрес. Аналізуючи MAC-адресу призначення Ethernet-кадра, прозорий міст визначає, чи слід передати дані до іншого сегмента чи залишити їх у тому самому сегменті.

Прозорий міст відіграє ключову роль у забезпеченні зв'язку між пристроями, підключеними до різних сегментів мережі. Коли пристрій в одному сегменті має намір зв'язатися з пристроєм в іншому сегменті, прозорий міст перевіряє MAC-адресу призначення в Ethernet-кадрі. Якщо MAC-адреса призначення належить пристрою в тому ж сегменті, що й відправник, міст не пересилає трафік за межі сегменту. Однак, якщо MAC-адреса призначення відповідає пристрою в іншому сегменті, міст передає дані у відповідний сегмент, забезпечуючи безшовний зв'язок.

Прозорі мости використовують у різних мережевих сценаріях:

– у великих офісних середовищах, із кількома сегментами мережі, прозорі мости з'єднують та інтегрують ці сегменти, забезпечуючи безшовний зв'язок між різними відділами чи поверхами;

– прозорі мости необхідні у віртуалізованих середовищах, де віртуальні машини (VM) знаходяться у різних сегментах мережі (поєднуючи ці сегменти, прозорі мости дозволяють віртуальним машинам спілкуватися одна з одною та з пристроями в інших сегментах мережі);

– прозорі мости об'єднують бездротові та дротові мережі, дозволяючи пристроям на цих різних типах мереж спілкуватися безшовно (це особливо корисно у офісних будівлях, освітніх закладах та громадських місцях);

– інтеграція застарілих мереж: у ситуаціях, коли організації мають застарілу мережну інфраструктуру, прозорі мости можуть бути розгорнуті для інтеграції нових мережевих сегментів без необхідності значних змін у існуючій мережі.

Незважаючи на значну роль прозорих мостів у мережному зв'язку, сучасні мережеві технології базуються на рішеннях у вигляді комутаторів та маршрутизаторів, які забезпечують оптимальні показники продуктивності, масштабованості та гнучкості у сегментації мережі та обробці трафіку.

Протокол *Spanning Tree* (STP) – це мережевий протокол, який використовується прозорими мостами та комутаторами для запобігання *петель* в мережах Ethernet.

Петля комутації (цикл) – це мережева проблема, яка виникає, коли два або більше комутатори з'єднані в кругову топологію (створюючи петлю), внаслідок чого пакети даних безперервно циркулюють мережею по колу, множачись кожне коло поки мережа не перевантажиться і не перестане пропускати трафік взагалі.

Програмно-визначена мережа (Software-defined Networking, SDN) – це сучасний підхід до архітектури мережі, який абстрагує керуючий рівень від

апаратного забезпечення, дозволяючи централізовано керувати та контролювати мережу (прозорі мости можуть бути частиною інфраструктури SDN, забезпечуючи динамічний та гнучкий мережевий зв'язок).

Прозорі мости та мережеві комутатори мають схожість, але вони виконують різні завдання. Першочергове призначення прозорих мостів з'єднання мережних сегментів, тоді як комутатори надають розширені функції, такі як підтримка VLAN та пріоритизація трафіку. Комутатори також працюють на канальному рівні, але пропонують більш детальний контроль та високу продуктивність для керування мережним трафіком.

Сучасні комутатори Ethernet є спадкоємцями мостів локальних мереж, що використовувалися в мережах, побудованих на технологіях з розподіленим середовищем. Базові алгоритми роботи комутатора та моста тотожні та визначаються одним стандартом IEEE 802.1D. Відмінність комутатора від мосту полягає у більшій кількості портів та більш високій продуктивності, яка обумовлена одночасною передачею кадрів між парами портів.

Сьогодні комутатори є основним типом комунікаційних пристроїв, які застосовуються при побудові локальних мереж. Розвиток і удосконалення цього обладнання суттєво впливає на еволюцію технології Ethernet. Починаючи з версії 10G Ethernet стандарт IEEE описує роботу вузлів мережі тільки в середовищі, що комутується.

Основні складові/функції роботи комутатора:

1. *Комутація кадрів* (Frame Switching). Коли комутатор отримує Ethernet-кадр, він виконує такі дії:

– перевіряє MAC-адресу отримувача кадру (аналіз заголовка кадру);

– використовує таблицю MAC-адрес (CAM, Content Addressable Memory) для визначення порту, до якого підключений пристрій з потрібною MAC-адресою;

– відправляє кадр тільки на відповідний порт, а не на всі порти, що знижує загальне навантаження мережі (переадресація).

2. *Таблиця MAC-адрес*. Комутатор постійно оновлює свою таблицю MAC-адрес, реєструючи джерело кожного кадру (динамічне навчання). Для оптимізації пам'яті та безпеки записи в таблиці можуть автоматично видалятися через певний час простою (видалення старих записів).

3. *Способи переадресації кадрів*:

– Store-and-Forward: зберігає весь кадр, перевіряє його на помилки (CRC) і потім передає (висока надійність, але більша затримка);

– Cut-Through: передає кадр, як тільки зчитана MAC-адреса отримувача (мінімальна затримка, але ризик помилок);

– Fragment-Free: поєднує підходи Store-and-Forward і Cut-Through, перевіряючи перші 64 байти кадру (мінімальна довжина Ethernet-кадру).

4. *Управління смугою пропускання*:

– Flow Control: використання механізмів, таких як PAUSE-кадри (802.3x) для уникнення перевантажень;

– QoS (Quality of Service): пріоритизація трафіку для забезпечення мінімальної затримки для критичних застосувань (наприклад, VoIP).

5. *Віртуальні локальні мережі* (VLAN). Результатом створення віртуальної мережі через налаштування комутатора (за допомогою консолі, веб-інтерфейсу або SSH) є:

– ізоляція трафіку: можливість розділяти мережевий трафік між різними групами пристроїв для покращення безпеки та продуктивності;

– транкінг: використання 802.1Q для передачі VLAN-тегованих кадрів між комутаторами.

SSH (Secure Shell, безпечна оболонка) – мережевий протокол прикладного рівня, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань.

Додатковими функціями комутаторів є:

– захист від петель у мережі (Spanning Tree Protocol, STP);

– об'єднання кількох фізичних каналів в один логічний для збільшення пропускної здатності (Link Aggregation, LACP);

– живлення пристроїв через кабель Ethernet – підтримка PoE (Power over Ethernet).

4.2 Швидкісні версії Ethernet

На початку 90-х років почала відчуватися недостатня пропускну здатність Ethernet, тому що швидкість обміну даними з мережею стала значно менше швидкості внутрішньої шини комп'ютера. Вирішення цього питання призвело до появи нових швидкісних стандартів Ethernet: Fast Ethernet зі швидкістю 100 Мбіт/с, Gigabit Ethernet зі швидкістю 1000Мбіт/с (1 Гбіт/с), 10 G Ethernet (10 Гбіт/с), 100 G Ethernet (100 Гбіт/с), 400 G Ethernet (4000 Гбіт/с). Ці розроблені швидкісні стандарти зберегли основні риси класичної технології Ethernet і насамперед простий спосіб обміну кадрами без додавання до технології складних перевірочних процедур.

Застосування комутаторів в локальних мережах призвело до відмови від середовища, що розділяється. Це зняло наявність проблем, які виникали через випадковий характер методу доступу. Починаючи з версії 10 G Ethernet розробники стандартів відмовилися від підтримки розподіленого середовища. Підвищення швидкості роботи Ethernet було досягнуто за рахунок кількох факторів:

– покращення якості застосовуваних у комп'ютерних мережах кабелів;

– вдосконалення методів кодування даних;

– використання паралельних потоків даних.

Всі відмінності швидкісних версій Ethernet від класичної 10M Ethernet проявлені на фізичному рівні (рис. 31). Рівні MAC і LLC у Fast Ethernet залишилися тими ж і описуються тими ж розділами стандартів IEEE 802.3 та 802.2.

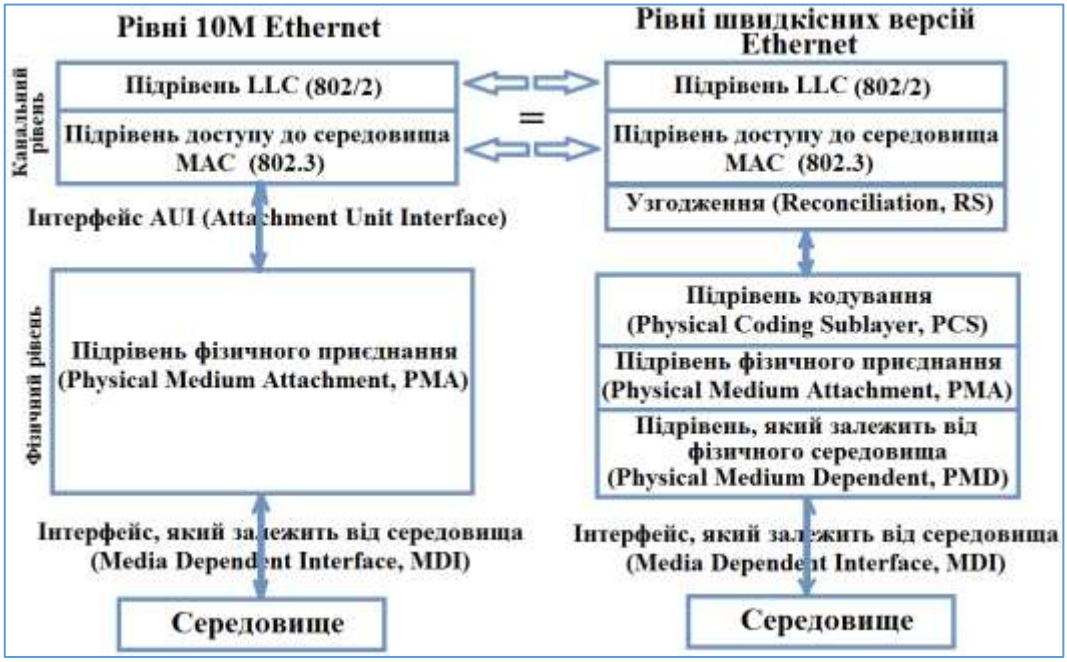


Рисунок 31 – Структура рівнів версії 10M Ethernet і швидкісних версій Ethernet

Організація фізичного рівня швидкісних версій Ethernet є модульною. Модульність забезпечує гнучкість фізичного рівня Ethernet, коли шляхом заміни певного модуля можна забезпечити підтримку різних методів кодування даних чи різних середовищ поширення сигналу.

Швидкісні версії Ethernet розвивалися для підтримки зростаючих вимог до пропускної здатності мереж. Основні поштовхи для розвитку технології Ethernet та її потенційні застосування спрямовані на задоволення зростаючих потреб у пропускній здатності для:

– забезпечення високошвидкісних з'єднань між серверами та сховищами даних дата-центрів гіперскейлу (такі хмарні провайдери, як AWS, Microsoft Azure, Google Cloud, постійно розширюють свої мережі);

– розвитку інфраструктур інтернету речей (IoT), штучного інтелекту (AI) та машинного навчання (ML), які потребують передачі великих обсягів даних для тренування моделей (моделі GPT потребують величезних обсягів даних і миттєвого обміну інформацією);

– розвитку високошвидкісних магістралей для обробки мобільного трафіку мобільного зв'язку 5G і в майбутньому 6G.

Fast Ethernet (100 Mbps)

Fast Ethernet було впроваджено у 1995 році як частина стандарту IEEE 802.3u. Специфікація Fast Ethernet була першою із серії специфікацій швидкісних версій Ethernet, тому і була названа «швидкою» (Fast). Розробники цієї технології забезпечили її наступність із класичною технологією Ethernet 10 Мбит/с. Збільшивши швидкість передачі даних до 100 Мбіт/с були збережені базові принципи Ethernet, такі як:

– метод доступу CSMA/CD;

– формат кадру Ethernet;

– структура адресації.

Основні характеристики технології Fast Ethernet:

– стандарт: 100BASE-TX (вита пара Cat 5), 100BASE-FX (оптоволокно, великі відстані); 100BASE-T4 (вита пара Cat 3; використовує 4 пари проводів); 100BASE-T2 (вита пара Cat 3, 4, 5; використовує 2 пари проводів);

– швидкість: 100 Мбіт/с;

– кабелі: Cat 5 (UTP/STP), оптичне волокно;

– дальність: до 100 м (мідь), до 2 км (оптика);

– використання: локальні мережі офісів, перехідний етап між 10BASE-T та Gigabit Ethernet.

Gigabit Ethernet (1 Gbps)

Gigabit Ethernet був впроваджений у 1998 році як частина стандарту IEEE 802.3z. У 1998 році відбулося прийняття стандарту 1000BASE-X (802.3z) для оптоволоконних і коротких мідних з'єднань (1000BASE-SX, 1000BASE-LX, 1000BASE-CX). 1999 рік став прийняттям стандарту 1000BASE-T (802.3ab) для витої пари категорії 5e і вище – є найбільш популярною версією Gigabit Ethernet.

Впровадження даної технології стало важливим етапом у розвитку мереж, дозволивши значно збільшити швидкість передачі даних у локальних мережах, що було критично для таких додатків, як потокове відео, хмарні сервіси та великі корпоративні мережі. Основні характеристики технології Gigabit Ethernet:

– стандарт: 1000BASE-T, 1000BASE-SX, 1000BASE-LX;

– швидкість: 1 Гбіт/с;

– кабелі: Cat 5e, Cat 6, оптичне волокно;

– дальність: до 100 м (мідь), до 10 км (оптика);

– використання**:** основні мережі підприємств, серверні комунікації, агрегація трафіку

10 Gigabit Ethernet (10 Gbps)

10 Gigabit Ethernet був впроваджений у 2002 році як частина стандарту IEEE 802.3ae, ставши важливим етапом у розвитку високошвидкісних мереж, дозволивши використовувати Ethernet у дата-центрах, хмарних обчисленнях та великих корпоративних мережах (Amazon Web Services, AWS використовує 10GbE і вище для підтримки масштабованих хмарних рішень; Microsoft Azure – створює високошвидкісні канали для гібридних хмарних сценаріїв; Netflix – застосовує швидке кешування контенту для глобальної аудиторії; Bloomberg,

Nasdaq – робота бірж, що використовують низьколатентні рішення для фінансових транзакцій. Основні характеристики технології:

– стандарт: 10GBASE-T, 10GBASE-SR, 10GBASE-LR, 10GBASE-ER;

– швидкість: 10 Гбіт/с;

– кабелі: Cat 6a, Cat 7, оптичне волокно;

– дальність: до 100 м (мідь), до 40 км (оптика);

– використання: центри обробки даних, високошвидкісні магістральні з'єднання.

25 Gigabit Ethernet (25 Gbps)

Початок розробки стандарту 25 Gigabit Ethernet (25GbE) для задоволення потреб дата-центрів з високою щільністю комутації почався у 2014 році, а впроваджений був у 2016 році як частина стандарту IEEE 802.3by. У 2018 році відбулося прийняття стандарту IEEE 802.3cc для довгих оптичних з'єднань. Практичні приклади впровадження технології: AWS – використовує 25GbE для внутрішніх комунікацій між серверами і зберіганням даних; Microsoft Azure – для високопродуктивних обчислень і аналізу великих обсягів даних; Google Cloud Platform (GCP) – для мінімізації затримок і прискорення хмарних сервісів; Netflix, YouTube – для швидкої доставки відеоконтенту з мінімальними затримками; HFT (High-Frequency Trading) – фінансові компанії використовують 25GbE для надшвидких транзакцій; IBM Watson – швидка обробка медичних та фінансових даних.

25GbE підтримує:

– протоколи RDMA (Remote Direct Memory Access), NVMe-oF (Non-Volatile Memory Express over Fabrics) та RoCE (RDMA over Converged Ethernet) для надшвидкісного доступу до даних;

– сучасні серверні архітектури, такі як GPU-обчислення, машинне навчання, обробка великих даних;

– сумісність з Docker, Kubernetes та іншими контейнерними платформами.

Контейнеризація – це об'єднання програми з усіма її необхідними бібліотеками, залежностями та файлами конфігурації в єдину сутність, звану контейнером. Контейнер створюється для роботи в будь-якому середовищі (ноутбук розробника, хмарний сервер), щоб мінімізувати проблеми сумісності. Контейнеризація пов'язана з практиками, що стосуються розробки та розгортання додатків.

GPU-обчислення (Graphics Processing Units) – це використання графічних процесорів (GPU) для виконання загальних (не графічних) обчислень, які раніше виконувалися лише на центральних процесорах (CPU).

25 Gigabit Ethernet (25GbE) суттєво вплинув на розвиток таких технологій, як Інтернет речей (IoT) і штучний інтелект (AI). Ці технології вимагають не лише високих швидкостей передачі даних, але й мінімальних затримок для роботи в реальному часі.

Зв'язок і вплив 25GbE на Інтернет речей (IoT)

Швидка обробка великих обсягів даних. IoT-пристрої генерують великі обсяги даних, які потрібно швидко обробляти. 25GbE забезпечує високу пропускну здатність для транспортування цих даних у дата-центри і хмарні сховища (як приклад, інтелектуальні камери безпеки, що передають HD-відео в реальному часі.

Низькі затримки для критичних додатків – промислові IoT-системи іноді вимагають майже миттєвої передачі команд для точного контролю виробничих процесів; Smart Grid (інтелектуальні енергосистеми) потребують швидкої обробки даних для балансування навантаження.

Підтримка автономних систем – автономні транспортні засоби, дрони, ро́боти покладаються на швидку передачу великих масивів сенсорних даних, що є критично важливим для уникнення аварій і точного маневрування.

Зв'язок і вплив 25GbE на штучний інтелект (AI) та машинне навчання (ML)

Потужна інфраструктура для тренування моделей. Тренування AI-моделей вимагає обробки великих наборів даних, часто паралельно на багатьох графічних процесорах (GPU). 25GbE дозволяє значно швидше передавати дані між серверами та GPU, що скорочує час тренування моделей. Використовується в компаніях OpenAI, NVIDIA і Tesla.

Швидка інференція (Inference). У додатках реального часу (розпізнавання голосу, комп'ютерний зір) критичне значення мають мінімальні затримки. Наприклад, системи розпізнавання обличчя або автономні роботи, що швидко реагують на зміну середовища.

Розподілені нейронні мережі. Багато сучасних AI-моделей (наприклад, ChatGPT) працюють на розподілених системах, що вимагає високошвидкісної передачі даних між вузлами. 25GbE мінімізує затримки при розподілених обчисленнях, роблячи модель більш продуктивною.

Технології, що підтримують AI та IoT на основі 25GbE:

– RDMA (Remote Direct Memory Access): прискорює обмін даними між серверами, мінімізуючи затримки;

– NVMe-oF (Non-Volatile Memory Express over Fabrics): дозволяє блискавичний доступ до флеш-пам'яті з мінімальними затримками;

– RoCE (RDMA over Converged Ethernet): дозволяє працювати з великими обсягами даних без значних затримок;

– PCIe Gen4 і Gen5: підтримка високошвидкісних мережевих карт для AI-серверів;

– DPDK (Data Plane Development Kit): прискорює роботу мережевих функцій для низьких затримок.

40 Gigabit Ethernet (40GbE)

40 Gigabit Ethernet було вперше стандартизовано в 2010 році як частину стандарту IEEE 802.3ba. Технологія призначена для надшвидкої передачі даних у високошвидкісних мережах, таких як великі дата-центри, суперкомп'ютерні кластери, високопродуктивні обчислювальні системи (High-Performance Computing, HPC). Часто використовується в агрегаційних лінках, магістральних з'єднаннях та з'єднаннях між комутаторами, підтримує агрегацію кількох 10GbE каналів. Висока пропускна здатність, яку забезпечує 40GbE, підходить для завантажених мереж з великим трафіком, зменшення затримок важливо для фінансових бірж, наукових розрахунків та обчислювальних центрів. Основні характеристики:

– стандарт: 40GBASE-SR4, 40GBASE-LR4;

– швидкість: 40 Гбіт/с;

– кабелі: мультиволоконні кабелі (OM3/OM4);

– дальність: до 7 м (мідний кабель), до 150 м (оптика MM), до 10 км (оптика SM).

100 Gigabit Ethernet (100 Gbps)

100 Gigabit Ethernet було стандартизовано в 2010 році як частина стандарту IEEE 802.3ba, разом із 40GbE. Цей стандарт забезпечує швидкість передачі даних 100 Гбіт/с і призначений для високошвидкісних магістральних мереж, дата-центрів (підключення між дата-центрами) та провайдерів інтернет-послуг. Основні характеристики:

– стандарт: 100GBASE-SR4, 100GBASE-LR4;

– швидкість: 100 Гбіт/с;

– кабелі: мульти- і одномодове оптоволокно;

– дальність: до 10 км, до 40 км з розширеними технологіями.

200/400 Gigabit Ethernet (200/400 Gbps)

200 Gigabit Ethernet (200GbE) і 400 Gigabit Ethernet (400GbE) були стандартизовані в 2017 році як частина стандарту IEEE 802.3bs. Ці технології були розроблені для задоволення зростаючих потреб дата-центрів, провайдерів хмарних сервісів і високопродуктивних обчислювальних центрів (HPC) у надвисокій пропускній здатності. Вони забезпечують значно вищу щільність передачі даних та енергоефективність порівняно з попередніми поколіннями Ethernet. Основні характеристики:

– стандарт: 200GBASE-SR4, 400GBASE-LR8;

– швидкість: 200/400 Гбіт/с;

– кабелі: високошвидкісні волокна з багатоканальною передачею;

– дальність: до 10 км (оптика).

Сучасні тенденції в розвитку Ethernet включають надшвидкісні технології, такі як 800G та навіть 1.6Tbps Ethernet, які стають критичними для великих дата-центрів, провайдерів хмарних сервісів та телекомунікаційних магістралей.

Terabit Ethernet (800 Gbps)

Стандарт 800 Gigabit Ethernet (800GbE) був офіційно затверджений у 2024 році як частина специфікації IEEE 802.3df-2024 [8]. Цей стандарт визначає параметри MAC, фізичні рівні та керування для передачі кадрів Ethernet зі швидкістю 800 Гбіт/с. Основні характеристики 800GbE [8]:

– структура передачі: використовує 8 паралельних каналів по 100 Гбіт/с кожен (8×100G), що забезпечує загальну пропускну здатність 800 Гбіт/с;

– типи середовища: підтримує передачу даних через різні типи кабелів, включаючи мідні кабелі, багатомодові (MMF) та одномодові (SMF) оптичні волокна, з досяжністю до 2 км.

– застосування: призначений для високошвидкісних магістральних з'єднань у дата-центрах, хмарних сервісах та мережах провайдерів, де потрібна надвисока пропускна здатність;

– інтерфейси: 8×100G (PAM4), 4×200G (PAM4) або 2×400G (PAM4);

– формати модулів: QSFP-DD800, OSFP, COBO;

– дальність: до 10 км (SMF), до 100 м (MMF), через мідний кабель (800GBASE-CR8, twinax) до 2 метрів.

Ключові технології стандарту 800GbE:

– PAM4 (Pulse Amplitude Modulation, 4-level): використовує 4 рівні сигналів для передачі більшої кількості даних на одному каналі;

– DSP (Digital Signal Processing): забезпечує корекцію помилок та покращену передачу сигналу;

– FEC (Forward Error Correction): знижує ймовірність втрат пакетів при високих швидкостях;

– Co-Packaged Optics: інтеграція оптики безпосередньо в мережеві ASIC для зменшення затримок і втрат.

Мережеві ASIC (Application-Specific Integrated Circuit) – це спеціалізовані інтегральні схеми, розроблені для високошвидкісної обробки мережевого трафіку і використовуються в комутаторах, маршрутизаторах, мережевих процесорах та інших пристроях.

Реалізації та впровадження технології 800GbE:

– китайський виробник *H3C* (комутатор *S9827* з 64 портами 800G, забезпечуючи загальну пропускну здатність 51,2 Тбіт/с) [9];

– *T-Mobile Polska* впровадила технологію Ciena WL5e для надання послуг 400G Ethernet з використанням 800G хвиль [10];

– *Omantel* використовує технологію *Ciena WL5e* для з'єднання дата-центрів, підводних кабельних станцій та телекомунікаційних вузлів, забезпечуючи передачу даних зі швидкістю до 800 Гбіт/с [10];

– *Spirent* провела перше велике тестування 800G Ethernet з *H3C*, використовуючи платформу *B2 800G* для перевірки продуктивності та сумісності нових комутаторів [11];

– *Keysight Technologies* на виставці OFC 2024 Keysight продемонструвала інтероперабельність 800G ZR модулів, включаючи тести з Luxshare, Cisco та Celestica, що підтверджує готовність технології до широкого впровадження [9];

– *Siemon* представила високощільні кабельні збірки DAC та AEC для 800G мереж, що оптимізують продуктивність та спрощують управління кабелями в сучасних дата-центрах [11].

1.6 Tbps Ethernet (1.6T Ethernet)

1.6 Tbps Ethernet наразі перебуває на стадії розробки в рамках проєкту IEEE 802.3dj, який фокусується на стандартизації фізичних рівнів (PHY) для швидкостей 800 Гбіт/с та 1.6 Тбіт/с, зокрема з використанням ліній передачі зі швидкістю 200 Гбіт/с. Технологія дозволяє передавати приблизно 200 гігабайт даних за секунду при пропускній здатності 1600 Гбіт/с (1.6 Tbps). Особливості даної технології: високі швидкості, які створюють проблеми з охолодженням; складність маршрутизації у вигляді необхідності оптимізації затримок і пропускної здатності; питання інтероперабельності – забезпечення сумісності між різними поколіннями обладнання; потреба у вдосконалених волокнах для мінімізації втрат сигналу; вимога кращих матеріалів і дизайну інтерфейсів для забезпечення високої частоти.

Дослідження та експериментальні реалізації вказують на наступні потенційні відстані передачі для 1.6T Ethernet [12]:

– мідні кабелі (twinax): передача на короткі відстані до 1 метра;

– мультимодові оптичні волокна (OM5): до 100 метрів;

– одномодові оптичні волокна (SMF): до 2 кілометрів;

– розширені відстані: дослідження компанії NTT демонструють можливість передачі сигналів 1.6 Тбіт/с на відстань до 10 кілометрів з використанням багатоядерних волокон (multi-core fiber) та вдосконалених методів модуляції, таких як *PAM-8.*

Реалізації та впровадження технології 1.6T Ethernet наступні:

– компанія *CoMira Solutions* розробила спеціалізований апаратний компонент (IP-блок) 1.6T Ethernet UMAC IP, який забезпечує пропускну здатність 1.6 Тбіт/с з низькою затримкою та мінімізованим розміром логіки [13];

– провідні компанії у світі електронних вимірювань *Keysight Technologies* та *Credo Semiconductor* розробили першу в галузі тестову платформу, яка відповідає проєкту стандарту IEEE P802.3dj та здатна генерувати, приймати та вимірювати трафік Ethernet на швидкості 1.6 Тбіт/с (що демонструє можливість реального впровадження 1.6T Ethernet у мережевих пристроях) [14];

– американський постачальник телекомунікаційного мережевого обладнання та програмного забезпечення Ciena Corporation розробляє рішення WaveLogic 6 Extreme, для забезпечення передачи даних на швидкості до 1.6 Тбіт/с [10];

– китайська компанія Eoptolink розвиває оптичні трансивери, здатні передавати дані на швидкості 1.6 Тбіт/с.

Основними виробниками обладнання з підтримкою 800G / 1.6T Ethernet є:

– тайванська компанія *Accton Technology* (Edgecore Networks) виробляє високопродуктивні комутатори 800G, орієнтовані на сучасні центри обробки даних та робочі навантаження штучного інтелекту/машинного навчання;

– американська компанія, виробник телекомунікаційного обладнання *Juniper Networks* (комутатори для AI-центричних мереж);

– американська компанія *Microchip Technology* розробляє апаратні компоненти для роутерів, комутаторів, лінійних карт для дата-центрів, 5G та AI/ML інфраструктур);

– *Synopsys Inc,* американський виробник програмного забезпечення для проектування мікросхем, компанія, що працює в галузі САПР для проектування електроніки;

– *Marvell Technology*, американська компанія розробник напівпровідникової продукції: процесорів, мікроконтролерів, телекомунікаційного обладнання та споживчих напівпровідникових приладів.

4.3 Відмовостійкі мережі. Алгоритм покриваючого дерева.

У наш час топологія ієрархічна зірка (розширена зірка або дерево) – найпоширеніше рішення для створення локальних і глобальних комп'ютерних мереж. Топологія утворюється з неповнозв'язної мережі типу зірка, шляхом підключення нових вузлів, які не мають безпосереднього контакту з центральним елементом. У таких мережах, зазвичай, безпосередню взаємодію з центральним елементом мають лише мережні пристрої, до яких підключаються кінцеві користувачі. Ієрархічна зірка використовується в офісах, на малих, великих і дуже великих підприємствах.

У мережах Ethernet, що побудовані на основі комутаторів, легко утворити *цикли* (петлі). Уникнення мережевих циклів є критично важливим питанням в управлінні комутованими мережами. Зазвичай це рішення реалізоване через

протокол STP або його варіанти, які забезпечують надійну та безпечну мережеву інфраструктуру [1].

Алгоритм покриваючого дерева (spanning tree algorithm) – це алгоритм, який будує дерево без циклів, що з’єднує всі вузли мережі, використовуючи мінімальну кількість зв’язків і уникаючи формування петель. Основна мета застосування алгоритму у локальних мережах – це створення найефективнішої структури з'єднань між комутаторами та іншими мережевими пристроями, уникнення мережевих циклів, які можуть викликати широкомовні шторми (broadcast storms) і суттєво сповільнити роботу мережі.

STP (Spanning Tree Protocol), *RSTP* (Rapid Spanning Tree Protocol) та *MSTP* (Multiple Spanning Tree Protocol) є ключовими технологіями для забезпечення стабільності Ethernet-мереж.

Для надійної роботи мережі, крім основного маршруту між її вузлами, необхідна наявність альтернативних маршрутів між вузлами, які можна використовувати при відмові основного маршруту. Автоматична побудова мережі з альтернативними маршрутами та пошук зв'язної деревоподібної топології, блокування всіх портів, які не входять у винайдену топологію, конфігурування активної деревоподібної топології, моніторинг стану її зв'язків і перехід до нової деревоподібної топології при виявленні відмови зв'язку в комутованих локальних мережах виконується на підставі алгоритму покриваючого дерева (STA) і протоколу покриваючого дерева (STP), що реалізує цей алгоритм.

Протокол STP

STP (Spanning Tree Protocol) – мережевий протокол, розроблений для запобігання/усунення петель у мережах Ethernet, які можуть виникати через надмірні з'єднання (шляхи) між комутаторами. Петля – це будь-яке з'єднання між

декількома комутаторами, яке призводить до кільцевої передачі трафіку в мережі. STP визначений стандартом IEEE 802.1D, був розроблений у 1985 році інженером IBM Ромпертом Брасом і використовується для створення єдиного активного шляху між усіма парами вузлів у мережі, блокуючи надлишкові шляхи. STP використовує алгоритм Берлекампа, який забезпечує правильну роботу у великих та складних мережах.

Основні позиції STP:

– *кореневий комутатор*: STP вибирає один комутатор як кореневий, з якого будується логічна топологія мережі;

– *вибір кореневого порту*: для кожного комутатора визначається кореневий порт, який є портом з найменшою «вартістю» шляху до кореневого комутатора;

– *вибір призначеного порту*: на кожному сегменті мережі вибирається один призначений порт, який передаватиме трафік на цьому сегменті;

– *блокування порту*: порти, які не є кореневими або призначеними, блокуються, щоб запобігти петлям.

Складнощі STP: хоча STP ефективно запобігає петлям, його основні недоліки пов'язані з часом, необхідним для змін у топології мережі. У разі збою одного з активних шляхів, STP вимагає часу для повторного розрахунку топології та переходу до резервних шляхів, що може призвести до значних затримок. STP підходить для невеликих мереж з низьким рівнем надмірності, де простота налаштування та надійність важливіша за швидкодію.

Протокол RSTP

RSTP (Rapid Spanning Tree Protocol) був стандартизований в 2001 році як IEEE 802.1w і є покращеною версією STP, що значно *зменшує час*, необхідний для *реакції* на зміни в топології мережі.

Основні позиції RSTP:

– *швидке відновлення*: RSTP використовує новий механізм швидкого переходу в робочий стан при зміні топології, що дозволяє скоротити час простою мережі;

– *перехідні стани*: RSTP використовує лише три стани порту (Forwarding, Learning, Discarding) замість п'яти у STP, що спрощує та прискорює процес. RSTP підтримує сумісність із STP, що дозволяє впроваджувати його в існуючі мережі, де використовуються старі версії STP.

RSTP значно швидше реагує на зміни топології, рекомендується для середніх та великих мереж, де потрібне швидке відновлення після збоїв та мінімальні затримки.

Протокол MSTP

MSTP (Multiple Spanning Tree Protocol) був розроблений для вирішення проблеми масштабованості у мережах, що використовують RSTP. MSTP дозволяє створювати кілька екземплярів (інстанцій) STP, що забезпечує кращу підтримку VLAN та розподіл навантаження по мережі. MST протокол входить до сімейства протоколів STP, створених для запобігання петлям у комутованих мережах Ethernet. MST є частиною стандарту IEEE 802.1s і розширює можливості базового STP та RSTP.

Протоколи типу MST обирають кореневий комутатор (Root Bridge) та створюють дерево шляхів від цього кореня до всіх інших комутаторів. Це мінімізує затримки і забезпечує ефективне використання смуги пропускання. MSTP є найбільш використовуваним для складних та масштабованих мереж з безліччю VLAN, де необхідно підтримувати кілька політик маршрутизації та оптимізувати розподіл навантаження.

Основні характеристики технології MST у локальних мережах:

– *запобігання циклам* (у мережах Ethernet навіть один цикл може викликати нескінченне дублювання кадрів; протоколи MST гарантують, що кадри досягають пункту призначення лише одним шляхом);

– *максимальна продуктивність* (мінімізує затримки, використовуючи найкоротші можливі шляхи; зменшує загальне навантаження на мережеве обладнання);

– *надійність та відмовостійкість* (автоматично перебудовує топологію у разі відмови зв'язку, забезпечуючи безперервність мережевих послуг).

До основних особливостей протоколу MST відносять:

– *підтримку множинних дерев* (множинні інстанції), що дозволяє створювати кілька незалежних spanning trees всередині однієї мережі значно покращуючи балансування навантаження порівняно з традиційним STP;

– *покращене використання пропускної здатності*: кожне spanning tree може використовувати різні фізичні шляхи, що зменшує перевантаження каналів зв'язку;

– *сумісність*: MST сумісний з класичними STP та RSTP, що дозволяє легко інтегрувати його в існуючу мережеву інфраструктуру;

– *зони MST* (MST Regions): мережа ділиться на зони, кожна з яких має свій набір spanning trees, що дозволяє більш ефективно керувати великими мережами;

– *швидку конвергенцію*: завдяки використанню швидших механізмів для виявлення змін у топології мережі, MST забезпечує швидшу конвергенцію порівняно з класичним STP, надає гнучкість та масштабованість для великих мереж, де різні VLAN вимагають різних політик маршрутизації.

Конвергенція в контексті комп'ютерних мереж – це процес узгодження стану всієї мережі після будь-яких змін у топології, це час, який потрібен маршрутизаторам або комутаторам для відновлення стабільного стану

маршрутизації після зміни в мережевій інфраструктурі, наприклад, після відключення лінії зв'язку або додавання нового маршрутизатора.

Фактори, що впливають на конвергенцію: топологія мережі; швидкість обміну інформацією між пристроями; тип маршрутизуючого протоколу; налаштування таймерів і розмір таблиць маршрутизації.

Швидкість конвергенції – показник, що визначає, як швидко мережа може відновити нормальну роботу після збою (швидка конвергенція зменшує час простою та втрату даних).

Маршрутизуючі протоколи (різні протоколи мають різну швидкість конвергенції):

– *RIP* (Routing Information Protocol): повільна конвергенція (до 180 секунд);

– *OSPF* (Open Shortest Path First): швидка конвергенція (кілька секунд);

– *EIGRP* (Enhanced Interior Gateway Routing Protocol): дуже швидка конвергенція (залежить від налаштувань).

4.4 Віртуальні локальні мережі

Віртуальною локальною мережею (VLAN) називається група вузлів мережі, трафік якої, зокрема широкомовний, на канальному рівні повністю ізольований від трафіку інших вузлів мережі. Це означає, що передача кадрів між різними віртуальними мережами на підставі адреси канального рівня неможлива незалежно від типу адреси (унікальної, групової або широкомовної). У той самий час усередині локальної мережі кадри передаються за технологією комутації, тобто тільки на той порт, який пов'язаний з адресом призначення кадру [2].

Побудова віртуальної локальної мережі базується на концепції логічного розділення фізичної мережі для підвищення її ефективності, безпеки та керованості.

Основні принципи створення VLAN

Логічне сегментування мережі VLAN: дозволяє об'єднувати пристрої в логічні групи незалежно від їх фізичного розташування (це допомагає зменшити широкомовні домени і трафік у мережі).

Ізоляція трафіку: дані, які передаються в одній VLAN, ізольовані від інших VLAN, що підвищує безпеку і знижує ризик несанкціонованого доступу.

Підвищення продуктивності VLAN зменшує кількість широкомовних пакетів, що покращує ефективність використання мережевих ресурсів.

Спрощене управління: легше керувати групами користувачів або пристроїв, об'єднаних за функціональними чи організаційними ознаками.

Гнучкість і масштабованість: додавання нових пристрої до VLAN не потребує фізичної зміни підключення – достатньо налаштувати їх на комутаторі.

Тегування VLAN: використання тегів для позначення VLAN у кадрах Ethernet, що дозволяє передавати дані різних VLAN через один фізичний канал (транк).

Безпека VLAN: захист від між-VLAN атак, таких як VLAN hopping, Double Tagging, використання Access Control Lists (ACLs) і Private VLANs (PVLANs).

Технології VLAN:

– статичні VLAN (портові VLAN): пристрої прив'язуються до VLAN через фізичний порт комутатора;
– динамічні VLAN: пристрої прив'язуються на основі їх MAC-адрес, ідентифікаторів або інших параметрів;
– Voice VLAN: використовується для сегментації голосових даних.

Віртуальні локальні мережі можуть перекриватися, якщо один або кілька комп'ютерів входять до складу більш ніж однієї віртуальної мережі. На рисунку 32 сервер електронної пошти входить до складу віртуальних мереж

VLAN_3 та VLAN_4. Це означає, що його кадри передаються комутаторами всім комп'ютерам, які входять до цих двох мереж. Якщо ж якийсь комп'ютер входить до складу тільки VLAN_3 (у нашому випадку це комп'ютери 9 і 10), то його кадри до мережі VLAN_4 доходити не будуть, але він зможе взаємодіяти з комп'ютерами мережі VLAN_4 через загальний поштовий сервер 3. Така схема захищає віртуальні мережі один від одного не повністю, широкомовний шторм, що виникне на сервері 3 поглине і VLAN_3, і VLAN_4.

Рисунок 32 – Схема віртуальних локальних мереж

Важливою властивістю комутаторів локальної мережі є можливість контролювати передачу кадрів між сегментами мережі. Обмеження такого типу можна реалізувати за допомогою фільтрів користувача – набором умов, що задаються комутатору адміністратором для обмеження звичайної логіки передачі кадрів. Однак, фільтр користувача може заборонити комутатору передачу кадрів тільки за конкретними адресами, а широкомовний трафік він, відповідно до алгоритму роботи, зобов'язаний передати всім сегментам мережі. Тож, у мережах, створених з урахуванням комутаторів, відсутні бар'єри на шляху широкомовного трафіку. Технології віртуальних мереж дають змогу це подолати.

Техніка віртуальних мереж вирішує завдання обмеження взаємодії вузлів мережі, використовуючи інший механізм.

Технологія VLAN дозволяє створювати повністю ізольовані сегменти мережі шляхом логічного конфігурування комутаторів, не вдаючись до зміни фізичної структури. Для зв'язування віртуальних мереж у загальну мережу необхідні засоби мережного рівня, що може бути реалізовано через маршрутизатор, або в програмному забезпеченні комутатора, який є комбінованим пристроєм, що називається комутатором 3-го рівня.

Створення віртуальних мереж на базі одного комутатора

При створенні віртуальних мереж на базі одного комутатора зазвичай використовують механізм групування портів комутатора (рис. 33). Це дозволяє розділити фізичну мережу на кілька логічно ізольованих підмереж, що підвищує безпеку, керованість і ефективність мережевих ресурсів. При цьому кожен порт приписується певній віртуальній мережі. Кадр, що надходить від порту VLAN_1, ніколи не буде переданий порту іншої віртуальної мережі. Один порт можна прописати кільком віртуальним мережам, але тоді зникає ефект повної ізоляції. Створення віртуальних мереж шляхом групування портів не вимагає від адміністратора мережі великого обсягу ручної роботи.

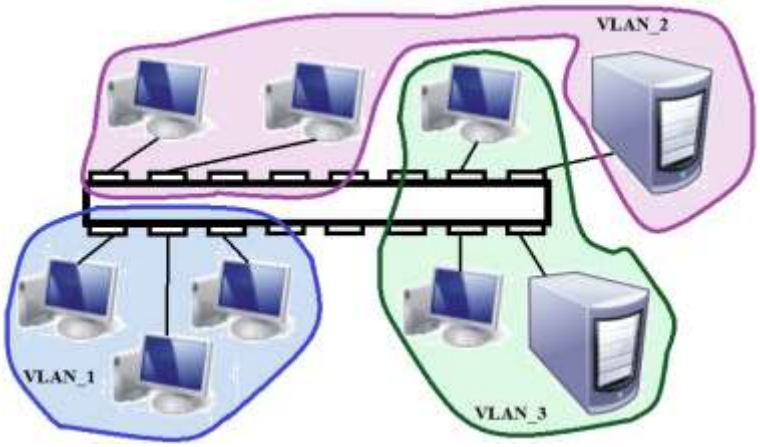


Рисунок 33 – Віртуальні мережі, побудовані на одному комутаторі

Ще один спосіб утворення віртуальних мереж заснований на групуванні MAC-адрес, кожна з яких (якщо вона вивчена комутатором) приписується тій чи іншій віртуальній мережі. Якщо у мережі є безліч вузлів, такий спосіб вимагає великого обсягу ручної роботи від адміністратора мережі.

Основні етапи створення VLAN на одному комутаторі:

1. *Ізоляція трафіку*: пристрої в різних VLAN не можуть спілкуватися без маршрутизації, навіть якщо фізично підключені до одного комутатора.
2. *Оптимізація трафіку*: зменшується кількість широкомовного трафіку (broadcast).
3. *Підвищення безпеки*: доступ між VLAN можна суворо контролювати.
4. *Гнучке управління*: легко переносити пристрої між VLAN без фізичних змін у підключенні.

Створення віртуальних мереж на базі кількох комутаторів

У випадку, коли вузли віртуальної мережі підключені до різних комутаторів, для підключення кожної такої підмережі на комутаторах повинна бути виділена спеціальна пара портів. Інакше, якщо комутатори будуть пов'язані лише однією парою портів, інформацію про належність кадру тій чи іншій віртуальної мережі під час передачі кадру з комутатора до комутатора буде втрачено.

Групування MAC-адрес у віртуальну мережу на кожному комутаторі позбавляє необхідності зв'язувати їх по кількох портах, оскільки в цьому випадку MAC-адреса стає *міткою* віртуальної мережі. Такий підхід у віртуальних мережах з великою кількістю вузлів є неприйнятним з причини великої кількості ручних операцій з маркування MAC-адрес на кожному комутаторі мережі. Крім того, такий спосіб передбачає тільки додавання додаткової інформації до адресних таблиць комутаторів і не забезпечує можливості вбудовування в

переданий кадр інформації про належність кадру віртуальній мережі. Тому широко використовується спосіб, заснований на введенні в кадр *додаткового поля*, яке зберігає інформацію про належність кадру до тієї чи іншої віртуальної мережі. При цьому немає необхідності запам'ятовування у кожному комутаторі належності всіх MAC-адрес *складової мережі* віртуальним мережам. Додаткове поле з позначкою про номер віртуальної мережі використовується тільки тоді, коли кадр передається від комутатора до комутатора, а при передачі кадру кінцевому вузлу воно зазвичай видаляється.

Сегментація за міткою VLAN з ідентифікатором VLAN

Віртуальні локальні мережі реалізовані з маркерами/тегами Ethernet кадрів. Теги є орієнтиром для комутаторів мережі. Стандарт IEEE 802.1Q вводить у кадрі Ethernet додатковий заголовок – тег віртуальної локальної мережі.

Тег VLAN – це ідентифікатор, який використовується для розділення мережевого трафіку в межах однієї фізичної мережі. Він дозволяє створювати логічно ізольовані підмережі, навіть якщо вони використовують однакове фізичне обладнання, таке як комутатори та маршрутизатори. Основні характеристики VLAN тегу:

1. Ідентифікація VLAN:
   – кожна VLAN має унікальний ідентифікатор (номер), зазвичай в діапазоні від *1* до *4094* (у стандарті IEEE 802.1Q);
   – VLAN ID *1* зазвичай зарезервований як нативний (властивий для певного середовища) VLAN;
   – деякі номери VLAN зарезервовані для спеціальних цілей, наприклад, VLAN *0* для пріоритизації трафіку.
2. Тегування кадрів:
   – тег VLAN додається до заголовка Ethernet кадру;

– використовується теговий протокол IEEE 802.1Q, який додає 4 байти до Ethernet кадру;

– поле тегу включає VLAN ID та поле пріоритету (Priority Code Point, PCP).

3. Тегова структура: після тегування кадр має структуру, яку показано на рисунку 34.

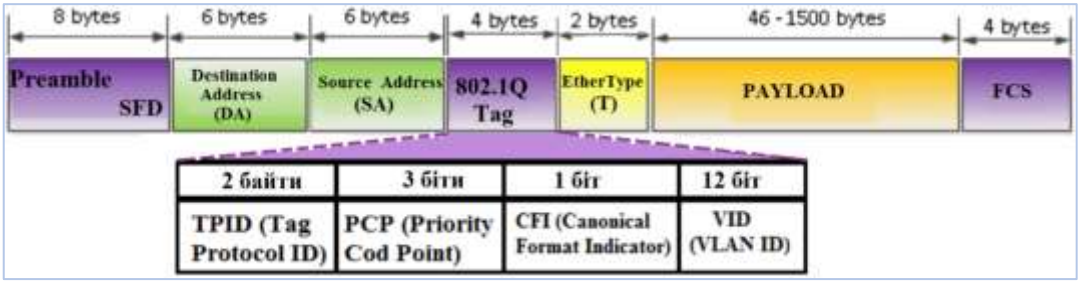


Рисунок 34 – Тегований ethernet-кадр

Тег віртуальної локальної мережі складається із 4-х частин:

– TPID (Tag Protocol ID) або *ідентифікатор* тегованого протоколу: складається з 2-х байт і для VLAN завжди дорівнює 0x8100.

– PCP (Priority Code Point) або *значення пріоритету*: складається з 3-х біт. Використовується для пріоритезування трафіку.

– CFI (Canonical Format Indicator) або індикатор канонічного формату: поле, що складається з одного біта (якщо має значення 0 – є стандартним форматом MAC-адреси).

– VID (VLAN ID) або *ідентифікатор VLAN*: складається з 12 біт і показує, до якої VLAN належить кадр.

Тегування кадрів здійснюється між мережевими пристроями (комутатори, маршрутизатори), а між кінцевим вузлом (комп'ютер, ноутбук) і мережевим пристроєм кадри не тегуються. Тому порт мережного пристрою може бути у 2-х станах: access або trunk.

Access port (порт доступу) – порт, який знаходиться у певній VLAN і передає не теговані кадри. Як правило, це порт, що налаштований на пристрій користувача.

Trunk port або магістральний порт – це порт, що передає тегований трафік. Як правило, цей порт налаштовується між мережевими пристроями.

Є два способи позначити пакети тегами VLAN:

– *перший*: комутатор призначає тег кожному вхідному кадру Ethernet із залежністю MAC-адреси або без неї, який має бути налаштований на стороні комутатора;

– *другий*: окремі хости надають вихідні пакети даних із тегами.

При другому способі конфігурація локальної мережі кожного пристрою повинна бути відрегульована таким чином, щоб правильний ідентифікатор записувався в заголовок кадру. Перевага: комутатор може обробляти пакети з різних VLAN через один і той самий порт.

Можливо 4096 (2^{12} біт) віртуальних локальних мереж (від 0 до 4095). Однак ідентифікатори *0* та *4095* зарезервовані. ID *1* зазвичай використовується як VLAN адміністратора, так що всіма мережевими компонентами можна керувати централізовано. На практиці кількість VLAN, що настроюються, часто обмежена – типова кількість 24 або 256.

VLAN реалізуються за допомогою комутаторів, які певним чином поєднують у собі переваги комутації та маршрутизації. Для налаштування обміну даними між VLAN (маршрутизації**,** Inter-VLAN Routing) потрібен маршрутизатор або комутатор 3-го рівня: використовуються *Router-on-a-Stick, SVI* **(**Switched Virtual Interface) або *Layer 3 Switches*.

Основні протоколи та стандарти для VLAN: IEEE 802.1Q – найпопулярніший стандарт тегування; *VTP* (VLAN Trunking Protocol) – спрощує

управління VLAN між комутаторами (переважно на пристроях Cisco); *GVRP* (GARP VLAN Registration Protocol) – більш стандартизований аналог *VTP*.

При створенні VLAN на комутаторах існує ряд технічних та апаратних обмежень: кількість VLAN, транкові обмеження, таблиці CAM і TCAM, широкомовні домени, пропускна здатність і затримка, сумісність обладнання, безпека [2].

Кількість VLAN. Комутатори рівня 2 (L2) зазвичай підтримують до 4094 VLAN (від 1 до 4094) відповідно до стандарту IEEE 802.1Q, оскільки поле VLAN ID має 12 біт (2^{12} - 2), є моделі комутаторів з апаратним лімітом – 256 або 1024 VLAN. VLAN *1* зазвичай зарезервована як нативна VLAN для керування, що зменшує кількість доступних VLAN.

Транкові обмеження. Кожен транковий порт може передавати лише ті VLAN, які явно дозволені (дозвіл або фільтрація VLAN). Існують комутатори, які мають обмеження на кількість VLAN, котрі можна пропускати через один транковий порт.

Таблиці CAM (Content Addressable Memory) і *TCAM* (Ternary Content Addressable Memory): комутатори мають обмежену ємність для зберігання даних, що може обмежити загальну кількість пристроїв у кожній VLAN.

Проблеми з широкомовними доменами. VLAN зменшує кількість широкомовних доменів, але кожна VLAN створює свій окремий домен, що може перевантажувати комутатори у великих мережах.

Пропускна здатність і затримка. VLAN можуть збільшувати затримки в мережі через необхідність додаткової обробки тегів 802.1Q. Додаткові механізми, такі як QoS (Quality of Service), також впливають на продуктивність.

Проблеми безпеки. VLAN можуть бути вразливі до атак, таких як VLAN Hopping або Double Tagging, якщо не налаштовано належний захист.

Сумісність обладнання. Не всі комутатори підтримують однакові протоколи для VLAN (наприклад, VTP на Cisco), через що можуть виникати проблеми при підключенні обладнання різних виробників.

4.5 Бездротова передача даних

До кінця 1970-х років технології радіодоступу досягли певної міри зрілості та забезпечили виробництво порівняно компактних та недорогих радіотелефонів. Бездротовий зв'язок не обов'язково означає мобільність. Широко використовується так званий фіксований бездротовий зв'язок, коли вузли, що взаємодіють, постійно розташовуються в межах невеликої території.

Бездротові мережі Wi-Fi в більшості випадків використання є мережами з фіксованим бездротовим доступом, оскільки переміщення користувачів обмежено. Такі переміщення не вимагають зміни IP-адреси вузла, оскільки вузол весь час знаходиться в зоні покриття однієї і тієї ж IP-підмережі точки доступу мережі Wi-Fi. У той же час мережа Wi-Fi може бути мобільною, якщо її точки доступу пов'язані в загальну IP-мережу з IP-маршрутизацією між окремими зонами покриття точок доступу, які в цьому випадку стають аналогом стільникової мобільної телефонної мережі.

З появою стандарту IPPP 802.11 (1997 рік) стало можливим будувати мобільні мережі Wi-Fi, що за функціональністю близькі до Ethernet і забезпечують як фіксований, так і мобільний доступ користувачів.

З розвитком технологій, стільникові телефонні мережі стали широко використовуватися для мобільного доступу до Інтернету і, починаючи з покоління 4G, стали швидкими мобільними комп'ютерними мережами, оскільки основною послугою в них став доступ до Інтернету, а телефонні послуги стали надаватися також з використанням протоколу IP та Інтернету.

Відстань між вузлами, територія охоплення, швидкість передачі – це характеристики бездротової лінії зв'язку, багато в чому залежить від частоти використання електромагнітного сигналу.

Існують три частотні діапазони – 900 МГц, 2.4 МГц та 5ГГц, які рекомендовані міжнародним союзом електрозв'язку (ITU, International Telecommunication Union), як діапазони для міжнародного використання без ліцензування. Ці діапазони (ISM-діапазони) виділені промисловим товарам бездротового зв'язку загального призначення (пристрої блокування дверей автомобілів, науковим та медичним приладам). Діапазон 900 МГц найбільш затребуваний, оскільки низькочастотна техніка завжди коштувала дешевше.

Діапазон 2.4 ГГц використовують у технологіях Bluetooth та Wi-Fi – IEEE 802.11b (g, n, ax). Діапазон 5.5 ГГц використовують у технологіях Wi-Fi – IEEE 802.11a (n, ac, ax, be).

Технології стільникового зв'язку 5G використовуються по всьому світу, станом на 2025 рік 5G-мережі розгорнуті у 354 країнах та регіонах, покриття 5G становить близько 55% населення світу, з прогнозом збільшення до 85% до 2030 року [23].

Стандарт 5G працює в декількох діапазонах частот, які поділяються на три основні категорії:

– Low-band (низькочастотний діапазон): частоти нижче 1 ГГц (зазвичай 600–900 МГц); як переваги – має гарне покриття, дальність дії, здатність проходити через стіни; як недоліки – невисока швидкість порівняно з іншими діапазонами.

– Mid-band (середньочастотний діапазон): частоти від 1 до 6 ГГц, компроміс між швидкістю та дальністю дії – забезпечує широке покриття, але з нижчою швидкістю передачі даних; найбільш використовуваний діапазон (особливо 3.5 ГГц) для 5G у багатьох країнах.

– mmWave (міліметрові хвилі): частоти від 24 до 100 ГГц (частіше 24–40 ГГц); забезпечує дуже високу швидкість передачі даних та мінімальні затримки, але має коротку дальність дії, слабке проникнення через перешкоди.

Використання антен в комп'ютерних мережах

Антени є невід'ємною частиною бездротових комп'ютерних мереж. Навіть якщо вони непомітні (наприклад, вбудовані в ноутбук або точку доступу), вони завжди присутні у пристроях, що працюють по радіоканалу (рис. 35).

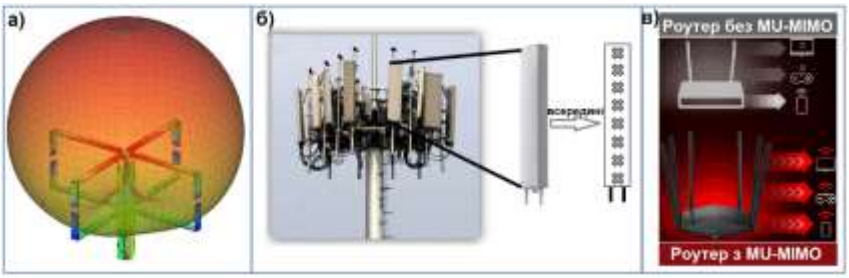


Рисунок 35 – Приклади антен

Антени активно використовуються в комп'ютерних мережах, особливо в тих, де дані передаються бездротовими каналами: Wi-Fi, мобільні та професійні мережі, технології Bluetooth, Zigbee, інтернет речей (IoT), супутниковий інтернет. Роутери та точки доступу оснащені антенами для передачі та прийому радіосигналів. Типи антен, що використовуються у комп'ютерних мережах, надано в таблиці 4.

Таблиця 4 – Характеристики антен

Тип антени	Характеристика	Застосування
Всеспрямована	Випромінює на всі боки	Wi-Fi роутери
Спрямована	Сфокусована на одному напрямку	Зв'язок між будинками
Панельна	Компактна, спрямована	Вуличні точки доступу
Параболічна	Велика дальність і вузький промінь	Супутниковий зв'язок
Вбудована	Всередині корпусу пристроїв	Ноутбуки, смартфони

Для підключення антен у комп'ютерних мережах використовується коаксіальний кабель, найчастіше RG-6, RG-58, LMR-240 або LMR-400, з роз'ємами SMA, N-type (відповідно до обладнання).

Особливості підключення антен

Частота сигналу, відстань, тип пристроїв є основними чинниками під час вибору кабелю. Чим довше кабель – тим більше втрат сигналу. На частотах 2.4 ГГц, 5 ГГц і особливо 24–40 ГГц (mmWave) важливо використовувати якісний кабель та коротку довжину.

Для поліпшення характеристик бездротового обміну даними (швидкості, дальності передачі, захисту ліній зв'язку від завад) використовують різноманітні методи: підвищення потужності сигналу, різні способи модуляції та кодування, частотне та тимчасове мультиплексування, накладання фільтрів, використання на одній лінії зв'язку кілька передавачів і приймачів (технологія MIMO).

Прийом та передача з використанням декількох антен – це технологія MIMO (Multiple Input Multiple Output), що широко застосовується в сучасних бездротових системах зв'язку, включаючи Wi-Fi (наприклад, 802.11n/ac/ax), 4G LTE та 5G.

MIMO (Multiple Input Multiple Output) – метод просторового кодування сигналу, що дозволяє збільшити смугу пропускання каналу, в якому одночасно здійснюються передача та прийом даних системами з кількох антен, метод дозволяє збільшити продуктивність, надійність і пропускну здатність бездротового зв'язку.

Один із ключових аспектів MIMO – можливість передавати різні потоки даних одночасно за тією самою частотою, але через різні антени. Це називається просторовим мультиплексуванням. Типи MIMO:

– SU-MIMO (Single-User MIMO): дані передаються одному користувачеві за раз;

– MU-MIMO (Multi-User MIMO): одночасно обслуговуються кілька користувачів, кожен отримує один або кілька потоків даних;

– Massive MIMO: використовується в 5G, десятки антен (наприклад, 64×64) для обслуговування безлічі користувачів одночасно.

Використання технології MIMO надано в таблиці 5

Таблиця 5 – Застосування методу Multiple Input Multiple Output

Технологія	**Використовувана схема MIMO**
Wi-Fi 4 (802.11n)	до 4×4 MIMO (4 антени на прийом потоку, 4 на віддачу)
Wi-Fi 5 (802.11ac)	до 8×8 MIMO
Wi-Fi 6 (802.11ax)	до 8×8 MIMO + OFDMA
4G LTE	до 4×4 MIMO
5G NR	до 64×64 Massive MIMO

OFDM (Orthogonal Frequency-Division Multiplexing, мультиплексування з ортогональним частотним поділом каналів) – це метод мультиплексування (схема модуляції), який перетворює високошвидкісний потік даних на ряд низькошвидкісних потоків, якими передається інформація.

OFDMA (Orthogonal Frequency Division Multiple Access) є розрахованою на багато користувачів версією цифрової модуляції OFDM. У Wi-Fi 6 (802.11ax) OFDMA – одна з найважливіших функцій для підвищення продуктивності мережі.

OFDM і OFDMA поділяють передані дані на кілька невеликих пакетів, щоб переміщати невеликі біти інформації. OFDMA поділяє канал на менші частотні виділення (групи), що називаються піднесущими. Завдяки розподілу каналу

невеликі пакети можуть одночасно передаватися на кілька пристроїв. Пакети, які прибули, продовжують переміщатися і їм не потрібно чекати інших пакетів. У низхідній лінії OFDMA-зв'язку маршрутизатор може використовувати різні групи для відправки пакетів різним клієнтам, що уможливлює керування затримкою.

Бездротові локальні мережі

Бездротові локальні мережі (Wireless Local Area Network, WLAN) в деяких випадках кращі, ніж мережі з дротовим рішенням, а іноді є єдиним варіантом зв'язку. У WLAN сигнал поширюється за допомогою електромагнітних хвиль високої частоти. Сучасні локальні бездротові мережі передають дані на швидкостях до кількох гігабіт за секунду. Поряд з перевагою бездротового зв'язку є і проблемні моменти, що створюють серйозні труднощі для надійного прийому інформації: перешкоди від різноманітних побутових приладів та інших телекомунікаційних систем, атмосферні перешкоди, відбиття сигналу.

Бездротова локальна мережа є неповнозв'язковою і не має точно обмеженої області покриття. У цих мережах використовується пряма корекція помилок (FEC) та протоколи з повторною передачею втрачених кадрів. Мережі та обладнання стандарту IEEE 802.11 (Wi-Fi) займають лідируючі позиції у світі бездротових локальних мереж.

Сімейство стандартів IEEE 802.11

Стандарт IEEE 802.11, розробка якого була завершена у 1997 році, є базовим стандартом та визначає протоколи, необхідні для організації бездротових мереж. Стек протоколів IEEE 802.11 відповідає загальній структурі стандартів комітету 802 – складається з фізичного рівня та рівня MAC, поверх яких працює рівень LLC. Як і у всіх технологій сімейства 802, технологія 802.11

визначається нижніми двома рівнями – фізичним та MAC, а рівень LLC виконує свої стандартні функції, загальні для всіх технологій LAN.

Рівень MAC у бездротових мережах виконує більше функцій, ніж у дротових. Функції рівня MAC у стандарті 802.11 включають:

– доступ до середовища, що розділяється;

– забезпечення мобільності станції за наявності декількох базових станцій;

– забезпечення безпеки, що дорівнює безпеці дротових локальних мереж.

В таблиці 6 представлені найбільш популярні варіанти фізичного рівня стандартів сімейства IEEE 802.11.

Таблиця 6 – Стандарти родини IEEE802.11

Назва	**Робочий діапазон частот,** ГГц	**Максимальна швидкість ***	**Спосіб модуляції**	**Рік прий-няття**
IEEE 802.11 (Wi-Fi)	2.4	до 2 Мбіт/с	DSSS/FHSS	1997
IEEE 802.11b (Wi-Fi 1)	2.4	11 Мбіт/с	DSSS	1999
IEEE 802.11a (Wi-Fi 2)	5	54 Мбіт/с	OFDM	1999
IEEE 802.11g (Wi-Fi 3)	2.4	54 Мбіт/с	OFDM	2003
IEEE 802.11n (Wi-Fi 4)	2.4 5	288.8 Мбіт/с 600 Мбіт/с	OFDM MIMO	2008
IEEE 802.11ac (Wi-Fi 5)	5	до 3.5 Гбіт/с	OFDM MIMO	2013/2014
IEEE 802.11ax (Wi-Fi 6)	2.4/5/6	до 9.6 Гбіт/с	OFDMA MIMO	2019
IEEE 802.11be (Wi-Fi 7)	2.4/5/6	до 46 Гбіт/с	OFDMA MIMO	2024
IEEE 802.11bn (Wi-Fi 8)	В розробці (на 2028 р), має працювати в діапазонах радіочастот 2.4, 5, 6, 7, 42.5 і 71 ГГц. Очікувана швидкість 100 Гбіт/с [15].			

*(без перешкод, на відстані 1 м між передавачем та отримувачем)

Загальні властивості стандартів сімейства IEEE 802.11:

– однакова топологія;

– підтримка робочого спектру частот: 2.4 ГГц, 5 ГГц чи обидва діапазони;

– один і той же спосіб доступу до середовища CSMA/CA (метод прослуховування несучої частоти з множинним доступом і запобіганням колізій);

– однакова структура кадру канального рівня;

– усі стандарти мають адаптивний механізм зміни швидкості передачі залежно від відстані до приймача.

Вузли мережі Wi-Fi оснащені мережним адаптером, що виконує функції фізичного та канального рівнів, відрізняючись від мережевого адаптера дротової мережі наявністю антени.

Відмінності між різними стандартами IEEE 802.11:

– максимальна швидкість сигналу (в біт/с);

– радіус дії сигналу (в метрах): географічна відстань, на якій можливий прийом Wi-Fi;

– частота сигналу (в ГГц): складається з коротких хвиль і забезпечує бездротову роботу Wi-Fi, найчастіше використовувані сьогодні частоти 2.4 ГГц та 5 ГГц.

Стандарт 802.11 визначає як основний структурний елемент WLAN мережу з базовим набором послуг – BSS (Basic Service Set). BSS являє собою набір бездротових мережевих пристроїв, що розділяють середовище передачі та працюють з однаковими характеристиками доступу до середовища: частота та схема модуляції сигналів (рис. 36).

Рисунок 36 – Інфраструктура бездротової мережі

Сучасні топології локальних мереж стандарту IEEE 802.11 відображають спосіб організації бездротових з'єднань між пристроями. Основні топології, які використовуються у бездротових локальних мережах (WLAN), згідно з IEEE 802.11, включають:

1. *Індивідуальний режим* (Ad Hoc, IBSS – Independent Basic Service Set). Тимчасова мережа між ноутбуками для обміну файлами, є простою при налаштуванні, не потребує інфраструктури. Але присутня обмеженість масштабованості, відсутнє централізоване керування. Кожен пристрій з’єднується безпосередньо з іншими без використання точки доступу (Access Point).

Мережа *Ad Hoc* являє собою набір вузлів, що взаємодіють через загальне електромагнітне середовище на основі децентралізованого алгоритму доступу, це мережа, що створюється самовільним способом на невеликий період часу. Базова станція в мережі *Ad Hoc* відсутня і в кожний момент часу в мережі є один або кілька вузлів, які беруть на себе провідну роль. Ці мережі працюють автономно, у них немає жодних засобів для зв'язку з іншими мережами.

2. *Інфраструктурний режим* (Infrastructure Mode, BSS – Basic Service Set). Мережа має централізоване керування, підтримку безпеки, масштабованість. Усі пристрої з'єднуються через точку доступу (AP, Access Point), існує залежність від AP.

3. *Розширений набір базових служб* (ESS – Extended Service Set). Wi-Fi мережа в офісі або навчальному закладі. Покриття великих площ, роумінг. Кілька точок доступу з’єднані між собою через дротову мережу (зазвичай Ethernet) і координуються для забезпечення безперервного покриття. Складність налаштування та адміністрування.

4. *Меш-топологія* (Mesh Network, WMN – Wireless Mesh Network). Міські Wi-Fi мережі, розгортання у віддалених місцях, системи «розумного міста». Кожен вузол (пристрій або точка доступу) може передавати трафік інших пристроїв, створюючи динамічну маршрутизовану мережу. Мережі з високою надійністю, мають можливості самовідновлення, масштабованість.

5. *P2P-топологія* (Peer-to-Peer). Дана топологія є різновидом *Ad Hoc*, але більш спрямована на безпосереднє з'єднання між двома пристроями без використання мережевої інфраструктури. Забезпечує пряме підключення смартфона до принтера або ноутбука (табл. 7).

Таблиця 7 – Коротке порівняння мереж з різними топологіями

Топологія	**Централізованість**	**Масштабованість**	**Сценарії використання**
Ad Hoc	Ні	Обмежена	Тимчасові, малі мережі
Infrastructure	Так	Висока	Домашні та офісні мережі
ESS	Так	Дуже висока	Великі мережі з роумінгом
Mesh	Частково	Дуже висока	Розподілені, міські та польові
P2P	Ні	Дуже обмежена	Тимчасові прямі з’єднання

Формат кадру технології Wi-Fi

У стандарті Ethernet є кадр лише одного типу (кадр даних), у технології Wi-Fi існують кадри трьох типів:

– кадри даних;

– кадри шару управління;

– кадри шару менеджменту.

Тип і підтип кадру визначаються значенням полів, що становлять структуру поля керування кадром *Frame control* (рис. 37).

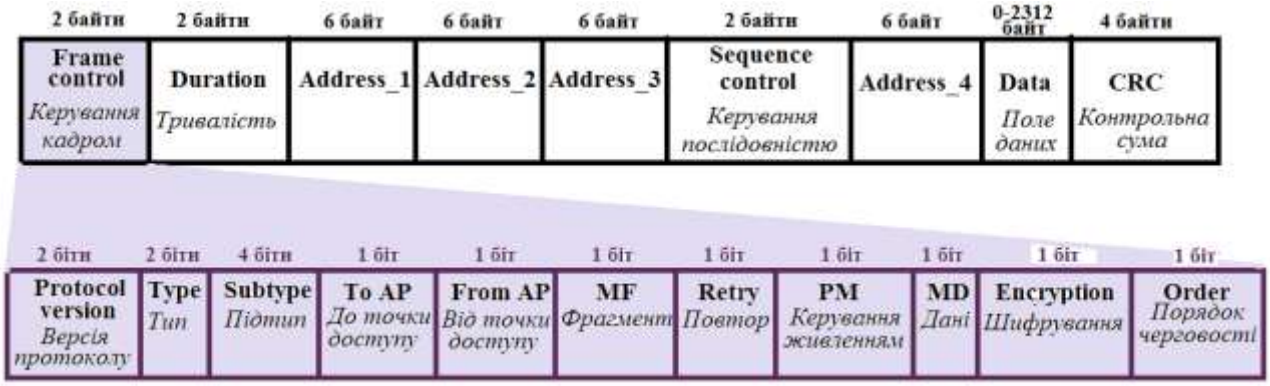


Рисунок 37 – Фрагмент кадру Wi-Fi

Однією з особливостей кадру Wi-Fi є наявність чотирьох полів MAC-адрес (Address_1-4). Їхнє призначення залежить від конфігурації мережі. Коли дві точки доступу безпосередньо взаємодіють одна з одною, використовуються всі чотири MAC-адреси – станції джерела, двох точок доступу та станції призначення. Коли станція обмінюється даними з вузлом Інтернету, використовуються три адреси – станції користувача, точки доступу та маршрутизатора розподільчої системи.

Поле даних (Data) дозволяє переносити до 2312 байт даних користувача.

При спотворенні бітів у радіосередовищі станція-відправник передає не весь кадр, а лише його фрагмент. Для підтримки фрагментування в полі *керування послідовністю* вказується не лише номер кадру, а й номер фрагмента.

Поле *тривалість* визначає час зайнятості середовища, яке станція додатково резервує після передачі кадру.

Одиниця в полі *шифрування* означає, що дані зашифровані. Одиниця в полі *дані* означає, що станція має дані, які вона хоче передати в наступних кадрах. Одиниця в полі *порядок черговості* повідомляє приймаючу станцію, що порядок має значення. Поля *до точки доступу* та *від точки доступу* показують напрямок передачі кадрів. У полі *керування кадром* кадру Wi-Fi є біт *управління живленням*, який станція встановлює в *1* у будь-який час, який вона вважає придатним для переходу в сплячий режим, коли вона не передає і не прийме дані (економія енергії батареї).

Процедура приєднання до мережі

Для роботи з точкою доступу станція користувача повинна виконати процедуру приєднання до мережі. Існують два режими приєднання – *пасивний* та *активний*.

У пасивному режимі станція пасивно прослуховує радіоефір і намагається на всіх частотних каналах виявити кадри спеціального типу – кадри маячки (beacon frames). Ці кадри періодично (з інтервалом 100 мс) посилає точка доступу, вони містять її MAC-адресу і ідентифікатор мережі SSID.

В активному режимі станція сама посилає у радіосередовище спеціальні пробні кадри (probe frames). Точка доступу, отримавши пробний кадр, відповідає на нього, повідомляючи станції відомості про себе – свою MAC-адресу та ідентифікатор мережі SSID.

Станція може одночасно отримувати кадри-маячки від кількох точок доступу. Рішення про підключення до однієї з доступних мереж приймає користувач. Станція запам'ятовує у своєму кеші ідентифікатор мережі та параметри аутентифікації, що дозволяє виконати автоматичне підключення до цієї мережі наступного разу, як тільки станція опиниться у зоні покриття точки доступу цієї мережі (автоматичне з'єднання можна заборонити).

Коли мережу вибрано, станція надсилає точці доступу кадр *запит на приєднання*. Потім точка доступу ініціює процедуру аутентифікації і якщо вона успішна, маршрутизатор розподіленої системи, користуючись протоколом DHCP, призначає станції IP-адресу. Для адрес IPv4 маршрутизатором, швидше за все, буде видана приватна IP-адреса, що вимагає застосування техніки трансляції адрес (NAT) для доступу станції до мережі Інтернет. Для адрес IPv6, швидше за все буде видана глобальна, так що трансляція адрес не знадобиться.

Тема 5. Поняття та визначення глобальних мереж

Перші комп'ютери 1950-х років були дуже дорогими, громіздкими, без надання можливості інтерактивної роботи користувачам. Через високу вартість обчислювальної техніки підприємства не могли собі дозволити придбання великої кількості комп'ютерів, тому не було й потреби у створенні локальних мереж, бо просто не було чого об'єднувати в мережу. А ось потреба у з'єднанні кількох комп'ютерів, що знаходяться на великій відстані один від одного, до цього часу вже назріла.

Почалося все з вирішення простого завдання – організації доступу до окремого комп'ютера терміналів, віддалених від нього на сотні/тисячі кілометрів. Термінали з'єднувалися з комп'ютерами через телефонні мережі за допомогою модемів, надаючи численним користувачам можливість отримувати віддалений доступ до розподілених ресурсів потужних суперкомп'ютерів. Пізніше з'явилися системи, у яких поруч із віддаленим з'єднанням типу *термінал-комп'ютер* було реалізовано тип зв'язку *комп'ютер-комп'ютер*.

Головним технологічним нововведенням, яке привнесли перші глобальні комп'ютерні мережі, була відмова від принципу комутації каналів, який використовувався в телефонних мережах. Виділяємий на весь час сеансу зв'язку составний телефонний канал, яким передавалася інформація з постійною

швидкістю і у якого періоди інтенсивного обміну чергувалися з довгими паузами, не міг ефективно використовуватися пульсуючим трафіком комп'ютерних даних. Численні дослідження показали, що пульсуючий і значною мірою не чутливий до затримок комп'ютерний трафік набагато ефективніше передається мережами, що працюють за принципом *комутації пакетів*, коли дані поділяються на невеликі порції (пакети), які самостійно переміщуються по мережі, досягаючи кінцевого вузла завдяки наявній адресі в заголовку пакета.

Протягом багатьох років глобальні мережі будувалися на основі телефонних каналів, здатних у кожний момент часу вести передачу лише однієї розмови в аналоговій формі, що зумовлювало дуже низьку швидкість передачі дискретних комп'ютерних даних одночасно із значними спотвореннями сигналів, що передаються.

Прогрес глобальних комп'ютерних мереж багато в чому визначався прогресом телефонних ліній. З кінця 1960-х років у телефонних мережах стала застосовуватись передача голосу в цифровому форматі, що стало поштовхом появи високошвидкісних цифрових каналів, з'єднання яких забезпечували автоматичні телефонні станції, дозволяючи одночасно створювати десятки-сотні сеансів зв'язку.

Сьогодні глобальні мережі за різноманітністю та якістю послуг, що надаються, наздогнали локальні мережі, які довгий час лідирували в цьому відношенні, хоча й з'явилися вони значно пізніше глобальних.

5.1 Мережні технології

Протягом всього часу існування глобальних комп'ютерних мереж важливу роль в них відігравали транспортні технології, засновані на техніці віртуальних каналів. Еволюція технологій цього типу відбувалася від *X.25* через *frame relay* і *ATM* до *MPLS*.

У мережі з віртуальними каналами два вузли можуть розпочати обмін даними лише після встановлення логічного з'єднання – віртуального каналу. Просування кадрів уздовж віртуального каналу відбувається не на основі адрес кінцевих вузлів, а на основі *мітки*, яка дозволяє комутаторам мережі визначати належність кадрів тому чи іншому віртуальному каналу і просувати їх відповідно. Значення мітки потоку змінюється у кожному комутаторі під час передачі кадру з вхідного інтерфейсу на вихідний – у разі говорять, що відбувається комутація за мітками.

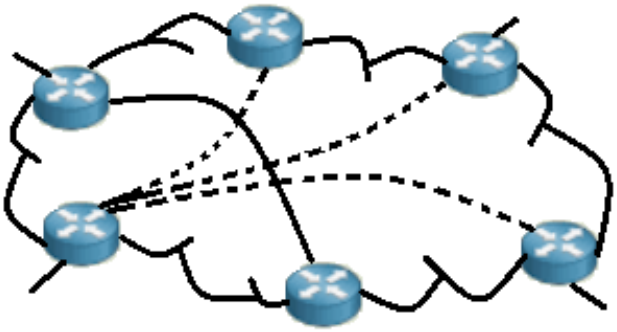
Технічне встановлення віртуального каналу означає формування записів у таблицях просування кадрів на кожному комутаторі вздовж віртуального каналу. Така таблиця включає інформацію про просування – на який вихідний порт необхідно передати кадр із певною міткою, яке нове значення необхідно присвоїти мітці після передачі кадру на вихідний інтерфейс.

Створення віртуального каналу, що комутується, відбувається за ініціативою кінцевого вузла мережі за допомогою спеціального протоколу, що посилає пакет із запитом на встановлення з'єднання в напрямку до вузла призначення віртуального каналу (такий канал створюється динамічно). По відношенню до пакета із запитом на з'єднання мережа працює в дейтаграмному режимі і такий пакет повинен містити адресу призначення кінцевого вузла, а не мітку.

Постійний віртуальний канал встановлюється вручну, адміністратор створює його на достатньо тривалий час. Прикордонний комутатор мережі приймає пакети від зовнішньої мережі (яка може і не підтримувати техніку віртуальних каналів) та відбиває їх на один із віртуальних каналів мережі. Таке відбиття виконується на основі вхідного фізичного інтерфейсу – всі кадри, що приходять на деякий вхідний інтерфейс, відбиваються на один і той же віртуальний канал.

У випадках, коли необхідно розрізняти декілька потоків, що приходять на вхідний інтерфейс і відображати їх на різні віртуальні канали, у прикордонному комутаторі поряд із таблицею просування має існувати таблиця відображення потоків.

Віртуальні канали можуть мати двоточкову топологію або топологію типу зірка. У такому каналі той самий кадр передається від джерела (центру зірки) вздовж каналів усім кінцевим вузлам. Кінцеві вузли не можуть використовувати віртуальний канал зіркоподібної топології для обміну кадрами між собою (рис. 38).



—— віртуальний канал «точка-точка» ----- віртуальний канал «зірка»

Рисунок 38 – Топології віртуальних каналів

Технологія віртуальних каналів X.25 з'явилася практично одночасно з мережею ARPANet і до середини 80-х років XX століття була основною технологією для побудови як мереж операторів зв'язку, так і корпоративних мереж. Поширення високошвидкісних цифрових оптичних каналів у середині 80-х призвело до появи нової технології глобальних мереж Frame Relay.

Технологія Frame Relay – перша технологія глобальних мереж із комутацією пакетів, яка надала користувачам мережі гарантію пропускної спроможності мережевих з'єднань. Мережі даної технології набули великого поширення у 80-х і першій половині 90-х років.

Протокол Frame Relay не підтримує процедури надійної передачі кадрів, залишаючи повторну передачу спотворених/втрачених даних протоколам вищих рівнів (наприклад, TCP). Мережі Frame Relay були розраховані лише на передачу комп'ютерного трафіку та не справлялися з мультимедійним. Тому поступилися місцем новій технології глобальних мереж, що отримала назву асинхронного режиму передачі.

Технологія ATM. Асинхронний режим передачі (Asynchronous Transfer Mode, ATM) – це технологія, заснована на техніці віртуальних каналів і призначена для використання як єдиний універсальний транспорт мереж з інтегрованим обслуговуванням. У даній технології застосовується метод комутації пакетів, який ґрунтується на асинхронному тимчасовому мультиплексуванні. Мережі здатні передавати трафік різного типу: чутливий до затримок (голосовий) та еластичний, тобто той, що дозволяє затримки в широких межах (трафік електронної пошти, перегляд веб-сторінок). Незважаючи на свої переваги, технологія ATM значною мірою була замінена технологіями на основі IP (Internet Protocol) з кількох причин, основні з яких пропускна спроможність, складність, вартість (інфраструктура ATM складна та вимагає спеціалізованого обладнання, що робить її дорожчою порівняно з мережами на основі Ethernet та IP*)*.

Пасивні оптичні мережі, **PON** (Passive Optical Network). Проведення оптоволокна від *точки присутності* оператора зв'язку до будівлі користувача є найякіснішим рішенням в питанні забезпечення віддаленого доступу. Для роботи такої оптичної мережі потрібна наявність наступних комунікаційних пристроїв: підсилювачів, повторювачів, мультиплексорів – тобто приладдя, яке потребує електроживлення. Таке рішення є досить коштовним. Для здешевлення оптичної мережі доступу ще в 90-х роках XX століття було запропоновано технологію *пасивних оптичних мереж*, побудовану на застосуванні пасивних оптичних

пристроїв – розгалужувачів (splitter), які не потребують електроживлення. За допомогою розгалужувачів організується деревоподібна оптоволоконна структура, що з'єднує точку присутності оператора (point of presents, POP) із приміщеннями користувачів. Розгалужувач виконує просту операцію – він спрямовує світловий сигнал з одного вхідного волокна в декілька вихідних, що йдуть у напрямку до користувачів. Розгалужувач також виконує зворотну операцію мультиплексування сигналу користувачів в одне волокно, що йде до точки присутності оператора.

Мультиплексування сигналу в телекомунікаційних мережах – це метод, за допомогою якого кілька сигналів об'єднуються (ущільнюються) в один сигнал через загальний носій (прикладом може бути відео-файл, в якому потік (канал) відео об'єднується з одним або декількома каналами аудіо). Мультиплексування ділить пропускну здатність каналу зв'язку на кілька логічних каналів, по одному для кожного сигналу або потоку даних, що передаються. Зворотний процес, відомий як *демультиплексування*

Демультиплексування – це розподіл потоку, що приймається, процес надсилання вхідних повідомлень відповідним клієнтам на основі певних полів у заголовках протоколів. Є найважливішою функцією в протоколах передачі даних, маршрутизації та транспорту для забезпечення ефективного зв'язку між кінцевими користувачами, програмами та іншими протоколами.

PON є технологією високошвидкісної передачі даних оптоволоконними лініями зв'язку для доставки інформації безпосередньо до термінального пристрою клієнта (рис. 39). Вона передбачає підключення всіх абонентських пристроїв через один оптичний кабель, в таких мережах використовується пасивний спліттер, який розділяє оптичний канал на декількох абонентів. Такий підхід дозволяє одночасно користуватися кількома телекомунікаційними послугами – інтернетом, телебаченням, телефоном.

Рисунок 39 – Загальна схема PON

PON – це загальний термін типу мереж, які використовують оптичні волокна передачі даних і телекомунікаційних сигналів. GPON є конкретною реалізацією технології PON, яка використовує архітектуру «точка-багато точок», дозволяючи кільком користувачам спільно використовувати одне й те саме оптоволоконне з'єднання (рис. 40).

Рисунок 40 – Архітектура PON

Технологія GPON (Gigabit-Capable Passive Optical Networks) є останнім варіантом пасивної оптичної мережі PON, який описано у стандарті ITU-T G.984.x. Типова мережа GPON містить такі основні активні компоненти: передатний пристрій OLT (рис. 40), який встановлюється на стороні провайдера, та обладнання, що приймає ONT (Optical Network Terminal) або ONU (Optical Network Unit), яке встановлюється на стороні абонента.

OLT (Optical Line Terminal) є точкою з'єднання різних терміналів оптичної мережі (ONT) в середовищі GPON. OLT об'єднує трафік даних від ONT і може надсилати дані до відповідних пунктів призначення. OLT є аналогом мережного комутатора, може мати кілька портів, і кожен порт може керувати однією мережею PON з коефіцієнтами поділу близько 1:32 або 1:64 (для кожного порту OLT до 32 або 64 ONU на клієнтських сайтах);

ONT/ONU (абонентський термінал) – це невеликий пристрій у пластиковому корпусі, призначений для прийому трафіку по оптичному волокну та передачі даних назад. Він оснащений оптичним портом для підключення до мережі GPON і мідним портом для підключення по крученій парі (кабелю UTP). Принцип роботи ONU пристрою полягає в тому, що він приймає оптичний сигнал від центрального комутатора OLT і перетворює його на електричний. За крученою парою підключається пристрій користувача (комп'ютер, телевізор, роутер), від якого ONU приймає електричні сигнали, перетворює в оптичні і відправляє назад до OLT. Управління роботою ONU повністю здійснюється дистанційно із центрального оптичного комутатора, який розташований на стороні провайдера

Технологія MPLS. Технологія багатопротокольної комутації за мітками (Multi protocol label switching, MPLS) поєднує техніку віртуальних каналів з функціональністю стека TCP/IP, надаючи різноманітні транспортні послуги в IP-мережах (насамперед послуги віртуальних приватних мереж). Технологія MPLS поєднує в одному комунікаційному пристрої (маршрутизаторі з комутацією за мітками) два методи просування пакетів – дейтаграмний метод та метод комутації віртуальних каналів.

Дейтаграмне просування реалізується протоколом IP, принцип його роботи такий самий, як і в звичайному IP-маршрутизаторі: його таблиця маршрутизації може створюватися як вручну, так і за протоколами маршрутизації стека TCP/IP.

Одночасно в цьому комунікаційному пристрої (маршрутизатор з комутацією за мітками) є другий модуль просування, що працює відповідно до техніки комутації віртуальних каналів (модуль комутації за мітками).

Обидва модулі просування координуються/керуються одним шаром управління, куди поряд з традиційними протоколами IP-маршрутизації (RIP, OSPF, IS-IS, BGP) входять сигнальні протоколи, які потрібні для автоматичного встановлення в мережі віртуального шляху – шляху комутації за мітками (label switching Path). Наявність спільного шару управління дозволяє маршрутизатору гнучко використовувати обидва модулі просування – одну частину потоку даних він може просувати, застосовуючи техніку IP-просування, іншу – техніку комутації за мітками. Шар управління має інформацію про топологію мережі, необхідну для кожного рівня просування.

MPLS покращує керування трафіком, використовуючи систему маркування для більш ефективної маршрутизації пакетів даних у порівнянні з традиційною IP-маршрутизацією. Кожному пакету даних призначається мітка, яка визначає його шлях через мережу. Постачальники послуг та підприємства використовують MPLS для визначення пріоритетів обслуговування різним типам трафіку (QoS). Наприклад, мережа може пропонувати два рівня обслуговування, кожен з яких віддає пріоритет різним типам трафіку – один рівень для голосу, інший для чутливого до часу трафіку.

QoS (Quality of Service, якість обслуговування) – це технологія або набір механізмів, що забезпечують контрольований рівень продуктивності мережевих сервісів (інтернету, передачі даних, відео, голосу).

Надання послуг віртуальних приватних мереж (Virtual Private Network, VPN) є однією з основних областей застосування технології MPLS. Такі її властивості, як логічний поділ потоків трафіку різних користувачів на основі техніки віртуальних каналів (у формі просування по мітках) та тісна інтеграція з

протоколами шару керування стеком TCP/IP, забезпечують застосування MPLS у створенні VPN.

Технології Ethernet у глобальних мережах. Carrier Ethernet (Ethernet для операторів) – набір технологій і стандартів для надання Ethernet як послуги між віддаленими об’єктами (офісами, філіями, дата-центрами).

Carrier Ethernet – це Ethernet, адаптований під використання телеком-операторами (Carriers) для надання послуг зв’язку своїм клієнтам (корпораціям, провайдерам, дата-центрам). Carrier Ethernet – це модель надання Ethernet-послуг операторами зв’язку, включаючи архітектуру, стандарти та протоколи (тобто те, що надається – сервіс).

Carrier-grade Ethernet – це технічний рівень якості й надійності Ethernet-рішень, що відповідає вимогам телеком-індустрії. Carrier-grade Ethernet – це характеристика обладнання та рішень, що відповідає стандартам надійності та обслуговування, необхідним для операторів зв’язку (тобто те, як воно реалізоване – якість, надійність, стабільність).

Основні стандарти Ethernet у глобальних мережах:

– Metro Ethernet: Ethernet у межах міста або агломерації;

– MEF (Metro Ethernet Forum): організація, яка розробила специфікації Carrier Ethernet;

– Ethernet over MPLS (EoMPLS): інкапсуляція Ethernet у MPLS для передачі по глобальній мережі;

– Ethernet Private Line (EPL): виділене Ethernet-з'єднання точка-точка;

– VPLS (Virtual Private LAN Service): створення віртуальної LAN поверх глобальної мережі.

Переваги Ethernet у глобальних мережах: простота (використання вже наявних і відпрацьованих LAN-технологій); висока швидкість (100 Гбіт/с і більше); масштабованість (починаючи з малого офісу і до великих

міжконтинентальних зв’язків); гнучке ціноутворення (оператори надають послуги з різними SLA); QoS та безпека (можна застосовувати політики пріоритезації та шифрування).

SLA (Service Level Agreement) – це угода про рівень обслуговування, яка визначає гарантовані параметри якості послуги, що надає провайдер або постачальник сервісу.

Ethernet у глобальних мережах використовується при підключенні філій банку в різних містах до головного офісу; для з'єднання дата-центрів між країнами; під час передавання відео, бекапів, віртуальних мереж (VPN) поверх Ethernet; в організації корпоративної хмари.

5.2 Загальна структура та функціонування глобальних мереж

Глобальні мережі охоплюються телекомунікаційними структурами, які об'єднують локальні інформаційні мережі. Кожна з глобальних мереж (Internet, ARPANet, Usenet, FIDONet, ALOHAnet, Bitnet та інші) організовувалася для конкретних цілей, а в подальшому поширювалася за рахунок під'єднання локальних мереж, які використовували її послуги та ресурси.

Концепція глобальних мереж достатньо ємне поняття – вони допомагають інтегрувати ринки та культури, долаючи розриви між розрізненими частинами світу, суттєво впливають на те, як взаємодіють країни, організації та окремі особи, полегшуючи потік інформації, товарів та послуг через географічні кордони. Глобальні мережі включають різні компоненти, такі як:

– *комунікаційні мережі*: Інтернет, мобільний зв'язок, платформи соціальних та освітніх мереж, що забезпечують взаємодію в режимі реального часу (UA-IX, Datagroup, Укртелеком, Facebook, Zoom, Moodle);

– *економічні мережі*: міжнародні торгові угоди, ланцюжки поставок та глобальні фінансові системи (SWIFT);

– *культурні мережі* (глобальний туризм, культурні обміни, взаємодія ЗМІ).

Всесвітня мережа – це розгалужена інфраструктура *наземних* та *підводних* магістральних каналів, в основі якої лежать різні технології. Найвідомішою глобальною мережею є Інтернет, структуру якої складають сервери, маршрутизатори, комунікаційні канали, кінцеві вузли та служби (електронна пошта, файлові архіви, форуми, спілкування у реальному часі, месенджери, хмарні сховища даних).

Інфраструктура глобальної мережі Інтернет

Фундамент для сучасної глобальної мережі було закладено ще ARPANET. Цей фундамент – *опорну мережу Інтернету*, надалі закріпили такі некомерційні мережі як NSFNET (США), NORDUNET (Європа). Згодом, наявні на той час публічні NAP (точки доступу до мережі) ставали критично перевантаженими, тому провідні телекомунікаційні компанії, які були одними з перших справжніх інтернет-провайдерів, почали створювати власну магістральну мережу з якіснішими та швидшими точками доступу.

У 1994 році опорна мережа Інтернету була приватизована комерційними компаніями. Чотирма найбільшими приватними провайдерами мережевого зв'язку США виявилися UUNet, AT&T, Sprint, Level 3.

Починаючи з 1995 року, комерційне використання Інтернету швидко зростало. Після того, як найбільші інтернет-провайдери зарекомендували себе на ринку, вони почали взаємодіяти, уклавши між собою *пірингові* угоди. Найбільші інтернет-провайдери, яких об'єднувала угода про піринг без розрахунків, стали інтернет-провайдерами *першого рівня* і склали оснóву Інтернету (розширивши цим магістраль). Так почала формуватися *ієрархія*, згідно з якою всіх інтернет-провайдерів, представлених сьогодні на ринку телекомунікаційних послуг, можна розділити на три рівня [16].

Інтернет-провайдери першого рівня (Tier-1). Кількість компаній, яким належать магістральні мережі Інтернет не доходить двадцяти, вони відіграють центральну роль у магістральній інфраструктурі Інтернету. Такі компанії володіють міжконтинентальними кабелями і обмінюються між собою трафіком безкоштовно, або купують транзитні послуги лише в інших провайдерів рівня 1, тоді як продають транзит провайдерам усіх рівнів.

Представниками магістральних провайдерів послуг є такі компанії: Lumen Technologies (США), Arelion (Швеція), NTT Communications (Японія), Liberty Global (Нідерланди), Telecom Italia Sparkle тощо.

Інтернет-провайдери другого рівня (Tier-2). Зазвичай це національні телекомунікаційні оператори зв'язку, які працюють в конкретному регіоні, країні, чи групі країн певного регіону і є найбільш поширеними інтернет-провайдерами. Вони укладають транзитні угоди з інтернет-провайдерами першого рівня та купують у них пропускну спроможність (трафік). Крім того, вони беруть участь у пірингу між собою і продають трафік провайдерам третього рівня.

Отже, провайдер Tier-2 має доступ до частини мережі Інтернет через пірингові з'єднання, та ще купує транзит IP-трафіку для доступу до решти Інтернету (рис. 41).

Швидкий піринг забезпечується через *точки обміну інтернет-трафіком* (TOIT, IXP), які розташованим по всьому світу. У цих точках (хабах/вузлах) концентрується як трафік, так і мережна інфраструктура (дата-центри, хостинг), які з'єднують між собою кілька інтернет-провайдерів.

Загалом сьогодні у світі близько 250 таких точок (DE-CIX (Франкфурт), AMS-IX (Амстердам), LINX (Лондон), France-IX (Париж), DTEL-IX (Київ), UA-IX (Київ), TDC (Данія), RETN (Великобританія), GigaNet (Київ), China Unicom).

Рисунок 41 – Карта мережі 1-IX [17]

Українські ТОІТ для пірингу українських і міжнародних операторів: *RUDAKi-IX* (Київ, Львів, Рівне, Дніпро, Житомир, Варшава, Франкфурт); *1-IX* (Київ, Львів, Одесса, Дніпро, Варшава, Амстердам, Франкфурт); *DTEL-IX*; *KMIX*. Точки організації з'єднань міжоператорського обміну IP-трафіком між незалежними регіональними мережами: *UA-IX*, *Giganet-IX*, *OD-IX*, *LVIV-IX*, *RV-IX*, *IF-IX*.

Інтернет-провайдери третього рівня (Tier-3). До них належать невеликі регіональні телекомунікаційним компанії, які займаються продажом підключення до Інтернету кінцевим споживачам. Інтернет для перепродажу вони або купують у Tier-2 операторів, або обмінюються безкоштовно паритетними включеннями один з одним безпосередньо чи на точках обміну трафіком з іншими Tier-3 провайдерами [18].

Організація глобальної мережі Інтернет

Компоненти структури мережі Інтернет поєднуються у загальну ієрархію. На фізичному рівні Інтернет представляє мережу вузлів (точок обміну інтернет-трафіком, ТОІТ), пов'язаних магістральними каналами. У точках обміну трафіком концентрується як трафік, так і мережна інфраструктура (дата-центри, хостинг

тощо.). Найбільші точки обміну розташовані по всьому світу (Франкфурт, Амстердам, Лондон, Париж, Нью-Йорк).

Майже всі канали зв'язку між континентами прокладаються дном океану, основою основ є трансокеанські кабелі: Європа – Америка через Атлантичний океан, Америка – Азія через Тихий океан, Азія – Європа уздовж узбережжя Східної Азії, через Бенгальську затоку, Аравійське море, Червоне море і до Середземномор'я (рис. 42).

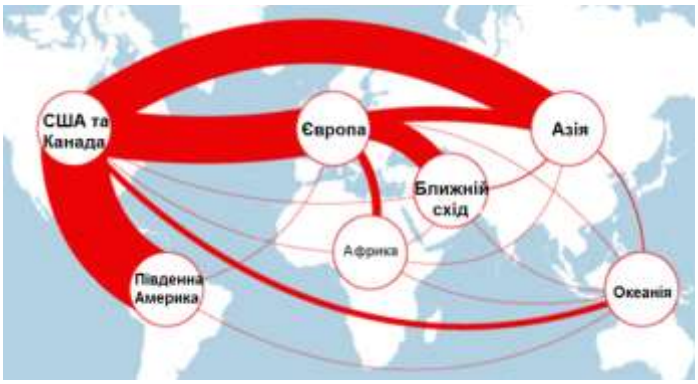


Рисунок 42 – Підводні магістральні канали [19]

Прокладання підводного кабелю та введення його в експлуатацію – тривала і досить дорога процедура, тому кілька корпорацій зазвичай спільно фінансують такі проєкти, а потім ділять між собою оптоволоконні пари в кабелі. Як приклад – спільний проєкт по введенню в експлуатацію підводного транстихоокеанського кабелю FASTER (2016 р.) компанії Google з партнерами (China Mobile International, China Telecom Global, Global Transit, KDDI, Singtel). Вартість прокладки магістралі FASTER склала $300 млн, але для інтернет-компанії це дешевше, ніж орендувати такі ж канали в інших. Додатково з цього Google отримала збільшений контроль над лініями зв'язку, які пов'язують її дата-центри.

Microsoft та Facebook мають свій трансатлантичний кабель MAREA (рис. 43), що надає зв’язок між Вірджинія-Біч (США) та Більбао (Іспанія) і управляється «Telxius» – дочірньою фірмою іспанської телекомунікаційної

компанії «Telefónica». Укладання кабелю почалося у серпні 2016 року і закінчилося у вересні 2017 року, експлуатацію розпочато у лютому 2018 року. Кабель вагою 4650 т і довжиною 6600 км має розрахункову пропускну здатність 160 Тбіт/с – по 20 Тбіт/с на кожну з 8 пар його оптоволоконних кабелів, оточених міддю, жорстким пластиковим захисним шаром і водонепроникним покриттям.

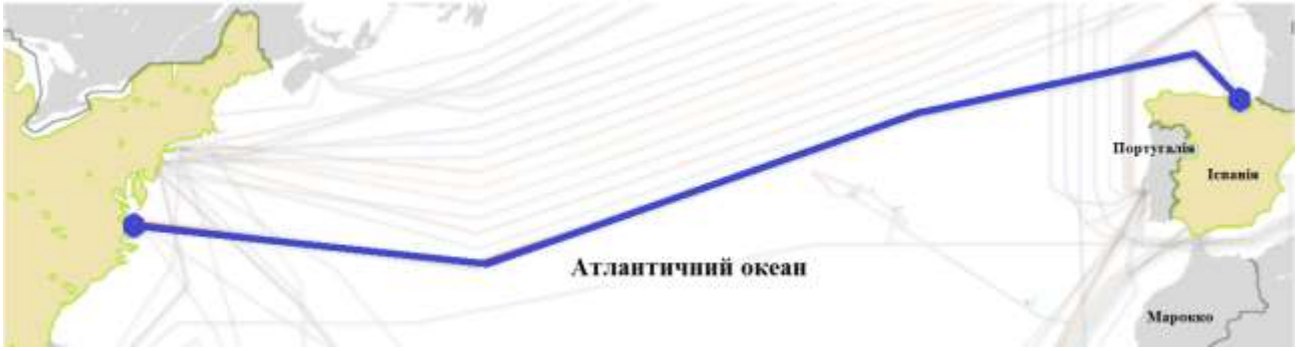


Рисунок 43 – Маршрут кабелю MAREA

В епоху технологій, здається, що космос є ідеальним середовищем для з'єднання «всесвітньої павутини», а закладка підводних кабелів, що використовується з 1960 року, давно застаріла. Але й сьогодні кабель залишається найкращим способом передачі інформації. Поки ще більш 90% усієї міжконтинентальної інформації передається за допомогою кабелів, що лежать на дні океанів (рис. 44).

Рисунок 44 – Карта світових підводних цифрових кабелів [20]

Головний недолік «космічного зв'язку» – затримка, спотворення або втрата сигналів. Відправлення повідомлення через «космос» та отримання відповіді потребує набагато більше часу, ніж за допомогою кабелю. Супутниковий інтернет-провайдер Starlink використовує *низькоорбітальні* супутники для надання інтернет-послуг по всьому світу (проєкт належить компанії SpaceX, заснованій Ілоном Маском). Згідно з офіційними даними компанії SpaceX, швидкість завантаження в мережі Starlink може досягати 150-200 Мбіт/с, а швидкість відправлення даних – до 20-40 Мбіт/с. Традиційний супутниковий інтернет, який використовує геостаціонарні супутники, зазвичай пропонує нижчу швидкість і вищу затримку порівняно із Starlink. Це обумовлено більш високою орбітою розташування супутників.

Основні принципи побудови мережі Інтернет

Організація глобальних мереж заснована на розподіленій архітектурі і має складну структуру, яка включає *мережі доступу*, мережі *агрегування трафіку*, *магістральну* мережу і багаточисельні *центри даних* (рис. 45, 46), за допомогою яких провайдери надають високорівневі послуги – офісні додатки, електронна пошта, інтернет-телефонія, послуги Інтернета речей.

Рисунок 45 – Схематичне зображення рівнів глобальної мережі

Технологія Ethernet операторського класу також широко використовується в глобальних мережах і тісно співіснує з технологією MPLS. Під час використання MPLS протоколи маршрутизації стека IP/TCP необхідні для дослідження топології мережі та винаходу раціональних маршрутів. Комбінація, створена інтеграцією IP та MPLS, видалила із глобальних мереж технології Frame Relay і ATM. Мобільні телефонні мережі сьогодні є повноцінними IP-мережами.

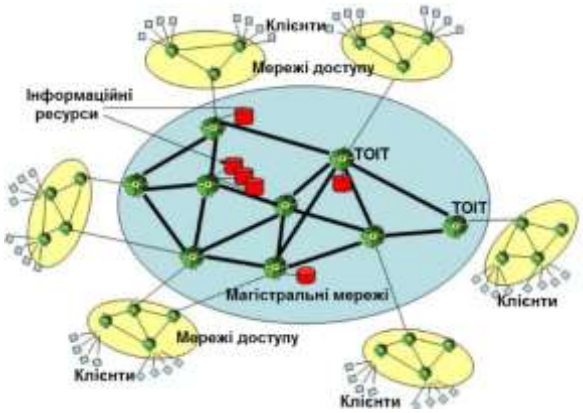


Рисунок 46 – Структура глобальної мережі

Опорна мережа Інтернету (internet backbone, хребет) – це *головні магістралі передачі* даних між величезними, стратегічно взаємозалежними мережами. Ці магістралі контролюються комерційними, державними, науковими центрами, *точками обміну трафіком* та *точками доступу до мережі*, які обмінюються інтернет-трафіком між країнами та континентами.

Магістральні мережі являють собою найбільш швидкісну частину (ядро) глобальної мережі, яка об’єднує чисельні мережі доступу в єдину мережу.

Мережі доступу – це мережі, які надають доступ індивідуальним та корпоративним абонентам від їх приміщень (квартир, офісів) до першого приміщення (пункту присутності) оператора мережі зв’язку або оператора корпоративної мережі. Ці мережі «відповідають» за розповсюдження глобальної мережі до приміщень її клієнтів.

Агрегування каналів інтернет (MultiWAN) – це технологія, яка дозволяє об’єднати кілька інтернет-підключень від різних провайдерів в одному пристрої. Це забезпечує підвищену пропускну здатність, збільшену швидкість та резервування у випадку відмови одного з підключень. Використовуючи технологію MultiWAN, можна об’єднати чотири і більше інтернет-канали в одному роутері.

Для надання інформаційних комп’ютерних послуг в мережах існують центри даних (ЦД). Центр даних загалом є локальною мережею з комутаторами, маршрутизаторами та серверами, на яких працює програмне забезпечення, за допомогою якого провайдери надають свої послуги.

Глобальна мережа має магістральні ЦД, які підключені до маршрутизаторів магістралі, а також периферійні ЦД, які розташовані у мережах доступу у безпосередній близькості від користувачів. Наприклад, керування об’єктами Інтернету речей, яке відбувається в реальному масштабі часу потребує обміну даними з мінімальними затримками. Таке керування досягається за рахунок розподілу в *мережах доступу* обчислювальних ресурсів провайдера між крупними ЦД, які розташовані на магістральній мережі і невеликими ЦД периферійних мереж. Таке розподілене керування має назву периферійні обчислення (Edge Computing).

Мережі доступу для об’єктів Інтернету речей є дротовими і бездротовими. Бездротові призначені для зв’язку з такими мобільними об’єктами, як ро́боти, автомобілі. Часто бездротовий зв’язок кращий для певних приміщень і тоді використовуються мережі технології Wi-Fi або радіомережі мобільної мережі 5G, технологія якої розроблена і для послуг Інтернету речей.

5.3 Послуги глобальних мереж

Послуги глобальних мереж – це комплекс телекомунікаційних послуг, що дозволяють об'єднувати локальні мережі та окремі комп'ютери, розташовані на великих відстанях, в єдину систему. Такі послуги забезпечують передачу даних між різними географічними точками, що необхідно для функціонування розподілених компаній, міжнародних організацій та інших суб'єктів, які потребують зв'язку на великі відстані. Послуги, які надаються операторами зв’язку на підставі технологій канального та мережевого рівнів є: *доступ* у Інтернет та *зв'язування* (об’єднування) територіально рознесених локальних мереж.

Завдяки тому, що IP-мережі операторів зв’язку об’єднані в глобальну мережу Інтернет, користувач цієї послуги має можливість отримувати доступ до всіх вузлів Інтернет і до всіх його послуг. Відповідно до принципу роботи IP-мереж, навіть тоді, коли необхідний користувачу вузол знаходиться у мережі, що не належить його провайдерові послуг, пакети клієнта мають можливість достатися цього вузла через мережі інших операторів. Послуга доступу у Інтернет є транспортною, тобто сама по собі вона не надає ніяких прикладних сервісів (веб-сервіс, IP-телефонія). Ці прикладні сервіси працюють поверх служби доступу в Інтернет і для самого транспорту Інтернету вони прозорі.

Об'єднання локальних мереж клієнтів може виконуватися як на IP-рівні, так і на канальному рівні. Пріоритетом у виборі рівня об’єднання мереж є тип адресації, що використовується для даної операції. Якщо мережі об’єднуються на рівні IP-адрес, то це об’єднання на IP-рівні. Якщо ж це об’єднання виконується без урахування IP-адрес вузлів мережі, а з урахуванням адрес канального рівня, то це об’єднання на канальному рівні. В обох випадках мережі, що об’єднуються, обмінюються IP-пакетами, які інкапсульовані у кадри канального рівня, однак при наданні послуги канального рівня ці пакети не беруться до уваги.

На IP-рівні об’єднання локальних мереж може бути виконано як додаткова послуга на підставі послуги доступу до Інтернет. Для цього оператор повинен надати клієнту пул публічних IP-адрес для призначення їх вузлам локальної мережі та забезпечити маршрутизацію цих адрес у Інтернеті.

Послуги віртуальних приватних мереж (VPN) є важливим типом послуги об’єднання локальних мереж, тому що VPN має деякі критичні для клієнта властивості, які створюють ефект ізольованості клієнтських мереж. Послуга може надаватися як на IP-рівні, так і на канальному рівні.

Під час об’єднання мереж клієнтів на канальному рівні ці мережі здійснюють обмін трафіком через мережу канального рівня провайдера послуги – тобто через мережу MPLS або Carrier Ethernet. Маршрутизатори провайдера послуг в цій операції участі не приймають, трафік клієнтських мереж до них не заходить.

Основні послуги глобальних мереж становлять:

– оренда каналів зв'язку;

– віртуальні приватні мережі, що дозволяють створювати захищені канали передачі даних через загальнодоступні мережі, такі як Інтернет;

– послуги інтернет-провайдерів (ISP);

– хмарні послуги (Cloud Services), що надаються через інтернет для обробки та зберігання даних;

– телекомунікаційні послуги (Telecommunication Services), що забезпечують зв'язок між різними об'єктами (передавання голосу, даних, відео).

ЗАПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ ДО РОЗДІЛУ 2

1. Що таке локальна мережа (LAN), її основні характеристики?
2. Як працює протокол Ethernet у локальних мережах?
3. Які стандарти і документи регламентують роботу локальних мереж Ethernet?
4. Що таке колізія в локальній мережі і як вона виникає?
5. В чому різниця між методами доступу CSMA/CD та CSMA/CA.
6. Що таке мультиплексування:
    a. технологія шифрування
    b. метод об’єднання кількох сигналів в один канал
    c. тип маршрутизатора
    d. вид протоколу передачі
7. Поясніть принцип роботи протоколу Spanning Tree Protocol (STP).
8. Як IP-адреса присвоюється пристроям у локальній мережі?
9. Що таке DHCP, поясніть принцип роботи, яку роль він виконує?
10. Поясніть поняття підмережі (subnet) і маски підмережі.
11. Основні стандарти бездротових локальних мереж (IEEE 802.11).
12. Що таке бездротова локальна мережа (WLAN)? Поясніть різницю між режимами роботи бездротової мережі: інфраструктурним і ad-hoc.
13. Які основні проблеми можуть виникнути при проєктуванні і експлуатації локальної мережі?
14. Що розуміється під поняттям «технології локальних мереж»? Які основні технології фізичного рівня використовуються в локальних мережах?
15. Поясніть принцип роботи технології Ethernet. Чим різняться між собою основні стандарти Ethernet?
16. Які типи кабелів підтримує технологія Ethernet?
17. Які переваги використання VLAN у локальних мережах? Як реалізується

VLAN на апаратному рівні?

18. Як працює протокол Rapid Spanning Tree Protocol (RSTP)?
19. Що таке PoE (Power over Ethernet) і які переваги ця технологія дає?
20. Що таке QoS? Як реалізується якість обслуговування у мережах?
21. Що таке глобальна мережа (WAN) і які її основні характеристики?
22. Які основні відмінності між локальними (LAN) і глобальними мережами (WAN)?
23. Які сучасні технології використовуються для побудови глобальних мереж?
24. Що таке комутація каналів і комутація пакетів? Наведіть приклади.
25. Технологія MPLS, де вона використовується?
26. Що таке VPN, технології реалізації в глобальних мережах.
27. Які протоколи маршрутизації використовуються у глобальних мережах?
28. Що таке широкомовлення (broadcast) і мультикастинг (multicast) у контексті мереж?
29. Які типи каналів передачі даних використовуються в глобальних мережах?
30. Що таке протокол PPP і де він використовується?
31. Які особливості роботи мобільних глобальних мереж (3G, 4G, 5G)?
32. Що таке CDN, її роль у глобальних мережах?
33. Що таке тунелювання і які його типи існують у глобальних мережах?
34. Сучасні тенденції розвитку технологій глобальних мереж.
35. Які рівні моделі OSI задіяні при побудові глобальних мереж?
36. Що таке ієрархічна структура глобальної мережі? Поясніть роль провайдерів послуг Інтернет (ISP) Що таке точка обміну трафіком (IXP)?
37. Що таке транзитний і піринговий трафік?
38. Що таке автономна система (AS) у контексті глобальних мереж?
39. Які технології комутації використовуються у глобальних мережах?
40. Які протоколи внутрішньої і зовнішньої маршрутизації існують?

РОЗДІЛ 3. МЕРЕЖЕВІ СЛУЖБИ ТА БЕЗПЕКА МЕРЕЖ

Тема 6. Служби в глобальних мережах

Служби в глобальних мережах – це сервіси або функціональні можливості, які надаються користувачам через глобальні комп'ютерні мережі, найчастіше через Інтернет. Ці служби забезпечують обмін інформацією, зберігання даних, комунікацію, обчислення. Вони є невід'ємною частиною глобального інформаційного середовища, формуючи сучасний цифровий простір.

Мережна служба надає користувачам мережі певний набір послуг. Ці послуги іноді називають мережевим сервісом. Зазначені терміни іноді використовуються як синоніми, але в деяких випадках відмінність у цих значеннях суттєва. Службою є мережевий компонент, який реалізує певний набір послуг, а сервісом є опис набору послуг, який надається цією службою.

Служби Інтернету – це системи, які надають послуги його користувачам. До них належать: всесвітня павутина (WWW); поштова служба, списки розсилки; служба передавання файлів; служба новин; служба інтерактивного спілкування, телеконференції, форуми, месенджери, спілкування у реальному часі; хмарні сховища даних; Інтернет розумних речей; служби пошуку інформації; методи забезпечення безпеки в Інтернеті.

Веб-служби – це незалежні, самодостатні, модульні програми з можливістю публікації, пошуку та виклику по мережі Інтернет. Доступ до веб-сторінок здійснюється через браузери, використовуючи протокол HTTP/HTTPS (приклад: сайти новин, блоги, онлайн-магазини).

Всесвітнє павутиння (World Wide Web)

Всесвітнє павути́ння або *Всесвітня мере́жа* (*World Wide Web*, *WWW*, всемере́жжя, веб) – найбільше всесвітнє багатомовне сховище інформації в електронному вигляді: десятки мільйонів пов'язаних між собою документів, що

розташовані на комп'ютерах, розміщених на всій земній кулі, служба мережі Інтернет, яка дозволяє отримувати доступ до інформації незалежно від місця її розташування.

WWW – інформаційна система, яка може бути позначена як: гіпертекстова, гіпермедійна, розподілена, інтегруюча, глобальна. Користувачі автоматично переходять від однієї бази даних (сайту) до іншої за допомогою *гіперпосилань*. Кількість серверів WWW постійно зростає, а швидкість росту WWW навіть більша ніж у самої мережі Інтернет. WWW є найрозвиненішою технологією Інтернет, яка давно вже стала масовою.

WWW працює за принципом клієнт-сервер: існує велика кількість серверів, які за запитом клієнта надають йому гіпермедійний документ, в якому кожен елемент може бути посиланням на інший документ чи його частину. Посилання в WWW організовані так, що кожний інформаційний ресурс в глобальній мережі Інтернет однозначно адресується, а надісланий сервером документ може посилатися на інші документи цього ж сервера, чи на документи інших комп'ютерів Інтернет. Більшість програм-клієнтів WWW (браузери) не просто розуміють такі посилання, а є додатково програмами-клієнтами відповідних сервісів: FTP, новин мережі, електронної пошти тощо.

WWW є сервісом прямого доступу, який потребує повноцінного підключення до Інтернет і вимагає швидких ліній зв'язку для пересилання документів, що містять багато графічної або іншої нетекстової інформації. Коли швидкості нижчі, втрачається частина переваг, які зробили WWW таким популярним.

Складові WWW:

– *HTML* (*hyper text markup language, мова розмітки гіпертексту*): формат гіпермедійних документів, які використовують в WWW для представлення інформації.

– *URL* (*uniform resource locator, універсальний вказівник на ресурс*). Таку назву носять словесні посилання на будь-які інформаційні ресурси Internet. Доступ до ресурсів Інтернет можна отримувати і за *IP*-адресою певного комп'ютера.

– *HTTP* (*hypertext transfer protocol, протокол передачі гіпертексту*): протокол, за яким взаємодіють клієнт та сервер WWW для передавання гіпермедійного документа клієнту.

– *HTTPS* є безпечною версією HTTP, де всі дані передаються через зашифроване з'єднання за допомогою протоколів SSL/TLS, що забезпечує захист переданих даних.

SSL (Secure Sockets Layer, рівень захищених сокетів): криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером. SSL спочатку розроблений компанією *Netscape Communications*. Згодом на підставі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC 2246, що отримав ім'я TLS.

Служба обміну файлами

Служба передавання файлів (*служба обміну файлами*) зберігає файли на спеціальних FTP-серверах та, за потребою, копіює їх на комп'ютери користувачів. Служба дозволяє пересилати мережею файли будь-якого типу. FTP сервер відповідає за аутентифікацію клієнтів (приклад: WeTransfer, Google Drive, FTP-сервери).

FTP (File Transfer Protocol, протокол передавання файлів) – стандартний мережевий протокол прикладного рівня, призначений для пересилання файлів між клієнтом та сервером в комп'ютерній мережі.

Клієнт та сервер створюють окремі канали для передачі даних та обміну командами. Можлива автентифікація клієнтів із використанням відкритого

тексту, зазвичай це ім'я користувача (логін) та пароль. Також сервер може бути налаштований для роботи без автентифікації користувачів (так звані «анонімні сеанси»).

Для захисту даних (а також процесу автентифікації) використовують побудований на основі SSL/TLS варіант FTPS, або розширення протоколу SSH – *SSH File Transfer Protocol* (SFTP).

SSH (Secure Shell, «безпечна оболонка») – мережевий протокол прикладного рівня, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів). IP-тунель – це інтернет-протокол (IP) мережі, канал зв'язку між двома мережами. В IP tunneling кожен IP-пакет, в тому числі і адресна інформація джерела і призначення IP-мережі, інкапсулюється в формат пакета, рідного для транзитної мережі.

Найбільш поширене застосування FTP це робота з файлами хостингу. Використання FTP є найпростішим методом передачі файлів на сервер, гарною альтернативою звичним носіям інформації, забезпечує швидку та зручну передачу файлів між користувачами глобальної мережі, файли на FTP-сервері доступні користувачам з різних куточків світу (послуга «FTP хостинг»).

FTP сервер підтримує передачу файлів у двох режимах:

– текстовий (ASCII): використовується для передачі текстових даних (HTML, php скриптів, perl скриптів), а також *css* та *JS* файлів;

– бінарний (BINARY): зображення та бінарні файли передаються в цьому режимі.

Сучасні FTP клієнти автоматично визначають необхідний режим для завантаження файлів.

Для того щоб підключитися до FTP необхідні наступні дані: ім'я серверу (хост), логін, пароль, порт FTP (стандартно 21).

FTP сервер, що не вимагає авторизації, називається анонімним FTP сервером (anonymous FTP).

За замовчуванням обмін даними між клієнтом та сервером здійснюється у відкритому вигляді, що може призвести до несанкціонованого доступу. Щоб уникнути подібного, можна скористатися додатковими протоколами FTPS.

FTPS – протокол прикладного рівня, створений як розширення FTP протоколу. Він призначений для встановлення захищеного з'єднання за допомогою TLS (всі команди та дані, що передаються по каналу зв'язку, шифруються).

Хмарні служби (Cloud services)

Концепцією хмарних обчислень є зберігання, обробка даних і доступ до них через Інтернет (приклади: Google Drive, Dropbox, Microsoft OneDrive).

Згідно з документом IEEE P2301 хмарні обчислення є парадигмою, в рамках якої інформація постійно зберігається на серверах у мережі Інтернет і тимчасово кешується на клієнтській стороні, наприклад на персональних комп'ютерах, ігрових приставках, ноутбуках, смартфонах тощо. Хмарні обчислення (cloud computing) дозволяють розвантажити комп’ютер користувача і перенести обчислення на віддалені комп’ютери, пов’язані з користувачем через мережу.

Хмарні технології (Cloud Technology) – це технології надання комп'ютерних ресурсів як онлайн-послуги через Інтернет. Користувачі можуть отримувати доступ до обчислювальних потужностей, зберігання даних і програмного забезпечення без необхідності купувати та обслуговувати власну інфраструктуру. Один з найбільших плюсів хмарних технологій – відсутність необхідності в купівлі, налаштуванні та підтримці фізичного серверного обладнання, оскільки це обов'язок хмарного провайдера, який надає послугу.

Хмарні технології працюють на віддалених серверах, які розташовані в дата-центрах (ЦОД, центрах обробки даних). При зверненні користувача до хмарного сервісу запит надсилається на відповідний сервер. Цей сервер виконує запит користувача і повертає результат.

Типи хмарних технологій

Хмарні технології поділяються на типи IaaS, SaaS, PaaS.

Інфраструктура як послуга (IaaS) – це надання хмарним провайдером обчислювальних ресурсів, таких як віртуальні сервери, мережі та сховища у вигляді онлайн-сервісів. Клієнти можуть використовувати IaaS-ресурси для запуску своїх власних програм, мереж та інших систем.

Програмне забезпечення як послуга (SaaS) – це надання хмарним провайдером програмного забезпечення як онлайн-сервісу. Користувачі можуть використовувати програмне забезпечення без необхідності купівлі, встановлення та підтримки на своєму власному комп'ютері.

Платформа як послуга (PaaS) – це надання платформи для розробки та розгортання програм. Користувачі можуть використовувати PaaS-платформи для створення та запуску власних програм без необхідності володіння та управління інфраструктурою.

За способом реалізації хмарні середовища розподіляються на *публічні*, *приватні* та *гібридні* хмари (рис.47).

Публічна хмара: дає можливість замовлення послуг та одночасного доступу до IT-інфраструктури хмарного провайдера будь-яких користувачів. Публічна хмара перебуває в юрисдикції постачальника хмарних послуг, управління хмарою та обслуговування здійснюється її власником.

Приватна хмара: контроль, обслуговування та експлуатація хмари можливі лише одним абонентом. Така хмарна інфраструктура призначена для

використання виключно однією організацією, що включає декілька користувачів (наприклад, підрозділів). Приватна хмара може перебувати у власності, керуванні та експлуатації як самої організації, так і третьої сторони (чи деякої їх комбінації). Така хмара може фізично знаходитись як у, так і поза юрисдикцією власника.

Рисунок 47 – Схема хмарних технологій

Гібридна хмара: це інфраструктура, яка створена на основі публічної та приватної хмари, коли в одну мережу об'єднані як приватні, так і публічні хмарні сервіси. Фізичне обладнання всієї IT-інфраструктури знаходиться у користувача або в дата-центрі, віртуальна частина знаходиться у хмарного провайдера. Для кінцевого користувача передача даних між хмарами відбувається прозоро – він бачить це як єдину мережу. Необхідність в гібридній хмарі виникає тоді, коли власних ресурсів компанії недостатньо для забезпечення необхідної продуктивності, але повністю відмовлятися від приватної хмари не доречно або це неможливо з інших причин (наприклад, за вимогами безпеки).

Переваги хмарних технологій: дозвіл користувачам працювати з хмарними платформами (документи, презентації та інші файли) незалежно від місцезнаходження; економія витрат на купівлю апаратного та програмного забезпечення, витратах на апгрейд та підтримку фізичного обладнання; зберігання великих обсягів даних; гнучкість та масштабованість, доступність.

Хмарні технології доступні з будь-якої точки світу через Інтернет, безпека захисту даних на різних рівнях.

Недоліки хмарних технологій: необхідна наявність якісного підключення до Інтернету; залежність безпеки даних у хмарі від провайдера, що надає послугу; відсутність повного контролю за даними користувача, які розміщені на онлайн-майданчиках; відсутність фізичного доступу до даних, розміщених у хмарі провайдера послуги.

Приклади хмарних технологій:

– хмарні платформи для спільної роботи: Google Docs, Microsoft Office 365 та Slack;

– хмарні сховища даних: Google Drive, iCloud, Dropbox;

– хмарні програми: Gmail, Google Maps, YouTube;

– обчислення у хмарі: Amazon Web Services, Microsoft Azure (дозволяють компаніям орендувати обчислювальні потужності, сховища та інші ресурси).

Галузі використовуються хмарних технологій дуже різноманітні – освіта, бізнес-напрямок, розваги, державні установи тощо.

Бізнес-напрямок: підвищення ефективності організації виробничого процесу (можливість для спільної роботи співробітників незалежно від їхнього місцезнаходження), зниження витрат та забезпечення безпеки.

Освіта: надання доступу до навчальних матеріалів/ресурсів, проведення онлайн-курсів/занять/семінарів в режимі реального часу.

Розваги: доступ до фільмів, музики, ігор та інших розваг (наприклад, такі багатопотокові сервіси, такі як Netflix, Spotify використовують хмарні технології для зберігання та доставки контенту користувачам).

Державні установи: хмарні технології використовуються урядами для надання державних послуг.

Електронна пошта (Email)

Електронна пошта (email, e-mail, electronic mail) – технологія та служба з пересилання та отримання електронних повідомлень (званих «листи», «електронні листи» або «повідомлення») між користувачами комп'ютерної мережі. Електронні повідомлення надсилаються за допомогою програм та веб-браузерів, які разом називаються поштовими клієнтами. Окремі проходять через кілька серверів, перш ніж потрапити на поштовий сервер одержувача.

Поява електронної пошти відноситься до 1965 року, коли співробітники Массачусетського технологічного інституту Ноель Морріс та Том Ван Влек написали програму *mail* для операційної системи CTSS (Compatible Time-Sharing System), встановлену на комп'ютері IBM 7090/7094. У 1971 року Рей Томлінсон розробив першу програму електронної пошти для ARPANET яка вперше на адресах використовувала символ @.

Протокол надсилання

Загальноприйнятим у світі протоколом обміну електронною поштою є *SMTP* (Simple Mail Transfer Protocol, простий протокол *передачі* пошти). У своїй реалізації він використовує DNS для визначення правил пересилання пошти. Взаємодія між серверами в рамках однієї поштової системи може бути як підпорядкована загальним правилам (використання DNS і правил маршрутизації пошти за допомогою протоколу SMTP), так і дотримуватися власних правил компанії (програмного забезпечення, що використовується).

Протоколи отримання

POP3 (Post Office Protocol 3) – протокол, який використовується для отримання електронної пошти з поштового сервера клієнтом. Він дозволяє завантажувати повідомлення на пристрій користувача і (за замовчанням), видаляти їх із сервера. Тобто, після завантаження пошти на комп'ютер вона

більше не доступна на сервері (якщо не встановлено спеціальних налаштувань) У концепції поштового сховища пошта на сервері зберігається тимчасово, в обмеженому обсязі, а користувач періодично звертається до скриньки та «забирає» листи (тобто поштовий клієнт завантажує копію листа до себе та видаляє оригінал з поштової скриньки).

IMAP (Internet Message Access Protocol) – це протокол доступу до електронної пошти, який дозволяє користувачам отримувати доступ до своїх листів, що зберігаються на сервері, та керувати ними безпосередньо на сервері. На відміну від POP3, IMAP забезпечує можливість одночасної роботи з поштою з кількох пристроїв та синхронізацію змін між ними, а також можливість пошуку за ключовими словами без завантаження листів на пристрій. Концепція поштового терміналу передбачає, що вся кореспонденція, пов'язана з поштовою скринькою, зберігається на сервері, а користувач звертається до сховища (поштової скринькои) для перегляду кореспонденції (як нової, так і архіву) і написання нових листів (включаючи відповіді на інші листи).

З точки зору продуктивності сервера IMAP більш вимогливий до ресурсів, ніж POP3, так як вся робота з обробки пошти (така як пошук) лягає на плечі сервера, POP3 тільки передає пошту клієнту. З точки зору пропускної здатності каналу IMAP краще: POP3 передає «тіло» всіх листів повністю, тоді як IMAP може передавати окремі частини повідомлень, наприклад тільки текстову, а решту – на запит.

Структура листа

Електронний лист складається із заголовків (headers), які містять службові відомості про відправника та отримувача листа, шлях проходження листа (слугують, умовно кажучи, *конвертом*), та власне вміст самого листа (body, тіло).

Для шифрування пошти застосовуються два основні стандарти: S/MIME (використовує інфраструктуру відкритих ключів) і OpenPGP (використовує сертифікати зі схемою довіри, що групується навколо користувача). Ці стандарти дозволяють забезпечити три види захисту: захист від зміни, невідкликаний підпис (авторство) та конфіденційність (шифрування). Стандарт S/MIME починаючи з третьої версії дозволяє використовувати захищене квитування (при якому квитанція про отримання листа може бути успішно згенерована тільки в тому випадку, коли лист дійшов до одержувача в незмінному вигляді).

Розсилка електронної пошти – засіб масової комунікації, групового спілкування та реклами, один із інструментів Інтернет-маркетингу. Полягає в автоматизованій розсилці повідомлень електронної пошти групі адресатів за заздалегідь складеним списком. Розсилка може бути у формі поштових розсилок (листи, буклети, каталоги, листівки, запрошення), електронних листів або SMS.

Розсилки розрізняють за типом, а саме: список розсилки, групова адреса та інформаційне та/або рекламне розсилання (спам).

Служби миттєвого обміну повідомленнями

Служби для миттєвого обміну повідомленнями є системами, які працюють в режимі реального часу. Ці інтернет-сервіси дозволяють користувачам обмінюватися текстовими повідомленнями, зображеннями, відео, файлами, голосовими повідомленнями та здійснювати відеодзвінки.

Основними характеристиками таких служб є:

– швидкість (повідомлення доставляються майже миттєво);

– двостороннє спілкування (підтримується діалог або групове спілкування);

– мультимедійність (можна надсилати фото, відео, документи);

– інтерактивність (реакції, стікери, голосові повідомлення, дзвінки);

– підключення через Інтернет (працюють через мобільні мережі або Wi-Fi);

– підтримка кількох платформ (мобільні додатки, веб-версії, десктопні клієнти).

До розповсюджених служб миттєвого обміну повідомленнями належать: WhatsApp, Viber, Facebook Messenger, Signal, WeChat.

Використання цих служб різноманітне – особисте спілкування (друзі, родина); робоча комунікація (команди, віддалена робота); клієнтська підтримка (чат-боти, звернення в компанії); освіта (онлайн-групи, повідомлення викладачів).

Служби миттєвого обміну повідомленнями – це важливий тип служби глобальної мережі, який забезпечує швидке й зручне спілкування між користувачами по всьому світу.

Відеоконференції та VoIP

Відеоконференції та VoIP (Voice over Internet Protocol) – це служби глобальної мережі, що забезпечують голосовий та відеозв’язок через Інтернет в режимі реального часу.

VoIP (Voice over IP) – це технологія, яка дозволяє передавати голосові дзвінки через інтернет або IP-мережі, замість традиційної телефонної мережі: Skype, Viber, WhatsApp (дзвінки).

Відеоконференції – це розширена версія VoIP, яка включає не лише передачу голосу, а й відео, чат, обмін файлами, спільний доступ до екрана, дозволяє проводити онлайн-зустрічі у відео та аудіо форматі з кількома учасниками одночасно. Використовується для: онлайн-навчання, робочих нарад, вебінарів, дистанційного спілкування (Zoom, Google Meet, Microsoft Teams, Skype)

Основні протоколи, які використовуються в VoIP та відеоконференціях:

– *SIP (Session Initiation Protocol)*: протокол для ініціації, підтримки та завершення мультимедійних сесій (дзвінків, відеоконференцій). Відповідає за встановлення зв'язку між учасниками (дзвінок, відеодзвінок). SIP працює на рівні сигналізації – керує «дзвінком», але не передає аудіо чи відео.

– *RTP (Real-time Transport Protocol)*: основний протокол для передачі медіаданих (аудіо та відео в реальному часі). Працює разом із SIP: SIP встановлює сесію, а RTP передає самі аудіо та відео пакети. Підтримує синхронізацію потоків і маркування часу для коректного відтворення.

– *RTCP (Real-time Transport Control Protocol)*: допоміжний протокол для RTP. Використовується для контролю якості передачі, звітування про втрати пакетів, затримки тощо.

– *H.323*: старіший комплексний протокол для VoIP і відеоконференцій. Включає різні компоненти для сигналізації, передачі аудіо, відео і керування викликами. Використовується деякими корпоративними системами і обладнанням.

– *WebRTC (Web Real-Time Communication)*: технологія і набір API для організації VoIP і відеоконференцій безпосередньо у веб-браузері без додаткових плагінів. Застосовується у сучасних додатках (Google Meet, Discord, Zoom) з використанням протоколів:

- SCTP (Stream Control Transmission Protocol) через DTLS (Datagram Transport Layer Security) для передачі даних;
- SRTP (Secure RTP) для безпечної передачі аудіо та відео.

– *MGCP (Media Gateway Control Protocol)* та *Megaco/H.248*: протоколи для контролю медіашлюзів (пристроїв, що з'єднують традиційну телефонну мережу з IP). Використовуються у великих VoIP-мережах та операторах.

Перевагами VoIP є більш дешевше (порівняно з мобільними дзвінками) спілкування; можливість дзвонити з будь-якої точки світу, де є Інтернет; використання функцій відеодзвінків, чатів, передачу файлів.

Соціальні мережі

Соціальні мережі мають величезне значення в сучасному світі. Існують спеціалізовані служби, які допомагають користувачам та організаціям ефективно використовувати ці платформи для досягнення своїх цілей.

– *Керування акаунтами та контентом*

Hootsuite, Buffer, Sprout Social: платформи, які дозволяють автоматизувати публікації, відслідковувати взаємодії з підписниками, аналізувати ефективність контенту і керувати кількома акаунтами одночасно.

Canva: інструмент, що дозволяє створювати графічний контент, який потім можна використовувати в публікаціях на платформах як Instagram, Facebook, Twitter.

– *Аналіз та моніторинг соціальних медіа*

Brandwatch, Mention: інструменти для моніторингу певного бренду, слідкування за ключовими словами та аналітики соціальних медіа (дозволяють брендам відслідковувати, як їх сприймають у мережах, на які пости варто звернути увагу, які тенденції з’являються).

Socialbakers: платформа для вимірювання ефективності кампаній в соціальних мережах, порівняння з конкурентами та моніторинг соціальних медіа на основі важливих метрик.

– *Реклама в соціальних мережах*

Facebook Ads Manager, Twitter Ads, LinkedIn Campaign Manager: платформи, які дозволяють створювати та оптимізувати рекламні кампанії в

соціальних мережах (надають розширені інструменти для таргетингу, визначення бюджету, аналізу результатів).

Google Ads: інструмент, який дозволяє інтегрувати рекламу на YouTube і інших платформах, має певні перехресні ефекти з соціальними мережами.

– *Інфлюенс-маркетинг*

Upfluence, Influencity: сервіси, які допомагають знаходити інфлюенсерів для співпраці, керувати партнерськими програмами, вимірювати ефективність кампаній за участю блогерів та інфлюенсерів.

Інфлюенсер – людина, думка якої має значення для певної аудиторії.

– *Автоматизація чатів та взаємодії*

ManyChat, Chatfuel: чат-боти для автоматизації спілкування з користувачами у соціальних мережах. Допомагають швидко реагувати на питання, проводити опитування, збирати зворотний зв’язок тощо.

– *Менеджмент репутації*

Reputology, Yotpo: платформи для управління онлайн-репутацією, які дозволяють збирати відгуки, працювати з негативними коментарями та зберігати позитивний імідж у соціальних мережах.

– *Збір і аналіз зворотного зв'язку*

SurveyMonkey, Typeform: інструменти для створення опитувань, анкет, що дозволяють отримувати зворотний зв'язок від користувачів соціальних мереж. Вони можуть бути використані для визначення рівня задоволення, збору ідей для контенту або кампаній.

– *Робота з відео-контентом*

InShot, Adobe Premiere Rush: програми для створення і редагування відео, які можна безпосередньо публікувати в соціальних мережах, таких як Instagram, YouTube, TikTok.

– *Краудфандинг і просування проектів через соцмережі*

Kickstarter, GoFundMe: сервіси, які дозволяють запускати кампанії на соціальних платформах і залучати фінансування від спільноти.

– *Інструменти для планування контенту*

CoSchedule, Trello, Notion: платформи, що допомагають організувати та планувати пости, визначати стратегії для контенту, координувати роботу команди.

Означені служби допомагають бізнесам, брендам і окремим користувачам ефективно використовувати соціальні мережі для досягнення конкретних цілей, таких як залучення нової аудиторії, підвищення лояльності, збільшення продажів або покращення взаємодії з користувачами.

Пошукові системи

Пошукові системи – це сервіси, які допомагають користувачам знаходити потрібну інформацію в інтернеті. Вони *збирають*, *індексують* і *обробляють* величезну кількість веб-сторінок, щоб у відповідь на запит користувача швидко показати релевантні результати.

Список *глобальних* пошукових систем, які використовуються в Інтернеті:

– *Google*: найпопулярніша і найвідоміша пошукова система у світі.

– *Bing*: пошукова система від Microsoft.

– Yahoo! Search: раніше популярна, зараз часто використовує результати Bing.

– *DuckDuckGo*: пошуковик, який фокусується на конфіденційності користувачів.

– *Baidu*: найбільша пошукова система в Китаї.

– *Ecosia*: пошукова система, яка використовує прибуток для посадки дерев.

– *Startpage*: пошуковик, який також орієнтований на приватність користувачів.

Спеціалізовані пошукові системи:

– *WolframAlpha*: пошукова система для наукових та обчислювальних запитів.

– *Google Scholar*: пошук наукових публікацій і досліджень.

– *Archive.org* (Wayback Machine): пошук історичних версій веб-сторінок.

Робота пошукової системи розподілена на такі етапи:

Індексація: пошукові ро́боти (краулери) обходять веб-сторінки, збирають їхній контент. *Краулінг* (сканування веб-сторінок) відбувається через HTTP-запити, які виконують пошукові ро́боти (Googlebot, Bingbot тощо).

Збереження інформації: всі зібрані дані зберігаються в базах даних пошукової системи.

Обробка запитів: коли користувач вводить запит, система шукає відповідні документи в *індексі*.

Вивід результатів: результати відображаються у вигляді списку посилань з короткими описами.

Основні протоколи, що використовуються пошуковими системами

HTTP/HTTPS – основний протокол для передачі даних в Інтернеті. Пошукові ро́боти (боти) використовують HTTP або HTTPS для доступу до веб-сторінок.

DNS (Domain Name System) – протокол, який переводить доменні імена у IP-адреси. Пошукові ро́боти і користувачі використовують DNS для доступу до потрібних сайтів.

Robots.txt – текстовий файл, а не протокол, який розміщують на сайті. Пошукові ро́боти звертаються до файлу robots.txt, щоб дізнатися, які сторінки можна або не можна індексувати. Файл керує поведінкою краулерів і допомагає власникам сайтів контролювати доступ до їхніх сторінок.

Sitemaps (карти сайту) XML-файли, які веб-майстри створюють для покращення індексації, вказують пошуковим системам, які сторінки є на сайті, як

часто вони оновлюються. Пошукові системи отримують і читають ці файли через HTTP/HTTPS.

API (Application Programming Interface). Деякі пошукові системи (наприклад, Google Search API) надають спеціальні інтерфейси для доступу до результатів пошуку або іншої інформації. API працюють за різними протоколами, але найчастіше через HTTPS.

Пошукові системи і веб-браузери не одне й теж саме. Веб-браузери – це програмне забезпечення, яке дозволяє користувачам переглядати веб-сайти в інтернеті. Браузер отримує веб-сторінки через інтернет-протоколи (найчастіше HTTP/HTTPS), відображає їх і забезпечує взаємодію користувача з сайтом.

Основні функції браузера:

1. *Відображення веб-сторінок*: браузер завантажує HTML, CSS, JavaScript та інші файли, і рендерить (малює) сторінку для користувача.

2. *Введення і відправка пошукових запитів*. Більшість браузерів має адресний рядок (omnibox), куди можна вводити як URL сайту, так і пошукові запити (за замовчуванням браузер відправляє пошукові запити до обраної пошукової системи).

3. *Керування вкладками і вікнами*: браузери дозволяють відкривати багато вкладок одночасно, щоб працювати з кількома сайтами.

4. *Збереження паролів і автозаповнення форм*: для зручності користувачів браузери можуть зберігати паролі та автоматично заповнювати поля.

5. *Розширення (доповнення)*: можливість встановлювати додаткові плагіни і розширення, які додають функції (наприклад, блокування реклами, менеджери паролів, VPN).

6. *Захист і безпека*: сучасні браузери мають вбудовані засоби захисту від шкідливих сайтів, підтримують безпечне з’єднання HTTPS, інформують про фішингові ресурси.

Перелік популярних браузерів: Google Chrome, Opera, Mozilla Firefox, Microsoft Edge, Safari, Brave.

Служби електронної комерції

Служби електронної комерції (eCommerce services) – це широкий спектр послуг, які підтримують бізнес-процеси, спрямовані на продаж товарів і послуг через Інтернет (Amazon, eBay, Rozetka). Вони охоплюють аспекти від технічної підтримки до маркетингу, доставки, платіжних систем і обробки даних. Основні категорій таких служб:

1. *Платформи електронної комерції* – це сервіси, які надають інструменти для створення і керування онлайн-магазинами. Платформи для створення інтернет-магазинів – *Shopify*, *Magento*, *BigCommerce*; *WooCommerce*: плагін для WordPress.

2. *Платежі та обробка транзакцій*. Системи для обробки платежів і забезпечення безпеки транзакцій: PayPal, Stripe, Apple Pay/Google Pay.

3. *Логістика та доставка* – це сервіси, які допомагають бізнесам забезпечити доставку товарів покупцям. Вони можуть включати: служби доставки, інструменти для моніторингу доставок, мультимодальні платформи для доставки.

4. *Маркетинг і просування* застосовують інструменти для просування продуктів і брендів:

– SEO (Search Engine Optimization): оптимізація вебсайтів для підвищення видимості в пошукових системах;

– PPC-реклама (Pay-per-click): реклама через Google Ads, Facebook Ads;

– Email-маркетинг: сервіси для створення і розсилки маркетингових листів (наприклад, MailChimp).

5. *Аналітика та звітність* передбачають системи для збору та аналізу даних про продажі, поведінку клієнтів: Google Analytics, Hotjar: Kissmetrics.

6. *Технічна підтримка та обслуговування* – це послуги, які підтримують технічну стабільність і безпеку сайту: *хостинг* (сервіси, які надають місце для розміщення вебсайтів), *резервне копіювання* та *відновлення* (інструменти для автоматичного збереження даних і відновлення сайту у разі несправності); *захист від кібератак* (сервіси, що допомагають забезпечити безпеку транзакцій та захистити сайт від хакерських атак).

7. *Мобільні додатки для електронної комерції* – це сервіси, які допомагають створювати та підтримувати мобільні додатки для продажу: BuildFire, Appy Pie.

8. *Клієнтська підтримка* передбачає інструменти для взаємодії з покупцями, надання консультацій та обробки запитів.

Протоколи служб електронної комерції:

– *HTTP/HTTPS*: передавання інформації між веб-серверами та браузерами.

– *SSL/TLS*: криптографічні протоколи, які використовуються для забезпечення безпечної передачі даних через Інтернет. Вони гарантують шифрування даних, автентифікацію та цілісність інформації, що передається. Використовуються для захисту персональних і платіжних даних покупців під час здійснення покупок в Інтернеті. Веб-сайти, які використовують SSL / TLS, мають піктограму у вигляді *замка́* в браузері, що сигналізує про наявність захищеного з'єднання.

– *FTP/SFTP*: протоколи обміну великими обсягами даних між постачальниками, підприємствами та торговими платформами.

– *XML/JSON*: формати даних, які використовуються для обміну інформацією між системами. Використовуються для структурованої передачі

даних між різними службами (для інтерфейсу між магазином і постачальником товарів або для інтеграції платіжних систем).

– *SOAP*: протокол обміну повідомленнями, який використовується для взаємодії між веб-сервісами.

– *REST*: архітектурний стиль для побудови веб-сервісів.

– *PCI DSS*: стандарт безпеки, що встановлює вимоги до зберігання, обробки та передавання платіжних карткових даних.

– *OAuth*: стандарт авторизації, який дозволяє стороннім додаткам отримувати обмежений доступ до ресурсу без потреби у передачі паролів.

– *X.509* (Цифрові сертифікати): стандарт для створення цифрових сертифікатів, які використовуються для автентифікації і шифрування в системах.

Служби потокового мультимедіа

Служби потокового мультимедіа (streaming services) – це онлайн-платформи, які надають можливість користувачам переглядати чи слухати мультимедійний контент (відео, аудіо) в реальному часі, без необхідності попереднього завантаження файлів. Ці служби широко використовуються для трансляцій фільмів, музики, подкастів, онлайн-телебачення та інших мультимедійних матеріалів.

Основні типи служб потокового мультимедіа:

– відео за запитом (Video on Demand, VOD): платформи, що дозволяють користувачам переглядати відео за запитом (Netflix, Amazon Prime Video, Disney+);

– музика за запитом (Music on Demand): платформи для прослуховування музики без завантаження файлів (Spotify, Apple Music, Tidal, Deezer);

– прямі трансляції (Live streaming): платформи для трансляції живих подій (YouTube Live, Twitch, Facebook Live, Instagram Live);

– подкасти та інші аудіоформи: платформи для прослуховування подкастів і аудіокниг (Apple Podcasts, Spotify, Google Podcasts).

Подкасти – це аудіофайли або серії аудіофайлів, що доступні через Інтернет для прослуховування або завантаження. Подкасти зазвичай записуються у форматах *MP3*, *AAC* або *OGG*

Служби потокового мультимедіа використовують різні протоколи для забезпечення ефективної та безперебійної доставки контенту. Вибір протоколу залежить від типу контенту (відео, аудіо, подкасти), платформи (мобільні пристрої, браузери) і вимог до затримок і якості. Протоколи та стандарти, які підтримують потокове мультимедіа: HTTP Live Streaming (HLS); Dynamic Adaptive Streaming over HTTP (DASH); Real-Time Messaging Protocol (RTMP); Real-Time Transport Protocol (RTP); набір стандартів WebRTC (Web Real-Time Communication); стандарт MPEG-2 Transport Stream (TS).

Інтернет речей / IoT (Internet of Things)

Інтернет речей не є окремою службою, а є технологічною системою, яка базується на службах глобальної мережі і використовує їх (зокрема Інтернет) для своєї роботи. IoT використовує наявну інфраструктуру Інтернету, щоб забезпечити нові види взаємодії між фізичними об'єктами та людьми.

Інтернет речей – це концепція, за якою фізичні пристрої (сенсори, прилади, побутова техніка, транспорт) з'єднуються з мережею (переважно з Інтернетом), щоб: збирати дані; передавати їх до хмарних або локальних серверів; отримувати команди; автоматизувати процеси. Ці пристрої використовують різні служби глобальної мережі:

– *хмарні обчислення* (cloud computing): для зберігання та обробки даних;

– *служби обміну даними*: через протоколи MQTT, HTTP, CoAP тощо;

– *служби віддаленого управління*: керування пристроями через додатки чи веб-інтерфейси;

– *служби безпеки*: автентифікація, шифрування, VPN.

IoT є технологією передачі даних між фізичними пристроями, яка передбачає збирання даних з пристроїв, які мають датчики та сенсори, передавання цієї інформації (найчастіше у хмарне сховище) на відповідне програмне забезпечення для аналізу і подальшого генеруванням зворотного сигналу (від системи до пристроїв-одержувачів), який перетворюється у певні дії.

Інфраструктура IoT для налаштування повинна мати:

– розумні датчики та сенсори, оснащені спеціальними IoT-картками;

– IoT-платформу для керування, збору та обробки даних;

– мережу для зв’язку пристроїв між собою та з платформою.

Архітектура IoT складається з сенсорів, мережі та серверів для обробки даних. Сенсори збирають інформацію з навколишнього середовища, а мережа передає ці дані до серверів, де вони обробляються та аналізуються для подальшого використання (рис. 48). Мережа може бути різною: IP, Wi-Fi, Bluetooth, LoRaWAN, 5G тощо. Протоколи MQTT та CoAP часто застосовуються для забезпечення ефективного обміну даними між пристроями з обмеженими ресурсами. Наприклад, так корегується робота оприскувачів на полях, відстежується місцезнаходження вантажівок, рівень запасів на складах тощо [21].

Для ідентифікації кожного об'єкту потрібна система унікальної ідентифікації, яка дозволяє збирати та накопичувати інформацію про певний предмет. Такий функціонал забезпечують мікросхеми RFID (Radio-Frequency IDentification). Вони здатні без власного джерела живлення передавати інформацію приладам зчитування. Кожна мікросхема має індивідуальний номер. Альтернативою до даної технології для ідентифікації об'єктів є використання

QR-коду. Для визначення точного місця знаходження речі задійснюється технологія GPS.

Рисунок 48 – Схема IoT https://translations.com.ua/internet-rechei.html

Для обробки та накопичення даних з сенсорів повинен використовуватися вбудований комп'ютер (наприклад Raspberry Pi, Intel Edison).

Для передачі даних використовуються оптимізовані та легковісні протоколи типу *MQTT* (Message Queue Telemetry Transport), регламентують процеси обміну повідомленнями між пристроями, ґрунтуються на принципах публікації і підписок де кожен пристрій (давач чи сенсор) взаємодіє з програмою на сервері (брокером). Обмін інформацією між пристроями побудовано на технологіях бездротових мереж: Wi-Fi, Bluetooth, ZigBee, 6LoWPAN (стандарт IEEE 802.15.4 управляє доступом для організації енергоефективних персональних мереж).

ZigBee – це комунікаційна технологія, заснована на протоколі IEEE 802.15.4 для реалізації низькошвидкісних бездротових приватних мереж і має такі характеристики, як знижене енергоспоживання, невелика швидкість передачі даних, низька вартість і висока пропускна здатність. Технологія ZigBee

використовується в при передаванні інформації між різними речами електронного обладнання, які знаходяться в межах короткої відстані і швидкість передачі даних не дуже висока (периферійні пристрої: миша, клавіатура і побутова електроніка), а також пристрої промислового управління (монітори, давачі і засоби автоматизації).

WiFi – це локальна бездротова технологія, яка використовує радіохвилі з частотою 2,4 ГГц або 5 ГГц, застосовується для передавання великих обсягів даних по бездротовій мережі між пристроями, але вимагає багато енергії для роботи і має невеликий рівень пропускної здатності даних. При використанні даної технології потрібно замінювати батареї у всіх пристроях на регулярній основі.

Bluetooth – це бездротова технологія, яка використовується для передачі даних в персональних мережах, дані передаються по смузі частот від 2,4 до 2,485 ГГц, працює на коротших відстанях, ніж Wi-Fi (10-100 метрів).

Інтеграція з Інтернетом передбачає використання IP-адреси. Значною мірою, майбутнє IoT не буде можливим без підтримки IPv6.

Серед провідних технологій важливу роль у розповсюдженні інтернету речей відіграють рішення PLC – технології побудови мереж передачі даних по лініях електропередач, оскільки у багатьох додатках присутній доступ до електромереж (наприклад, торгові автомати, банкомати, інтелектуальні лічильники, контролери освітлення спочатку підключені до мережі електропостачання). Стандарт 6LoWPAN, який реалізує шар IPv6 як над IEEE 802.15.4, так і над PLC, являючись відкритим протоколом, стандартизованих IETF, відзначається як особливо важливий для розвитку інтернету речей.

Тема 7. Мережева безпека.

Мережева безпека – це сукупність заходів, політик та технологій, що спрямовані на захист комп’ютерних мереж та переданої інформації від несанкціонованого доступу, змін, знищення чи витоку. Безпека інформаційної мережі включає захист *обладнання*, *програмного забезпечення*, *даних* і *персоналу*.

Комп'ютерна безпека – це сукупність методів захисту у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і їх впровадження з точки зору конфіденційності, цілісності і доступності.

Концепція розподілу ресурсів є основним критерієм у питанні захисту системних даних і даних користувача від помилкових і зловмисних дій, які можуть спричинити проблеми безпеки інформаційної системи [4]. Контрольований доступ є важливим напрямом забезпечення безпеки, поряд з іншими засобами: криптографічний захист, аудит, сегментація мережі. Найважливішими елементами керованого доступу є процедури *ідентифікації*, *автентифікації* та *авторизації*.

Ідентифікація – це присвоєння суб'єктам чи об'єктам інформаційної системи унікальних імен (ідентифікаторів). Тільки за наявності унікальних ідентифікаторів система отримує можливість розпізнавати чи оперувати суб'єктами чи об'єктами.

Ідентифікація користувачів є процедурою, що виконується при логічному вході в систему, коли користувач у відповідь на виведене на екрані запрошення надає свій ідентифікатор (ім'я), а система, звіряючись зі своїми даними, визначає, чи входить це ім'я до числа зареєстрованих (легальних) користувачів.

Аутентифікація (справжній, достовірний, що відповідає самому собі) – це процедура доказу суб'єктом/об'єктом того, що він є тим, за що/кого себе видає.

Процедура встановлення справжності (автентифікація) може застосовуватися як до користувачів, так і до інших об'єктів/суб'єктів, зокрема до даних, програм, додатків, пристроїв, документів.

Аутентифікація даних означає підтвердження їх автентичності, тобто. того, що вони надійшли у незмінному вигляді і саме від тієї людини (суб'єкта), яка оголосила про це. У процедурі аутентифікації беруть участь дві сторони:

– *автентифікований* доводить свою автентичність, пред'являючи деякий доказ (автентифікатор);

– *аутентифікуючий* перевіряє цей доказ та приймає рішення.

Аутентифікація буває односторонньою та двосторонньою (взаємною).

Одностороння автентифікація відбувається під час виконання логічного входу в захищену систему: після повідомлення системі свого ідентифікатора, користувач має пройти процедуру автентифікації, тобто довести, що саме йому належить запроваджений ним ідентифікатор (ім'я користувача). Як аутентифікатор суб'єкт/об'єкт може продемонструвати знання якогось спільного для обох сторін секрету: слова (пароля), унікального предмета (ключа), власні біохарактеристики (відбитки пальців).

Двостороння автентифікація може виконуватися, коли користувач звертається із запитом до корпоративного веб-сервера. При цьому він повинен довести йому свою легальність, але також сам повинен переконатися, що веде діалог дійсно з веб-сервером свого підприємства – сервер і клієнт повинні пройти процедуру *взаємної аутентифікації*. Це випадок двосторонньої автентифікації на рівні додатків.

При встановленні сеансу зв'язку між двома пристроями часто передбачаються процедури взаємної автентифікації пристроїв на нижчому, канальному рівні.

Авторизація – процедура контролю доступу суб'єктів (користувачів, обчислювальних процесів, пристроїв) до об'єктів (файлів, додатків, сервісів) та надання кожному з них саме тих прав, які для них визначені правилами доступу. На відміну від автентифікації, яка дозволяє розпізнати легальних та нелегальних користувачів, авторизація стосується лише легальних користувачів, які успішно пройшли процедуру автентифікації. Доступ до об'єктів, отриманий в обхід дозволів системи контролю доступу, називається несанкціонованим або неавторизованим.

7.1 Моделі інформаційної безпеки

Суть моделей безпеки полягає в наступному – безліч усіх видів порушень безпеки ділиться на кілька базових груп таким чином, щоб будь-яке можливе порушення можна було віднести хоча б до однієї з цих груп. І якщо система здатна протистояти кожній із цих груп порушень – вона вважається безпечною.

Однією з перших (та працездатних і досі) моделей безпеки вважається модель, запропонована Джеррі Зальцером і Майклом Шредером – тріада CIA (***C****onfidentiality/конфіденційність, **I**ntegrity/цілісність, **A**vailability/доступність)*, відповідно до якої всі можливі порушення інформаційної безпеки завжди можуть бути віднесені щонайменше до однієї з трьох груп:

– порушення конфіденційності (до інформаційних ресурсів мають доступ лише ті, кому він легально дозволений);

– порушення цілісності (інформація, що зберігається та обробляється інформаційною системою, не може бути змінена або видалена неавторизованим чином);

– порушення доступності (послуги, що надаються системою, можуть гарантовано та з допустимою затримкою бути надані користувачам, які мають на це право).

Сьогодні перелік властивостей безпечної системи розширено, до нього додалися автентичність (невідмовність), володіння, корисність (рис. 49). Ця розширена модель безпеки отримала назву Паркерівська гексада (група із шести предметів).

Автентичність (*Authenticity)* – стан інформаційної системи, при якому користувач не може видати себе за іншого, а документ завжди має достовірну інформацію про його джерело (автора).

Володіння чи контроль (*Possession or Control*) – фізичний контроль над пристроєм або іншим середовищем зберігання інформації надається лише тим, хто має право.

Корисність (*Utility)* – забезпечення зручності практичного використання як інформації, так і пов'язаних з її обробкою та підтримкою процедур.

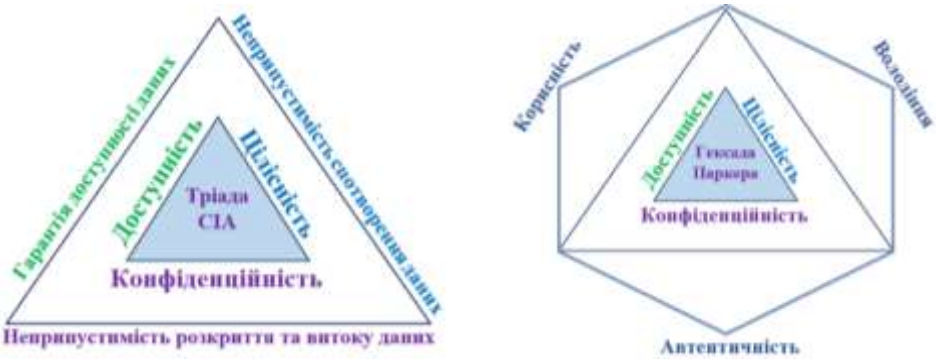


Рисунок 49 – Моделі безпеки

Інформаційна безпека включає всі аспекти, пов'язані з визначенням, досягненням та підтриманням конфіденційності, цілісності, доступності, невідмовності, підзвітності, автентичності та достовірності інформації або засобів її обробки.

Однією з основних частин інформаційної безпеки IT-систем підприємства (обладнання, програмне забезпечення, дані) є *кібербезпека*. Стратегію кібербезпеки на державному рівні регламентує Закон України «Про основні

засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [22].

Кібербезпека та мережева безпека тісно пов'язані, але не є синонімами. Вони мають спільну мету – захист інформації та систем, проте охоплюють різні рівні й аспекти безпеки. Основні відмінності між ними показані в таблиці 8.

Кібербезпека спрямована на захист всієї цифрової екосистеми. Мережева безпека є частиною кібербезпеки, що відповідає за безпечну комунікацію між пристроями (табл. 8).

Таблиця 8 – Основні аспекти кібербезпеки та мережевої безпеки

Параметр	Кібербезпека	Мережева безпека
Обсяг	Ширше поняття: охоплює всі аспекти захисту у цифровому просторі.	Вужче поняття: зосереджується лише на захисті комп'ютерних мереж.
Фокус	Захист даних, пристроїв, систем, користувачів, програмного забезпечення, мереж.	Захист інфраструктури передачі даних та мережевого трафіку.
Сфера дії	Увесь кіберпростір: Інтернет, хмарні сервіси, мобільні пристрої тощо.	Локальні мережі (LAN), глобальні мережі (WAN), маршрутизатори, комутатори.
Інструменти	Антивіруси, DLP-системи, SIEM, криптографія, моніторинг користувачів, IAM.	Фаєрволи, VPN, IDS/IPS, протоколи безпеки, сегментація мережі.

Кібербезпека включає мережеву безпеку як один із її компонентів, оскільки більшість атак відбувається через мережу. Щоб забезпечити повноцінну кібербезпеку, потрібно мати надійні засоби захисту мереж, бо саме через них часто відбувається доступ до критичних даних [3].

7.2 Методи захисту комп'ютерних мереж

Надійний захист комп'ютерних мереж передбачає застосування багаторівневого (комплексного) підходу, який включає технічні, програмні,

адміністративні та фізичні методи, спрямовані на запобігання несанкціонованому доступу, витоку, зміні або знищенню даних (рис. 50).

Рисунок 50 – Види захисту комп'ютерних мереж

Фізичний захист запобігає несанкціонованому фізичному доступу до мережевого обладнання. Заходи фізичного захисту: обмеження доступу до серверних приміщень; відеоспостереження та охоронні системи; захист від перенапруги, пожежі, клімат-контроль.

Технічний (апаратний) захист реалізується за допомогою мережевого обладнання. Заходи технічного захисту: мережеві екрани (Firewall) – фільтрують трафік за IP-адресою, портами, протоколами; маршрутизатори з правилами безпеки; апаратні VPN-шлюзи; сегментація мереж (VLAN) – розділення мережі на ізольовані ділянки.

Програмний захист здійснюється на рівні програмного забезпечення:

– антивірусні програми;

– IDS/IPS (системи виявлення та запобігання вторгненням);

– шифрування даних (TLS, IPsec);

– програмні фаєрволи (host-based firewall);

– програми аутентифікації (2FA, SSO);

– SIEM-системи: аналіз та реагування на інциденти.

Адміністративний (організаційний) захист регулює політику поведінки користувачів і адміністраторів:

– політики управління доступом;

– ролі та права користувачів (RBAC);

– навчання персоналу (інформаційна гігієна);

– регламенти резервного копіювання;

– регулярний аудит і тестування безпеки (penetration testing).

Криптографічний захист – захист даних шляхом шифрування, цифрових підписів і сертифікації. Заходи криптографічного захисту:

– шифрування переданих даних (SSL/TLS, IPsec);

– використання публічних/приватних ключів (RSA, ECC);

– цифрові сертифікати та підписи;

– електронна ідентифікація.

Політика резервного копіювання (Backup) забезпечує збереження даних у разі атаки або збою:

– локальні та хмарні резервні копії;

– автоматизовані системи відновлення;

– перевірка цілісності резервних даних.

7.3 Програмний захист

Вразливості. Загрози. Атаки.

Захист від вразливостей, загроз і атак – це основа безпеки комп'ютерних мереж.

Вразливість (Vulnerability) – це слабке місце або недолік у системі, програмному забезпеченні, апаратному забезпеченні чи мережевій інфраструктурі, який може бути використаний зловмисником для несанкціонованого доступу або порушення роботи системи. Вона виникає через

помилки в програмному забезпеченні, неправильне налаштування обладнання або навіть через людський фактор. Розрізняють такі види вразливостей:

– програмні баги: помилки в коді, які дозволяють виконати небезпечні дії (наприклад, переповнення буфера);

– неправильні налаштування: відкриті без необхідності програмні порти;

– вразливості в паролях: слабкі або стандартні паролі;

– соціальна інженерія: недостатня підготовка користувачів.

Приклади вразливостей: в системі є помилка, яка дозволяє зловмиснику виконати команди від імені адміністратора; незашифроване з'єднання; помилка в програмному коді.

Загроза (Threat) – це потенційна небезпека, яка може використати вразливість і завдати шкоди інформаційній системі або мережі. Загроза може бути навмисною (хакерська атака) або ненавмисною (збій обладнання). Типи загроз:

– навмисні: хакери, зловмисні програми (віруси, трояни), інсайдери;

– ненавмисні: помилки користувачів, технічні збої;

– фізичні: пожежа, повінь, крадіжка обладнання.

Приклад загроз: при наявності вразливості у вигляді незахищеного веб-сервера, загрозою може бути хакер, який спробує скористатися цим; віруси; природні катастрофи.

Атака (Attack) – це конкретна дія або серія дій, спрямованих на використання вразливості для реалізації загрози і нанесення шкоди системі, це фактичний напад на мережу або комп’ютер. Розрізняють наступні види атак:

– *DoS/DDoS атаки* (атаки відмови в обслуговуванні): перевантаження (навмисне) сервера або мережі запитами, що призводить до їх непрацездатності.

Приклад: масивний трафік (запити) одночасно від багатьох ботів, через що сайт стає недоступним.

DDoS – розподілена атака, коли трафік йде з великої кількості комп'ютерів.

– *Sniffing, сніффінг-атака*: спосіб перехоплення даних, що передаються мережею. Відбувається прослуховування та аналіз мережевого трафіку в певному сегменті без активного втручання в нього. Цей метод дозволяє несанкціоновано отримувати конфіденційну інформацію (логіни, паролі, службові пакети), що передається відкритим текстом. Приклад: використання програми Wireshark для захоплення паролів у незашифрованих мережах Wi-Fi.

– *«Людина посередині» (MITM, Man-In-The-Middle)*: зловмисник таємно ретранслює / змінює зв'язок між двома сторонами, які вважають, що вони безпосередньо спілкуються один з одним (рис. 51). *MITM* є методом компрометації каналу зв'язку, у якому зломщик, підключившись до каналу між контрагентами, здійснює втручання у протокол передачі, видаляючи чи спотворюючи інформацію. Приклад: відкрита Wi-Fi мережа, через яку зловмисник може підміняти сторінки або красти дані.

Рисунок 51 – Атака «Man-In-The-Middle»

– *Brute force, Dictionary attack, атаки на аутентифікацію*: злом паролів шляхом перебору варіантів. Приклад: автоматичний перебір паролів для входу в акаунт.

– *Phishing*, ф*ішинг*: шахрайські листи, відповідь на які дозволяє отримати незаконний доступ до конфіденційних даних користувача (заволодіння паролями). Приклад: підроблені електронні листи або сайти, які імітують банківські портали для крадіжки логінів.

– *Exploits, атаки на вразливості програмного забезпечення*. Експлойт – це комп'ютерна програма, фрагмент програмного коду або послідовність команд, які використовують уразливості в програмному забезпеченні та застосовуються для проведення атаки на обчислювальну систему. Метою атаки може бути захоплення контролю над системою, порушення її функціонування. Приклад: зловмисник надсилає велику кількість запитів на сервер, викликаючи його збій або вразливість у веб-сервері, яка дозволяє виконати довільний код.

– *SQL-ін'єкції*: спосіб злому сайтів та програм, які працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду (вставка шкідливого коду в базу даних через веб-форми щоб отримати доступ до бази даних). Приклад: веб-сайт без захисту від SQL-ін'єкції, через який можна витягнути паролі користувачів.

– *Cross-Site Scripting (XSS)*: впровадження шкідливого скрипта у веб-сторінку, який виконується у браузері інших користувачів. Приклад: зловмисник вставляє код, який краде файли *кукі* або виконує дії від імені користувача.

– *ARP Spoofing*: підміна ARP-записів у локальній мережі для перехоплення трафіку. Приклад: зловмисник видає себе за шлюз мережі, щоб отримати всі дані, що проходять через мережу.

Взаємозв'язок між поняттями: *вразливість* – це недолік (пробоїна) в системі; *загроза* – це *потенційна* «небезпека», яка хоче скористатися *недоліком*; *атака* – це *спроба* використати «пробоїну» для нанесення шкоди.

Основні підходи та заходи для зменшення ризиків

Захист від вразливостей:

– *регулярне оновлення програмного забезпечення*: виробники часто випускають патчі (оновлення), які виправляють знайдені вразливості, тому дуже важливо своєчасно оновлювати операційні системи, програми та мережеве обладнання;

– *впровадження політик безпеки*: створення складних паролів, регулярна їх зміна, обмеження прав доступу користувачів;

– *аудит і тестування безпеки*: періодичний пошук і виправлення вразливостей за допомогою спеціальних сканерів, тестування на проникнення (пентести);

– *використання захисного програмного забезпечення*: антивірусні програми, системи виявлення вторгнень (IDS), фаєрволи.

Захист від загроз:

– *навчання користувачів*: інформувати співробітників про фішинг, соціальну інженерію та правила безпечної роботи;

– *моніторинг і аналіз подій*: впровадження систем логування і моніторингу для виявлення підозрілої активності (*логи*, log-файли, журнали – це текстові файли, куди автоматично записуються всі події, що відбувалися у комп'ютерній системі);

– *резервне копіювання (бекапи)*: регулярне створення копій важливих даних допоможе швидко відновити систему після атаки або збою;

– *фізичний захист*: контроль доступу до серверних кімнат, захист від пожежі та інших фізичних небезпек.

Захист від атак:

– *фаєрволи (Firewall)*: фільтрують трафік і блокують небажані з’єднання;

– *антивірусні програми* (антишкідливе програмне забезпечення): виявляють і блокують шкідливі програми;

– *системи запобігання вторгненням (IPS)*: активно блокують підозрілі атаки в реальному часі;

– *впровадження багатофакторної аутентифікації (MFA)*: підвищує рівень захисту доступу навіть при викраденні пароля.

– *обмеження прав користувачів*: користувачі повинні мати лише ті права, які їм потрібні для роботи (принцип найменших привілеїв).

Додатковими засобами зменшення ризиків можуть бути: заздалегідь продуманий план реагування на інциденти (мінімізування збитків); шифрування даних (захищає інформацію під час зберігання та передачі); використання VPN (надає можливість безпечного з'єднання для віддаленого доступу) [4].

Антивірусні програми

Антивірус – програмний засіб, призначений для боротьби з вірусами. Основними завданнями антивірусу є: перешкоджання проникненню вірусів у комп'ютерну систему; виявлення наявності вірусів у комп'ютерній системі; усунення вірусів з комп'ютерної системи без нанесення ушкоджень іншим об'єктам системи; мінімізація збитку від дій вірусів.

Основні функції антивірусу:

– *виявлення шкідливих програм*: антивірус сканує файли і системні процеси, щоб знайти віруси або інший шкідливий код;

– *видалення або ізоляція*: якщо знайдено загрозу, антивірус може видалити її або помістити у карантин (ізольовану область, де вірус не може зашкодити системі);

– *запобігання зараженню*: антивірус може блокувати небезпечні сайти, шкідливі завантаження або підозрілі програми.

– *автоматичне оновлення*: віруси постійно оновлюються, тому антивірус регулярно оновлює свої бази даних, щоб вчасно виявляти нові загрози.

Технології, застосовувані в антивірусах, можна розбити на дві групи: технології сигнатурного аналізу та технології імовірнісного аналізу.

Сигнатурний аналіз (сигнатурне сканування) – метод виявлення вірусів, що полягає в перевірці наявності у файлах сигнатур вірусів.

Сигнатура – це певний рядок двійкового коду, який функціонує як *ідентифікатор* конкретного вірусу. Кожен вірус (і його варіації) має унікальну сигнатуру.

Сигнатурний аналіз є найбільш відомим методом виявлення вірусів. Для проведення перевірки використовується набір вірусних сигнатур, що зберігається в антивірусній базі. Коли файл завантажується або запускається, антивірус порівнює його з цією базою. Якщо збіг знайдено – файл вважається зараженим. Аналіз дає дуже точне виявлення *відомих* загроз, не гарантує стовідсотковий захист від нових, раніше невідомих вірусів.

Принцип роботи сигнатурного аналізу визначає межі його функціональності – можливість виявляти лише вже відомі віруси, проти нових вірусів сигнатурний сканер неспроможний. Антивірусна база має потребу в періодичному оновленні для підтримки актуальності антивірусного ПЗ.

Наявність сигнатур вірусів припускає можливість лікування інфікованих файлів, виявлених за допомогою сигнатурного аналізу. Однак, лікування припустиме не для всіх вірусів – трояни й більшість хробаків не піддаються лікуванню по своїх конструктивних особливостях, оскільки є цільними модулями, створеними для завдання збитків.

Технології імовірнісного аналізу підрозділяються на три категорії: *евристичний* аналіз, *поведінковий* аналіз, аналіз *контрольних сум*.

Евристичний аналіз – технологія, заснована на *імовірнісних алгоритмах*, результатом роботи яких є виявлення підозрілих об'єктів.

Антивірус розпізнає, що *робить* програма, а не тільки що вона *містить*. Якщо файл «поводиться» підозріло (намагається змінити системні файли, підключитися до мережі без дозволу тощо) – його позначають як потенційно небезпечний.

У процесі евристичного аналізу перевіряється *структура* файлу, його відповідність вірусним шаблонам. Найбільш популярною евристичною технологією є перевірка вмісту файлу на предмет наявності модифікацій уже відомих сигнатур вірусів та їхніх комбінацій. Це допомагає визначати гібриди й нові версії раніше відомих вірусів без додаткового відновлення антивірусної бази. Евристичний аналіз застосовується для виявлення невідомих вірусів, і, як наслідок, не припускає лікування. Дана технологія не здатна на 100% визначити вірус перед нею чи ні, і як будь-який імовірнісний алгоритм може спрацювати помилково.

Поведінковий аналіз – технологія, у якій рішення про характер об'єкта, що перевіряється, приймається на основі аналізу виконуваних ним дій. Передбачає постійний моніторинг роботи програм у реальному часі. Якщо додаток починає виконувати підозрілі операції (наприклад, швидко копіює себе, змінює системні налаштування), антивірус блокує його. Важливий для захисту від нових типів загроз, наприклад, вірусів-шифрувальників (ransomware).

Поведінковий аналіз досить вузько застосовується на практиці, тому що більшість дій, характерних для вірусів, можуть виконуватися й звичайними додатками. Найбільшу популярність одержали поведінкові аналізатори *скриптів* і *макросів*, оскільки відповідні віруси практично завжди виконують ряд однотипних дій. Наприклад, для впровадження в систему, майже кожен макровірус використає той самий алгоритм: у який-небудь стандартний макрос,

що запускається автоматично середовищем Microsoft Office при виконанні стандартних команд (наприклад, «Save», «Save As», «Open», і т.д.), записується код, що заражає основний файл шаблонів normal.dot і відповідно – кожен документ, що відкривається знову.

Засоби захисту, що вшивають в BIOS, також можна віднести до поведінкових аналізаторів. При спробі виконати зміни в MBR комп'ютера, аналізатор блокує дію й виводить відповідне повідомлення користувачеві.

Поведінкові аналізатори не використають для роботи додаткових об'єктів, подібних до вірусних баз і, як наслідок, нездатні розрізняти відомі й невідомі віруси – всі підозрілі програми апріорі вважаються невідомими вірусами.

Аналіз контрольних сум – це спосіб відстеження змін в об'єктах комп'ютерної системи. На підставі аналізу характеру змін, таких як *одночасність*, *масовість, ідентичні зміни довжин файлів* можна робити вивід про зараження системи. Аналізатори контрольних сум («ревізори» змін), як і поведінкові аналізатори, не використовують у роботі додаткові об'єкти і видають вердикт про наявність вірусу в системі винятково методом експертної оцінки. Подібні технології застосовуються в сканерах при доступі – при першій перевірці з файлу знімається контрольна сума й міститься в кеші, перед наступною перевіркою того ж файлу сума знімається ще раз, рівняється, і у випадку відсутності змін файл вважається незараженим.

Sandboxing (пісочниця) – антивірус запускає потенційно небезпечну програму в ізольованому середовищі (пісочниці), щоб подивитися, як вона поводиться. Якщо програма робить щось шкідливе – її не запускають у основній системі.

Для того, щоб антивірус виконував свої функції, необхідні правильні налаштування, активними/увімкнутими повинні бути наступні опції:

– *автоматичне оновлення* бази даних сигнатур вірусів;

– *планове сканування* системи має бути регулярним (наприклад, раз на тиждень);

– *реальний час (Real-time protection)*: функція, яка уможливлює миттєве реагування на загрози;

– *сканування зовнішніх носіїв* перед використанням;

– *карантин* дає можливість не втратити важливі файли через помилку;

– *брандмауер (Firewall)* підсилює захист мережевих з'єднань у поєднанні з антивірусом.

Світове програмне антивірусне забезпечення:

– Norton: американський антивірус від компанії Symantec.

– Bitdefender: продукт румунської компанії;

– Avast: чеський антивірус з безкоштовною і платною версіями.

– McAfee продукт американського виробництва;

– Trend Micro: японська компанія, що спеціалізується на кібербезпеці.

– ESET NOD32: виробником є словацька компанія;

– Sophos: виробником є британська компанія;

– Windows Defender: вбудований антивірус у Windows, розроблений Microsoft (США).

Реалізація програмно-технічного захисту комп'ютерних мереж

Мережевий екран (Firewall) – це локальний або функціонально розподілений програмний чи апаратний засіб, який контролює і фільтрує мережевий трафік, що входить / виходить з комп'ютерної мережі, відповідно до заданих правил безпеки (рис. 52). Основне завдання фаєрвола – *дозволити* або *заборонити* трафік на основі встановлених політик, з метою захисту від атак, вторгнень, несанкціонованого доступу.

Firewall є захисною стіною між *локальною* та *зовнішньою* мережами. Він запобігає загрозам, дає змогу відключати реклами і банери, рекламні скрипти, вспливаючі вікна, унеможливлює роботу програм-троянів і засобів віддаленого адміністрування.

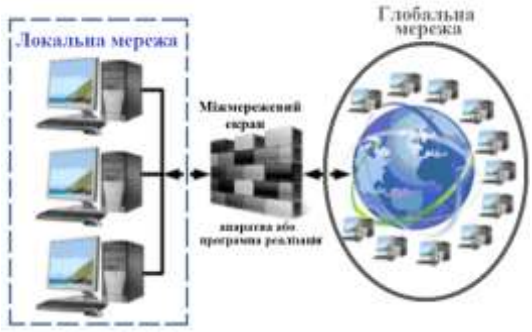


Рисунок 52 – Загальна схема роботи локальної мережі через МЕ

Робота мережевого екрану полягає в *аналізуванні структури* і *вмісту інформаційних пакетів*, що надходять із зовнішньої мережі. В залежності від результатів аналізу пакети пропускаються у внутрішню мережу (сегмент мережі) або відфільтровуються.

Мережеві екрани виконують наступні функції:

– фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв’язку, розмежування зон мережі: поділ на зони з різними рівнями довіри (внутрішня мережа, DMZ, Інтернет);

– багатоетапна ідентифікація запитів, що надходять в мережу;

– перевірка повноважень і прав доступу користувача до внутрішніх ресурсів мережі;

– моніторинг та логування: ведення журналів про проходження мережевого трафіку, реєстрація всіх запитів до компонентів внутрішньої підмережі ззовні;

– контроль цілісності програмного забезпечення і даних;

– економія адресного простору мережі;

– приховування IP-адреси внутрішніх серверів з метою захисту від хакерів; захист від відомих атак, таких як: SYN-флуд, порт-сканування, фальсифікація IP (spoofing).

DMZ (Demilitarized Zone) – демілітаризована зона, є проміжним мережевим сегментом, розташованим між довіреною локальною мережею і небезпечною зовнішньою мережею, наприклад, Інтернетом. Основна її функція – захист внутрішньої мережі від потенційних зовнішніх атак.

Різновиди мережевих екранів

Мережеві екрани різняться залежно від певних характеристик:

– екран забезпечує з'єднання між одним вузлом і мережею, між двома (або більше) різними мережами;

– контроль потоку даних відбувається на мережевому рівні або на більш високих рівнях моделі OSI;

– відстежуються стани активних з’єднань чи ні.

Залежно від охоплення контрольованих потоків даних мережеві екрани поділяються на:

– традиційний мережевий (або міжмережевий) екран: *програма* (або невід'ємна частина операційної системи) на шлюзі (сервері, який передає трафік між мережами) або *апаратне рішення*, що контролює вхідні і вихідні потоки даних між підключеними мережами;

– персональний мережевий екран: програма, встановлена на комп'ютері користувача і призначена для захисту від несанкціонованого доступу тільки цього комп'ютера.

Залежно від рівня, на якому відбувається контроль доступу, існує поділ мережевих екранів, що працюють на:

– мережевому рівні: фільтрація відбувається на основі адрес відправника і одержувача та статичних правил, заданих адміністратором;

– сеансовому рівні (також відомі як stateful): відслідковують сеанси між додатками, не пропускаючи пакети з порушеннями специфікації TCP / IP, що часто використовуються у зловмисних операціях (скануванні ресурсів, злому через неправильні реалізації TCP / IP, обрив / уповільнення з'єднань, ін'єкція даних);

– рівні додатків: фільтрація на підставі аналізу даних програми, які передаються всередині пакету (такі типи екранів дозволяють блокувати передачу небажаної і потенційно небезпечної інформації, на підставі політик і налаштувань);

– існують рішення (які відносять до мережевих екранів рівня програми), що являють собою проксі-сервер з можливостями мережного екрана.

Можливості проксі-сервера і багатопротокольна спеціалізація роблять фільтрацію значно більш гнучкою, ніж на класичних мережевих екранах, але такі програми мають всі недоліки проксі-серверів (наприклад, анонімізація трафіку).

Залежно від відстеження активних з’єднань мережеві екрани бувають:

Stateless (проста фільтрація): не відслідковують поточні з'єднання (наприклад, TCP), а фільтрують потік даних виключно на основі статичних правил;

Stateful packet inspection (SPI, фільтрація з урахуванням контексту): екрани з відслідковуванням поточних з'єднань та пропуском тільки таких пакетів, які задовольняють логіці й алгоритмам роботи відповідних протоколів і додатків. Такі типи мережних екранів більш ефективні при захисті від DoS-атак різних видів, та можуть захищати уразливі місця мережевих протоколів. Також вони забезпечують функціонування таких протоколів, які використовують складні

схеми передачі даних між адресатами (H.323, SIP, FTP) і погано піддаються опису статичними правилами.

Криптографічний захист

Криптографія – це наука про математичні методи забезпечення конфіденційності, цілісності даних, аутентифікації, шифрування.

Шифрування – це оборотне перетворення даних, з метою приховання інформації, воно є базовою технологією всіх служб інформаційної безпеки.

Дешифрування – зворотний процес шифрування, передбачає відтворення інформації із шифртексту.

Криптосистема – це алгоритм здійснення оборотних перетворень вихідного тексту в шифрований та навпаки. Зазвичай криптосистема передбачає наявність спеціального елемента – секретного ключа.

Криптографічний захист – це застосування методів криптографії для забезпечення конфіденційності, цілісності, автентичності, авторства, підтвердження її справжності та доступності даних, які передаються через комп'ютерні мережі. Цей вид захисту передбачає перетворення інформації шляхом використанням спеціальних алгоритмів. Мета – захистити інформацію від несанкціонованого доступу, підробки або зловмисних дій.

Засоби криптографічного захисту в мережах:

– протоколи безпеки;

– криптографічні системи управління ключами: механізми генерації, розповсюдження, зберігання і знищення ключів (рис. 53);

– аутентифікація і управління доступом: використання цифрових сертифікатів, токенів, паролів, біометрії.

Рисунок 53 – Схема криптографічного захисту мереж

Протоколи безпеки

Під час обміну інформацією в комп'ютерних мережах важливу роль в забезпеченні її захисту відіграє робота протоколів безпеки, які гарантують захист даних у процесі їх передавання. Вони забезпечують: конфіденційність (шифрування даних); цілісність (перевірка, що дані не змінені); автентичність (підтвердження сторін спілкування); неспростовність (неможливість заперечення факту передачі). До основні протоколів безпеки комп'ютерних мереж відносять: SSL / TLS, HTTPS, IPsec, SSH, PGP / GPG, Kerberos, RADIUS / TACACS+, WPA2 / WPA3, S/MIME, MACSec.

SSL / TLS (Secure Sockets Layer / Transport Layer Security): протоколи безпеки, що створюють захищене/зашифроване з'єднання між веб-сервером та веб-браузером/клієнтом, захищають передачу даних в Інтернеті (найчастіше використовуються в HTTPS). SSL-сертифікат – це цифровий сертифікат, що засвідчує справжність веб-сайту та дозволяє використовувати зашифроване з'єднання.

Принцип роботи протоколів безпеки: встановлюють зашифроване з’єднання між клієнтом і сервером; використовують асиметричне шифрування для обміну ключами, далі симетричне шифрування для основної передачі даних; перевіряють цифрові сертифікати серверів (і іноді клієнтів). Версії: SSL на даний час вже вважаються застарілими (SSL 2.0, SSL 3.0); сучасними є стандарти TLS 1.2 і TLS 1.3.

IPsec (Internet Protocol Security): шляхом шифрування і автентифікації IP-пакетів, здійснює їх безпечне передавання на *мережевому* рівні. Використовується для побудови VPN. Складовими протоколу вважаються компоненти:

- AH (Authentication Header): автентифікація і цілісність;
- ESP (Encapsulating Security Payload): шифрування і автентифікація.

Протокол має два режими роботи: *транспортний* – захищає тільки дані (корисне навантаження); *тунельний* – захищає весь IP-пакет, використовується для VPN.

SSH (Secure Shell): мережевий протокол прикладного рівня, який забезпечує зашифроване з’єднання, передачу команд і даних у зашифрованому вигляді, віддалене адміністрування серверів, безпечне копіювання файлів (scp, sftp), захищений доступ до віддалених систем, використовує асиметричну криптографію для аутентифікації.

VPN (Virtual Private Network): технологія, призначення якої створення захищеного «тунелю» для передачі даних через публічний інтернет, забезпечує аутентифікацію користувачів і пристроїв, захист приватності при роботі в публічних Wi-Fi мережах. Існують два різних типи VPN: *IPsec VPN* і *SSL VPN*. Обидва використовуються для створення захищених каналів зв'язку через Інтернет, але їх основні принципи роботи, сфери застосування та налаштування мають суттєві відмінності.

- *IPsec VPN*: використовує протокол *IPsec*, який працює на *мережевому* рівні (Layer 3) і забезпечує шифрування та аутентифікацію всіх переданих пакетів даних між кінцевими точками (наприклад, між віддаленим комп'ютером і корпоративною мережею або між двома офісами компанії). Забезпечує доступ до всіх мережевих ресурсів, а не лише до певних додатків або сервісів. Потребує спеціального *VPN-клієнта* для кожного користувача.

- *SSL VPN*: використовує *SSL* (або його більш сучасний аналог *TLS*), протокол працює на *транспортному* рівні (Layer 4), що дозволяє здійснювати захищене з'єднання між браузером користувача і сервером без потреби в спеціальному VPN-клієнті. Найчастіше використовується для надання доступу до конкретних ресурсів або додатків. Зазвичай не потребує додаткових клієнтів або спеціальних налаштувань, можливе підключення через веб-браузер.

Kerberos: протокол аутентифікації, який використовується для безпечного підтвердження особи користувачів і сервісів у комп’ютерних мережах. Його основна мета – гарантія того, що користувачі або служби, які хочуть отримати доступ до ресурсів мережі, є тими, ким вони себе називають, без передачі паролів у відкритому вигляді.

Використовує принцип централізованої аутентифікації: у мережі є центральний сервер (або служба) – *KDC* (Key Distribution Center), який перевіряє користувачів. Після успішної аутентифікації користувач отримує спеціальний квиток (ticket), який він використовує для доступу до різних сервісів у мережі без повторного введення пароля. Усі квитки і повідомлення шифруються за допомогою секретних ключів, щоб захистити їх від підробки чи перехоплення.

WPA2 / WPA3 (Wi-Fi Protected Access): стандарти захисту бездротових мереж, що забезпечують надійне шифрування даних, які передаються по Wi-Fi.

- *WPA2* (рік появи 2004): використовує протокол шифрування *AES* (Advanced Encryption Standard); слабкий захист відкритих мереж.

- *WPA3* (рік появи 2018), покращена безпека: використовує протокол шифрування *AES* і механізми *SAE* (Simultaneous Authentication of Equals), захист при слабких паролях та *Enhanced Open*, шифрування навіть у відкритих мережах (без пароля), що захищає трафік від прослуховування.

S/MIME (Secure/Multipurpose Internet Mail Extensions): захист електронної пошти, шифрування листів і цифрові підписи.

MACSec (Media Access Control Security): шифрування кадрів Ethernet, високозахищені локальні мережі.

Аутентифікація і управління доступом

Механізми аутентифікації і управління доступом передбачають використання різних засобів. Основними методами аутентифікації є: паролі, цифрові сертифікати, токени, біометрія.

Пароль (ключ безпеки) – умовне слово або довільний набір знаків, що складається з букв, цифр та інших символів, і призначений для підтвердження особи або повноважень. Якщо допустиме використання лише цифр, то таку комбінацію іноді називають ПІН-кодом.

Цифрові сертифікати – це електронні документи, які підтверджують особу (або пристрій) і містять *відкритий* ключ. Сертифікат видає довірений центр сертифікації (CA). Використовуються в інфраструктурі відкритих ключів (PKI), у HTTPS для безпечного з'єднання, у VPN для ідентифікації користувачів.

Токени – фізичні або програмні пристрої, які генерують тимчасові коди (OTP – одноразові паролі) або зберігають цифрові ключі, застосовуються у двофакторній аутентифікації (2FA).

Біометрія – використання унікальних фізичних або поведінкових характеристик людини: відбитки пальців, розпізнавання обличчя, сітківка ока,

голос. Забезпечує високу безпеку з причин складності підробки, але можливі помилки в розпізнаванні або проблеми з конфіденційністю.

Управління доступом – це процес визначення, хто і які ресурси може використовувати після того, як він пройшов аутентифікацію.

Основні моделі управління доступом:

– *DAC (Discretionary Access Control)*: користувач або власник ресурсу сам вирішує, хто може отримати доступ;

– *MAC (Mandatory Access Control)*: доступ керується централізовано на основі політик безпеки (наприклад, секретність документів);

– RBAC (Role-Based Access Control): доступ надається залежно від ролі користувача (наприклад, адміністратор, співробітник, гість).

Криптографічні системи управління ключами

Криптографічні системи управління ключами – це системи (процеси, протоколи та інструменти), які відповідають за створення, розподіл, зберігання, оновлення та знищення криптографічних ключів.

Криптографічний ключ – це секретна інформація (рядок бітів або символів), яку використовують у криптографії для шифрування та дешифрування даних або для аутентифікації.

Без правильного управління ключами навіть найсильніше шифрування стає марним, якщо ключ загублений (викрадений або скомпрометований) – безпека системи порушується. Розрізняють два типи ключів:

– *симетричний* ключ (алгоритми симетричного шифрування): один і той самий ключ використовується і для шифрування, і для дешифрування;

– *асиметричний ключ* (алгоритми асиметричного шифрування): використовується пара ключів – *публічний* (для шифрування) і *приватний* (для дешифрування).

Довжина ключа вимірюється в бітах (128 біт, 256 біт і т.д.). Чим довший ключ, тим він складніший для злому. Секретний ключ має бути випадковим і достатньо довгим, щоб унеможливити перебір усіх варіантів.

Основні функції систем управління ключами:

– *генерація ключів*: створення випадкових, складних ключів для шифрування та аутентифікації;

– *розподіл ключів*: безпечна передача ключів між учасниками системи, щоб ніхто сторонній не отримав доступ;

– *зберігання ключів*: надійне збереження ключів у спеціальних апаратних (HSM, Hardware Security Module) або програмних сховищах;

– *оновлення ключів*: періодична заміна ключів для зниження ризику компрометації;

– *анулювання ключів*: відкликання або знищення ключів, які більше не використовуються або скомпрометовані;

– *аудит і контроль*: відстеження використання ключів і забезпечення відповідності політикам безпеки.

Системи управління ключами:

– *PKI* (Public Key Infrastructure): інфраструктура відкритих ключів, яка автоматизує управління публічними/приватними ключами і цифровими сертифікатами.

– *HSM* (Hardware Security Module): апаратні пристрої для захищеного зберігання і обробки криптографічних ключів.

– *програмне забезпечення* для керування ключами: спеціальні програми або сервіси, що реалізують всі функції управління ключами.

Симетричне шифрування

Метод кодування інформації, у якому для шифрування та розшифровування повідомлень використовується *один* і той самий секретний ключ, називається *симетричним* шифруванням.

Алгоритми симетричного шифрування:

– AES (Advanced Encryption Standard): найпоширеніший і найнадійніший симетричний алгоритм, використовується урядами, фінансовими установами, у Wi-Fi (WPA2/WPA3), підтримує ключі довжиною 128, 192 і 256 біт, швидкий і стійкий до атак;

– DES (Data Encryption Standard): старий стандарт шифрування, вважається застарілим через невелику довжину ключа (56 біт), легко зламується;

– 3DES (Triple DES): покращена версія DES; дані шифруються тричі з трьома різними ключами; використовується, коли потрібно підтримати старі системи, але поступається AES по швидкості і безпеці; в процесі заміни на більш сучасні алгоритми;

– ChaCha20: високошвидкісний і безпечний потоковий шифр; використовується у мобільних пристроях і інтернет-протоколах (у TLS, заміна AES у певних випадках);

– IDEA (International Data Encryption Algorithm): використовувався у ранніх версіях криптосистеми PGP (Pretty Good Privacy), добре захищений, має ліцензійні обмеження.

– RC4, RC5, RC6: сімейство симетричних алгоритмів шифрування, розроблених компанією RSA Security; швидкий і простий шифр, вразливий до кількох атак, вважається недостатньо безпечним.

Головна особливість методу симетричного шифрування полягає у складності створення умов для безпечного передавання секретного ключа від

однієї сторони іншій. Цю проблему вирішено у алгоритмах асиметричного шифрування.

Асиметричне шифрування

Концептуальна можливість асиметричного підходу до шифрування за допомогою *спеціальних функцій* дозволяє побудувати криптографічну систему, у якій текст шифрується одним ключем, а розшифровується іншим.

Функції асиметричної криптосистеми повинні відповідати двом принциповим вимогам:

– зашифроване повідомлення має бути результатом *односторонньої функції*, щоб ніхто не міг виконати зворотні перетворення та отримати вихідний текст;

– ця одностороння функція повинна мати певний *секретний елемент* (ключ), знаючи який одержувач шифрованого тексту може легко виконати зворотне перетворення.

Функції, які відповідають описаним вимогам, називають *односторонніми функціями із секретом*.

У сфері інформаційної безпеки існує спеціальний клас односторонніх функцій, які називають *хеш-функціями*. Хеш-функція, застосована до певних даних, *дає* в результаті *значення* з фіксованого числа байтів, яке не залежить від довжини вихідних даних.

У 1978 році американські вчені Рівест, Шамір та Адлеман вперше створили алгоритм асиметричного шифрування RSA (Rivest, Shamir та Adleman), який дозволив *шифрувати* дані *публічним* ключем і *розшифровувати* їх *приватним* ключем.

Асиметричне шифрування використовує два різних, але *пов'язаних* ключі. Схема алгоритму асиметричного шифрування наступна:

– користувач генерує пару ключів: публічний і приватний;

– публічний ключ мають можливість отримати всі, хто буде надсилати йому зашифрованого повідомлення;

– відправник шифрує повідомлення публічним ключем;

– лише власник приватного ключа може розшифрувати зашифроване повідомлення.

Алгорити асиметричного шифрування: RSA, Elliptic Curve Cryptography (ECC), DSA (Digital Signature Algorithm).

Застосування асиметричного шифрування у HTTPS

У роботі протоколу HTTPS використовується метод асиметричного шифрування. Спрощену схему встановлення безпечного з'єднання (рис. 54) можна розділити на декілька етапів.

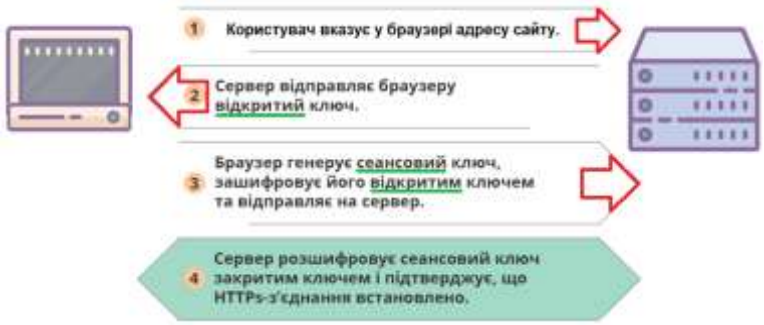


Рисунок 54 – Схема встановлення безпечного з'єднання

Початок з'єднання: TLS Handshake. Перед тим, як розпочати захищений обмін інформацією, клієнт та сервер мають узгодити алгоритм шифрування та відповідний ключ. Це відбувається під час процедури «рукостискання» – відкриття сеансу зв'язку.

Браузер відправляє запит на встановлення безпечного зв'язку із сервером.

У відповідь сервер відправляє браузеру свій цифровий сертифікат, який містить його публічний ключ. Використані під час рукостискання сертифікати з відкритими ключами можуть мати різну довжину і тому різну стійкість до атак.

Перевірка сертифіката. Браузер перевіряє сертифікат: чи його підписав довірений центр сертифікації (CA), чи не прострочений він, чи відповідає домену. Якщо все добре – браузер довіряє серверу.

Обмін ключами – генерація спільного секрету. Браузер генерує симетричний сеансовий ключ (AES або інший). Цей сеансовий ключ шифрується публічним ключем сервера (асиметричне шифрування RSA або інший алгоритм). Зашифрований сеансовий ключ відправляється серверу.

Розшифровка ключа на сервері. Сервер розшифровує отриманий сеансовий ключ за допомогою свого приватного ключа. Після цього і сервер, і браузер мають спільний симетричний ключ.

Захищений обмін даними. Вся подальша передача даних шифрується за допомогою симетричного ключа.

Шифрування ключів відбувається асиметричними алгоритмами, для шифрування повідомлень застосовують симетричні алгоритми. Симетричне шифрування швидше за асиметричне, тому на шифрування і розшифрування повідомлень потрібно менше обчислювальних ресурсів.

При перехопленні трафіка, надісланого за протоколом HTTPS, повідомлення буде виглядати як набір випадкових символів, для його порозуміння потрібен ключ. Зашифровані деталі банківської карти будуть виглядати приблизно як на рисунку 55.

Рисунок 55 – Зашифрований код банківської карти

Ключи шифрування мають певну довжину, щоб навіть найпотужнішому комп’ютеру знадобилися роки безперервної роботи для можливості їхнього підбору.

Стандарти довжини ключів

Довжина ключа шифрування – це кількість бітів або символів, які складають ключ, що використовується в криптографії для шифрування й дешифрування даних. Вона впливає на безпеку шифру: чим довший ключ, тим складніше зламати шифр перебором.

Довжина ключа 128 біт у симетричному шифруванні вважається мінімальною для надійного шифрування (рекомендована становить 256 біт). Відповідна безпека асиметричного шифрування починається від 2048 біт і більше.

Симетричні алгоритми шифрування

– AES: 128, 192 або 256 біт;

– DES: 56 біт (вже вважається небезпечним);

– 3DES: 112 або 168 біт;

– Blowfish: 32-448 біт (зазвичай 128 біт).

Асиметричні алгоритми (публічний/приватний ключ)

– RSA: зазвичай від 1024 до 4096 біт (сучасний стандарт 2048 біт);

– ECC (еліптичні криві): 256 біт (еквівалент приблизно 3072 біт RSA);

– DSA: 1024-3072 біт.

У асиметричних алгоритмах довжини ключів значно більші, тому що безпека базується на складності певних математичних задач.

ЗАПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ ДО РОЗДІЛУ 3

1. Що таке служби глобальних мереж, служби Інтернет? Їх роль у сучасних мережах?
2. Основні типи/категорії служб глобальної мережі?
3. Поясніть принцип роботи служби потокового відео (Streaming).
4. Що таке хмарні сервіси і які основні моделі їх надання?
5. Як працюють служби ідентифікації та аутентифікації в глобальних мережах?
6. Як відбувається передача великих обсягів даних через глобальні мережі?
7. Що таке протокол ICMP і яка його роль?
8. Що таке служби повідомлень в реальному часі?
9. Як працює служба пошти у глобальних мережах? Які протоколи використовуються для відправлення і отримання електронної пошти?
10. Що таке веб-служби і які основні протоколи вони використовують? Поясніть принцип роботи протоколу HTTP/HTTPS.
11. Що таке FTP, призначення і основні функції?
12. Які основні функції служби доменних імен?
13. Що таке VoIP і як працює ця служба в Інтернеті? Як відбувається передача голосу і відео по IP? Які протоколи підтримують голосовий зв’язок через IP?
14. Як працюють служби соціальних мереж в Інтернеті?
15. Що таке кешування і як воно використовується в службах Інтернет?
16. Як працює служба пошуку?
17. Основні складові безпеки комп’ютерних мереж.
18. Які загрози безпеки комп’ютерних мереж існують?
19. Основні стандарти і нормативи в області безпеки комп’ютерних мереж.
20. Що таке політика безпеки мережі? Які основні компоненти політики безпеки?

21. Які існують методи запобігання несанкціонованому доступу до мережі?

22. Які існують інструменти для аналізу безпеки мережі? Основні засоби захисту локальних мереж.

23. Системи моніторингу мережевого трафіку. Принцип роботи системи контролю доступу в локальні мережі

24. Як працюють системи виявлення та запобігання вторгнень? Що таке IDS і IPS?

25. Що таке журналювання і логування подій безпеки?

26. Аутентифікація, її роль в безпеці мережі? Які існують методи аутентифікації, що таке MFA?

27. Які типи мережевих атак існують?

28. Що таке MITM-атака?

29. Що таке DoS і DDoS атаки? Як їх розпізнати і протидіяти?

30. Що таке міжмережевий екран (firewall) і які його функції? Які типи файєрволів існують і в чому їхні відмінності?

31. Як працюють антивірусні системи в мережах? Які методи захисту від вірусів і шкідливого програмного забезпечення існують?

32. Криптографічний захист. Поясніть принцип роботи шифрування даних. Які види шифрування використовуються для захисту мережевого трафіку?

33. Що таке криптографічний ключ і які типи ключів існують? Різниця між симетричним і асиметричним шифруванням.

34. Що таке сертифікаційний центр у контексті мережевої безпеки? Що таке сертифікат безпеки і як він використовується?

35. Які основні протоколи забезпечують безпеку мережевого з’єднання?

36. Що таке фішинг і як його розпізнати?

37. Що таке сегментація мережі і як вона покращує безпеку?

38. Як працюють VLAN і яку роль вони відіграють у безпеці мережі?

39. Що таке політика резервного копіювання і відновлення даних?

40. Які особливості безпеки бездротових мереж? Як захистити Wi-Fi мережу від несанкціонованого доступу? Що таке WPA2 і WPA3 і чим вони відрізняються?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. Ч. 2. 372 с. URL: https://ela.kpi.ua/items/ffe5594e-c560-4744-ab07-08cd35ebe63a
2. Комп'ютерні мережі : навч. посіб. / Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Львів : Магнолія-2006, 2023. Кн. 2. 328 с.
3. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. / В. М. Богуш та ін. ; за ред. В. М. Богуша. Київ : Вид-во Ліра-К, 2020. 554 с.
4. Технології забезпечення безпеки мережевої інфраструктури : підручник / В. Л. Бурячок та ін. Київ : КУБГ, 2019. 218 с.
5. Бенько С. М. Smart-технології та технології колективного інтелекту. *Всеосвіта*. URL: https://vseosvita.ua/library/smart-tekhnolohii-ta-tekhnolohii-kolektyvnoho-intelektu-795978.html (дата звернення: 02.05.2025).
6. Козацький С. Велика Британія та США шукають альтернативу GPS через ризики дій Росії. *Militarnyi*. URL: https://militarnyi.com/uk/news/velyka-brytaniya-ta-ssha-shukayut-alternatyvu-gps-cherez-ryzyky-dij-rosiyi/ (дата звернення: 12.05.2025).
7. IEEE – The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. *IEEE*. URL: https://www.ieee.org/ (date of access: 25.05.2025).
8. IEEE 802.3df-2024. *IEEE Standards Association*. URL: https://standards.ieee.org/ieee/802.3df/11107 (date of access: 25.05.2025).
9. What Is Signal Integrity? *Altium*. URL: https://resources.altium.com/p/signal-integrity (date of access: 26.05.2025).
10. Meet the fastest in the industry. *Ciena*. URL: https://www.ciena.com/ (date of access: 30.05.2025).

11. Siemon Unveils High-Density 800G Cable Assemblies for Data Centers. *Siemon*. URL: https://www.siemon.com/en/siemon-unveils-high-density-800g-cable-assemblies-for-data-centers/ (date of access: 12.06.2025).
12. Narayan L. Ethernet 1.6T Verification IP & Protocol Solutions for Next-Gen Networking & Communication Systems. *Synopsys*. URL: https://www.synopsys.com/blogs/chip-design/ethernet-1-6t-vip-and-protocol-solutions.html (date of access: 12.06.2025).
13. CoMira Solutions unveils its new 1.6T Ethernet UMAC IP. *Design & Reuse*. URL: https://www.design-reuse.com/news/202501314-comira-solutions-unveils-its-new-1-6t-ethernet-umac-ip (date of access: 12.06.2025).
14. Keysight Demonstrates First Full Line Rate 1.6 Terabit Ethernet Test Capability. *Keysight*. URL: https://www.keysight.com/us/en/about/newsroom/news-releases/2024/0319-pr24-051-keysight-demonstrates-first-full-line-rate-1-6-ter.html (date of access: 04.06.2025).
15. 5G Statistics and Facts (2025). *Market.us Scoop*. URL: https://scoop.market.us/5g-statistics/ (date of access: 12.05.2025).
16. Оператори та провайдери. *Інтернет субвенція*. URL: https://bb.gov.ua/operator (дата звернення: 12.06.2025).
17. Карта мережі–1х. *1х*. URL: https://1-ix.net/karta-merezhi/ (дата звернення: 04.06.2025).
18. Всі українські провайдери інтернету: повний список 2024. *Uablocklist*. URL: https://uablocklist.com/providers (дата звернення: 12.06.2025).
19. Всесвітня мережа інтернет провайдерів. *АРМ-ІНСТАЛ*. URL: https://www.mit-net.com.ua/всесвітня-мережа-інтернету/ (дата звернення: 12.06.2025).
20. Gera S. What Makes Satellite Internet So Revolutionary? *The Digital Archive*. URL: https://thedigitalarchive.info/what-makes-satellite-internet-so-revolutionary/ (date of access: 12.06.2025).
21. NB-IoT і бізнес: рішення для розумної інфраструктури. *Kyivstar Business Hub – корпоративний блог для бізнесу*. URL: https://hub.kyivstar.ua/articles/nb-io-t-i-biznes-rishennya-dlya-rozumnoyi-infrastrukturi (дата звернення: 12.06.2025).
22. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.04.2025).

Навчальне видання

Петречук Ліна Миколаївна, Іващенко Юрій Сергійович,

Підгорна Катерина Дмитрівна

КОМП'ЮТЕРНІ МЕРЕЖІ ТА ТЕЛЕКОМУНІКАЦІЇ

Навчальний посібник

Електронне видання

Відповідальний редактор Л. М. Петречук
Комп'ютерна верстка Л. М. Петречук
Дизайн обкладинки Л. М. Петречук

Експертний висновок склав канд. екон. наук, доц. К. О. Удачина

Зареєстровано НМВ УДУНТ (№ 59 від 25.08.2025)

Формат 60x84 1/16. Ум. друк. арк. 11,75. Обл.-вид. арк. 11,89.
Зам. № 112

Видавець: Український державний університет науки і технологій
вул. Лазаряна, 2, ауд. 2216, ауд. 263 (наукова бібліотека)
м. Дніпро, 49010.
Свідоцтво суб'єкта видавничої справи ДК № 7709 від 14.12.2022