Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет Комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи

магістр
(освітній ступінь)

на тему: Методи та засоби розгортання і конфігурування комп'ютерних мереж

Виконав: студент (ка) 6 курсу, групи СІм-61
спеціальності
123 Комп'ютерна інженерія
(шифр і назва спеціальності)

О. Луць — Луць О.В.
(підпис) (прізвище та ініціали)

Керівник — Гнатів Б.В.
(підпис) (прізвище та ініціали)

Нормоконтроль — Луцик Н.С.
(підпис) (прізвище та ініціали)

Рецензент — Мацюк О.В.
(підпис) (прізвище та ініціали)

м. Тернопіль – 2019

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

Факультет Комп'ютерно-інформаційних систем і програмної інженерії
Кафедра Комп'ютерні системи та мережі
Освітній ступінь магістр
Напрям підготовки
(шифр і назва)
Спеціальність 123 „Комп'ютерна інженерія"
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри КС
Осухівська Р.М.
«30» 09 2019 р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Ліщуку Олегу Богдановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби резервування та агрегації каналів комп'ютерних мереж

Керівник роботи Тиш Євгеній Володимирович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «24» 09 2019 року №4/7-854

2. Термін подання студентом роботи 24.12.2019

3. Вихідні дані до роботи математико-модельний підхід до методів та засобів резервування та агрегації

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз існуючих методів та технологій резервування та агрегації. 2. Аналіз та вибір оптимальних методів та технологій резервування та агрегації каналів передачі даних. 3. Дослідження ефективності використання протоколів агрегації та резервування для побудови комп'ютерної мережі. 4. Обґрунтування економічної ефективності. 5. Охорона праці та безпека в надзвичайних ситуаціях. 6. Екологія. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Актуальність і мета роботи. 2. Об'єкт, предмет, задачі і методи дослідження, наукова новизна та практична цінність одержаних результатів. 3. Логічне представлення макету комп'ютерної мережі. 4. Графічна [illegible] модель мережі. 5. Принципи забезпечення подвійного резервування. 6. Технології агрегації та алгоритм балансування навантаження. 7. Оцінка ефективності роботи протоколів подвійного резервування STP та RSTP. 8. Результати дослідження методів балансування навантаження [illegible] рівня. 9. Результати дослідження [illegible] та динамічної агрегації каналів. 10. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата завдання видав	Підпис, дата завдання прийняв
Екологія	Лесота О.М., доцент		
Безпека в НС	Стручок В.С., ст.викл. каф. ВС		
Обґрунт. екон. ефект.	Жирич Н.Б.	21.11.19	
Охорона праці	Осуховська Г.М.		

7. Дата видачі завдання 30.09.2019

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз існуючих методів та техній розрахунку та охорони	02.10.19	Виконав
2	Вибір та вибір оптимальних методів та техній розрахунку та охорони праці в процесі даних	21.10.19	Виконав
3	Розділ Організація виконання проектів охорони та розрахунок за допомогою методу комп'ютерних мережі	7.11.19	Виконав
4	Обґрунтування економічної ефективності	20.11.19	Виконав
5	Охорона праці та безпека в надзвичайних ситуаціях	25.11.19	Виконав
6	Екологія	27.11.19	Виконав
	Попередній захист дипломної роботи	28.11.19	Виконав
	Захист дипломної роботи	24.12.19	Виконав

Студент _____ Ліщук О.Б.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Жирич Н.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи та засоби резервування та агрегації каналів комп’ютерних мереж // Дипломна робота // Ліщук Олег Богданович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно – інформаційних систем та програмної інженерії, група СІм – 61 // Тернопіль, 2019 // с. – 119, рис. – 57 , табл. – 6, аркушів А1 – 10, додат. – 2, бібліогр. – 48.

Ключові слова: КОМП’ЮТЕРНА МЕРЕЖА, РЕЗЕРВУВАННЯ, АГРЕГАЦІЯ, ПРОТОКОЛ, МЕТОД.

У дипломній роботі магістра проведено аналіз методів та технологій, які забезпечують надійну роботу комп’ютерних мереж. Завдяки цьому зроблені висновки щодо доцільності використання тих чи інших технічних рішень у відповідних сегментах мережі.

Обґрунтовано використання протоколів та технологій на різних рівнях мережевої взаємодії, це дозволило зменшити навантаження на мережеве обладнання, що в свою чергу підвищує надійність системи.

Досліджена доцільність використання методів балансування навантаження мережевого та прикладного рівня для забезпечення відмовостійкості серверного обладнання (TFTP,DHCP,DNS серверів).

Досліджена ефективність використання протоколів надлишкового резервування мережевих екранів для забезпечення безпеки прикордонних шлюзів, а також демілітаризованої(DMZ) зони. Такі технічні рішення дозволили підвищити захищеність мережі від атак зловмисників.

Змодельована комп’ютерна мережа для дослідження ефективності використання обраних протоколів та технологій забезпечення резервування та агрегації каналів передачі даних.

Апробовано запропоновані для кожного рівня представлення методи та засоби резервування та агрегації каналів комп’ютерних мереж, методи балансування навантаження.

ANNOTATION

Methods and means of reservation and aggregation of channels of computers networks // Master thesis // Lishchuk Oleh Bohdanovych // Ternopil Ivan Pul’uj National Technical University, Faculty of Computer Information Systems and software engineering, group CIm – 61 // Ternopil, 2019 // p. – 119, fig. – 57 , tab. – 6, Sheets A1 – 10, Add. – 2, Ref. – 48.

Keywords: COMPUTER NETWORK, RESERVATION, AGGREGATION, PROTOCOL, METHOD.

The master's thesis deals with the methods and technologies that ensure the reliable operation of computer networks. This leads to the conclusion that it is advisable to use certain technical solutions in the respective segments of the network.

The use of protocols and technologies at different levels of network interaction is justified, which has reduced the load on network equipment, which in turn increases the reliability of the system.

The feasibility of using network and application load balancing methods to ensure the resiliency of server hardware (TFTP, DHCP, DNS servers) is explored.

The effectiveness of the use of redundancy protocols of network screens for the security of border gateways as well as the demilitarized (DMZ) zone has been investigated.

A simulated computer network to investigate the effectiveness of using selected protocols and technologies to provide backup and aggregation of data channels.

The methods and means of redundancy and aggregation of computer network channels and load balancing methods proposed for each level of presentation have been tested.

ЗМІСТ

ВСТУП

Актуальність теми роботи. У зв’язку з зростанням кількості мережевих пристроїв, які використовують глобальну мережу для обміну інформацією, зростає необхідність у розширені пропускних можливостей каналів передачі даних. Сучасні концерни та великі фірми встановлюють нові критерії щодо забезпечення надійності передачі даних, адже навіть хвилина простою може вартувати їм дуже багато.

Ці та інші фактори підштовхнули фахівців до створення та удосконалення технологій, які б забезпечували надійність та безвідмовність роботи, при цьому забезпечуючи швидкісний доступ до інформації в будь-якому сегменті мережі.

Для забезпечення та підвищення надійності інформаційних систем розроблено ряд вітчизняних та закордонних стандартів (стандарти серії ГОСТ 34.xxx, ISO/IEC 15288, EIA 632, EIA 731, DOD 2167A, DEF Stan 00-55 та ін.). Це дозволило сформувати шаблон, згідно якому повинні проводитися наступні розробки у сфері комп’ютерних систем та мереж.

Дослідженню надійності таких систем, присвячено ряд наукових та науково-прикладних публікацій, авторами яких є провідні науковці у цій галузі, такі як Andrew Tanenbaum, Jim Kurose, Larry L. Peterson та інші. До таких праць відносять наукові статті з ґрунтовним описом тих чи інших методів забезпечення надійності та агрегації, періодичні видання та книги, які здобули всесвітнє визнання.

Незважаючи на понад сорок років роботи над проблемами галузі, дослідники дійшли згоди, що продовження праці в цьому напрямку є важливим елементом для забезпечення надійної роботи мереж, тому дослідження методів та засобів резервування та агрегації каналів у комп’ютерних системах та мережах є актуальною задачею.

Метою роботи є дослідження методів та засобів резервування та агрегації каналів комп’ютерних мереж, їх детальний аналіз та вибір оптимальних рішень для забезпечення функціонування.

Для досягнення вказаної мети в роботі поставлено наступні задачі:

- аналіз наукових публікацій та стандартів для забезпечення резервування та агрегації комп’ютерних мереж;
- дослідження ефективності роботи протоколів та технологій резервування та агрегації на різних рівнях моделі представлення;
- дослідження можливості комплексного використання різних груп протоколів для збільшення відмовостійкості комп’ютерних мереж;
- обґрунтування доцільності використання комплексу технічних рішень для реалізації резервних з’єднань та агрегації;
- побудова макетної моделі мережі з використанням технологій резервування та агрегації;
- апробація запропонованих методів для забезпечення резервування та агрегації каналів комп’ютерних мереж.

Об’єкт дослідження: надлишкове резервування та агрегація каналів передачі даних в комп’ютерних мережах.

Предмет дослідження: методи та засоби резервування та агрегації каналів комп’ютерних мереж та систем.

Методи дослідження. Для вирішення поставлених задач використано наступні методи: аналіз та узагальнення – при проведенні аналізу існуючих методів та технологій резервування та агрегації; теорії надійності, математичної статистики, теорії графів – для формалізації та побудови моделі взаємодії груп протоколів та технологій; проектування – при побудові макету комп’ютерної мережі; експеримент та вимірювання – для апробації запропонованого комплексу методів та технологій.

Наукова новизна одержаних результатів:

- досліджено вплив методів та технологій на мережеве обладнання, обрано оптимальні методи уникнення перевантажень у сегментах мережі;
- обґрунтовано алгоритми реалізації агрегації та резервування на всіх рівнях моделі OSI, що дало змогу підвищити надійність мережі, ефективніше здійснювати балансування навантаження та збільшити пропускну здатність каналів передачі даних;

- вперше досліджено застосування комплексу методів та технологій резервування та агрегації каналів комп’ютерної мережі, з подальшою апробацією обраних технічних рішень.

Практичне значення одержаних результатів. Впровадження запропонованих технологій та методів резервування та агрегації каналів комп’ютерних мереж реалізовано та впроваджено у комплексі рекомендацій щодо використання певних технічних рішень для забезпечення безвідмовної роботи мережі на різних сегментах.

Публікації. Результати дослідження апробовано на VIII Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій» (27-28 листопада 2019 р.) Тернопільського національного технічного університету імені Івана Пулюя та на VII науково-технічній конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (11-12 грудня 2019 року) у вигляді тез конференцій.

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається із вступу, шести розділів, висновків, переліку посилань та додатків. Обсяг роботи: пояснювальна записка – 119 арк. формату А4, графічна частина – 10 аркушів формату А1.

РОЗДІЛ 1 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ТЕХНОЛОГІЙ РЕЗЕРВУВАННЯ ТА АГРЕГАЦІЇ

1.1. Сучасне застосування комп’ютерних мереж та вимоги до них. Забезпечення надійності систем за допомогою протоколів резервування та агрегації

Абсолютна більшість сучасних організацій використовують велику кількість комп’ютерів. Такі компанії можуть мати ЕОМ для кожного працівника окремо для розробки продуктів, брошур, так само як і застосовувати робочі станції для систематизації баз даних, ведення бухгалтерії тощо. В сучасних реаліях для всіх машин необхідно забезпечити надійний та швидкісний зв’язок для обміну інформацією. Масштабованість дозволила будувати мережі різних розмірів, від маленького офісу до континенту. Малі і великі компанії та організації однаково залежать від обігу інформації незалежно від її типу. Якщо б відмовили ключові вузли одного з кращих банків світу то він би став банкрутом за лічені хвилини. Це поставило непросту задачу перед інженерами та розробниками програмного забезпечення – досягти максимальної надійності системи при використанні найменшої кількості обробляючої потужності. З ростом популярності комп’ютерних мереж та збільшенням інформації яка передається через них, стандарти та погляди на забезпечення безвідмовної роботи постійно змінюються та потребують покращень.

Одним з перших технічних рішень щодо забезпечення якості стало надлишкове резервування вузлів у комп’ютерних мережах. Резервування застосовують у випадках, коли треба забезпечити високий рівень надійності (насамперед безвідмовності) системи при недостатньо надійних вузьких місцях. Метод надлишковості не є новаторством, проте його використання у комп’ютерних мережах потребував значного переосмислення, оскільки авторам перших протоколів резервування довелося зіткнутися з логічними особливостями маршрутизації та розподілення пакетів у мережі, щоб уникнути неправильної роботи. Детальніше про протоколи резервування, їх особливості, проблеми та вирішення буде сказано нижче.

З збільшенням апетитів користувачів, комп'ютерні мережі повинні були передавати все більші обсяги інформації, забезпечуючи при цьому задовільний рівень надійності. Протоколи резервування перестали бути панацеєю, оскільки ціна на нове обладнання та його резервування ставала все більшою. Оптимальним рішенням стала логічна агрегація каналів передачі даних за допомогою протоколів на другому та третьому рівні мережевої моделі OSI, перший же рівень традиційно резервується за допомогою додаткових каналів зв'язку, які в залежності від протоколу вищого рівня або використовуються разом або перебувають в режимі очікування (standby).

Подальший розвиток цих двох методів забезпечення відмовостійкості мереж докорінно відрізняється. Агрегування каналів отримує все більшу популярність через відносно легку масштабованість у порівнянні з фізичним резервуванням, гнучкість та підтримку середнього та великого бізнесу.

Протоколам надлишкового резервування приділяють все менше уваги, це пов'язано з вартістю резервування багаторівневих моделей, де використовується складне та дороге обладнання. Проте сімейство протоколів все ще зберігає позиції у сегменті малих мереж. Також надлишкове резервування залишається основною технологією забезпечення надійності дата-центрів та інших структур які спеціалізуються на обробці великих масивів даних.

Подальший детальний аналіз методів та протоколів агрегації та резервування дозволить зробити висновки щодо ефективності їх використання на різних рівнях мережевої моделі.

1.2. Логічні петлі комутації у мережах Ethernet. Протокол STP

При використанні додаткових з'єднань між комутаторами або маршрутизаторами та без додаткових обмежень, мережа може зіткнутися з випадком коли пакети даних без єдиної логічної структури починають передаватися всіма комутаторами одночасно та в безкінечній кількості, оскільки службові пакети не мають часу життя (TTL). Логічний приклад утворення класичної петлі комутації зображено на рис. 1.1 [1].

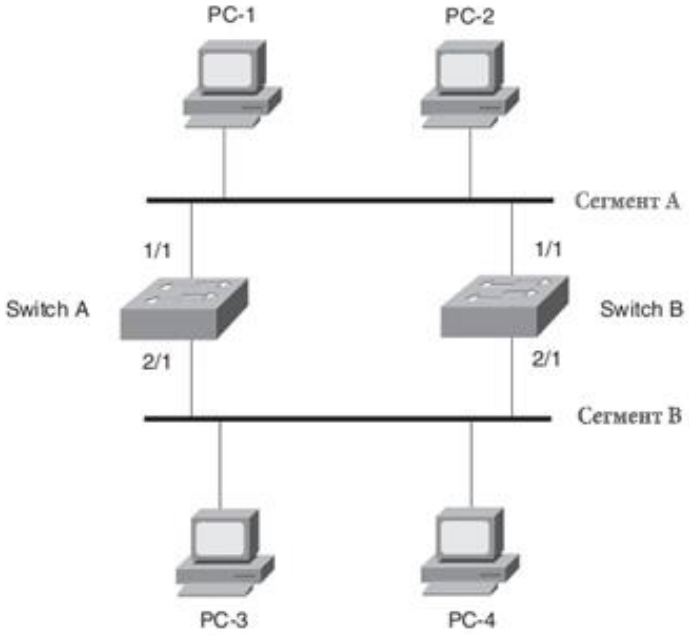


Рис. 1.1. Приклад сегменту мережі з виникненням логічних петель

Для виникнення петлі у такому сегменті, достатньо відправки одного пакету з хоста 1 до хоста 2. Це приводить до логічного конфлікту, коли обидва мереживі пристрої не знають про існування іншого і реагують на розсилання пакетів у всьому сегменті. Такий самий принцип утворення петель через використання широкомовної передачі даних хостами чи комутаторами. Такий вид петель називається широкомовним штормом, а пакет який запустив весь процес – чорнобильським.

Логічні петлі дуже небезпечні тим, що створюють серйозні перенавантаження комутаторів. Чим більш масштабованою є мережа, тим більш небезпечним є шторм, якщо не було дотримано рекомендацій щодо сегментування. Така ситуація може перенавантажити та вивести з ладу весь сегмент мережі, що може привести до критичних відмов всієї мережі.

Єдиною можливістю уникнення створення циркуляції фреймів в сегменті мережі є логічне вимкнення одного з каналів передачі даних, які зв’язують мережеві пристрої. Таку функцію реалізує протокол STP [2].

Протокол зв’язуючого дерева (STP) – це мережевий протокол, який був розроблений для вирішення логічних петель при надлишковому резервуванні вузлів в Ehternet-мережах, детально описаний в стандарті IEEE 802.1D.

Завдання протоколу полягає у забезпеченні надлишкового резервування на фізичному рівні та блокування на логічному, створюючи таким чином запасні з'єднання які знаходяться в режимі очікування виходу з ладу головного каналу зв'язку.

Принцип його роботи полягає у розсиланні BDPU (Bridge Protocol Data Unit) пакетів, які пристої використовують для обміну інформацією між собою про вибір кореневого (root) комутатора. Такий пристрій отримує найменший ідентифікатор моста (bridge id). Комутатор такого типу може бути лише один і він використовується протоколом як центральний, всі інші мережеві пристрої в сегменті повинні прораховувати оптимальний шлях до кореневого порту (root port). Після аналізу та прорахування найкоротшого шляху фреймів, утворений міст стає призначеним (designated bridge). Після визначення кореневого комутатора та моста по якому передаються дані, всі інші з'єднання блокуються, таким чином отримується математичний граф з кореневим комутатором по центрі. При втраті призначеного каналу зв'язку алгоритм автоматично перебудовує таблицю, аналізуючи всі можливі шляхи доставки даних, та створює новий граф, де використовується доступний лінк, а інші блокуються. При будь якій зміні конфігурацій у структурі, всі комутатори надсилають пакет TCN (Topology Change Notification) до кореневого пристрою з затримкою в дві секунди, пакети надсилаються до зміни конфігурації дерева всіма учасниками мережі. Приклад роботи мережі з застосуванням протоколу STP показаний на рис. 1.2. Метод ваг, який використовує протокол, дозволяє здійснювати обрахунок шляху кореневим комутатором та надсилати результати всім іншим. Мережеві пристрої знаходяться в режимі прослуховування (listening), який здійснюється за допомогою BDPU. Режим не змінюється навіть після вибору оптимального маршруту, в такому стані комутатор знаходиться 15 секунд, а після переходить у режим навчання (learning).

Це пов'язано з унеможливленням обрання неправильного маршруту передачі даних. Після закінчення навчання та forward delay, який рівний 15 секундам, порт комутатора переходить з стану блокування (blocking) в стан передачі (forwarding), коли комутатор готовий до передачі як пакетів BDPU так і звичайних пакетів з даними.

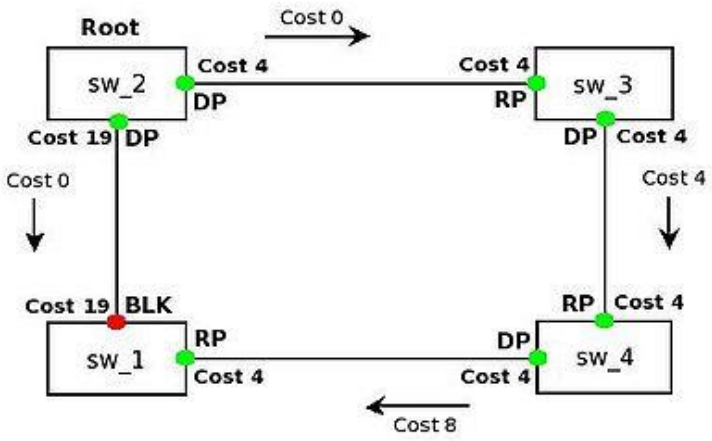


Рис. 1.2. Реалізація протоколу STP в мережі Ethernet

До недоліків протоколу можна віднести довге навчання обладнання при зміні конфігурації, де зведення нового маршруту може займати до хвилини часу, що у деяких випадках є неприпустимим. Важливим недоліком є також неможливість взаємодії протоколу та логічних каналів, таких як VLAN, що значно ускладнює реалізацію протоколу у сучасних мережах з активним використанням цієї технології [3].

Створення такого протоколу дозволило використовувати метод надлишкової агрегації у комп'ютерних системах різних масштабів та орієнтацій. Його ідейним наступником став протокол RSTP, який бореться з багатьма недоліками STP, розширює функціонал сімейства протоколів для роботи з сучасними мережами.

1.3. Протокол RSTP

Робота з усунення недоліків протоколу STP почалась одразу після загального тестування та збору достатньої кількості інформації. Головним пріоритетом став час сходження системи після виникнення збою. Мережі, які з кожним роком нарощували пропускну здатність та все більше впливали на бізнес, вимагали все досконаліших інструментів з забезпечення безвідмовної роботи. Таким інструментом став протокол RSTP (rapid STP).

Протокол опирається на роботу механізмів, не пов’язаних з стандартним таймерами, які використовує STP. В класичному варіанті протоколу BPDU пакети генерує лише кореневий комутатор, а всі інші займаються ретрансляцією цього повідомлення. Таким чином, якщо комутатори нижчого рівня не отримують пакети від кореневого пристрою, це свідчить про можливу проблему між пристроями. Для цього використовується функція MaxAge, яка має таймер 20 секунд. В реалізації RSTP повідомлення BPDU поступилися місцем так званим Hello-пакетам, протокол передбачає, що при втраті трьох таких пакетів необхідно перемикатися на резервну лінію зв’язку [4].

Введення нового типу пакетів, яке дозволяло мережевим пристроям швидше змінювати вид топології значно пришвидшив час реконфігурації, проте не оптимізував її. Для цього був розроблений механізм Proposal/Agreement (рис. 1.3). Він дозволяє пропустити стадії класичного навчання портів, які присутні у протоколі STP, та одразу перейти до стану передачі інформації [5].

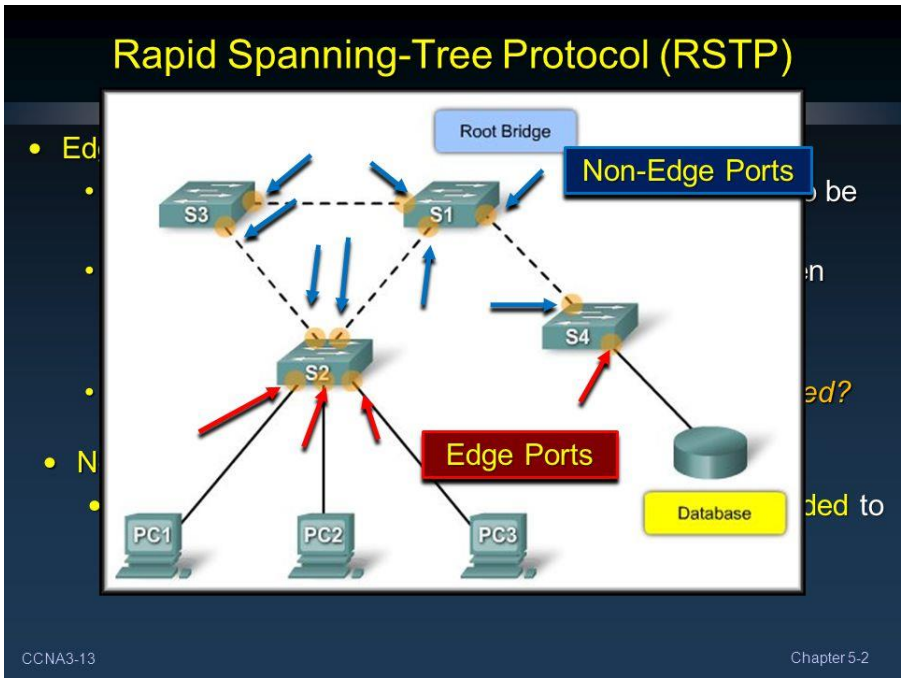


Рис. 1.3. Реалізація класифікації портів у протоколі RSTP

Для того, щоб протокол розрізняв коли варто застосовувати цей механізм, порти, які використовує RSTP були поділені на два класи – Edge port та non-Edge port. В

першому випадку у такі порти підключаються кінцеві пристрої (ЕОМ, сервери, деякі маршрутизатори тощо). В порти класу non-Edge підключаються мережеві пристрої, які безпосередньо беруть участь у формуванні топології мережі з використанням RSTP. Таке розділення дозволяє здійснювати оцінку мостів передачі даних, та здійснювати автоматичний контроль над цими групами портів комутаторами, які знаходяться вище по логічній ієрархії мережі.

Протокол RSTP використовує механізм Proposal/Agreement, який запускається коли конфігурація портів знаходиться в стані Root port. В такому випадку механізм вимикає всі порти комутатора, які не є Edge-портами. Паралельно з цим комутатор сповіщає кореневий пристрій про зміну, після чого включає режим Forwarding для Root-port. Порти які залишилися знаходяться в заблокованому стані до тих пір, поки не відбудеться одна з наступних подій:

- комутатор обмінюється повідомленнями Proposal/Agreement з іншим пристроєм;

- анулюються таймери очікування переходу стану Learning та Forwarding, кожен з яких дорівнює 15 секундам. Це означає, що обладнання, до якого звертається комутатор, не підтримує протокол RSTP.

Повідомлення Proposal (рис. 1.4) відправляється розблокованим портом, який хоче стати назначеним для передачі даних, як і в протоколі STP він називається Designated. Комутатор, який стоїть вище по логічній ієрархії, отримує від розблокованого порту повідомлення і записує в своїй таблиці адресації порт-відправник як кореневий (Root). Такий каскадний механізм дозволяє реструктурувати весь математичний граф для продовження обміну даними.

Нові методи, які використовує протокол RSTP, дозволили протоколу значно покращити час збіжності та реконфігурації мережі, проте ці механізми лише покращували або допрацьовували вже існуючі. Принциповою різницею між протоколами RSTP та STP є відв’язка від концепції ролі стану порту комутатора. Завдяки цьому інженери отримали можливість описувати роль того чи іншого порту мережевого пристрою в загальній топології, незважаючи на його стан у даний момент часу. Це дозволяє оперативно реагувати на зміни в мережі та підлаштовуватись до них.

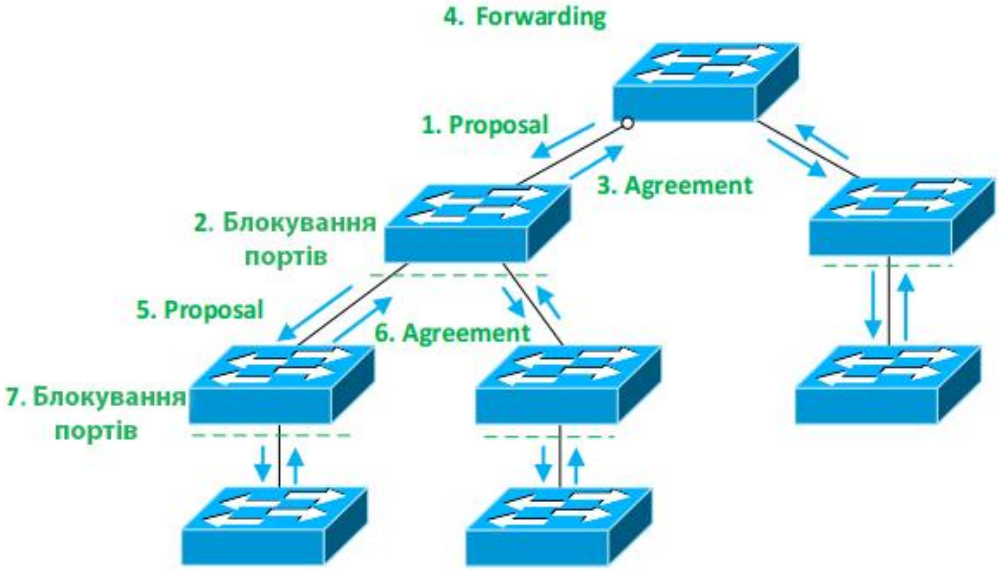


Рис. 1.4. Принцип роботи функційProposal/Agreement

RSTP змінив самий підхід до проблеми резервування. Якщо його попередник, протокол STP, використовував реактивну систему реагування на проблему (яка починає пошук проблеми тоді, коли виникла поломка), то новий протокол працює за реактивною логікою, тобто починає створювати резервні шляхи ще до відмови системи, що за необхідності відразу здійснює перемикання лінків та продовжує роботу в штатному режимі.

Технічно це забезпечується двома функціями портів, які виділяє комутатор – Alternative та Backup (рис. 1.5). Альтернативний порт виступає у ролі резерву для основного мосту передачу даних. Він конфігурується паралельно з основним, і отримавши вагу ребра у моделі графа за допомогою BDPU залишається вимкненим, і вступає у роботу одразу після виходу з ладу кореневого. Резервний порт, назначений комутатором, проводить налаштування після того як альтернативний почав свою роботу, таким чином створюючи механізм, який завжди готовий до змін в каналі передачі даних. Негайна реакція на пакети BPDU з інформацією про гірший з можливих шляхів до кореневого комутатора, дозволяє відкидати кроки навчання нових портів та відразу перемкнутися в режим передачі даних, це реалізовано за допомогою відмови протоколм RSTP від таймера MaxAge.

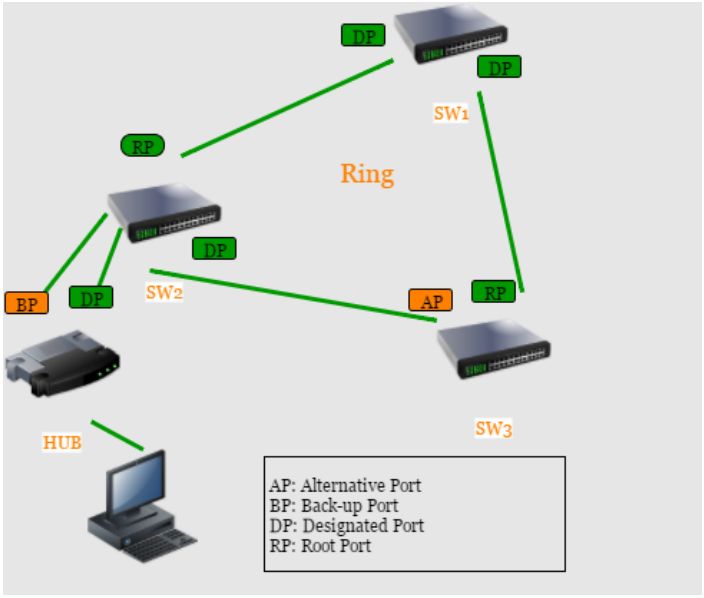


Рис. 1.5. Використання Backup та Alternative портів протоколом RSTP

У класичному протоколі STP прийнято вважати, що топологія мережі зазнала змін якщо порт одного з учасників топології перейшов у стан передавання або навпаки заблокувався. Таці зміни приводять до того, що MAC адреси стають доступними іншим портам, що приводить до циклічних перепосилань пакетів комутатором. Для уникнення таких збоїв використовується пакет TCN, про який було сказано у розділі 1.2. Через особливості пакета та таймерів, які використовує STP, цей процес займає 30 секунд, і щоб уникнути цього RSTP вважає зміну в топології лише таку, коли порт переходить в стан передачі даних. При цьому беруться до уваги лише ті порти які не являється прикордонними (Edge-портами), оскільки зміна MAC адреси в таких портах зробить недоступними хост-станції. Коли протокол бачить зміну в топології, він розсилає прапорець TC всім комутаторам в топології за допомогою пакету BDPU [6]. Отримавши пакети з відповідними маркерами, комутатори видаляють з таблиць MAC-адреси які доступні не через edge-порти, оскільки прикордонні порти ніколи не викликають зміни топології, то і BDPU пакети ці інтерфейси будуть ігнорувати.

Завдяки доопрацюванням та новим механізмам, які отримав протокол RSTP, розробники досягнули миттєвої реакції системи на зміни, покращивши при цьому якість та швидкість опрацювання керуючих сигналів обладнанням.

Незважаючи на досягнуті результати, протокол має критичний недолік, який не дозволяє повноцінно використовувати його у сучасних комп'ютерних мережах для резервування каналів передачі даних, оскільки RSTP може працювати лише з фізичними каналами передачі даних. Логічні групи такі як VLAN, що є основою сучасних комп'ютерних мереж, протоколи STP та RSTP не можуть сприймати як канал даних, що створює фіксовані рамки де ці протоколи можуть використовуватися задля уникнення конфліктних ситуацій. Для вирішення цієї проблеми провідні розробники мережевого обладнання почали розробляти пропрієтарні протоколи, які дозволили подолати проблеми з використанням VLAN у мережах, компанія CISCO розробила протоколи PVST+ і RPVST+, про які піде мова нижче [7].

1.4. Пропрієтарні рішення та протоколи резервування в комп'ютерних мережах. Протоколи PVST , PVST+ і RPVST+

Мережеві технології розвиваються в різний спосіб. Яскравим прикладом є історія розвитку двох моделей представлення комп'ютерних мереж: OSI та TCP/IP. Перша була приватною, закритою розробкою і удосконаленням якої займалося певне коло осіб. Стек TCP навпаки був відкритим і вклад в його розвиток могли вносити всі бажаючі [8]. Такий самий принцип працює в світі сучасних мережевих технологій.

Cisco Systems – це транснаціональна компанія, яка займається виробництвом мережевого обладнання, розробкою програмного забезпечення та обслуговування комп'ютерних мереж. Такі протоколи та технічні рішення, згідно політики компанії, можуть використовуватися лише на обладнанні Cisco. Це дозволило уніфікувати мережеві стандарти, розробити цілі групи протоколів для покращення обслуговування об'єктів. Стандартизація не лише обладнання а й фізичних носіїв передачі даних дозволили модифікувати вже існуючі протоколи, які знаходяться у вільному доступі, для певних цілей та вимог, які компанія ставила перед собою. Компанією був розроблений протокол, який дозволяв виконувати функції RSTP для VLAN.

VLAN – це логічна група пристроїв, яка має можливість для взаємодії безпосередньо між собою, для цього використовується другий рівень моделі OSI. Такі

групи пристроїв можуть взаємодіяти навіть тоді, коли вони підключені до різних комутаторів. Цей принцип працює в обидві сторони, і хости, які підключені до різних VLANів та одного комутатора, не зможуть встановити зв’язок один з одним (рисунок 1.6). Встановити зв’язок таким пристроям можна лише на мережевому та вищих рівнях. В сучасних комп’ютерних мережах ця технологія є одним з головних механізмів, оскільки дозволяє будувати логічні групи хостів ігноруючи різниці в топології, а також захищати користувачів від потенційних ARP-атак [9].

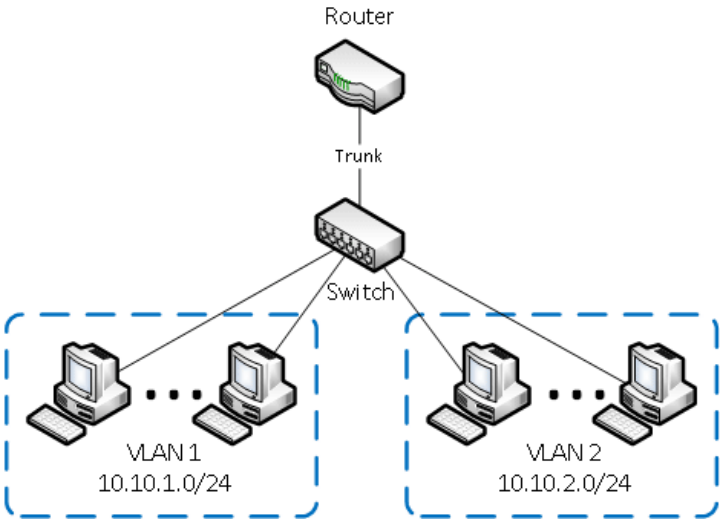


Рис. 1.6. Побудова мережі за допомогою VLAN

Створення такої технології дозволило сегментувати мережу та її трафік. Це в свою чергу дозволило організувати широкомовні домени та підвищити безпеку мережевих з’єднань, частково захистивши мережу від широкомовних штормів, оскільки пакети які він буде створювати будуть розповсюджуватись лише в тому сегменті мережі, в якому виник на другому рівні моделі OSI.

Неможливість протоколів STP та RSTP працювати з цією технологією підштовхнула компанію Cisco на розробку пропрієтарних рішень, результатом яких стали протоколи PVST, PVST+ та RPVST+.

Протокол резервування PVST заснований на протоколі STP з використанням пропрієтарних рішень, що дозволило значно розширити його можливості у порівнянні з попередником. Протокол дозволяє будувати окреме топологічне дерево для кожного

VLAN. Для цієї задачі він використовує ISL. Це протокол канального рівня, який призначений для передачі інформації про VLAN до кожного пакету в мережі. Принцип роботи протоколу ISL полягає у інкапсуляції пакету з даними з додатковою інформацією про його приналежність до того чи іншого VLANу, з додаванням нової контрольної суми в кінці кадру (рис. 1.7). Маршрутизатор, отримуючи такий пакет, деінкапсулює пакет з даними, зчитує інформацію ISL та направляє пакет по заданій адресі. Розмір службового пакету, в який інкапсулюються решта даних, складає 30 байт [10].

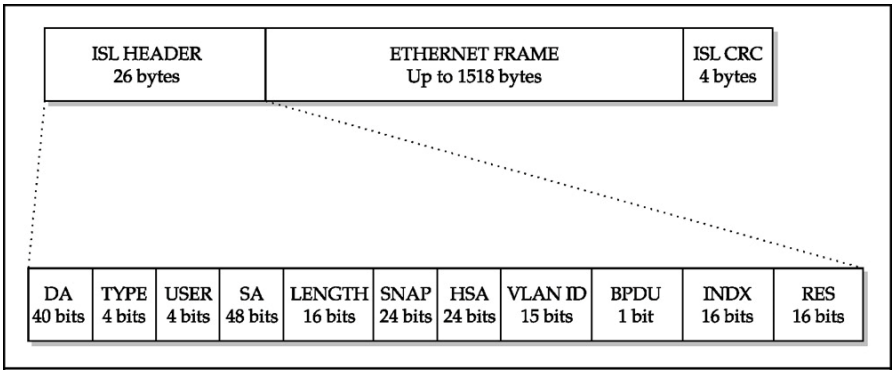


Рис. 1.7. Структура пакету даних з використанням ISL

Таким чином протокол PVST за допомогою ISL створює транк-порти, які в свою чергу дозволять порту бути розблокованим для одних VLAN-груп, та заблокованим для інших.

Таке технічне рішення дозволило обладнанню реалізовувати резервування мережі з використанням VLANів, проте реалізація мала і суттєві недоліки. Головним став сам протокол ISL, який був пропрієтарною розробкою Cisco, не підтримувався іншим мережевим обладнанням і мав деякі логічні вади. Все це спонукало розвиток наступного покоління протоколів, які змогли б досягти кращої ефективності. Такими протоколами стали PVST+ та RPVST+.

Ці два протоколи за структурою повторюють протоколи STP та RSTP відповідно, відрізняючись лише в можливості роботи з VLAN за допомогою пропрієтарних рішень компанії-розробника. Обидва протоколи використовують транк-порти як метод керування віртуальними мережами, проте на відмінну від PVST

використовують не протокол ISL, а загальнодоступний стандарт IEEE 802.1Q. Це мережевий стандарт, який дозволяє без використання інкапсуляції здійснювати управління VLAN-маршрутизацією.

В середину пакета додається 32-бітне поле після MAC-адреси отримувача та інформаційними полями оригінального кадру. Два байти з цього поля є ідентифікатором (TPID), ще два як управляючі команди (TCI). Сам TCI поділяється також на PCP, CFI та VID поля, загальну структуру кадру показано на рис. 1.8.

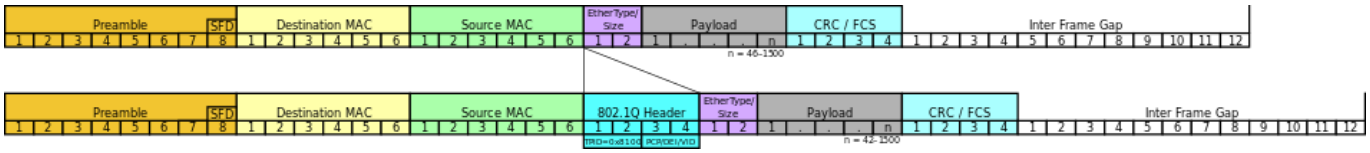


Рис. 1.8. Структура кадру даних з додаванням поля 802.1Q

Ідентифікатор тегування TPID розташоване в заголовку поля і служить для розпізнавання кадрів з додатковим тегом (tagged) та без них (untagged). Код пріоритету (PCP) вказує можливі рівні пріоритету, в діапазоні від 1 до 7, де 1 – найнижчий, 7 – найвищий. CFI – ідентифікатор “канонічного” формату. Значення 0 означає належність кадру до мережі Ethernet, значення 1 до кільцевих мереж типу Token Ring. Ці кадри можуть бути сумісні за умови, що кадр CFI 1, якщо він потрапив до мережі Ethernet, не має потрапити в порт без тегування TPID. Останнє поле VID служить ідентифікатором VLAN-інтерфейсу, до якого належить кадр даних. Значення 0 завжди вказує, що пакет не належить до VLANів і є самостійним, решта значень налаштовуються в залежності від пріоритетів комутатора.

Завдяки універсальності протоколу він успішно виконує свою функцію як в PVST+ так і в RPVST+. Окрім нового стандарту, протоколи отримали цілий ряд пропрієтарних розробок, які дозволяють ефективніше конфігурувати та підтримувати мережу. Серед цих функцій деяким необхідно надати більше уваги, ніж іншим.

Для протоколу PVST+ були розроблені функції Uplink Fast Convergence та Backbone Fast Convergence, які дозволяють протоколу зменшити час сходження після змін в топології в декілька разів. З цими пропрієтарними розширеннями протокол стає

достатньо швидким для використання у сучасних мережах, проте все ще зберігає недоліки реактивної системи реакції на проблему, навіть якщо ця реакція стала в рази швидшою. Тому наступні функції безпеки стосуються протоколу RPVST+.

Функція PortFast розроблена для протоколів PVST, PVST+ та RPVST+. Її робота – відміна блокування вказаних портів, які не беруть участі у побудові топології. В сучасній термінології ця функція називається edge port, про який було сказано вище, проте розроблена вона була для протоколу PVST+, коли функцію прикордонних портів ще не було інтегровано. Налаштування відбувається на рівні доступу.

Технологія успішно виконує покладену на неї роль, проте має один серйозний мінус, який грозить безпеці всього сегменту, і вирішення цього недоліку не є можливим. Ахілесова п’ята захована у таймерах відправки повідомлень BPDU – а саме кожні дві секунди реального часу. У сегментах з великим навантаженням, пакет BPDU за дві секунди може не дійди до кореневого комутатора, проте порт залишиться активним. Як результат отримується широкомовний шторм, коли мережевий пристрій не в змозі обробити BPDU пакет і починає бомбардуватися ARP-запитами комутаторів, які стараються уникнути переповнення таблиці маршрутизації.

Для захисту від штормів використовується функція BPDU guard, яка не дозволяє підключитися до загальної мережі пристрою, який активно відсилає пакети BPDU (як в прикладі описаному вище). Таким чином функція захищає топологію мережі від змін, які можуть вноситись ненавмисно (підключення комутатора в неправильний порт, неправильне використання IP-розеток) та навмисне (підключення зловмисником пристрою з низьким пріоритетом для зміни топології (рис. 1.9) і наступним збором корисної інформації про пакети такі як IP та MAC адреси). Проте дана функція не гарантує 100% захист від небажаних штормів, оскільки у комутатора може не вистачити ресурсів погасити шторм програмними методами навіть при його діагностуванні.

Для цього в парі з BPDU guard активно використовуються функції Port security (для ранжування максимальної кількості пристроїв за портом) та Storm Control, яка обмежує максимальну кількість групових, широкомовних та невизначених фреймів, які приймає і передає мережевий пристрій.

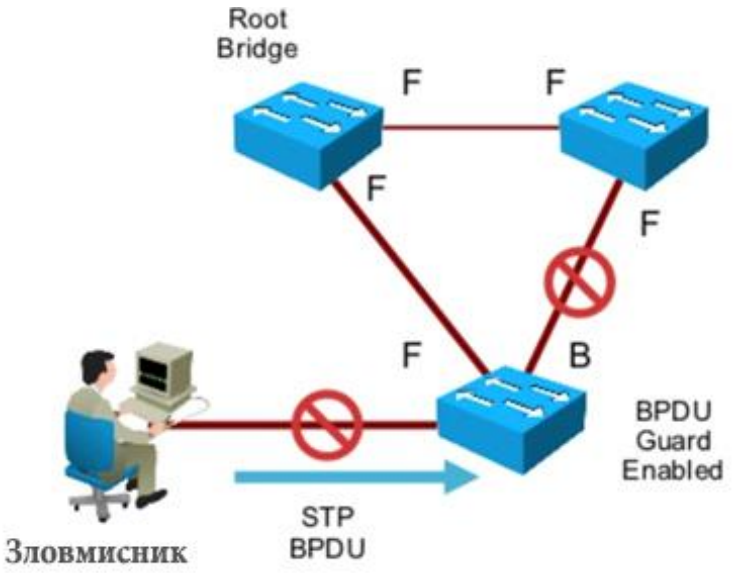


Рис. 1.9. Приклад атаки зловмисника з використанням вразливостей BPDU

Незважаючи на можливі проблеми з реалізацією деяких функцій, протоколи компанії Cisco дозволили зробити якісний стрибок у розвитку резервування, та здійснити доопрацювання протоколу для подальшого його використання у сучасних комп'ютерних мережах. Безкоштовним аналогом протоколів резервування, які можуть працювати з VLAN є протокол MSTP.

1.5. Сучасний етап розвитку технологій резервування комп'ютерних мереж. Протокол MSTP

В сучасних комп'ютерних мережах протоколи резервування відіграють роль не лише механізму захисту від збоїв, а також забезпечують інструментами балансування інженерів та адміністраторів. З постійним збільшенням навантаження на мережі всіх класів все більш нагальною стає проблема рівномірного розподілення навантаження, обрахунок фізичних можливостей мережевого обладнання. Всі ці функції включає в собі MSTP.

Протокол резервування MSTP на даний момент є найдосконалішим інструментом, який забезпечує безвідмовну роботу мережі. Ключовою відмінністю

від попередніх протоколів є те, що MSTP вміє працювати з VLANами. Це дозволило імплементувати протокол у сучасні комп’ютерні мережі.

На відмінну від пропрієтарних протоколів таких як PVST+, RPVST+ та інших, MSTP володіє глибокими архітектурними відмінностями, що дозволяє ефективніше використовувати його у великих масштабованих мережах. Протоколи Cisco лише запускають автономні екземпляри протоколів STP та RSTP для кожного VLANa, і це накладає певні обмеження:

- оскільки пропрієтарні рішення використовуються лише на обладнанні одного вендору, що виключає можливість участі в топології пристроїв інших виробників, це здійснює прямий вплив на гнучкість системи в цілому;
- кожний екземпляр здійснює обмін BPDU з інтервалом в дві секунди. Це накладає певні обмеження, якщо в топології бере участь велика кількість комутаторів;
- обладнання може обслуговувати лише певну кількість екземплярів STP/RSTP, це пов’язано з обчислювальними можливостями комутаторів та маршрутизаторів. В протоколах Cisco максимальна можлива кількість таких екземплярів = 128.

Всі проблеми попередніх версій протокол вирішує MSTP, оскільки використовує інший підхід до масштабування мереж. Для прикладу розглянемо мережу, зображену на рис. 1.10. У випадку роботи RSTP, протокол побудує математичний грав з кореневим комутатором, і буде здійснювати передачу даних з VLANів 1-100 по одному з шляхів, при цьому інший, резервний шлях буде простоювати. З точки зору забезпечення надійності такий підхід логічний, проте для забезпечення балансування та збільшення пропускної здатності алгоритм роботу RSTP не підходить.

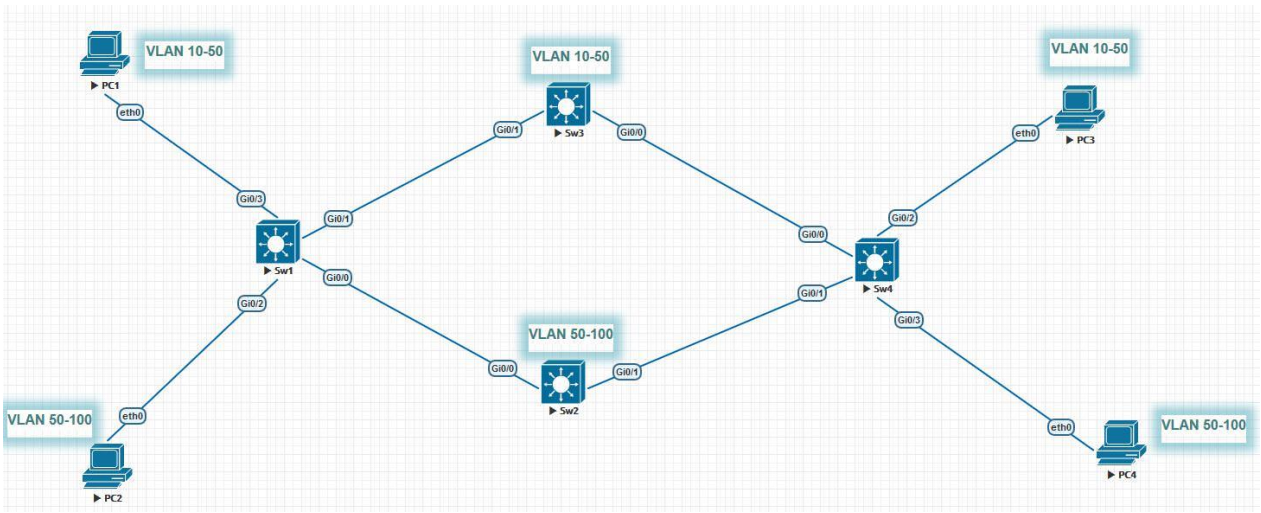


Рис. 1.10. Комп’ютерна мережа з використанням технології VLAN

MSTP кардинально змінює підхід до розгляду VLANів. Якщо попередні протоколи враховують лише топологію мережі ігноруючи при цьому налаштування віртуальних каналів, то в MSTP ми отримуємо можливість об'єднувати різні VLANи в групи, і для кожної окремої групи здійснювати побудову окремих топологій. Для мережі зображеної на рисунку 1.10 протокол MSTP надає інструменти для створення двох екземплярів на базі протоколу RSTP Для груп VLANів 1-50 та 51-100. Для першої групи вланів протокол слугуватиме Sw3, для другої відповідно Sw2, а мости передачі даних виглядатимуть як Sw1-Sw3-Sw4 для першої групи та Sw1-Sw2-Sw4 для другої.

Ідея створення екземплярів для VLANів з’явилась в протоколах Cisco, проте через обмеження таких інстанцій не набула широкої популярності в мережах великих підприємств, де кількість таких логічних об’єднань досягає тисяч. Протокол MSTP дозволяє створювати кластери дерев з використанням RSTP, що дозволяє масштабувати мережі з великою кількістю екземплярів мережевого обладнання [11].

Комутатори з ідентичною конфігурацією як на рис. 1.10 створюють окремий регіон. В цей регіон входять всі комутатори які мають власні екземпляри – MSTI (multiple spanning-tree instances). Для уніфікації таких комутаторів вони повинні мати одинакові параметри:

- region name – назва регіону;
- revision name – параметр змін в конфігурації;

- MSTI.

В кожному регіоні є інстанція MSTI 0, яка виконує аналогічну роль до VLAN 0, в який входять всі структури які не увійшли до складів інших MSTI. Копія 0 (Instance 0) називається Internal Spanning Tree (IST), і є спеціальною копією зв'язуючого дерева яка по замовчуванню існує в кожному MST-регіоні. Вона може відправляти та отримувати пакети BPDU і використовується для керування топологією всередині регіону. Всі VLAN, налаштовані в регіоні, по замовчуванню відносяться до IST.

Кореневий міст для регіону називається Regional Root Bridge. По структурі кадру BPDU в MSTP майже не відрізняється аналогічного пакету в RSTP [12]. В новій версії протоколу до стандартного пакету додається інформація про MSTI. Таким чином, для всіх VLAN і копій відправляється лише один BPDU, що значно зменшує навантаження на канал.

Для передачі пакетів за межі одного регіону протокол використовує прикордонні (як і в випадку з RSTP) порти, які називаються Boundary. Такий тип порту присвоюється також портам які стають на кордоні з протоколами STP або RSTP, оскільки MSTP може підтримувати старіші протоколи без втрати продуктивності для основної мережі. Для ілюстрації роботи протоколу з двома регіонами використаємо мережу, зображену на рис. 1.11.

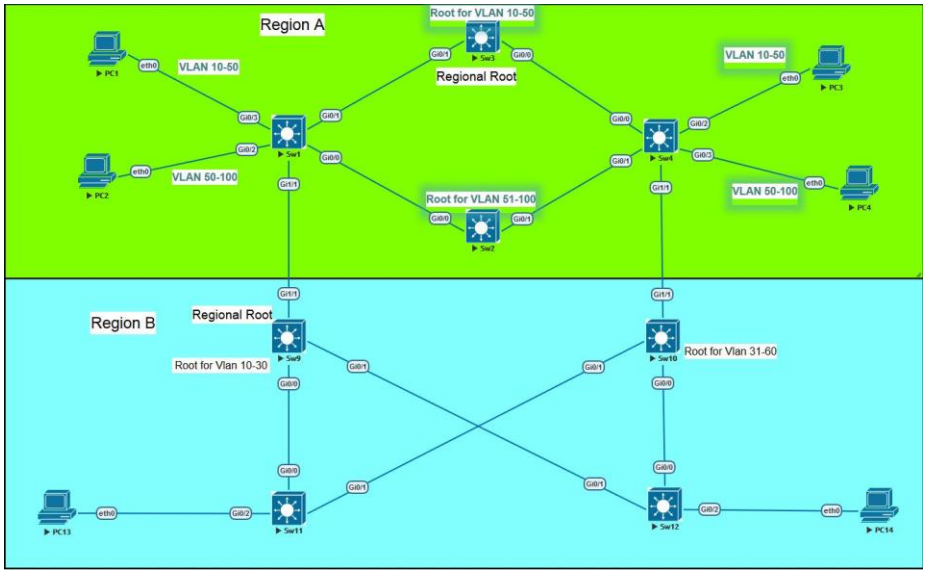


Рис. 1.11. Реалізація протоколу MSTP з використанням двох регіонів

Побудова дерева для іншого регіону має такий самий алгоритм, за виключенням необхідності вибору кореневого комутатора не за MAC-адресом (функція по замовчуванню). Щоб дерево STP будувалось в залежності від вимог за допомогою MST0 (IST) створюється загальне дерево з'єднань двох регіонів. Таке дерево називається CIST (common and internal spanning Tree). В таке дерево входять всі канали зв'язку які використовуються для з'єднання комутаторів прикордонної зони з іншим регіоном. Загальне ж дерево двох регіонів називається CST (common spanning tree).

Загальна логіка протоколу полягає в тому, що кожен регіон топології комутатори інших регіонів бачать як один великий віртуальний комутатор. Якщо подивитись на рис. 1.11 то комутатор регіону А буде бачити регіон В як один комутатор, так само як і В буде бачити А. Кожен комутатор регіону має порт, який з'єднує його з кореневим комутатором регіону, наступним вибирається один порт для регіону, який з'єднується з CIST-портами, який в свою чергу з'єднує регіони. Такі порти не відправляють BPDU пакетів а лише отримують їх, на відмінну від портів P2P в RSTP. Виключенням є лише пакети BPDU з прапором TC про зміну топології.

Для визначення пріоритетів комутаторів в кожному регіоні використовуються спеціальні функції Lowest External path cost to CIST Root bridge та Lowest Regional Bridge Identifier, які виключають можливість випадкових призначень прав.

Оскільки протокол MSTP підтримує старіші версії протоколів, розглянемо (рис. 1.12) як поводитиме себе MST якщо до регіону В приєднати сегмент де для резервування використовується пропрієтарний протокол RPVST+.

Через логічні особливості пряма взаємодія протоколів не рекомендується технічною документацією, хоча й можлива з деякими особливостями. Помилки пов'язані з використанням протоколом RPVST+ VLAN0 як службовим каналом за аналогією MST0.

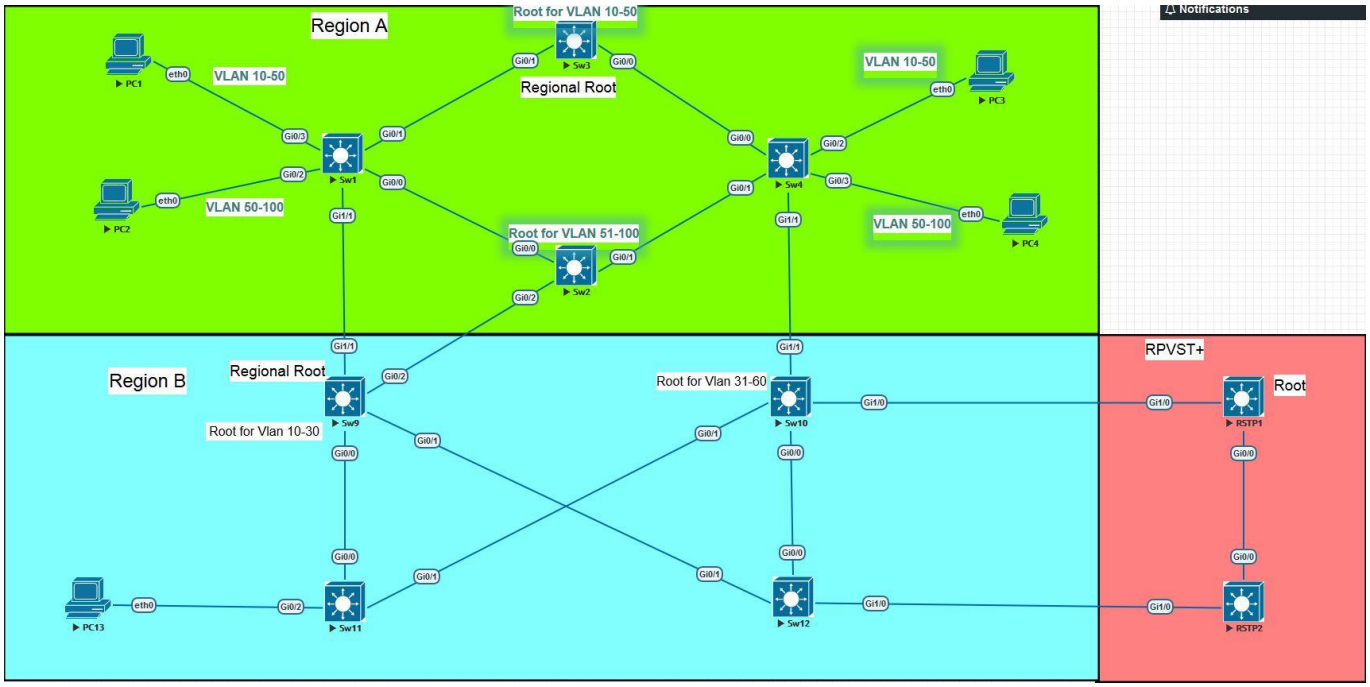


Рис. 1.12. Взаємодія мережі MSTP з протоколом RPVST+

Цілісність топології порушується, оскільки з однієї сторони для цього каналу повинен бути кореневий порт, а отримання більш високих пріоритетів змушує перейти порт в стан Designated. Протокол MSTP блокує такий порт переводячи його в стан заблокованого (BKN). Вирішенням проблеми є зміна пріоритетів VLAN-груп.

Існує більш прийнятний шлях, який в протоколі MSTP реалізований за допомогою функції PVST Simulation. Функція змушує прикордонні комутатори приймати пакети від комутаторів RPVST+, і пересилати копії їх BPDU для MSTI0 (без поля MST Extension) по всіх портах які дозволені цим портом. Таким чином протоколи які знаходяться ближче до ядра регіону не помітять змін і продовжать працювати в штатному режимі.

В цілому, завдяки роботою над помилками, розробникам вдалося створити протокол який виконує сучасні вимоги до комп’ютерних мереж. До мінусів протоколу можна віднести лише недостатню гнучкість у конфігурації дерева, оскільки всі регіони та комутатори в них повинні мати одинакові налаштування. Також MSTP підтримується не всім обладнанням. Оскільки для забезпечення адекватного функціонування необхідна велика кількість апаратних ресурсів, то можливість підтримки протоколу у обладнання початкового рівня відсутня.

Зважаючи на переваги цього протоколу над іншими він вважається найбільш досконалим протоколом резервування на сьогодні. Активно ведуться роботи над доопрацюванням протоколу MSTP та створення на його базі нового протоколу, який би усунув обмеження по кількості копій VLAN-груп та збільшив гнучкість конфігурації.

До цього моменту ми розглядали алгоритми, протоколи та функції резервування для канального рівня (2 рівень моделі OSI), проте з розвитком технологій резервування стало доступним і на рівні маршрутизації, про що піде мова нижче [13].

1.6. Методи резервування на мережевому рівні. Протоколи CARP, HSRP, VRRP та GLBP

У попередніх розділах були розглянуті різні протоколи резервування комп'ютерних мереж на другому, канальному рівні моделі представлення. PDU канального рівня є кадри, які складаються на рівні комутаторів та передаються на третій, мережевий рівень моделі OSI. Третій рівень працює з маршрутизаторами і як PDU на ньому виступають пакети даних, які передаються за допомогою четвертого рівня.

CARP – Безкоштовний протокол мережевого рівня OSI, основною задачею якого є резервування з’єднань мережевих пристроїв (хост-станції, маршрутизатори, брандмаузери), за допомогою використання одноєї IP-адреси декількома пристроями в рамках одного сегмента мереж (рис. 1.13).

Для своєї роботи протокол використовує ARP запити, і хоча він має механізми захисту, такий вибір ставить під сумнів захищеність такого інструменту від зовнішніх впливів зловмисників. CARP дозволяє виділити окрему групу хостів і задати їм одну IP-адресу. Така група отримує назву redundancy group. В межах цієї новоствореної групи один пристрій буде знаходитися в режимі передачі (master) а інші знаходитися в режимі очікування (slave). В кожен момент часу майстер відповідає ARP запитами і обробляє трафік, хост в свою чергу може одночасно належати до декількох таких груп.

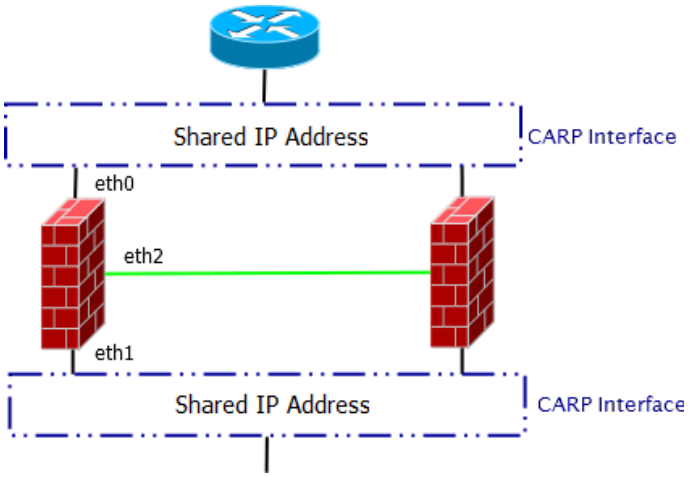


Рис. 1.13. Приклад реалізації протоколу CARP для резервування брандмаузерів

Протокол широко застосовується як інструмент для резервування брандмаузерів у мережах корпорацій. Віртуальна IP-адреса майстра виступає в ролі шлюза за замовчуванням для хостів. У випадку відмову майстра групи, його роль відразу переймає інший брандмаузер і продовжить обслуговувати хост-станції в мережі. Архітектура протоколу CARP зобов'язує пристрої, які його використовують, фізично знаходитися в межах однієї мережі.

В протоколі, як і в MSTP, присутня функція балансування трафіку в одному сегменті мережі, де він використовується. Для виконання балансування протокол використовує ARP-запити, що значно впливає на безпеку не лише сегмента, а й мережі в цілому. В інструкціях та технічній літературі протокол рекомендується використовувати в парі з інструментами захисту вразливих місць ARP (рис. 1.14).

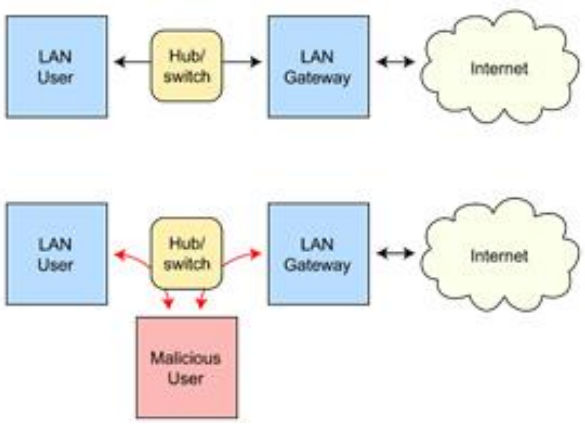


Рис. 1.14. Приклад атаки на мережу за допомогою вразливості протоколу ARP

Оскільки протокол був розроблений в 90-х роках минулого сторіччя, незважаючи на імплементування сімейства протоколів резервування на мережевий рівень, наділений серйозними недоліками, а саме:

- сервіси, яким необхідне постійне стабільне з’єднання, як от протокол захищених ключів SSH, не можуть в повній мірі співпрацювати з протоколом CARP, оскільки вони відчують зміну ведучого мережевого екрану та запросять нове з’єднання;
- протокол не може здійснювати синхронізацію даних між застосунками. Для вирішення цієї проблеми необхідно застосовувати додаткові інструменти, що є небажаним в мережах великих масштабів;
- неможливість використання протоколу для між сегментних з’єднань, оскільки при відправці ARP запитів, маршрутизатори завжди будуть відправляти їх на один і той самий хост.

Незважаючи на недоліки, протокол CARP часто використовується як безкоштовна альтернатива пропрієтарним протоколам HSRP, VRRP та GLBP, про які нижче [14].

Створення цілого сімейства протоколів резервування для третього рівня мережевої взаємодії, компанія Cisco почала з протоколу HSRP.

Протокол HSRP за принципом роботи схожий з вищеописаним CARP. Проте завдяки інтеграції пропрієтарного протоколу в уніфіковане середовище, розробники отримали більше можливостей щодо розширення його функціоналу у порівнянні з безкоштовним аналогом.

Активний маршрутизатор групи займається передачею пакетів з однієї підмережі в іншу. Пасивні ж мережеві пристрої очікують своєї черги для роботи, фактично простоюючи цей час (рис.1.15). Згідно термінології Cisco, група об’єднаних маршрутизаторів, які очікують, називаються групою резервування (Standby group).

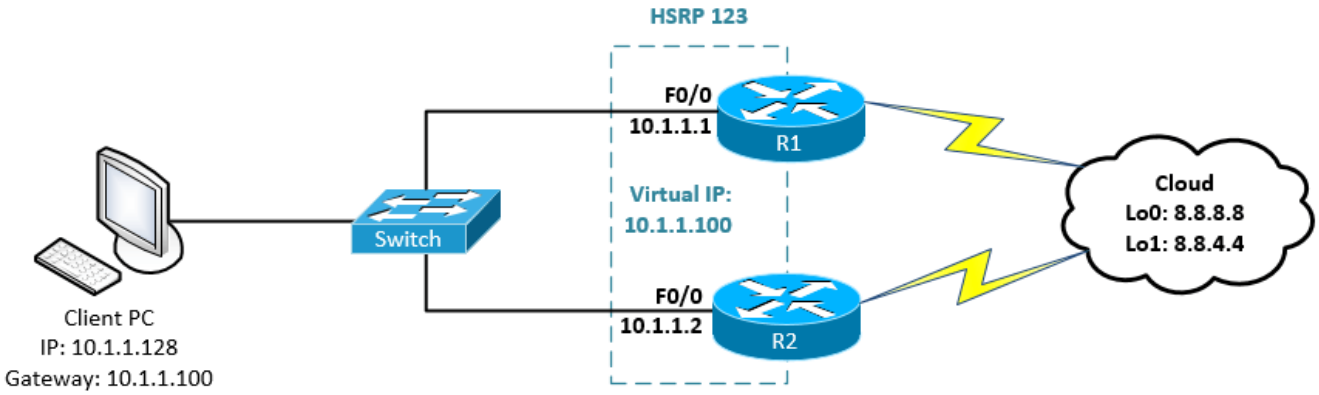


Рис. 1.15. Використання протоколу HSRP

Для вибору основного маршрутизатора протокол використовує пріоритети, якщо ж у двох мережевих пристроїв пріоритет однаковий, то головним буде вибраний то пристрій, який обслуговує більшу кількість запитів.

Маршрутизатори взаємодіють між собою за допомогою hello-повідомлень, які надсилаються за допомогою групової (multicast) передачі на UDP порт 1985. Повідомлення coup відправляється маршрутизатором, який знаходиться в режимі очікування якщо він хоче взяти на себе роль активного пристрою в групі. Для цього він має отримати повідомлення Resign від активного пристрою на даний момент, яке означає, що пристрій виходить з ладу, і виникає необхідність зміни активного пристрою в мережі.

Окрім таких керуючих сигналів групи, пристрої які знаходяться в режимі очікування, можуть перебувати у таких станах:

- початковий стан, який вказує на те, що протокол HSRP вимкнений (Initial);
- пристрій отримав повідомлення hello від активного пристрою, проте ще не визначив свою IP-адресу (Learn);
- маршрутизатор визначив IP-адресу, але не став активним пристроєм, і лише отримує повідомлення (Listen);
- при виході активного пристрою з ладу, маршрутизатор бере участь в обміні повідомлення про обрання нового активного пристрою (Speak);
- прилад є кандидатом на роль активного пристрою, він відправляє hello-повідомлення. Пристрій з таким станом має бути лише один.

Таким чином протокол HSRP виконує резервування шлюзу «останньої надії», по якому здійснюється передача даних до інших сегментів мережі [15]. Основною вимогою до такого типу протоколів є балансування, оскільки вся інформація в сегменті проходить через канали, які обслуговує HSRP. Для цього використовується покращена версія протоколу MHSRP. Вона дозволяє здійснювати налаштування резервування не як одної великої групи маршрутизаторів, а як декількох груп в одному широкомовному сегменті. Таким чином отримується два активних маршрутизатора в кожній з груп замість одного. Така схема часто застосовується при використанні протоколів динамічної маршрутизації пакетів, оскільки MHSRP дозволяє координувати ICMP запити для знаходження кращого шляху трафіку в сегменті.

Після завершення створення M/HSRP компанією Cisco одразу почалась робота над протоколом VRRP, яка велась паралельно з групою ентузіастів. Після закінчення роботи над протоколом компанія відсудила права на використання протоколу для себе, таким чином де-факто зробивши його пропрієтарним, хоча участь в розробці брало безліч людей.

Новий протокол не став переробляти архітектуру свого попередника а лише вдосконалив наявні механізми. Протокол VRRP використовує декілька таймерів для більш узгодженої дії маршрутизаторів всередині кластеру. Для обміну командами використовується той самий механізм, що в протоколі HSRP, проте завдяки таймерам нова версія протоколу може взаємодіяти з IP-телефонією, що дозволяє повноцінно використовувати протокол у мережах сучасних підприємств. Також протокол отримав підтримку IPv6. Завдяки цьому він став домінуючим протокол резервування третього рівня до закінчення робіт GLBP, ще одним пропрієтарним рішенням Cisco.

Протокол GLBP – на сьогоднішній день є найновішим протоколом у сімействі FHRP. Нова версія працює аналогічно проте не ідентично попереднім версіям протоколу. Протокол забезпечує розподіл навантаження на декілька маршрутизаторів кластера (рис 1.16).

Мережеве обладнання в середині групи вибирає шлюз, який буде використовуватись як активний AVG для даної групи. Паралельно з цим вибирається резервний маршрут, де AVG призначає MAC-адресу кожному члену групи. Такі

пристрої називаються AVGs. Механізм AVG відповідальний за розсилання ARP-пакетів на запити до віртуального маршрутизатору.

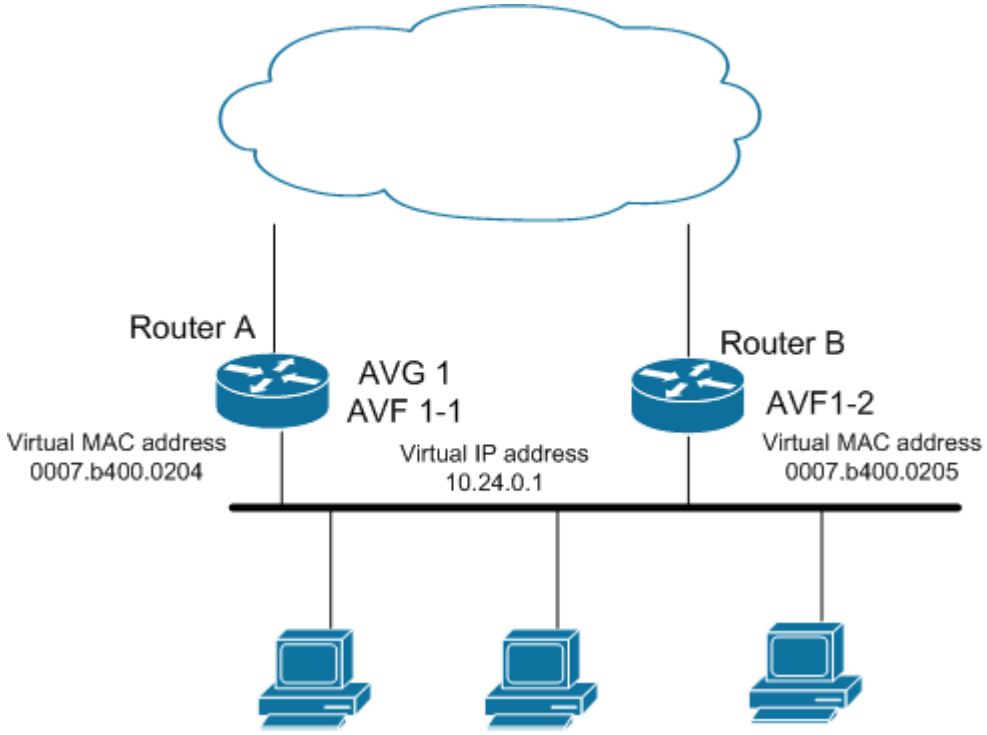


Рис.1.16. Створення мостів передачі даних протоколом GHBP

Маршрутизатори обмінюються hello пакетами кожні три секунди і надсилають їх на UDP порт 3222. Пріоритет для кожної групи роутерів вибирається за допомогою функції GLBP Gateway Priority. Пріоритет задається в діапазоні значень від 1 до 255 за допомогою команди ghlp priority.

Окрім забезпечення оптимального використання пропускної здатності кластеру, протокол також здійснює ефективне балансування навантаження для запобіганню перенавантаження сегменту [16]. По замовчуванню протокол не проводить балансування, вибираючи на запити клієнтів таблицею MAC-адресації. Існують також режими балансування за допомогою ваги маршрутизатора з використанням протоколу NAT. В такому випадку по замовчуванні буде використовуватися метод балансування Round-robin, який ми детальніше розглянемо пізніше.

Таким чином, завдяки розвитку технологій наразі ми маємо цілу низку протоколів резервування для мережевого рівня. Це дозволяє використовувати метод

надлишковості в сучасних мережах, незважаючи на поступовий відхід від резервування у малих мережах. У розподільчих мережах провайдерів, дата-центрах та інших великих мережевих вузлах, методи резервування залишаються необхідними для забезпечення відмовостійкості у випадках, коли програмні методи виходять з ладу. У мережах менших масштабів конкурентом фізичного резервування стала технологія агрегації каналів, яка збільшила гнучкість мережі та дозволила створювати нові способи резервування.

1.7. Технологія агрегації каналів комп'ютерних мереж. Статична агрегація

Як було сказано у розділі 1.6, економічні аспекти реалізації надлишковості в комп'ютерних мережах змушували шукати нові методи для забезпечення відмовостійкості. Окрім фінансової частини, проблема підходу з використанням резервних пристроїв все більше впливала на загальну конфігурації мережі. Стало критичним ігнорування додаткової пропускної здатності яку могла б отримати мережа, проте протоколи зв'язуючих дерев тримали їх вимкненими для забезпечення контролю над логічними петлями. Комітет з розробки рішень цих проблем пожертвував певною гнучкістю системи, ввівши уніфікацію з'єднань між комутаторами та їх налаштуваннями, проте це дозволило агрегувати канали передачі даних в один логічний, що дало початок розвитку технології.

Агрегація каналів дозволяє об'єднувати багато фізичних каналів передачі даних в один логічний. Така логічна структура дозволяє збільшити пропускну здатність мережі, сумуючи швидкість передачі даних кожного каналу в загальний логічний. На рис. 1.17 показана фундаментальна різниця підходів до вирішення проблеми відмовостійкості. На відмінну від надлишкового резервування, агреговані канали застосовують всі наявні з'єднання для передачі даних, таким чином збільшуючи пропускну здатність каналу. Це дозволяє ефективно застосовувати технологію в сучасних комп'ютерних мережах.

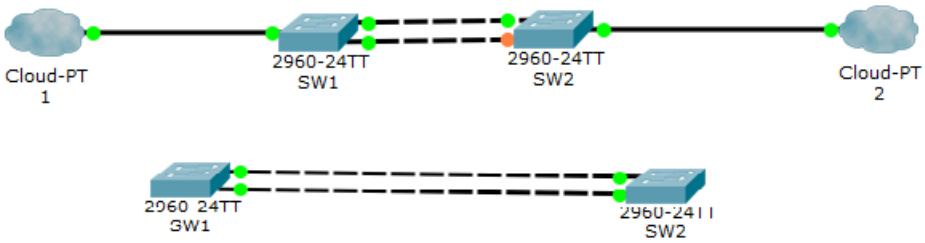


Рис. 1.17. Порівняння технологій резервування та агрегації

Уніфікація, необхідна для створення агрегованого каналу, повинна зберігатися у наступних параметрах портів обладнання:

- швидкість передачі даних (speed);
- дуплексний режим передачі даних (full duplex);
- керований канал для адресування VLANів (native VLAN);
- дзеркальний діапазон дозволених логічних груп;
- режим trunk для обох сторін передачі даних;
- тип інтерфейсу, які беруть участь в передачі.

Такі обмеження створюють певні бар'єри при роботі з багатовендорним обладнанням мережі, проте крім недоліків це має і свої переваги. Попередні розділи були присвячені протоколам надлишкового резервування, і оскільки перевагою цих протоколів є мультивендорність, це зумовили появу цілих груп протоколів, які не можуть співпрацювати один з одним, тобто теоретичний плюс перетворився в практичний мінус. Діаметрально протилежна ситуація склалася з технологією агрегації. Завдяки своїм чітким вимогам в обладнанні та логічній адресації, протоколи які забезпечують роботу агрегованих каналів, взаємопідтримувані практично на всіх мережевих пристроях, а відмінності реалізації пропрієтарних рішень такі незначні, що ними можна знехтувати.

Агрегування каналів можна налаштувати двома способами: статично та динамічно. Статична агрегація каналів – це ручний процес налаштування адміністратором комутаторів в мережі, які потребують резервування. Для цього на обладнанні різних вендорів існують спеціальні інструкції, які дозволяють мінімізувати людський фактор і здійснити правильне налаштування. Перевагою

такого методу є статичність, при безпомилковому налаштуванні сегменту відповідно до запитів мережі, такий канал не потребуватиме додаткових змін впродовж всієї роботи сегменту. Це дозволяє відсутність затримок пов’язані з зміною конфігурації мережі. До недоліків такого агрегування відноситься традиційно людський фактор і відсутність підтримки зворотного зв’язку. При помилках конфігурації в статичній агрегації існує ризик отримання логічних петель та некоректної роботи сегмента мережі в цілому.

Як альтернатива статичному існує динамічне агрегування. Для реалізації такого типу агрегування використовуються безкоштовний протокол LACP та пропрієтарна розробка Cisco – протокол PAgP. Оскільки відмінності між протоколами несуттєві, надалі розглядається безкоштовний та прийнятий всіма виробниками LACP.

1.8. Динамічна агрегація каналів комп'ютерних мереж. Протокол LACP

Через різні масштаби мереж та сегментів мережі, статична агрегація мережі стає менш ефективно. Це пов’язано з необхідністю ручного налаштування кожного комутатора, де уникнути помилок стає все важче. Протокол LACP (link aggregation control protocol) призначений для об’єднання каналів передачі в один логічний. В випадку використання динамічного агрегування, протокол може діагностувати пошкоджений канал передачі та повідомити про це комутатор, що в статичній маршрутизації неможливо. Протокол описаний в стандарті IEEE 802.3ad.

Перед налаштуванням фізичних аспектів для правильної роботи протоколу необхідно ознайомитися з логікою агрегування. По замовчуванню протокол STP буде блокувати друге з’єднання задля уникнення логічних петель в сегменті. Для того, щоб змусити його зняти блокування необхідно об’єднати канали передачі даних в одну логічну групу, після чого STP буде бачити два з'єднання як один канал передачі даних. Відповідно конфігурація каналу буде відбуватися для всіх каналів передачі одночасно.

Протокол підтримує одночасну агрегацію до 16-ти фізичних з'єднань, пропрієтарні ж рішення підтримують сотні з'єднань і сфера їх застосування дещо відрізняється. Після утворення групи каналів, протокол LACP починає розсилання

пакету suspended всім портам комутатора (рис. 1.18). Якщо порт не відповідає налаштуванням групи, йому присвоюється статус неактивного. Оскільки для передачі даних в каналі використовується схема master-slave, то для початку передачі даних одна сторона каналу зобов'язана заходитися в пасивному стані (passive) а інша у активному (active). Для передачі службової інформації протокол використовує широкомовну адресу 0180.C200.0002, яку слухають всі учасники.

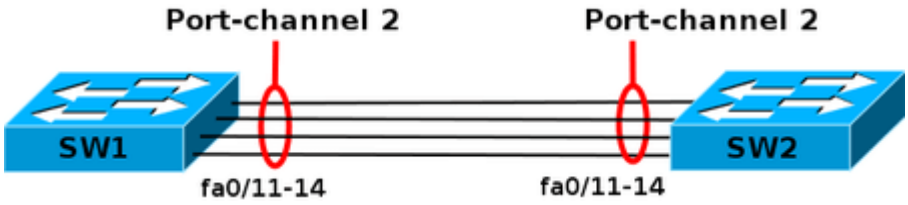


Рис. 1.18. Агрегування каналів за допомогою протоколу LACP

Агрегування третього рівня мережевої взаємодії відрізняється лише відсутністю агрегування фізичних з'єднань, оскільки протоколи які працюють на цьому рівні можуть взаємодіяти лише з каналами даних. В всьому іншому налаштування та реалізація протоколу відбувається ідентично.

1.9. Методи балансування навантаження в агрегованих каналах передачі даних

Завдяки агрегації каналів передачі ми отримуємо можливість використовувати мережу для передачі великої кількості даних. У мережах великих підприємств гостро постає питання балансування всього трафіку, який передають такі канали. Балансування – це сукупність методів які дозволяють оптимізувати використання ресурсів обладнання таким чином підвищуючи відмовостійкість мережі в цілому.

Таке балансування може застосовуватись на третьому рівні моделі OSI та вище, оскільки фізичний та канальний рівні працюють з електричними сигналами та кадрами відповідно, функціоналу обладнання яке працює з цими PDU недостатньо для забезпечення балансування. Єдиним винятком є використання балансування для агрегованих каналів з використанням протоколу LACP. Для балансування такого

трафіку використовується схема маршрутизації та трансляції адрес хостів, або ж за допомогою TCP-проксі серверів.

Балансування на канальному рівні забезпечується за рахунок спеціальних інтерфейсів, які відповідають за розподілення ARP-запитів до серверів. Отримуючи запит від клієнта, балансувальник буде розподіляти навантаження між серверами завдяки перетворенню направлений запит в груповий або широкомовний. Всі сервери повинні відповідати на ARP запит одною MAC-адресою. Це дозволяє відправити запит на групу (multicast) чи на всі (broadcast) сервери одночасно, де кожен згідно налаштувань обирає, відповідати йому на запит чи проігнорувати його. До плюсів такого балансування можна віднести те, що воно не залежить від протоколів вищих рівнів, мінімізація витрат на розгортання балансування та використання однієї публічної адреси. З мінусів можна виділити те, що такі сервери які підлягають балансуванню повинні знаходитись в одній підмережі, що викликає проблеми з масштабованістю.

В цілому механізм балансування навантажень мережевого рівня мало відрізняється від канального, за однією особливістю. Оскільки пакети даних, які отримує балансувальник, повинні бути змінені в полі destination IP, для сервера який буде виконувати запит. Сервер отримує такий пакет, обробляє його і надсилає відповідь (рис 1.19). Балансувальник знову приймає пакет з даними, переробляє його та відправляє адресату. Це приводить до додаткового навантаження на балансувальник, проте серверна взаємодія цілком прозора для інших елементів в мережі, що дозволяє уникнути конфлікті, оскільки сервер думає, що отримує запити напряму від клієнта.

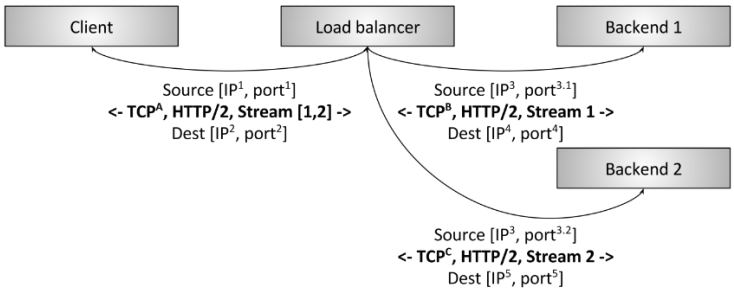


Рис. 1.19. Алгоритми балансування трафіку мережевого рівня

Балансування на четвертому (транспортному) рівні здійснюється в основному за допомогою алгоритму ECMP (equal-cost multi-path). Сучасні маршрутизатори здатні здійснювати балансування навантаження TCP пакетів, транслюючи для цього одну підмережу по різних маршрутах передачі. Балансувальник в такому випадку повинен вибирати оптимальні шляхи розподілення навантаження. Обмеження виникають у розподілення маршрутизатром пакетів даних таким чином, щоб дані в рамках однієї TCP сесії потрапляли на один і той самий сервер. Друге обмеження виникає при використанні статичної маршрутизації в сегменті мережі, оскільки необхідно вносити зміну про стан серверів. Для цього використовується протоколи динамічної маршрутизації, такі як BGP, EIGRP та інші. Для цього на кожен з серверів необхідно встановити BGP маршрутизатор, який буде анонсувати мережу для передачі пристроям, які підтримують аналогічну технології маршрутизації даних. Через фізичні обмеження BGP існують затримки, що зменшують загальну відмовостійкість мережі. Існують також обмеження у кількості ECMP для кожного маршрутизатора.

Балансування даних на глобальних рівнях OSI (прикладний, мережевий) відбувається з урахуванням апаратних обмежень пристроїв. Популярним алгоритмом для забезпечення балансування за допомогою DNS є метод Round Robin [17]. Суть алгоритму полягає у використанні DNS-сервера як балансувальника навантаження. Для цього в таблицю добавляються записи з різними IP-адресами всіх необхідних серверів, в циклічному порядку. Тобто отримавши запит, алгоритм буде направляти його до першого сервера, наступний запит до другого, третій до третього, п’ятий до першого і так далі (рис. 1.20). Популярність такого рішення забезпечується низькою вартістю та швидкістю розгортання його роботи, а також можливістю здійснювати балансування як на канальному так і на глобальних рівнях моделі представлення.

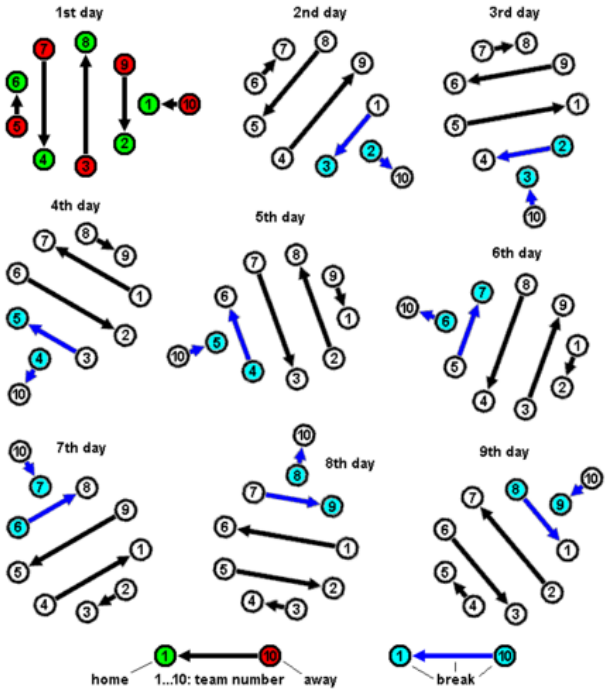


Рис.1.20. Використання алгоритму Round Robin для балансування запитів

До мінусів такого методу можна віднести проблеми з відключенням серверів які беруть участь у обміні, оскільки DNS сервер розраховує на кожен з них. Для вирішення такого обмеження використовуються описані вище протоколи резервування маршрутизаторів CARP або VRRP.

Також для балансування на глобальному рівні використовуються методи проксі з’єднань та переправлення запитів. Суть алгоритму full proxy полягає в тому, що балансувальником виступає проксі сервер який має можливість зазирати всередину пакетів [18]. Це дозволяє йому редагувати HTTP заголовки і добавляти туди інформацію про IP адресата, щоб сервер одразу знав куди відправити сформовану відповідь. При правильному використанню цієї функції також можна забезпечити мережевий захист від багатьох видів атак ззовні. Це дозволяє сортувати типи запитів і розподіляти їх між групами серверів. До мінусів методу традиційно відносять додаткову точку можливого виходу з ладу, що зменшує загальну надійність системи, оскільки проксі використовує багато ресурсів і потребує налаштування окремих з’єднань для кожного з протоколів.

Метод пересилання запитів як засіб балансування має дуже обмежене коло використання, в основному він використовується для балансування HTTP трафіку.

Коли балансувальник отримує HTTP запит від клієнта, він відправляє у зворотному напряму помилку 302 move temporary з даними про адресу необхідного сервера, до якого і буде звертатися хост в подальшому. За рахунок додаткового відклику до клієнта та збільшення запитів вдвічі, алгоритм використовується лише вибірково.

Окрім цього існують і вузькоспеціалізовані методи балансування [19]. Такі алгоритми використовуються у спеціалізованих дата-центрах, мережах провайдерів та інших схожих мережевих структурах для забезпечення відмовостійкості з урахуванням специфічних потреб обладнання [20].

1.10. Висновки до розділу 1

Здійснивши оглядSTP втратила роль протоколу який забезпечує резервування вузлів, проте практично в всіх сучасних мережах протокол присутній і виконує важливу роль щодо знаходження та відсікання можливих петель в мережі, забезпечуючи таким чином надійний захист від широкомовних штормів, які здатні вивести з ладу весь сегмент мережі.

Активно сімейством протоколів надлишкового резервування користуються великі мережі, оскільки зважаючи на кількість даних які обробляють такі центри, покладатися лише на логічні методи резервування не є доцільним. Таким чином протокол не втратив своєї актуальності, а лише змінив пріоритет свого застосування, ставши певного роду страхувальником більш сучасних технологій по обробці, балансуванні та агрегації даних в комп’ютерних мережах.

Технологія агрегації в свою чергу з часу створення все більше і більше стає основною технологією організації передачі даних в мережах. Завдяки уніфікації та підтримки технології всіма вендорами практично без змін, що дозволяє організовувати відмовостійкі мережі, збільшувати пропускну здатність каналів та забезпечувати захист передачі інформації. У зв’язку новими рівнями пропускної здатності каналів та відповідним збільшенням навантаження на мережеві пристрої через це, технологія агрегації активно звертається до резервування кореневих вузлів мережі за допомогою надлишковості та алгоритмів балансування.

РОЗДІЛ 2
АНАЛІЗ ТА ВИБІР ОПТИМАЛЬНИХ МЕТОДІВ ТА ТЕХНОЛОГІЙ РЕЗЕРВУВАННЯ ТА АГРЕГАЦІЇ КАНАЛІВ ПЕРЕДАЧІ ДАНИХ

Протоколи резервування та агрегації каналів в комп'ютерних мережах почали розвиватися паралельно з часу створення першого з'єднання між двома робочими станціями. Завдяки цьому до сьогодні в наших руках є велетенська кількість інструментів для забезпечення надійної передачі даних між мережами. Одночасно це можна вважати як перевагою так і недоліком.

На практиці часто використовуються найсучасніші технічні рішення, що не завжди доцільно. У своїй науковій праці я хочу досягнути певного рівня балансування з використання технологій забезпечення надійності та відмовостійкості мереж. Для цього необхідно визначити пріоритет, який має виконувати той чи інших сегмент мережі. Здійснити обґрунтування технічної доцільності використання тих чи інших пристроїв, затрат ресурсів для підтримки тих чи інших технічних рішень тощо.

Проведення дослідження з ефективності використання методів резервування та агрегації, відбувається на таких рівнях моделі представлення – фізичному, канальному, мережевому прикладному. Завдяки такому підходу та отриманим результатам можна зробити висновки, а технічні рішення які були прийняті на їх основі, використовувати в реальних системах.

2.1. Порівняльний аналіз методів резервування та агрегації комп'ютерних мереж на фізичному рівні

Фізичне середовище передачі даних у моделі OSI оперує бітами даних, які передаються за допомогою електричних сигналів від відправника до отримувача. До обладнання яке працює на першому рівні відносяться повторювачі, хаби, точки доступу та інше обладнання, яке виконує функцію підсилення сигналу, проте не його обробку.

До методів резервування фізичного середовища відносять перш за все фізичні з’єднання між мережевими пристроями рівня 2 та вище. Для передачі даних за допомогою фізичного середовища використовується кодування та відповідне декодування сигналу (рис. 2.1).

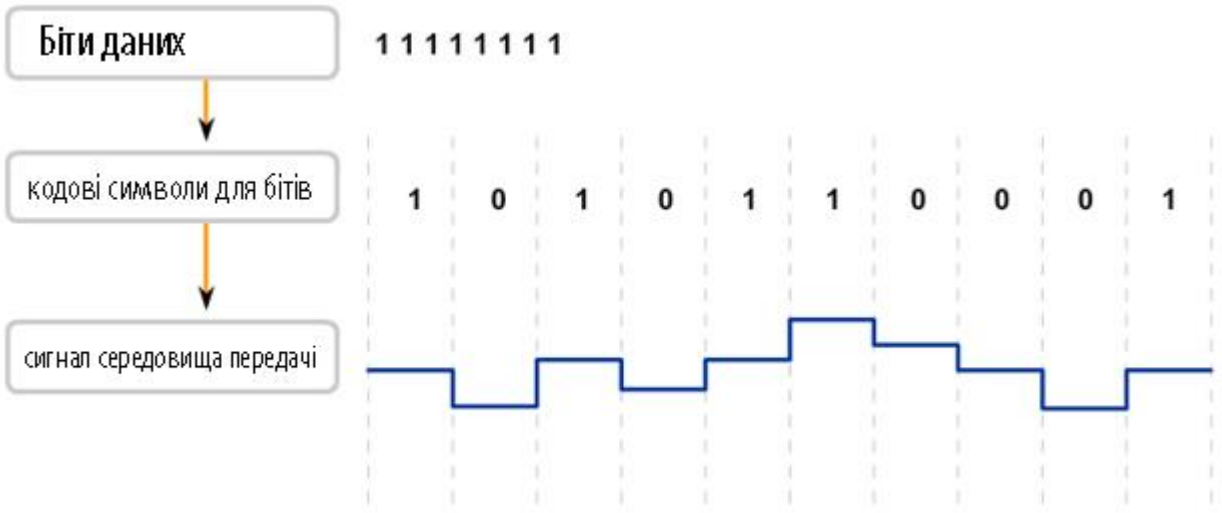


Рис. 2.1. Декодування сигналу на фізичному рівні

Найбільш поширеними рішеннями середовища передачі даних є вита пара та оптоволоконний кабель. Кожен з рішень має свої переваги та недоліки. Вита пара – це одна або декілька пар ізольованих провідників, які служать для передачі електричних сигналів по них. Складає основу сучасних комунікаційних систем. Завдяки дешевизні та простоті розгортання використовується практично в всіх комп’ютерних мережах. До ключових недоліків кабелю відноситься погане масштабування, оскільки через фізичні обмеження довжина кабелю для передачі даних не може перевищувати 200м. За допомогою повторювачів довжина кабелю може сягати до 800 метрів. Така відстань є прийнятною практично для всіх видів мереж типу LAN, які будуються у межах офісу, поверху та будівлі [21]. Для впорядкування черг зчитування в таких мережах використовують синхронізацію (рис. 2.2). Кабель оптичного волокна – це сучасне технологічне рішення, яке використовує для передачі сигналів не електричні а світлові імпульси, що значно впливає на якість

надання послуг. Використання такого тип кабелю дозволяє масштабувати мережі типу WAN та MAN.

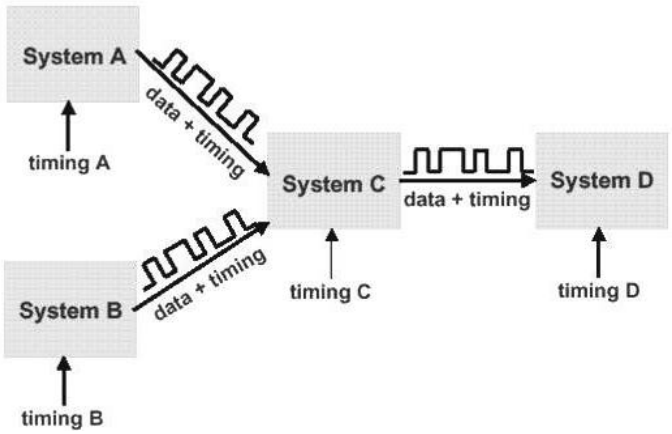


Рис. 2.2. Синхронізація даних в LAN-мережах

Співвідношення до одномодових волокон:

$$\sigma = 10^{-12} \cdot \Delta\lambda \cdot \sigma_{\text{н}}$$

де Δλ – ширина смуги джерела випромінення.

Зважаючи на особливості кабелю, довжина ділянки регенерації:

$$L_{p2max} = \frac{0{,}25}{\sigma \cdot B}$$

де B – швидкість передачі даних в каналі.

Таким чином використання оптоволоконного кабелю є доцільним з точки зору масштабованості мережі та забезпечення надійності через відсутність електромагнітних перешкод [22]. Однак для використання такого середовища передачі необхідне спеціальне обладнання та перетворювачі сигналів, які здійснюватимуть перетворення оптичних імпульсів в електричні для подальшого транспортування. Проблема оптоволоконних кабелів полягає у вартості конструкції та

її обслуговуванні, що робить доцільним використання витої пари в багатьох рішеннях, оскільки недоліки мідного середовища проявляються лише на великих відстанях.

Кількість з'єднань для забезпечення функціонування резервного каналу зв'язку обмежується не лише протоколами, а також їх доцільністю. Максимальна кількість інтерфейсів в протоколі LACP = 4. Проте для забезпечення безвідмовної роботи між двома комутаторами L2 з використанням протоколів сімейства STP така кількість з'єднань приведе до збільшення кількості BDPU запитів, що негативно вплине на роботу сегмента мережі з використанням такої кількості з'єднань.

2.2. Обґрунтування вибору засобів резервування канального рівня

Основна робота по забезпеченню резервування на другому рівні моделі OSI виконується сімейством протоколів STP, детально описаних в розділі 1. Окрім їх можливостей щодо забезпечення безвідмовної роботи необхідно звернути увагу на ряд їх особливостей, підтримку обладнання та витрату ресурсів.

Протокол MSTP на сьогодні є найбільш технічно досконалим протоколом сімейства. Однак для використання його на комутаторах другого рівня, навіть таких як Cisco 2960, необхідна велика кількість апаратних ресурсів. Протокол здійснює обробку даних та виконує балансування згідно заданого алгоритму, це приводить до великого навантаження на комутатори [23]. При надлишковому використання ресурсів комутатор може не встигати обробляти BPDU пакети через зайнятість пошукам кращих шляхів для пакетів, створюючи простій в сегменті. В такому режимі роботи комутатор починає втрачати оптимальну швидкість роботи, як зображено на рис. 2.3.

Можна зробити висновок, що використання складних протоколів як MSTP слід обмежити центральним сегментом мережі, оскільки обладнання яке використовується для ядра здатне опрацьовувати збільшену кількість пакетів від протоколу. Для локальних сегментів мережі доцільно використовувати протоколи резервування STP та RSTP. Незважаючи на довгу збіжність першої версії протоколу, він виконує функцію обмеження створення петель в сегменті.

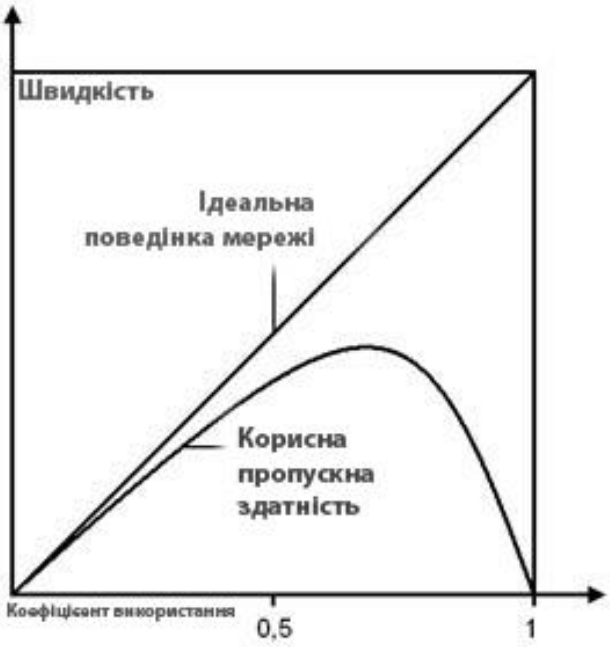


Рис. 2.3. Графік залежності пропускної здатності від коефіцієнта використання

Протокол не рекомендується вимикати навіть при відсутності петель в топології. Середнє напрацювання на відмову в сегментах мережі які обслуговують протоколи STP та RSTP складає 1035 секунд згідно з дослідженнями Маліка Кхіяла [24].

Рис. 2.4. Графік напрацювання на відмову

Середній наробіток на відмову:

$$T_o = \frac{\sum_i^n t_{oi}}{n},$$

де t_{oi} – наробіток відновного об’єкта між двома його сусідніми відмовами,

n – кількість відмов об’єкта.

У випадку необхідності надійного зв’язку та уникнення втрат даних, протокол STP, зважаючи на внутрішні затримки таймерів втрачає велику кількість пакетів (рис. 2.5) через перебудову топологічного дерева кожен раз, коли в сегменті з’являється новий пристрій.

Рис. 2.5. Втрати пакетів протоколом STP

Аналізуючи отримані дані можна дійти висновку про взаємозамінність протоколів резервування в локальних сегментах мережі якщо йдеться лише про захист від широкомовних штормів. У випадку забезпечення безперебійної передачі з врахуванням навантаження мережевого обладнання, доцільніше використовувати протокол RSTP.

2.3. Комбінування технологій агрегації та резервування для мережевого рівня

Резервування пристроїв третього рівня можливе з застосуванням різних технологій. Використання агрегації каналів для забезпечення збільшення пропускної здатності каналу для маршрутизаторів є необхідністю, оскільки мережеві пристрої третього рівня складають ядро мережі, яке приймає основну частину навантаження. Протокол LACP підтримується всіма вендорами, тому для забезпечення агрегації він використовується практично в всіх технічних рішеннях, винятком є пропрієтарні протоколи для використання у спеціалізованих структурах.

Існують два режими агрегування, динамічне та статичне, були розглянуті у розділі 1. За допомогою статичного агрегування можна отримати монолітну структуру. Такий варіант агрегування пропонує виконувати компанія Cisco при конфігуруванні свого обладнання (яке попри це підтримує динамічний LACP). З точки зору безпеки статичне агрегування краще, оскільки такий метод не використовує ARP запитів, унеможливлюючи таким чином цілий ряд атак з використанням недоліків протоколу. Згідно з дослідженням Шаміма, збільшення запитів з використанням динамічного LACP (рис. 2.6), підвищує можливість загрози атаки на мережу за допомогою номеру послідовності в протоколі TCP [25].

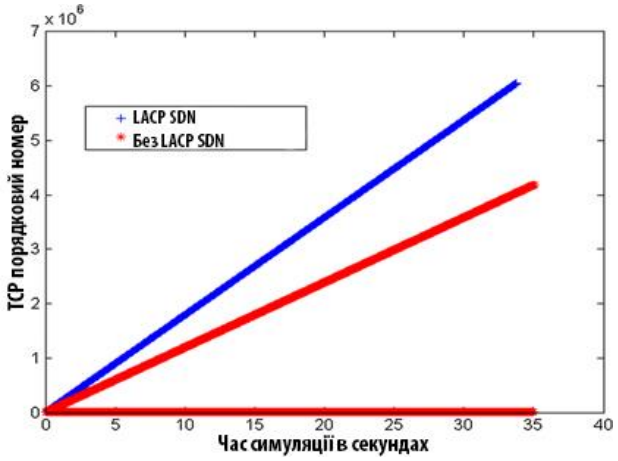


Рис. 2.6. Ризик успішної атаки за допомогою недоліків TCP

Незважаючи на суттєві недоліки в захисті, протокол динамічного агрегування дозволяє діагностувати проблеми з каналами передачі даних, здійснюючи моніторинг станів з'єднань та навантаження на них, що неможливе у статичному агрегуванні. Тому доцільно здійснювати використання протоколу в ядрі мережі, яке надійно захищене від зловмисників іншими протоколами та пристроями які забезпечують безпеку [26].

До таких мережевих пристроїв відносяться брандмауери, які як і маршрутизатори можуть об'єднуватися в віртуальні одиниці для забезпечення збільшення пропускної здатності та забезпечення надійності у випадку виходу одного члена групи з ладу. Для забезпечення захисту центральної частини мережі, маршрутизатори групують за допомогою безкоштовного протоколу CARP або пропрієтарного VARP. Розробка компанії Cisco дозволяє не лише здійснювати контроль над безвідмовною роботою ядра мережі, а й забезпечувати балансування трафіку сегменту, що значно підвищує час безвідмовної роботи.

З недоліків протоколу VARP можна окремо виділити проблему роботи з динамічними протоколами безпеки SSL та передачі даних (UPD) [27]. При виході з ладу одного з маршрутизаторів групи, з'єднання таких динамічних протоколів повинне налаштовуватись знову, що приводить до втрат продуктивності (рис. 2.7 та 2.8).

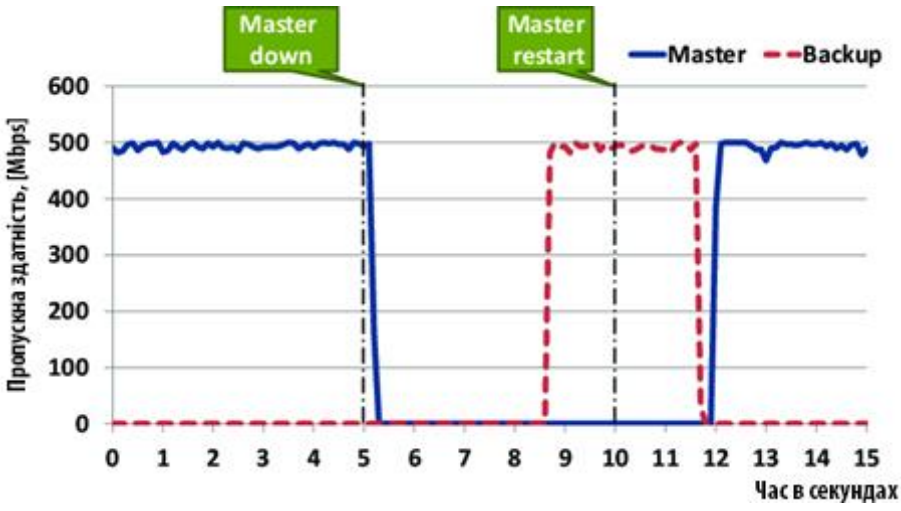


Рис. 2.7. Час простою VRRP при роботі з протоколом UDP

Рис. 2.8. Втрати пакетів під час простою

2.4. Оптимальні методи для організації резервування та балансування навантаження для прикладного рівня

Забезпечення надійності для прикладного рівня значно відрізняється від попередньо розглянутих ситуацій. Оскільки прикладний рівень оперує даними, його зв’язок з фізичним мережвим обладнанням мінімальний. Серверна взаємодія натомість чутлива до перенавантажень мережі та окремих її сегментів.

Для боротьби з перевантаженнями використовується два підходи: нарощування продуктивності за рахунок збільшення ресурсів, та кластеризації [28]. Перший метод є ефективним рішення для ситуацій, коли навантаження є стрибковим, піковим, та не збільшується з часом. У випадку ж постійного нарощування навантаження на сервери, продовжувати нарощувати апаратну потужність перестає бути доцільним. Для вирішення проблеми декілька серверів об’єднують в кластери. Навантаження між такими кластерами розподіляється за допомогою комплексу методів, які називаються балансування. Кластеризація також дозволяє забезпечувати резервування серверів, використовуючи в якості резерву один з серверів кластеру (рис. 2.9).

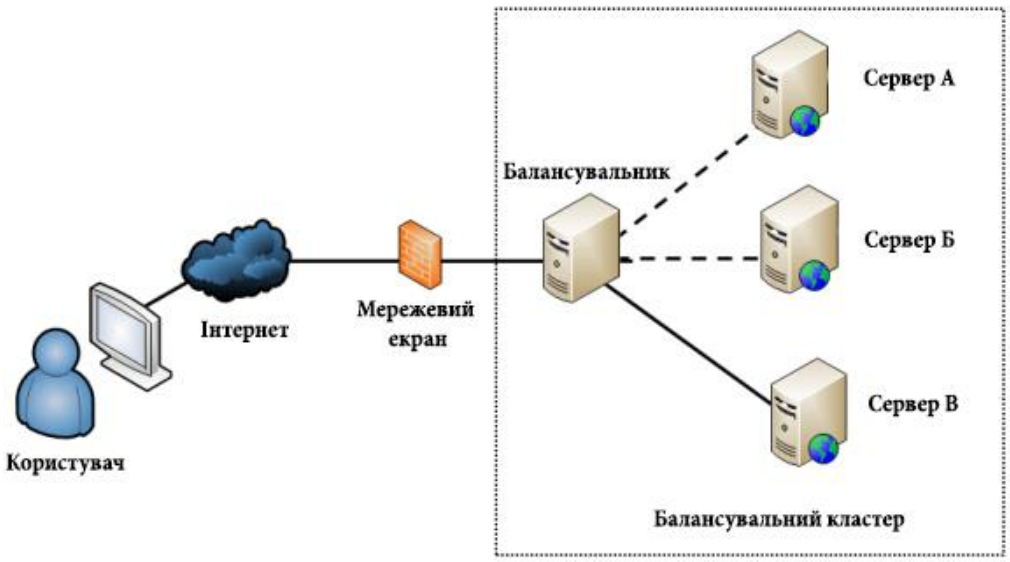


Рис. 2.9. Реалізація кластеризації серверів з використанням балансувальника

Методом балансування, який потребує мінімальної кількості мережевих та апаратних ресурсів є Round Robin, який описаний в першому розділі [29]. Завдяки простоті реалізації, даний протокол отримав популярність в мережах з низькими вимогами до критичних моментів навантаження. Проте такий метод має безліч суттєвих недоліків, а саме:

- для правильного балансування метод потребує однакових ресурсів на всіх серверах;
- при виконані всіх операцій повинна бути задіяна однакова кількість ресурсів;
- при балансуванні не враховується завантаженість того чи іншого сервера який входить в групу кластера.

В ситуації, коли Round Robin обслуговує два сервери, один з яких завантажений на 100% а інший на 15%, алгоритм все одно буде відправляти запити на кожен з них по черзі. При тестуванні латентності методів для балансування кластерів, Round Robin показав один з найгірших результатів у випадку, коли кількість серверів для балансування була >4 [30].

Метод Round Robin також не враховує кількість активних на певний момент підключень клієнтів до сереверів. Такий недолік може суттєво вплинути на надійність кластеру, оскільки чим триваліше з’єднання, тим більший об’єм роботи сервер

проводить для опрацювання та відправки запитів. Для запобігання таким ситуаціям створений алгоритм least connections [31]. За його допомогою можна визначити кількість активних з'єднань на даний момент часу. Зважаючи на недоліки протоколу стосовно визначення рівня навантаження серверів в даний момент, існує вдосконалена версія алгоритму під назвою Weighted Least Connections [32]. За його допомогою можна задавати пріоритет кожного сервера окремо. Можливість кластерів відповідати на запити залежить від кількості серверів в одній логічній групі (рис. 2.10).

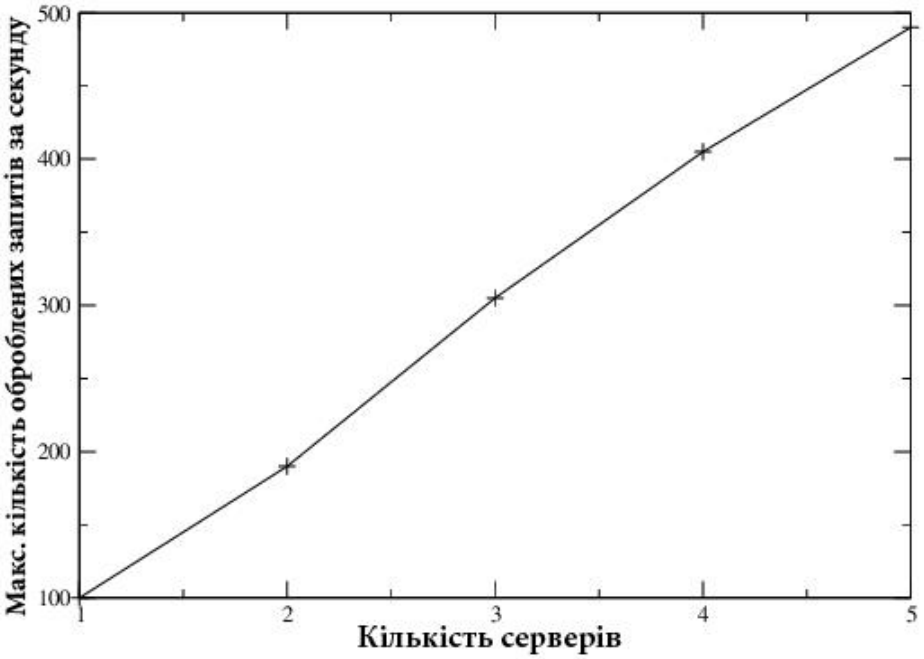


Рис. 2.10. Залежність реалізованої кількості запитів кластера від кількості серверів в групі

Виходячи з отриманих даних можна зробити висновки щодо доцільності використання тих чи інших методів балансування навантаження для серверів. При малих запитах та невеликої масштабованості мережі, доцільнішим буде використання протоколів типу Round Robin, оскільки він не потребує надлишкових ресурсів для первинного балансування даних, для його коректної роботи необхідний лише DNS сервер. Проте з ростом навантаження та ускладнення запитів до серверів, необхідно не лише збільшувати їх кількість в кластері (рис. 2.10), а й змінювати методи самого балансування.

2.4. Висновки до розділу 2

Кожен рівень мережевої взаємодії унікальний і потребує різних підходів щодо збільшення надійності та балансування навантажень.

Найменш гнучким в цьому плані є фізичний рівень, функцією якого є передача бітів інформації від одного мережевого пристрою до іншого. На етапі проектування комп'ютерної мережі необхідно звертати уваги на специфікації щодо передачі даних різними методами.

Для забезпечення резервування на другому рівні працює сімейство протоколів STP. Кожен з протоколів цієї групи має за мету певну область застосування.

З впровадженням технології агрегації був отриманий доступ до збільшення пропускної здатності завдяки використанням всіх ліній зв'язку. Технологія агрегування каналів підтримується всіма виробниками мережевого обладнання, що дозволяє впроваджувати її в всі класи мереж з використання абсолютно різного обладнання, на що варто звертати увагу.

Протокол CARP, як безпечнішу альтернативу VRRP, доцільніше використовувати для резервування мережевих екранів та прикордонних маршрутизаторів. Для пристроїв яра мережі, більш адаптивним рішенням буде протокол VRRP, оскільки його алгоритми для балансування пакетів є ефективним рішенням для балансування навантаження мережевого рівня.

Для балансування даних на прикладному та глобальному рівнях використовуються алгоритми рівномірного розподілу запитів та моніторинг стану з'єднань з серверами, як в середині сегментів так і в демілітаризованій зоні.

Завдяки комплексу дій з використанням інструментів для резервування та агрегації на всіх рівнях з'єднання, можна досягнути балансу пропускної здатності та надійності мережі. Математична оцінка таких методів, їх порівняння, аналіз та висновки щодо доцільності їх використання наведені у розділі 3.

РОЗДІЛ 3
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ПРОТОКОЛІВ АГРЕГАЦІЇ ТА РЕЗЕРЕРВУВАННЯ ЗА ДОПОМОГОЮ МАКЕТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Для проведення досліду ефективності застосування методів резервування та агрегації використовується модель комп'ютерної мережі, яка розроблена за допомогою програми Cisco Packet Tracer. Програма дозволяє створювати та адмініструвати мережі різних масштабів. У якості мережевого обладнання у програмі використовуються пропрієтарні рішення компанії Cisco.

Згідно з планом досліду, в програмі була змодельована багаторівнева мережа, яка включає в себе:

- хост-станції;
- бездротову точку доступу;
- комутатори другого рівня моделі OSI;
- маршрутизатори третього рівня;
- мережеві екрани;
- сервери внутрішнього доступу;
- сервери зовнішнього доступу демілітаризованої зони;
- кабелі витої пари категорії 5 для з’єднання пристроїв в мережі;
- бездротове з'єднання.

3.1. Аналіз використання протоколів STP та RSTP для резервування локальних сегментів мережі

Програмне забезпечення Packet Tracer дозволяє здійснювати емуляцію відправлення та отримання пакетів даних, як службових так і з корисним навантаженням. Просування пакетів по каналу можна відслідковувати покроково, що дозволяє отримувати достовірну інформацію про поведінку системи та даних в ній в кожен період часу.

Згідно до вимог експерименту, мережа повинна забезпечувати можливість зв’язку з зовнішньої мережею за допомогою прикордонного шлюзу, забезпечувати підключення локальних мереж до вторинних телекомунікаційних вузлів (ВТМВ), які в свою чергу об’єднуються в кластер з первинним телекомуніційним вузлом (ПТМВ), утворюючи ядро мережі. Будь який мережевий прилад повинен мати змогу звернутися до внутрішніх серверів та серверів в демілітаризованій зоні, права доступу в свою чергу повинні адмініструватися за допомогою мережевих екранів. Структурна схема модельованої мережі показана на рис. 3.1:

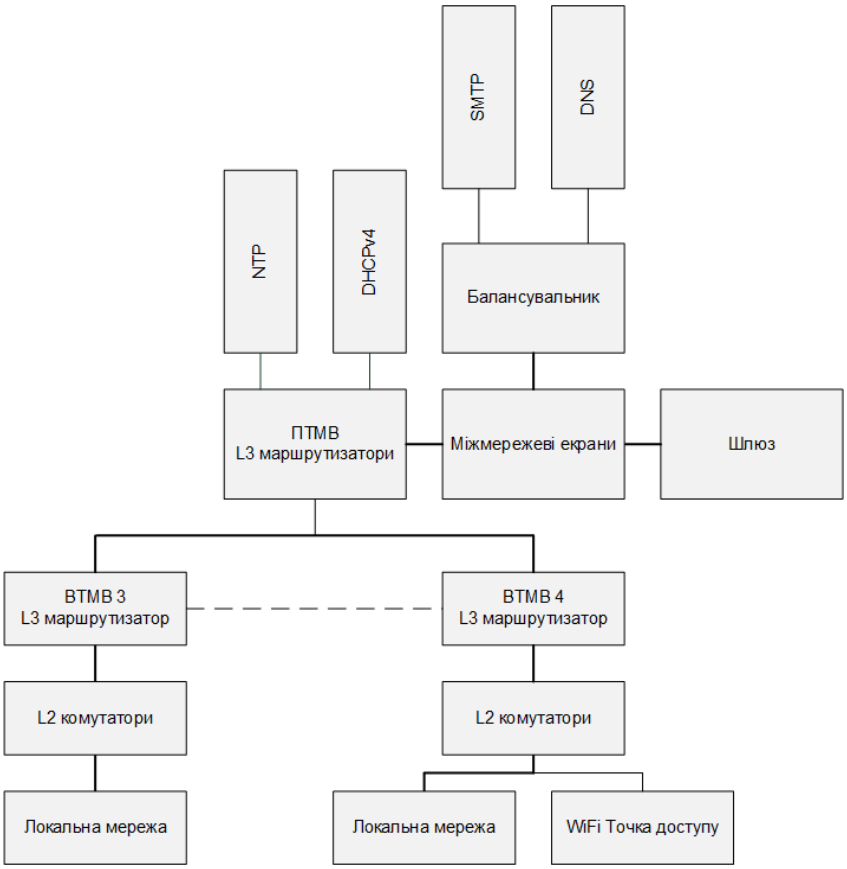


Рис. 3.1. Структурна схема модельованої мережі

На структурній схемі жирними лініями показані об’єднанні канали передачі даних, пунктирною лінією показані резервні з’єднання. Топологія змодельованої мережі – розширена зірка [33]. Така топологія утворюється при об’єднанні декількох сегментів мережі, кожен з яких побудований за топологією звичайної зірки. Завдяки особливостям її будови, отримується сегментована та відповідно добре контрольована

мережа, яка у порівнянні з іншими варіантами топології забезпечує більшу надійність та відмовостійкість, а також покращене балансування навантаження на кожен з сегментів та ядро мережі. Розширена зірка (рис. 3.2) дозволяє здійснювати передачу даних багатьом вузлам мережі, що неможливо реалізувати у топології шини, де дані передаються згідно визначеної черги.

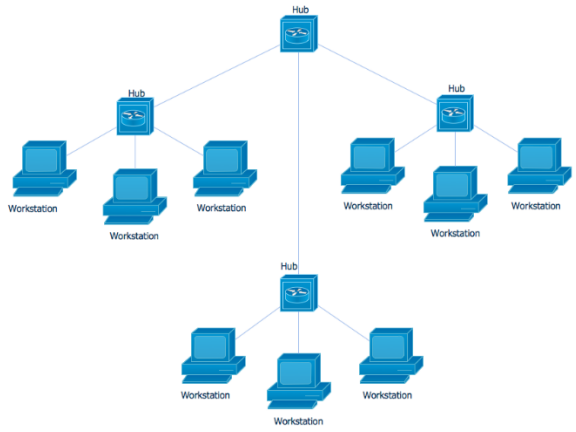


Рис. 3.2. Топологія “розширена зірка”

Детальна схема мережі з фізичними з’єднаннями інтерфейсів наведена в додатку Б. При моделюванні в якості фізичного середовища передачі даних використовується кабель витої пари, оскільки не все обладнання підтримує оптоволоконний кабель, а масштаб мережі дозволяє використання більш дешевого та простого у використані екранованого мідного кабелю.

Для резервування максимально наближеного до хост-станцій сегменту мережі доцільно застосувати протоколи сімейства STP без забезпечення додаткового балансування. Це пов’язано з кількістю даних якими оперує сегмент, пропускної здатності інтерфейсу Fast Ethernet достатньо для забезпечення ефективної передачі даних від станцій до серверів та за межі мережі.

Для проведення дослідження ефективності протоколів використовується протокол мережевого рівня ICMP [34]. Це службовий пакет даних, який використовується для контролю коректної роботи мережі. Він не створює серйозного навантаження на пропускний канал і дозволяє відслідковувати рух кожного пакету.

Протокол ICMP використовується при виконанні команди ping, яким необхідно звернутися до іншого сегменту VLAN та задіяні іншого комутатора мережі (рис. 3.3).

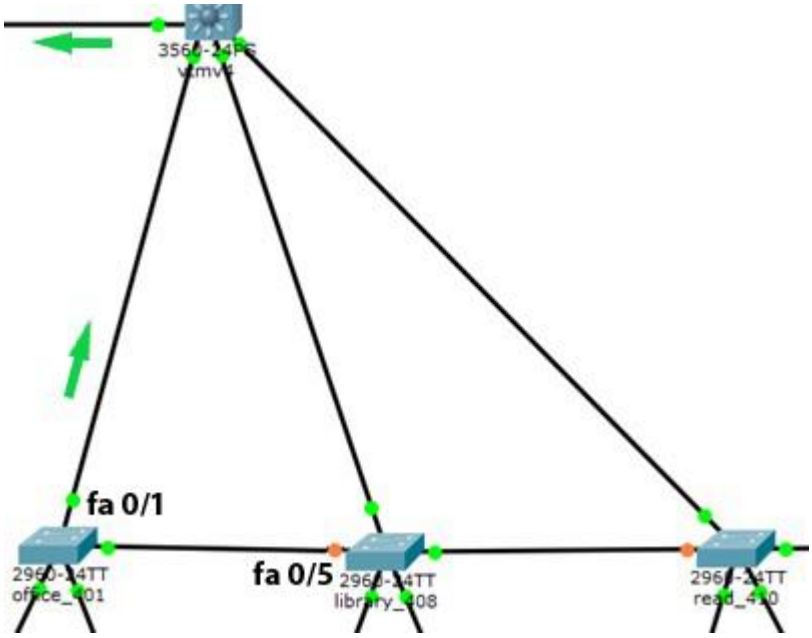


Рис. 3.3. Робочий стан мережі до початку дослідження

Як видно з рисунка 3.3, активні лінії передачі даних при резервуванні протоколами STP та RSTP будуть зеленими, лінії які знаходяться в стані очікування – помаранчевими. Для передачі даних комутатор office_401 використовує інтерфейс Fast Ethernet 0/1, для зв'язку з vtmv4. Завдяки побудові математичного графа, протоколи визначають вагу такого шляху як найменшого і використовують його по замовчуванню. Згідно доктрини протокол STP вважає інтерфейс комутатора library_408 резервним, і тримає його в такому стані до виходу з ладу головної лінії зв'язку. RSTP також тримає лінк неактивним, проте здійснює налаштування інтерфейсу, готуючи його до передачі даних, таким чином забезпечуючи швидке включення в роботу інтерфейсу, у випадку виходу з ладу основного маршруту.

Для початку досліду необхідно виконати команду ping з хост-станції, яка належить комутатору office_401, до будь-якого мережевого пристрою за межами vtmv4. Протокол ICMP не розрахований на встановлення з'єднань, тому якщо його пакет буде втрачено, він не підлягає відновленню. ICMP повідомлення створюються мережевими пристроями у випадку виникнення неполадок у каналі передачі даних

(виключенням є самі ICMP- пакети, оскільки такий алгоритм привів би до широкомовного шторму в сегменті). Після введення кінцевої IP-адреси активуємо з’єднання та отримуємо наступний результат (рис. 3.4):

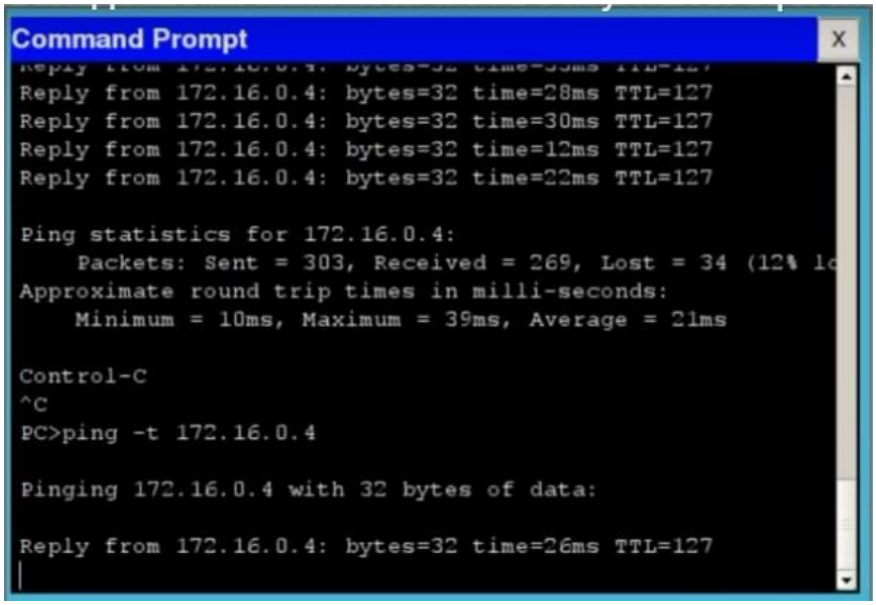


Рис. 3.4. Успішне встановлення з’єднання між пристроями

Результатом дії буде отримання пакета-відповіді з службовою інформацією щодо затримки, часу життя пакета та кількість даних, які були передані цим пакетом. Після отримання відповіді автоматично генерується наступний пакет з запитом до вказаного вище мережевого пристрою, таким чином створюючи цикл, вихід з якого здійснюється за командою оператора.

Для активації протоколу STP комутатор vtmv4 не повинен отримувати BPDU пакети від нижніх комутаторів. Для цього відключаємо інтерфейс fa0/1 (рис. 3.3), і спостерігаємо за виконанням команди ping з локальної мережі комутатора (див. рис. 3.5).

Після втрати зв’язку з комутатором vtmv4, пристрій надсилає BPDU пакети до інших комутаторів в сегменті, сигналізуючи про неполадку та початок прокладання обхідного шляху за допомогою інтерфейсу fa 0/5 комутатора library_408, який знаходиться в списку резервованих шляхів. Як видно з рис. 3.5, час який витрачається на перебудову топології та навчання інтерфейсу для передачі, канал fa 0/1 неактивний,

і пакети даних які передаються ним втрачаються, про що сигналізує ICMP за допомогою повідомлення “Request time out”. По завершенню реструктуризації дерева, STP вказує каналом передачі даних fa 0/5 і пакети починають досягати адресата.

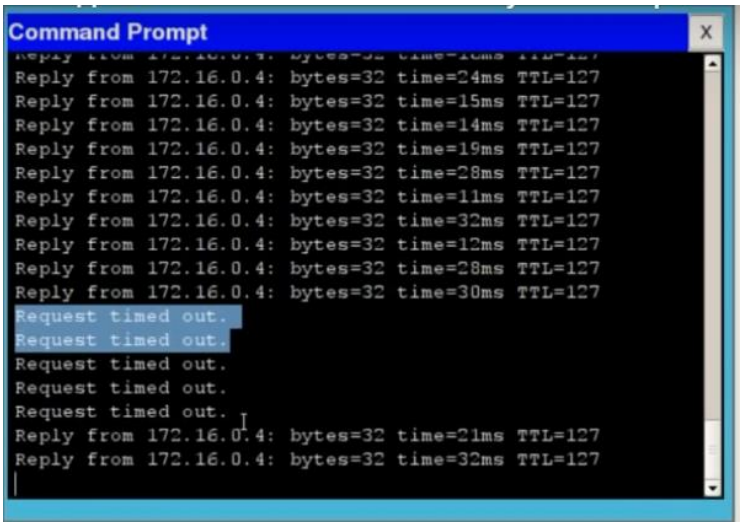


Рис. 3.5. Втрата пакетів протоколом STP під час перебудови логічного дерева

Аналогічний дослід проводиться для сегменту мережі з використанням протоколу RSTP. Під час зміни протоколу резервування топологічне дерево перебудовується, тому спостерігається втрата пакетів (рис. 3.6):

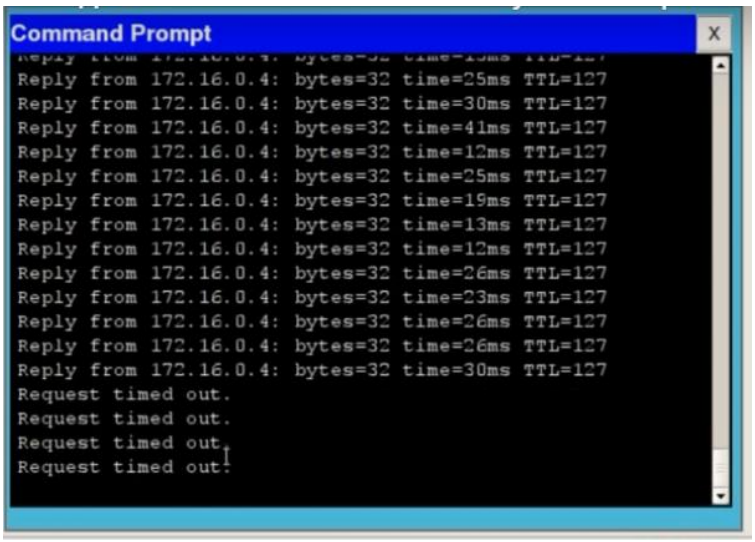


Рис. 3.6. Втрата пакетів під час перебудови топологічного дерева

Після відновлення з’єднання проводимо дослід з використанням протоколу RSTP. Інтерфейсу fa 0/5 присвоюється стан Alternative, в такому стані він знаходиться до надходження інформації про вихід з ладу пріоритетного каналу зв’язку, після чого відразу починає свою роботу. Результати дослідження показані на рис. 3.7.

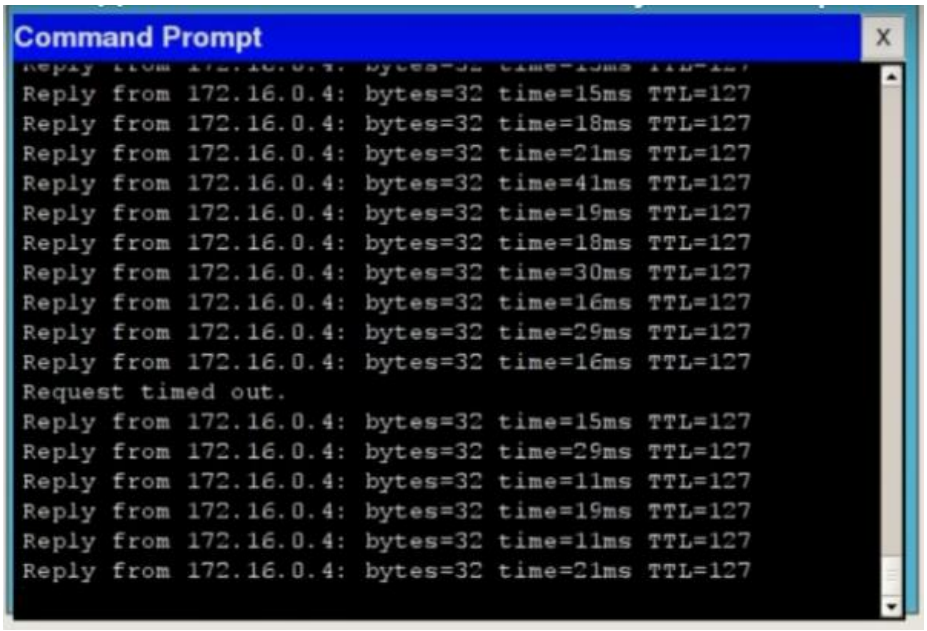


Рис. 3.7. Втрати пакетів протоколом RSTP

При постійній передачі даних з використанням RSTP, при виникненні неполадок був втрачений один пакет ICMP. Для проведення детальнішого дослідження вибірка збільшена до ста пакетів ICMP для кожного протоколу резервування. Для оцінки простою каналу зв’язку, середній час передачі одного пакету даних = 22,25 ms. Результат експерименту наведений у табл. 3.1. З отриманих даних можна зробити висновок щодо доцільності використання протоколу RSTP як основного інструменту надлишкового резервування локальних вузлів в мережі. Протокол використовує практичну кількість ресурсів обладнання та каналу зв’язку як і STP, при цьому демонструє кращий результат.

Таблиця 3.1

Успішна передача пакетів даних та простій мережевого каналу

Тип протоколу резервування	Тип кадру даних	Кількість пакетів для передачі, шт	Кількість успішно доставлених пакетів, шт	У відсотковому значенні, %	Час який канал зв’язку був неактивний, ms
STP	ICMP	100	93	93%	155.75
RSTP	ICMP	100	98	98%	44.5

3.2. Дослідження технології статичної та динамічної агрегації

Окрім сімейства STP на канальному рівні моделі OSI працює технологія LAG, яка об’єднує в собі методи забезпечення аргрегації фізичних каналів. Для налаштування та адміністрування каналів можна використовувати два підходи – статичний та динамічний. При налаштуванні з’єднань вручну, адміністратор отримує змогу налаштувати поведінку каналу згідно свого бачення навантаження та резервування тої чи іншої групи. Саме такий тип агрегації рекомендують використовувати виробники мережевого обладнання. Протокол динамічного резервування LACP використовується в випадках великих масштабованих систем, що дозволяє швидко розгортати агрегування за необхідністю.

Для проведення досліду щодо ефективності використання динамічної та статичної агрегації використовується макет мережі, наведений у додатку Б. Для імітації реального навантаження на мережу використовуються інструменти Cisco Pocket Tracer, а саме можливість оновлення програмної оболонки IOS за допомогою TFTP сервера. Пакети оновлення несуть в собі дані для оновлення оболонки L3 комутатора vtmv4, який буде використовувати статичну та динамічну агрегацію портів fa 0/4-6. Оскільки програмно ці фізичні з'єднання знаходяться в одній групі, то дії по

відношенню до такого каналу даних має здійснюватися за допомогою групового звернення.

Роль TFTP сервера виконуватиме сервер dhcpv4_pvt, який також є сервером DHCP для мережі [35]. Вибір використання саме тривіальної версії FTP пов’язаних з простотою його реалізації та невибагливість щодо мережевого обладнання. TFTP дозволяє записувати та зчитувати дані, проте він не здатен виводити список наявних файлів на сервері та не підтримує автентифікацію. Проблеми з безпекою вирішуються за допомогою налаштувань політик доступу мережевими екранами. Сегмент мережі для дослідження, з зображенням руху трафіку від TFTP сервера до комутатора, зображений на рис. 3.8.

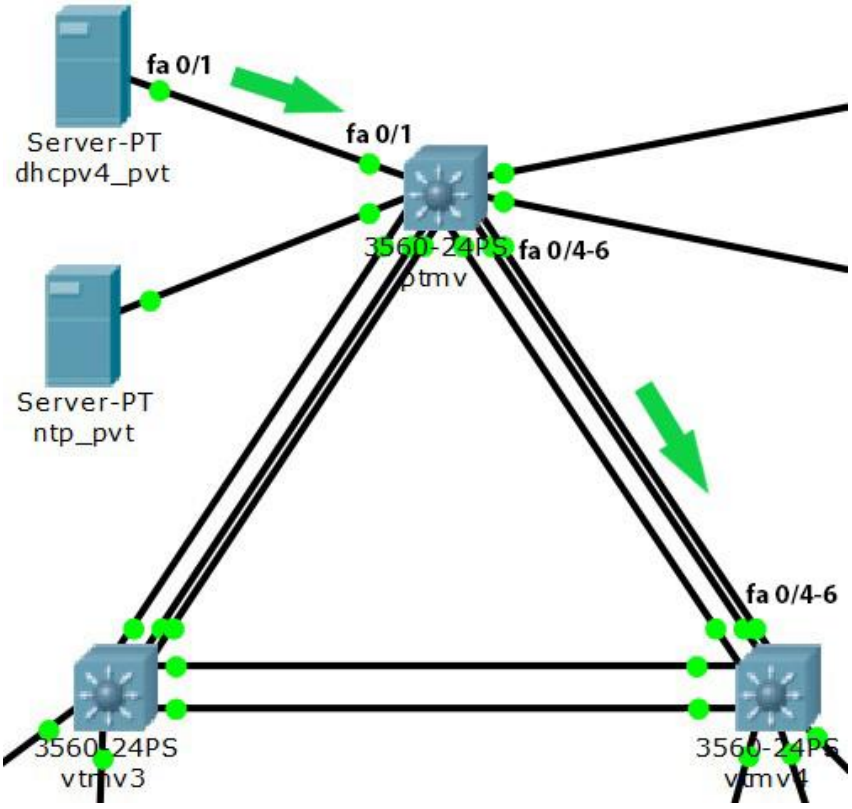


Рис. 3.8. Ядро модельованої мережі для дослідження

Ядро мережі використовує агрегацію каналів для збільшення максимальної пропускної здатності та забезпечення відмовостійкості. При моделюванні максимальна можлива швидкість передачі даних в каналі fa 0/4-6, для проведення

дослідження = 300 Мбіт/с. Інтерфейс TFTP сервера та можливі файли для передачі показані на рис. 3.9.

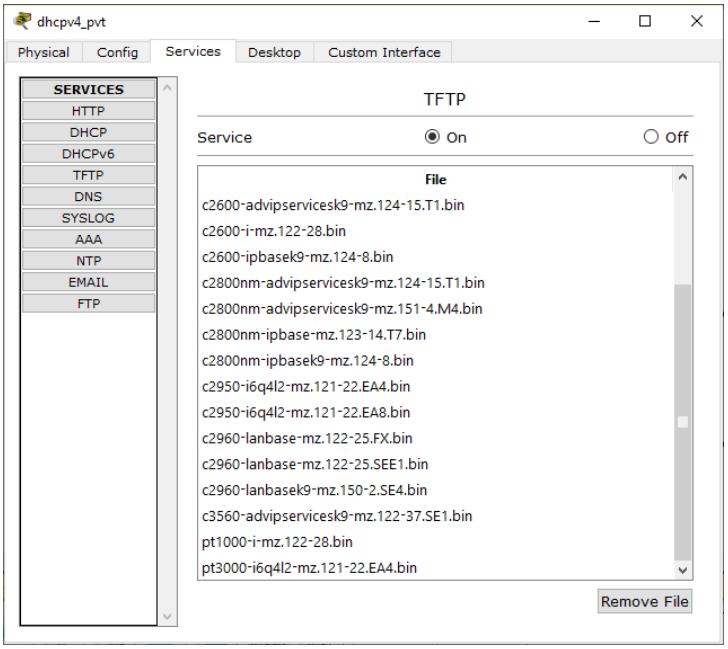


Рис. 3.9. Інтерфейс TFTP сервера модельованої мережі

Для проведення дослідження ефективності використання статичного агрегування здійснювався моніторинг стану навантаження агрегованого каналу передачі даних fa 0/4-6. Результати досліду наведені на рис. 3.10.

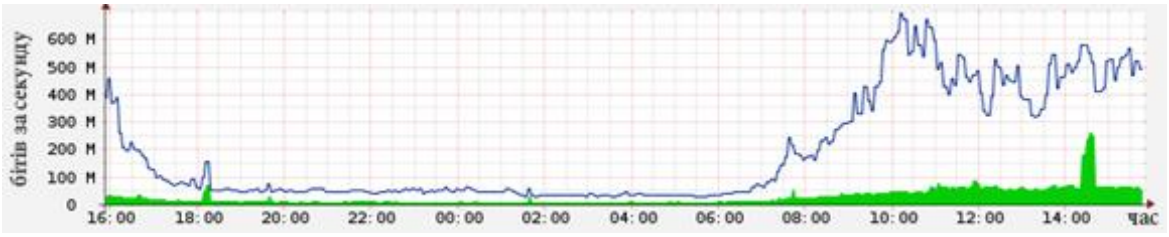


Рис. 3.10. Результати дослідження навантаження статично агрегованого каналу

З результатів можна зробити висновок щодо неоднорідності розподілення навантаження на мережу. Статичне агрегування даних має швидший час збіжності та не потребує додаткового часу при зміні конфігурації, на відмінну від динамічного LACP. Проте такий метод агрегації не здатен виявляти помилки та балансувати пікові навантаження на канал, здійснюючи передачу даних в одному режимі протягом всього

часу роботи. Такий метод резервування доцільно використовувати для локальних сегментів мережі з прогнозованим навантаженням.

Для проведення аналогічного експерименту з динамічним агрегуванням необхідно здійснити налаштування інтерфейсів. Згідно рис. 3.8, головним пристроєм в каналі буде ptmv, його група отримує статус active, відповідно канал vtmv4 буде мати статус passive. Таке налаштування дозволяє протоколу обмінюватися службовими пакетами і проводити діагностику каналу. Це дозволяє здійснювати балансування. Результати дослідження наведені на рис. 3.11.

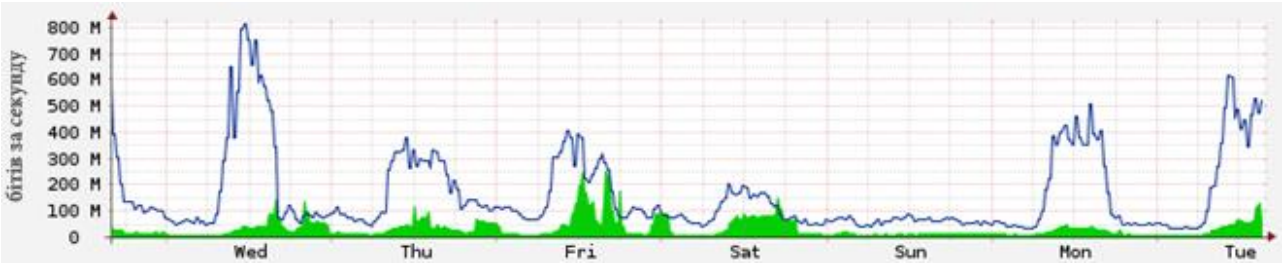


Рис. 3.11. Результати дослідження навантаження динамічного агрегованого каналу

Результати досліду дозволяють зробити висновок щодо спроб протоколу LACP здійснювати первинне балансування кадрів всередині каналу, що відображається на пікових навантаженнях мережі. Для уточнення результатів проведене дослідження з значно меншим часом передачі даних по каналу, результати зображені на рис. 3.12.

Рис. 3.12. Результати дослідження нетривалого навантаження динамічного агрегованого каналу

З графіку видно доцільність використання протоколу LACP для балансування навантаження на канал, ефективність якого спадає з зростанням часу активної роботи.

Отримавши дані всіх дослідів, можна зробити висновки щодо доцільності використання протоколів агрегації. Статичний метод агрегації через свої обмеження щодо балансування доцільно використовувати в локальних сегментах або в мережах з прогнозованим навантаженням та меншою масштабованістю, виключаючи таким чином можливість помилки оператора. Динамічний протокол агрегації LACP підтримується всіма вендорами, дозволяє використовувати технологію для агрегації великих масштабованих мереж, при цьому здійснюючи балансування трафіку в межах своїх апаратних можливостей. Таке балансування канального рівня не забезпечує балансування всієї мережі, тому для його забезпечення в парі з динамічним протоколом агрегації використовуються протоколи балансування мережевого рівня та методи розподілення навантаження прикладного рівня моделі OSI.

3.3. Дослідження ефективності методів забезпечення відмовостійкості мережевого рівня

Пакети даних – це PDU мережевого рівня, робота якого полягає в маршрутизації цих даних для подальшої доставки їх до адресата. Мережеве обладнання, яке потребує додаткового резервування, об’єднується в віртуальні кластери. Приклад такого кластера було наведено на рисунку 3.8, проте в випадку з агрегацією каналів (технологією 2 рівня), протоколи не звертають увагу на налаштування та принципи роботи маршрутизаторів. Таким чином отримується можливість реалізувати одразу декілька мережевих технологій щодо забезпечення резервування та агрегації на одному сегменті мережі, зважаючи на рівні застосування різних протоколів. Для канального рівня ядра мережі може застосовуватися протокол LACP, а для мережевого – пропрієтарний VRRP або безкоштовна альтернатива CARP.

Для дослідження ефективності протоколів мережевого та прикладного рівня використовується сегмент мережі, зображений на рис. 3.13.

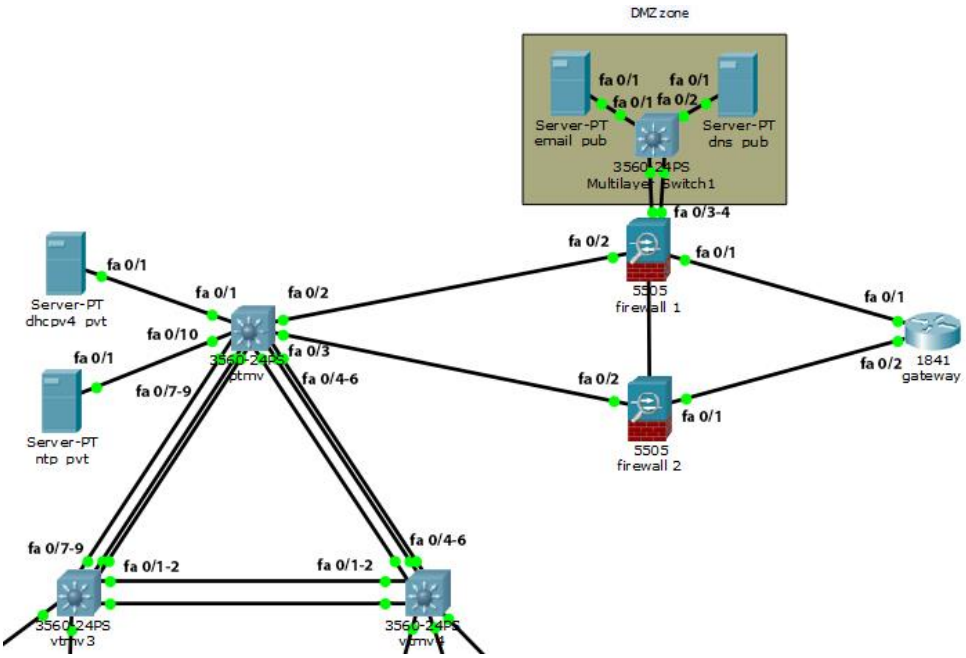


Рис. 3.13. Сегмент макету комп'ютерної мережі для дослідження ефективності балансування, резервування та агрегації мережевого та прикладного рівнів

Пропрієтарні засоби компанії Cisco, розроблені для забезпечення надлишкового резервування мережевого рівня включать в собі протоколи HSRP, VRRP та GLBP, детально вони описані в розділі 1, а їх коротка характеристика наведена на рис. 3.14.

Атрибути	HSRP	VRRP	GLBP
Стандарт	RFC 2281	RFC 3768	Cisco
Балансування	ні	ні	так
IPv6	так	ні	так
Транспортування	UDP/1985	IP/112	UDP/3222
Пріоритет	100	100	100
Hallo-пакет	3 сек	1 сек	3 сек
Мультикаст	224.0.0.2	224.0.0.18	224.0.0.102

Рис. 3.14. Сімейство протоколів FHRP

На сьогоднішній день протокол HSRP вважається застарілим і не підтримується обладнанням Cisco. Для забезпечення резервування мережевого рівня методом

надлишковості, використовуються як VRRP так і GLBP. Різниця між протоколами полягає у можливостях балансування. VRRP як і його безкоштовний аналог CARP, виконують балансування за допомогою ARP запитів. GLBP окрім загальної віртуальної адреси групі пристроїв також присвоює окремі MAC-адреси кожному члену групи. Коли хост відправляє запит ARP для визначення MAC-адреси шлюзу, протокол видає одну з адрес групи. Таким чином здійснюється балансування навантаження.

Протокол GLBP, незважаючи на свій розширений діапазон можливостей, підтримується лише професійною лінійкою обладнання компанії Cisco. Це пов'язано з навантаженням службових запитів а також необхідністю використання потужного обладнання для забезпечення його коректної роботи.

Проведення досліду доцільності використання протоколу GLBP для сегменту мережі (рис. 3.13), проводиться з використанням TFTP сервера dhcpv4_pvt та його інтерфейсу fa 0/1. Оновлення оболонки IOS передається для прикордонного маршрутизатора gateway [36]. Таким чином пакети даних повинні балансуватися по інтерфейсах fa 0/2-3 маршрутизатора ptmv. Аналогічні дії виконуються для сегменту з використанням HSRP. Отримані результати наведені на рис. 3.15.

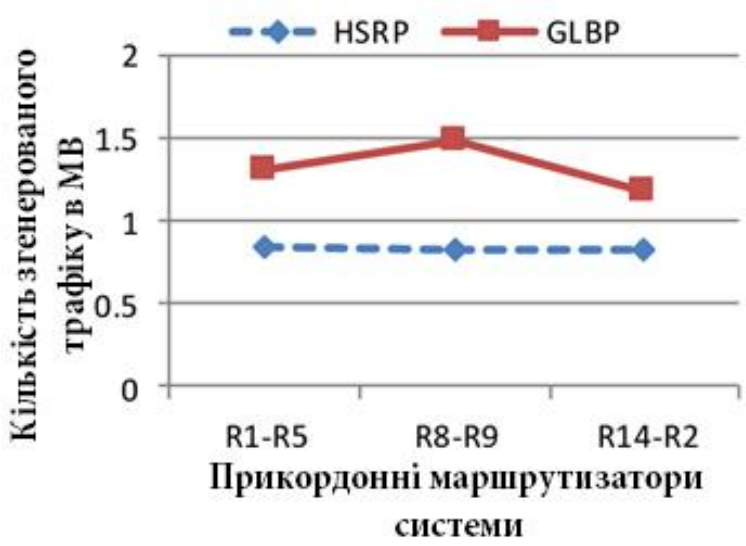
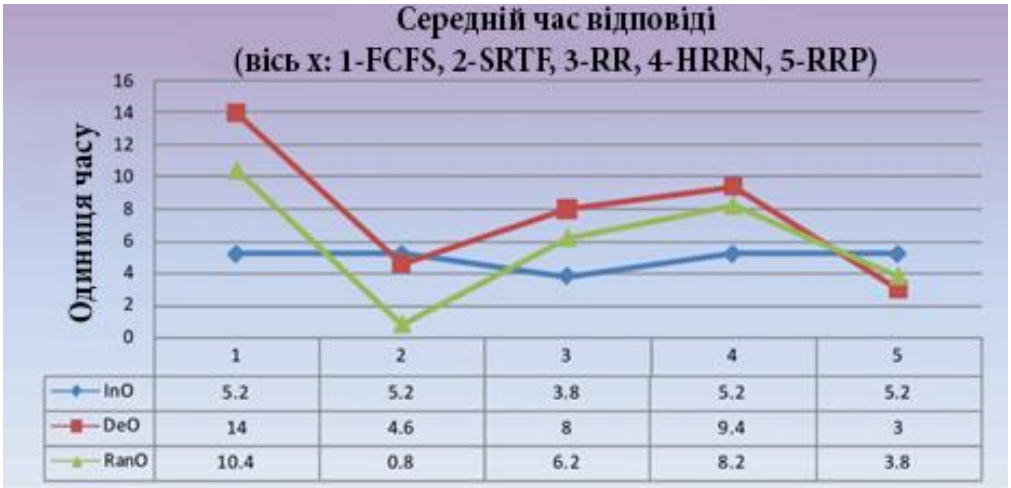


Рис. 3.15. Об'єм даних який генерується службовими командами

З отриманих даних можна зробити висновок про використання протоколом GLBP більшої кількості мережевих ресурсів. Це пов’язано з частотою оновлення ARP-таблиці а також додатковим балансуванням трафіку по каналах. Протокол HSRP в свою чергу здійснює балансування за допомогою ARP запитів, не створюючи додаткового навантаження на канал зв’язку.

Протокол VRRP, як і HSRP, не створює надлишкового трафіку всередині каналу зв’язку, і підтримується більшістю мережевих пристроїв. VRRP також забезпечує швидку реакцію на запити (рис. 3.16) у порівнянні з математичним алгоритмом маршрутизації HRRN (Highest Response Ratio Next) та іншими [37].



	1	2	3	4	5
InO	5.2	5.2	3.8	5.2	5.2
DeO	14	4.6	8	9.4	3
RanO	10.4	0.8	6.2	8.2	3.8

Рис. 3.16. Порівняння швидкості реакції відповіді протоколу VRRP

Завдяки меншим вимогам до мережевого обладнання та швидкості реакції на запити, пропрієтарний протокол VRRP доцільно використовувати для забезпечення резервування центральних сегментів мережі. Протокол GLBP в свою чергу варто застосовувати для сегментів які обслуговують передачі великих об’ємів даних, для додаткового балансування, за умови використанням сегменту мережі професійного обладнання.

Альтернативою пропрієтарним рішенням існує протокол CARP, який детально описаний в розділі 1. Завдяки проектуванню для BSD-систем, протокол отримав вищий ступінь захисту, що є ключовим фактором використання його для резервування брандмауерів та прикордонних груп [38].

Вразливість VRRP полягає можливості генерування певної кількості пакетів зловмисникам, результатом втручання є забезпечення доступу до основного маршрутизатора кластера. Програмний засіб, який здійснює атаку на L3 протоколи, які включають в себе протоколи маршрутизації та резервування BGP, LDP, OSPF, VRRP, отримав назву Loki [39]. Приклад атаки на протокол VRRP з використанням Loki показаний на рис. 3.17.

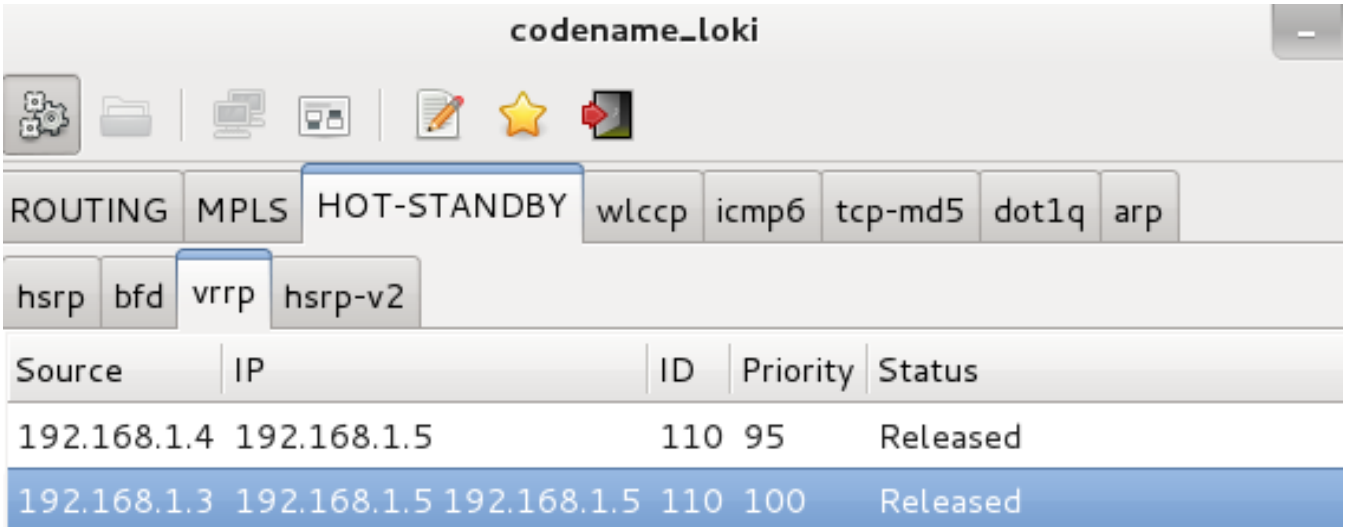


Рис. 3.17. Успішна атака на протокол VRRP

Таким чином, згідно аналізу результатів дослідження і зважаючи на особливості роботи протокол VRRP не рекомендується використовувати в прикордонних (DMZ) зонах, де значно вищі вимоги до безпеки. Для резервування мережевих екранів доцільно використовувати протокол CARP. В сучасних мережах для демілітаризованої зони використовують метод з двох або трьох брандмауерів. Такий метод передбачає, що один з мережевих екранів групи перевіряє трафік всередині мережі, а інший – ззовні. В випадку атаки, для доступу до мережі необхідно скомпрометувати обидва пристрої. Для забезпечення ще більшого рівня захисту мережеві екрани можуть бути різних вендорів та архітектури, а їх підтримка може бути реалізована лише за допомогою CARP.

3.4. Аналіз ефективності методів глобального балансування навантаження

Надмірне навантаження на сегмент мережі чи його окремі компоненти впливають на надійність мережі та якість обслуговування. Для запобіганню перевантажень кожен рівень мережевої взаємодії старається здійснювати балансування PDU. На канальному рівні це протокол MSTP та технологія агрегації каналів. На мережевому рівні – VRRP, GLBP та CARP, для рівня транспортування та представлення – глобальні методи резервування з використанням DNS (Round Robin, Least Connections та інші). Детальніше про глобальні протоколи балансування сказано у розділі 1.

Для дослідження ефективності методів балансування використовується сегмент мережі зображений на рисунку 3.13. Оцінка ефективності балансування буде проводитися за рахунок звернення до приватних серверів dhcpv4_pvt та ntp_pvt маршрутизаторами ядра мережі. В якості пакетів з навантаженням виступатимуть DHCP-запити (рис. 3.18) [40].

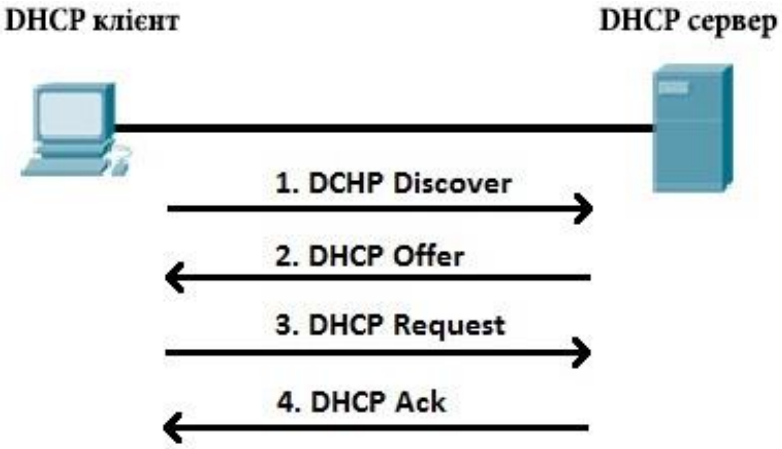


Рис. 3.18. Процес обміну пакетами DHCP клієнта та сервера

Хост-станції локальних сегментів маршрутизаторів vtmv3 та vtmv4 одночасно надсилають DHCP запити до приватних серверів, для цього вони здійснюють запит до DNS-сервера, який знаходиться в демілітаризованій зоні. Алгоритм Round Robin здійснює покрокове балансування запитів, направляючи відповіді до хост-станцій з

адресою серверів. Натомість алгоритм Least Connections здійснює прослуховування серверів і визначає кількість наявних з’єднань для кожного з них, після чого обирає в якості адреси сервер з меншою кількістю активних з’єднань. Результати досліду з навантаження наведені на рис. 3.19.

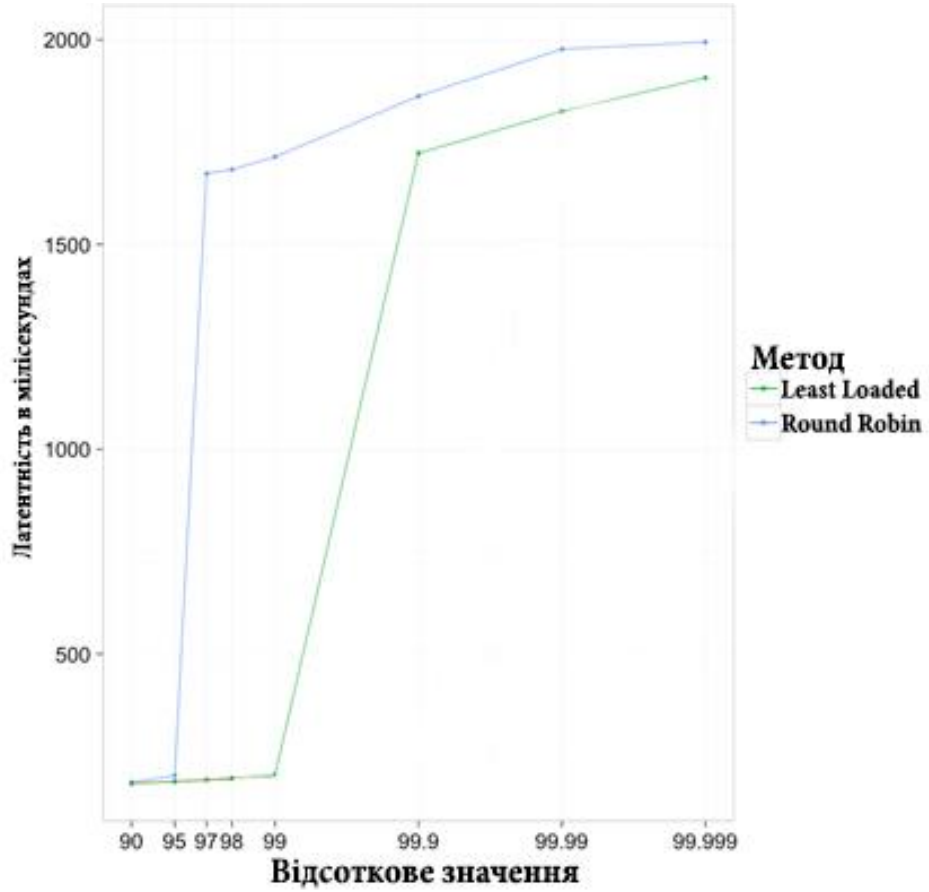


Рис. 3.19. Латентність запитів з використанням балансувальника

Згідно результатів досліду видна чітка деградація обробки запитів алгоритмом Round Robin при збільшені навантаження. Максимальне навантаження на сервери для адекватної роботи протоколу = 95%. Алгоритм Least Connections показав значно кращі результати, поріг роботи алгоритму при зростаючому навантажені = 99%. Це дозволяє зробити висновки щодо використання методів глобального балансування при різних нормах навантаження. Кількість можливих оброблених запитів до сервера за секунду, з використанням обох алгоритмів балансування, наведений на рис. 3.20.

Результати дослідження продуктивності (рис. 3.20) методів балансування Round Robin та Least Connections підтверджують залежність продуктивності сервера (рис. 3.19) від пікового навантаження на нього.

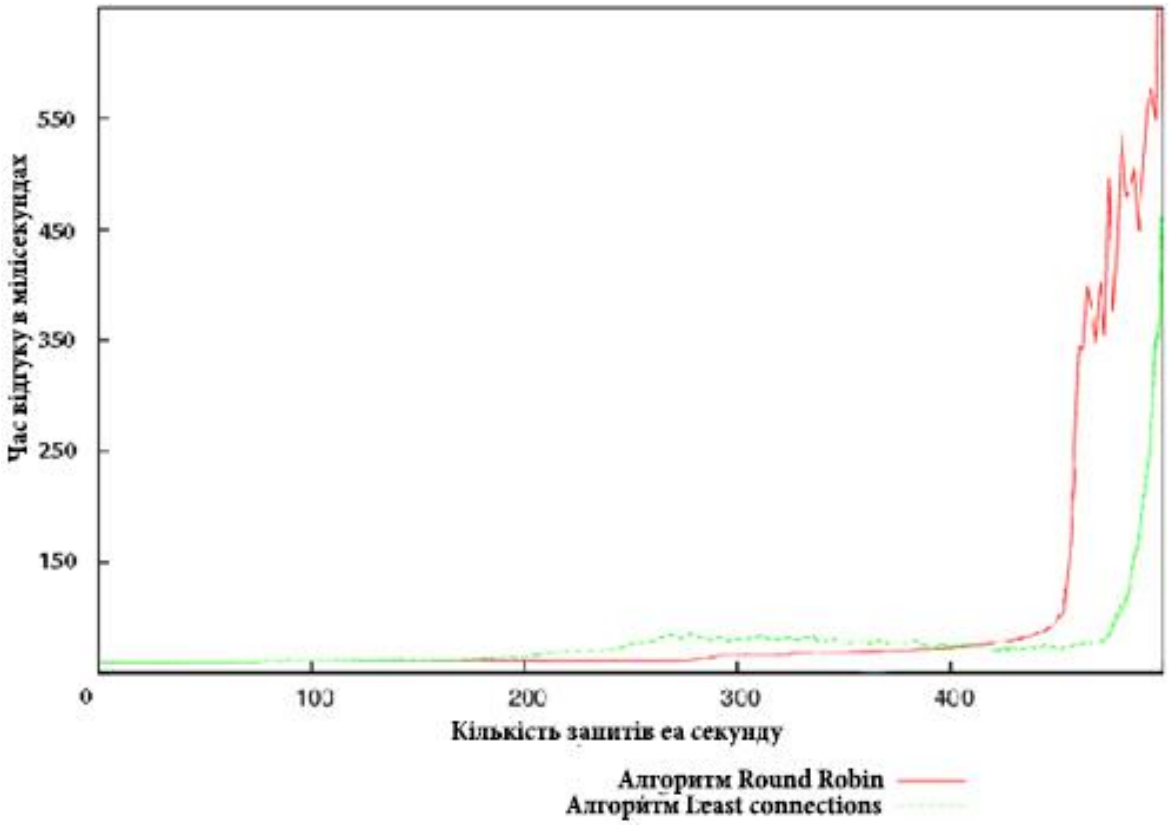


Рис. 3.20. Продуктивність обробки запитів сервером з використанням різних методів балансування навантаження.

Метод циклічного планування доцільно використовувати в мережах з стабільним помірним навантаженням на сервери. Це дозволяє проводити балансування з рівномірним розподілом. У випадку нерівномірного часу навантаження з критичними піковими значеннями доцільно використовувати метод Least Connections. Він дозволяє здійснювати моніторинг активних підключень, які впливають на латентність та надійність серверів в цілому. Завдяки цьому у моментах пікового навантаження запити, без втрати продуктивності, будуть розподілятися рівномірно між всіма серверами групи.

3.5. Висновки до розділу 3

Завдяки аналітичним можливостям програмного забезпечення Cisco Pocket Tracer, отримані результати можна вважати наближеними до реальних умов використання мережевого обладнання.

Вперше досліджено та проаналізовано ефективність та доцільність використання обраних методів та технологій резервування та агрегації в комп’ютерних мережах.

Проведене порівняння ефективності алгоритмів балансування дозволило зробити висновок щодо можливого застосування різних методів, відповідно до вимог мережі стосовно безпеки, кількості та типів навантаження.

Результатом роботи є комплекс методів, технологій резервування та агрегації, який згідно апробації моделі, можна ефективно застосовувати у сучасних комп’ютерних мережах з різними пріоритетами та степенями їх навантаження.

РОЗДІЛ 4 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Економічне обґрунтування дипломної роботи магістра є метою даного розділу. Даний розділ дозволяє встановити доцільність проведення науково– дослідних робіт і економічно обґрунтувати доцільність застосування тих чи інших засобів. Саме проведення економічних розрахунків, спрямованих на визначення економічної ефективності науково–дослідницької роботи (НДР) і прийняття рішення про її подальший розвиток та впровадження або ж недоцільність проведення відповідної розробки.

Метою дипломної роботи магістра дослідження методів та засобів резервування та агрегації комп’ютерних мереж.

В економічній частині дипломного проекту будуть проведені такі етапи розрахунку вартості НДР:

- описати технологічний процес розробки із зазначенням трудомісткості кожної операції;
- визначити суму витрат на оплату праці основного і допоміжного персоналу, включаючи відрахування на соціальні заходи;
- визначити суму матеріальних затрат;
- обчислити витрати на електроенергію для науково– виробничих цілей;
- нарахувати суму амортизаційних відрахувань;
- визначити суму накладних витрат;
- скласти кошторис та визначити собівартість НДР;
- розрахувати ціну НДР;
- визначити економічну ефективність та термін окупності продукту.

На основі отриманих розрахунків будуть розроблені техніко-економічні показники проектованого виробництва.

Як відомо, розробка надійної і ефективної інформаційної системи вимагає значних затрат часу. Слід зауважити, що затрати часу залежать від кваліфікації розробника і його можливостей. Розробник повинен у достатній мірі володіти

навиками програмування, вміти адекватно застосовувати математичний апарат, бути добре обізнаним з об'єктом дослідження.

4.1. Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для оцінки тривалості виконання окремих робіт використовують нормативи часу або попередній досвід. До таких нормативів відносять тривалість написання операцій (команд), які в деяких підприємствах становлять: для одної операції від 30 хвилин до 1,6 годин та 8 годин для п'яти операцій (тривалість зміни).

У разі їх відсутності звертаються до експертних оцінок по встановленню тривалості кожного етапу (стадії):

при трьох оцінках:

$$T_{\text{вс}} = \frac{(t_{min} + 4t_{\text{н.й}} + t_{max})}{6}, \tag{4.1}$$

при двох оцінках:

$$T_{\text{вс}} = \frac{(3t_{min} + 2t_{max})}{5}, \tag{4.2}$$

де $T_{\text{вс}}$ – очікуване (середнє) значення тривалості виконання етапу (стадії); t_{min}, $t_{\text{н.й}}$, t_{max} – відповідно мінімальна, найбільш імовірна і максимальна оцінки тривалості виконання етапу (стадії).

Розробку даної інформаційної системи можна поділити на такі етапи:

- постановка задачі;
- проведення огляд публікацій авторів, які займались питанням дослідження методів та засобів резервування та агрегації комп’ютерних мереж;

- прийняття рішень щодо вибору оптимального шляху розв'язання поставленої задачі;
- аналіз математичної моделі інформаційної системи;
- обґрунтування використання обраних методів та засобів резервування та агрегації комп’ютерних мереж;
- розробка архітектури та алгоритмічного забезпечення комп’ютерної мережі з використанням запропонованих методів;
- розробка макету комп’ютерної мережі з використанням резервування та агрегації;
- тестування та оцінка роботи обраних методів резервування та агрегації мережі;
- написання і оформлення документації (електронної та паперової).

Для зручного представлення і визначення загальної тривалості проведення НДР доцільно дані витрат часу по окремих операціях технологічного процесу звести у таблицю 4.1.

Витрати часу наукового керівника на виконання окремих стадій (етапів) при недостатній кількості інформації доцільно приймати в межах 5% сумарних витрат часу інженерів на виконання цих стадій (етапів).

Таблиця 4.1

Основні етапи і час їх виконання у НДР

№ з/п	Етап	Середній час виконання етапу, год	
		інженер	керівник
1	Постановка задачі	3	1
2	Проведення огляд публікацій авторів, які займались питанням дослідження методів та засобів резервування та агрегації комп’ютерних мереж;	10	5
3	Прийняття рішень щодо вибору оптимального шляху розв'язання поставленої задачі;	5	4

Продовж.табл 4.1

№ з/п	Етап	Середній час виконання етапу, год	
		інженер	керівник
4	Аналіз математичної моделі інформаційної системи	1	1
5	Обґрунтування використання обраних методів та засобів резервування та агрегації комп'ютерних мереж	7	2
6	Розробка архітектури та алгоритмічного забезпечення комп'ютерної мережі з використанням запропонованих методів	45	7
7	Розробка макету комп'ютерної мережі з використанням резервування та агрегації	6	1
8	Написання програмного забезпечення для контролера та WI-FI модуля для запропонованої системи	25	1
9	Тестування та оцінка роботи обраних методів резервування та агрегації мережі	1	1
10	Написання і оформлення документації (електронної та паперової)	85	2
разом		188	25

Отже, сумарний час виконання операцій технологічного процесу інженером становить 188 годин, а керівником 25 годин [41].

4.2. Визначення витрат на оплату праці та відрахувань на соціальні заходи

Заробітна плата працівника незалежно від виду підприємства визначається його особистим трудовим вкладом, залежить від кінцевих результатів роботи підприємства, регулюється податками і максимальними розмірами не обмежується. Розміри, порядок нарахування і виплати заробітної плати регулюються чинним законодавством України, відповідними указами і постановами, галузевими інструкціями. Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна заробітна плата складається із прямої заробітної плати та доплати, яка при укрупнених розрахунках становить 25% – 35% від прямої заробітної плати. При розрахунку заробітної плати кількість робочих днів в місяці слід приймати – 25,4 дні/міс., що відповідає 203,2 год./міс. Розмір місячних окладів керівника та інженерів слід приймати згідно існуючих на даний час норм. Основна заробітна плата розраховується за формулою:

$$З_{осн} = Т_С \cdot К_Г, \qquad (4.3)$$

де Т С – тарифна ставка, грн., К Г - кількість відпрацьованих годин.

Посадові оклади (тарифні ставки) за розрядами Єдиної тарифної сітки визначаються шляхом множення окладу (ставки) працівника 1 тарифного розряду на відповідний тарифний коефіцієнт. У разі коли посадовий оклад (тарифна ставка) визначені у гривнях з копійками, цифри до 0,5 відкидаються, від 0,5 і вище – заокруглюються до однієї гривні.

Законом України "Про Державний бюджет України на 2019 рік" від 23.11.2018 р. №2629 – VIII із змінами, внесеними згідно із Законом № 2696-VIII від 28.02.2019, ВВР, 2019, № 14, ст.66 та № 149-IX від 02.10.2019, установлено у 2019 році мінімальну заробітну плату: у місячному розмірі: з 1 січня - 4173 гривні; у погодинному розмірі: з 1 січня - 25,13 гривні. Приймемо 65 грн. для інженера, для керівника — 81 грн.

Тарифні ставки: керівник проекту – 81 грн./год., інженер – 65 грн./год.

Тоді скориставшись формулою 4.3 розрахуємо основну заробітну плату для інженера та керівника проекту.

Керівник проекту:

$$З_{осн} = 81 \cdot 25 = 2025 \text{ грн.}$$

Інженер:

$$З_{осн} = 65 \cdot 188 = 12220 \text{ грн.}$$

Додаткова заробітна плата становить 10–15% від суми основної заробітної плати:

$$З_{дод} = З_{осн} \cdot K_{допл}, \quad (4.4)$$

де $K_{допл}$ – коефіцієнт додаткових виплат працівникам 0,1.

Керівник проекту:

$$З_{осн} = 2025 \cdot 0{,}1 = 202{,}5 \text{ грн.}$$

Інженер:

$$З_{осн} = 12220 \cdot 0{,}1 = 1222 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{ОП}$) визначаються за формулою, і становлять:

$$В_{ОП} = З_{осн} + З_{дод}, \quad (4.5)$$

Керівник проекту:

$$В_{оп} = 2025 + 202{,}5 = 2227{,}5 \text{ грн.}$$

Інженер:

$$В_{оп} = 12220 + 1222 = 13442 \text{ грн.}$$

Таким чином загальна сума становить 15669,5 грн. Крім того, слід визначити відрахування на соціальні заходи:

- податок на доходи фізичних осіб: 18%;
- військовий збір 1,5%;
- єдиний соціальний внесок 22%.

У сумі зазначені відрахування становлять 41,5%.

Отже, загальна сума відрахувань на соціальні заходи становитиме:

$$В_{с.з} = ФОП \cdot 0{,}415 \quad (4.6)$$

де ФОП – фонд оплати праці, грн

Тоді, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з} = 15669{,}5 \cdot 0{,}415 = 6502{,}84 \text{ грн.}$$

Таблиця 4.2

Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн. 6=3+4+5
		Тариф на ставка, грн.	К-сть відпрацьов. год.	Фактично нарах. з/пл., грн.			
1	2	3	4	5	6	7	8
А	Б	1	2	3	4	5	6
1	Керівник проекту	81	25	2025	202,5	924,41	3 151,91
2	Інженер	65	188	12220	1222	5 578,43	19 020,43
Разом				14245	1424,5	6 502,84	22 172,34

4.3. Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_E = W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт; T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Згідно з постановою НКРЕ України від 05.10.2018 року № 1177 вартість електроенергії становить 308,25 коп./кВт·год.

Потужність ноутбука – 40 Вт з підключеним маршрутизатором і комутатором, кількість годин роботи обладнання згідно таблиці 4.1 – 213 год.

$$З_E = 0{,}04 \cdot 213 \cdot 3{,}0825 = 26{,}26 \text{ грн.}$$

4.4. Розрахунок витрат на матеріали

Результати розрахунку затрат на матеріали зводяться в таблицю 4.3.

Таблиця 4.3

Визначення величини затрат на матеріали

Найменування матеріальних ресурсів	Одиниця виміру	Норма витрат	Ціна за одиницю грн	Затрати матеріалів грн	Транспортно-заготівельні витрати, грн	Загальна сума витрат на матеріали, грн
Папір А4 ZOOM	Пачка	1	82	82	-	82
Ватман	Штук	10	10	100	-	100
Кабель витої пари	Штук	5	15	75	-	75
Концентратор	Штук	1	120	120	55	175
Провідники	Пачка	2	15	30	-	30
Разом						462

4.5. Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення. Для заміщення зношеної частини основних засобів виробництва підприємства роблять амортизаційні відрахування, тобто відрахування певних грошових сум відповідно до розмірів фізичного і морального зносу засобів виробництва.

Комп’ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$А = \frac{Б_в \cdot Н_а}{100}, \quad (4.8)$$

де А – амортизаційні відрахування за звітний період, грн., $Б_в$ – балансова вартість комп'ютера, на початок звітного періоду, грн., $Н_а$ – норма амортизації, %.

Для роботи використовується один ноутбук (вартість якого становить 12000 грн.), який працює 213 годин.

$$A = \frac{12000 \cdot 15\%}{100\%} = 1800 \text{ грн.}$$

4.6. Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

Накладні витрати можуть становити 20% від суми основної та додаткової заробітної плати працівників:

$$Н_в = В_{о.п} \cdot 0{,}2, \quad (4.9)$$

$$Н_в = 15669{,}5 \cdot 0{,}2 = 3133{,}9 \text{ грн.}$$

4.7. Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4. Собівартість ($С_в$) НДР розрахуємо за формулою:

$$С_в = В_{о.п} + В_{с.з} + З_{м.в} + З_е + Т_в + A + Н_в, \quad (4.10)$$

$$С_в = 15669{,}5 + 6502{,}84 + 462 + 26{,}26 + 1800 + 3133{,}9 = 27594.5 \text{ грн.}$$

Таблиця 4.4

Кошторис витрат на НДР

Зміст витрат	Сума, грн.	У % до загальної суми
1	2	3
Витрати на оплату праці (основну і додаткову заробітну плату)	15669,5	56,78
Відрахування на соціальні заходи	6502,84	23,56
Матеріальні витрати	462	1,67
Витрати на електроенергію	26,26	0,09
Амортизаційні відрахування	1800	6,52
Накладні витрати	3133,9	11,35
Собівартість	27594,5	100

4.8. Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_в \cdot (1 + P_{рен}) + K \cdot В_{н.і}}{K} \cdot (1 + ПДВ), \qquad (4.11)$$

де $Р_{рен}$ – рівень рентабельності, 30%; К – кількість замовлень; $В_{н.і}$ – вартість носія інформації, грн, ПДВ – ставка податку на додану вартість, (20%).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та Ві.н , оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_в \cdot \left(1 + P_{рен}\right) \cdot (1 + ПДВ), \quad (4.12)$$

Таким чином ціна ціна на проект складе:

$$Ц = 27594{,}5 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = \ 43047{,}42$$

Визначимо величину прибутку за формулою

$$П = Ц - С_в, \quad (4.13)$$

$$П = 43047{,}42 \ - \ 27594{,}5 \ = \ 15452{,}92 \text{ грн.}$$

Згідно даної формули отримаємо 15452,92 грн.

4.9. Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу. Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$Е_р = \frac{П}{С_в}, \quad (4.14)$$

де П – прибуток; $С_в$ – собівартість.

$$Е_р = \frac{15452{,}92}{27594{,}5} = 0{,}56.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_р$):

$$T_р = \frac{1}{E_р}, \tag{4.15}$$

$$T_р = \frac{1}{0{,}56} = 1{,}78 \text{ роки.}$$

Про доцільність розробки програми можна сказати при врахуванні критеріїв, які наведено у таблиці 4.5.

Таблиця 4.5

Техніко-економічні показники НДР

№ п/п	Показник	Значення
1	Собівартість, грн.	27594,5
2	Плановий прибуток, грн.	15452,92
3	Ціна, грн.	43047,42
4	Економічна ефективність	0,56
5	Термін окупності, рік	1,78

4.10. Висновки до розділу 4

У результаті проведення розрахунків можна зробити висновок: розробка матиме оптимальну економічну ефективність 0,56 і термін окупності становитиме менше двох років (1.78 року). Варто зазначити, що дані розрахунки носять номінальний характер і основна їх мета оцінити приблизну вартість дослідження та створення даного продукту. Номінальний характер розрахунків зумовлений тим, що даний програмний продукт має дослідницьке призначення.

РОЗДІЛ 5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1. Охорона праці

У роботі досліджуються методи резервування та агрегації каналів комп’ютерних мереж, які в свою чергу використовують мережеве обладнання, зокрема: маршрутизатори, комутатори, повторювачі, сервери, тому при роботі з даною технікою є необхідним дотримання правил охорони праці, техніки безпеки та протипожежної безпеки.

Згідно з законом України, нормативно-правові акти з охорони праці є обов'язковими для виконання у виробничих майстернях, лабораторіях, цехах, на дільницях та в інших місцях трудового і професійного навчання, облаштованих у будь-яких навчальних закладах [42].

Всі пристрої мережевої взаємодії потребують живлення від електромереж, при цьому електромагнітні поля, які створюються цими пристроями, особливо негативно впливають на організм людини, яка безпосередньо працює з джерелом випромінювання. При дії випромінювання на людину можливі гострі та хронічні форми порушення фізіологічних функцій організму. Такі порушення виникають в результаті дії електричної складової випромінювання на нервову систему, а також на структуру кори головного та спинного мозку, серцево-судинної системи. Детальніше про вплив електромагнітного випромінювання та методи захисту від нього описано у розділі 5.3.

Приміщення, в яких планується установка та подальша робота з комп’ютеризованими приладами, за допомогою яких буде будуватися віртуальний макет комп’ютерної мережі, повинні відповідати проектній документації будинку, погодженій з уповноваженими державними органами. Крім того, повинні бути враховані санітарні нормативи освітлення, вимоги до параметрів мікроклімату (температура, відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення.

Конкретні показники зазначених санітарних норм знаходяться в Державних санітарних правилах і нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98 [43].

Відповідне приміщення повинно бути укомплектоване системами центрального або індивідуального опалення, кондиціонування чи вентиляції повітря. При установці зазначених систем, необхідно переконатись, що батареї опалення, водопровідні труби, вентиляційні кабелі тощо, надійно сховані під захисними щитками, які перешкоджатимуть можливому потраплянню робітника під напругу.

У процесі роботи з модельованою комп'ютерною мережею, необхідно дотримувати правильний режим праці та відпочинку. В іншому випадку у робочого персоналу значно збільшується напруга зорового апарату, з'являються скарги на незадоволеність роботою, головні болі, дратівливість, порушення сну, втому і хворобливі відчуття в очах, попереку, в області шиї і руках.

Робочі місця слід розташовувати так, щоб уникнути попадання в очі прямого світла. Джерела освітлення рекомендується розташовувати з обох боків екрану паралельно напрямку погляду. Для уникнення світлових відблисків екрану, клавіатури в напрямку очей користувача, від світильників загального освітлення або сонячних променів, необхідно використовувати антиполискові сітки, спеціальні фільтри для екранів, захисні козирки, на вікнах - жалюзі.

Екран дисплея повинен бути розташованим перпендикулярно до напрямку погляду. Якщо він розташований під кутом, то стає причиною сутулості. Відстань від дисплея до очей повинна трохи перевищувати звичну відстань між книгою та очима. Перед екраном монітора, особливо старих типів, повинен бути спеціальний захисний екран. При його відсутності треба сидіти на відстані витягнутої руки від монітора.

Фільтри з металевої або нейлонової сітки використовувати не рекомендується, тому що сітка спотворює зображення через інтерференцію світла. Найкращу якість зображення забезпечують скляні поляризаційні фільтри. Вони усувають практично всі відблиски, роблять зображення чітким і контрастним.

При роботі з текстовою інформацією (в режимі введення даних та редагування тексту, читання з екрану даних про поточний стан мережі, зміна конфігурації

мережевих пристроїв тощо) найбільш фізіологічним правильним є зображення чорних знаків на світлому (чорному) фоні.

Монітор повинен бути розташований на робочому місці так, щоб поверхня екрана знаходилась в центрі поля зору на відстані 400-700 мм від очей користувача.

Залежно від джерела світла виробниче освітлення може бути: природним, що створюється прямими сонячними променями та розсіяним світлом небосхилу; штучним, що створюється електричними джерелами світла, та суміщеним, при якому недостатнє за нормами природне освітлення доповнюється штучним. Природне освітлення поділяється на: бокове (одно - або двостороннє), що здійснюється через світлові отвори (вікна) в зовнішніх стінах; верхнє - через ліхтарі та отвори в дахах і перекриттях; комбіноване - поєднання верхнього та бокового освітлення. Штучне освітлення може бути загальним та комбінованим.

Окрім вищезазначеного, важливою складовою охорони праці є пожежна безпека приміщень. Основними напрямками забезпечення пожежної безпеки є усунення умов виникнення пожежі та мінімізація її наслідків. Об'єкти повинні мати системи пожежної безпеки, спрямовані на запобігання пожежі, дії на людей та матеріальні цінності небезпечних факторів пожежі, в тому числі їх вторинних проявів. До таких факторів, згідно з ГОСТ 12.1.004-91, належать [44]:

- полум'я та іскри;
- підвищена температура навколишнього середовища;
- токсичні продукти горіння й термічного розкладу матеріалів і речовин;
- знижена концентрація кисню;

Відповідно до ГОСТ 12.1.004-91, пожежна безпека об'єкта повинна забезпечуватися системою запобігання пожежі, системою протипожежного захисту і системою організаційно-технічних заходів.

Основними вихідними даними при розробці комплексу технічних і організаційних рішень щодо забезпечення потрібного рівня пожежної безпеки в кожному конкретному випадку є чинна законодавча і нормативно-технічна база з питань пожежної безпеки, властивості матеріалів і речовин, що застосовуються у виробничому циклі, матеріалів, речовин і особливості виробництва.

Згідно з Положенням про порядок розроблення, затвердження, перегляду, скасування та реєстрації нормативних актів з питань пожежної безпеки, створено Державний реєстр нормативних актів з питань пожежної безпеки (НАПБ), до якого включено близько 360 найменувань документів, які поділені на 8 груп різних рівнів та видів: загальнодержавні, міжгалузеві, галузеві нормативні акти, нормативні акти міністерств, інших центральних органів виконавчої влади, міждержавні стандарти з питань пожежної безпеки, державні стандарти України (ДСТУ) з питань пожежної безпеки, галузеві стандарти з питань пожежної безпеки, нормативні документи в галузі будівництва з питань пожежної безпеки.

Окрім документів, що увійшли до вищезгаданого реєстру, існує низка нормативних актів спеціального призначення, окремі розділи яких регламентують вимоги пожежної безпеки, такі як ДНАОП 0.00-1.32-01 "Правила будови електроустановок. Електрообладнання спеціальних установок", який визначає вимоги до електрообладнання. На основі цих даних визначаються критерії небезпеки об'єкта, категорії приміщень і будівель за вибуховою і пожежною небезпекою, а також класи вибухонебезпечних і пожежонебезпечних зон.

5.2. Проведення аварійно-відновлювальних робіт на комп’ютерних та електричних мережах

У разі настання надзвичайної ситуації будь якого характеру (техногенного, природнього, соціального чи воєнного характеру), для забезпечення ліквідації наслідків та захисту цивільного населення, працює єдина державна система цивільного захисту. Система представляє собою сукупність органів управління, сил і засобів центральних та місцевих органів виконавчої влади, Ради міністрів Автономної Республіки Крим (РМ АРК), виконавчих органів рад, підприємств, установ та організацій, які забезпечують реалізацію державної політики у сфері ЦЗ (захист населення, територій навколишнього природного середовища та майна від НС шляхом запобігання таким ситуаціям, ліквідації їх наслідків і надання допомоги постраждалим у мирний час та в особливий період) [45].

Для забезпечення надання допомоги та ліквідації наслідків катастрофи, необхідно забезпечити можливість комунікації всіх органів. Підтримка зв’язку є важливим фактором для координування органів управління у надзвичайних ситуаціях. Кожний рівень єдиної державної системи має координаційні та постійно діючі органи управління щодо розв’язання завдань у сфері запобігання надзвичайним ситуаціям, захисту населення і територій від їх наслідків, систему повсякденного управління, сили і засоби, резерви матеріальних та фінансових ресурсів, системи зв’язку та інформаційного забезпечення.

З метою виконання завдання у всіх ланках міських і позаміських пунктів на основі автоматизованих систем централізованого оповіщення, мережі зв'язку і радіомовлення, а також спеціальних засобів, створюється система оповіщення та інформаційного забезпечення. Вона являє собою комплекс організаційно-технічних засобів для передачі відповідних сигналів і розпоряджень органам державної виконавчої влади, адміністрації підприємств, установ і організацій, силам ЦЗ і населенню.

Автоматизована система оповіщення та інформаційного забезпечення створюється на базі загальнодержавної мережі зв’язку та радіомовлення і поділяється на державну і регіональну. Система має забезпечити циркулярне оповіщення посадових осіб із застосуванням для цього міської телефонної мережі, засобів радіомовлення і телебачення. Система оповіщення та інформаційного забезпечення використовується централізовано. Архітектура технології провідного доступу зображена на рис. 5.1.

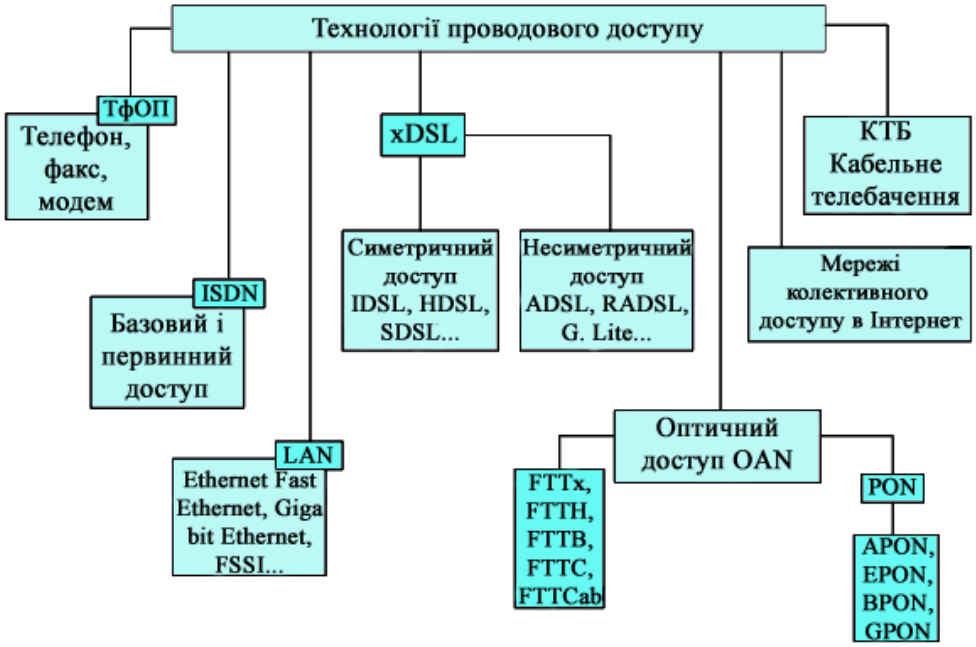


Рис. 5.1. Технології проводового доступу для передачі інформації

Оскільки комп'ютерні мережі також використовуються для передачі інформації, підтримка їх робочого стану та ліквідація можливих аварій є однією з пріоритетних завдань. Основними документами, що регламентують порядок оперативного виконання рятувальних та інших невідкладних робіт у районі НС є Кодекс цивільного захисту України, постанова Кабінету Міністрів України від 14 червня 2002 року №843 про затвердження Загального положення про спеціальну Урядову комісію з ліквідації надзвичайних ситуацій техногенного та природного характеру і Загального положення про спеціальну комісію з ліквідації надзвичайних ситуацій техногенного та природного характеру регіонального, місцевого та об'єктового рівня", постанова Кабінету Міністрів України від 19 серпня 2002 року №1201 "Про затвердження Положення про штаб з ліквідації надзвичайної ситуації техногенного та природного характеру".

Невідкладні роботи по відновленню пошкоджених лінії зв'язку (комп'ютерних та телефонних) проводяться комплексно з роботами по відновленню електроживлення, укріплення конструкцій та створення проїздів, якщо вони були заблоковані. Лінії телефонного зв'язку можуть одночасно виступати в ролі середовища передачі сигналів для мережі за допомогою технології ADSL (рис. 5.2).

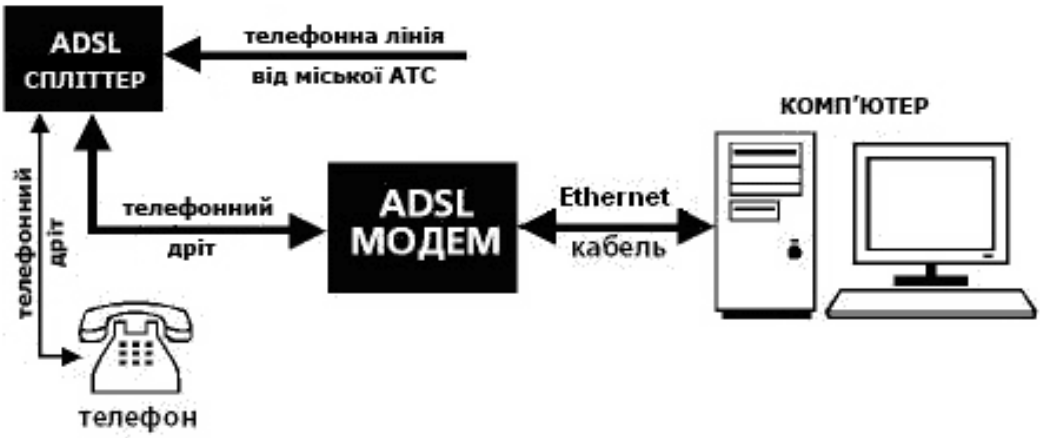


Рис. 5.2. Використання телефонних ліній технологією ADSL для передачі даних мережі Інтернет.

Для проведення аварійно-відновлювальних робіт залучаються сили цивільного захисту: сили Оперативно-рятувальної служби цивільного захисту, воєнізовані аварійно-рятувальні загони, спеціалізовані формування, невоєнізовані формування цивільного захисту. На об'єкті створюються групи працівників та службовців, які поділяються за призначенням та специфікацією робіт. Для виконання роботи щодо відновлення інформаційних мереж використовуються групи цивільного захисту загального призначення. До них відносяться:

- ведені рятувальні загони (команди, групи);
- зведені загони (команди) механізації робіт;
- рятувальні загони (команди, групи);
- формування загальної розвідки (розвідувальні команди, групи, ланки).

Роботи щодо відновлення комп'ютерних та електричних мереж відносяться до складу невідкладних. Це пов'язано з їх важливістю для забезпечення ліквідації наслідків надзвичайних ситуацій, отримання оперативного доступу до інформації та забезпечення нагальних потреб населення.

5.3. Оцінка дії електромагнітного поля, хвиль, імпульсу на людину та апаратуру, способи захисту

Вчений М.Фарадей відкрив явище електромагнітної індукції, що в подальшому призвело до створення електротехніки та відкриття електромагнітних хвиль, існування яких передбачив Д. Максвелл, а використання їх А. С. Поповим для радіозв'язку призвело до створення радіотехніки і радіоелектроніки. Такі важливі відкриття фізики як допомагають людині, так і шкодять її здоров'ю.

Електромагнітне поле (ЕМП) – особлива форма матерії, за допомогою якої здійснюється взаємодія між електрично зарядженими частинками. Воно складається з двох окремих полів – електричного та магнітного. Силові лінії цих полів взаємно перпендикулярні. Через електромагнітне поле передаються всі види електромагнітного випромінювання – від низькочастотного (радіохвилі) до високочастотного (рентгенівське та гамма-випромінювання) [46].

Електромагнітне поле у просторі поширюється у вигляді електромагнітної хвилі, яка перенасить енергію, замкнену в електричному та магнітному полях. Електричні та магнітні поля змінюються одночасно одне з одним. При цьому співвідношення між їх миттєвими значеннями завжди залишаються сталими. Лише на близьких від джерела відстанях, у так званій зоні несформованого поля, ця закономірність порушується.

Біологічна активність електромагнітних полів збільшується зі зменшенням довжини хвилі; найвища активність ЕМП – в області НВЧ. Так, наприклад, у початковій фазі спостерігається підвищене збудження, а потім зниження біоелектричної активності мозку, порушення умовно-рефлекторної діяльності, погіршення роботи серцевого м'язу. Функціональні порушення в ранній стадії, які викликані біологічною дією електромагнітних полів, зникають, якщо заборонити використання НВЧ випромінювання або поліпшити умови праці. Вивчаючи умови праці в галузі, гігієністи прийшли до висновку, що робітники-розробники НВЧ-приладів і установок, в більшій мірі зв'язані з мікрохвильовим опроміненням, яке при певних умовах може викликати професійне захворювання. Тому для кількісної оцінки опромінення електромагнітними полями прийнята інтенсивність опромінення, яка виражається у величинах густини потоку середньої потужності в просторі даної дільниці.

Електромагнітна енергія використовується у радіо-, радіорелейному і космічному зв’язках, телебаченні, радіолокації, радіонавігації. Вона застосовується у металургії та металообробних галузях промисловості для індукційного плавлення, зварювання, напилення металів, у деревообробній, текстильній, легкій та харчовій промисловості, у радіоспектроскопії, сучасній обчислювальній техніці, медицині (терапевтичні і діагностичні установки) тощо.

Джерелами електромагнітного випромінювання у виробничому приміщенні можуть бути неекрановані робочі елементи високочастотних установок (індуктори, конденсатори, ВЧ-трансформатори, фідерні лінії, батареї конденсаторів, котушки коливальних контурів тощо).

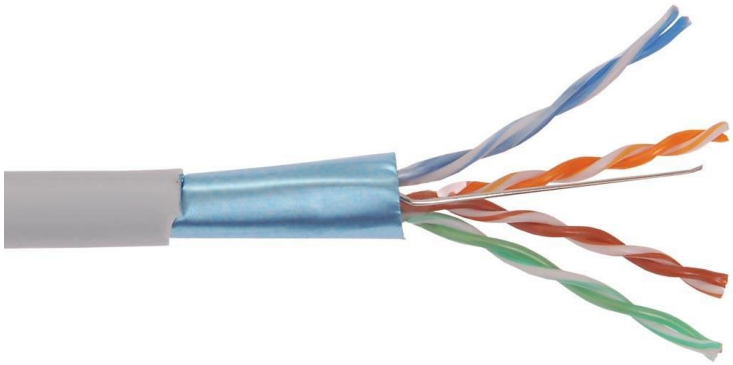
Електромагнітні поля особливо негативно впливають на організм людини, яка безпосередньо працює з джерелом випромінювання. В діапазоні промислових частот більше негативний вплив на біологічний об’єкт має електрична складова поля.

Найчутливішими до ЕМП є нейродинамічні процеси, які прямо чи побічно перемикають хронобіологічні процеси організму на патологічний або стресовий режим функціонування. При дії ЕМП на людину можливі гострі та хронічні форми порушення фізіологічних функцій організму. Такі порушення виникають в результаті дії електричної складової ЕМП на нервову систему, а також на структуру кори головного та спинного мозку, серцево-судинної системи.

Негативного впливу випромінювання зазнає також і апаратура. Особливо чутливими до зовнішніх електромагнітних перешкод є кабелі передачі даних у комп’ютерних мережах.

Вита пара - це кабель, який має дві або чотири кручених пари дротів (ізольованих або не ізольованих), у пластиковій оболонці. Неекранована вита пара характеризується слабкою захищеністю від зовнішніх електромагнітних перешкод, а також від підслуховування, яке може здійснюватися з метою, наприклад, промислового шпигунства. Причому перехоплення переданої в мережі інформації можливо як з допомогою контактної методу (наприклад, за допомогою двох голок, уткнутих у кабель), так і з допомогою безконтактного методу, який зводиться до радіоперехоплення випромінюваних кабелем електромагнітних полів. Кабель

неекранованої витої пари зображений на рис 5.3.



.

Рис. 5.3. Кабель неекранованої витої пари категорії CAT 4

Електромагнітні перешкоди здебільшого носять несиметричний характер. Це означає, що зміна напруги, створюваного цим джерелом, відбувається щодо землі. Симетричні кабельні ланцюги ефективно пригнічують перешкоду незалежно від природи її виникнення, якщо тільки перешкода діє на обидва дроти симетричного каналу передачі однаковим чином. Чисельною мірою відхилення від ідеального випадку служить спеціальний параметр - загасання несиметричних завад (Transverse Conversion Loss, TCL). В результаті гранична величина придушення перешкоди обмежена 40 дБ, що в ряді практично важливих випадків виявляється недостатнім. Для доведення ступеня придушення зовнішньої перешкоди до потрібного значення використовується додатковий провідник, виготовлений у формі трубки, який захищає пару проводів з усіх боків. Замість трубки зручніше використовувати її аналог у вигляді обплетення, що забезпечує необхідний захист і майже не обмежує гнучкість кабелю.

Електростатичний вплив блокується повністю за рахунок ефекту клітки Фарадея. Магнітне поле в значній мірі пригнічується завдяки явищу взаємної індукції (рис. 5.4). В результаті високочастотне випромінювання має порівняно невелику глибину проникнення і не досягає внутрішнього контуру.

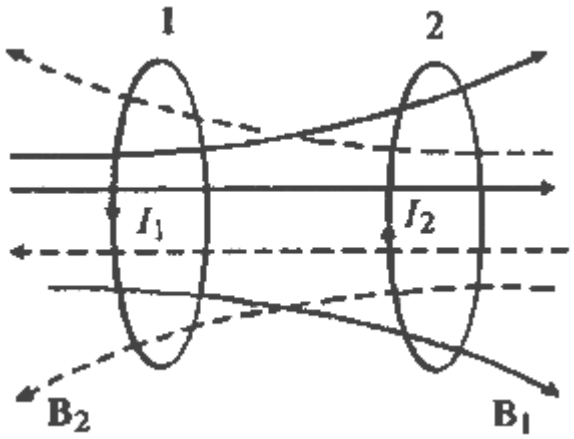


Рис. 5.4. Фізичне явище взаємоіндукції

Звивання провідників проводиться з метою підвищення ступеня захисту зв’язку провідників однієї пари (електромагнітні перешкоди однаково впливають на обидва дроти пари) і подальшого зменшення електромагнітних перешкод від зовнішніх джерел, а також взаємних перешкод при передачі диференціальних сигналів. Для зниження впливу окремих пар кабелю (періодичного зближення провідників різних пар) в кабелях UTP категорії 5 і вище дроти пари звиваються з різним кроком. Для поглинаючих екранів використовують основу з каучуку, поролону, полістиролу тощо з електропровідними добавками (активоване вугілля, сажа, порошок карбонільного заліза), а також керамічно-металеві композиції. Екран також може бути з'єднаний з неізольованим дренажним проводом, який служить для заземлення та механічно підтримує екран. (рис. 5.5).

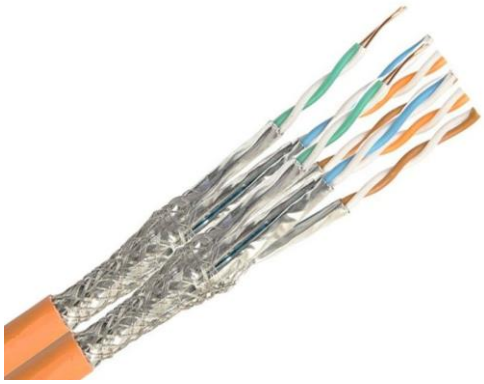


Рис. 5.5. Екранована вита пара CAT 6

Для екранування обладнання (комутатори, маршрутизатори, концентратори, повторювачі тощо), використовують відбивні екрани. Для відбивних екранів найкращими матеріалами є мідь, латунь, алюміній, а також сталь. Ефективність екранів залежить від частоти ЕМП, матеріалу екрана, його розмірів і якості конструкції. Екрани можуть бути суцільними і сітчастими. Максимальне проникнення електромагнітної перешкоди спостерігається в тих випадках, коли вектор напруженості магнітного поля спрямований по дотичній до площини отвору, а електричного поля - по перпендикуляру. При цьому в безпосередній близькості від отвори перешкода надає максимально шкідливий вплив. Тому при розробці конструкції електронного пристрою його особливо чутливі елементи намагаються розмістити далеко від щілин і отворів. Ефективним методом боротьби з такого з перешкодами є гальванічна розв'язка (рис 5.6). Для цього використовується роздільне живлення силових і слабкострумових пристроїв, пристроїв генерування керуючих та виконавчих сигналів тощо. Для захисту оператора від впливу ЕМП використовується метод екранування приміщення. Електромагнітне екранування приміщень дозволяє захистити людину від впливу електромагнітного поля а також радіоелектронні прилади від впливу зовнішніх полів і локалізувати їх власні випромінювання, перешкоджаючи їх появі в навколишньому просторі.

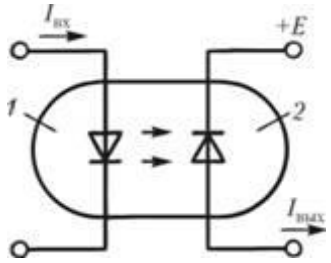


Рис 5.6. Гальванічна розв’язка

Екранування технічних засобів опрацювання інформації та приміщень, в яких відбувається приймання, передавання й опрацювання конфіденційної інформації, дозволяє знизити рівень електромагнітних випромінювань до заданих величин. У результаті практично неможливе несанкціоноване знімання інформації, що підвищує рівень безпеки.

Сучасні вимоги до екранованих приміщень визначаються комплексом чинників, що впливають або можуть впливати в конкретних умовах на інформацію, яка захищається та обслуговуючий персонал. Основні чинники, що впливають або можуть впливати на інформацію, яка захищається, мають електромагнітну природу, визначено ГОСТ Р 51275. Приклад екранованого приміщення для захисту апаратури та операторів, зображений на рис. 5.7.

Рис. 5.7. Модель екранованого приміщення

5.4. Висновки до розділу 5

Отже, зважаючи на особливості роботи з обладнанням, був проведений аналіз діючих законодавчих актів та норм щодо облаштування робочих приміщень. Було проаналізовано забезпечення нівелювання негативного впливу електромагнітного випромінювання та імпульсу на людину та апаратуру. Здійснено перелік невідкладних дій у разі виникнення надзвичайних ситуацій, детально досліджено роль комп’ютерних мереж для комунікації населення та органів влади. Проведений опис параметрів, особливостей розміщення джерел світла та заходів протипожежної безпеки у приміщеннях, де проводиться робота над проектуванням макету для дослідження методів та засобів резервування та агрегації каналів комп’ютерних мереж.

РОЗДІЛ 6 ЕКОЛОГІЯ

6.1. Роль матеріало- та ресурсозбереження у вирішенні екологічних проблем

Світовий досвід свідчить про те, що раціональне природокористування та ресурсозбереження забезпечуються завдяки впровадженню ефективних економічних механізмів управління природними ресурсами, використанню маловідходних і безвідходних технологій, ефективних систем і засобів контролю за використанням та збереженням ресурсів і захистом довкілля від забруднення. Проведення такої політики неможливе без фахівців із економіки довкілля і природних ресурсів, які орієнтували б на такий розвиток економіки і виробництва, що забезпечує оптимальний обсяг споживання природних ресурсів [47].

Ресурсозбереження – це організаційна, економічна, науково-технічна, практична та інформаційна діяльність, яка супроводжує усі стадії життєвого циклу об’єктів і спрямована на забезпечення мінімальної витрати речовини та енергії на одиницю кінцевого продукту, враховуючи існуючий рівень розвитку техніки і технології та найменший вплив на людину і природні системи.

Поняття ресурсозбереження ґрунтується на тенденції дбайливого ставлення до природних ресурсів. Вона охоплює будь-які види діяльності, що спрямовані на охорону і відтворення природного середовища. Ресурсозбереження передбачає підвищення ефективності виробництва при зниженні його ресурсоємності. Однак підвищення ефективності виробництва направлене на задоволення суспільних потреб і вимагає збільшення використання кількості ресурсів. Водночас підвищення ролі соціальних і економічних чинників вимагає зменшення ресурсоємності виробництва та обсягів використання природних ресурсів. Отже, стає актуальною проблема оптимізації співвідношення обсягів використання природних ресурсів у суспільному виробництві та ступеня задоволення суспільних потреб, використовуючи при цьому досягнення науки і техніки.

Ресурсозбереження охоплює багато аспектів і складається із різних видів діяльності, зокрема виробничо-технічну, організаційно-економічну, правову,

маркетингову, освітню, науково-дослідну, соціальну та екологічну. Екологічна діяльність спрямована на екологічні результати ресурсозбереження внаслідок чого поліпшується якість довкілля, знижується рівень антропогенного та техногенного забруднення, зменшуються обсяги використання природних ресурсів у промисловому виробництві. Усі складові ресурсозбереження взаємопов'язані і взаємозалежні.

З метою раціонального використання ресурсів та їх збереження в різних галузях необхідною є правильна оцінка еколого-економічної ефективності ресурсозберігаючих заходів. Вона потрібна для вибору оптимальних ресурсозберігаючих проектів при обмежених фінансових коштах, визначення найперспективніших заходів враховуючи бюджетне фінансування, подальшого розвитку та забезпечення конкурентоспроможності галузі; планування та прогнозування розвитку галузевих комплексів. За допомогою такої оцінки передбачають соціальні, економічні, екологічні та політичні наслідки ресурсозберігаючих проектів, які представляють інтерес для галузі.

Екологічні інновації ресурсозберігаючого напряму можуть бути впроваджені в технологічній, організаційній і управлінській сферах виробництва. Зокрема, використання у виробництві еколого-орієнтованих технологій сприяє зменшенню шкідливого впливу на довкілля, а також дає можливість отримати економічний ефект завдяки зниженню обсягів споживання енергії та більш ефективним використанням ресурсів. Впровадження екологічних інновацій може реалізовуватися як з метою зменшення шкідливого впливу на навколишнє середовище, так для підвищення продуктивності праці та якості продукції. З огляду на це, екологічні інновації можна поділити на: природоохоронні технології, еко ефективні інновації та системні інновації. Важливим джерелом системних інновацій є ресурсозбереження – створення та застосування нових матеріалів, біотехнологій, поновлюваних джерел енергії, а також інформаційно - комунікаційних технологій.

У розвинених країнах світу спостерігається збільшення випуску продукції та розширення промислового виробництва, внаслідок того зростає забруднення довкілля, глобалізуються екологічні проблеми, нагромаджуються відходи виробництва. Безальтернативним напрямом подальшого економічного розвитку є

ресурсозберігаюча діяльність, яка використовує новітні досягнення науково-технічного прогресу і тим самим забезпечує економію природних ресурсів, зниження рівня забруднення довкілля, завдяки застосуванню екологічно досконалих технологій, зменшення генерування та підвищення рівня рециркуляції відходів. Розвиненим країнам світу у певній мірі вдалося пригальмувати швидкість росту глобальної небезпеки внаслідок впровадження природоохоронних і ресурсозберігаючих заходів, однак у світовому масштабі ця проблема ще не розв’язана. Багато європейських країн спрямовують до 1% свого валового національного продукту на розвиток міжнародних програм для захисту довкілля.

6.2. Державна та громадська екологічна експертиза

Екологічна експертиза – це встановлення відповідності планованої господарської й іншої діяльності екологічним вимогам і визначення допустимості її здійснення з метою попередження можливих несприятливих впливів на довкілля і пов'язаних з ними соціальних, економічних й інших наслідків. Екологічну експертизу в Україні можуть проводити державні структури та громадські організації. В тому випадку, коли ЕЕ організовується та проводиться спеціально уповноваженими державними органами, вона називається державною екологічною експертизою (ДЕЕ).

Відповідно до Конституції України, ЗУ "Про охорону навколишнього природного середовища", "Про екологічну експертизу", Конвенції "Про доступ до інформації, участь громадськості в процесі прийняття рішень та доступу до правосуддя з питань, що стосуються довкілля" тощо та з метою забезпечення прав громадськості щодо участі у прийнятті рішень у сфері охорони довкілля МЕПР було затверджено "Положення про участь громадськості у прийнятті рішень у сфері охорони довкілля". Згідно цього Положення наведені нижче терміни вживаються в такому значенні. Громадськість - одна або більше фізичних чи юридичних осіб, їх об'єднання, організації або групи, які діють згідно з чинним законодавством України або практикою. Зацікавлена громадськість - громадськість, на яку впливає реалізація рішень з питань, що справляють чи можуть справити негативний вплив на стан

довкілля. Громадське обговорення (публічне слухання або відкрите засідання) - процедура виявлення громадської думки з метою її урахування при прийнятті органами виконавчої влади рішень з питань, що справляють чи можуть справити негативний вплив на стан довкілля (розміщення, проектування, будівництво або реконструкція об'єктів; розробка проектів нормативно-правових актів тощо.

Державна і громадська екологічні експертизи в Україні регулюються тими самими законами, однак функції цих процедур, а також їх місце у системі прийняття рішень істотно різняться [48]. При цьому процедура ГЕЕ практично не регламентована підзаконними актами. Право українських громадян на участь у проведенні ГЕЕ є одним із елементів закріпленої у ст. 8, 9, 10, 11 ЗУ "Про охорону навколишнього природного середовища" системи екологічних прав громадян. Законодавче закріплення правових засад ГЕЕ (ст. 26) зумовлене підвищеною зацікавленістю громадськості у безпосередньому вирішенні екологічних проблем, в усуненні прогалин, які мають місце в законодавстві, а також, у кінцевому результаті - у відверненні аварій і катастроф техногенного походження, попередженні й ліквідації проявів стихійних сил природи. Ст. ЗО визначає, що ГЕЕ здійснюється незалежними групами фахівців з ініціативи громадських об'єднань, а також місцевих органів влади за рахунок їх власних коштів або на громадських засадах. ГЕЕ проводиться незалежно від ДЕЕ.

Громадські природоохоронні об'єднання мають право: а) брати участь у розробці планів, програм, пов'язаних з охороною довкілля, розробляти і пропагувати свої екологічні програми; б) утворювати громадські фонди охорони природи; за погодженням з місцевими Радами за рахунок власних коштів і добровільної трудової участі членів громадських об'єднань виконувати роботи з охорони і відтворення природних ресурсів, збереження та поліпшення стану довкілля; в) брати участь у проведенні спеціально уповноваженими державними органами управління в галузі охорони довкілля перевірок виконання підприємствами, установами та організаціями природоохоронних планів і заходів; г) проводити ГЕЕ, обнародувати її результати і передавати їх органам, уповноваженим приймати рішення; д) вільного доступу до екологічної інформації; е) виступати з ініціативою проведення державного І місцевих

референдумів з питань, пов'язаних з охороною довкілля, використанням природних ресурсів і забезпечення екологічної безпеки; є) вносити до відповідних органів пропозиції- про організацію територій та об'єктів ПЗФ; ж) подавати до суду позови про відшкодування шкоди, заподіяної внаслідок порушення законодавства про охорону довкілля; з) брати участь у заходах міжнародних неурядових організацій з питань охорони довкілля; и) брати участь у підготовці проектів нормативно-правових актів з екологічних питань; І) оскаржувати в установленому законом порядку рішення про відмову чи несвоєчасне надання за запитом екологічної інформації або неправомірне відхилення запиту та його неповне задоволення.

Діяльність громадських об'єднань в галузі охорони довкілля здійснюється відповідно до законодавства України на основі їх статутів. До форм участі громадськості в прийнятті рішень належать: робота в складі експертних і робочих груп, комісій, комітетів з розробки програм, планів, стратегій, проектів нормативно-правових актів, оцінок ризиків; робота в складі державних еколого- експертних комісій; громадське обговорення проектів рішень центральних органів виконавчої влади та їх органів на місцях, що справляють чи можуть справити негативний вплив на стан довкілля, під час проведення парламентських слухань, конференцій, семінарів, круглих столів, обговорення результатів соціологічних досліджень, зборів громадян за місцем проживання.

6.3. Висновки до розділу 6

Отже, розглядаючи питання ресурсозбереження у вирішенні екологічних проблем, а також питання проведення екологічних експертиз уповноваженими органами влада та за громадськістю, можна зробити висновок щодо необхідності подальшої роботи у цьому напрямку.

ВИСНОВКИ

Основні наукові та практичні результати роботи полягають у наступному:

- Проведено детальний аналіз наукових публікацій та мережевих стандартів з забезпечення надійності, дана оцінка сучасному стану розвитку технологій та методів резервування та агрегації каналів комп’ютерних мереж, обґрунтована доцільність подальших робіт у даній галузі. В сучасних комп’ютерних мережах для забезпечення надлишкового резервування важливих вузлів комп’ютерної мережі, використовуються протоколів сімейства STP. З часу першої реалізації, сімейство активно розвивається, розширюючи спектр своїх інструментів для забезпечення відмовостійкості мережі. Зважаючи на сучасні вимоги, нові версії протоколів дозволяють здійснювати балансування кадрів на канальному рівні моделі OSI.

- Досліджена технологія агрегації каналів комп'ютерної мережі для підвищення пропускної здатності мережі а також забезпечення відмовостійкості. Перевагами такої технології є підтримка практично всім мережевим обладнанням, що дозволяє здійснювати ефективне масштабування мережі без втрати продуктивності. Порівняння переваг та недоліків статичної та динамічної агрегації дозволило здійснити висновок щодо ефективності використання кожного з методів в різних умовах.

- Здійснена оцінка доцільності одночасного використання різних методів резервування та агрегації для забезпечення ефективної роботи комп’ютерної мережі. Це дало змогу зменшити навантаження на мережеве обладнання, що в свою чергу впливає на надійність системи в цілому.

- Проаналізований вплив використання протоколів резервування та агрегації на пропускну здатність мережі, що дозволило обґрунтувати вибір методів, зважаючи на особливості мережевого обладнання сегментів.

- Обґрунтовано доцільність використання методів балансування навантаження мережевого та прикладного рівня для забезпечення відмовостійкості серверного обладнання (TFTP,DHCP,DNS серверів).

- Досліджена ефективність використання протоколів надлишкового резервування мережевих екранів для забезпечення безпеки прикордонних шлюзів, а також демілітаризованої(DMZ) зони. Такі технічні рішення дозволили підвищити захищеність мережі від атак зловмисників.

- Змодельована комп’ютерна мережа для дослідження ефективності використання обраних протоколів та технологій забезпечення резервування та агрегації каналів передачі даних.

- Апробовано запропоновані для кожного рівня представлення методи та засоби резервування та агрегації каналів комп’ютерних мереж, методи балансування навантаження.

- Обґрунтовано економічну ефективність проведення досліджень дипломної роботи магістра шляхом проведення відповідних розрахунків, що дало змогу встановити термін окупності.

- Проаналізовано вимоги з охорони праці та безпеки в надзвичайних ситуаціях, що дало змогу визначити шляхи мінімізації негативного впливу комп’ютерної техніки на себе та операторів, проаналізована важливість комутації органів влади за допомогою комп’ютерних мереж у разі виникнення надзвичайних ситуацій.

- Проаналізована роль матеріало та ресурсозбереження у вирішені екологічних проблем та досліджено важливість державної та громадської екологічної експертизи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. А. Г. Микитишин., М. М. Митник., П. Д. Стухляк.В., В. В. Пасічник. Комп'ютерні мережі: [навчальний посібник]. Львів, 2013. 373 с.

2. Буров Є. В. Комп'ютерні мережі: підручник. Львів, 2010. 262 с.

3. Day J. Patterns in Network Architecture: A Return to Fundamentals. 2007. 429 p.

4. Bates R. J., D. W. Gregory. Voice & data communications. 2011. 650 p.

5. Єсаулов С. М., Бабічева О. Ф. Автоматизація технологічних процесів та установок. Конспект лекцій. Харків, 2009. 78 с.

6. Lammale T., S. Odom., K. Wallase. CCNP: Routing Study Guide. 2015. 444 p.

7. Inter-Switch Link and IEEE 802.1Q Frame Format. 2006. URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html (дата звернення: 06.10.2019).

8. Abouzeid A., S. Roy. Stochastic modeling of TCP in networks with abrupt delay variations. 2003. 524 p.

9. Grady Butch., Jim Conallen., Michael Engle. Object Oriented Analysis and Design with Application Examples. 2008.

10. IEEE 802.3ad Link Bundling. 2006. URL: https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/sbcelacp.html (дата звернення: 06.10.2019).

11. Akan O.B., I.F. Akyildiz. ATL: an adaptive transport layer suite for next-generation wireless internet. 2004. 817 p.

12. Andrew Tanenbaum. Structured Computer Organization. 2013. 947 p.

13. Сучасні технології побудови комп’ютерних мереж. 2013. URL: http://m.programming.in.ua/other-files/internet/234-technology-for-creting computer-network (дата звернення: 08.10.2019).

14. Implementation of Versatile Resilience Packet Ring protocol (VRPR) in Datacenter Network. 2017. URL: https://www.researchgate.net/publication/314259259_Implementation_of_Versatile_Resili

ence_Packet_Ring_protocol_VRPR_in_Datacenter_Network (дата звернення: 10.10.2019).

15. IEEE 802.3ad Link Aggregation (LAG). 2007. URL: http://www.ieee802.org/3/hssg/public/apr07/frazier_01_0407.pdf (дата звернення: 11.10.2019).

16. Adjih C., E. Baccelli., P. Jacquet. Link State Routing in Wireless Ad-Hoc Networks. Perkins, 2003.

17. Jenson S. Beyond Round Robin: Load Balancing for Latency. 2016. URL: https://linkerd.io/2016/03/16/beyond-round-robin-load-balancing-for-latency/ (дата звернення: 12.10.2019).

18. C. Perkins., E. Belding-Royer. Quality of service for Ad Hoc on-demand distance vector routing. 2005. 284 p.

19. Israel K., K. Mani. Fault-Tolerant Systems. San Francisco, 2007. 400 p.

20. Николайчук Я. М., Н. Я. Возна., І. Р. Пітух. Проектування спеціалізованих комп'ютерних систем. Тернопіль, 2010. 394 с.

21. The LAN turns 30, but will it reach 40?. 2008. URL: https://www.computerworld.com/article/2538907/the-lan-turns-30--but-will-it-reach-40-.html (дата звернення: 16.10.2019).

22. Radio Frequency Interference - And What to Do About It. 2011. URL: http://www.radiosky.com/journal0901.html (дата звернення: 17.10.2019).

23. Catalyst 2960 Switch Command Reference. San Jose, 2007. 766 p.

24. Implementation of Versatile Resilience Packet Ring protocol (VRPR) in Datacenter Network. 2017. URL: https://www.researchgate.net/publication/314259259_Implementation_of_Versatile_Resilience_Packet_Ring_protocol_VRPR_in_Datacenter_Network (дата звернення: 18.10.2019).

25. Shamim S. M. Data Communication Speed and Network Fault Tolerant Enhancement over Software Defined Networking. 2018. URL: https://link.springer.com/article/10.1007/s11277-018-5759-5 (дата звернення: 20.10.2019).

26. Khalid R. Cisco Network Topology and Design. San Jose, 2002. 520 p.

27. Biryukov A., G. Gong., D. Stinson. Selected Areas in Cryptography. 2011. 411 p.

28. Vargas E. Sun Cluster Environment Sun Cluster 2.2. New Jersey, 2001. 432 p.

29. Stalling W. Operating Systems: Internals and Design Principles. New Jersey, 2012. 768 p.

30. Jenson S. Beyond Round Robin: Load Balancing for Latency. 2016. URL: https://linkerd.io/2016/03/16/beyond-round-robin-load-balancing-for-latency/ (дата звернення: 24.10.2019).

31. Load balancer groups. 2013. URL: https://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0/com.ibm.dp.doc/lbg_loadbalancergroup.html (дата звернення: 25.10.2019).

32. Gurasis S. An Improved Weighted Least Connection Scheduling Algorithm for Load Balancing in Web Cluster Systems. 2018. URL: https://pdfs.semanticscholar.org/5b6e/4a4948b422276db4b78415173cd888bc457d.pdf (дата звернення: 25.10.2019).

33. Rouse M. What is star network?. 2017. URL: https://searchnetworking.techtarget.com/definition/star-network. (дата звернення: 26.10.2019).

34. Behrouz A. F., S. Chung. Data Communications and Networking. New York, 2007. 279 p.

35. Unified Extensible Firmware Interface Specification. 2013. URL: https://uefi.org/sites/default/files/resources/2_4_Errata_A.pdf (дата звернення: 27.10.2019).

36. Edgeworth B., A. Foss., R. Garza. Data Communications and Networking. 2014. 840 p.

37. Mohammadi S. A new scheduling algorithm for server farms load balancing. 2010. URL:https://www.researchgate.net/publication/224173356_A_new_scheduling_algorithm_for_server_farms_load_balancing (дата звернення: 28.10.2019).

38. BSD Overview. 2017. URL: https://developer.apple.com/library/archive/documentation/Darwin/Conceptual/KernelProgramming/BSD/BSD.html (дата звернення: 28.10.2019).

39. Taking Over Master Membership and Securing VRRP. 2016. URL: https://blog.cadre.net/taking-over-master-membership-and-securing-vrrp (дата звернення: 29.10.2019).

40. Harrington D. CCNP Practical Studies: Troubleshooting. 2003. 262 p.

41. Шевченко Л. С. Основи економічної теорії. Харків, 2008. 448 с.

42. Закон України «Про охорону праці». Відомості Верховної ради України (ВВР), 1992, №2694-XII, ст. 1.

43. ДСанПіН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин.

44. ГОСТ 12.1.004-91. Система стандартів безпеки праці. Пожежна безпека. Загальні вимоги.

45. Кодекс цивільного захисту України. 2019. URL: https://zakon.rada.gov.ua/laws/main/5403-17 (дата звернення: 01.11.2019).

46. Стеблюк М. І. Цивільна оборона та цивільний захист (підручник). Київ, 2013. 487 с.

47. Дзякевич Ю. В. Економічні основи ресурсозбереження. Навчальний посібник. Тернопіль, 2015. 76 с.

48. Добровольський В. В. Екологічна експертиза. Навчальний посібник. Миколаїв, 2013. 220 с.

Додаток А Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Національна академія наук України
Університет імені П'єра і Марії Кюрі (Франція)
Маріборский університет (Словения)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Шяуляйська державна колегія (Литва)
Жешувський політехнічний університет ім. Лукасевича (Польща)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Національний університет біоресурсів і природокористування України (Україна)
Наукове товариство ім. Шевченка
ГО «Асоціація випускників Тернопільського національного технічного університету імені Івана Пулюя»

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том ІІ

VIII Міжнародної науково-технічної конференції молодих учених та студентів

27-28 листопада 2019 року

УКРАЇНА
ТЕРНОПІЛЬ – 2019

УДК 004.7
О.Б. Ліщук, Є.В Тиш канд. техн. наук
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МЕТОДИ ТА ЗАСОБИ РЕЗЕРВУВАННЯ ТА АГРЕГАЦІЇ КАНАЛІВ КОМП'ЮТЕРНИХ МЕРЕЖ

O.B. Lishchuk, I. V. Tysh Ph.D.

METHODS AND MEANS OF RESERVATION AND AGGREGATION OF CHANNELS OF COMPUTER NETWORKS

На сьогодні надзвичайно важливою характеристикою комп'ютерної мережі є надійність – здатність системи до штатного функціонування протягом необхідного періоду часу. З розвитком комп'ютерних мереж резервування та забезпечення стабільної роботи глобальної мережі Інтернет, яка налічує мільйони серверів та клієнтів, стало однією з пріоритетних задач.

Покращення надійності системи полягає в запобіганні відмов і збоїв завдяки використанню електронних схем і компонентів з високим рівнем ітерації, а також мінімізація фізичних перешкод, розробки менш навантажених режимів роботи всіх схем, дотримання режимів роботи з певними температурами та завдяки вдосконаленню технологій складання конструкції і допоміжних елементів систем.

Агрегування каналів у комп'ютерних мережах – це технологія яка дозволяє збільшувати пропускну здатність та надійність каналу. При застосуванні технології до фізичного середовища всі зв'язки залишаються в робочому стані, і весь наявний трафік рівномірно розподіляється по пропускному каналі для балансування навантаження на середовище. В ідеалі сьута пропускання агрегованого каналу може дорівнювати сумі сьут пропускання всіх об'єднаних в ньому каналів.

Надлишкове резервування активно застосовується в проектуванні комп'ютерних мереж не лише для забезпечення надійності а й для балансування навантаження між мережевими пристроями, що дозволяє застосовувати резервування в сучасних масштабованих комп'ютерних мережах.

Вченими, актуальні дослідження яких стосуються області агрегації та резервування каналів комп'ютерних мереж, є Andrew Tanenbaum, Jim Kurose, Larry L. Peterson та інші.

Дослідники дійшли згоди, що продовження праці в цьому напрямку є важливим елементом для забезпечення роботи мереж, тому дослідження методів та засобів резервування та агрегації каналів у комп'ютерних системах та мережах є актуальною задачею.

Література

1. Tanenbaum A. S. Computer Networks / A. S. Tanenbaum, D. J. Wetherall. – New Jersey: Prentice Hall, 2010. – 884 c.

2. Здолбіцька Н. В. Дослідження пропускної здатності агрегованих інтернет-каналів / Н. В. Здолбіцька, А. П. Здолбіцький, Ю. В. Янчук // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. - 2015. - № 18. - С. 87-91. - URL: http://nbuv.gov.ua/UJRN/Kitonv_2015_18_16

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ »

11–12 грудня 2019 року

ТЕРНОПІЛЬ
2019

УДК 004.7
О. Ліщук, Є. Тиш
(Тернопільський національний технічний університет імені Івана Пулюя)

ПЕРЕВАГИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ АГРЕГАЦІЇ КАНАЛІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ

UDC 004.7
O. Lishchuk, E. Tysh
(Ternopil Ivan Puluj National Technical University, Ukraine)

ADVANTAGES OF USE OF COMPUTER NETWORK CHANNEL AGGREGATION TECHNOLOGY

Технологія агрегування каналів (link aggregation) дозволяє здійснювати об'єднання декількох фізичних каналів зв'язку в один логічний [1].

Завдяки стандартизації технічних засобів для практичного використання технології статична (static) та динамічна (dynamic) агрегація каналів підтримується більшістю мережевих пристроїв. Це дозволяє будувати масштабовані мережі з використанням технології, уникаючи конфліктних ситуацій в локальних сегментах.

Статична агрегація каналів дозволяє налаштовувати ділянки мережі для активної (active) передачі даних в режимі дуплексу. Така конфігурація дозволяє здійснювати гарячу зміну конфігурації без додаткових затримок для перебудови.

Динамічна модель агрегації реалізується за допомогою протоколу LACP (link aggregation control protocol), який підтримується всіма виробниками мережевого обладнання. Використання динамічної моделі дозволяє уникнути можливих помилок при ручному налаштуванні. Завдяки використанню програмних методів для побудови та керування каналу, можна здійснювати його моніторинг для забезпечення кращого часу реакції на несправності.

Збільшення пропускної здатності каналу в ідеальних умовах буде дорівнювати сумі каналів, які беруть участь в агрегації. LACP дозволяє об'єднувати до восьми каналів передачі, таким чином, при використанні інтерфейсів Fast Ethernet з швидкістю 100 Mbit/s отримується агрегований та відмовостійкий канал передачі даних з швидкістю 800 Mbit/s.

Пропріетарні розширення загальнодоступного протоколу, такі як MLT [2], дозволяють використовувати більшу кількість каналів для агрегації, а також включають в себе технічні рішення для вузькоспеціалізованої роботи в сфері передачі великих об'ємів даних.

Зважаючи на можливість агрегації забезпечувати надійність каналу зв'язку та збільшувати швидкість передачі даних, практичне застосування технології є доцільним в сучасних комп'ютерних мережах.

Література

1. Understanding Link Aggregation Control Protocol [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://community.fs.com/blog/understanding-link-aggregation-control-protocol.html.
2. Russell J. Multi-Link Trunking / Jesse Russell., 2012. – 162 с.

Додаток Б Графічне представлення макету комп’ютерної мережі

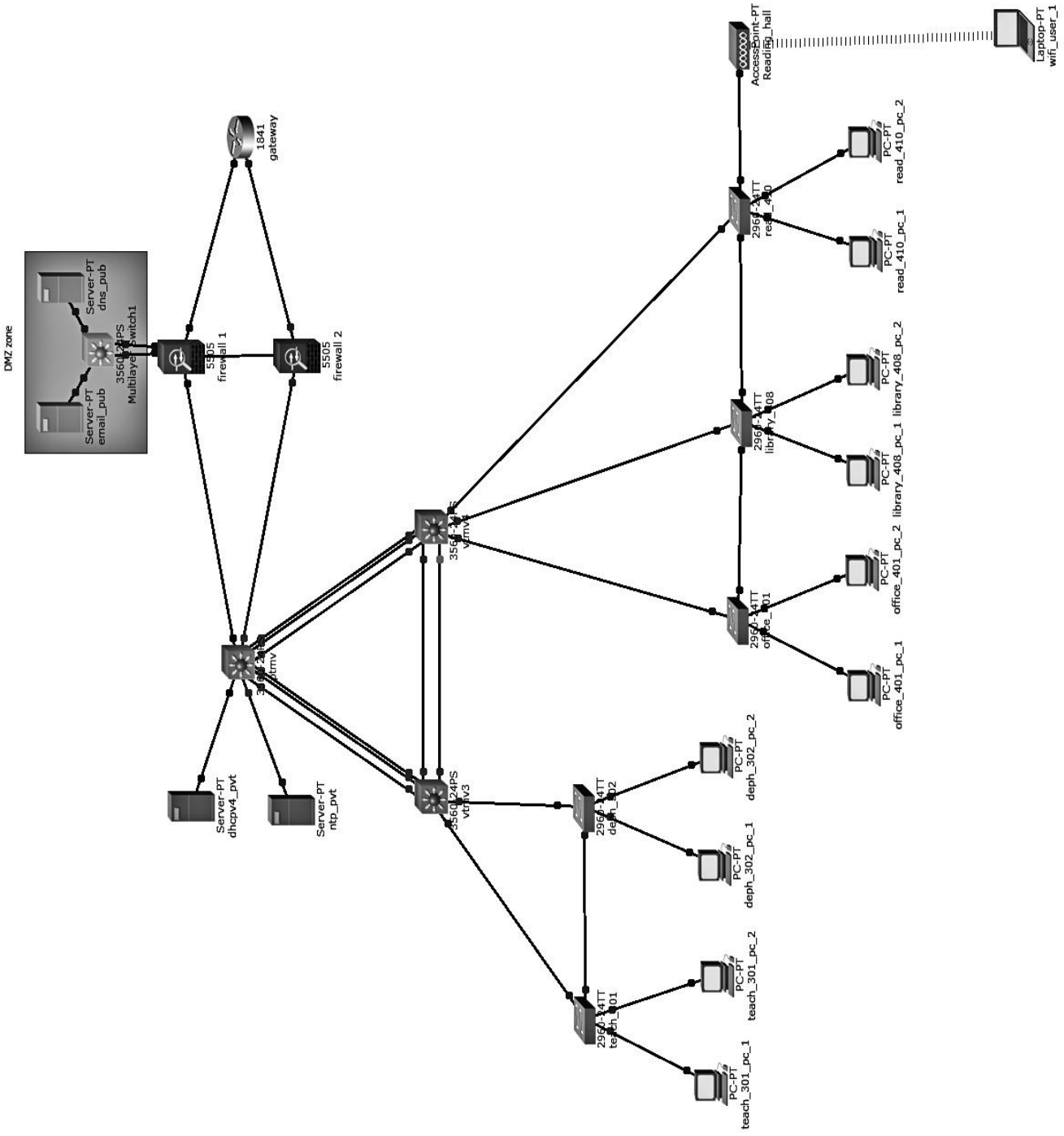


Рис. Б.1.1. Макет комп’ютерної мережі для дослідження