

ЗАТВЕРДЖУЮ
Директор ЗПО «ДІТК»
31.08.2026 р.
Олександр СТІПЛЕЦЬ
ПОГОДЖЕНО
Заступник директора з навчально-методичної
роботи ЗПО «ДІТК»
31.08.2026 р.
Сергій ГОРДІЄНКО

ВСТУП

Опанування навичок роботи з комп'ютерними мережами є критично важливим для здобувачів фахової передвищої освіти технічних спеціальностей, оскільки сучасні інформаційні технології, радіоелектронне обладнання та інженерні рішення значною мірою базуються на мережевій взаємодії. У зв'язку з цим вивчення принципів побудови, функціонування, налаштування та пошуку несправностей у комп'ютерних мережах відіграє важливу роль при формуванні цілісного пулу компетентностей фахівця з електроніки, електронних комунікацій, приладобудування та радіотехніки.

Пропонований конспект лекцій розроблено з метою всебічного охоплення як теоретичної, так і практичної підготовки здобувачів освіти для роботи з основними технологіями та обладнанням комп'ютерних мереж, функціонуючими в них протоколами, базовими моделями і стандартами. Матеріал структуровано таким чином, щоб забезпечити поетапне засвоєння знань — від основних концепцій до практичної реалізації складних мережових рішень, необхідних у професійній діяльності фахівця з експлуатації радіоелектронного, телекомунікаційного і мережевого обладнання.

Основна увага приділена функціонуванню стеку протоколів TCP/IP, моделі взаємодії відкритих систем OSI, стандартам дротових мереж Ethernet та бездротових мереж типу Wi-Fi. У конспекті розкрито питання використання схем IP-адресації з маскою змінної довжини при реалізації підмереж, зокрема для віртуальних локальних мереж (VLAN), застосування складових корпоративних мереж — таких як технології магістральних каналів та протоколи агрегації каналів, методи резервування основного шлюзу, застосування статичної та динамічної маршрутизації, а також базові прийоми забезпечення безпеки мережі.

РОЗДІЛ 1

СУЧАСНІ ТЕХНОЛОГІЇ МЕРЕЖНОГО ЗВ'ЯЗКУ

У сучасному світі мережні технології відіграють критично важливу роль. Вони забезпечують швидке та надійне передавання даних між різними пристроями та користувачами, що є основою для функціонування інформаційних систем, бізнес-процесів, соціальних мереж, електронної комерції, наукових досліджень і навіть розваг. Мережі дозволяють організаціям та приватним особам обмінюватися інформацією, спільно використовувати ресурси та співпрацювати незалежно від географічного розташування.

Важливість використання мереж у сучасних системах важко переоцінити. Наприклад, компанії використовують мережі для зв'язку між філіями, співробітники отримують доступ до корпоративних ресурсів із будь-якої точки світу, завдяки хмарним сервісам зберігання даних, користувачі можуть зберігати, обробляти та обмінюватися файлами без необхідності в локальному зберіганні. Інтернет, як глобальна мережа, об'єднує мільярди пристроїв і користувачів, забезпечуючи доступ до безмежного обсягу інформації та сервісів, таких як електронна пошта, соціальні мережі, онлайн-банкінг і потокове відео.

Щоб мережа могла забезпечувати послуги ефективно, вона складається з кількох ключових компонентів, кожен з яких має свою унікальну роль. Ці компоненти працюють разом, щоб забезпечити надійний і зручний доступ до інформації.

Вузли або кінцеві пристрої є базовими елементами будь-якої мережі. Це пристрої, такі як комп'ютери, планшети або смартфони, які підключені до мережі і безпосередньо беруть участь у мережному спілкуванні. Кожен вузол має унікальну IP-адресу, що дозволяє ідентифікувати його в межах мережі.

На відміну від кінцевих пристроїв, сервери є спеціалізованими комп'ютерами, які надають послуги іншим пристроям у мережі. Сервери можуть надавати різні послуги, такі як електронна пошта або доступ до вебзастосунків, і використовують відповідне програмне забезпечення для цього. Клієнти, з іншого боку, є пристроями, які використовують програмне забезпечення для запиту та отримання інформації з серверів. Наприклад, веббраузери є клієнтським програмним забезпеченням, яке звертається до вебсерверів для отримання вебсторінок.

У малих мережах, таких як домашні або невеликі офісні мережі, один комп'ютер може виконувати функції і клієнта, і сервера одночасно. Це створює мережі типу *peer-to-peer*, які прості в налаштуванні і мають низькі накладні витрати, але можуть бути менш безпечними і масштабованими.

Кінцеві пристрої, такі як комп'ютери і принтери, є основними учасниками мережі: через них або надсилають, або отримують дані. Для забезпечення зв'язку між кінцевими пристроями та мережею використовуються проміжні пристрої (рисунки 1.1), які забезпечують підключення, регенерацію сигналів,

управління маршрутизацією даних та інші функції, що сприяють безперебійній передачі інформації.

Один з таких пристроїв – комутатор, який з'єднує різні кінцеві пристрої в межах однієї мережі. Комутатор отримує дані і надсилає їх лише на той порт, до якого підключений конкретний пристрій, що допомагає зменшити навантаження на мережу.

Маршрутизатор, з іншого боку, з'єднує різні мережі між собою і відповідає за визначення оптимального маршруту для передачі даних між ними. Він забезпечує взаємодію між мережами і підключення до Інтернету.

Шлюзи виконують роль перекладачів між мережами, які використовують різні протоколи або технології. Вони конвертують дані з одного формату в інший, що дозволяє взаємодіяти різним мережам.

Модеми перетворюють цифрові сигнали в аналогові і назад, що дозволяє передавати дані через телефонні лінії або інші аналогові канали зв'язку.

Точки доступу надають бездротовий доступ до мережі для різних пристроїв, як-то ноутбуки чи смартфони, розширюючи можливості мережі без використання дротових з'єднань.

Нарешті, дані в мережі передаються через різні типи середовищ: через металеві дроти, оптоволоконні кабелі або з використанням бездротових технологій. Кожен тип середовища має свої особливості, які визначають його відповідність для конкретних завдань і вимог мережі.

Загалом, ці компоненти разом забезпечують ефективну та надійну роботу мережі, що дозволяє користувачам здійснювати обмін інформацією та використовувати ресурси без значних перешкод.

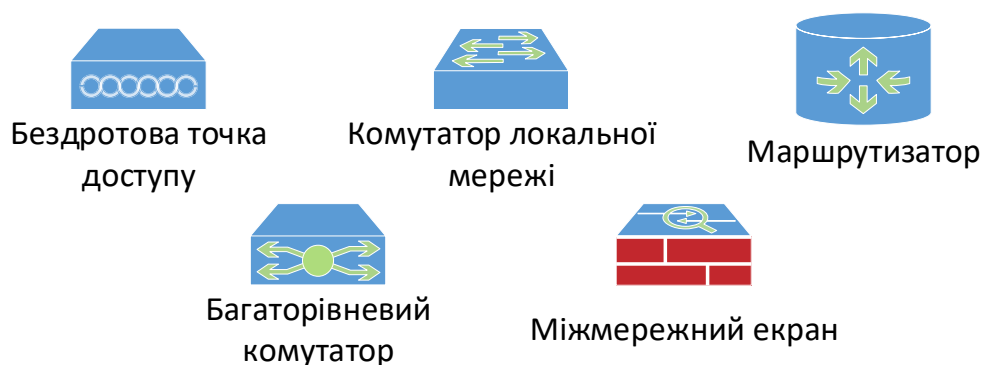


Рисунок 1.1 – Проміжні пристрої мережі

Інфраструктура мережі документується за допомогою спеціальних символів та різних типів діаграм, які відображають з'єднання між пристроями в мережі. Розуміння цих символів та діаграм є важливим аспектом для того, щоб повністю зрозуміти мережну комунікацію.

Використання топологій є критично важливим для ефективного проектування, реалізації та обслуговування мереж. Топології надають чітке уявлення про те, як компоненти мережі з'єднані між собою, що дає змогу:

- Планувати та проектувати мережі: Знання топології допомагає в розробці мереж, визначаючи оптимальні розташування пристроїв і підключення між ними. Це забезпечує ефективне використання ресурсів і уникнення можливих проблем.
- Виявляти і усувати проблеми: Топології спрощують ідентифікацію і локалізацію проблем у мережі. Коли виникають неполадки, топології допомагають швидко знайти місце збою і вжити заходів для його усунення.
- Оцінювати продуктивність і масштабованість: Розуміння топології дозволяє оцінити, як мережа справляється з навантаженням і як вона може бути розширена або змінена без порушення її функціонування.
- Забезпечувати безпеку: Топології допомагають виявити потенційні вразливості в мережі і спроектувати заходи безпеки, щоб захистити мережу від загроз.
- Документувати мережу: Топології забезпечують документацію, яка є важливою для майбутнього обслуговування мережі, навчання нових співробітників та планування оновлень.

Топології мереж можна поділити на фізичні та логічні, кожна з яких має свої особливості і призначення.

Фізична топологія (рисунок 1.2) показує реальне фізичне розташування пристроїв і кабелів в мережі. Вона включає інформацію про те, де саме розміщені проміжні пристрої, комп'ютери, сервери та інші елементи мережі, а також про те, як фізично прокладені кабелі між ними. Фізична топологія є важливою для розуміння того, як саме з'єднані пристрої, і для планування фізичної інфраструктури мережі. Вона допомагає при встановленні нового обладнання та проведенні обслуговування.

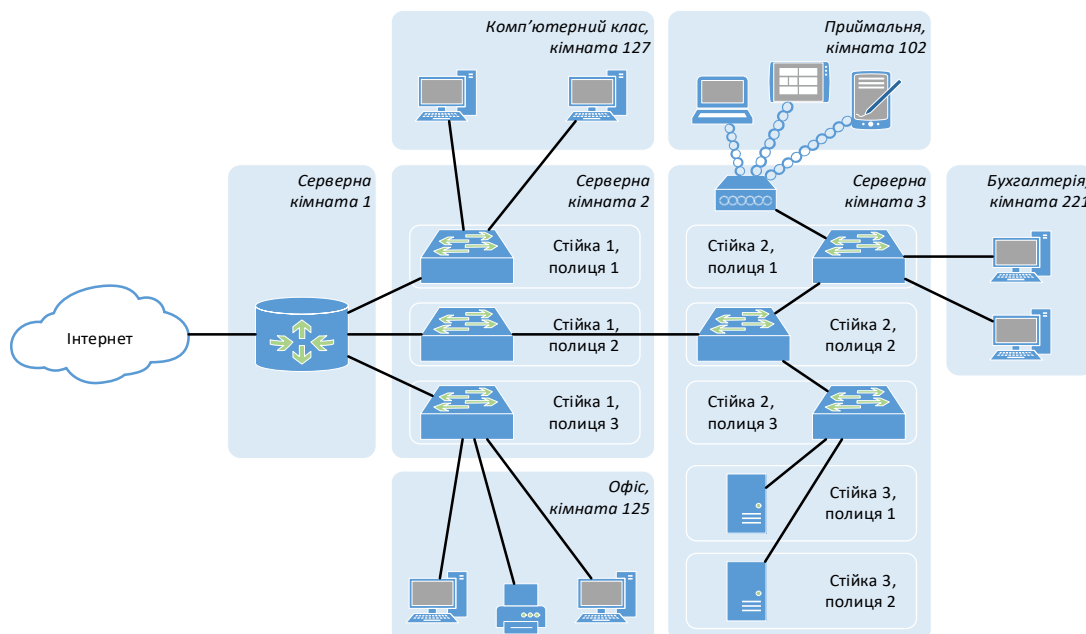


Рисунок 1.2 – Приклад фізичної топології

Логічна топологія описує, як саме дані переміщуються через мережу. Вона відображає логічні з'єднання між пристроями, порти, *VLAN* і схему адресації. Логічна топологія показує, як інформація проходить між пристроями, які використовують різні протоколи та адреси для комунікації. Цей тип топології допомагає зрозуміти, як мережний трафік обробляється і передається, і є корисним для налаштування мережі, управління трафіком та забезпечення безпеки. Приклад логічної топології зображено на рисунку 1.3.

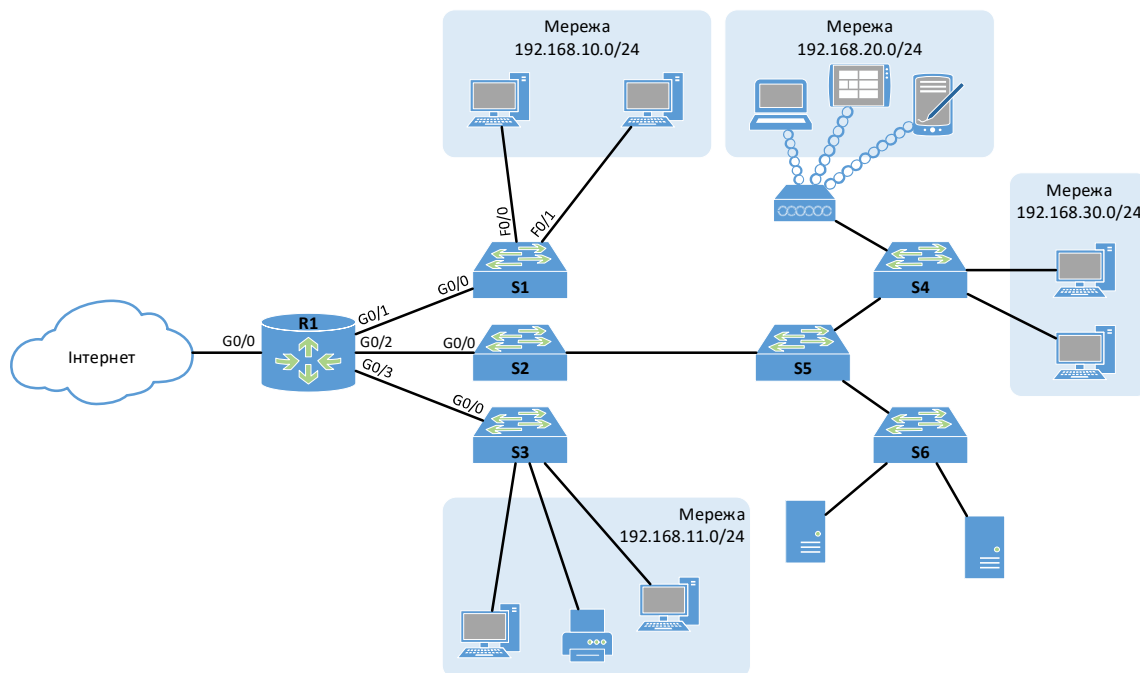


Рисунок 1.3 – Приклад логічної топології

Обидва типи топологій разом забезпечують повну картину мережної інфраструктури. Фізичні топології дають уявлення про реальну конфігурацію обладнання, тоді як логічні топології пояснюють, як саме дані переміщуються та обробляються в мережі. Розуміння обох аспектів є необхідним для ефективного управління і підтримки мережних систем.

Надійність мережі є критичним аспектом, що забезпечує стабільність і ефективність у передачі даних та наданні послуг. Вона включає в себе кілька ключових концепцій, які допомагають забезпечити безперебійність роботи мережі, її здатність до розширення, високу якість обслуговування та безпеку.

Відмовостійкість мережі забезпечує її стабільну роботу навіть у випадку збоїв або відмов компонентів. Це досягається шляхом створення резервних шляхів для передачі даних. Якщо один шлях виходить з ладу, дані автоматично перенаправляються іншим шляхом, завдяки чому забезпечується безперервність комунікації. Наприклад, у мережах з пакетною комутацією дані розбиваються на пакети, які можуть подорожувати різними маршрутами до одного й того ж пункту призначення. Це дозволяє уникнути переривань у зв'язку та забезпечити безперебійне передавання інформації.

Масштабованість мережі означає її здатність адаптуватися до зростаючих потреб у користувачах та обсягах даних без значного зниження продуктивності. Мережа має бути спроєктована так, щоб нові пристрої та послуги могли бути легко інтегровані без порушення роботи існуючих сервісів. Це досягається через дотримання стандартів і протоколів, що забезпечують безшовну інтеграцію нових елементів в існуючу мережу.

Якість обслуговування (*Quality of Service – QoS*) є критично важливою для забезпечення високої якості послуг, таких як голосові та відеотрансляції. *QoS* дозволяє управляти трафіком у мережі, надаючи пріоритет критичним додаткам і сервісам, особливо у випадку перевантаження мережі. Це допомагає уникнути затримок і втрат пакетів, що може погіршити якість обслуговування.

Безпека мережі включає захист як фізичної інфраструктури, так і даних, що передаються мережею. Основні аспекти безпеки включають: конфіденційність (забезпечення того, що дані можуть бути доступні лише авторизованим користувачам); цілісність (гарантія, що дані не були змінені або пошкоджені під час передачі); доступність (забезпечення своєчасного та надійного доступу до даних для авторизованих користувачів).

У мережних комунікаціях існують кілька основних типів доставки повідомлень, які визначають, як саме дані передаються від відправника до одержувача (рисунк 1.4).

При **індивідуальній розсилці (*unicast*)** повідомлення надсилається від одного джерела до одного призначення. Це найпоширеніший тип доставки у мережах, коли одне повідомлення направляється конкретному отримувачу. Протоколи, як-то *TCP* і *UDP*, можуть використовувати індивідуальну розсилку для передавання даних між однією парою пристроїв.

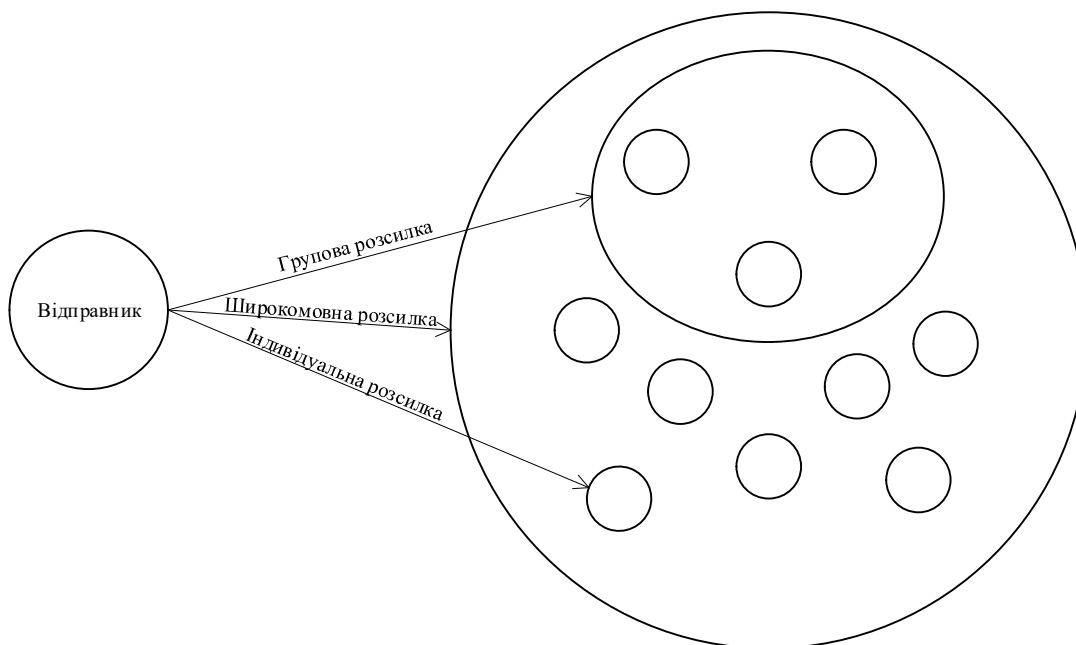


Рисунок 1.4 – Типи розсилок в мережі

При **груповій розсилці** (*multicast*) повідомлення надсилається до вибраної групи пристроїв у мережі, але не до всіх пристроїв. Це дозволяє зменшити навантаження на мережу, передаючи дані лише тим пристроям, які підписані на певну групу. Протокол *IGMP (Internet Group Management Protocol)* використовується для управління членством у групах групової розсилки.

При **широкомовній розсилці** (*broadcast*) повідомлення надсилається всім пристроям у мережі або підмережі. Це означає, що одне повідомлення надходить до всіх пристроїв без розрізнення, хто є одержувачем. Ця розсилка підходить для сценаріїв, коли потрібно розповсюдити інформацію серед усіх пристроїв, наприклад, для автоматичного виявлення пристроїв або оголошень у мережі.

1.1 ПРОТОКОЛИ ТА МОДЕЛІ

Протокол є набором правил і стандартів, які визначають, як дані передаються між різними пристроями в мережі. Це свого роду мова спілкування між комп'ютерами, подібно до того, як люди спілкуються мовами. Якщо два комп'ютери використовують однаковий протокол, вони можуть ефективно обмінюватися інформацією – як люди, що говорять однією мовою. Уявіть, що двоє людей намагаються спілкуватися, але один говорить англійською, а інший – китайською. Без перекладача або спільної мови їхня комунікація буде неефективною або навіть неможливою. Так само, якщо комп'ютери використовують різні протоколи без можливості взаємодії, вони не зможуть обмінюватися даними.

Протоколи виконують різні функції, які є критично важливими для забезпечення успішної комунікації між пристроями в мережі. Основні функції мережних протоколів включають: адресацію, забезпечення надійності, контроль потоку, сегментування, виявлення помилок, надання програмного інтерфейсу.

Протоколи використовують визначені схеми **адресації** для ідентифікації відправника та одержувача повідомлення. Це дозволяє пристроям у мережі точно визначити, куди саме слід доставити дані. Наприклад, протоколи *Ethernet*, *IPv4* та *IPv6* забезпечують адресацію, що дозволяє безпомилково направляти дані до відповідного пристрою.

Функція **надійності** забезпечує доставку повідомлень навіть у випадку їх втрати чи пошкодження під час передачі. Наприклад, протокол *TCP* гарантує доставку даних шляхом повторних спроб передачі пакетів, якщо вони не були отримані належним чином.

Керування потоком регулює швидкість передачі даних між двома пристроями, щоб уникнути перевантаження приймача. Це необхідно для того, щоб пристрій, який отримує дані, міг обробити їх вчасно. Протокол *TCP*, наприклад, реалізує керування потоком, регулюючи швидкість передачі даних залежно від можливостей приймача.

Сегментування забезпечує унікальне маркування кожного сегмента даних, що передається. Це дозволяє приймаючому пристрою правильно зібрати

дані в потрібному порядку, навіть якщо сегменти були доставлені з затримкою або в неправильному порядку. Протокол *TCP* виконує сегментування, що є необхідним для відновлення цілісності повідомлень.

Функція **виявлення помилок** перевіряє, чи дані не були пошкоджені під час передачі. Це дозволяє виявити помилки, які могли статися через завади чи інші проблеми з передаванням. Протоколи – такі як *Ethernet*, *IPv4*, *IPv6* і *TCP* – використовують різні методи для виявлення помилок і забезпечення цілісності переданих даних.

Програмний інтерфейс містить інформацію, яка використовується для комунікації між процесами різних мережних додатків. Наприклад, коли користувач звертається до вебсторінки, протоколи *HTTP* або *HTTPS* використовуються для взаємодії між веббраузером (клієнтом) і вебсервером. Це дозволяє додаткам ефективно обмінюватися інформацією через мережу.

Протоколи групуються в стеки або моделі, щоб упорядкувати й стандартизувати процес передавання даних. Це забезпечує сумісність і ефективність роботи мереж різних типів. Найвідоміші моделі протоколів – це модель *OSI* (*Open Systems Interconnection*) та *TCP/IP* (*Transmission Control Protocol/Internet Protocol*). Їх порівняння сумісно з поширеними протоколами зображено на рисунку 1.5.

Модель *OSI* була розроблена в 1978 році Міжнародним комітетом зі стандартизації (*ISO*). Ця модель складається з семи рівнів, кожен з яких виконує певну функцію. Рівні моделі *OSI* знизу вгору: фізичний, канальний, мережний, транспортний, сеансовий, рівень подання даних і прикладний. Кожен рівень моделі *OSI* спирається на функціонал нижнього рівня і надає сервіси верхньому рівню. Важливою перевагою моделі *OSI* є її універсальність і незалежність від конкретних технологій.

Модель OSI	Протоколи	Модель TCP/IP
Прикладний	DHCP, DNS, FTP, HTTP, IMAP, LDAP, POP3, SIP, SMB, SMTP, SSH, RDP	Прикладний
Рівень подання даних		
Сеансовий		
Транспортний	TCP, UDP	Транспортний
Мережний	IPv4, IPv6, ICMPv4, ICMPv6	Міжмережний
Канальний	Ethernet, WLAN	Рівень мережного доступу
Фізичний		

Рисунок 1.5 – Порівняння моделей *OSI* та *TCP/IP*

Модель *TCP/IP*, що виникла на початку 1970-х років у результаті досліджень Управління перспективних науково-дослідних розробок (*Advanced Research Project Agency, ARPA*) Міністерства оборони США, більш спрощена й практична. Вона складається з чотирьох рівнів: рівень мережного доступу, міжмережний рівень, транспортний і прикладний рівні. Ця модель була створена для забезпечення надійного передавання даних у мережах *ARPANET*, які стали основою Інтернету. Однією з переваг моделі *TCP/IP* є її практична орієнтація та широке використання в сучасних мережах.

Одне велике повідомлення, наприклад, велике зображення або відео, може бути передано мережею як один великий безперервний потік бітів. Однак це може викликати проблеми для інших пристроїв, що використовують ті ж канали зв'язку, оскільки великі обсяги даних можуть призвести до значних затримок, передавання великих обсягів даних монополізує канал. Якщо під час передавання повідомлення якась частина мережі зазнає збоїв, усе повідомлення може бути втрачено і його доведеться передавати заново.

Більш ефективним методом є розділення даних на менші частини. Сегментування – це процес розподілу великого потоку даних на менші, зручніші блоки для передачі через мережу. У мережах, побудованих на основі стека *TCP/IP*, дані передаються у вигляді окремих *IP*-пакетів. Пакети, що містять частини одного і того ж повідомлення, можуть бути відправлені різними маршрутами.

Оскільки великі обсяги даних розбиваються на пакети, передача через мережу відбувається без залежності від одного каналу зв'язку. Це також дозволяє ефективно управляти численними обмінами даних у мережі, забезпечуючи мультиплексування. У випадку проблем з мережею або перевантаженням, при втраті одного сегмента необхідно повторно передати лише цей сегмент, а не весь обсяг даних.

Сегментування дозволяє мережним протоколам адаптуватися до різних умов мережі, наприклад, до змінної пропускної здатності або затримок, що може бути корисним для підтримки високої якості обслуговування. Якщо під час передачі даних виникає помилка, вона зазвичай обмежується конкретним сегментом, що спрощує діагностику і виправлення помилок. Менші сегменти даних можна ефективніше маршрутизувати мережею, що дозволяє краще використовувати мережні ресурси та зменшити затримки.

Сегментування є ключовим елементом для забезпечення ефективної і надійної передачі даних у мережах, особливо в умовах високих навантажень або змінних умов зв'язку.

На етапі підготовки користувацьких даних до передачі, кожен рівень моделі додає свою інформацію до даних, що надходять з верхнього рівня. Цей процес (рисунок 1.6) можна порівняти з надсиланням поштового листа: лист вкладається в конверт, на який додається адреса, потім конверт може бути вкладений в інший конверт для відправлення через поштову службу. На кана-

льному рівні інкапсульовані дані разом із заголовками називаються кадрами, на мережному рівні – пакетами, а на транспортному – сегментами.

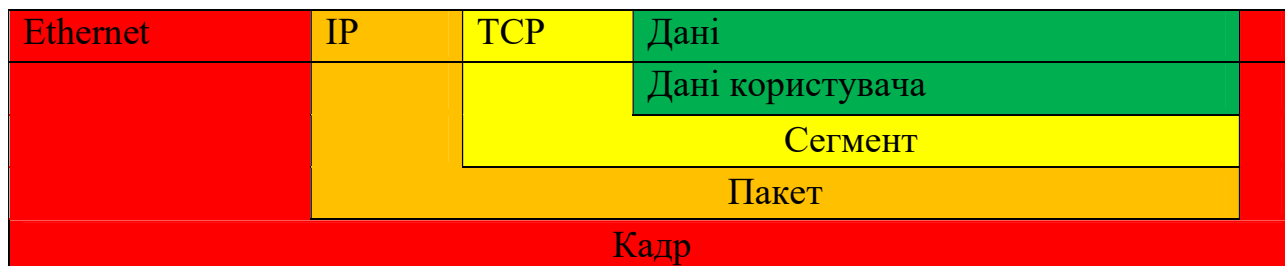


Рисунок 1.6 – Процес інкапсуляції повідомлень

Інкапсуляція – це процес обгортання даних у відповідні заголовки та трейлери на кожному рівні протокольного стека перед їх передачею мережею.

Спочатку дані створюються на рівні додатка, наприклад, текст повідомлення або вебсторінка. Дані розбиваються на сегменти (у випадку *TCP*) і отримують заголовок транспортного рівня. Цей заголовок містить важливу інформацію, як-то порти відправника та отримувача, номер сегмента та контроль помилок. Кожен сегмент інкапсулюється у пакет, до якого додається заголовок мережного рівня. Заголовок мережного рівня включає інформацію про *IP*-адреси відправника та отримувача. Пакет отримує заголовок і трейлер канального рівня, що включає інформацію про фізичну адресу (*MAC*-адресу) та контроль помилок на канальному рівні. Отриманий кадр перетворюється у біти і передається фізичним середовищем.

Деінкапсуляція – це процес, при якому заголовки та трейлери, додані під час інкапсуляції, видаляються на кожному рівні при отриманні даних.

Біти, отримані мережею, конвертуються назад у кадри. На канальному рівні відкидаються заголовок та трейлер і отриманий пакет передається на мережний рівень. Від пакета відкидається мережний заголовок і отриманий сегмент передається на транспортний рівень. Транспортний рівень відкидає заголовки сегментів та збирає сегментоване повідомлення в дані, які потім передаються додаткам у їх первісному вигляді.

Таким чином, інкапсуляція та деінкапсуляція забезпечують правильне форматування і обробку даних на різних етапах їх передачі мережею, що є критично важливим для забезпечення надійної і коректної комунікації.

Стандартизація протоколів є критично важливою для забезпечення ефективної роботи комп'ютерних мереж. Коли протоколи стандартизовані, це дозволяє різним пристроям і системам, виготовленим різними виробниками, працювати разом без проблем. Це створює основу для безперебійної комунікації між різними компонентами мережі, що знижує витрати на розробку нових продуктів та технологій, оскільки виробники можуть орієнтуватися на спільні специфікації.

Стандарти також сприяють підвищенню якості, оскільки всі пристрої, які відповідають стандартам, повинні пройти певні тестування і сертифікацію, що забезпечує стабільність і ефективність мережі. Крім того, відкриті стандарти стимулюють інновації, дозволяючи розробникам створювати нові технології без обмежень, що забезпечує швидше впровадження нових рішень.

Стандарти також відіграють важливу роль у забезпеченні безпеки, визначаючи кращі практики і методи захисту даних. Це допомагає запобігти загрозам і вразливостям у мережах. Нарешті, стандартизація спрощує інтеграцію нових елементів у мережу та обслуговування існуючих компонентів, оскільки не потрібно вносити великі зміни в інфраструктуру для підтримки нових технологій.

Організації, як-то *ISOC (Internet Society)*, *IAB (Internet Architecture Board)*, *IETF (Internet Engineering Task Force)*, *IRTF (Internet Research Task Force)*, *ICANN (Internet Corporation for Assigned Names and Numbers)*, *IANA (Internet Assigned Numbers Authority)* займаються стандартизацією протоколів та моделей.



Рисунок 1.7 – Організації зі стандартизації

Таким чином, протоколи є основою сучасних мережних технологій. Вони забезпечують стандартизовані методи передавання даних, що дозволяє різним пристроям і мережам ефективно взаємодіяти між собою, забезпечуючи надійну та ефективну комунікацію.

1.2 ФІЗИЧНИЙ РІВЕНЬ

Фізичний рівень є основою мережного зв'язку, оскільки саме він відповідає за безпосередню передачу даних між пристроями в мережі. Його головна мета полягає у забезпеченні фізичної передачі бітів через різноманітні середовища, як-то електричні кабелі, оптичні волокна або бездротові канали. Цей рівень займається перетворенням цифрових даних у сигнали, які можна переда-

вати через ці фізичні середовища, та зворотним перетворенням сигналів у бітові потоки на приймальній стороні.

Процес роботи фізичного рівня починається з того, що він приймає дані з вищого рівня (наприклад, кадри з канального рівня) і перетворює їх на сигнали, які можуть бути зрозумілі для конкретного середовища передачі. Це можуть бути електричні імпульси у випадку мідного кабелю, світлові імпульси для оптоволоконного зв'язку або радіохвилі для бездротових мереж. Потім ці сигнали передаються через середовище до приймального пристрою.

На приймальній стороні пристрій на фізичному рівні зчитує ці сигнали з середовища, перетворює їх назад у бітові потоки, і передає їх на канальний рівень для подальшої обробки. Важливо відзначити, що фізичний рівень не займається розпізнаванням або обробкою даних на рівні кадрів чи пакетів; його завдання – лише передати послідовність бітів з одного пристрою на інший з мінімальними втратами.

Фізичний рівень також відповідає за такі важливі аспекти, як визначення фізичних характеристик середовища передачі, управління швидкістю передачі даних, синхронізацію сигналів і контроль за цілісністю переданих бітів. Він забезпечує базову інфраструктуру, на якій будується вся інша мережа, гарантуючи, що дані можуть бути надійно передані від відправника до отримувача фізичним середовищем.



Рисунок 1.8 – Мережева інтерфейсна карта

Для передачі сигналу використовуються мережеві інтерфейсні карти (*NIC – Network Interface Controller*), які підключають пристрої до мережі та забезпечують передачу сигналів через різні середовища, такі як дротові або бездротові з'єднання. Середовища передачі можуть включати кабелі та інші фізичні

компоненти, що забезпечують фізичну передачу сигналів між пристроями. Інтерфейси та з'єднувачі також є важливими елементами, які з'єднують пристрої і забезпечують їх взаємодію в межах мережі.

Для передавання даних фізичними середовищами над ними відбувається процес кодування. Це процес, під час якого групи бітів представляються в певному шаблоні, що є зрозумілим як для відправника, так і для отримувача. Кодування необхідне для забезпечення надійної та ефективної передачі даних у мережах. Воно перетворює цифрову інформацію в спеціальні сигнали, які можуть бути розпізнані та правильно інтерпретовані як відправником, так і отримувачем. Це допомагає уникнути помилок під час передачі даних фізичним середовищем, забезпечує синхронізацію між пристроями та підвищує загальну ефективність передачі, особливо на високих швидкостях.

У мережах використовуються різні типи кодування, щоб забезпечити коректну передачу даних. Наприклад, Манчестерське кодування використовується в старих стандартах *Ethernet*, таких як *10BASE-T*, де перехід від високого до низького рівня напруги представляє **0**, а перехід від низького до високого – **1**. Для передачі даних на більших швидкостях використовуються більш складні методи кодування, такі як *4B/5B* в *Ethernet 100BASE-TX* або *8B/10B* в *1000BASE-T*.

Фізичне середовище характеризується пропускнуою здатністю – це здатність фізичного середовища передавати дані. Вона вимірюється в кількості бітів, які можуть бути передані з одного місця в інше за певний проміжок часу. Основними одиницями вимірювання пропускнуої здатності є біти на секунду (б/с, bps), кілобіти на секунду (Кб/с, Kbps), мегабіти на секунду (Мб/с, Mbps), гігабіти на секунду (Гб/с, Gbps) і терабіти на секунду (Тб/с, Tbps). Зверніть увагу, що літера «б» у одиницях вимірювання є маленькою, і це показує, що це біти. Для байтів літера «б» була б великою – «Б», як-от МБ/с.

Пропускна здатність використовується для оцінки того, скільки даних може бути передано мережею за певний час, що є ключовим показником ефективності мережних підключень і загальної продуктивності мережі.

Реальна мережа завжди характеризується такими особливостями, як затримка, пропускна здатність і корисна пропускна здатність.

Затримка відображає час, необхідний для передачі даних від джерела до отримувача. Вона включає в себе всі затримки, які виникають при передачі і обробці даних через різні пристрої і мережі. Затримка найчастіше вимірюється в мілісекундах (мс) і є важливою для оцінки швидкості реагування мережі.

Пропускна здатність визначає максимальну кількість даних, яка може бути передана через мережне з'єднання за одиницю часу. Це теоретичний максимум швидкості передачі. Пропускна здатність показує потенціал мережі щодо швидкості передачі даних.

Корисна пропускна здатність описує реальну кількість корисних даних, що можуть бути передані мережею за одиницю часу, з урахуванням різних на-

кладних витрат, таких як заголовки пакетів, підтвердження отримання і інші витрати на протокол. Корисна пропускна здатність завжди менша за пропускну здатність, оскільки враховує ці додаткові витрати.

Мідний кабель є одним із найстаріших і найпоширеніших засобів для передачі даних у мережах. Він має декілька ключових характеристик, а також переваги і недоліки, що впливають на його застосування.

Мідний кабель може бути представлений у формі незахищеної крученої пари (*UTP*), екранованої крученої пари (*STP*) або коаксіального кабелю. Основні характеристики мідного кабелю базуються на тому, що мідь є хорошим провідником електричного струму, що забезпечує високу ефективність передачі сигналів. При цьому мідні кабелі можуть мати різний рівень захисту від фізичних пошкоджень і електромагнітних завад.

Переваги мідного кабелю:

- **Вартість:** Мідний кабель зазвичай дешевший у порівнянні з оптичними волокнами, що робить його економічно вигідним вибором для багатьох мереж.
- **Простота встановлення:** Встановлення мідного кабелю є менш складним і потребує менше спеціалізованого обладнання, ніж оптичне волокно.
- **Сумісність:** Мідний кабель має добре розвинуту інфраструктуру і підтримується багатьма пристроями та стандартами, що полегшує інтеграцію в існуючі мережі.
- **Гнучкість:** Мідні кабелі є досить гнучкими, що полегшує їх прокладання в складних умовах.

Недоліки мідного кабелю:

- **Обмежена дальність:** Сигнали в мідних кабелях зазнають ослаблення на великій відстані, що обмежує їх використання на довгі дистанції.
- **Завади:** Мідний кабель підлягає впливу електромагнітних завад (*EMI*) і радіочастотних завад (*RFI*), що може погіршити якість сигналу.
- **Швидкість передачі:** Хоча мідні кабелі підтримують високі швидкості передачі даних, вони зазвичай не можуть досягати швидкостей, доступних для оптичних волокон.

Вибір мідного кабелю для конкретної мережі залежить від багатьох факторів, включаючи вартість, вимоги до швидкості передачі даних, відстані та рівня завад.

Типи кабелів на основі крученої пари, що використовуються в мережах: незахищена кручена пара і екранована кручена пара.

Неекранована кручена пара (Unshielded Twisted-Pair, *UTP*) – це найпоширеніший тип кабелів у сучасних мережах (рисунок 1.9). Він складається з чотирьох пар кольорових дротів, які скручені разом і захищені лише тонким пластиковим покриттям. Таке скручування допомагає зменшити вплив електромагнітних завад та взаємної завади (перешкоди між сусідніми парами проводів). *UTP*-

кабелі зазвичай використовуються для з'єднання комп'ютерів, маршрутизаторів і комутаторів в локальних мережах (*LAN*). Попри свою простоту та доступність, *UTP*-кабелі не мають додаткового екранування для захисту від сильних завад.

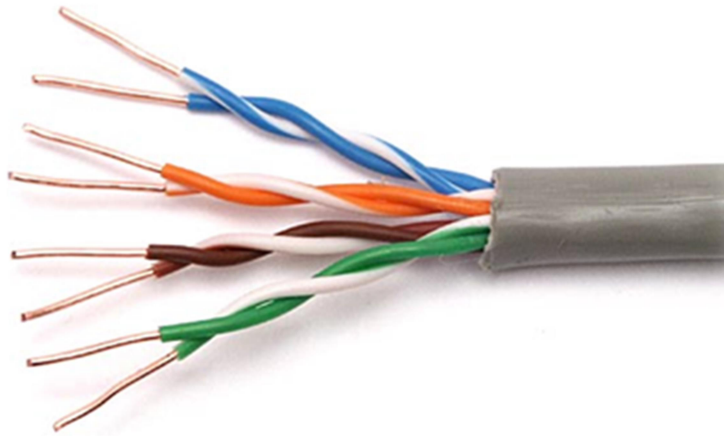


Рисунок 1.9 – Неекранована кручена пара

Екранована кручена пара (Shielded Twisted-Pair, *STP*) забезпечує кращий захист від електромагнітних перешкод і взаємних завад завдяки додатковому екрануванню (рисунок 1.10). У *STP*-кабелях кожна пара дротів може мати окремий шар фольги або екранування, а весь кабель може бути обгорнутий додатковим металевим плетінням. Це робить *STP*-кабелі ідеальними для середовищ з високим рівнем електромагнітних перешкод, як-то промислові зони або великі офісні будівлі, де звичайний *UTP* може не забезпечити достатнього захисту.



Рисунок 1.10 – Екранована кручена пара

UTP кабелі класифікують за категоріями (рисунок 1.11), які визначають їх характеристики і максимальні швидкості передачі даних:

- **Cat 5:** Підтримує швидкість до 100 Mbps на відстані до 100 метрів. Використовується для *Fast Ethernet*.
- **Cat 5e:** Покращена версія Cat 5, яка підтримує швидкість до 1 Gbps і знижує взаємні завади.

- **Cat 6:** Підтримує швидкість до 10 Gbps на коротких відстанях (до 55 метрів) і має покращене екранування для зменшення перешкод.
- **Cat 6a:** Додатково покращене екранування дозволяє досягти швидкості до 10 Gbps на відстані до 100 метрів.
- **Cat 7:** Забезпечує ще краще екранування і підтримує швидкість до 10 Gbps на довгих відстанях.
- **Cat 8:** Призначений для швидкостей до 40 Gbps на відстані до 30 метрів.

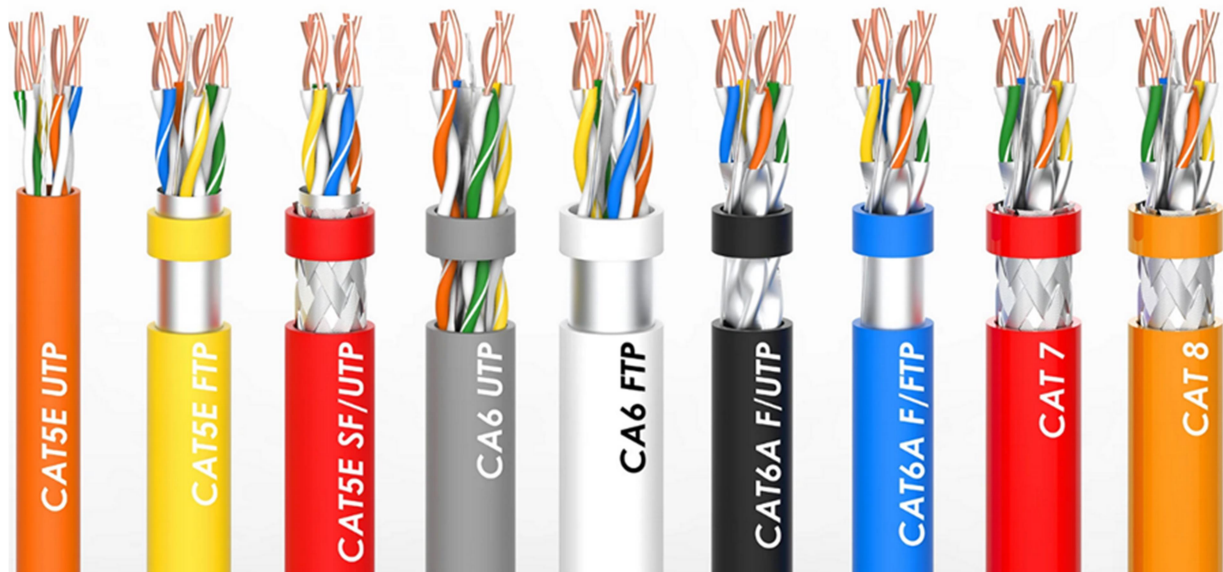


Рисунок 1.11 – Категорії кабелів

Для *UTP* кабелів переважно використовуються роз'єми *RJ-45*. Цей тип з'єднувачів найпоширеніший, особливо для *Ethernet*. Він має вісім контактів і використовується для підключення кабелів до мережних пристроїв, як-то комутатори, маршрутизатори і комп'ютери.

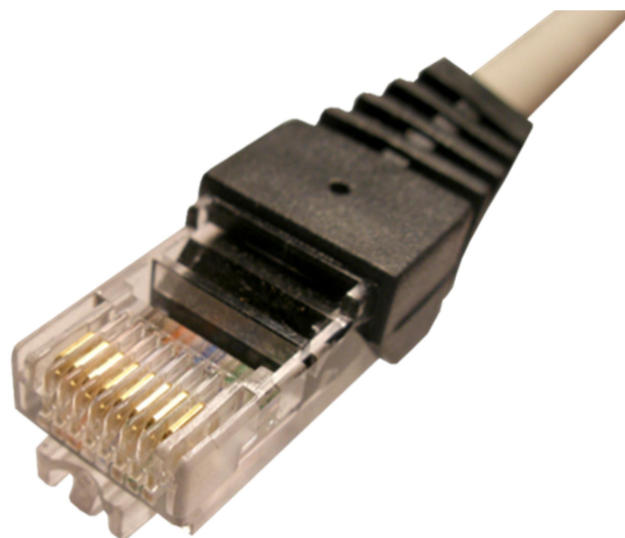


Рисунок 1.12 – Роз'єм *RJ-45*

Типи обтиснення *RJ-45* визначаються за стандартами *T568A* і *T568B*. Ці стандарти визначають, як саме проводи всередині кабелю повинні бути підключені до контактів роз'єму *RJ-45*.

Вибір між *T568A* і *T568B* залежить від того, який стандарт використовують ваші мережеві пристрої (рисунок 1.13). Для правильного функціонування мережі важливо, щоб обидва кінці кабелю мали однаковий стандарт обтиснення: або обидва *T568A*, або обидва *T568B*. Стандарт *T568B* використовується частіше.

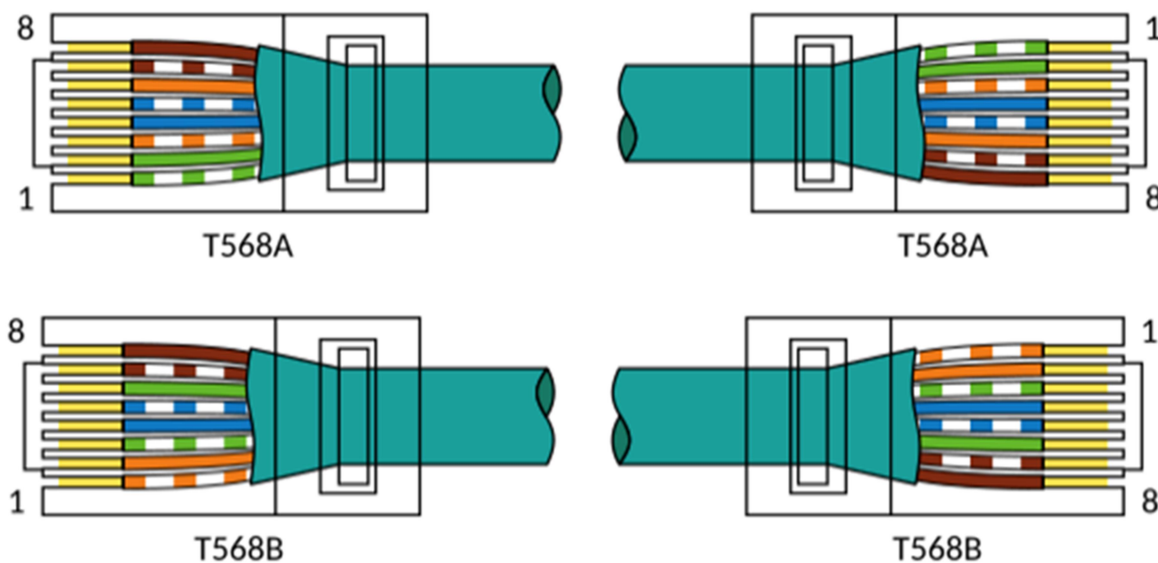


Рисунок 1.13 – Стандарти з'єднання провідників кабелю типу «кручена пара»

На відміну від мідної крученої пари, оптичні лінії зв'язку відзначаються високою пропускнуою здатністю та здатністю передавати дані на великі відстані з мінімальним загасанням сигналу. Вони є повністю нечутливими до електромагнітних та радіочастотних завад, що забезпечує високу надійність передачі даних. Оптичні кабелі складаються з тонких, дуже чистих скляних ниток, які діють як світлові хвильоводи, передаючи світлові імпульси з незначними втратами. Це робить їх незамінними для використання в магістральних мережах, міжбудинкових з'єднаннях та інших застосуваннях, де критично важливі якість і стабільність передавання даних.

Оптичне волокно поділяють на два основні типи: одномодове (*SMF*) і багатомодове (*MMF*).

Одномодове волокно (*single-mode fiber – SMF*) має дуже маленьке ядро і в ньому використовується лазерна технологія для передачі одного променя світла. Цей тип волокна призначений для передачі сигналів на великі відстані, що робить його ідеальним для використання в телекомунікаційних мережах, де потрібна передача даних на сотні кілометрів. Одномодове волокно мінімізує ефект дисперсії, що дозволяє передавати сигнали з меншими втратами і на більші відстані.



Рисунок 1.14 – Одномодове волокно

Багатомодове волокно (*multimode fiber – MMF*) має більше ядро, і в ньому використовуються світлодіодні (*LED*) випромінювачі для передавання світлових імпульсів. Світло в багатомодовому волокні проходить під різними кутами, що приводить до більшої дисперсії, ніж в одномодовому волокні. Це обмежує відстань передачі до 550 метрів, проте *MMF* є популярним у локальних мережах (*LAN*) завдяки меншій вартості *LED* випромінювачів. Багатомодове волокно підтримує швидкість передачі даних до 10 Гбіт/с.

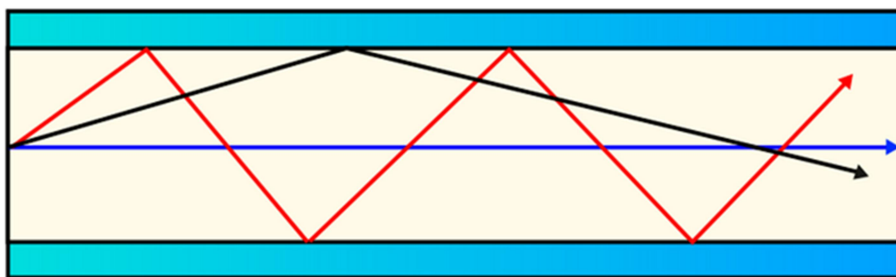


Рисунок 1.15 – Багатомодове волокно

Основною відмінністю між цими двома типами волокон є ступінь дисперсії, який вказує на розсіювання світлового імпульсу з часом. Через більшу дисперсію багатомодове волокно не може передавати сигнали на такі великі відстані, як одномодове волокно.

Оптоволокно використовується в кількох ключових сферах. У корпоративних мережах воно служить для прокладання магістральних ліній, що забезпечує високу пропускну здатність і надійність передачі даних. У технології «оптика до дому» (*FTTH*) оптоволокно застосовується для забезпечення постійного широкосмугового доступу до інтернету для домогосподарств і малого бізнесу. У міжміських та міжнародних мережах воно використовується провайдерами для з'єднання міст і країн. Також оптоволокно прокладається в підводних кабелях, що забезпечують надійні високошвидкісні з'єднання на великих відстанях під водою.

Оптичні конектори використовуються для забезпечення з'єднання між різними оптичними пристроями. Існує декілька типів конекторів, кожен із яких має свої характеристики і методи з'єднання.

ST-роз'єм (Straight-Tip) був одним із перших, який використовувався в оптоволоконних мережах. Він має байонетний механізм з фіксацією, що забезпечує надійне з'єднання. Цей тип роз'єму зазвичай застосовується в мережах локального та корпоративного рівня.



Рисунок 1.16 – ST-конектор

SC-роз'єм (Subscriber Connector), відомий також як квадратний або стандартний роз'єм, є одним із найпоширеніших роз'ємів для оптоволоконних з'єднань у локальних та глобальних мережах. SC-роз'єми можуть бути використані як із одномодовим, так і з багатомодовим оптоволоконном.

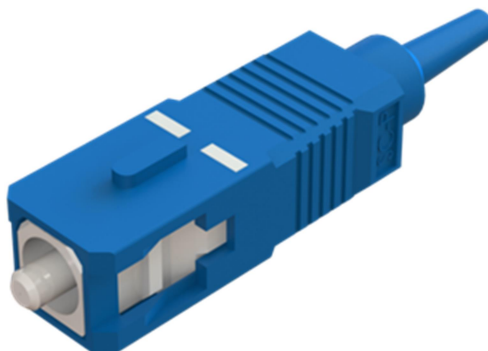


Рисунок 1.17 – SC-роз'єм

LC-роз'єм (Lucent Connector), відомий як компактний варіант SC-роз'єму, набуває дедалі більшої популярності завдяки своїм меншим розмірам, що дозволяє економити місце в розподільчих панелях. LC-роз'єми доступні як у простому, так і в дуплексному варіантах. Дуплексний LC-роз'єм дозволяє одночасно передавати і приймати сигнали через один з'єднувач, що зменшує кількість необхідних кабелів.

Також варто зазначити, що для повнодуплексної роботи оптоволоконний кабель раніше потребував використання двох окремих волокон для передавання і приймання сигналів. Але деякі сучасні роз'єми дозволяють передавати і приймати сигнали через один волоконний кабель за допомогою використання різних довжин хвиль світла.



Рисунок 1.18 – LC-роз'єм

Крім того, у роз'ємах оптоволоконних патч-кордів використовуються кольорові оболонки для розрізнення різних типів волокон. Наприклад, жовта оболонка вказує на одномодове волокно, тоді як помаранчева – на багатомодове.

Велика кількість пристроїв, наприклад, смартфони, планшети, ноутбуки, тощо, в наш час використовують бездротові методи передачі. Бездротове середовище забезпечує передачу даних за допомогою електромагнітних сигналів, що використовують радіохвилі для представлення двійкових даних. Це середовище надає користувачам високу мобільність, оскільки не потребує фізичних підключень для з'єднання з мережею. Такий підхід до підключення став основним у багатьох випадках, особливо з урахуванням зростаючої кількості бездротових пристроїв.

Однак бездротове середовище має певні обмеження. Наприклад, ефективність передачі сигналу може залежати від матеріалів будівель або рельєфу місцевості, що може обмежувати зону покриття. Бездротовий зв'язок також схильний до інтерференції, що може виникати через інші електронні пристрої, як-от бездротові телефони, мікрохвильові печі або флуоресцентні лампи.

Безпека є ще одним критичним аспектом. Оскільки бездротове середовище не вимагає фізичного кабелю для передачі даних, це створює ризики несанкціонованого доступу до мережі, що потребує ретельного адміністрування безпеки. Окрім того, оскільки бездротові локальні мережі (*WLAN*) працюють у напівдуплексному режимі, лише один пристрій може передавати або отримувати дані в певний момент часу. Це може призводити до зниження пропускної здатності мережі при збільшенні кількості користувачів, які одночасно використовують з'єднання.

Бездротове середовище представлено кількома основними типами технологій, що визначаються стандартами *IEEE* та використовуються для передачі даних на різних відстанях і в різних умовах.

WI-FI (IEEE 802.11) є найпоширенішою технологією бездротових локальних мереж (*WLAN*), що забезпечує підключення пристроїв до мережі. Ця технологія використовує протокол *CSMA/CA* для уникнення колізій під час передачі даних.

Bluetooth (IEEE 802.15) забезпечує зв'язок на коротких відстанях, створюючи бездротові персональні мережі (*WPAN*). Ця технологія використовується для підключення пристроїв на відстанях від одного до ста метрів.

WiMAX (IEEE 802.16) призначений для бездротового широкосмугового доступу і використовує топологію «точка-багатоточка». Ця технологія забезпечує передачу даних на великі відстані та використовується для організації бездротових мереж у масштабах міст або регіонів.

Zigbee (IEEE 802.15.4) створений для передачі даних на невеликі відстані з низькою швидкістю і низьким енергоспоживанням. Ця технологія широко використовується в промислових мережах та Інтернеті речей (*IoT*), наприклад, для керування освітленням або збору даних з різних пристроїв.

Таким чином, фізичний рівень мережі визначає способи передачі даних через різні типи середовищ. Мідні кабелі використовують електричні сигнали для передачі даних, забезпечуючи різну відстань та швидкість, але мають обмеження, такі як чутливість до електромагнітних завад і згасання сигналу на великих відстанях. Оптичні волокна передають дані за допомогою світлових імпульсів, що дозволяє досягти високих швидкостей і великих відстаней без значних втрат сигналу і зовнішніх перешкод. Бездротові технології забезпечують мобільність, використовуючи радіочастоти для передачі даних, але їх ефективність може бути знижена через перешкоди, обмежену зону покриття і питання безпеки. Кожен тип середовища має свої переваги і недоліки, що впливають на вибір у різних мережних сценаріях.