МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ETHERCHANNEL ТА ПІДВИЩЕННЯ НАДІЙНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ

Виконав: студент групи 1К-22
Спеціальності
123 Комп’ютерна інженерія
Олександр ПАЦЬОРА
Керівник:
Майя ЛЮТА

Черкаси 2026

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Циклова комісія комп'ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувачка циклової комісії КІ та ІТ

_____ Наталя ФАЛЬЧЕНКО

(підпис)

«_____» _____2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Пацьорі Олександру Володимировичу

1. Тема кваліфікаційної роботи Впровадження технології EtherChannel та підвищення надійності корпоративної мережі

Керівник роботи Люта Майя В'ячеславівна, викладач вищої категорії

затверджені наказом закладу фахової передвищої освіти від «06» жовтня 2025 року № 84/1-у.

2. Строк подання студентом кваліфікаційної роботи 02.06.2026

3. Вихідні дані до кваліфікаційної роботи: Рівень мережі – канальний. Емулятор мережевого устаткування – Cisco Packet Tracer. Кількість фізичних каналів – 2. Максимальна швидкість була розвинута до 1628 Мбіт/с. Вибраний LACP-протокол для стабільної роботи.

4. Зміст кваліфікаційної роботи: Вступ. 1 Основи комп'ютерних мереж. 2 Технологія агрегації каналів у комп'ютерних мережах. 3 Практична реалізація агрегації каналів. Висновки.

5. Дата видачі завдання 15.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	14.10.2025	
2	Розділ 1 Основи комп’ютерних мереж	09.12.2025	
3	Розділ 2 Технологія агрегації каналів у комп’ютерних мережах	10.03.2026	
4	Розділ 3 Практична реалізація агрегації каналів	28.04.2026	
5	Висновки	12.05.2026	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2026	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2026	
8	Подання кваліфікаційної роботи на затвердження завідувачці циклової комісії (за 7 днів до захисту)	10.06.2026	

Студент _____ Олександр ПАЦЬОРА
(підпис)

Керівник роботи _____ Майя ЛЮТА
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота присвячена дослідженню та практичній реалізації технології агрегації каналів EtherChannel для підвищення продуктивності, надійності та відмовостійкості корпоративних комп'ютерних мереж.

У роботі проведено аналіз технології Ethernet, моделі OSI, мережевого обладнання та середовищ передачі даних. Досліджено принципи агрегації та резервування каналів, визначено переваги використання технології EtherChannel для підвищення пропускної здатності мережі та забезпечення стабільності її роботи.

Розглянуто основні методи реалізації EtherChannel: протокол LACP, протокол PAgP та статичне налаштування. Розроблено модель корпоративної мережі у середовищі Cisco Packet Tracer та виконано практичне налаштування агрегації каналів між комутаторами.

Проведене тестування підтвердило ефективність використання EtherChannel для балансування навантаження та резервування мережевих з'єднань. Встановлено, що протокол LACP є найбільш доцільним рішенням для використання у сучасних корпоративних мережах завдяки відповідності стандартам та надійності роботи.

Результати роботи можуть бути використані під час проєктування та модернізації локальних мереж для забезпечення високої швидкості передачі даних, стабільності та відмовостійкості.

Ключові слова: КОМП'ЮТЕРНА МЕРЕЖА, ETHERNET, ETHERCHANNEL, АГРЕГАЦІЯ КАНАЛІВ, LACP, PAgP, РЕЗЕРВУВАННЯ, CISCO PACKET TRACER, ВІДМОВОСТІЙКІСТЬ.

ABSTRACT

The qualification work is devoted to the research and practical implementation of EtherChannel link aggregation technology to improve the performance, reliability, and fault tolerance of corporate computer networks.

The work analyzes Ethernet technology, the OSI model, network equipment, and data transmission media. The principles of link aggregation and network redundancy are investigated, and the advantages of using EtherChannel technology to increase network bandwidth and ensure stable operation are determined.

The main methods of EtherChannel implementation are considered: LACP protocol, PAgP protocol, and static configuration. A corporate network model was developed in the Cisco Packet Tracer environment, and practical configuration of link aggregation between switches was performed.

The conducted testing confirmed the effectiveness of EtherChannel technology for load balancing and network connection redundancy. It was determined that the LACP protocol is the most suitable solution for modern corporate networks due to its compliance with standards and reliable operation.

The results of the work can be used for designing and modernizing local networks to ensure high data transmission speed, stability, and fault tolerance.

Keywords: COMPUTER NETWORK, ETHERNET, ETHERCHANNEL, LINK AGGREGATION, LACP, PAgP, REDUNDANCY, CISCO PACKET TRACER, FAULT TOLERANCE.

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

IP – реалізація ієрархічної схеми мережевої адресації

LACP – протокол управління канальною агрегацією для управління групуванням разом декількох фізичних портів для формування одного логічного каналу

PAgP – протокол агрегування каналів; пропрієтарний протокол компанії Cisco Systems, що служить для автоматизації агрегування фізичних Ethernet-портів комутатора в один логічний

STP – мережевий протокол, що працює на другому рівні моделі OSI

RSTP – наступна версія STP, що характеризується значними вдосконаленнями, серед яких зменшення часу збіжності і вища стійкість

EtherChannel – технологія агрегації каналів, розробка компанії Cisco Systems

Ethernet – протокол кабельних комп’ютерних мереж, що працює на фізичному та канальному рівні мережевої моделі OSI

VLAN – віртуальна локальна комп’ютерна мережа

WAN – комп’ютерна мережа, що охоплює величезні території

ЗМІСТ

ВСТУП

Повсюдна комп’ютеризація є невід’ємною частиною сучасного життя. На поточний день практично будь-яка сфера життя неможлива без застосування того чи іншого комп’ютеризованого пристрою. Це сприяє збільшенню числа комп’ютерів і ускладненню взаємозв’язків між ними. Для спрощення взаємодії комп’ютерів їх об’єднують в мережу. Але й на даний момент підприємство потребує швидшу та надійнішу мережу.

Мережа складається з двох або більше комп’ютерів, пов’язаних між собою для спільного використання ресурсів (наприклад, принтерів та компакт-дисків), обміну файлами або забезпечення електронного зв’язку. Комп’ютери в мережі можуть бути пов’язані за допомогою кабелів, телефонних ліній, радіохвиль, супутників або інфрачервоних променів світла.

До двох дуже поширених типів мереж належать:

– Локальна мережа (LAN);

– Глобальна мережа (WAN).

Комп’ютери, підключені до мережі, широко класифікуються як сервери або робочі станції. Сервера, як правило, не використовуються безпосередньо людьми, а працюють постійно, щоб надавати "послуги" іншим комп’ютерам (та їхнім користувачам) у мережі. Послуги, що надаються, можуть включати друк та надсилання факсів, розміщення програмного забезпечення, зберігання та обмін файлами, обмін повідомленнями, зберігання та отримання даних, повний контроль доступу (захист) для ресурсів мережі та багато інших.

Актуальність теми

Мережеві ресурси дають змогу зекономити місце та час при організації колективної роботи. Проте питанням надійності та швидкості роботи мережевих систем часто не надають потрібного значення і в результаті доводиться зустрічатися зі збоями роботи мережі. Що може призвести до зупинки роботи самого підприємства, і негативно вплинути на його репутацію, та втратити як інвесторів так і клієнтів.

Мета роботи – на основі отриманої проблеми виконати аналіз даної мережі та підібрати правильний метод налаштування технології «ETHERCHANNEL», який дозволить підвищити пропускну здатність та надійність корпоративної мережі. На основі поставленої цілі, в роботі виділені наступні задачі:

– дослідити методи налаштування технології;
– дослідити переваги та недоліки технології;
– дослідити протоколи технології.

Об’єктом дослідження являється підвищення надійності мережі за допомогою технології

Предметом для дослідження є мережа побудована на основі Ethernet.

Методи дослідження. Робота заснована на базі аналізу корпоративної мережі та її топології. Інформаційна база була взята з підручників та від мережевих адміністраторів підприємства.

Робота складається з опису технології агрегування каналів, опису алгоритму та реалізації підсистем балансування навантаження каналів з прикладом програмного забезпечення та протоколів. Практична робота полягає у побудові надійної мережі у будь-якій реалізації, наприклад комутатор – комутатор.

РОЗДІЛ 1 ОСНОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Технологія Ethernet

Ethernet – це традиційна технологія підключення пристроїв до дротової локальної мережі (LAN) або глобальної мережі (WAN), що дозволяє їм спілкуватися між собою за допомогою протоколу – набору правил або загальної мови мережі. Ethernet описує, як мережеві пристрої можуть форматувати та передавати дані, щоб інші пристрої в тому ж сегменті локальної мережі чи мережі кампусу могли розпізнавати, отримувати та обробляти інформацію. Ethernet-кабель – це фізичний кабельний кабель, по якому проходять дані.

Підключені пристрої, що отримують доступ до географічно локалізованої мережі за допомогою кабелю – тобто за допомогою дротового, а не бездротового з'єднання – скоріше за все використовують Ethernet. Від бізнесу до геймерів різноманітні кінцеві користувачі залежать від переваг підключення Ethernet, які включають надійність та безпеку.

Порівняно з технологією бездротової локальної мережі (WLAN), Ethernet, як правило, менш вразливий до збоїв. Він також може запропонувати більший ступінь мережевої безпеки та контролю, ніж бездротова технологія, оскільки пристрої повинні підключатися за допомогою фізичних кабелів. Це ускладнює доступ сторонніх осіб до мережевих даних або викрадає смугу пропускання несанкціонованих пристроїв.

1.2 Використання та переваги Ethernet

Ethernet використовується для підключення пристроїв у мережі і досі є популярною формою мережевого підключення. Для локальних мереж, що використовуються певними організаціями – наприклад, офісами компаній, шкільними містечками та лікарнями – Ethernet використовується для високої швидкості, безпеки та надійності.

Спочатку Ethernet набув популярності завдяки своїй недорогій ціні порівняно з конкуруючими технологіями того часу, такими як Token Ring від IBM . У міру

вдосконалення мережевих технологій здатність Ethernet розвиватися та забезпечувати більш високий рівень продуктивності, одночасно підтримуючи зворотну сумісність, забезпечила її стійку популярність. Оригінальна пропускна здатність Ethernet 10 мегабіт в секунду збільшилася в десятки разів до 100 Мбіт / с у середині 1990-х років, Інститут Інженерів Електротехніки та Електроніки (IEEE) продовжує підвищувати продуктивність завдяки послідовним оновленням. Поточні версії Ethernet можуть підтримувати операції до 400 гігабіт в секунду (Гбіт/с).

Переваги і недоліки

Ethernet має багато переваг для користувачів, саме тому він став настільки популярним. Однак є і кілька недоліків.

Переваги:

– відносно низька вартість;
– зворотня сумісність;
– загалом стійкий до шуму;
– хороша якість передачі даних;
– швидкість;
– надійність;
– безпека даних – можна використовувати загальнодоступні брандмауери.

Недоліки:

– він призначений для мережі невеликої відстані;
– рухливість обмежена;
– використання довших кабелів може створити перехресні перешкоди;
– це погано працює з програмами реального часу або інтерактивними програмами;
– збільшення трафіку змушує швидкість Ethernet падати;
– приймачі не підтверджують отримання пакетів даних;

– під час усунення несправностей важко простежити, який саме кабель або вузол викликає проблему.

1.3 Принцип роботи Ethernet

IEEE вказує в сімействі стандартів, що називається IEEE 802.3, що протокол Ethernet торкається як рівня 1 (фізичний рівень), так і рівня 2 (рівень каналу передачі даних) на моделі мережевого протоколу Open Systems Interconnection (OSI).

– Ethernet визначає дві одиниці передачі: пакетну та фреймову. Кадр включає не тільки корисне навантаження даних, що передається, але також наступне: адреси фізичного контролю доступу до носія (MAC) як відправника, так і одержувача;

– позначення віртуальної локальної мережі (VLAN) та інформація про якість обслуговування (QoS);

– інформація про виправлення помилок для виявлення проблем передачі.

Кожен кадр загортається в пакет, що містить кілька байтів інформації, щоб встановити з’єднання та позначити, з чого починається кадр.

1.4 Модель OSI та її рівні

Модель OSI (модель взаємозв’язку відкритих систем) – це концептуальна основа, що використовується для опису функцій мережевої системи. (див. рис. 1.1).

Рисунок 1.1 – Опис моделі OSI

Модель OSI характеризує обчислювальні функції в універсальний набір правил та вимог для підтримки взаємодії між різними продуктами та програмним забезпеченням. У еталонній моделі OSI комунікації між обчислювальною системою поділяються на сім різних рівнів абстракції: фізичний, канальний, мережевий, транспортний, сеансовий, предсталення та додаток.

Створена в той час, коли мережеві обчислення були в зародковому стані, OSI була опублікована в 1984 році Міжнародною організацією зі стандартизації (ISO). Незважаючи на те, що вона не завжди безпосередньо відображається у певних системах, модель OSI все ще використовується сьогодні як засіб для опису архітектури мережі.

В моделі OSI є 7 рівнів які відповідають за свої функції.

Фізичний рівень

Найнижчий рівень моделі OSI стосується електричної або оптичної передачі необроблених неструктурованих бітів даних через мережу від фізичного рівня відправляючого пристрою до фізичного рівня приймального пристрою. Він може включати такі специфікації, як напруга, схема контактів, кабелі та радіочастоти. На фізичному рівні можна знайти «фізичні» ресурси, такі як мережеві концентратори, кабелі, ретранслятори, мережеві адаптери чи модеми.

Канальний рівень

На рівні каналу передачі даних безпосередньо підключені вузли використовуються для здійснення передачі даних від вузла до вузла, де дані упаковуються у кадри. Рівень каналу даних також виправляє помилки, які могли виникнути на фізичному рівні.

Рівень каналу даних охоплює два власні підрівні. Перший, контроль доступу до медіа (MAC), забезпечує контроль потоку та мультиплексування для передачі пристрою через мережу. Другий, контроль логічного зв’язку (LLC), забезпечує контроль потоку та помилок на фізичному носії, а також визначає лінійні протоколи.

Мережевий рівень

Мережевий рівень відповідає за отримання кадрів від рівня каналу передачі даних та їх доставку до призначених їм пунктів призначення на основі адрес, що містяться всередині кадру. Мережевий рівень знаходить пункт призначення за допомогою логічних адрес, таких як IP (Інтернет-протокол). На цьому рівні маршрутизатори є найважливішим компонентом, який використовується для буквального спрямування інформації туди, де вона повинна переходити між мережами.

Транспортний рівень

Транспортний рівень керує доставкою та перевіркою помилок пакетів даних. Він регулює розмір, послідовність і зрештою, передачу даних між системами та хостами. Одним з найпоширеніших прикладів транспортного рівня є TCP або протокол управління передачею.

Сеансовий рівень

Рівень сеансу контролює «розмови» між різними комп’ютерами. Сеанс або зв’язок між машинами налаштовується, управляється і завершується на пятому рівні. Послуги рівня сеансу також включають аутентифікацію та повторні підключення.

Рівень представлення

Шар презентації форматує або перекладає дані для рівня додатку на основі синтаксису або семантики, які приймає програма. Через це його іноді також називають синтаксичним шаром. Цей рівень також може обробляти шифрування та дешифрування, необхідні рівню програми.

Прикладний рівень

На цьому рівні як кінцевий користувач, так і прикладний рівень взаємодіють безпосередньо з програмним додатком. Цей рівень бачить мережеві послуги, що надаються програмам для кінцевих користувачів, таким як веб-браузер або Office 365. Рівень додатків визначає партнерів у зв’язку, доступність ресурсів та синхронізує зв’язок.

1.5 Мережеве обладнання

Для того щоб з’єднати певну кількість комп’ютерного обладнання в одну єдину систему вам не обійтися без ряду спеціальних пристроїв, призначених для вирішення такого типу завдань. Отже що таке мережеве обладнання.

Мережеве обладнання – це спеціальні пристрої, завданням яких є з’єднання комп’ютерного обладнання (або будь-якого іншого пристрою маючи можливість роботи з мережею) в одну або кілька взаємодіючих систем.

На перший погляд завдання з’єднати кілька пристроїв між собою здається нескладною і це дійсно так. Але якщо перед вами стане завдання з’єднати сотні пристроїв між собою, Вам доведеться трохи розібратися в особливостях роботи мережевих пристроїв.

Мережеві пристрої діляться на дві великі групи: активне мережеве обладнання та пасивне .

Активне обладнання

На відміну від пасивного, вимагає для своєї роботи підключення до джерела живлення. Перед такими пристроями зазвичай ставиться завдання управління потоками даних, які передаються між комп’ютерами, посилення або перетворення сигналу і тд.

До пристроїв подібного типу відносяться: комутатори, PoE-комутатори, роутери і бездротові точки доступу.

Пасивне обладнання

Не вимагає живлення від мережі. Його завдання – це розподіл сигналів або зниження їх рівня до необхідного.

При установці мережі проблем з налаштуванням пасивного обладнання зазвичай не виникає. А ось активне обладнання вимагає деякого розуміння принципів його роботи і відмінностей між типами пристроїв.

1.5.1 Комутатори

Мережевий комутатор (або світч) – це пристрій, який призначений для з’єднання декількох елементів комп’ютерного обладнання в одну мережу (див. рис. 1.2).

Рисунок 1.2 – Мережевий комутатор

Пристрій даного типу має більш просту структуру ніж роутер, він не займається розрахунками маршруту даних і передає дані строго від одного комп’ютера до іншого. Дані, які передаються від одного користувача до іншого, мають спеціальну інформацію, яка повідомляє світчу від кого прийшли дані і куди їх передати. При підключенні пристроїв в одну мережу комутатор створює комутаційну таблицю в яку записує номер порту і MAC-адреса кожного елемента

мережі. Це гарантує передачу даних строго від одного користувача до іншого позбавляючи всіх інших від зайвої обробки інформації.

Розрізняються всі світчи всього лише кількістю вхідних портів і пропускною спроможністю. Деякі додатково можуть бути оснащені модулями бездротового зв’язку.

1.5.2 POE-комутатори

POE-комутатор – мережевий пристрій, який має функцію подачі живлення на пристрої підключені по витій парі. Такими пристроями можуть бути точки доступу, IP-камери, мережеві концентратори і інші пристрої, які потребують подачі живлення подібним чином (див. рис. 1.3).

Рисунок 1.3 – POE комутатор

Простіше кажучи POE-комутатор є звичайним мережевим комутатором, який не тільки передає сигнал між пристроями, а також і живлення.

Відповідно до стандартом IEEE802.3af / at напруга на виході портів PoE становить 48 Вольт, що значно більше ніж потрібно типовим споживачам. Так для підключення ip-камери (яка живиться від мережі 12В) необхідно додаткове допоміжне обладнання, яке знижує напругу до певного рівня. Велике вихідне живлення в 48 вольт зробили не даремно – такий підхід дозволяє компенсувати електричні втрати при великій довжині кабелю.

1.5.3 Роутер

Роутер (іноді також називають маршрутизатор) – мережеве обладнання, яке призначене для організації бездротової мережі WI-Fi з можливістю підключення до інтернету (див. рис. 1.4).

Рисунок 1.4 – Роутер

Говорячи простими словами, роутери призначені для об’єднання деякої кількості пристроїв (телефонів, комп’ютерів, планшетів і тощо). В одну мережу Wi-Fi, яка часто має доступ до інтернету. Таким чином маючи одну точку підключення до інтернету (один кабель) ви можете підключити велику кількість пристроїв. При виборі роутера ви можете побачити такий пристрій як Wi-Fi-адаптер.

Wi-Fi адаптер – це невеликий пристрій, який купується для підключення комп’ютера до мережі Wi-Fi (тобто до роутера).

Роутер, на відміну від комутаторів, представлявляє собою більш складний і розумний пристрій, який не просто приймає і передає дані, а ще й здійснює управління мережею. Також для них характерно мати кілька портів для підключення проводів.

Вибираючи роутер ви побачите безліч пристроїв різних виробників. Найпопулярніші виробники маршрутизаторів – ASUS, TP-LINK, NETIS, TRENDNE. Всі пристрої випускаються в різних модифікаціях, вони відрізняються формами, стандартами, інтерфейсом.

1.5.4 Бездротові точки доступу

Роботу бездротової точки доступу можна порівняти з "подовжувачем" бездротового сигналу (див. рис. 1.5).

Рисунок 1.5 – Бездротова точка доступа

Має такий пристрій зазвичай один порт для підключення зовнішнього кабелю (для вхідного трафіку). Встановлювати таке обладнання можна як на вулиці, так і в приміщенні.

Працює точка в декількох режимах:

– режим «точка доступу» В даному режимі роботи точка приймає зовнішні підключення для об’єднання їх в одну бездротову мережу (ви підключаєтесь від комп’ютера через спеціальний Wi-Fi адаптер);

– режим «міст» У режимі міст точка працює на об’єднання фізично віддалених сегментів мережі в одну мережу. Простіше кажучи утворюється зв’язок між віддаленими об’єктами;

– режим «ретрансляція» (ретранслятор). Робота точки доступу в цьому режимі полягає в посиленні прийнятого сигналу. Точка доступу виступає в ролі приймально-передавача або повторювача. Слабкий сигнал, який виходить від іншої подібної точки, приймається, усиляється і передається далі до адресата.

Отже мережеве обладнання було розглянуто. Але це не все з чого складається сама мережа, для її створення потрібно мати хороший кабель як оптичний що

прокладається зовні будівлі, так і вита пара яка прокладається в середині цієї будівлі. Для цього і розглянемо види мережевих кабелів.

1.6 Мережеві кабелі

Мережеві кабелі використовуються для підключення одного мережевого пристрою до інших пристроїв мережі або для з’єднання двох або більше комп’ютерів, для мережевого користування принтером, сканером і тощо.

1.6.1 Оптоволоконні кабелі

Оптоволоконний кабель (він же волоконно-оптичний) – це принципово інший тип кабелю в порівнянні з іншими типами електричних або мідних кабелів. Інформація по ньому передається не електричним сигналом, а світловим. Головний його елемент – це прозоре скловолокно, по якому світло проходить на величезні відстані (до десятків кілометрів) з незначним ослабленням (див. рис. 1.6).

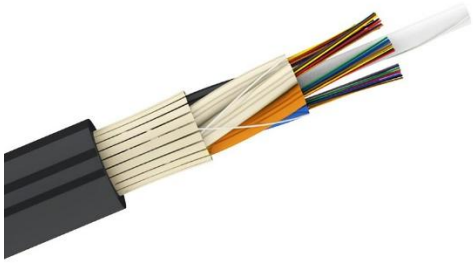

Рисунок 1.6 – Оптоволоконний кабель

Структура оптоволоконного кабелю дуже проста і схожа на структуру коаксіального електричного кабелю, тільки замість центрального мідного дроту тут використовується тонке (діаметром близько 1-10 мкм) скловолокно, а замість внутрішньої ізоляції – скляна або пластикова оболочка, що не дозволяє світлу виходити за межі скловолокна. В даному випадку ми маємо справу з режимом так званого повного внутрішнього відбиття світла від кордону двох речовин з різними коефіцієнтами заломлення (у скляній оболонкі коефіцієнт заломлення значно

нижче, ніж у центрального волокна). Металеве обплетення кабелю зазвичай відсутнє, так як екранування від зовнішніх електромагнітних перешкод тут не потрібне, однак іноді її все-таки застосовують для механічного захисту від навколишнього середовища (такий кабель іноді називають броньовим).

Оптоволоконний кабель володіє винятковими характеристиками по перешкодозахищеності і секретності переданої інформації. Ніякі зовнішні електромагнітні перешкоди в принципі не здатні спотворити світловий сигнал, а сам цей сигнал принципово не породжує зовнішніх електромагнітних випромінювань. Підключитися до цього типу кабелю для несанкціонованого прослуховування мережі практично неможливо, так як це вимагає порушення цілісності кабелю. Теоретично можлива смуга пропускання такого кабелю досягає величини 1012 Гц, що незрівнянно вище, ніж у будь-яких електричних кабелів. Вартість оптоволоконного кабелю постійно знижується і зараз приблизно дорівнює вартості тонкого коаксіального кабелю. Однак в даному випадку необхідне застосування спеціальних оптичних приймачів і передавачів, що перетворять світлові сигнали в електричні і назад.

Однак оптоволоконний кабель має і деякі недоліки. Найголовніший з них – висока складність монтажу (при установці роз’ємів необхідна мікронна точність, від точності відколу скловолокна і ступеня його полірування сильно залежить загасання в роз’ємі). Для установки роз’ємів застосовують зварювання або склеювання за допомогою спеціального гелю, що має такий же коефіцієнт заломлення світла, що і скловолокно. У будь-якому випадку для цього потрібна висока кваліфікація персоналу і спеціальні інструменти. Тому найчастіше оптоволоконний кабель продається у вигляді заздалегідь нарізаних шматків різної довжини, на обох кінцях яких уже встановлені роз’єми потрібного типу.

Хоча оптоволоконні кабелі і допускають розгалуження сигналів (для цього випускаються спеціальні розгалужувачі на 2-8 каналів), як правило, їх використовують для передачі. Адже будь-яке розгалуження неминуче сильно послаблює світловий сигнал, і якщо розгалужень буде багато, то світло може просто не дійти до кінця мережі.

Оптоволоконний кабель менш міцний, ніж електричний, і менш гнучкий (типова величина допустимого радіусу вигину становить близько 10-20 см). Чутливий він і до іонізуючих випромінювань, через які знижується прозорість скловолокна, тобто збільшується загасання сигналу. Чутливий він також до різких перепадів температури, в результаті яких скловолокно може тріснути. В даний час випускаються оптичні кабелі з радіаційно стійкого скла (стоять вони, природно, дорожче).

Оптоволоконні кабелі чутливі також до механічних впливів (удари, ультразвук) – так званий мікрофонний ефект. Для його зменшення використовують м'які звукопоглинальні оболонки.

Застосовують оптоволоконний кабель тільки в мережах з топологією «зірка» та «кільце». Ніяких проблем узгодження і заземлення в даному випадку не існує. Кабель забезпечує ідеальну гальванічну розв'язку комп'ютерів в мережі. У майбутньому цей тип кабелю, ймовірно, витіснить електричні кабелі всіх типів або, у всякому разі, сильно потіснить їх. Запаси міді на планеті виснажуються, а сировини для виробництва скла більш ніж достатньо.

Існують два різних типи оптоволоконних кабелів:

– багатомодовий, або мультимодових, кабель, дешевший, але менш якісний;

– одномодовий кабель, дорожчий, але має кращі характеристики.

Багатомодовий кабель

В багатомодовому кабелі траєкторії світлових променів мають помітний розкид, в результаті чого форма сигналу на приймальному кінці кабелю спотворюється. Центральне волокно має діаметр 62,5 мкм, а діаметр зовнішньої оболонки – 125 мкм (це іноді позначається як 62,5 / 125) (див. рис. 1.7). Для передачі використовується звичайний (НЕ лазерний) світлодіод, що знижує вартість і збільшує термін служби приймачів в порівнянні з одномодовим кабелем. Довжина хвилі світла в многомодовому кабелі дорівнює 0,85 мкм. Допустима довжина кабелю досягає 2-5 км. В даний час багатомодовий кабель – основний тип оптоволоконного кабелю, так як він дешевше і доступніше. Затримка поширення

сигналу в оптоволоконному кабелі не сильно відрізняється від затримки в електричних кабелях. Типова величина затримки для найбільш поширених кабелів становить близько 4-5 нс / м.

Одномодовий кабель

В одномодовому кабелі практично всі промені проходять один і той же шлях, в результаті чого всі вони досягають приймача одночасно, і форма сигналу практично не спотворюється. Одномодовий кабель має діаметр центрального волокна близько 1,3 мкм і передає світло тільки з такою ж довжиною хвилі (1,3 мкм) (див. рис. 1.7). Дисперсія і втрати сигналу при цьому не є значними, що дозволяє передавати сигнали на значно більшу відстань, ніж у випадку застосування многомодового кабелю. Для одномодового кабелю застосовуються лазерні приймачі, що використовують світло винятково з необхідною довжиною хвилі. Такі приймачі поки ще порівняно дорогі і не дуже довговічні. Однак в перспективі одномодовий кабель повинен стати основним завдяки своїми чудовими характеристикам.

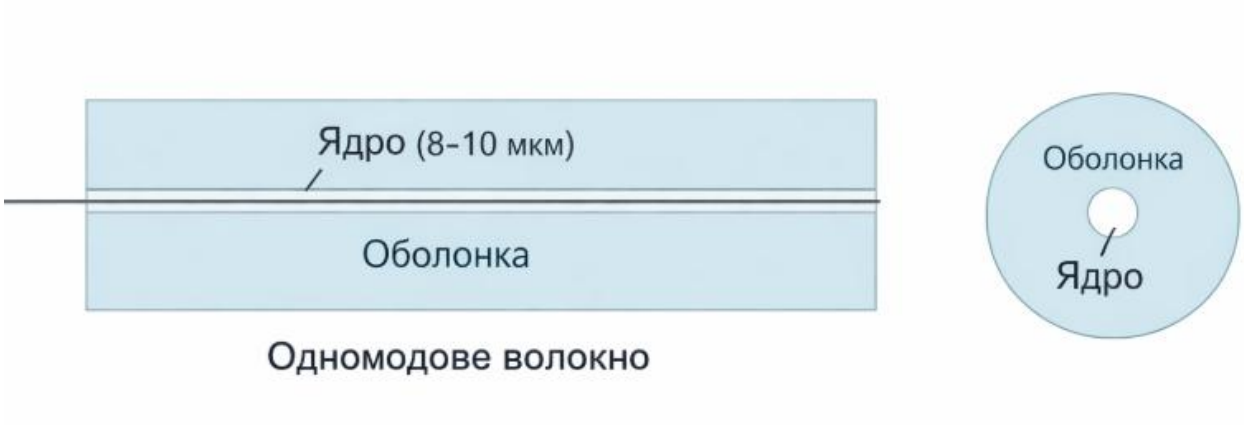

Рисунок 1.7 – Роз’єм RJ-45

1.6.2 Вита пара

Вита пара – це тип кабелю, який використовується для телефонного зв’язку та більшості сучасних мереж Ethernet. Пара проводів утворює ланцюг, який може передавати дані. Пари скручуються, щоб забезпечити захист від перехресних перешкод , шуму, що створюється сусідніми парами (див. рис. 1.8).

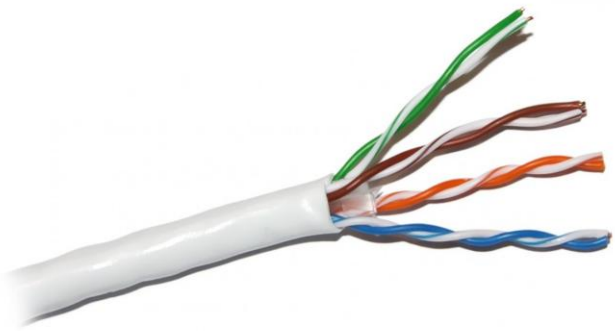

Рисунок 1.8 – Кабель витої пари

Коли електричний струм протікає по дроту, він створює невелике кругове магнітне поле навколо дроту. Коли два дроти в електричному ланцюзі розташовані близько один до одного, їх магнітні поля абсолютно протилежні один одному. Таким чином, два магнітних поля нейтралізують одне одного. Вони також нейтралізують будь-які зовнішні магнітні поля. Скручування проводів може посилити цей ефект скасування. Використовуючи ануляцію разом із скручуванням проводів, конструктори кабелів можуть ефективно забезпечити самоекранування пар проводів у мережевих носіях.

Існує два основних типи витої пари: неекранована вита пара (UTP) і екранована вита пара (STP).

UTP-кабель

UTP-кабель – це середовище, яке складається з пар проводів. Кабель UTP використовується в різних мережах. Кожен з восьми окремих мідних проводів в кабелі UTP покритий ізоляційним матеріалом. Крім того, дроти в кожній парі скручені навколо один одного.

Кабель UTP покладається виключно на ефект відміни, який виробляють скручені дротові пари, щоб обмежити погіршення сигналу, спричинене електромагнітними перешкодами та радіочастотними перешкодами. Щоб додатково зменшити перехресні перешкоди між парами в кабелі UTP, кількість скручувань в парах дротів змінюється. Кабель UTP часто встановлюється за допомогою роз’єму Registered Jack 45 (RJ-45). (див. рис. 1.9)

Рисунок 1.9 – Роз’єм RJ-45

RJ-45 – це восьмипровідний роз’єм, який зазвичай використовується для підключення комп’ютерів до локальної мережі (LAN), особливо до Ethernet.

UTP-кабель пропонує багато переваг. Кабель UTP повинен відповідати чітким специфікаціям, що регулюють, скільки скруток або плетінь дозволено на метр кабелю. Оскільки UTP має зовнішній діаметр приблизно 0,43 см (0,17 дюйма), його невеликий розмір може бути вигідним під час монтажу. Оскільки UTP має такий невеликий зовнішній діаметр, канали проводів не заповнюються так швидко, як інші типи кабелів. Це може бути надзвичайно важливим фактором, який слід враховувати, особливо при встановленні мережі в старому будинку. UTP-кабель простий у монтажі та є дешевшим за інші типи мережевих носіїв. Насправді UTP коштує менше за метр, ніж будь-який інший тип кабелів LAN. І оскільки UTP можна використовувати з більшістю основних мережевих архітектур, популярність продовжує зростати. Однак недоліки також пов’язані з використанням кабелів із витою парою. UTP-кабель більш схильний до електричних шумів та перешкод, ніж інші типи мережевих носіїв, і відстань між посиленнями сигналу для UTP коротша, ніж для коаксіального та волоконно-оптичного кабелів.

Хоча колись UTP вважали повільнішим при передачі даних, ніж інші типи кабелів, це вже не відповідає дійсності. Насправді UTP сьогодні вважається найшвидшим середовищем на основі міді. Далі узагальнено особливості кабелю UTP:

- швидкість і пропускна здатність – від 10 до 10000 Мбіт / с;
- середня вартість вузла – найменш дорога;
- розмір носія та роз’єму – невеликий;

– максимальна довжина кабелю – 100 м (короткий).

Найчастіше використовуються типи кабелів UTP:

– Категорія 1 – використовується для телефонного зв’язку. Не підходить для передачі даних;

– Категорія 2 – Здатність передавати дані зі швидкістю до 4 мегабіт в секунду (Мбіт / с);

– Категорія 3 – Використовується в мережах 10BASE-T. Може передавати дані зі швидкістю до 10 Мбіт / с;

– Категорія 4 – Використовується в мережах Token Ring. Може передавати дані зі швидкістю до 16 Мбіт / с;

– Категорія 5 – Може передавати дані зі швидкістю до 100 Мбіт / с.

– Категорія 5е – використовується в мережах, що працюють зі швидкістю до 1000 Мбіт / с (1 гігабіт на секунду [Гбіт / с]);

– Категорія 6 – Як правило, кабель категорії 6 складається з чотирьох пар 24 мідних проводів Американського дротового датчика (AWG). На даний момент кабель категорії 6 є найшвидшим стандартом для UTP.

Екранований кабель витої пари

Екранований кабель із витою парою (STP) поєднує в собі технології екранування, відміни та скручування дроту. Кожна пара проводів обмотана металевою фольгою. Потім чотири пари проводів обмотують загальною металевою оплеткою або фольгою, зазвичай 150-омним кабелем. STP зменшує електричні шуми як у кабелі (пара-пара, або перехресні перешкоди), так і зовні кабелю (EMI та RFI). STP зазвичай встановлюється за допомогою роз’єму для передачі даних STP, який створений спеціально для кабелю STP. Однак кабелі STP також можуть використовувати ті самі роз’єми RJ, що і UTP.

Хоча STP запобігає перешкодам краще, ніж UTP, він дорожчий і складніший в установці. Крім того, металевий екран повинен бути заземлений з обох кінців. Якщо він неправильно заземлений, екран діє як антена і вловлює небажані сигнали. Через свою вартість та труднощі з припиненням, STP рідко використовується в мережах Ethernet. STP в основному використовується в Європі.

Далі узагальнено особливості кабелю STP:

– швидкість і пропускна здатність – від 10 до 100 Мбіт / с;

– середня вартість на вузол – помірно дорога;

– розмір носія та роз’єму – від середнього до великого;

– максимальна довжина кабелю – 100 м (короткий).

Порівнюючи UTP та STP, майте на увазі наступні моменти:

– швидкість кабелів обох типів, як правило, задовільна для місцевих відстаней;

– це найдешевші носії для передачі даних. UTP дешевший за STP;

– оскільки більшість будівель вже підключені до UTP, багато стандартів передачі пристосовані для його використання, щоб уникнути дорогого підключення до кабелю іншого типу.

РОЗДІЛ 2 ТЕХНОЛОГІЯ АГРЕГАЦІЇ КАНАЛІВ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

2.1 Види реалізації агрегування каналів

Резервування є заходом забезпечення надійності, це використовується в мережі. Дублювання або вже як ми називали резервування каналів зв'язку підвищує пропускну здатність та надає можливість реагувати на проблеми за відмовами в окремих каналах (див. рис. 2.1).

Рисунок 2.1 – Приклад резервування каналів

Використання різних каналів дозволяє, забезпечити багаторівневу систему резервування каналів передачі даних:

– використання багатьох протоколів при організації передачею даних;

– алгоритм перебирання каналів обміну даних.

Кінцева ціль резервації каналів обміну даних виконується за для того, щоб виключення тих вузлів, відмова яких може вивести з ладу всю роботу системи. Так давайте розглянемо приклад, якщо банк займається великими фінансовими розрахунками та укладенням договорів, підключений до центрального сервера за допомогою загальної системи передачі даних через єдиний канал зв'язку. То відмова цього каналу зв'язку може призвести до непрацездатності самого банку, та втрати клієнтів. А втрата клієнтів призведе до втрати великих обсягів фінансів і самого банкротства банку. Отже, резервування каналів дозволяє системі залишатись «на плаву» на період ремонтування каналу, який вийшов за ладу.

Дублювання каналів використовуються для таких цілей:

– регулювання навантаження на мережу підвищення кількості резервних каналів збільшує пропускну здатність на виході, для цього і використовується агрегація каналів;

– покращення працездатності мережевого обладнання – резервні канали між вузлами дають змогу у разі виникнення збоїв на одному каналі перемикатися на запасні лінії зв’язку у разі відмови основної.

Другу мету можна досягти в рамках першої але пріоритет найчастіше віддається до підвищення надійності (але це не завжди так). У мережах для промисловості кількість даних менше, ніж у мережах для офісу, але вимоги для відмовостійкості мережі повинна бути вище. На постійну доставку даних орієнтовані мережеві технології та промислові протоколи зв’язку. Але завжди бувають несправності, їх неможливо виключити, але можливо призвести наслідки до мінімальних втрат.

У термінології комп’ютерних мереж вирівнювання навантаження трафіку – це розподіл завдань в мережі, де передача даних між двома та більше мережевими каналами зв’язку з метою оптимізації використання ресурсів, зниження часу обміну інформації, та забезпечення резервування. Агрегування каналів – це один із методів вирівнювання навантаження . Отже, що таке агрегація каналів?

Агрегування каналів (link aggregation на англ.) – технологія об’єднання декількох паралельних фізичних каналів в один логічний, це дозволяє нам збільшити пропускну здатність і підвищити надійність мережі. Агрегування каналів має декілька альтернативних назв, які використовуються в жаргонах мережевих адміністраторів:

– трекінг портів;

– пулінг мережевих карт;

– склейка адаптерів;

– Ether trunk – це назва агрегування каналів Cisco.

2.2 Протокол LACP

LACP (Англ Link aggregation control protocol) – це основний протокол для агрегації каналів. Як вказано в IEEE 802.3ad, реалізує динамічну агрегацію і дезагрегацію каналів, дозволяє комутаторам з підтримкою LACP на обох кінцях обмінюватись блоками даних протоколу керування агрегації каналів (LACPDU).

Історія виникнення протоколу. До середини 1990-х років більшість виробників мережевих комутаторів включили можливість агрегування як власного розширення для збільшення пропускної здатності між своїми комутаторами. Кожен виробник розробив свій метод, що призвело до проблем сумісності. Робоча група IEEE 802.3 взяла на себе дослідницьку групу зі створення стандарту функціонально сумісного канального рівня (тобто охоплює як фізичний, так і канальний рівні) на зборах в листопаді 1997 року. Група швидко погодилася включити функцію автоматичної настройки, яка також додає надмірності. Це стало відомо як протокол управління агрегацією каналів (LACP).

2.3 Агрегація на прикладі LACP

LACP надає стандартний механізм узгодження, який комутатор може використовувати для створення та включення агрегованого каналу в залежності від його конфігурації. Після того як агрегований канал сформований, LACP відповідає за його підтримку. LACP коректує канал, якщо статус агрегованого каналу змінюється.

Наприклад, (див. рис. 2.2) чотири інтерфейси на DeviceA повинні бути підключені до відповідних інтерфейсів на DeviceB, і всі ці інтерфейси об’єднані в Eth-Trunk. Однак, один інтерфейс на DeviceA підключений до інтерфейсу на DeviceC. В результаті, DeviceA може відправляти дані, призначені для DeviceB, на DeviceC. В ручному режимі ця несправність залишається непомітною.

В цьому випадку, якщо LACP включений на DeviceA й DeviceB, Eth-Trunk вибирає тільки активні канали (канали підключені до DeviceB) для переадресації даних після узгодження. Дані, відправлені DeviceA, призначені для DeviceB, досягають тільки DeviceB.

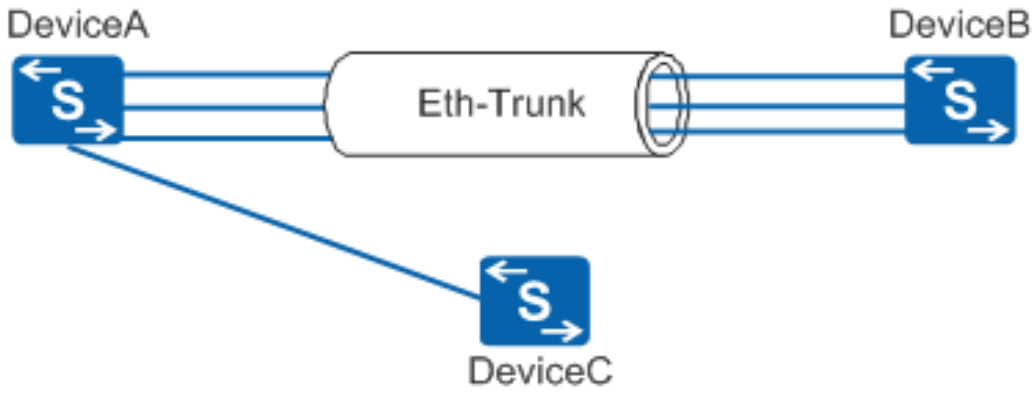

Рисунок 2.2 – Приклад неправильного з’єднання Eth-Trunk

Поняття в LACP включають:

– Пріоритет системи LACP

Пріоритети системи LACP визначають послідовність, в якій пристрої на двох кінцях Eth-Trunk вибирають активні інтерфейси для приєднання до LAG. Для того, щоб створити LAG, обидва пристрої повинні вибрати однакові інтерфейси як активні інтерфейси. Для цього один пристрій (з вищим пріоритетом) відповідає за вибір активних інтерфейсів. Потім інший пристрій (з нижчим пріоритетом) вибирає ті самі інтерфейси, що й активні інтерфейси. При порівнянні пріоритетів менші значення мають вищий пріоритет.

– Пріоритет інтерфейсу LACP

Пріоритети інтерфейсу LACP впливають на те, які інтерфейси Eth-Trunk обрані активними інтерфейсами. Менше числове значення представляє вищий пріоритет. Інтерфейси з найвищим пріоритетом інтерфейсу LACP стають активними інтерфейсами.

– M: N резервне копіювання інтерфейсів

Режим LACP також називається режимом M: N, де M означає кількість активних каналів, а N – кількість резервних каналів. Цей режим гарантує високу надійність і дозволяє збалансувати навантаження між M активними каналами.

На рисунку 2.3 між двома пристроями встановлено канал M + N з однаковими атрибутами (в одному і тому ж LAG). Коли дані передаються по агрегованому

каналу, трафік балансується навантаження між M активними каналами, без даних, що передаються через N резервних каналів. Отже, фактична пропускна здатність агрегованої лінії зв'язку є сумою пропускної здатності (M + N-1) каналів.

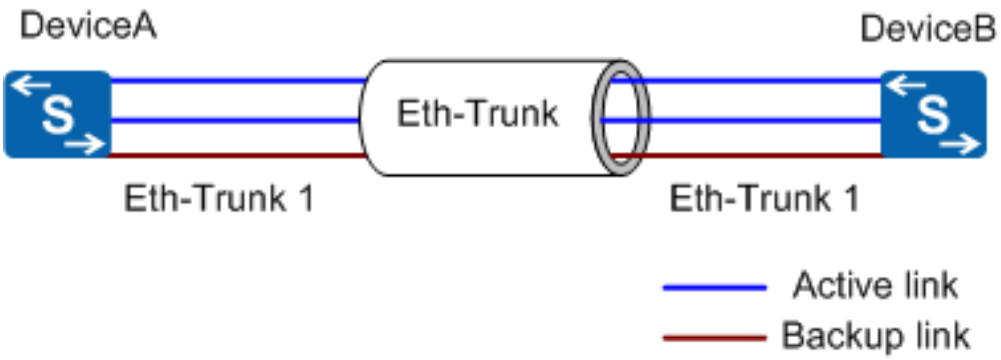

Рисунок 2.3 – Мережа резервного копіювання M: N

Щоб протокол запрацював його потрібно перевести в активний режим або пасивний. Різниця в тому, що активний режим відразу включає протокол LACP, а пасивний режим включить протокол LACP, якщо виявить LACP-повідомлення від сусіда. Відносно, щоб запрацювало агрегування з LACP, потрібно щоб обидва були включені в активний режим, або один працював в активному режимі, а інший в пасивному (див. табл. 2.1).

Таблиця 2.1 – Режими роботи LACP

Режими	Активний режим	Пасивний режим
Активний режим	Так	Так
Пасивний режим	Так	Ні

2.4 Технологія EtherChannel

EtherChannel це технологія агрегації портів, розроблена компанією Cisco, яка забезпечує відмовостійкість каналу між комутаторами, маршрутизаторами та серверами. Технологія EtherChannel дозволяє об'єднати декілька фізичних каналів Ethernet, Fast Ethernet або Gigabit Ethernet в один логічний канал.

EtherChannel дає об'єднувати до 8 портів Ethernet зі швидкістю 100 Мбіт/с, 1 Гбіт/с або 10 Гбіт/с. Максимальна швидкість яку можна розвинути за допомогою

цієї технології до 80 Гбіт/с. При цьому від одного до семи портів можуть бути резервними

Канал може встановлюватися між маршрутизаторами, комутаторами й мережевими адаптерами на сервері. Всі мережеві адаптери, які є частиною каналу, отримують один MAC-адресу, що робить канал прозорим для мережевих додатків. Балансування трафіку між портами провадиться на основі хеш-функції над MAC-адресу, IP-адресу або TCP і UDP портом джерела або одержувача. Таким чином, в деяких несприятливих випадках, весь трафік може передаватися по одній фізичному з'єднанню.

Для узгодження EtherChannel і Агрегація посилань використовуються два протоколи. Ми можемо налаштувати EtherChannel у комутаторах Cisco трьома способами:

– протокол агрегації портів (PAgP) – власний протокол Cisco;

– IEEE Link Aggregation Protocol (LACP) – відбивний стандарт;

– ручна настройка EtherChannel – без використання яких-небудь протоколів узгодження, перероблених вище.

Протокол агрегації портів (PAgP) та протокол управління агрегацією каналів (LACP) можуть використовуватися для узгодження каналів EtherChannel. Протокол агрегації портів (PAgP) – це власний протокол Cisco. Тому PAgP можна використовувати для узгодження каналів EtherChannels лише між комунікаторами Cisco.

Протокол управління агрегацією каналів (LACP) – це відбивний стандарт, визначений в IEEE 802.3AD. Використовуючи протокол управління агрегованим каналами (LACP), комутатори Cisco можуть узгоджувати агрегування каналів з комутаторами від різних постачальників, які підтримують протокол 802.3AD.

Протокол агрегації портів (PAgP) або протокол управління агрегацією каналів (LACP) використовується комутатором для визначення особистості партнерів, можливостей партнерів, а також своїх і можливостей інтерфейсу. Протокол агрегації портів (PAgP) або протокол управління агрегацією каналів (LACP) об'єднує інтерфейси з аналогічною конфігурацією в одному логічному

каналі та представляє групу для протоколу зв’язку з дерева (STP) як один порт комутатора.

2.5 Агрегування каналів NICTeaming

NICTeaming – це технологія об’єднання мережевих карт в групу, поширений метод групування фізичних мережевих адаптерів для підвищення продуктивності та надмірності. Основними перевагами об’єднання мережевих адаптерів є балансування навантаження (перерозподіл трафіку по мережах) і аварійне перемикання (забезпечення безперервності мережі в разі відмови обладнання системи) без необхідності в декількох фізичних з’єднаннях. По суті, об’єднання мережевих карт – це стратегічний план, який може збільшити час безвідмовної роботи.

Підключення декількох мережевих кабелів від сервера до декількох фізичних комутаторів – це метод досягнення відмовостійкості в мережевого налаштування фізичного сервера. Однак в цьому випадку балансування навантаження відсутня, навіть якщо на сервері постійно активні кілька IP-адрес. З іншого боку, об’єднання мережевих адаптерів в групи – це функція Windows Server, яка дозволяє групувати мережеві адаптери в групи. Члени групи – це мережеві адаптери, які використовуються для зв’язку з комутатором. Командні інтерфейси – це віртуальні мережеві адаптери, створені при створенні команди. Отже, об’єднання мережевих адаптерів підтримує з’єднання з кількома фізичними комутаторами, але використовує один IP-адреса. Це забезпечує доступне балансування навантаження і миттєву відмовостійкість (замість очікування тайм-ауту / оновлення записів DNS).

2.6 Мережева карта та її об’єднання

Об’єднання мережевих карт – це. це технологія угруповання фізичних або віртуальних мережевих карт в один або кілька програмних мережевих адаптерів, що розв’язують проблеми в разі збою обладнання.

Мережева плата – це електронний пристрій, який з’єднує комп’ютер до комп’ютерної мережі, як правило, в локальній мережі. Вважається частиною

комп’ютерного обладнання. Більшість сучасних комп’ютерів підтримують внутрішній контролер мережевого інтерфейсу, вбудований безпосередньо в материнську плату, а не як зовнішній компонент (див. рис. 2.4).

Рисунок 2.4 – Мережева карта

Мережеві карти дозволяють комп’ютеру обмінюватися даними з мережею. Для підключення мережеві карти використовують відповідний протокол, наприклад CSMA / CD . Мережеві карти, як правило, реалізують перші два рівні моделі OSI, тобто фізичний рівень, і рівень передачі даних. Існують старіші мережеві протоколи, такі як ARCNET, представлений в 1977 році, LocalTalk або Token Ring, але сьогодні більшість мережевих карт використовують Ethernet.

2.6.1 Переваги об’єднання мережевих карт

Основними перевагами є, об’єднання мережевих адаптерів є найкраще балансування навантаження і підвищення відмовостійкості.

Балансування навантаження

У випадку об’єднання мережевих адаптерів, мережевий трафік рівномірно розподіляється між усіма активними мережевими адаптерами. Отже, вихідний трафік автоматично балансується між доступним фізичним мережевими адаптерами на основі адреси призначення. Вихідний трафік контролюється комутатором та маршрутизацією трафіку на сервер. Сервер не контролює фізичний трафік NIC.

Відмовостійкість

Додаткова перевага об’єднання мережевих адаптерів – більш висока відмовостійкість. Якщо одна з основних фізичних мережевих адаптерів виходить з ладу або якщо патч-корд від мережевої карти відключений, сервер виявляє несправність і автоматично переміщує трафік на іншу мережеву карту. Це знижує ймовірність виходу з ладу всієї мережі, тим самим підвищуючи надійність системи.

2.6.2 Режими об’єднання мережевих карт

Два режими об’єднання мережевих карт – це незалежний перемикач та залежний від перемикача.

Незалежний перемикач

У режимі незалежного перемикання комутатори, до яких підключені члени групи NIC, не знають про присутність команди NIC. Отже, ці комутатори не знають, як розподілити мережевий трафік між членами команди NIC, і замість цього вони розподіляють вхідний мережевий трафік між членами команди NIC.

Використання режиму незалежного перемикання з динамічним розподілом розподіляє навантаження мережевого трафіку на основі хеш-адреси порту протоколу управління передачею (TCP). Алгоритм динамічного балансування навантаження перерозподіляє потік для оптимізації використання смуги пропускання членів команди, щоб гарантувати, що окремі передачі потоку переміщуються від одного активного члена команди до іншого. Алгоритм також розглядає можливість того, що перерозподіл трафіку спричиняє невпорядковане доставлення пакетів, і вживає заходів, які можуть мінімізувати цю можливість.

Залежний перемикач

У режимі залежності від комутатора комутатор, підключений до членів команди NIC, визначає розподіл вхідного мережевого трафіку між членами команди NIC. Отже, підключений комутатор має незалежність від визначення способу розподілу трафіку між членами команди мережевої карти. Усі члени команди повинні бути підключені до одного фізичного комутатора або комутатора

з декількома шасі, який використовує ідентифікатор комутатора. Режим перемикання залежних додатково має наступні два варіанти:

– Статичне об’єднання. Потрібна ручна конфігурація комутатора, а також хосту для ідентифікації посилань, що утворюють команду. Оскільки ця конфігурація статична, немає додаткового протоколу, який допомагає комутатору та хосту виявляти помилки, такі як неправильно підключені кабелі. Це може спричинити невдачу команди. Зазвичай цей режим підтримується комутаторами класу сервера.

– Динамічне об’єднання. Протокол управління агрегацією посилань (LACP). Ідентифікує зв’язки, з’єднані між комутатором і хостом. Це, своєю чергою, дозволяє автоматично створювати команду. Цей режим підтримується всіма комутаторами класу сервера, але оператори мережі повинні ввімкнути LACP на порту комутатора. Командування NIC працює в активному режимі LACP з коротким таймером, і на сьогодні немає механізму зміни таймера або режиму LACP.

Використання режиму залежності від комутатора з динамічним розподілом розподіляє навантаження мережевого трафіку на основі хешу адрес транспортних портів, який модифікується алгоритмом динамічного балансування навантаження. Цей алгоритм перерозподіляє потоки, оптимізує використання смуги пропускання членів команди та дозволяє окремим передачам потоків переходити від одного активного члена команди до іншого. Алгоритм також зменшує можливість неповноцінного постячання, але враховує його можливість.

2.7 Режими балансування навантаження

Хеш адреси

У цьому режимі створюється хеш на основі адресних компонентів пакету. Цей хеш присвоюється одному з доступних адаптерів, таким чином створюючи розумний баланс між доступними адаптерами.

Windows PowerShell можна використовувати для вказівки таких компонентів хешування, як:

– вихідні та цільові порти TCP та IP-адреси джерела та призначення;

– лише адреса джерела та пункту призначення;

– лише адреси джерела та пункту призначення доступу до медіа (MAC).

Порти TCP створюють детальний розподіл потоків трафіку, що призводить до менших потоків. Однак це не можна використовувати для трафіку, який не базується на TCP або User Datagram Protocol (UDP). У таких випадках хеш використовує хеш IP-адреси або хеш MAC-адреси.

Hyper-V Port

У цьому режимі команди NIC, налаштовані на хостах Hyper-V, надають незалежні MAC-адреси віртуальним машинам (VM). MAC-адреса віртуальних машин або портів віртуальної машини, підключених до комутатора Hyper-V, використовуються для розподілу мережевого трафіку між членами NIC-групи. Команди NIC, створені у віртуальних машинах, не можна налаштувати за допомогою режиму балансування навантаження Hyper-V Port, і натомість йому потрібен режим хеш-адреси.

Динамічний

У цьому режимі вихідні навантаження розподіляються на основі порту TCP та IP-адреси. Цей режим врівноважує навантаження в режимі реального часу, щоб забезпечити переміщення заданого вихідного потоку між членами команди. Вхідні навантаження розподіляються, так само як порт Hyper-V. Він використовує обидва аспекти адресного хешу та Hyper-V і є найбільш ефективним режимом балансування навантаження.

2.8 Технології та рішення промислових мереж Ethernet

Одне з ключових вимог для промислових мереж – це відсутність в топології замкнутих маршрутів, тобто повинен бути єдиний канал зв’язку між відправником та одержувачем. Поява замкнутого маршруту в таких мережах призведе до зростання трафіку і, отже, перевантаження мережі, тому в традиційних мережах Ethernet уникають виникнення таких петель. У промислових мережах задача протоколів – це моніторинг дублювання каналів за метою недопущення

перерозподілу трафіку в надзвичайних ситуаціях. Протокол резервування повинен гарантувати логічне існування одного шляху для обміну даними. З існуючих фізичних каналів зв'язку один вибирається на роль основного каналу, інші є резервними.

Таке вперше застосовувалось в протоколі STP, який відстежував стан каналів і при обриві перенаправляє трафік на резервний канал. Це каже про те що зв'язок втрачається на момент аналізу неполадок основного каналу і поки не буде активований новий канал зв'язку. Час обриву залежить від двох факторів, це розмір мережі та складність її топології.

2.9 Протокол RSTP / MSTP

Протокол RSTP це вдосконалений протокол STP. RSTP забезпечує підтримку безліч мережевих топологій і робить так що між двома вузлами мережі в кожний момент часу існує єдиний маршрут передачу даних і виділяється деревоподібна структура. А всі з'єднання, які не ввійшли в активний «дерево», вважаються резервними та залишаються поки не буде змінена топологія.

Протокол RSTP підтримує досить велику кількість вузлів, забезпечує велику швидкість відновлення зв'язку. Але точний час відновлення зв'язку вказати не можливо, бо все залежить від місця виникнення обриву.

Даний недолік можна вирішити, якщо змінити топологію мережі кільцевою структурою. Таким чином, можна досягнути часу відновлення мережі до 100 мс і менше.

MSTP – нова ітерація описаного протоколу резервованих «дерев», і працює вона за тим же принципом. Якщо RSTP працює незалежно від віртуальних мереж VLAN, то структури MSTP, навпаки, існують в складі віртуальної мережі і таким чином забезпечують більше зручностей і свобод в плані можливих топологій і розподілу навантаження. Обидва протоколу сумісні між собою і можуть бути реалізовані всередині однієї мережі.

2.10 Основи правильно агрегування каналів

Для агрегування каналів мінімально потрібно 2 кабелю максимальна кількість 8 каналів. Але рекомендовано використовувати 2, 4 або 8 інтерфейсів. А все через алгоритм хешування, який придумала Cisco. Алгоритм вираховує значення хешу від 0 до 7 (див. таб. 2.2).

Таблиця 2.2 – Алгоритм вирахування хеша

4	2	1	Десяткове значення
0	0	0	0
0	0	1	1
0	1	1	3
1	0	0	4
0	0	1	1
1	0	1	5
1	1	0	6
1	1	1	7

Дана таблиця відображає 8 значень в двоїчному і десятковому вигляді.

На підставі цієї величини вибирається порт EtherChannel і присвоюється значення. Після цього порт отримує якусь «маску», яка відображає величини, за які той порт відповідає. Ось приклад. Є два фізичні інтерфейси, які будуть об’єднуватись в один port-channel.

Значення розкидали таким чином:

1. 0x0 - fa0 / 1;
2. 0x1 - fa0 / 2;
3. 0x2 - fa0 / 1;
4. 0x3 - fa0 / 2;
5. 0x4 - fa0 / 1;
6. 0x5 - fa0 / 2;
7. 0x6 - fa0 / 1;
8. 0x7 - fa0 / 2.

В результаті отримаємо, що половину значень або патернів візьме на себе fa0 / 1, а другу половину fa0 / 2. Тобто отримуємо 4: 4. В такому випадку балансування буде працювати правильно (50/50).

Складаємо аналогічне зіставлення, але замість двох каналів буде використовуватись 3 канали:

1. 0x0 - fa0 / 1;
2. 0x1 - fa0 / 2;
3. 0x2 - fa0 / 3;
4. 0x3 - fa0 / 1;
5. 0x4 - fa0 / 2;
6. 0x5 - fa0 / 3;
7. 0x6 - fa0 / 1;
8. 0x7 - fa0 / 2.

В цьому прикладі показано, що fa0 / 1 візьме на себе 3 патерни, fa0 / 2 теж 3 патерни, а fa0 / 3 2 патерну. Відповідно навантаження буде розподілена не рівномірно. Отримаємо 3:3:2. Тобто перші два канали будуть завжди завантаженіші, ніж третій.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ АГРЕГАЦІЇ КАНАЛІВ

3.1 Налаштування агрегації каналів на основі протоколу LACP

Проведення реалізації кваліфікаційної роботи буде в середовищі Cisco Packet Tracer.

Огляд протоколу LACP. Щоб заробив цей протокол, віртуальний інтерфейс потрібно перевести в режим active або passive. Відмінність режимів в тому що, режим active відразу включає протокол LACP, а режим passive включить протокол, якщо виявить LACP-повідомлення від сусіда. Відповідно, щоб запрацювало агрегування каналу потрібно щоб обидва віртуальні порти були в режимі active, або один в active, а інший в passive.

Є 2 комутатори, з'єднані 2 проводами (див. рис. 3.1). Один канал активний (горить зеленим), а другий резервний (горить помаранчевим) через спрацювання протоколу STP. Але потрібно обидва канали об'єднати воєдино. Тоді протокол STP буде вважати, що це один провід і перестане блокувати.

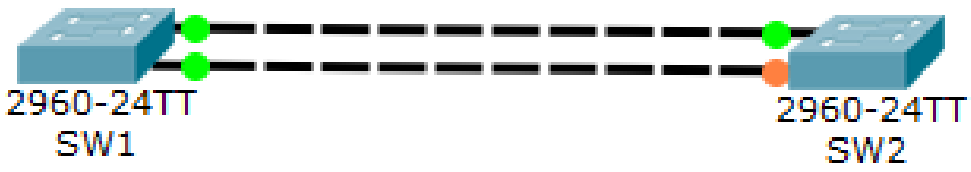

Рисунок 3.1 – З'єднання двох комутаторів

Для моделювання агрегації каналів, необхідно по черзі зайти в кожний комутатор в середовищі Cisco Packet Tracer та виконати налаштування портів пристрою (див. рис. 3.2).

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

SW1(config-if)#channel-group 1 mode active
SW1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed state to up

SW1(config)#interface fastEthernet 0/2
SW1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

SW1(config-if)#channel-group 1 mode active
SW1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

```

Рисунок 3.2 – Команди налаштування портів комутатора SW1

Налаштування портів містить в собі наступні команди:

1. заходимо на інтерфейс комутатора;
2. вимикаємо його, щоб не було проблем з STP, який раптом може його заблокувати;
3. створюємо інтерфейс port-channel 1 (це і буде віртуальний інтерфейс агрегованого каналу) і переводимо його в режим active. Creating a port-channel interface Port-channel 1 – з'являється службове повідомлення про його створення;
4. включаємо інтерфейс;
5. заходимо на другий інтерфейс;
6. вимикаємо;
7. визначаємо в port-channel 1;
8. вимикаємо.

На цьому налаштування на першому комутаторі закінчена. Для достовірності можна набрати команду show EtherChannel port-channel (див. рис. 3.3):

```
SW1#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:00h:08m:44s
Logical slot/port   = 2/1       Number of ports = 2
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    Active             0
  0     00     Fa0/2    Active             0
Time since last port bundled:    00d:00h:08m:43s    Fa0/2
```

Рисунок 3.3 – Результати виконання команди

На зображені видно, що є такий port-channel і в ньому присутні обидва інтерфейси.

Переходимо до налаштування наступного пристрою (див. рис. 3.4).

```
SW2(config)#interface range fastEthernet 0/1-2
SW2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

SW2(config-if-range)#channel-group 1 mode passive

Creating a port-channel interface Port-channel 1

SW2(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

```

Рисунок 3.4 – Команди налаштування портів комутатора SW2

1. переходимо до налаштування відразу декількох інтерфейсів;
2. вимикаємо їх;
3. створюємо port-channel та переводимо в режим passive (увімкнеться, коли отримає LACP-повідомлення);
4. вмикаємо знову.

Після цього канал узгоджується. Результат команди show EtherChannel summary зображений на рис. 3.5.

```
SW1#show etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-----------

1 Po1(SU) LACP Fa0/1(P) Fa0/2(P)
```

Рисунок 3.5 – Результат команди show EtherChannel summary

Тут зображено групу port-channel, використовуваний протокол, інтерфейси і їх стан. В такому випадку параметр SU говорить про те, що виконано агрегування другого рівня і те, що цей інтерфейс використовується. А параметр P вказує, що інтерфейси в стані port-channel (див. рис. 3.6).

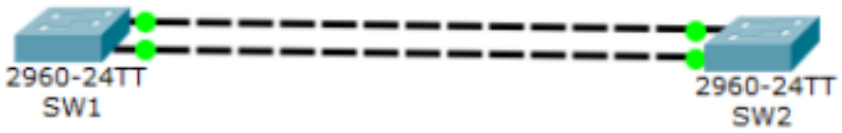

Рисунок 3.6 – Успішне агрегування каналів

Всі канали зелені й активні. STP на них не спрацьовує. Дослідимо роботу LACP. Включаємо режим симуляції і вибираємо тільки фільтр LACP, щоб інші не відволікали (див. рис. 3.7).

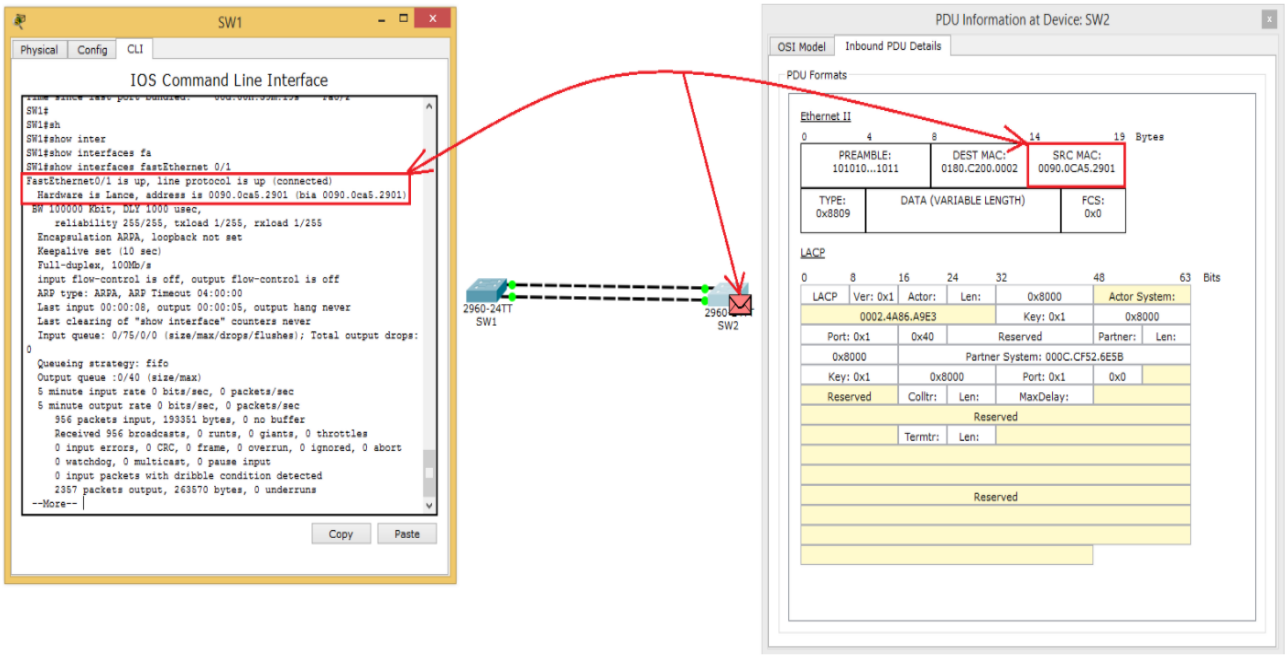

Рисунок 3.7 – Режим симуляції LACP

З рисунку видно, що SW1 відправляє сусідові LACP-повідомлення. Це відображено в полі Ethernet. У Source він записує свою MAC-адресу, а в Destination мультікастову адресу 0180.C200.0002. Ця електронна адреса слухає протокол LACP. Ось це повідомлення використовується пристроями для багатьох цілей. Це синхронізація, збір, агрегація, перевірка активності і так далі. Тобто у нього кілька функцій. І ось перед тим, як це все починає працювати, вони вибирають собі віртуальну MAC-адресу. Зазвичай це найменший з наявних (див. рис. 3.8).

Рисунок 3.8 – Список адрес Destination для комутаторів

Наступні адреси вони будуть записувати в поля LACP (див. рис. 3.9).

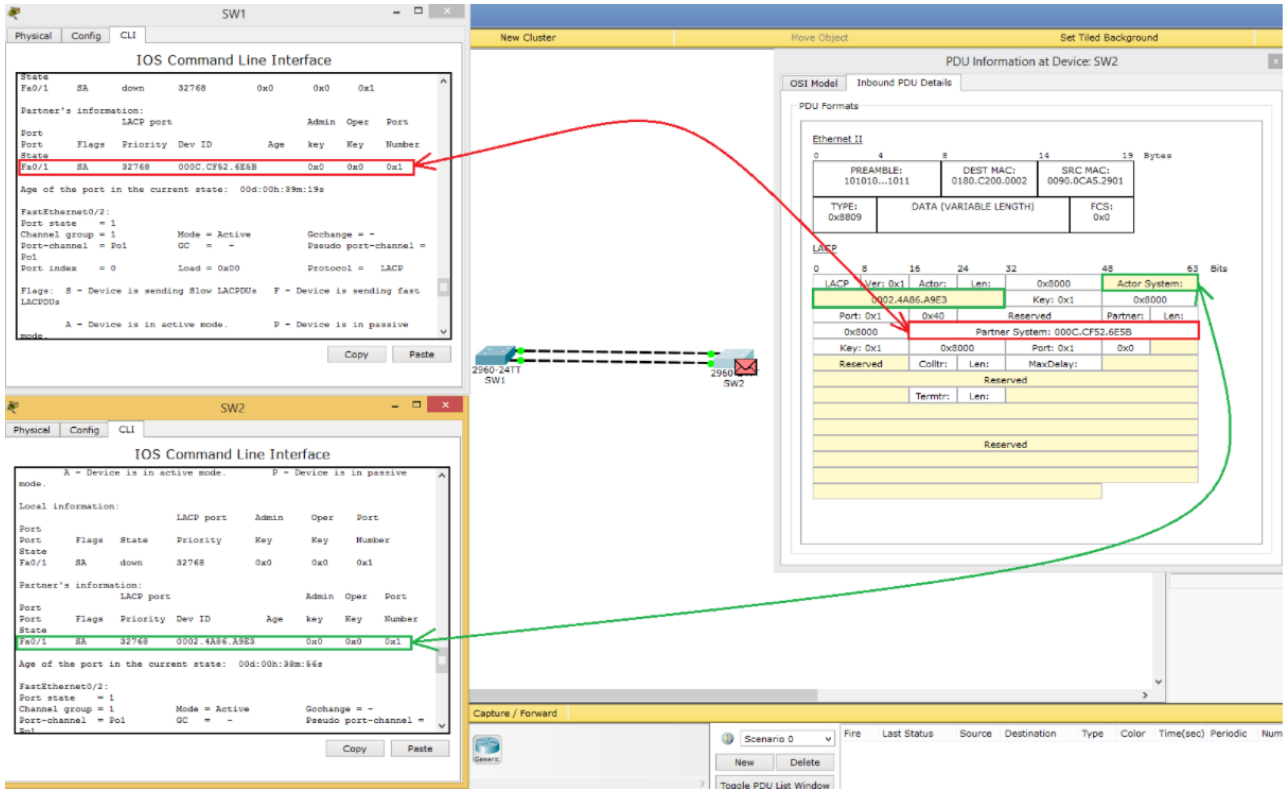

Рисунок 3.9 – Активні адреси для комутаторів

Всі дії, зроблені на даному інтерфейсі автоматично будуть приводити до змін на фізичних портах (див. рис. 3.10).

```
SW1(config-if)#switchport mode trunk

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

```

Рисунок 3.10 – Переведення порту в режим «trunk»

Варто було перевести port-channel в режим trunk і він автоматично потягнув за собою фізичні інтерфейси. Набираємо show running-config (див. рис. 3.11).

```
SW1 #show running-config

Building configuration...
Current configuration : 1254 bytes
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname SW1

spanning-tree mode pvst

interface FastEthernet0/1
channel-group 1 mode active
switchport mode trunk

interface FastEthernet0/2
channel-group 1 mode active
switchport mode trunk

interface Port-channel 1
switchport mode trunk

```

Рисунок 3.11 – Поточні налаштування каналу

Фізичні канали налаштувалися на режим trunk. В попередньому розділі було згадано технологію Load-Balance або як її називають по іншому «балансування». При створенні агрегованого каналу Потрібно не забувати що всередині нього фізичні канали, а також що трафік пропускають саме вони. Бувають випадки, що канал агрегований і працює, а весь трафік йде по одному інтерфейсу, але решта в режимі простою. Розглянемо як працює Load-Balance на рис. 3.12.

```
1   SW1 #show Etherchannel load-balance
2   Etherchannel Load-Balancing Operational State (src-mac):
3   Non-IP: Source MAC address
4   IPv4: Source MAC address
5   IPv6: Source MAC address
6
```

Рисунок 3.12 – Поточні налаштування Load-Balance активного каналу

На цей момент SW1 виконує балансування виходячи зі значення MAC-адреси. За замовчуванням балансування так і виконується. Тобто первий MAC-адрес вона пропустить через перший лінк, другий MAC-адресс через другий лінк, третій MAC-адрес знову через перший лінк і так буде чергуватися. Але такий підхід не завжди вірний (див. рис. 3.13).

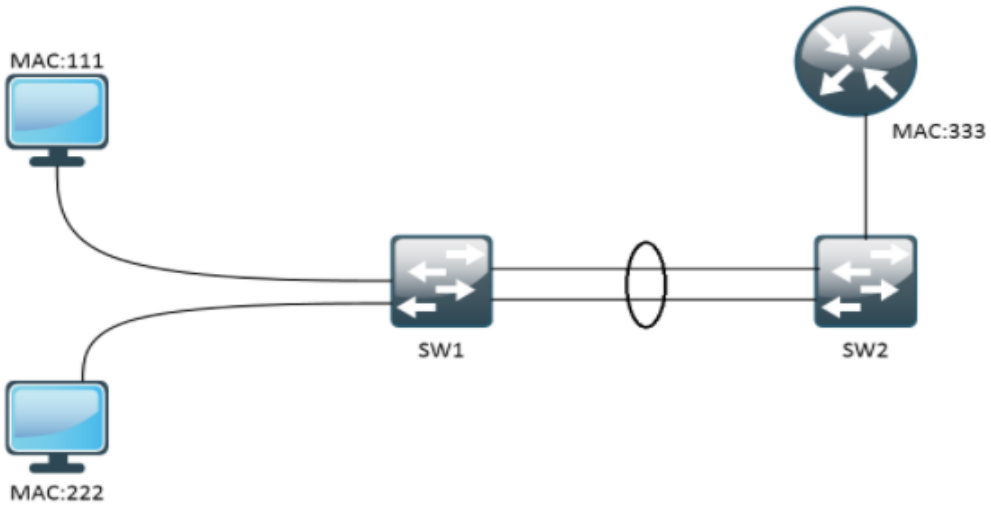

Рисунок 3.13 – Принцип роботи балансування

Є умовна мережа. До SW1 підключені 2 комп'ютери. Далі цей комутатор з'єднується з SW2 агрегованих каналом. А до SW2 підключається маршрутизатор. За замовчуванням Load-Balance налаштований на src-mac. І ось що буде відбуватися. Кадри з MAC-адресою 111 будуть передаватися по першому лінку, а з MAC-адресою 222 по другому лінку. Тут вірно. Переходимо до SW2. До нього підключений всього один маршрутизатор з MAC-адресою 333. І все кадри від маршрутизатора будуть відправлятися на SW1 по першому лінку. Відповідно другий буде завжди простоювати. Тому логічніше тут налаштувати балансування не по Source MAC-адресу, а по Destination MAC-адресу. Тоді, наприклад, все, що відправляється 1-го комп'ютера, буде відправлятися по першому лінку, а другого по другому лінку (див. рис. 3.14).

Це простий приклад, але він відображає суть цієї технології. Змінюється він у такий спосіб:

```
1   SW1(config) # port-channel load-balance ?
2   dst-ip Dst IP Addr
3   dst-mac Dst Mac Addr
4   src-dst-ip Src XOR Dst IP Addr
5   src-dst-mac Src XOR Dst Mac Addr
6   src-ip Src IP Addr
7   src-mac Src Mac Addr12
```

Рисунок 3.14 – Принцип роботи балансування в CLI

Слід брати до уваги, що це приклад балансування не тільки для LACP, але і для інших методів. Варто зазначити, що даний протокол застосовується найчастіше, в силу його відкритості та може бути використаний на більшості вендорів.

3.2 Налаштування агрегації каналів на основі протоколу PAgP

На цей момент буде розглядатися протокол PAgP. PAgP – це чисто протокол Cisco. Його застосовують рідше (оскільки мереж, побудованих виключно на обладнанні Cisco менше, ніж гетерогенних).

PagP має теж два режиму як і протокол LACP:

1. Desirable – вмикає PAgP;
2. Auto – увімкнеться, якщо прийде PAgP повідомлення.

Починаємо налаштування. Маємо два комутатори (див. рис. 3.15).

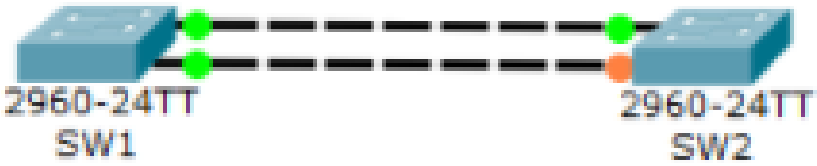

Рисунок 3.15 – Принцип підключення комутаторів

Щоб виконати налаштування агрегації каналів по протоколу PAgP. Потрібно перейти на комутатор з позначенням SW1 (див. рис. 3.16).

```
SW1(config)#interface range fastEthernet 0/1-2

SW1(config)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

SW1(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
```

Рисунок 3.16 – Налаштування комутатора SW1

1. вибираємо діапазон інтерфейсів;
2. вимикаємо;
3. створюємо port-channel і перемикаємо його в режим desirable (тобто увімкнути).

Тепер переходимо до налаштування SW2 (див. рис. 3.17) (не забуваємо, що на SW1 інтерфейси вимкнені й слід після до них повернутися):

```
SW2(config) #interface range fastEthernet 0/1-2

SW2(config-if-range) #channel-group 1 mode auto
Creating a port-channel interface Port-channel 1
```

Рисунок 3.17 – Налаштування комутатора SW2

1. вибираємо діапазон інтерфейсів;
2. створюємо port-channel та переводимо в режим auto (включиться, якщо отримає PAgP-повідомлення)

Повертаємося до SW1 і включаємо інтерфейси та перевіряємо командою show EtherChannel summary (див. рис. 3.18).

```
<source>SW1#show etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-------------

1 Po1(SU) PAgP Fa0/1(P) Fa0/2(P)
```

Рисунок 3.18 – Результати команди show EtherChannel summary

Та також робимо перевірку налаштування портів на комутаторі SW2 (див. рис. 3.19).

```
SW2#show etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+--------------

1 Po1(SU) PAgP Fa0/1(P) Fa0/2(P)
```

Рисунок 3.19 – Результати команди show EtherChannel summary

Тепер переходимо в симуляцію і налаштовуємо на фільтр PAgP. Можемо спостерігати за тим що було відправлене повідомлення від комутатора SW2 (див. рис. 3.20).

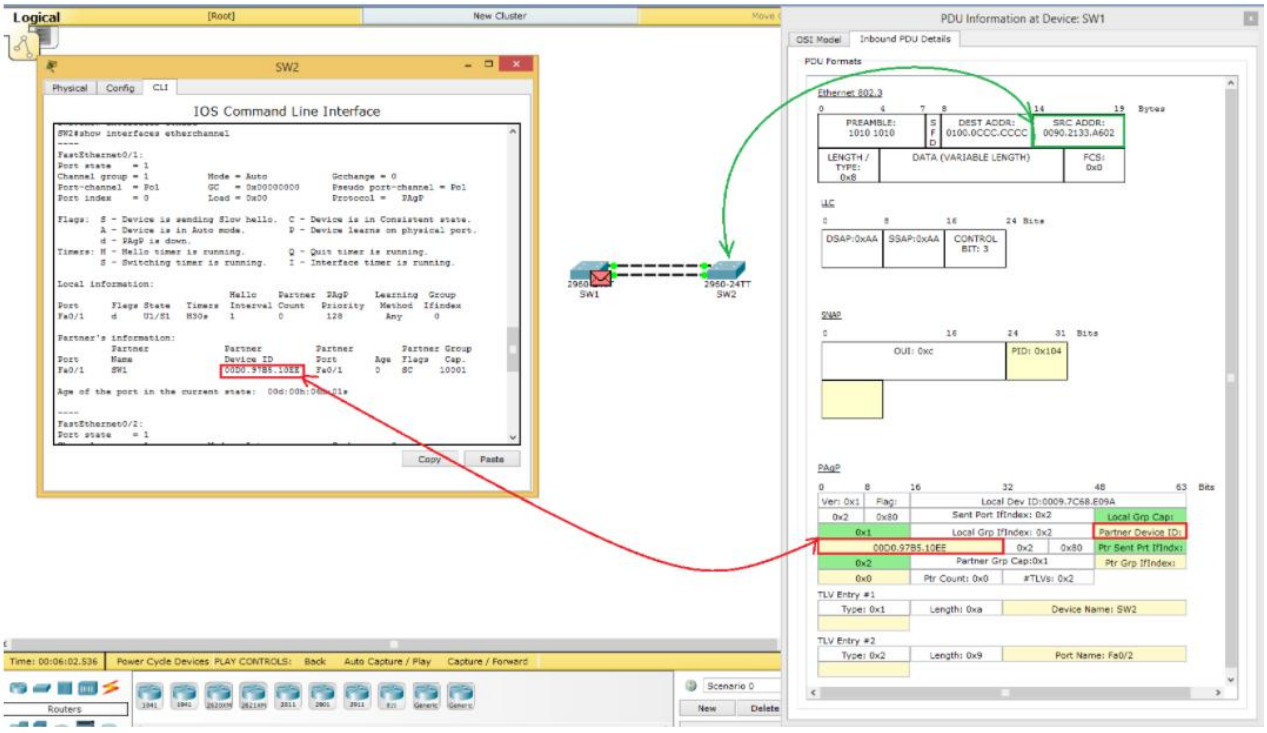

Рисунок 3.20 – Процес відправлення повідомлення від комутатора SW2

Тобто спостерігаємо що в полі Source записано MAC-адресу SW2. У полі Destination групову адресу для PAgP. В одному з полів пише віртуальну MAC-адресу SW1 (вибирається за тим же принципом, що і в LACP), а нижче записує своє ім’я та порт, з якого це повідомлення вийшло.

3.3 Ручне налаштування агрегації каналів

Як згадувалось вище, тут не використовується додатковий протокол узгодження, перевірки. Тому перед агрегуванням каналу потрібно перевірити ідентичність налаштувань інтерфейсів.

Налаштування агрегування в ручну (див. рис. 3.21)

```
SW1(config)#interface range fastEthernet 0/1-2

SW1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

SW1(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1

SW1(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

Рисунок 3.21 – Приклад налаштування агрегації в ручному режимі на комутаторі SW1

1. створюємо діапазон інтерфейсів для добавлення в віртуальну групу портів
2. вимикаємо групу портів
3. створюємо port-channel і відразу вмикається
4. вмикаємо групу портів

Аналогічно налаштуємо комутатор SW2 в ручному режимі (див. рис. 3.22).

```
SW2(config) #interface range fastEthernet 0/1-2

SW2(config-if-range) #channel-group 1 mode on
Creating a port-channel interface Port-channel 1

%LINK-5-CHANGED: Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

Рисунок 3.22 – Приклад налаштування агрегації в ручному режимі на комутаторі SW2

1. створюємо діапазон інтерфейсів у віртуальну групу портів
2. створюємо port-channel і відразу вмикається

Налаштування закінчена. Перевіримо командою show EtherChannel summary (див. рис. 3.23)

```
SW1#show etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-----------

1 Po1(SU) - Fa0/1(P) Fa0/2(P)
```

Рисунок 3.23 – Результат команди show EtherChannel summary

Отже, в полі протокол "-". Тобто додатково не використовується якийсь протокол.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було проведено дослідження технології Ethernet, принципів її функціонування та особливостей використання у сучасних комп'ютерних мережах. Було розглянуто модель OSI та призначення кожного її рівня, досліджено основне мережеве обладнання та типи мережевих кабелів, що використовуються для побудови локальних мереж. На основі отриманих теоретичних знань було розроблено модель мережевого з'єднання між комутаторами, які були об'єднані за допомогою UTP-кабелю.

У процесі виконання роботи було досліджено основні методи та протоколи агрегації каналів, проведено аналіз технології EtherChannel, визначено її переваги та недоліки. Встановлено, що використання агрегації каналів дозволяє підвищити пропускну здатність мережі, забезпечити балансування навантаження та підвищити рівень відмовостійкості мережевої інфраструктури. Також було проведено дослідження принципів резервування каналів та їх ролі у забезпеченні безперервної роботи мережі.

Практична частина кваліфікаційної роботи була реалізована у середовищі Cisco Packet Tracer, де було побудовано модель надійної корпоративної мережі та виконано налаштування агрегації каналів трьома різними способами:

1. агрегація каналів на основі протоколу LACP;
2. агрегація каналів на основі протоколу PAgP;
3. статичне налаштування агрегації каналів без використання протоколів узгодження.

За результатами проведених досліджень було встановлено, що всі методи агрегації каналів забезпечують коректну роботу мережі та мають незначні відмінності у процесі налаштування. Під час аналізу було визначено, що найбільш доцільним варіантом для використання у корпоративних мережах є протокол LACP, оскільки він є стандартним рішенням, забезпечує автоматичне узгодження параметрів та підтримує сумісність із різним мережевим обладнанням.

Окремо було проведено дослідження роботи резервування каналів. Під час експерименту було навмисно виконано відключення основного мережевого з’єднання, після чого система автоматично виконала перемикання на резервний канал. Це дозволило забезпечити подальшу передачу даних без повної втрати працездатності мережі та підтвердило ефективність використання механізмів резервування для підвищення надійності корпоративної мережі.

Таким чином, результати виконаної роботи підтвердили ефективність використання технології EtherChannel для модернізації комп’ютерних мереж. Застосування агрегації та резервування каналів дозволяє підвищити продуктивність, стабільність та відмовостійкість мережевої інфраструктури, що є важливим фактором для забезпечення надійної роботи сучасних корпоративних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco Systems. Cisco Packet Tracer User Guide. Cisco Networking Academy. URL: https://www.netacad.com/courses/packet-tracer (дата звернення: 24.05.2026).

2. Comer D. E. Computer Networks and Internets. 6th Edition. Pearson, 2018. 672 p.

3. IEEE 802.1AX-2020. IEEE Standard for Local and Metropolitan Area Networks Link Aggregation. URL: https://standards.ieee.org/ (дата звернення: 24.05.2026).

4. IEEE 802.1D-2004 - IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges. URL: https://standards.ieee.org/standard/802_1D-2004.html (дата звернення: 24.05.2026).

5. IEEE 802.3ad Link Aggregation Task Force. URL: http://www.ieee802.org/3/ad/ (дата звернення: 24.05.2026).

6. IEEE Computer Society. IEEE Standard for Local and Metropolitan Area Networks: Link Aggregation Control Protocol (LACP). IEEE 802.1AX. 2020.

7. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th Edition. Pearson, 2021. 864 p.

8. Link Aggregation and LACP basics - Thomas-Krenn-Wiki. URL: https://www.thomas-krenn.com/en/wiki/Link_Aggregation_and_LACP_basics (дата звернення: 24.05.2026).

9. PoE-комутатор - важливий компонент сучасної системи відеоспостереження. URL: https://worldvision.com.ua/ua/dlya-chego-nuzhny-poe-kommutatory-v-sistemakh-videonabludeniya/ (дата звернення: 24.05.2026).

10. Power over Ethernet - що це і навіщо потрібно? - EServer. URL: https://e-server.com.ua/uk/novini/power-over-ethernet-shho-ce-i-navishho-potribno (дата звернення: 24.05.2026).

11. Stallings W. Data and Computer Communications. 11th Edition. Pearson Education, 2020. 816 p.

12. Understanding EtherChannel Load Balancing and Redundancy on Catalyst Switches - Cisco. URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/EtherChannel/12023-4.html (дата звернення: 24.05.2026).

13. Буров Є. В. Комп’ютерні мережі: підручник. Львів: Магнолія 2006, 2019. 264 с.

14. Що таке Wi-Fi роутер. URL: https://nettech.ua/news/router-wi-fi-besprovodniy-marshrutizator-wi-fi (дата звернення: 24.05.2026).

15. Що таке оптоволокно, як воно працює і як підключити - блог svit-server. URL: https://svit-server.com.ua/ua/chto-takoe-optovolokno/ (дата звернення: 24.05.2026).

16. Що таке світч (switch) або мережевий комутатор. URL: https://nettech.ua/news/svitch-switch-setevoy-kommutator (дата звернення: 24.05.2026).