Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи та засоби оцінки надійності комп'ютерної мережі

(тема)

Виконав:

студент II курсу, групи КСМзм-21-1

Ткаченко В.М.
(прізвище, ініціали)

Спеціальність

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Комп’ютерні системи та мережі
(повна назва освітньої програми)

Керівник: проф. Кучук Г.А.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп'ютерні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Ткаченко Вікторії Миколаївні
(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби оцінки надійності комп'ютерної мережі

затверджена наказом по університету від " 24 " жовтня 2022 р. № 178 Стз

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня 2022 р.

3. Вхідні дані до роботи Методи резервування
Надійність, комп'ютерні мережі
Cisco
сервер
агрегація каналів передачі даних

4. Перелік питань, що потрібно опрацювати у роботі
1.Аналіз існуючих методів та технологій резервування та агрегації
2. Аналіз та вибір оптимальних методів та технологій резервування та агрегації даних каналів передачі даних
3. Дослідження ефективності використання протоколів агрегації тазерервування та резерервування

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 13 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд сучасної літератури та стандартів	25.10.22-30.10.22	
2	Аналіз методів та технологій резервування	30.10.22-05.11.22	
3	Аналіз методів агрегації	55.11.22-10.11.22	
4	Дослідження ефективності протоколів	10.11.22-24.11.22	
5	Моделювання комп'ютерної мережі	24.11.22-30.11.22	
6	Оформлення записки	30.11.22-12.12.22	

Дата видачі завдання 24 жовтня 2022 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Кучук Г.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 78 с., 40 рис., 1 табл., 1 дод., 36 джерел.

КОМП’ЮТЕРНА МЕРЕЖА, РЕЗЕРВУВАННЯ, АГРЕГАЦІЯ, ПРОТОКОЛ, МЕТОД.

Метою кваліфікаційної роботи є дослідження методів та засобів резервування та агрегації каналів комп’ютерних мереж для забезпечення надійності функціонування.

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.

ABSTRACT

Master’s thesis: 78 pages, 40 figures, 1 tables, 1 appendices, 36 sources.

COMPUTER NETWORK, RESERVATION, AGGREGATION, PROTOCOL, METHOD.

The major goal of this thesis is research of methods and means of reserving and aggregating computer network channels to ensure operational reliability.

In order to 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.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

STP – Spanning Tree Protocol

RSTP – Rapid spanning tree protocol

PVST – Per VLAN Spanning Tree

Round Robin – алгоритм планування процесів або комутації пакетів даних у мережі

Least Connections – алгоритм найменших підключень веде запис активних підключень до сервера та пересилає нове підключення до сервера з найменшою кількістю активних підключень

ВСТУП

У зв’язку з зростанням кількості мережевих пристроїв, які використовують глобальну мережу для обміну інформацією, зростає необхідність у розширенні 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 підштовхують 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. 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 науковоприкладних публікацій, 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 надійності 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.

1 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ТЕХНОЛОГІЙ РЕЗЕРВУВАННЯ ТА АГРЕГАЦІЇ

1.1 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.

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 рисунку 1.1 [1].

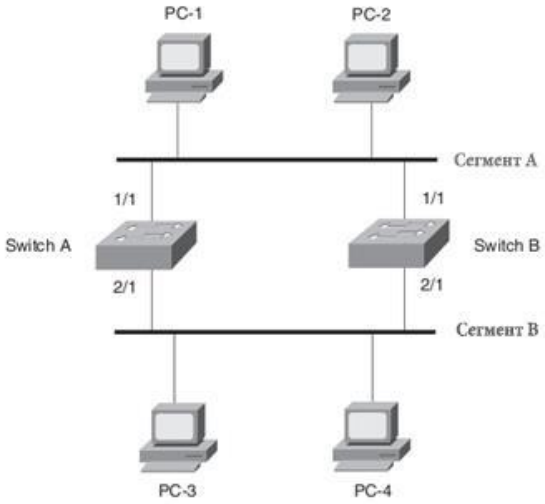


Рисунок 1.1 – Приклад сегменту мережі з виникненням логічних петель

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 рисунок 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.

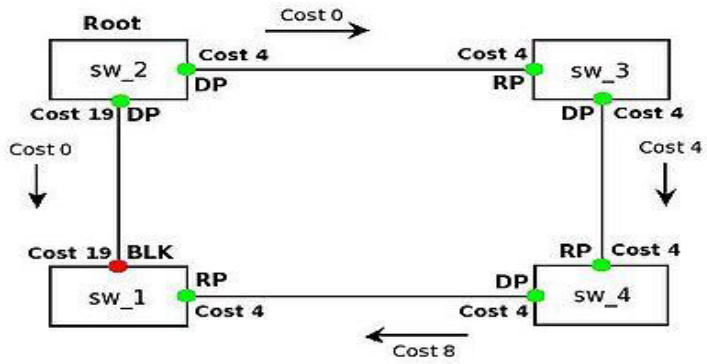


Рисунок 1.2 – Реалізація протоколу STP в мережі Ethernet

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 (рисунок 1.3). Він дозволяє пропустити стадії класичного навчання портів, які присутні у протоколі STP, та одразу перейти до стану передачі інформації [5].

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.

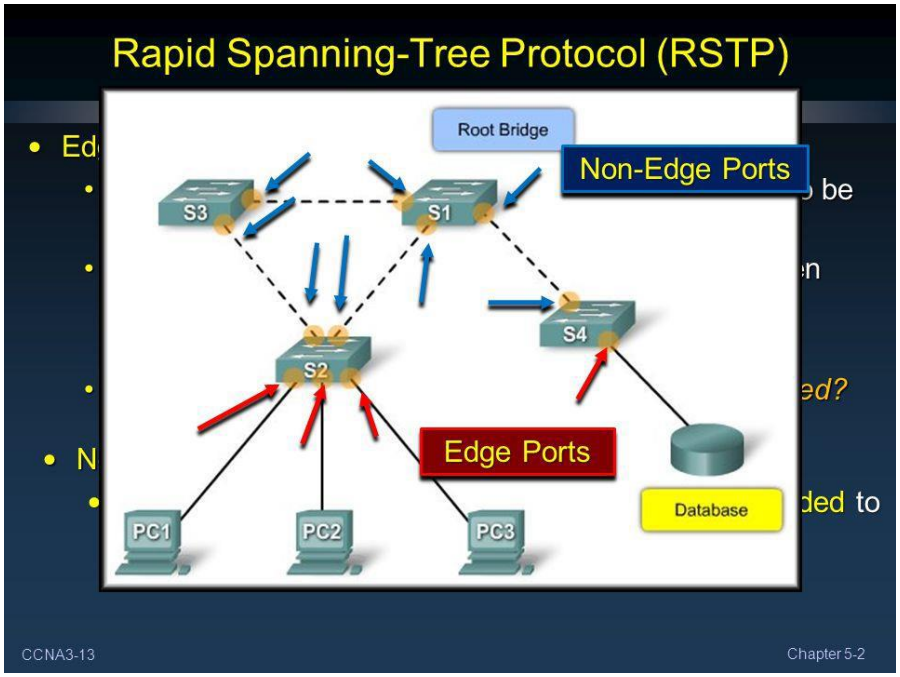


Рисунок 1.3 – Реалізація класифікації портів у протоколі RSTP

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 (рисунок 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 портвідправник 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.

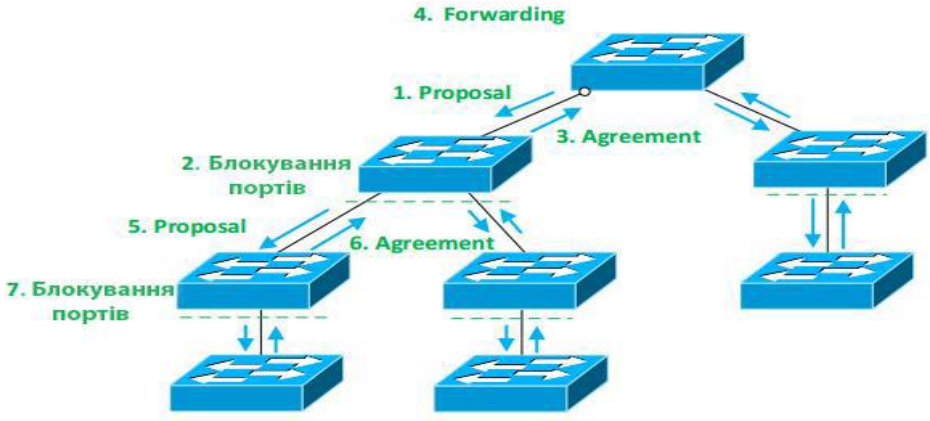


Рисунок 1.4 – Принцип роботи функцій Proposal/Agreement

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. 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.

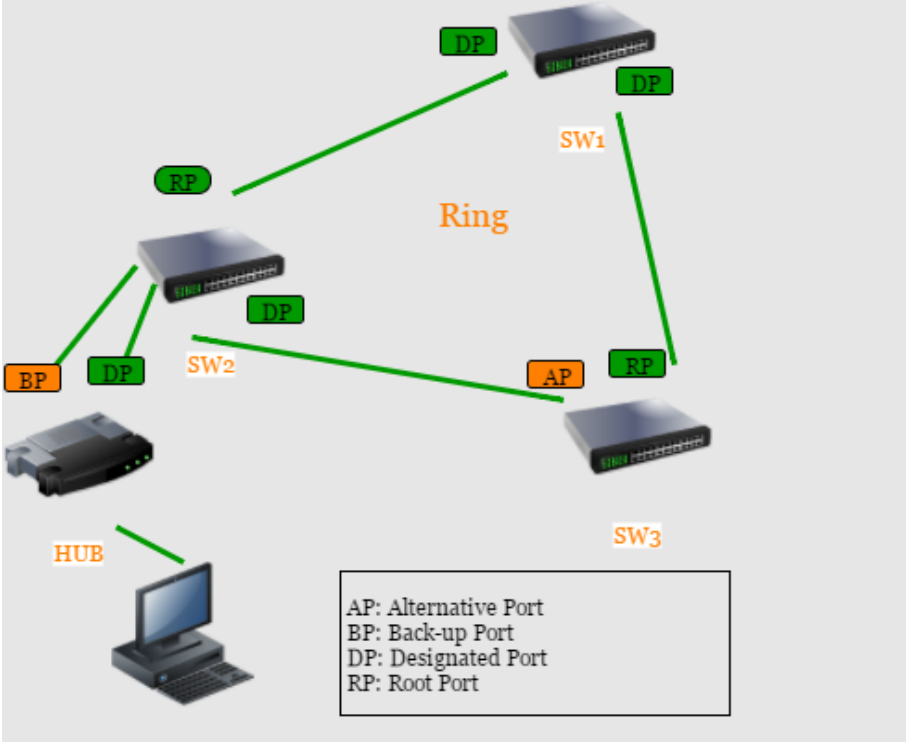


Рисунок 1.5 – Використання Backup та Alternative портів протоколом RSTP

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].

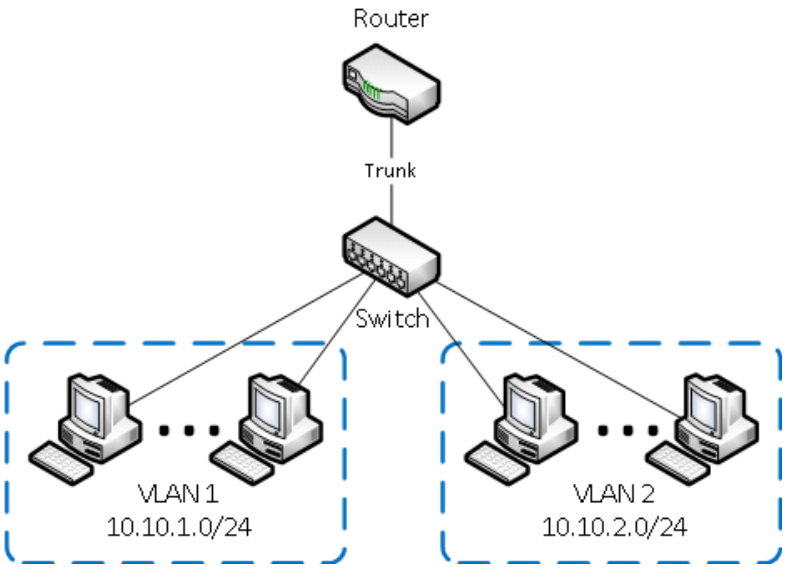


Рисунок 1.6 – Побудова мережі за допомогою VLAN

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 (рисунок 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].

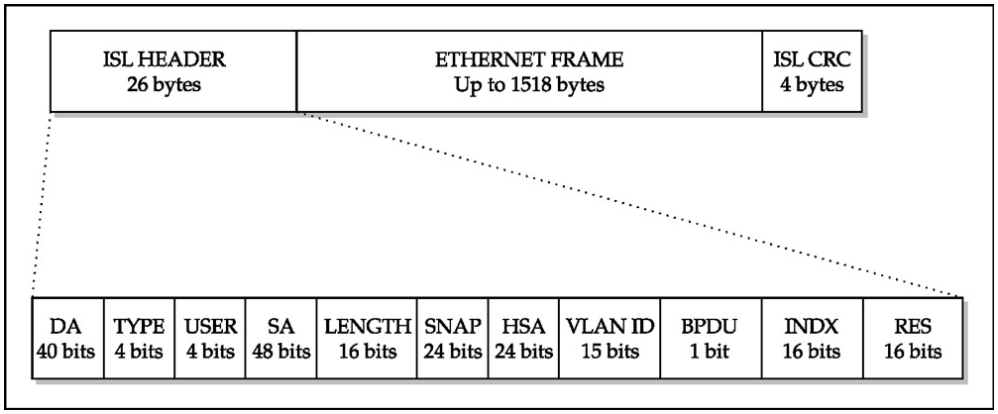


Рисунок 1.7 – Структура пакету даних з використанням ISL

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 рисунок 1.8.

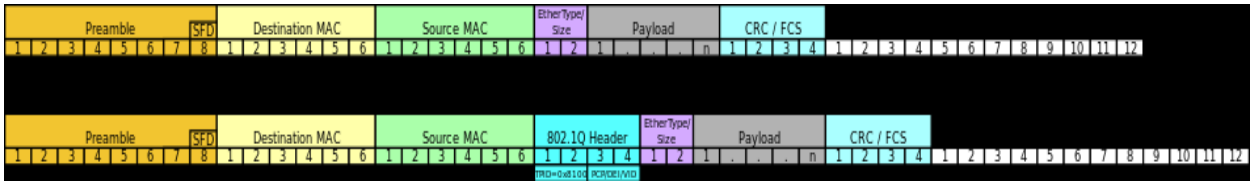


Рисунок 1.8 – Структура кадру даних з додаванням поля 802.1Q

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 розширенями 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 (рисунок 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.

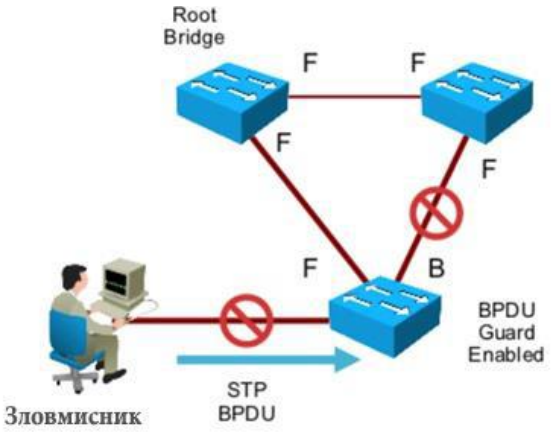


Рисунок 1.9 – Приклад атаки зловмисника з використанням вразливостей BPDU

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 рисунку 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.

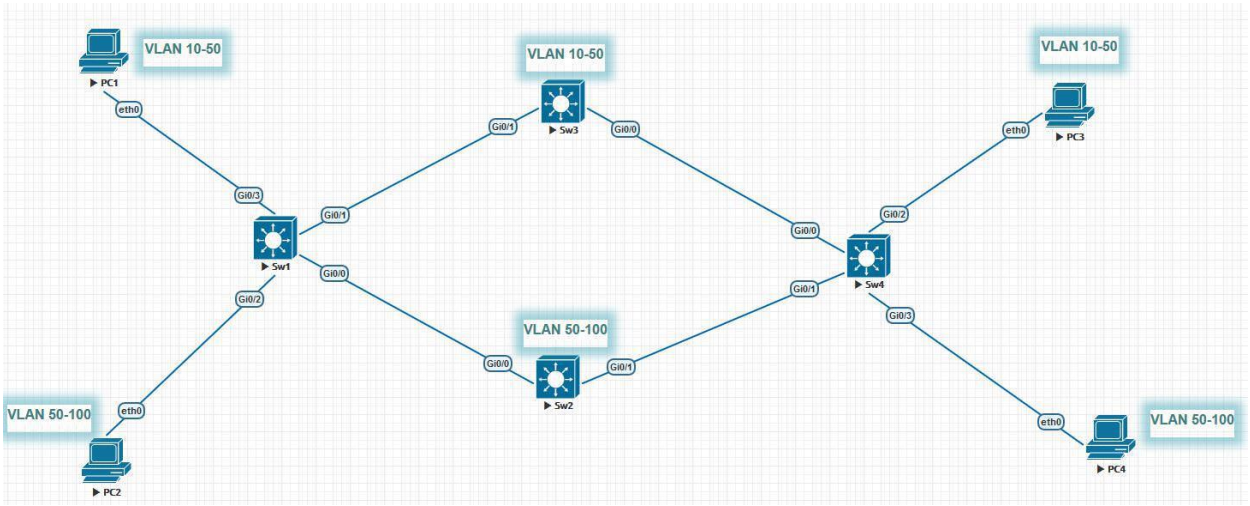


Рисунок 1.10 – Комп’ютерна мережа з використанням технології VLAN

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 рисунку 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 рисунку 1.11.

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).

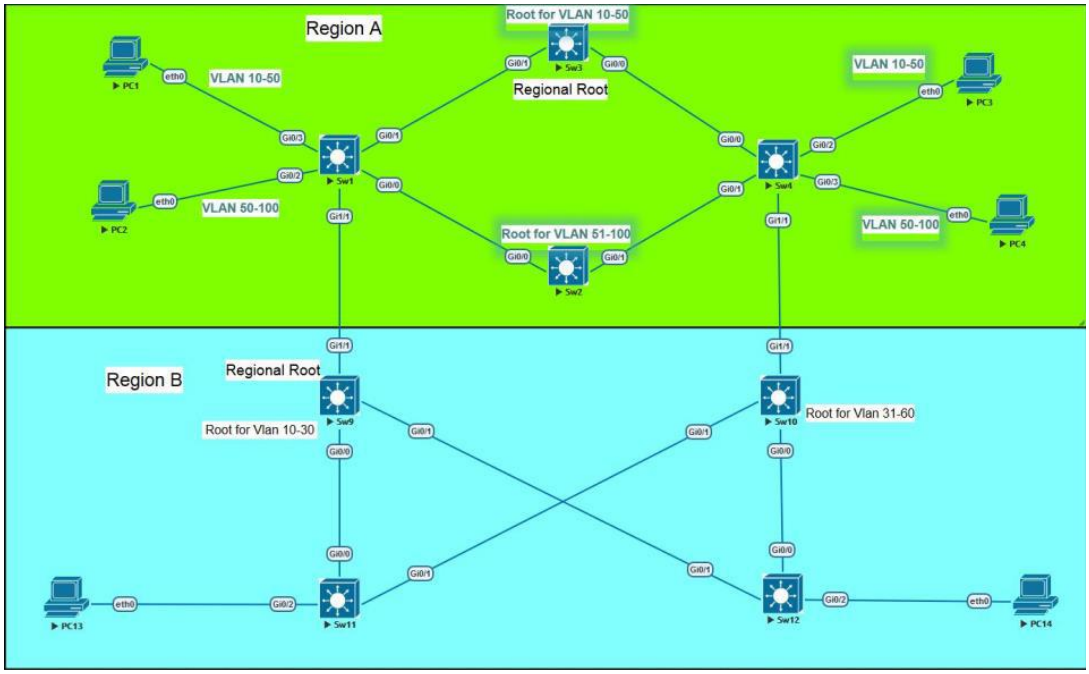


Рисунок 1.11 – Реалізація протоколу MSTP з використанням двох регіонів

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 B 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.

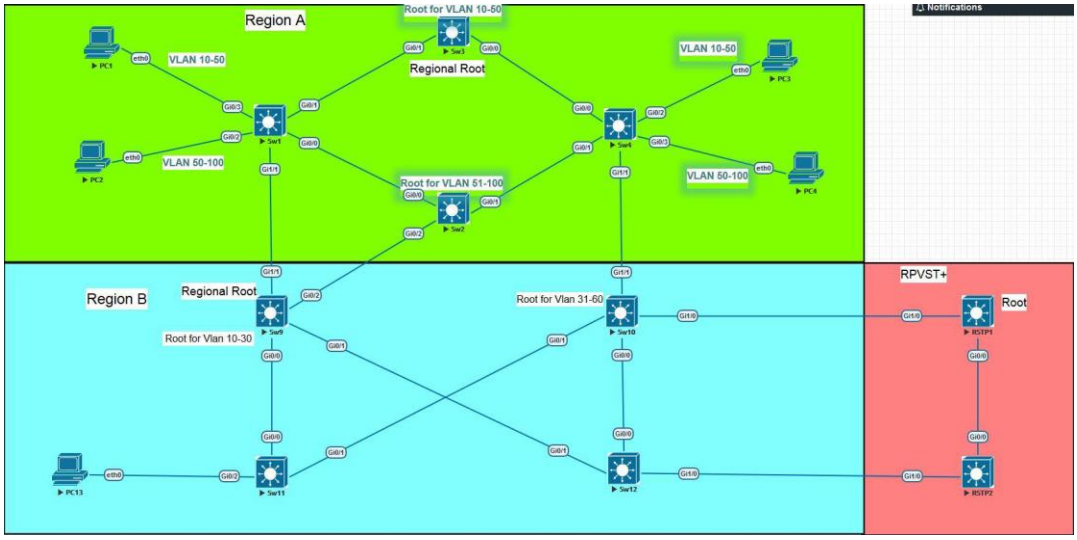


Рисунок 1.12 – Взаємодія мережі MSTP з протоколом RPVST+

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.

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. 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.

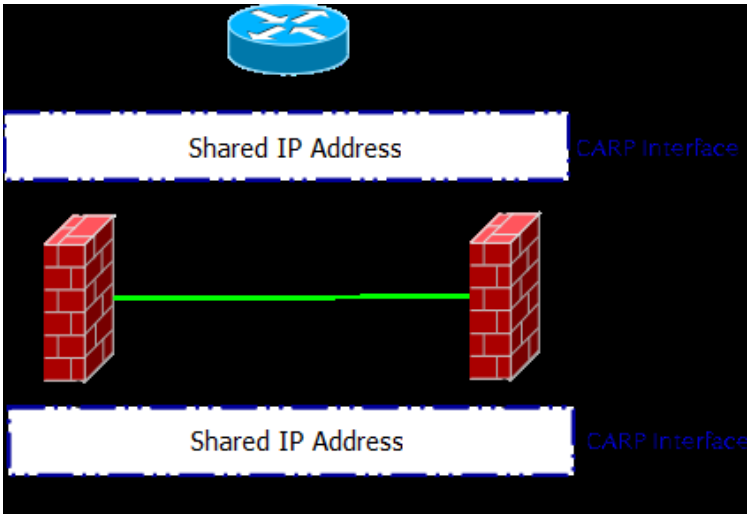


Рисунок 1.13 – Приклад реалізації протоколу CARP для резервування брандмаузерів

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 (рисунок 1.14).

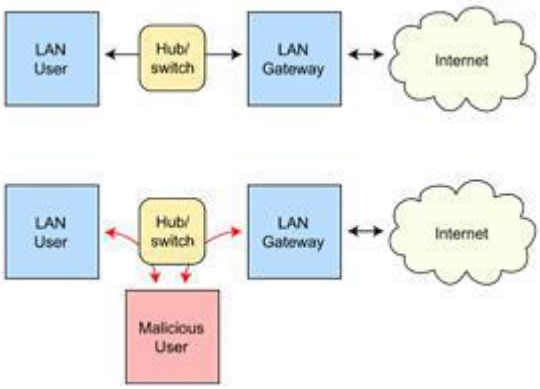


Рисунок 1.14 – Приклад атаки на мережу за допомогою вразливості протоколу ARP

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 (рисунок 1.15). Згідно термінології Cisco, група об'єднаних маршрутизаторів, які очікують, називаються групою резервування (Standby group).

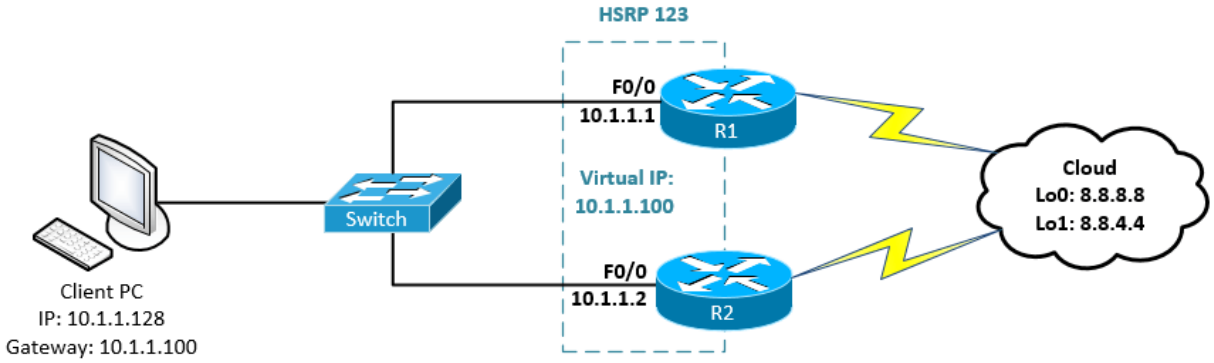


Рисунок 1.15 – Використання протоколу HSRP

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 helloповідомлення. 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.

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 ARPпакетів на запити до віртуального маршрутизатору.

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.

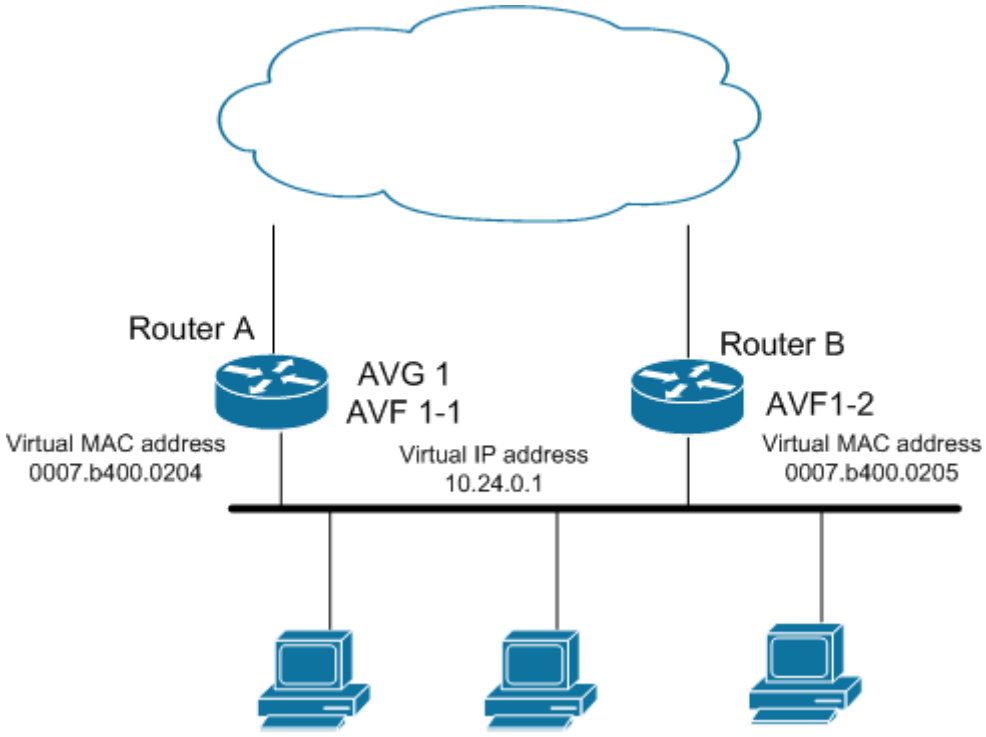


Рисунок 1.16 – Створення мостів передачі даних протоколом GHBP

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.

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 (рисунок 2.1).

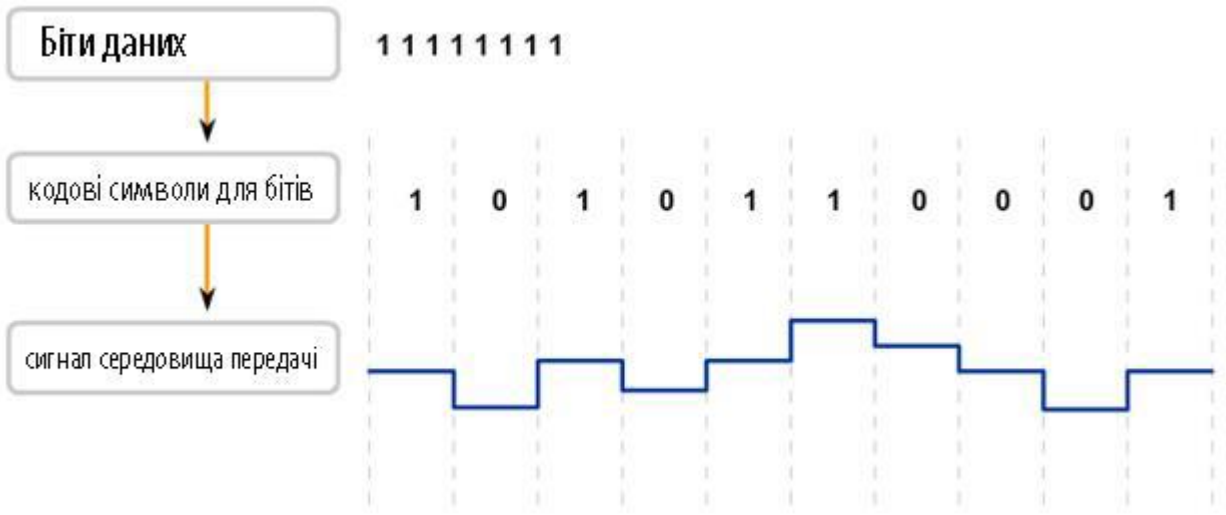


Рисунок 2.1 – Декодування сигналу на фізичному рівні

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 (рисунок 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.

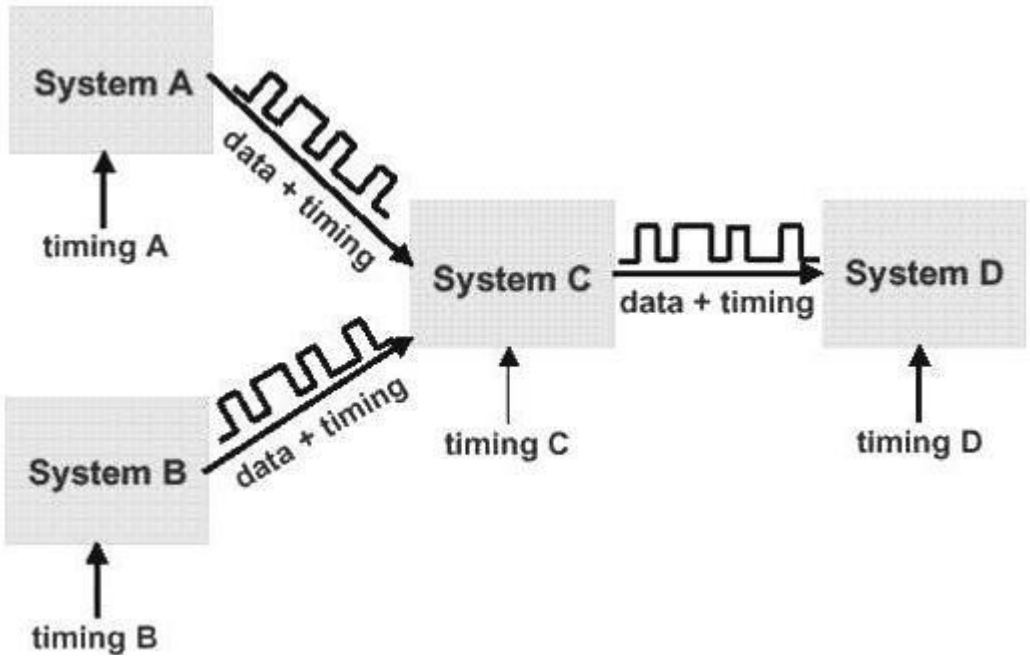


Рисунок 2.2 – Синхронізація даних в LAN-мережах

Співвідношення до одномодових волокон:

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

де $\Delta\lambda$ – ширина смуги джерела випромінення.

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

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 рисунку 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.

Рисунок 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].

Рисунок 2.4 – Графік напрацювання на відмову

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

Рисунок 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, підвищує можливість загрози атаки на мережу за допомогою номеру послідовності в протоколі TCP [25].

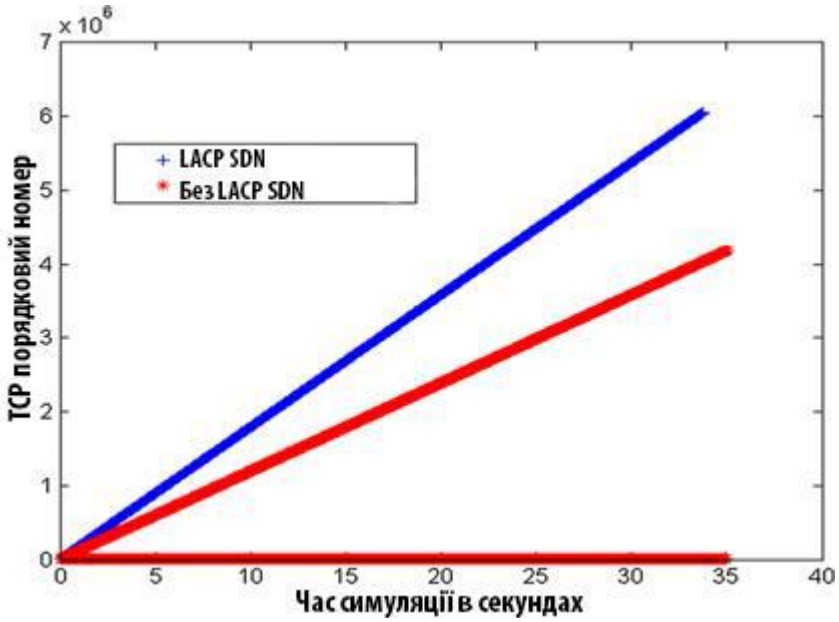


Рисунок 2.6 – Ризик успішної атаки за допомогою недоліків TCP

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.

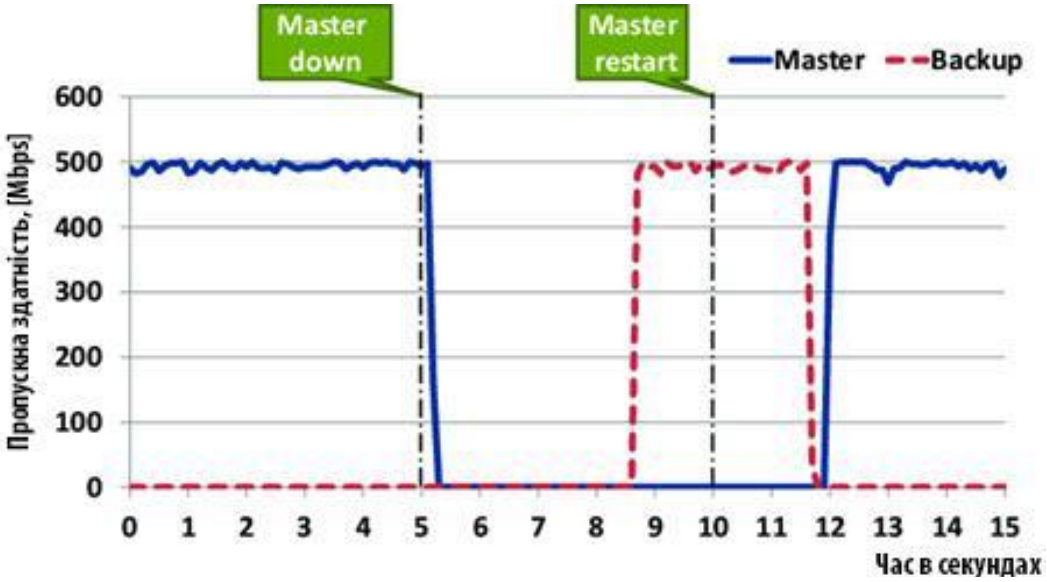


Рисунок 2.7 – Час простою VRRP при роботі з протоколом UDP

Рисунок 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.

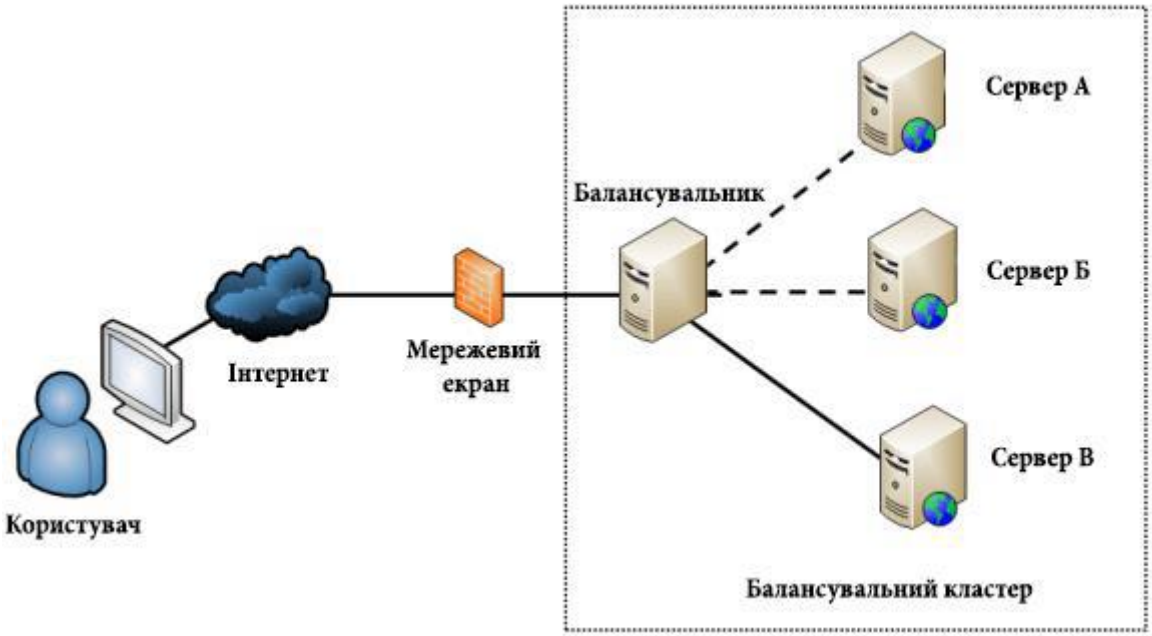


Рисунок 2.9 – Реалізація кластеризації серверів з використанням балансувальника

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.

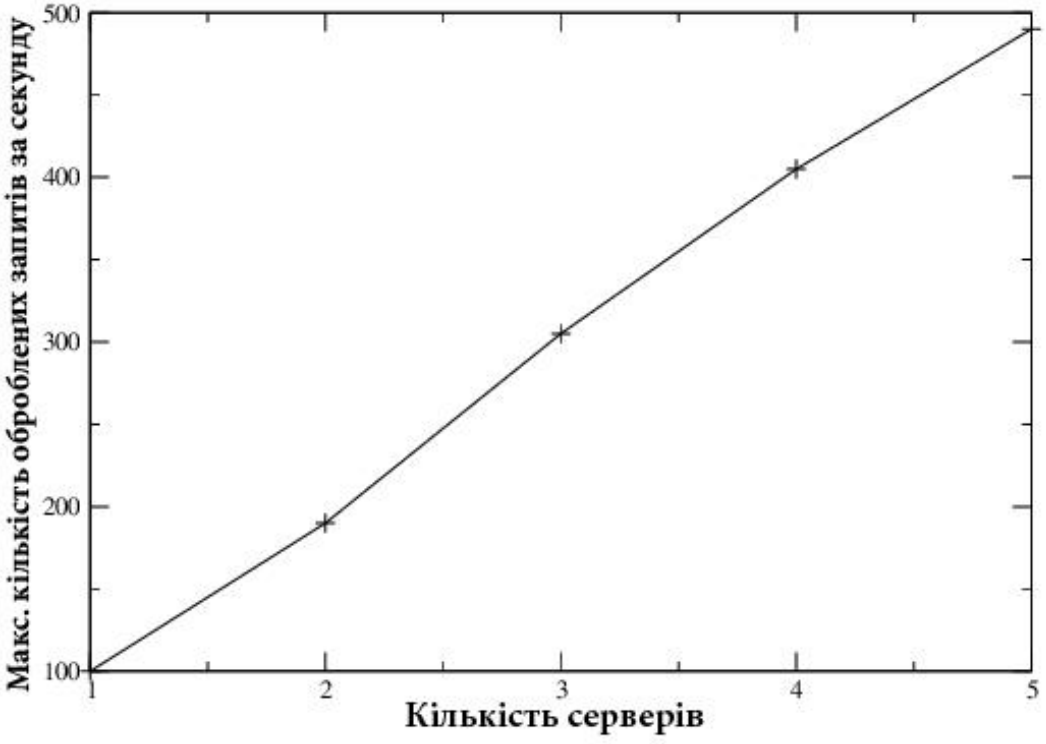


Рисунок 2.10 – Залежність реалізованої кількості запитів кластера від кількості серверів в групі

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, а й змінювати методи самого балансування.

3 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ПРОТОКОЛІВ АГРЕГАЦІЇ ТА РЕЗЕРВУВАННЯ

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 рисунку 3.1:

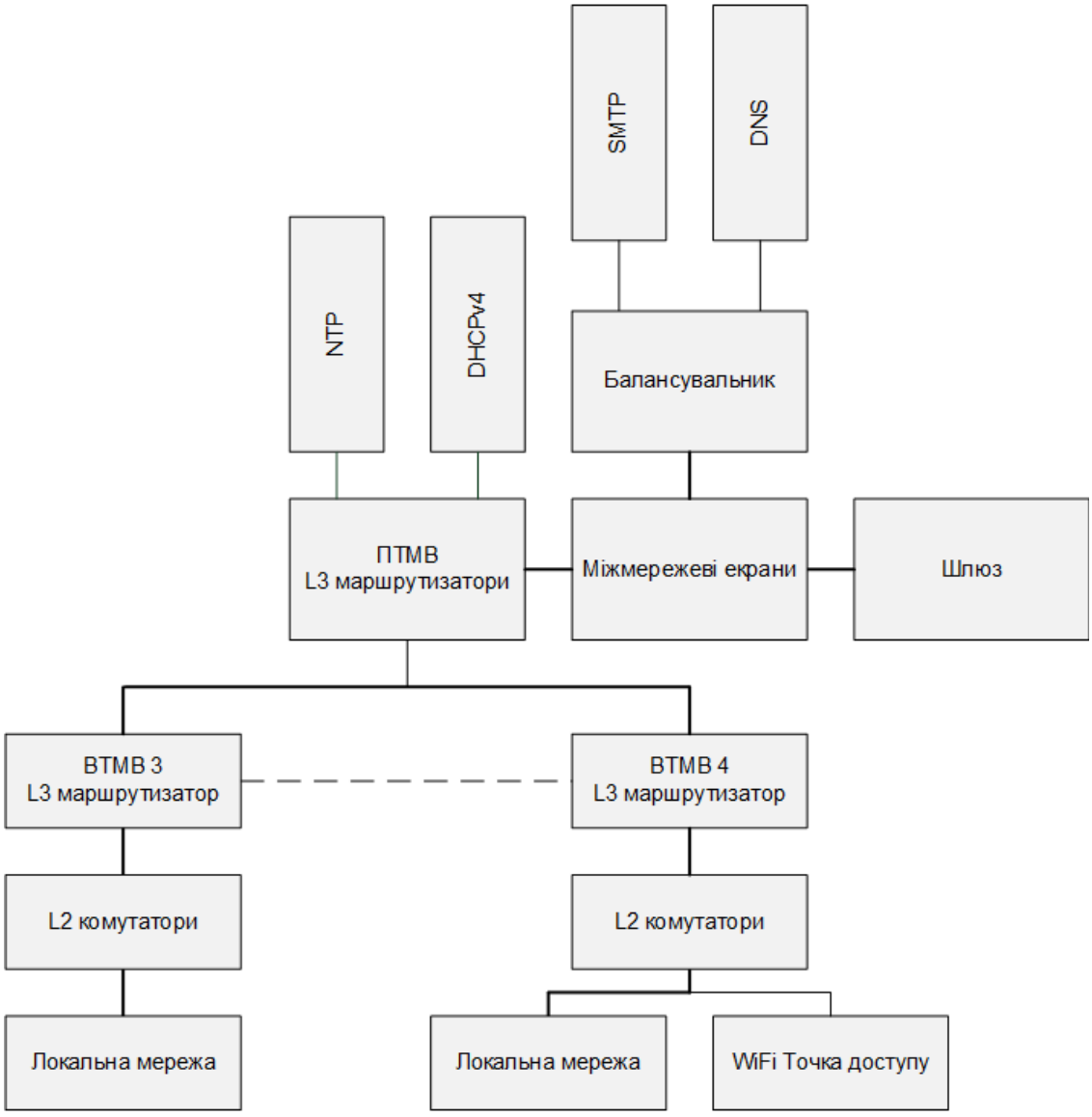


Рисунок 3.1 – Структурна схема модельованої мережі

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 (рисунок 3.2) дозволяє здійснювати передачу даних багатьом вузлам мережі, що неможливо реалізувати у топології шини, де дані передаються згідно визначеної черги.

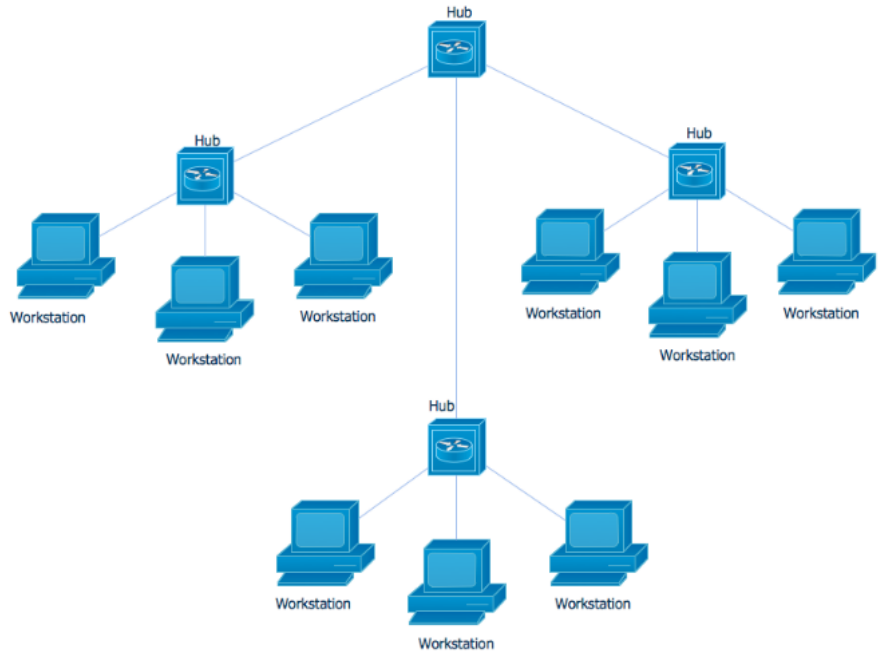


Рисунок 3.2 – Топологія “розширена зірка”

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.

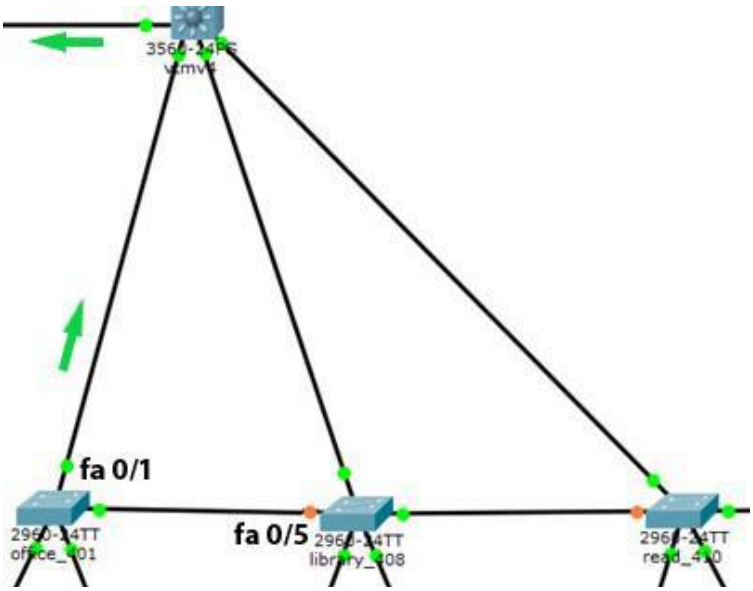


Рисунок 3.3 – Робочий стан мережі до початку дослідження

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.

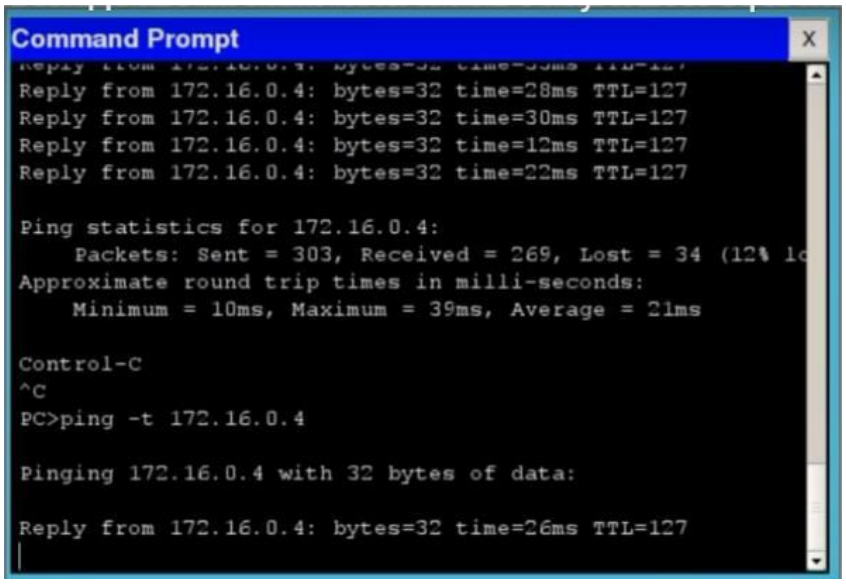


Рисунок 3.4 – Успішне встановлення з'єднання між пристроями

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 (рисунок 3.3), і спостерігаємо за виконанням команди ping з локальної мережі комутатора (рисунок 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 рисунку 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.

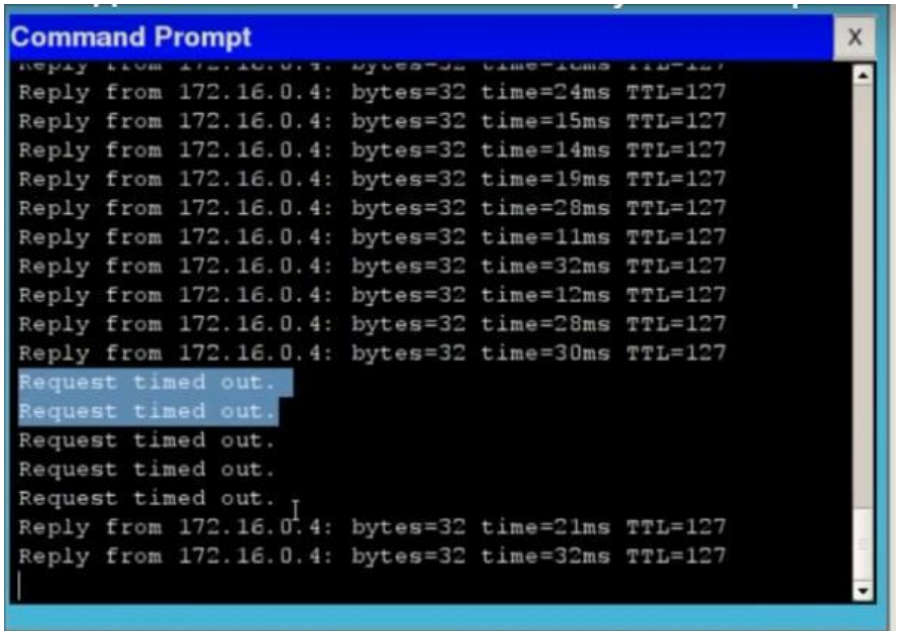


Рисунок 3.5 – Втрата пакетів протоколом STP під час перебудови логічного дерева

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

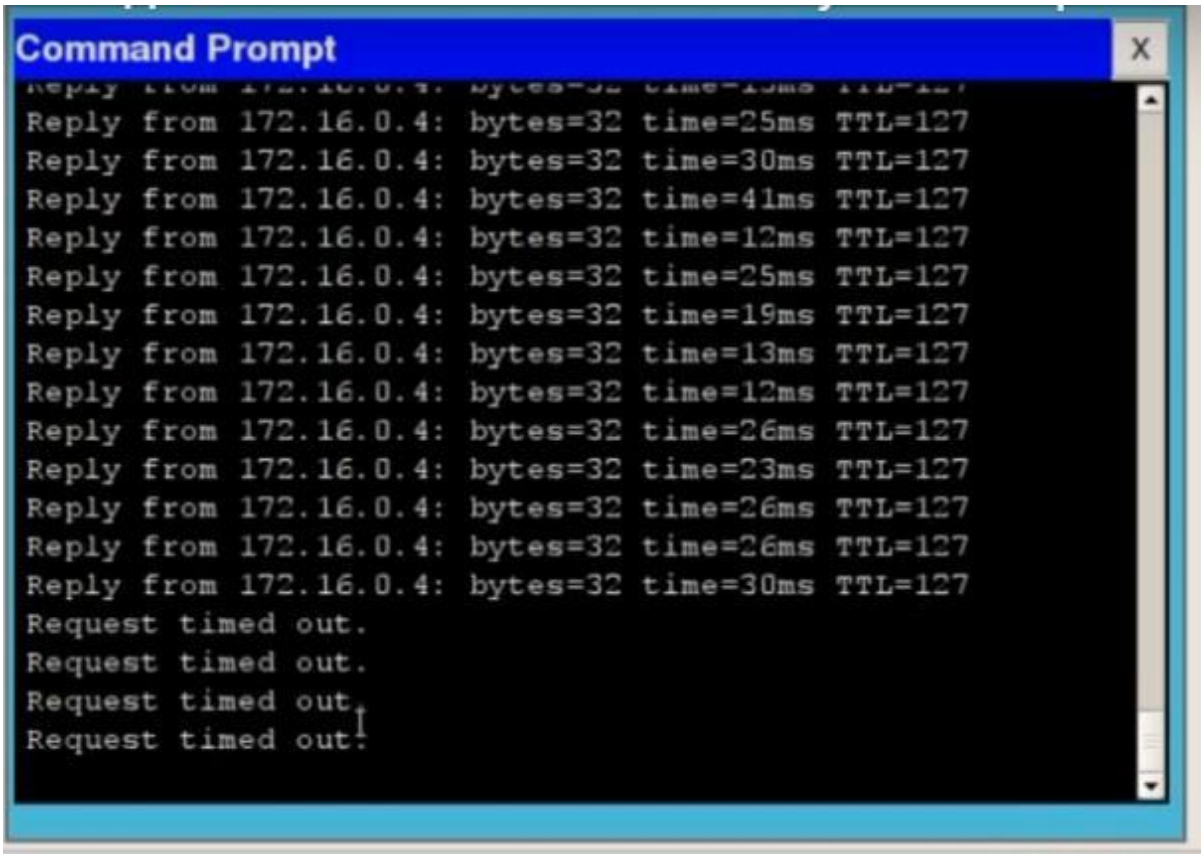


Рисунок 3.6 – Втрата пакетів під час перебудови топологічного дерева

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 рисунку 3.7.

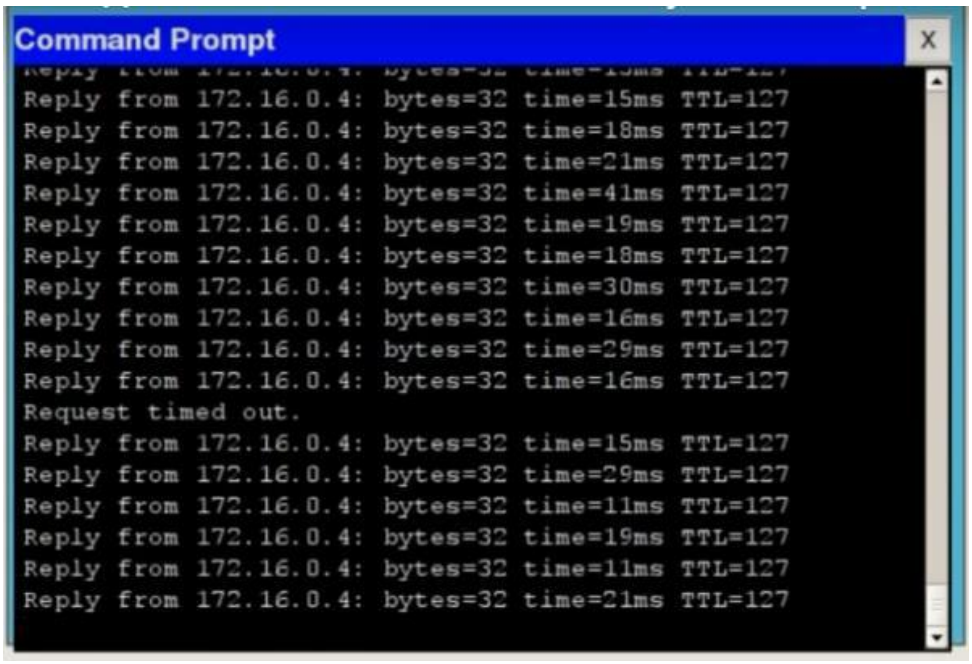


Рисунок 3.7 – Втрати пакетів протоколом RSTP

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 таблиці 3.1.

Таблиця 3.1 – 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%	155.76
RSTP	ICMP	100	98	98%	44.5

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.

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 рисунку 3.8.

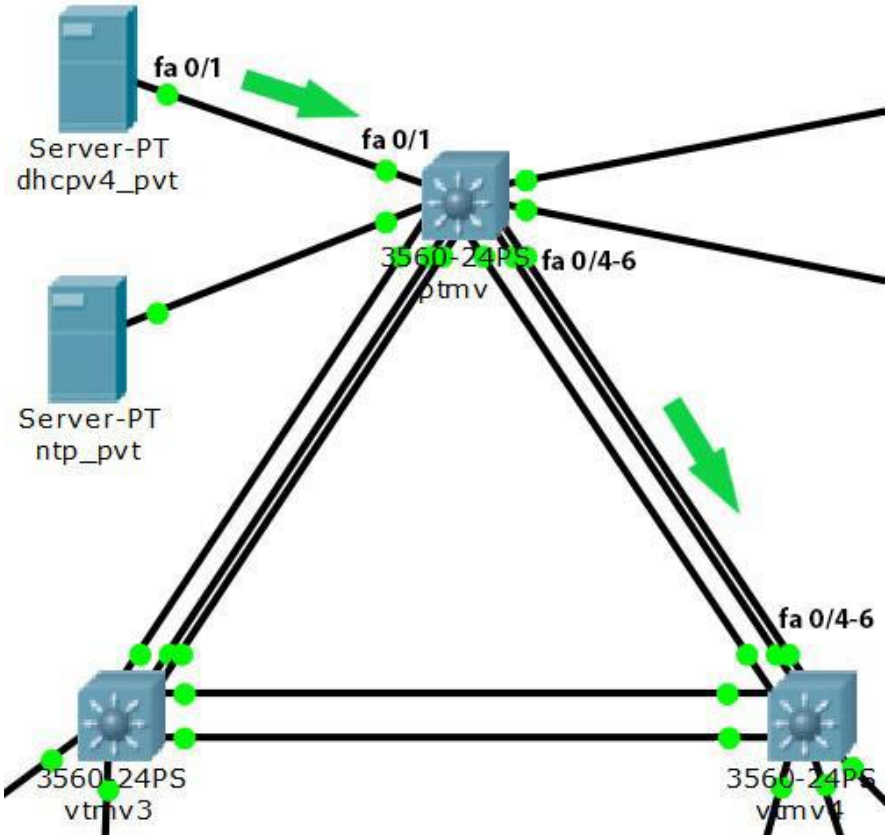


Рисунок 3.8 – Ядро модельованої мережі для дослідження

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 рисунку 3.9.

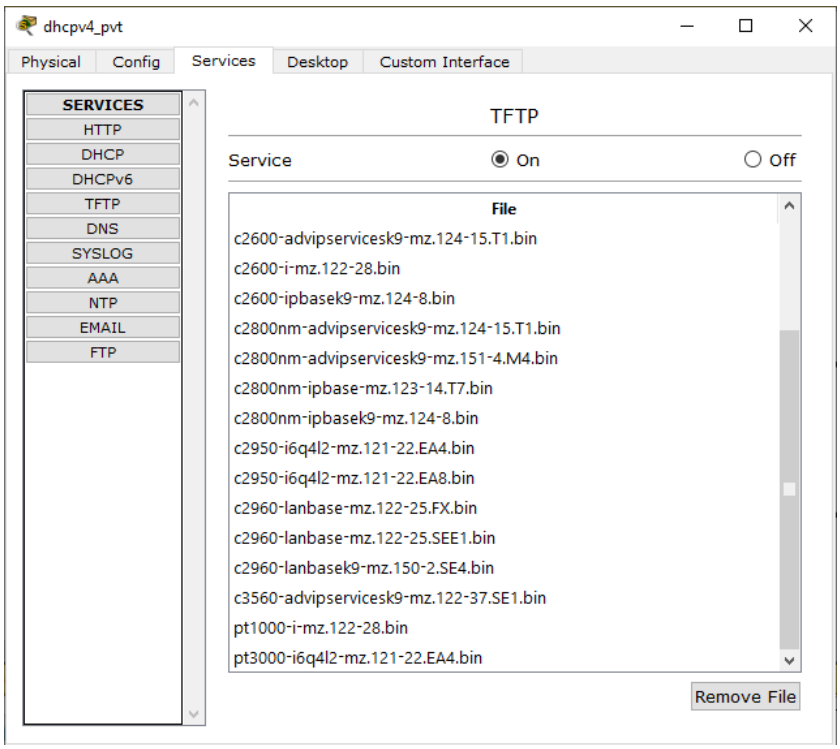


Рисунок 3.9 – Інтерфейс TFTP сервера модельованої мережі

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

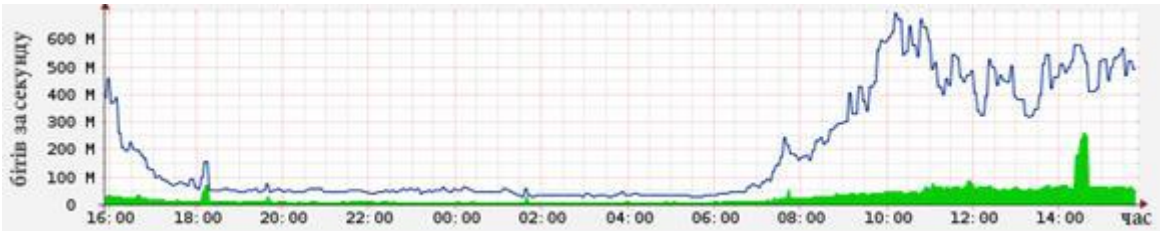
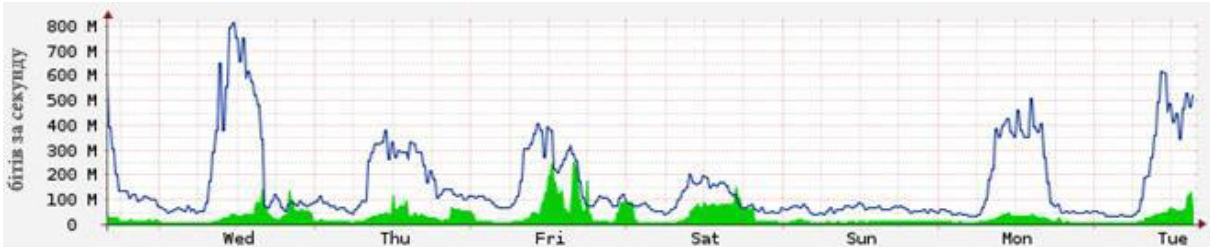


Рисунок 3.10 – Результати дослідження навантаження статично агрегованого каналу

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 рисунку 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 рисунку 3.11.



Рисунку 3.11 – Результати дослідження навантаження динамічного агрегованого каналу

3.3 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. 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 (рисунок. 3.12) [40].

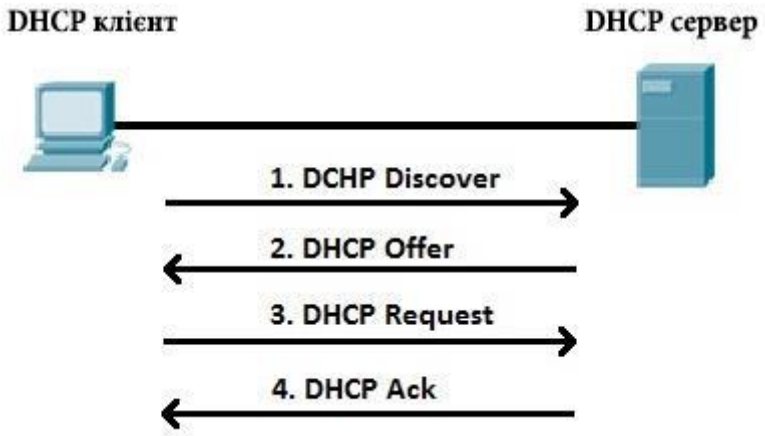


Рисунок 3.12 – Процес обміну пакетами DHCP клієнта та сервера

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. 3.13.

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%.

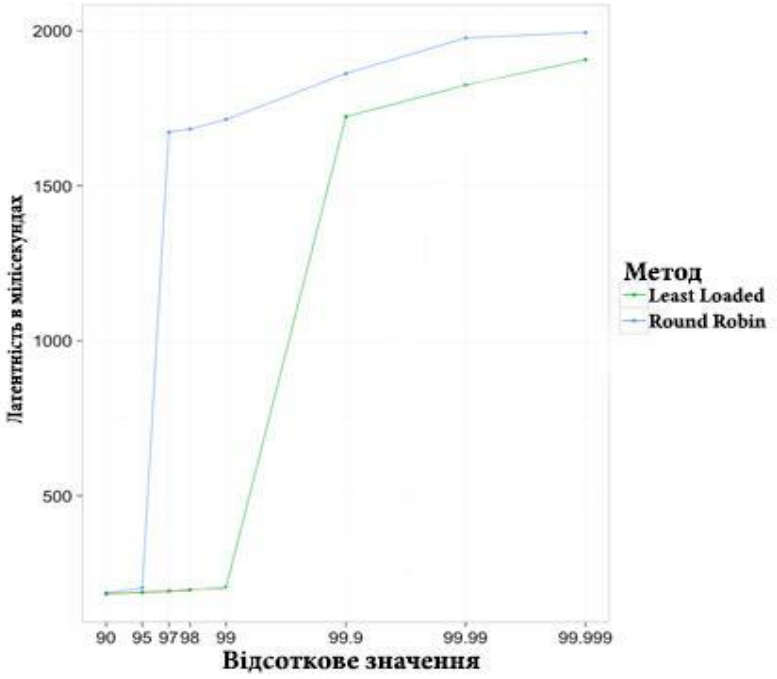


Рисунок 3.13 – Латентність запитів з використанням балансувальника

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 рисунок 3.14.

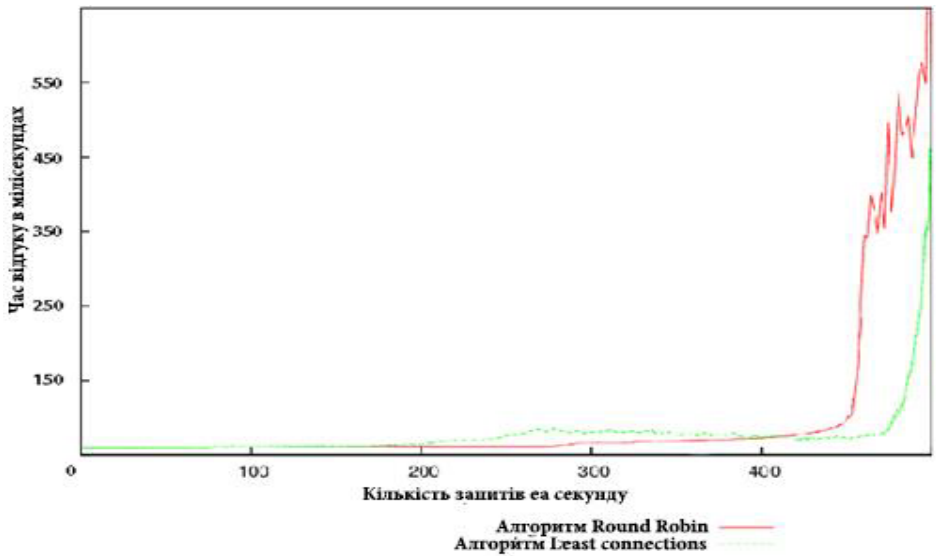


Рисунок 3.14 – Продуктивність обробки запитів сервером з використанням різних методів балансування навантаження

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.

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.

ВИСНОВКИ

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. 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.

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.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

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.

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.

11. Akan O.B., I.F. Akyildiz. ATL: an adaptive transport layer suite for nextgeneration 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 computernetwork (дата звернення: 08.10.2019).

14. Ткаченко В.М., Аналіз оцінки надійності комп’ютерних мереж / Ткаченко В.М., Крюкова І.В., Ляшенко О.С. // Проблеми інформатизації :

десята міжнародна науково-технічна конференція. ЧДТУ, ВА ЗС АР, УТіГН, НТУ “ХПІ”, ХНУРЕ, "ПД ПКНДІ АП", 2022. Т.2. С 114.

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

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/.

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-reach40-.html.

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

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_Resili ence_Packet_Ring_protocol_VRPR_in_Datacenter_Network.

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

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/.

31. Load balancer groups. 2013. URL: https://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0/com.ibm.dp.doc/lbg_loadb alancergroup.html.

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.

33. Rouse M. What is star network?. 2017. URL: https://searchnetworking.techtarget.com/definition/star-network..

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.

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