

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Навчально-науковий Інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«До захисту допущено»

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

«__» _____ 20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

**на тему: «Протоколи забезпечення відмовостійкості в мережах електронних
комунікацій»**

Виконав:

студент IV курсу, групи ТС-21

Кононенко Олег Русланович _____

Керівник:

Доцент, кандидат технічних наук,

Григоренко Олена Григорівна _____

Рецензент:

Доцент, кандидат технічних наук,

Репа Федір Михайлович _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.

Студент _____

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

«___» _____ 20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Кононенко Олегу Руслановичу

1. Тема роботи «Протоколи забезпечення відмовостійкості в мережах електронних комунікацій», керівник роботи Григоренко Олена Григорівна, доцент, кандидат технічних наук, затверджені наказом по університету від «26» травня 2026 р. № 1912 - С

2. Термін подання студентом роботи 10 червня 2026 р.

3. Вихідні дані до роботи:

4. Зміст роботи: обґрунтувати актуальність теми; проаналізувати теоретичні основи відмовостійкості, показники MTBF, MTTR і коефіцієнт готовності; розглянути архітектурні принципи резервування мережевої інфраструктури та дослідити протоколи STP/RSTP/MSTP, LACP/EtherChannel, VRRP/HSRP/GLBP і BFD. Побудувати тестову топологію в середовищі GNS3, виконати експериментальну перевірку роботи протоколів у типових відмовних ситуаціях, узагальнити результати моделювання та сформулювати практичні рекомендації щодо підвищення надійності мереж електронних комунікацій.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

1) Тема, мета, об'єкт та предмет дослідження

- 2) Класифікація протоколів забезпечення відмовостійкості
 - 3) Тестова топологія GNS3 та параметри моделювання
 - 4) Дослідження Rapid-PVST/RSTP та MSTP при зміні топології
 - 5) Дослідження LACP/EtherChannel при відмові фізичного каналу
 - 6) Дослідження VRRP при відмові основного шлюзу
 - 7) Узагальнення результатів моделювання та практичні рекомендації
6. Дата видачі завдання 7 січня 2026 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз теоретичних основ відмовостійкості мереж електронних комунікацій	30.04.2026	Виконано
2	Аналіз протоколів STP/RSTP/MSTP, LACP, VRRP/HSRP/GLBP та BFD	12.05.2026	Виконано
3	Побудова тестової топології GNS3 та налаштування VLAN, trunk, LACP, VRRP, OSPF/BFD	20.05.2026	Виконано
4	Експериментальне дослідження роботи протоколів при відмовах каналів і вузлів	01.06.2026	Виконано
5	Чистовий варіант дипломної роботи та презентаційні матеріали	08.06.2026	Виконано

Студент

Олег КОНОНЕНКО

Керівник роботи

Олена ГРИГОРЕНКО

РЕФЕРАТ

Структура та обсяг роботи: Дипломна робота містить **81 сторінку основного тексту, 20 рисунків, 8 таблиць. Список використаних джерел налічує 34 найменування.**

Тема роботи: «Протоколи забезпечення відмовостійкості в мережах електронних комунікацій».

Мета роботи: аналіз протоколів забезпечення відмовостійкості в мережах електронних комунікацій та експериментальне дослідження їхньої взаємодії в середовищі GNS3 на прикладі механізмів STP/RSTP, LACP, VRRP та BFD.

Об'єкт дослідження: процеси забезпечення безперервного функціонування та резервування в мережах електронних комунікацій.

Предмет дослідження: протоколи та механізми забезпечення відмовостійкості мережевої інфраструктури, зокрема STP/RSTP/MSTP, LACP (EtherChannel), VRRP/HSRP/GLBP та BFD.

У першому розділі розглянуто теоретичні основи відмовостійкості мереж електронних комунікацій, поняття відмови та простою, показники MTBF, MTTR і коефіцієнт готовності. Також проаналізовано архітектурні принципи резервування та роль протоколів відмовостійкості в забезпеченні безперервності мережевих сервісів.

У другому розділі досліджено протоколи STP, RSTP і MSTP для запобігання петлям і резервування на каналному рівні, технології EtherChannel та LACP для агрегації фізичних каналів, протоколи резервування шлюзу VRRP, HSRP і GLBP, а також механізми швидкого виявлення відмов BFD, keepalive та timer-based failover.

У третьому розділі побудовано тестову топологію в середовищі GNS3 та виконано моделювання роботи протоколів відмовостійкості у типових аварійних ситуаціях. Досліджено поведінку Rapid-PVST/RSTP та MSTP при зміні топології мережі, роботу LACP при відмові фізичного каналу зв'язку та роботу VRRP при відмові основного шлюзу.

У результаті роботи підтверджено, що досліджені протоколи виконують різні, але взаємопов'язані функції у забезпеченні стійкості мережевої інфраструктури. STP/RSTP/MSTP забезпечують резервування шляхів без утворення петель, LACP зберігає працездатність агрегованого каналу при відмові одного з фізичних з'єднань, VRRP забезпечує автоматичне перемикання шлюзу, а BFD прискорює виявлення втрати зв'язності. Отримані результати можуть бути використані для попереднього тестування мережевих конфігурацій, навчального моделювання та обґрунтування вибору протоколів резервування в мережах електронних комунікацій.

КЛЮЧОВІ СЛОВА: відмовостійкість, мережі електронних комунікацій, STP, RSTP, LACP, EtherChannel, VRRP, BFD, GNS3, резервування, MTTR, коефіцієнт готовності.

ABSTRACT

Structure and scope of the work: The bachelor thesis contains **81 pages of main text, 20 figures, 8 tables. The bibliography includes 34 titles.**

Topic: “Fault-Tolerance Protocols in Electronic Communications Networks.”

Goal: analysis of protocols for ensuring fault tolerance in electronic communications networks and experimental study of their interaction in the GNS3 environment using the example of STP/RSTP, LACP, VRRP and BFD mechanisms.

Object of study: processes ensuring continuous operation and redundancy in electronic communications networks.

Subject of study: protocols and mechanisms ensuring fault tolerance of the network infrastructure, in particular STP/RSTP/MSTP, LACP (EtherChannel), VRRP/HSRP/GLBP, and BFD.

The first section considers the theoretical foundations of fault tolerance in electronic communications networks, the concepts of failure and downtime, MTBF, MTTR and availability factor. The architectural principles of redundancy and the role of fault tolerance protocols in ensuring the continuity of network services are also analyzed.

In the second section, the STP, RSTP, and MSTP protocols for loop prevention and redundancy at the link level, EtherChannel and LACP technologies for physical channel aggregation, VRRP, HSRP, and GLBP gateway redundancy protocols, as well as BFD, keepalive, and timer-based failover rapid failure detection mechanisms are studied.

In the third section, a test topology is built in the GNS3 environment and the operation of fault tolerance protocols in typical emergency situations is simulated. The behavior of Rapid-PVST/RSTP and MSTP when changing the network topology, the operation of LACP when the physical communication channel fails, and the operation of VRRP when the main gateway fails are studied.

As a result of the work, it is confirmed that the studied protocols perform different but interrelated functions in ensuring the stability of the network infrastructure.

STP/RSTP/MSTP provide redundancy of paths without loop formation, LACP maintains the operability of the aggregated channel in case of failure of one of the physical connections, VRRP provides automatic gateway switching, and BFD accelerates the detection of loss of connectivity. The results obtained can be used for preliminary testing of network configurations, training modeling and justification of the choice of redundancy protocols in electronic communications networks.

KEYWORDS: fault tolerance, electronic communications networks, STP, RSTP, LACP, EtherChannel, VRRP, BFD, GNS3, redundancy, MTTR, availability.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ	9
ВСТУП.....	10
1 ТЕОРЕТИЧНІ ОСНОВИ ВІДМОВОСТІЙКОСТІ МЕРЕЖ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ	12
1.1 Відмови, простої та показники надійності мережевої інфраструктури ...	12
1.2 Архітектурні принципи резервування в мережах електронних комунікацій	16
1.3 Місце протоколів відмовостійкості в забезпеченні безперервності мережевих сервісів.....	19
Висновки до розділу 1	20
2 АНАЛІЗ ПРОТОКОЛІВ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ В МЕРЕЖАХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ.....	22
2.1 Протоколи усунення петель та резервування на канальному рівні: STP, RSTP, MSTP.....	22
2.2 Протоколи агрегації фізичних каналів: EtherChannel та LACP	27
2.3 Протоколи резервування шлюзу за замовчуванням: VRRP, HSRP, GLBP30	
2.4 Механізми швидкого виявлення та обробки відмов: BFD, Keepalive, timer-based failover	35
Висновки до розділу 2	39
3 МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛІВ ВІДМОВОСТІЙКОСТІ В СЕРЕДОВИЩІ GNS3.....	41
3.1 Опис тестової топології та параметрів моделювання	41
3.2 Дослідження роботи Rapid-PVST/RSTP та MSTP при зміні топології мережі	46
3.3 Дослідження роботи LACP при відмові фізичного каналу зв'язку	59
3.4 Дослідження роботи VRRP при відмові основного шлюзу.....	66
Висновки до розділу 3	72
ВИСНОВКИ.....	74
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	77

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

1. ISPs – Internet Service Providers – інтернет-провайдери
2. MTTR – Mean Time to Repair – показник середнього часу відновлення мережі.
3. BFD – Bidirectional Forwarding Detection – Виявлення двонаправленої передачі.
4. MTBF – Mean Time Between Failures – середній час роботи до відмови.
5. SLA – Service Level Agreement – це офіційний договір (або частина договору) між постачальником послуг та клієнтом, у якому чітко прописано, якої саме якості має бути послуга, і що буде, якщо ці умови не виконані.
6. HITL – Human-in-the-loop – це архітектурний підхід у проєктуванні систем, при якому машина виконує всю рутинну роботу, але для прийняття критичного фінального рішення вимагається втручання людини.
7. NOC – Network Operations Center – мережевий операційний центр.
8. IoT – Internet of Things – інтернет речей.
9. TOE - TCP/IP Offload Engine

ВСТУП

Актуальність теми визначається зростанням залежності корпоративних, операторських та інформаційних систем від безперервного функціонування мереж електронних комунікацій. Відмова каналу, комутатора, маршрутизатора або шлюзу може призвести до втрати зв'язності, зниження якості обслуговування та збільшення часу відновлення. Тому під час проєктування мереж важливо враховувати не лише продуктивність, а й здатність інфраструктури зберігати працездатність у разі часткових відмов.

Забезпечення відмовостійкості сучасних мереж є складною задачею, оскільки різні типи відмов потребують застосування різних механізмів резервування. Протоколи Spanning Tree запобігають виникненню петель у надлишкових канальних топологіях, механізми агрегації каналів забезпечують резервування фізичних з'єднань, протоколи резервування шлюзу підтримують доступність маршруту за замовчуванням, а механізми швидкого виявлення відмов скорочують час реакції мережі на аварійні події. Використання лише одного з цих механізмів не забезпечує повної стійкості мережі до відмов.

У зв'язку з цим виникає необхідність аналізу особливостей застосування протоколів відмовостійкості та перевірки їхньої роботи в умовах типових аварійних ситуацій із використанням засобів мережевого моделювання. Тому тема дипломної роботи є актуальною.

Метою роботи є аналіз протоколів забезпечення відмовостійкості в мережах електронних комунікацій та експериментальне дослідження їхньої взаємодії в середовищі GNS3 на прикладі механізмів STP/RSTP, LACP, VRRP та BFD.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Проаналізувати теоретичні основи відмовостійкості, основні поняття відмови, простою, MTBF, MTTR і коефіцієнта доступності.
2. Розглянути архітектурні принципи побудови резервованої телекомунікаційної інфраструктури.
3. Проаналізувати роботу STP/RSTP/MSTP, LACP/EtherChannel, VRRP/HSRP/GLBP, BFD, keepalive та timer-based failover.
4. Побудувати тестову топологію в середовищі імітаційного моделювання GNS3.
5. Виконати експериментальну перевірку роботи протоколів STP/RSTP, LACP, VRRP та BFD за умов моделювання типових аварійних ситуацій.
6. Узагальнити результати моделювання та визначити роль досліджених протоколів у забезпеченні безперервності мережевих сервісів.

Об'єкт дослідження – процеси забезпечення безперервного функціонування та резервування в мережах електронних комунікацій.

Предмет дослідження – протоколи відмовостійкості канального та мережевого рівнів, механізми швидкого виявлення відмов і особливості їхньої взаємодії під час виникнення аварійних подій.

Таким чином, забезпечення відмовостійкості мереж електронних комунікацій потребує комплексного підходу, що поєднує архітектурне резервування, використання спеціалізованих протоколів різних рівнів мережевої моделі та механізмів швидкого виявлення аварійних ситуацій. Аналіз особливостей роботи таких механізмів і перевірка їхньої поведінки в умовах типових відмов дають змогу краще зрозуміти їхні переваги, обмеження та доцільність застосування під час проєктування сучасних мережевих інфраструктур.

1 ТЕОРЕТИЧНІ ОСНОВИ ВІДМОВСТІЙКОСТІ МЕРЕЖ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

1.1 Відмови, простої та показники надійності мережевої інфраструктури

Безперервність роботи мереж електронних комунікацій є важливою умовою стабільного доступу до корпоративних сервісів, інформаційних систем, телефонії, систем відеоспостереження та інших мережевих служб. Навіть короткочасне порушення доступності може призвести до втрати зв'язності, зниження якості обслуговування та збільшення часу відновлення роботи обладнання. Тому аналіз відмов, простоїв і показників надійності є необхідною основою для подальшого розгляду механізмів відмовостійкості [2; 3; 4; 7].

Відповідно до ДСТУ 2860-94, надійність можна розглядати як властивість технічного об'єкта зберігати здатність виконувати потрібні функції протягом певного часу та в заданих умовах експлуатації. У міжнародній практиці також використовується поняття доступності (availability), яке характеризує здатність системи перебувати у працездатному стані в потрібний момент часу. Отже, надійність більше пов'язана з імовірністю безвідмовної роботи, а доступність – із часткою часу, протягом якого система фактично доступна для користувачів [6; 17; 21].

Під відмовою в межах цієї роботи розуміється подія, унаслідок якої мережевий елемент, канал або сервіс втрачає здатність виконувати свою функцію. Простої – це інтервал часу, протягом якого ця функція не виконується або виконується з неприйнятним рівнем якості. Для мережевої інфраструктури простій може бути спричинений як фізичною несправністю обладнання, так і помилкою конфігурації або втратою логічної зв'язності.

Основні групи причин, що призводять до відмов у телекомунікаційній інфраструктурі, узагальнено на рисунку 1.1 (на основі статистичних даних звіту ENISA «Telecom Security Incidents 2024») [1].

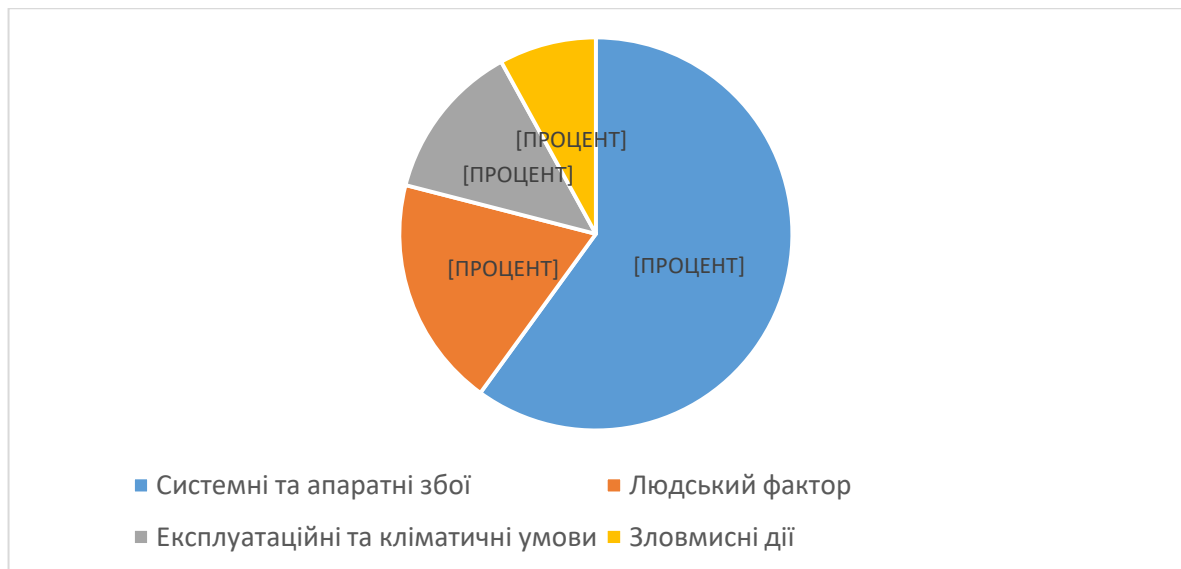


Рис. 1.1 — Аналіз телекомунікаційних інцидентів

До типових причин відмов належать системні й апаратні збої, людський фактор, експлуатаційні умови та зловмисні дії. Апаратні збої охоплюють несправності комутаторів, маршрутизаторів, портів, трансиверів, блоків живлення або програмного забезпечення мережевих пристроїв. Людський фактор пов'язаний із помилками конфігурації VLAN, списків доступу, протоколів маршрутизації чи резервування. Експлуатаційні умови включають перегрів, підвищену вологість, пил, нестабільне живлення або фізичне пошкодження кабельної інфраструктури. Зловмисні дії можуть проявлятися у вигляді DDoS-атак, несанкціонованого доступу або спроб впливу на службовий трафік.

Для кількісного оцінювання експлуатаційної надійності використовуються показники MTBF і MTTR. MTBF (Mean Time Between Failures) характеризує середній час роботи системи між відмовами [22]. У спрощеному вигляді він визначається як відношення сумарного часу працездатної роботи до кількості зафіксованих відмов:

$$MTBF = \frac{T_{\text{роб}}}{N_{\text{відм}}}, \text{ де}$$

- $T_{\text{роб}}$ – сумарний час безвідмовної роботи системи за період спостереження;
- $N_{\text{відм}}$ – кількість зафіксованих відмов.

MTTR (Mean Time to Repair) – середній час відновлення працездатності після інциденту. Він показує, скільки часу в середньому потрібно для повернення системи до нормальної роботи після відмови. У спрощеному вигляді цей показник розраховується так:

$$MTTR = \frac{T_{\text{прост}}}{N_{\text{інц}}}, \text{ де}$$

- $T_{\text{прост}}$ – сумарний час простою за період спостереження.
- $N_{\text{інц}}$ – кількість інцидентів.

У практичній експлуатації MTTR не зводиться лише до фізичного ремонту обладнання. Відновлення складається з кількох етапів: виявлення інциденту, діагностики причини, усунення несправності та перевірки працездатності після відновлення. Тому MTTR доцільно подати як суму цих складових:

$$MTTR \approx T_{\text{виявл}} + T_{\text{діагн}} + T_{\text{рем}} + T_{\text{тест}}, \text{ де}$$

- $T_{\text{виявл}}$ – час виявлення інциденту;
- $T_{\text{діагн}}$ – час діагностики та визначення причини;
- $T_{\text{рем}}$ – час усунення/ремонту несправності;
- $T_{\text{тест}}$ – час тестування/перевірки відновлення роботи.

Цей життєвий цикл інциденту відображено на рисунку 1.2.

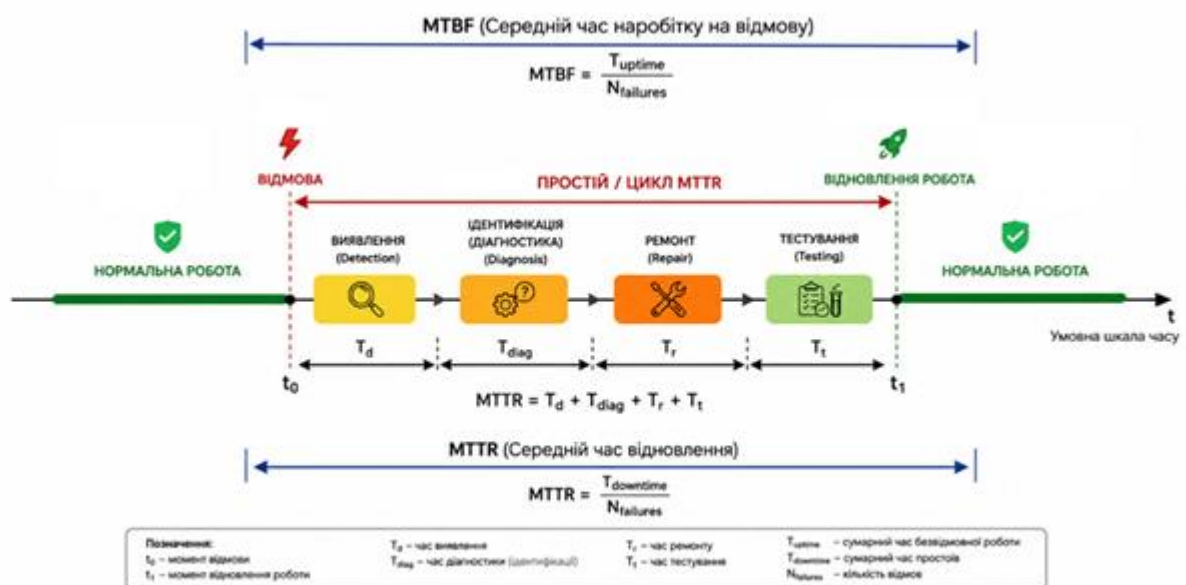


Рис. 1.2 — Життєвий цикл інциденту та етапи відновлення працездатності

Такий підхід наочно демонструє, що зменшення простою залежить не лише від надійності апаратних компонентів, а й від швидкості систем моніторингу та телеметрії.

Узагальненим показником надійності є коефіцієнт доступності A , який відображає частку часу, протягом якого система перебуває у працездатному стані:

$$A = \frac{MTBF}{MTBF + MTTR}$$

Цей показник відображає частку часу, протягом якого система перебуває у працездатному стані [23; 24]. Чим більший $MTBF$ і чим менший $MTTR$, тим вищою є доступність системи.

Для оцінювання допустимого річного часу простою зручно використовувати формулу:

$$T_{\text{прост, рік}} = (1 - A) \cdot 365 \cdot 24 \cdot 60$$

У телекомунікаційній практиці рівень доступності часто описують через «дев'ятки надійності», що визначають цільовий показник доступності сервісу. Рівні готовності сервісу наведені у таблиці 1.1.

Таблиця 1.1 — Рівні готовності сервісу за коефіцієнтом готовності

Рівень доступності сервісу	Коефіцієнт доступності (A)	Орієнтовний допустимий час простою на рік	Сфера застосування
«Одна дев'ятка»	90%	36 діб 12 год	Некритичні допоміжні системи
"Дві дев'ятки"	99%	3 доби 15 год 36 хв	Некритичні системи доступу
"Три дев'ятки"	99.9%	8 год 45 хв 36 с	Корпоративні сервіси
"Чотири дев'ятки"	99.99%	52 хв 34 с	Критична інфраструктура підприємств
"П'ять дев'яток"	99.999%	5 хв 15 с	Телекомунікаційне ядро

Таким чином, забезпечення відмовостійкості полягає не лише у збільшенні часу роботи обладнання між відмовами ($MTBF$), а й у скороченні часу виявлення, діагностики та усунення інцидентів ($MTTR$). Сучасна мережева архітектура

повинна поєднувати багаторівневе резервування каналів і засобів керування, архітектурні принципи якого детально розглядаються в наступному підпункті.

1.2 Архітектурні принципи резервування в мережах електронних комунікацій

Резервування є одним із ключових способів зменшення наслідків відмов у мережах електронних комунікацій. Якщо показники MTBF, MTTR і коефіцієнт доступності кількісно описують стан системи, то резервування визначає архітектурні рішення, завдяки яким мережа здатна зберігати працездатність під час часткової деградації. Йдеться не лише про дублювання окремих елементів, а про побудову комплексної структури, у якій відмова одного каналу, порту, вузла або маршрутизатора не призводить до повної втрати сервісу.

Загальний принцип резервування описується співвідношенням між робочими та надлишковими елементами:

$$N_{\text{заг}} = N_{\text{роб}} + N_{\text{рез}}, \text{ де:}$$

- $N_{\text{роб}}$ – кількість елементів, необхідних для штатної роботи;
- $N_{\text{рез}}$ – кількість резервних елементів.

Для спрощеної оцінки теоретичної доступності незалежної паралельної групи резервованих елементів використовується формула ймовірності успішної роботи:

$$A_{\text{ймов. усп.}} = 1 - \prod_{i=1}^n (1 - A_i), \text{ де:}$$

- A_i – коефіцієнт доступності i -го елемента;
- $(1 - A_i)$ – ймовірність його відмови [23; 26].

Проте, як зазначається в методологічних рекомендаціях Національного інституту стандартів і технологій США (NIST), класичні паралельні моделі ґрунтуються на припущенні абсолютної статистичної незалежності елементів. У реальних телекомунікаційних мережах досягти цього практично неможливо через наявність спільних точок відмови (common cause failures), таких як єдина кабельна каналізація, спільний розподільчий щит живлення або вразливість програмного

забезпечення одного вендора. Тому ефективне резервування повинно реалізовуватися на кількох незалежних рівнях інфраструктури [16].

На **фізичному рівні** резервування передбачає прокладання дублюючих оптоволоконних трас, використання запасних трансиверів, резервних портів та впровадження незалежних джерел безперебійного живлення (ДБЖ).

На **канальному рівні** надлишковість реалізується шляхом побудови резервних Ethernet-з'єднань між комутаторами. Згідно зі стандартом IEEE 802.1Q-2022, для запобігання утворенню комутаційних петель застосовуються алгоритми сімейства Spanning Tree (STP, RSTP, MSTP), які логічно блокують надлишкові маршрути. Водночас, для підвищення пропускної здатності та надійності без блокування ліній, стандарт IEEE 802.1AX визначає механізми агрегації каналів (наприклад, LACP), що об'єднують кілька фізичних ліній у єдиний логічний інтерфейс. Відповідно, на каналному рівні вирішуються дві паралельні задачі: динамічне усунення петель і керування об'єднаними каналами [9; 12].

На **мережевому рівні** пріоритетним є збереження доступності шлюзу за замовчуванням (First Hop Redundancy). Відповідно до актуального стандарту IETF RFC 9568, цю функцію виконує відкритий протокол VRRPv3, який динамічно призначає відповідальність за віртуальний маршрутизатор одному з активних вузлів групи. У корпоративних мережах також широко застосовуються пропрієтарні рішення Cisco: HSRP для прозорого перемикання шлюзу та GLBP для резервування з балансуванням навантаження [13; 18].

Окремим архітектурним шаром є **механізми швидкого виявлення відмов**. Сама по собі наявність резервного вузла не гарантує мінімізації часу простою мережі, якщо система не здатна миттєво зафіксувати аварію. Для прискорення перемикання використовуються апаратні індикатори стану інтерфейсів, службові keepalive-перевірки та спеціалізовані протоколи. Зокрема, специфікація IETF RFC 5880 регламентує роботу протоколу BFD (Bidirectional Forwarding Detection), який забезпечує субмілісекундне виявлення збоїв у двонаправлених шляхах пересилання даних незалежно від середовища передавання чи протоколів маршрутизації вищих рівнів [14; 15].

Спрощену логіку переходу від штатного до аварійного режиму роботи з використанням резервного вузла наведено на рисунку 1.1.



Рис. 1.1 — Принцип перемикавання трафіку на резервний шлях

У штатному режимі трафік проходить через активний елемент, тоді як резервний залишається доступним для прийняття ролі після виявлення відмови.

Таким чином, повноцінна архітектура резервування формується лише завдяки синергії механізмів різних рівнів: фізичне дублювання захищає від апаратних пошкоджень, каналні та мережеві протоколи забезпечують логічну перемаршрутизацію, а інструменти телеметрії прискорюють виявлення інцидентів. Функціональна роль кожної з цих груп протоколів у забезпеченні безперервності мережевих сервісів детальніше розглядається у наступному підпункті.

1.3 Місце протоколів відмовостійкості в забезпеченні безперервності мережевих сервісів

Протоколи відмовостійкості є ключовим інструментом реалізації багаторівневого архітектурного резервування. Їхнє основне призначення полягає не в усуненні фізичної причини аварії, а в мінімізації її впливу на користувацький трафік. Наприклад, логічний протокол не здатний відновити пошкоджений кабель або замінити несправний блок живлення, проте він забезпечує перемикання потоку даних через альтернативний канал, порт або резервний маршрутизатор. Таким чином, протоколи резервування діють як механізми збереження доступності сервісів в умовах часткової деградації інфраструктури.

З погляду забезпечення безперервності сервісів, ці протоколи доцільно класифікувати за їхнім цільовим призначенням та рівнем моделі OSI, на якому вони працюють:

- *Протоколи запобігання петлям (STP, RSTP, MSTP).* У комутованих Ethernet-мережах канального рівня (L2) вони підтримують резервні з'єднання без утворення логічних петель, які неминуче призводять до широкомовних штормів та перевантаження обладнання. Механізми сімейства Spanning Tree блокують надлишкові маршрути та динамічно розблоковують їх лише у разі відмови основного шляху [9; 12].
- *Протоколи агрегації каналів (EtherChannel, LACP).* На відміну від STP, ці технології дозволяють об'єднувати кілька фізичних ліній зв'язку в один логічний інтерфейс. Це одночасно збільшує сумарну пропускну здатність і забезпечує резервування: у разі обриву одного з кабелів трафік продовжує передаватися через активні з'єднання, що залишилися в групі.
- *Протоколи резервування шлюзу (VRRP, HSRP, GLBP).* На мережевому рівні (L3) доступність сервісів для кінцевих пристроїв залежить від стабільної роботи шлюзу за замовчуванням. Ці протоколи об'єднують кілька фізичних маршрутизаторів у єдиний віртуальний пристрій. Якщо активний вузол виходить із ладу, його роль автоматично перебирає на

себе резервний без необхідності зміни налаштувань на стороні клієнта [13; 18].

- *Механізми швидкого виявлення відмов (BFD, keepalive-перевірки).* Фізична наявність резервного маршруту не гарантує мінімізації часу простою без засобів швидкого моніторингу його стану. Службові механізми телеметрії впливають не на сам факт наявності резерву, а на швидкість його задіяння, гарантуючи виявлення недоступності сусіднього вузла із субмілісекундними затримками [14; 15].
- **Службові засоби моніторингу (SNMP, Syslog, NetFlow).** Забезпечують оцінку загального стану обладнання, аналіз пропускну здатності та фіксацію подій у системних журналах [5; 8].

Така класифікація показує, що жоден окремий протокол не забезпечує повної відмовостійкості всієї мережі. Захист інфраструктури досягається виключно завдяки синергії цих механізмів: STP захищає від петель, LACP резервує кабельні з'єднання, VRRP забезпечує роботу шлюзу, а BFD скорочує час реакції на аварію.

Водночас, класичні механізми відмовостійкості мають фундаментальну вразливість – їхня ефективність гарантується лише в межах основної смуги передавання даних (In-Band) за умови базової працездатності обладнання та наявності живлення. У випадку апаратного блокування вузла (втрати відгуку операційної системи), знеструмлення або критичного перегріву в телекомунікаційній шафі, стандартні мережеві протоколи виявляються безсилими для діагностики першопричини. Необхідність вирішення цієї проблеми формує потребу у впровадженні повністю незалежного контуру позасмугового (Out-of-Band) керування [5; 8].

Висновки до розділу 1

У першому розділі розглянуто теоретичні основи відмовостійкості мереж електронних комунікацій. Визначено, що відмова мережевого елемента або

сервісу призводить до простою, тривалість якого безпосередньо впливає на доступність мережі. Для кількісного оцінювання надійності та доступності використовуються показники MTBF, MTTR і availability. При цьому доступність системи залежить не лише від середнього часу роботи між відмовами, а й від швидкості виявлення, діагностики, усунення несправності та перевірки відновлення роботи.

Встановлено, що ефективне резервування має реалізовуватися на кількох рівнях мережевої інфраструктури. На фізичному рівні воно пов'язане з дублюванням каналів, портів, живлення та обладнання; на канальному рівні - із запобіганням петлям і резервуванням Ethernet-з'єднань; на мережевому рівні - із забезпеченням доступності шлюзу та маршрутів передавання даних. У цьому контексті протоколи STP/RSTP/MSTP, LACP, VRRP/HSRP/GLBP, BFD, keepalive-механізми та засоби моніторингу виконують різні, але взаємопов'язані функції.

Отже, жоден окремий протокол не забезпечує повної відмовостійкості мережі самостійно. Стійкість мережевої інфраструктури до відмов формується поєднанням архітектурного резервування, логічних протоколів перемикання, механізмів швидкого виявлення збоїв і засобів контролю стану обладнання. Водночас більшість класичних механізмів працює в межах основної мережевої інфраструктури, тому їх ефективність залежить від коректності налаштувань і працездатності базових каналів зв'язку. Це створює підставу для подальшого аналізу конкретних протоколів відмовостійкості, який виконується у другому розділі.

2 АНАЛІЗ ПРОТОКОЛІВ ЗАБЕЗПЕЧЕННЯ ВІДМОВСТІЙКОСТІ В МЕРЕЖАХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

2.1 Протоколи усунення петель та резервування на каналному рівні: STP, RSTP, MSTP

У комутованих Ethernet-мережах резервні фізичні з'єднання між комутаторами є необхідними для підвищення стійкості інфраструктури. Проте проста побудова кількох паралельних шляхів без додаткового керування створює небезпеку комутаційних петель. На відміну від IP-пакетів, Ethernet-кадри не мають поля TTL, яке б автоматично обмежувало їхнє “життя” в мережі. Тому в разі появи петлі широкомовні, multicast- або невідомі unicast-кадри можуть безкінечно циркулювати між комутаторами, спричиняючи широкомовний шторм, перевантаження процесора комутатора та нестабільність таблиць MAC-адрес [9; 12].

Базова логіка STP ґрунтується на виборі кореневого комутатора, або Root Bridge. Саме відносно нього інші комутатори визначають найкращі шляхи та ролі своїх портів. Root Bridge обирається за найменшим Bridge ID, який формується на основі пріоритету комутатора та його MAC-адреси. У практичних мережах адміністратор зазвичай задає пріоритет вручну, щоб кореневим став комутатор рівня ядра або агрегації, а не випадковий пристрій доступу.

Обмін службовою інформацією між комутаторами здійснюється за допомогою BPDU (Bridge Protocol Data Unit). У BPDU передаються дані про Bridge ID, вартість шляху до Root Bridge, ролі портів і стан топології. На основі цієї інформації комутатори визначають, який порт буде використовуватися як основний шлях до Root Bridge, а які порти мають залишатися активними або резервними [9; 12].

Принцип формування безпетльової логічної топології у фізично надлишковій мережі показано на рисунку 2.1.

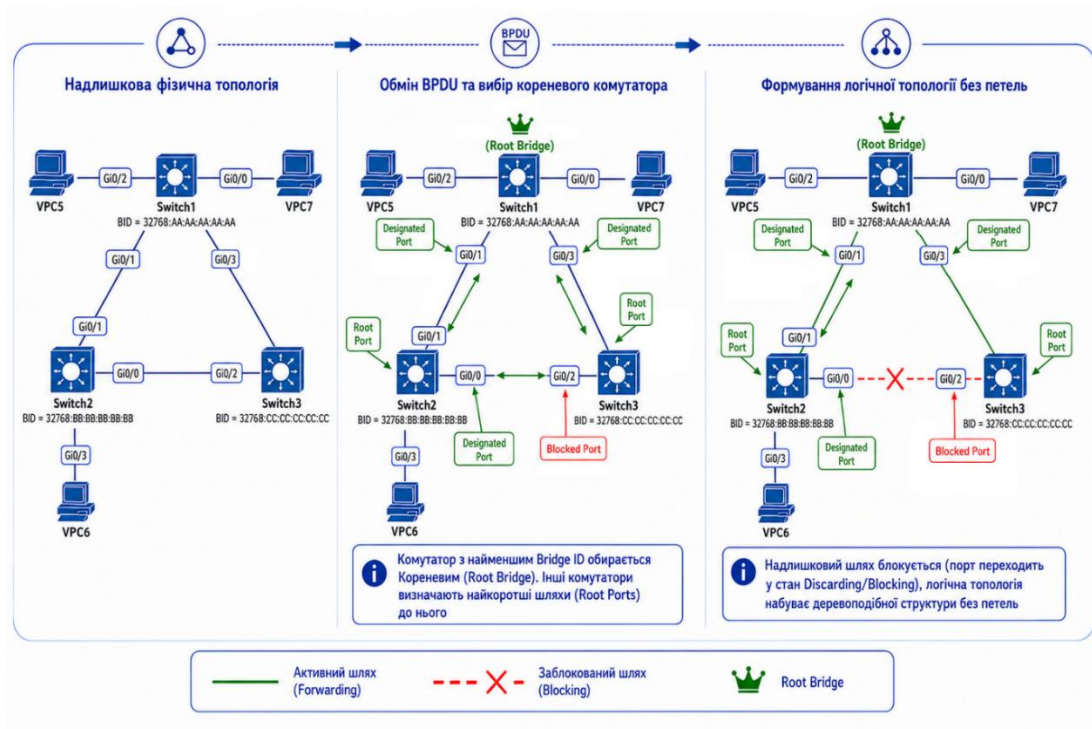


Рис. 2.1 — Принцип роботи STP у надлишковій мережі

Вартість шляху до кореневого комутатора визначається сумою вартостей окремих портів на шляху:

$$C_{root} = \sum_{i=1}^n C_i, \text{ де}$$

- C_{root} – сумарна вартість шляху до кореневого комутатора;
- C_i – вартість окремого каналу або порту;
- n – кількість ділянок шляху [25].

Порт із найменшою сумарною вартістю шляху до Root Bridge отримує роль root port. Інші порти розподіляються залежно від їхнього положення в топології: частина з них бере участь у передаванні кадрів, а частина залишається резервною для запобігання петлям. Основні ролі портів у протоколах сімейства STP наведено в таблиці 2.1.

Таблиця 2.1 — Основні ролі портів у протоколах сімейства STP

Роль порту	Протокол	Призначення
Root port	STP / RSTP / MSTP	Порт некореневого комутатора з найменшою акумульованою вартістю шляху до Root Bridge.
Designated port	STP / RSTP / MSTP	Активний порт у сегменті мережі, що ретранслює трафік у напрямку кореневого комутатора (Root Bridge).
Non-Designated	STP (802.1D)	Порт, що не отримав ролі RP або DP і переведений у стан блокування для запобігання петлям.
Alternate Port	RSTP / MSTP	Заблокований порт, що забезпечує альтернативний шлях до Root Bridge та безпосередньо резервує Root Port.
Backup Port	RSTP / MSTP	Заблокований порт, що резервує Designated Port у межах того ж колізійного домену (сегмента).

Класичний STP забезпечує побудову безпетльової топології, але має повільнішу збіжність, оскільки значною мірою спирається на таймерний механізм переходу портів між станами. Базові значення таймерів STP становлять: Hello Time – 2 с, Max Age – 20 с, Forward Delay – 15 с. Hello Time визначає періодичність надсилання BPDU, Max Age – час збереження отриманої BPDU-інформації, а Forward Delay – час перебування порту в проміжних станах Listening і Learning перед переходом у Forwarding [28].

RSTP (Rapid Spanning Tree Protocol) є прискореним розвитком STP. Його основна відмінність полягає в тому, що він використовує активне узгодження ролей портів між сусідніми комутаторами, а не лише очікування таймерів. У RSTP заблокований резервний порт може швидше перейти в стан передавання трафіку, якщо основний шлях стає недоступним. Для цього застосовуються механізми узгодження між комутаторами, зокрема обмін BPDU з інформацією про роль і стан порту. Найефективніше RSTP працює на повнодуплексних з'єднаннях типу «точка-точка», які характерні для сучасних міжкомутаторних Ethernet-інтерфейсів [9; 12; 29].

У RSTP також важливо правильно відрізнити транзитні порти від edge-портів. Edge/PortFast доцільно застосовувати на портах, до яких підключені

кінцеві пристрої, оскільки такі порти не повинні брати участь у транзитній побудові дерева. Водночас вмикати PortFast на міжкомутаторних trunk-з'єднаннях небезпечно, оскільки це може створити умови для тимчасової петлі. Для захисту access-портів доцільно застосовувати BPDU Guard: якщо на edge-порт надходить BPDU, це може свідчити про підключення стороннього комутатора або помилку в топології. Root Guard, у свою чергу, використовується для запобігання небажаному перехопленню ролі Root Bridge нижчестоящим або стороннім комутатором [30; 31].

У мережах із великою кількістю VLAN використання одного спільного дерева для всієї топології може бути неефективним. Якщо всі VLAN використовують однаковий активний шлях, частина резервних каналів залишається заблокованою і не бере участі в передаванні трафіку. З іншого боку, побудова окремого дерева для кожної VLAN дає гнучкість, але збільшує кількість логічних STP-екземплярів і навантаження на обладнання [9; 12].

MSTP (Multiple Spanning Tree Protocol) вирішує цю проблему шляхом об'єднання кількох VLAN у MST-instance (MSTI). Кожен MST-instance має власну логічну топологію, власні ролі портів і може використовувати інший активний шлях. Наприклад, одна група VLAN може передаватися через один uplink, а інша група VLAN – через інший. Завдяки цьому MSTP дозволяє поєднати резервування з більш раціональним використанням міжкомутаторних каналів.

Принцип розподілу VLAN між різними MSTP-instance показано на рисунку 2.2.

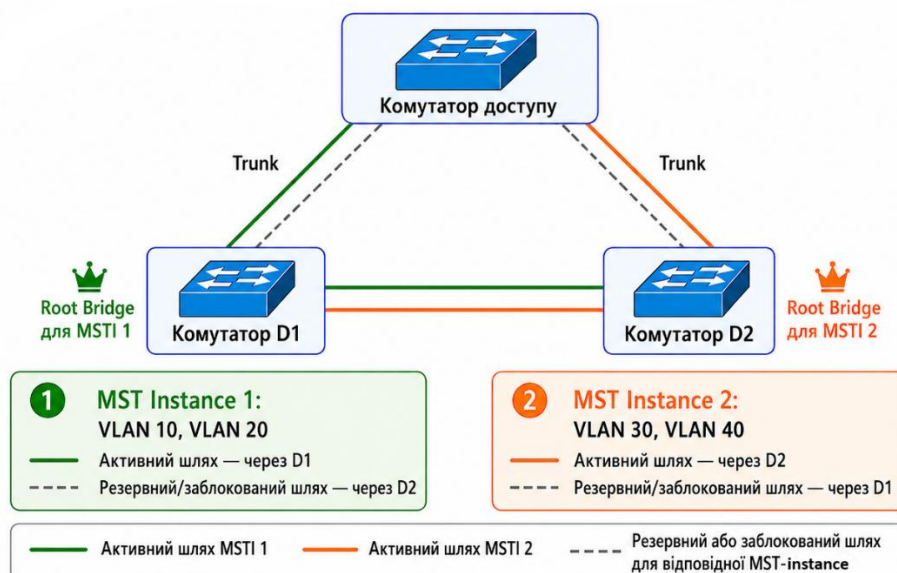


Рис. 2.2 — Принцип розподілу VLAN між MSTP-instance

Практична різниця між Rapid-PVST/RSTP і MSTP полягає у способі роботи з VLAN. Rapid-PVST/RSTP у реалізаціях Cisco зазвичай формує окреме дерево для кожної VLAN, що зручно для детального керування шляхами, але може бути менш ефективним у великих мережах. MSTP, навпаки, дозволяє об'єднати кілька VLAN в один MST-instance і зменшити кількість логічних дерев, зберігаючи можливість розподіляти різні групи VLAN між різними активними напрямками [9; 12].

З практичного погляду найчастіше змінюють не базові таймери Hello Time, Max Age або Forward Delay, а параметри, які визначають логіку побудови дерева: root bridge priority, path cost, port priority, edge/PortFast, BPDU Guard і Root Guard. Root bridge priority задає бажаний кореневий комутатор, path cost і port priority впливають на вибір активного та резервного шляху, а захисні механізми зменшують ризик помилок на access-рівні. Саме ці параметри безпосередньо впливають на передбачуваність топології без надмірного втручання в часову логіку STP [9; 12; 30; 31].

Без потреби не варто агресивно зменшувати Hello Time, Max Age або Forward Delay. Надто малі таймери можуть спричинити нестабільність STP-домену, зайві перебудови дерева або хибну реакцію на короточасні втрати

BPDU. У типовій резервованій топології кращий результат зазвичай досягається не за рахунок зменшення таймерів, а завдяки правильному призначенню Root Bridge, узгодженню trunk-з'єднань, перевірці allowed VLAN, контролю native VLAN і коректному використанню захисних механізмів STP [28; 30; 31].

Отже, STP, RSTP і MSTP виконують спільну функцію – запобігають петлям у надлишкових L2-топологіях і забезпечують використання резервних шляхів після відмови основного каналу. Водночас ці протоколи відрізняються швидкістю збіжності та способом роботи з VLAN: класичний STP є базовим механізмом побудови безпетльової топології, RSTP прискорює реакцію на зміну стану каналів, а MSTP дає змогу групувати VLAN у MST-instance та ефективніше використовувати резервні міжкомутаторні з'єднання.

2.2 Протоколи агрегації фізичних каналів: EtherChannel та LACP

У резервованих Ethernet-мережах між комутаторами часто прокладають кілька фізичних з'єднань. Якщо такі канали працюють як незалежні паралельні шляхи на каналному рівні, протоколи сімейства Spanning Tree можуть заблокувати частину з них для запобігання комутаційним петлям. У результаті фізичний резерв існує, але частина пропускної здатності не використовується для передавання користувацького трафіку.

Для ефективнішого використання кількох фізичних з'єднань застосовується агрегація каналів. EtherChannel – це технологія об'єднання кількох Ethernet-інтерфейсів між двома мережевими пристроями в один логічний інтерфейс. Такий логічний інтерфейс називається Port-channel або LAG (Link Aggregation Group). Для протоколів вищого рівня, а також для STP, група фізичних каналів виглядає як один канал, а не як кілька окремих паралельних з'єднань [10; 11].

Принцип об'єднання фізичних каналів у логічний Port-channel показано на рисунку 2.1.

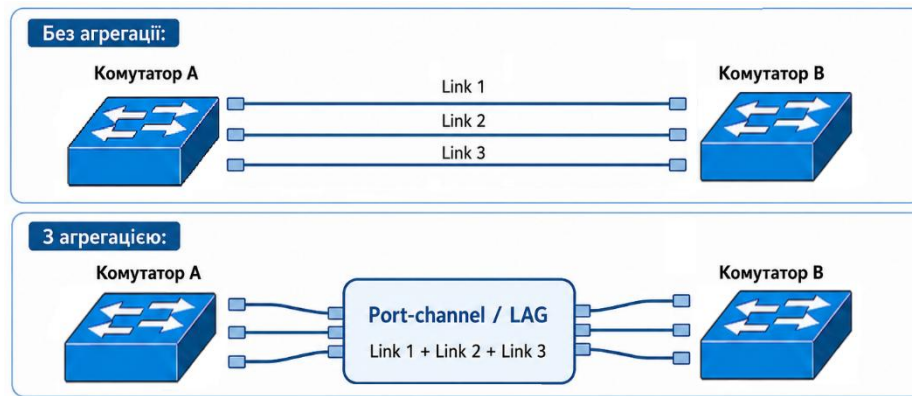


Рис. 2.1 — Принцип об'єднання фізичних каналів у логічний port-channel

Важлива відмінність між STP/RSTP/MSTP і LACP полягає в способі використання резервних з'єднань. STP/RSTP/MSTP формують безпетльову топологію шляхом вибору активних і резервних портів, тому частина шляхів може бути логічно заблокована. LACP працює інакше: він не блокує окремі канали як резервні, а об'єднує кілька фізичних інтерфейсів в один логічний канал. Якщо всі учасники агрегованого каналу працюють коректно, трафік може розподілятися між ними відповідно до алгоритму балансування [10; 11; 32].

LACP (Link Aggregation Control Protocol) є стандартним механізмом динамічного узгодження агрегованого каналу. Його завдання полягає в тому, щоб перевірити сумісність фізичних інтерфейсів на обох кінцях з'єднання та визначити, які з них можуть увійти до складу Port-channel. Для цього пристрої обмінюються службовими LACPDU-кадрами, у яких передається інформація про агрегований канал, системний ідентифікатор, порт і стан учасника [10; 32].

Базовими режимами LACP є active і passive. У режимі active пристрій сам ініціює обмін LACPDU, а в режимі passive лише відповідає на отримані LACPDU. Тому поєднання active-active або active-passive дозволяє сформувати агрегований канал, тоді як passive-passive не ініціює обмін службовими повідомленнями і зазвичай не приводить до формування LACP-групи [10].

Окремим параметром є LACP rate, який визначає частоту надсилання LACPDU. У практичних реалізаціях часто розрізняють normal/slow і fast. Повільний режим передбачає більший інтервал між службовими повідомленнями,

тоді як fast надсилає їх частіше і може швидше виявити втрату фізичного учасника. Наприклад, у документації Juniper для LACP описуються fast-інтервал 1 с і slow-інтервал 30 с [10].

LACP rate fast може бути корисним для критичних міжкомутаторних з'єднань, де важливо швидше вилучити несправний фізичний інтерфейс зі складу Port-channel. Водночас у стабільних мережах не завжди є потреба вмикати fast-режим на всіх агрегованих каналах. Частіший службовий обмін збільшує кількість control-plane трафіку, а в умовах нестабільного середовища може призводити до частіших змін стану учасників LAG. Тому цей параметр доцільно змінювати вибірково, з урахуванням критичності каналу та можливостей обладнання [10].

Щоб фізичні інтерфейси могли стабільно працювати в одному Port-channel, їхні параметри мають бути узгоджені. Зокрема, мають збігатися режим роботи порту, тип інкапсуляції trunk або access, набір дозволених VLAN, native VLAN для trunk-з'єднань, швидкість, duplex-режим та належність до однієї групи агрегації. Якщо ці параметри відрізняються, окремий фізичний порт може не увійти до агрегованого каналу або перейти в неактивний стан [10; 11].

У разі відмови одного фізичного інтерфейсу LACP виключає його зі складу агрегованого каналу. Якщо в Port-channel залишається хоча б один активний фізичний учасник, логічний інтерфейс може залишатися працездатним, а передавання трафіку продовжується через доступні канали. При цьому відмова одного учасника не означає повної втрати міжкомутаторного з'єднання, але призводить до зменшення сумарної доступної пропускної здатності агрегованого каналу [11].

Агрегація каналів також має обмеження. По-перше, вона не гарантує, що один окремий потік даних буде одночасно використовувати всі фізичні інтерфейси, оскільки розподіл трафіку залежить від алгоритму балансування. Зазвичай для вибору фізичного каналу враховуються параметри потоку, наприклад MAC-адреси, IP-адреси або номери портів, залежно від можливостей обладнання. По-друге, LACP не усуває потребу в коректному налаштуванні

VLAN, trunk-з'єднань і параметрів фізичних інтерфейсів. Помилки в цих параметрах можуть призвести до нестабільної роботи Port-channel [11].

Таким чином, EtherChannel і LACP підвищують ефективність використання фізичних міжкомутаторних з'єднань і зменшують вплив відмови одного каналу на логічну зв'язність. Однак LACP не є повною заміною STP/RSTP/MSTP, оскільки не вирішує задачу усунення петель у всій L2-топології. Так само LACP не вирішує проблему резервування шлюзу за замовчуванням, оскільки працює на каналному рівні та відповідає за агрегований канал, а не за доступність маршрутизатора або gateway для кінцевих пристроїв [9; 10; 11].

2.3 Протоколи резервування шлюзу за замовчуванням: VRRP, HSRP, GLBP

Механізми резервування на каналному рівні, зокрема STP/RSTP/MSTP та LACP, підвищують стійкість Ethernet-з'єднань між комутаторами, але не вирішують проблему відмови шлюзу за замовчуванням. Для кінцевих пристроїв шлюз є першою точкою виходу за межі локальної підмережі. Якщо маршрутизатор або L3-інтерфейс, який виконує роль gateway, стає недоступним, хости можуть втратити зв'язок з іншими мережами навіть за умови працездатності комутаційної інфраструктури [13; 18].

Для розв'язання цієї задачі застосовуються протоколи резервування першого шлюзу, або FHRP (First Hop Redundancy Protocol). До них належать VRRP, HSRP і GLBP. Їхня спільна ідея полягає у створенні віртуального шлюзу, який має virtual IP і virtual MAC. Саме цю віртуальну IP-адресу кінцеві пристрої використовують як gateway за замовчуванням. Завдяки цьому зміна активного фізичного маршрутизатора не потребує ручної зміни налаштувань на клієнтських пристроях [13; 18].

Логіку роботи віртуального шлюзу за замовчуванням показано на рисунку 2.1.

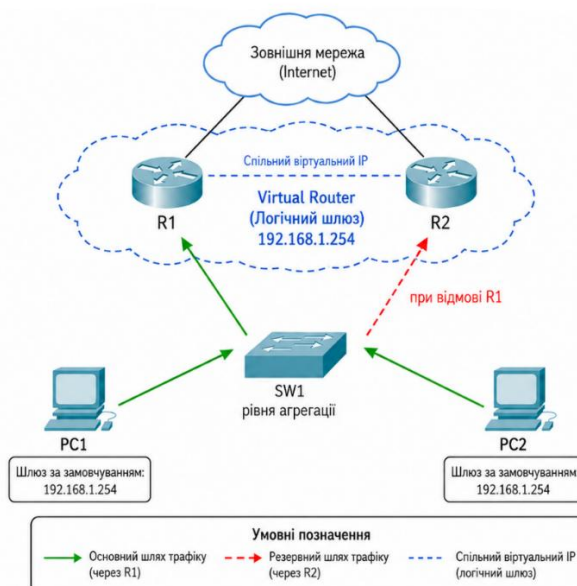


Рис. 2.1 — Логічна схема резервування шлюзу за замовчуванням (FHRP)

Основним протоколом резервування шлюзу, який доцільно використовувати в практичній частині роботи, є VRRP (Virtual Router Redundancy Protocol). VRRP є відкритим стандартним протоколом і не прив'язаний до обладнання одного виробника. У його основі лежить об'єднання кількох маршрутизаторів в одну VRRP-групу. Для цієї групи задається віртуальна IP-адреса, яку кінцеві пристрої використовують як шлюз за замовчуванням [13; 18].

У VRRP один маршрутизатор виконує роль Master. Саме він відповідає на ARP-запити до віртуальної IP-адреси та пересилає трафік, адресований віртуальному шлюзу. Інші маршрутизатори перебувають у стані Backup і контролюють доступність Master. Вибір активного маршрутизатора виконується за пріоритетом: пристрій із вищим priority має перевагу під час вибору Master. Якщо Master стає недоступним, резервний маршрутизатор переходить у роль Master і починає обслуговувати віртуальний шлюз. Механізм preempt дозволяє маршрутизатору з вищим пріоритетом повернути собі роль Master після відновлення роботи [13; 18].

Вибір Master у VRRP залежить від priority. Чим вищий priority, тим більша ймовірність, що саме цей маршрутизатор буде активним. Стандартне значення priority для резервного маршрутизатора часто становить 100, а маршрутизатор,

який є власником IP-адреси, може мати priority 255. Якщо priority однаковий, для вибору використовується додатковий критерій, зокрема IP-адреса інтерфейсу [13; 18].

Preempt визначає, чи може маршрутизатор із вищим priority повернути собі роль Master після відновлення. Це корисно тоді, коли основний маршрутизатор має кращі характеристики, оптимальніший маршрут або вищу пропускну здатність. Водночас preempt потрібно застосовувати обережно: якщо основний маршрутизатор часто втрачає і відновлює доступність, ролі можуть почати «гойдатись» між пристроями, що погіршує стабільність gateway [13; 18].

Контроль доступності активного маршрутизатора у VRRP виконується за допомогою VRRP Advertisement. Master періодично надсилає службові повідомлення, а Backup відстежує їх надходження. Якщо Backup не отримує повідомлення протягом визначеного часу, він вважає Master недоступним і може перебрати активну роль. У спрощеному вигляді Master Down Interval залежить від advertisement interval і додаткової поправки, пов'язаної з priority. Тобто час очікування не є лише механічним множенням одного таймера, а враховує логіку вибору активного маршрутизатора [13; 18].

Після зміни активного шлюзу важливу роль відіграє Gratuitous ARP. Він використовується для оновлення відповідності IP–MAC у локальній мережі після переходу virtual IP на інший фізичний маршрутизатор. Завдяки цьому хости й комутатори можуть швидше оновити ARP-таблиці та таблиці MAC-адрес, що зменшує тривалість перехідного стану після failover [13; 18].

Для ідентифікації віртуального маршрутизатора на каналному рівні VRRPv3 використовує стандартизований діапазон MAC-адрес IANA. Формування адреси базується на OUI 00-00-5E та ідентифікаторі віртуальної групи VRID, який займає останній байт. Для IPv4 використовується формат 00-00-5E-00-01-VRID, а для IPv6 – 00-00-5E-00-02-VRID. Завдяки цьому кінцеві пристрої взаємодіють із віртуальним шлюзом як з одним логічним маршрутизатором, хоча фізично роль активного вузла може переходити між різними пристроями [13; 18].

HSRP (Hot Standby Router Protocol) є пропрієтарним протоколом Cisco, який виконує подібну функцію резервування шлюзу. У HSRP також створюється віртуальна IP-адреса шлюзу, а фізичні маршрутизатори працюють у ролях Active і Standby. Active-маршрутизатор обслуговує трафік, а Standby готовий перебрати його роль у разі відмови. Ранні реалізації HSRPv1 використовують multicast-адресу 224.0.0.2, мають обмеження у 256 груп і поступаються HSRPv2 за масштабованістю. HSRPv2 розширює кількість груп і краще підходить для сучасних Cisco-мереж, однак сам протокол залишається менш універсальним порівняно з VRRP через прив'язку до екосистеми Cisco [33].

GLBP (Gateway Load Balancing Protocol) також є Cisco-пропрієтарним механізмом, але, на відміну від VRRP і HSRP, він поєднує резервування з балансуванням навантаження. У GLBP використовується роль AVG (Active Virtual Gateway), який відповідає на ARP-запити клієнтів, і ролі AVF (Active Virtual Forwarder), які фактично пересилають трафік. Завдяки цьому різні клієнти можуть отримувати різні віртуальні MAC-адреси та використовувати різні фізичні маршрутизатори як активні шлюзи. Такий підхід дозволяє ефективніше задіяти ресурси кількох маршрутизаторів, але ускладнює логіку роботи протоколу та робить його менш універсальним для змішаних середовищ [34]. Технічне порівняння протоколів резервування першого шлюзу наведено в таблиці 2.1.

Таблиця 2.1 — Технічне порівняння протоколів резервування першого шлюзу

Параметр порівняння	VRRPv3	HSRPv2	GLBP
Статус стандарту	Відкритий (RFC 9568)	Пропрієтарний (Cisco)	Пропрієтарний (Cisco)
Основна модель	Active / Backup	Active / Standby	Active / Active
Кількість активних шлюзів	Один на групу	Один на групу	До 4 на групу
Мультикаст-адреса (IPv4)	224.0.0.18	224.0.0.102	224.0.0.102

Формат Virtual MAC (IPv4)	0000.5E00.01xx	0000.0C9F.Fxxx	0007.B400.xxyy
Балансування навантаження	Налаштуванням груп	Налаштуванням груп	Нативне (AVG/AVF)

На практиці для VRRP, HSRP і GLBP найчастіше змінюють priority, preempt і interface tracking. Priority визначає, який маршрутизатор має бути основним; preempt визначає, чи повернеться основний маршрутизатор до активної ролі після відновлення; interface tracking дозволяє зменшити priority маршрутизатора, якщо в нього відмовив важливий uplink або інший критичний інтерфейс. Саме ці параметри безпосередньо пов'язують логіку вибору active/master із реальним станом мережі [13; 18; 33].

Advertisement/hello timers також можуть впливати на швидкість failover, але їх не варто надмірно зменшувати без потреби. Занадто короткі інтервали можуть викликати хибні перемикання при короткочасних затримках, перевантаженні CPU або нестабільності каналу. У результаті мережа може стати не швидшою, а менш стабільною через часте перемикання ролей між маршрутизаторами. Тому для VRRP/HSRP/GLBP важливо не лише прискорити failover, а й уникнути частого «гойдання» активної ролі [13; 18; 33].

Отже, протоколи VRRP, HSRP і GLBP вирішують завдання, яке не покривається механізмами канального рівня: забезпечують доступність шлюзу за замовчуванням для кінцевих пристроїв. Вони не усувають фізичну причину аварії та не гарантують повної відсутності короткочасних перерв, але зменшують вплив відмови активного маршрутизатора на роботу мережі. У межах цієї роботи основну увагу доцільно приділити VRRP, оскільки він є відкритим стандартним протоколом і добре підходить для моделювання резервування шлюзу між маршрутизаторами R1 та R2 у середовищі GNS3.

2.4 Механізми швидкого виявлення та обробки відмов: BFD, Keepalive, timer-based failover

У відмовостійкій мережі важлива не лише наявність резервного маршруту, каналу або вузла, а й швидкість виявлення самої відмови. Якщо резервний шлях існує, але протокол маршрутизації або резервування ще не зафіксував недоступність сусіда, трафік певний час може продовжувати спрямовуватися через несправний напрямок. Тому загальний час відновлення залежить від двох етапів: часу виявлення відмови та часу подальшої перебудови маршрутизації або перемикання на резервний елемент [14; 15].

У найпростішому випадку відмова фіксується на фізичному рівні. Наприклад, при обриві Ethernet-кабелю інтерфейс переходить у стан Down, після чого відповідні протоколи можуть змінити топологію або маршрут. Проте не всі аварії є прямими. У розподілених мережах можливі ситуації, коли локальний інтерфейс маршрутизатора залишається в стані Up, але зв'язність із сусіднім вузлом порушена через проміжне обладнання, помилки передавання або відмову на віддаленій ділянці. У таких випадках потрібні службові механізми контролю доступності сусіда [14; 15].

Базовим способом такого контролю є keepalive-перевірки. Keepalive – це періодичний обмін службовими повідомленнями, за допомогою якого пристрій або протокольна сесія підтверджує свою активність. Якщо відповіді не надходять протягом визначеного часу, сусід або сесія вважається недоступною. Такі перевірки застосовуються в різних мережних протоколах, однак їхня швидкість залежить від налаштованих інтервалів і механізму обробки службових повідомлень.

Іншим підходом є timer-based failover – перемикання після спрацювання певного таймера. До таких механізмів належать hello/dead timers у протоколах маршрутизації, hold timers у службових протоколах, а також інтервали очікування недоступності активного вузла в протоколах резервування шлюзу. Якщо таймери занадто великі, мережа повільніше реагує на аварію. Якщо їх зменшити надмірно,

зростає ризик хибних спрацювань через короточасні затримки, втрату окремих службових пакетів або перевантаження процесора мережевого пристрою [19].

BFD (Bidirectional Forwarding Detection) є спеціалізованим механізмом швидкого виявлення втрати двонаправленої зв'язності між двома мережевими пристроями. Його основна функція полягає не в маршрутизації трафіку, а в контролі доступності сусіднього вузла або шляху передавання. BFD працює як легкий службовий механізм: між двома пристроями встановлюється BFD-сесія, після чого вони періодично обмінюються контрольними пакетами. Для одноперехідних BFD-сесій використовуються UDP-пакети з портом призначення 3784, а для Echo-функції – порт 3785. Якщо протягом заданої кількості інтервалів один із пристроїв не отримує BFD-пакети від сусіда, BFD-сесія переходить у стан Down. Після цього BFD повідомляє пов'язаний клієнтський протокол, наприклад OSPF, про втрату сусіднього вузла. Завдяки цьому OSPF може не чекати власних стандартних dead timers, а раніше розпочати перерахунок маршрутів [14; 15; 19].

BFD працює як легкий службовий механізм: між двома пристроями встановлюється BFD-сесія, після чого вони періодично обмінюються контрольними пакетами. Для одноперехідних BFD-сесій використовуються UDP-пакети з портом призначення 3784, а для Echo-функції — порт 3785. Якщо протягом заданої кількості інтервалів один із пристроїв не отримує BFD-пакети від сусіда, BFD-сесія переходить у стан Down, а клієнтський протокол отримує повідомлення про втрату зв'язності [14; 15].

Процес встановлення BFD-сесії та перехід її станів доцільно подати на рисунку 2.1.

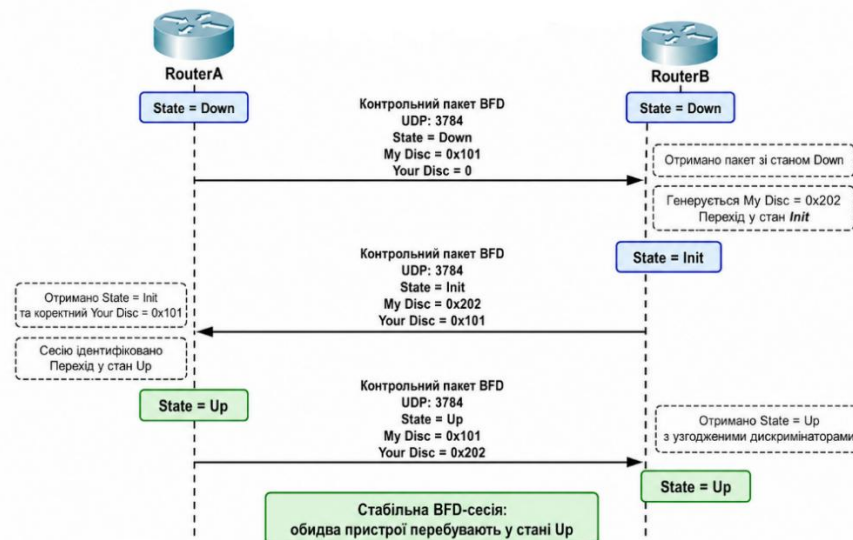


Рис. 2.1 — Послідовність станів та узгодження дискримінаторів при встановленні BFD-сесії

Важливо розрізняти час виявлення відмови та час збіжності маршрутизації. BFD скорочує саме час виявлення недоступності сусіда. Базовими параметрами BFD є transmit interval, receive interval і multiplier. Transmit interval визначає бажаний інтервал передавання BFD-пакетів, receive interval - мінімальний інтервал, із яким пристрій готовий приймати BFD-пакети, а multiplier - кількість пропущених пакетів або інтервалів, після яких сесія вважається недоступною. Після цього протокол маршрутизації, наприклад OSPF, виконує власну логіку обробки події: видаляє недоступне сусідство, оновлює інформацію про стан інтерфейсів і перераховує таблицю маршрутів. Тому загальний час відновлення мережі залежить як від параметрів BFD, так і від швидкості реакції протоколу маршрутизації [14; 15; 19].

Час виявлення відмови BFD можна подати у спрощеному вигляді:

$$T_{\text{виявл}} = M \cdot \max(I_{(\text{перед})tx, \text{відд}}, I_{(\text{прийм})rx, \text{лок}}), \text{ де:}$$

- $T_{\text{виявл}}$ – сумарний час виявлення відмови в мілісекундах (мс), після якого клієнтські протоколи отримують сповіщення про аварію;
- M – множник виявлення, що визначає кількість дозволених втрачених пакетів поспіль до моменту переведення сесії у статус *Down* (згідно з RFC 5880, є цілим числом, стандартно приймається рівним 3);

- $I_{(\text{перед})\text{tx,відд}}$ – мінімальний інтервал передавання BFD-пакетів віддаленим вузлом у мілісекундах, який він анонсує у полі *Desired Min TX Interval* під час встановлення сесії;
- $I_{(\text{прийм})\text{rx,лок}}$ – мінімальний інтервал приймання BFD-пакетів, який здатний апаратно обробити локальний пристрій у мілісекундах, що конфігурується параметром *Required Min RX Interval* [27].

З цієї формули видно, що фактична швидкість реакції BFD залежить не лише від бажаного інтервалу передавання, а й від можливостей обох пристроїв та значення *multiplier*. Тому агресивне зменшення таймерів до дуже малих мілісекундних значень не завжди є доцільним. У високонавантажених мережах це може збільшити кількість службового трафіку, навантажити площину керування або призвести до хибного падіння BFD-сесій при короткочасних затримках. Значення BFD-таймерів потрібно підбирати з урахуванням продуктивності обладнання, стабільності каналу та критичності сервісу [14; 15].

BFD може працювати разом із різними протоколами маршрутизації та резервування, однак у межах цієї роботи основний інтерес становить його взаємодія з OSPF. У типовому сценарії OSPF відповідає за побудову маршрутів, а BFD – за швидке виявлення втрати сусіда. Такий поділ функцій є практично зручним: немає потреби надмірно зменшувати стандартні таймери OSPF, оскільки контроль доступності сусіда виконує спеціалізований механізм [15; 19; 20].

Отже, *keepalive*-перевірки, *timer-based failover* і BFD виконують спільне завдання – визначають момент, коли мережа має реагувати на відмову. Водночас BFD є спеціалізованим механізмом, який дозволяє прискорити саме етап виявлення недоступності сусіда. Він не відновлює фізичний інтерфейс і не замінює OSPF, але допомагає маршрутизатору швидше отримати інформацію про аварію та розпочати перебудову маршрутів. Саме ця властивість є основою практичної перевірки BFD у середовищі GNS3.

Висновки до розділу 2

У другому розділі розглянуто основні групи протоколів і механізмів, які забезпечують відмовостійкість мереж електронних комунікацій на різних рівнях. Протоколи STP, RSTP/Rapid-PVST і MSTP працюють на каналному рівні та вирішують задачу запобігання петлям у фізично надлишкових Ethernet-топологіях. STP забезпечує базову безпетльову топологію, але має повільнішу таймерну збіжність. RSTP/Rapid-PVST пришвидшує реакцію на зміну стану лінків завдяки ролям портів і механізму узгодження між комутаторами. MSTP дозволяє групувати VLAN у MST-інстанси та ефективніше використовувати резервні uplink-з'єднання.

EtherChannel і LACP виконують іншу задачу: вони не блокують надлишкові шляхи, як STP, а об'єднують кілька фізичних лінків в один логічний Port-channel. Це дозволяє одночасно підвищити пропускну здатність і зберегти логічну зв'язність у разі відмови одного фізичного учасника агрегованого каналу. При цьому LACP не є заміною STP, оскільки не контролює всю L2-топологію, і не є заміною протоколів резервування шлюзу, оскільки не вирішує проблему доступності gateway.

Протоколи VRRP, HSRP і GLBP належать до First Hop Redundancy Protocols і забезпечують резервування шлюзу за замовчуванням. VRRP є відкритим стандартним протоколом IETF і працює через virtual router, virtual IP, virtual MAC, ролі Master/Backup і priority. HSRP виконує подібну функцію в Cisco-середовищі через ролі Active/Standby. GLBP, крім резервування шлюзу, може розподіляти навантаження між кількома маршрутизаторами. Отже, ці протоколи вирішують задачу, яку не покривають ні STP/RSTP/MSTP, ні LACP.

BFD, keepalive і timer-based failover відповідають не за створення резервного шляху, а за швидкість виявлення аварійної події. BFD є спеціалізованим механізмом швидкого виявлення втрати двонаправленої зв'язності та може прискорити реакцію клієнтських протоколів, наприклад OSPF. Keepalive і timer-based failover є простішими механізмами контролю доступності, але зазвичай

менш гнучкі й повільніші. Таким чином, повна відмовостійкість мережі досягається не одним протоколом, а поєднанням кількох механізмів: L2-захисту від петель, агрегації каналів, резервування шлюзу та швидкого виявлення відмов.

З МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛІВ ВІДМОВОСТІЙКОСТІ В СЕРЕДОВИЩІ GNS3

3.1 Опис тестової топології та параметрів моделювання

Для практичної перевірки роботи протоколів відмовостійкості було побудовано тестову мережеву топологію в середовищі Graphical Network Simulator-3 (GNS3). Використання GNS3 дає змогу відтворити типові аварійні ситуації в контрольованих умовах без впливу на реальну мережеву інфраструктуру. Метою моделювання є перевірка поведінки механізмів Rapid-PVST/RSTP, MSTP, LACP, VRRP та OSPF/BFD у межах однієї резервованої топології.

Тестовий стенд побудовано за спрощеною дворівневою структурою. Комутатори SW1 і SW2 виконують роль комутаторів рівня розподілу, оскільки до них підключені маршрутизатори R1/R2, міжкомутаторний агрегований канал і uplink-з'єднання від комутатора доступу. Комутатор SW3 виконує роль комутатора доступу, оскільки через нього підключаються кінцеві вузли PC1, PC2 і PC3 у відповідних VLAN. Маршрутизатори R1 і R2 використовуються для маршрутизації між VLAN та резервування шлюзу за замовчуванням. Загальну схему тестової топології наведено на рисунку 3.1.

До складу тестового стенда входять два маршрутизатори R1 та R2, три комутатори SW1, SW2, SW3 і три кінцеві вузли PC1, PC2 та PC3. Маршрутизатори R1 і R2 реалізовані на базі образів Cisco IOSv L3 версії 15.9. Комутатори SW1, SW2 та SW3 реалізовані на базі Cisco IOL L2 версії 17.15. Кінцеві вузли PC1–PC3 створені за допомогою VPCS і використовуються для перевірки доступності шлюзів, міжмережевої взаємодії та реакції топології на аварійні зміни.

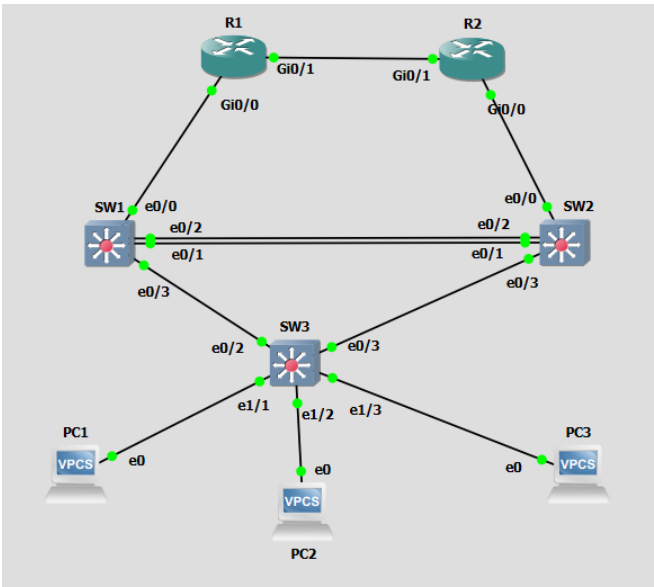


Рис. 3.1 — Схема інтегрованої тестової топології логічного та фізичного резервування в середовищі GNS3

У топології використовуються VLAN 10, VLAN 20 і VLAN 99. VLAN 10 та VLAN 20 імітують користувацькі сегменти, а VLAN 99 використовується як службовий сегмент керування. Для експерименту з MSTP додатково можуть використовуватися VLAN 30 і VLAN 40, що дає змогу показати розподіл різних груп VLAN між окремими MST-instance. VLAN-структуру тестової топології наведено в таблиці 3.1.

Таблиця 3.1 — VLAN-структура тестової топології

VLAN	Логічна назва	Адресний простір	Призначення
VLAN 10	USERS_VLAN_10	192.168.10.0/24	Користувацький сегмент PC1
VLAN 20	USERS_VLAN_20	192.168.20.0/24	Користувацький сегмент PC2
VLAN 99	Службовий сегмент керування PC3	192.168.99.0/24	Службовий сегмент керування PC3
VLAN 30	Додатковий сегмент для MSTP-експерименту	Задається в межах тесту MSTP	Залежить від сценарію
VLAN 40	Додатковий сегмент для MSTP-експерименту	Задається в межах тесту MSTP	Залежить від сценарію

Маршрутизація між VLAN реалізована за схемою router-on-a-stick. На маршрутизаторах R1 і R2 фізичний інтерфейс GigabitEthernet0/0 використовується як trunk-інтерфейс до комутаторів SW1 і SW2 відповідно. Для VLAN 10, VLAN 20 і VLAN 99 створено окремі підінтерфейси з тегуванням IEEE 802.1Q. На R1 налаштовано адреси 192.168.10.2/24, 192.168.20.2/24, 192.168.99.2/24, а на R2 – 192.168.10.3/24, 192.168.20.3/24, 192.168.99.3/24. Кінцеві вузли використовують як шлюзи віртуальні адреси VRRP: 192.168.10.1, 192.168.20.1 і 192.168.99.1. Основні міжпристроєві з'єднання наведено в таблиці 3.2.

Таблиця 3.2 — Основні інтерфейсні з'єднання тестової топології

З'єднання	Інтерфейс першого пристрою	Інтерфейс другого пристрою	Режим роботи	Призначення
R1 – SW1	R1 Gi0/0	SW1 Et0/0	802.1Q trunk	Передавання VLAN 10, 20, 99 від основного маршрутизатора
R2 – SW2	R2 Gi0/0	SW2 Et0/0	802.1Q trunk	Передавання VLAN 10, 20, 99 від резервного маршрутизатора
R1 – R2	R1 Gi0/1	R2 Gi0/1	Routed L3-link	OSPF-сусідство та BFD-контроль зв'язності
SW1– SW2	SW1 Et0/1, Et0/2	SW2 Et0/1, Et0/2	LACP Port-channel1, trunk	Агрегований канал між комутаторами розподілу
SW1 –SW3	SW1 Et0/3	SW3 Et0/2	802.1Q trunk	Trunk-з'єднання комутатора доступу з SW1
SW2 –SW3	SW2 Et0/3	SW3 Et0/3	802.1Q trunk	Резервне trunk-з'єднання комутатора доступу з SW2
SW3 – PC1	SW3 Et1/1	PC1 e0	Access VLAN 10	Підключення вузла користувацького сегмента VLAN 10
SW3 – PC2	SW3 Et1/2	PC2 e0	Access VLAN 20	Підключення вузла користувацького сегмента VLAN 20
SW3 – PC3	SW3 Et1/3	PC3 e0	Access VLAN 99	Підключення вузла службового сегмента VLAN 99

Trunk-з'єднання між комутаторами потрібні для передавання кількох VLAN через один фізичний або логічний канал. У базовій конфігурації через trunk-порти передаються VLAN 10, VLAN 20 і VLAN 99. Для MSTP-перевірки до allowed VLAN додатково додаються VLAN 30 і VLAN 40. У режимі Rapid-PVST/RSTP для VLAN 10, VLAN 20 і VLAN 99 використовується SW1 як основний root bridge, а SW2 як резервний комутатор розподілу. Для цього на SW1 встановлено пріоритет 4096, а на SW2 – 8192. У початковому стані SW3 використовує uplink у напрямку SW1 як основний шлях, а uplink у напрямку SW2 – як резервний.

Між SW1 і SW2 налаштовано LACP/EtherChannel Port-channel1. До складу агрегованого каналу входять два фізичні з'єднання: SW1 Ethernet0/1 – SW2 Ethernet0/1 та SW1 Ethernet0/2 – SW2 Ethernet0/2. Обидві сторони працюють у режимі LACP active, а логічний інтерфейс Port-channel1 налаштований як trunk. Така схема дозволяє перевірити, чи залишається логічне міжкомутаторне з'єднання активним після відмови одного фізичного учасника EtherChannel.

Для резервування шлюзу за замовчуванням використовується VRRP. У кожній базовій VLAN налаштовано окрему VRRP-групу: групу 10 для VLAN 10, групу 20 для VLAN 20 і групу 99 для VLAN 99. У штатному режимі R1 має пріоритет 110 і виконує роль Master, тоді як R2 із пріоритетом за замовчуванням перебуває в ролі Backup. Така конфігурація дозволяє кінцевим вузлам використовувати незмінні віртуальні IP-адреси шлюзу навіть у разі втрати доступності основного маршрутизатора [13; 18].

Окремий L3-інтерфейс між R1 і R2 використовується для перевірки роботи OSPF і BFD. На інтерфейсах GigabitEthernet0/1 маршрутизаторів налаштовано адреси 10.255.255.1/30 і 10.255.255.2/30. В межах OSPF використовується area 0, а інтерфейси, які не беруть участі у формуванні сусідства R1–R2, переведені в пасивний режим. Для прискореного виявлення втрати L3-зв'язності налаштовано BFD з параметрами interval 300, min_rx 300, multiplier 3. Теоретично такі параметри відповідають часу виявлення порядку 900 мс, однак у практичному

аналізі реакція оцінюється за станом BFD/OSPF-сусідства та системними повідомленнями, а не лише за звичайним ICMP-ping [14; 15; 19].

Для MSTP-експерименту на комутаторах використовується окрема MST-конфігурація: name GNS3-MST, revision 1, instance 1 vlan 10,20,99 та instance 2 vlan 30,40. У цій частині перевіряється не базова доступність шлюзів, а відмінність MSTP від Rapid-PVST/RSTP: VLAN 10, 20 і 99 об'єднуються в MST1, а VLAN 30 і 40 – в MST2. Для MST1 основним root bridge виступає SW1, а для MST2 – SW2, що дає змогу продемонструвати різні активні uplink-шляхи для різних груп VLAN.

Перед виконанням аварійних сценаріїв фіксується початковий стан топології. Для цього використовуються команди show spanning-tree, show interfaces trunk, show etherchannel summary, show vrrp brief, show ip ospf neighbor, show bfd neighbors і show logging. Після цього на відповідному інтерфейсі виконується адміністративне вимкнення за допомогою shutdown, фіксується реакція протоколу та перевіряється стан мережі після аварії.

Доступність перевіряється за допомогою ping з кінцевих вузлів до відповідних шлюзів або віддалених адрес. Проте звичайний ping не використовується як точний інструмент вимірювання часу збіжності, оскільки ICMP-запити надсилаються з певним інтервалом і можуть не зафіксувати короткочасне порушення зв'язності між двома запитами. Тому основними доказовими даними є зміна ролей портів, стан Port-channel, перехід VRRP-ролей, стан OSPF/BFD-сусідства, системні журнали та Wireshark Capture. Захоплення трафіку у Wireshark використовується для підтвердження фактичного проходження службових кадрів або користувацького трафіку через відповідні інтерфейси.

Таким чином, тестова топологія в GNS3 дозволяє в межах одного стенда перевірити роботу кількох механізмів відмовостійкості: Rapid-PVST/RSTP і MSTP при зміні L2-топології, LACP при відмові фізичного учасника Port-channel, VRRP при недоступності основного шлюзу та BFD/OSPF при втраті L3-зв'язності між маршрутизаторами.

3.2 Дослідження роботи Rapid-PVST/RSTP та MSTP при зміні топології мережі

У цьому підрозділі досліджується поведінка протоколів сімейства Spanning Tree при зміні L2-топології в тестовому середовищі GNS3. Перевірка виконувалася у двох частинах. Спочатку досліджено реакцію Rapid-PVST/RSTP на відмову основного uplink-з'єднання комутатора доступу SW3 у напрямку SW1. Далі розглянуто MSTP як механізм групування VLAN у різні MST-instance з можливістю використання різних активних trunk-шляхів.

Метою першого експерименту є перевірка того, чи зможе Rapid-PVST/RSTP автоматично перевести резервний uplink SW3–SW2 в активний стан після відмови основного з'єднання SW3–SW1. У початковій топології SW1 є root bridge для VLAN 10, VLAN 20 і VLAN 99, SW2 виконує роль резервного комутатора розподілу, а SW3 є комутатором доступу.

Перед створенням аварійного сценарію на SW3 було перевірено стан Spanning Tree для VLAN 10, VLAN 20 і VLAN 99 наступними командами:

```
show spanning-tree vlan 10
show spanning-tree vlan 20
show spanning-tree vlan 99
show interfaces trunk
show spanning-tree blockedports
```

Результати показали, що для всіх трьох VLAN основним шляхом до root bridge є інтерфейс Ethernet0/2 у напрямку SW1. Другий uplink Ethernet0/3 у напрямку SW2 перебуває в ролі Alternate і заблокований для запобігання L2-петлі. Початковий стан портів Rapid-PVST/RSTP на SW3 наведено в таблиці 3.1.

Таблиця 3.1 — Початковий стан портів Rapid-PVST/RSTP на SW3

VLAN	Порт SW3	Роль	Стан	Пояснення
VLAN 10	Et0/2	Root	Forwarding	Основний шлях до SW1
VLAN 10	Et0/3	Alternate	Blocking	Резервний шлях через SW2
VLAN 20	Et0/2	Root	Forwarding	Основний шлях до SW1
VLAN 20	Et0/3	Alternate	Blocking	Резервний шлях через SW2
VLAN 99	Et0/2	Root	Forwarding	Основний шлях до SW1
VLAN 99	Et0/3	Alternate	Blocking	Резервний шлях через SW2

Для наочності нижче наведено скорочений фрагмент виводу команди *show spanning-tree*, який підтверджує початковий стан SW3 для VLAN 10.

```
SW3#show spanning-tree vlan 10
```

```
VLAN0010
```

```
Spanning tree enabled protocol rstp
```

```
Root ID  Priority  4106
```

```
Address  aabb.cc00.0100
```

```
Cost      100
```

```
Port      3 (Ethernet0/2)
```

```
Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface      Role  Sts  Cost  Prio.Nbr  Type
```

```
-----
```

Et0/2	Root	FWD	100	128.3	P2p
Et0/3	Altn	BLK	100	128.4	P2p
Et1/1	Desg	FWD	100	128.6	P2p Edge

Аналогічний стан було зафіксовано для VLAN 20 і VLAN 99. Команда *show interfaces trunk* показала, що VLAN 10, VLAN 20 і VLAN 99 дозволені на обох trunk-портах SW3, однак у forwarding state до аварії перебував лише Ethernet0/2:

```
SW3#show interfaces trunk
```

```
Port      Vlans allowed on trunk
```

```
Et0/2      10,20,99
```

```
Et0/3      10,20,99
Port       Vlans in spanning tree forwarding state and not pruned
Et0/2      10,20,99
Et0/3      none
```

Початковий стан резервного uplink-з'єднання було перевірено командою *show spanning-tree blockedports*. Її використання дозволяє швидко визначити, які порти комутатора перебувають у заблокованому стані для окремих VLAN.

```
SW3#show spanning-tree blockedports
```

Name	Blocked Interfaces List
-----	-----
VLAN0010	Et0/3
VLAN0020	Et0/3
VLAN0099	Et0/3

```
Number of blocked ports (segments) in the system : 3
```

Значення Number of blocked ports (segments) in the system : 3 у цьому випадку не означає три різні фізичні порти. У режимі Rapid-PVST для кожної VLAN формується окремий екземпляр Spanning Tree, тому один фізичний trunk-порт Ethernet0/3 враховується окремо для VLAN 10, VLAN 20 і VLAN 99.

Для додаткової перевірки фактичного шляху трафіку було використано Wireshark Capture. До аварії на інтерфейсі SW3–SW1 з фільтром `icmp && vlan.id == 10` було зафіксовано ICMP-трафік між PC1 192.168.10.10 та віртуальним шлюзом 192.168.10.1. Це відповідає консольному стану, у якому Ethernet0/2 на SW3 є Root/Forwarding для VLAN 10, що підтверджено на рисунку 3.1.

No.	Time	Source	Destination	Protocol	Length	Info
760	144.772993	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x919f, seq=86/22016, ttl=64
761	144.940941	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x919f, seq=86/22016, ttl=255
765	145.962226	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x929f, seq=87/22272, ttl=64
769	146.161208	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x929f, seq=87/22272, ttl=255
773	147.182672	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x939f, seq=88/22528, ttl=64
775	147.211519	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x939f, seq=88/22528, ttl=255
781	148.232684	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x949f, seq=89/22784, ttl=64
782	148.243577	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x949f, seq=89/22784, ttl=255
786	149.269256	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x959f, seq=90/23040, ttl=64
787	149.304657	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x959f, seq=90/23040, ttl=255
794	150.321353	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x969f, seq=91/23296, ttl=64
795	150.345001	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x969f, seq=91/23296, ttl=255
801	151.373807	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x979f, seq=92/23552, ttl=64
802	151.411151	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x979f, seq=92/23552, ttl=255
807	152.438231	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x989f, seq=93/23808, ttl=64
810	152.476174	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x989f, seq=93/23808, ttl=255
813	153.487585	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x9a9f, seq=94/24064, ttl=64
815	153.504128	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x9a9f, seq=94/24064, ttl=255
820	154.524347	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x9b9f, seq=95/24320, ttl=64
821	154.699976	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x9b9f, seq=95/24320, ttl=255
828	155.717770	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x9c9f, seq=96/24576, ttl=64
829	155.916741	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x9c9f, seq=96/24576, ttl=255
836	156.938192	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x9d9f, seq=97/24832, ttl=64
837	157.158377	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x9d9f, seq=97/24832, ttl=255
843	158.174052	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x9e9f, seq=98/25088, ttl=64
845	158.215533	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x9e9f, seq=98/25088, ttl=255
849	159.243568	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x9f9f, seq=99/25344, ttl=64
850	159.451039	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x9f9f, seq=99/25344, ttl=255
857	160.461775	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xa19f, seq=100/25600, ttl=64

Рис. 3.1 — Проходження трафіку через основний канал SW3–SW1 (eth0/2)

На резервному каналі SW3–SW2 до аварії з тим самим фільтром `icmp && vlan.id == 10` ICMP-пакети не відображалися. Це узгоджується з консольним виводом, де Ethernet0/3 на SW3 перебував у стані Alternate/Blocking для VLAN.

Для створення аварійного сценарію було адміністративно вимкнено основний uplink SW3 у напрямку SW1:

```
SW3#conf t
SW3(config)#interface Ethernet0/2
SW3(config-if)#shutdown
SW3(config-if)#end
```

Факт відмови інтерфейсу зафіксовано в журналі SW3:

```
*May 31 20:00:37.824: %LINK-5-CHANGED:
Interface Ethernet0/2, changed state to administratively down
*May 31 20:00:38.824: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Ethernet0/2, changed state to down
```

Після вимкнення Ethernet0/2 протокол Rapid-PVST/RSTP перебудував дерево. Для VLAN 10 портом у напрямку root bridge став Ethernet0/3, а сумарна вартість шляху до SW1 збільшилася зі 100 до 156. Це пояснюється тим, що після

аварії SW3 досягає root bridge SW1 не напряму, а через SW2 та Port-channel між SW2 і SW1.

Скорочений фрагмент стану SW3 після аварії:

```
SW3#show spanning-tree vlan 10
```

```
VLAN0010
```

```
Spanning tree enabled protocol rstp
```

```
Root ID    Priority    4106
           Address    aabb.cc00.0100
           Cost      156
           Port      4 (Ethernet0/3)
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Et0/3	Root	FWD	100	128.4	P2p
Et1/1	Desg	FWD	100	128.6	P2p Edge

Для VLAN 20 і VLAN 99 було зафіксовано аналогічну поведінку: порт Ethernet0/3 отримав роль Root Port і перейшов у стан Forwarding.

Команда show interfaces trunk після аварії підтвердила, що єдиним активним trunk-портом SW3 для VLAN 10, VLAN 20 і VLAN 99 став Ethernet0/3. Зміну ролей портів SW3 після аварії Rapid-PVST/RSTP узагальнено в таблиці 3.2.

```
SW3#show interfaces trunk
```

Port	Vlans allowed on trunk
Et0/3	10,20,99
Port	Vlans in spanning tree forwarding state and not pruned
Et0/3	10,20,99

Таблиця 3.2 — Зміна ролей портів SW3 після аварії Rapid-PVST/RSTP

VLAN	Порт SW3	Стан до аварії	Стан після аварії
VLAN 10	Et0/2	Root / Forwarding	Shutdown / неактивний
VLAN 10	Et0/3	Alternate / Blocking	Root / Forwarding
VLAN 20	Et0/2	Root / Forwarding	Shutdown / неактивний
VLAN 20	Et0/3	Alternate / Blocking	Root / Forwarding
VLAN 99	Et0/2	Root / Forwarding	Shutdown / неактивний
VLAN 99	Et0/3	Alternate / Blocking	Root / Forwarding

Після перебудови на SW3 не залишилося заблокованих портів для досліджуваних VLAN:

```
SW3#show spanning-tree blockedports
```

```
Name          Blocked Interfaces List
```

```
-----
```

```
Number of blocked ports (segments) in the system : 0
```

Після вимкнення інтерфейсу Ethernet0/2 прямий шлях до Root Bridge став недоступним, що показано на рисунку 3.3. У відповідь Rapid-PVST/RSTP перебудував дерево: резервний uplink SW3–SW2 перейшов в активний стан і став єдиним доступним шляхом SW3 до Root Bridge, що підтверджено на рисунку 3.4.

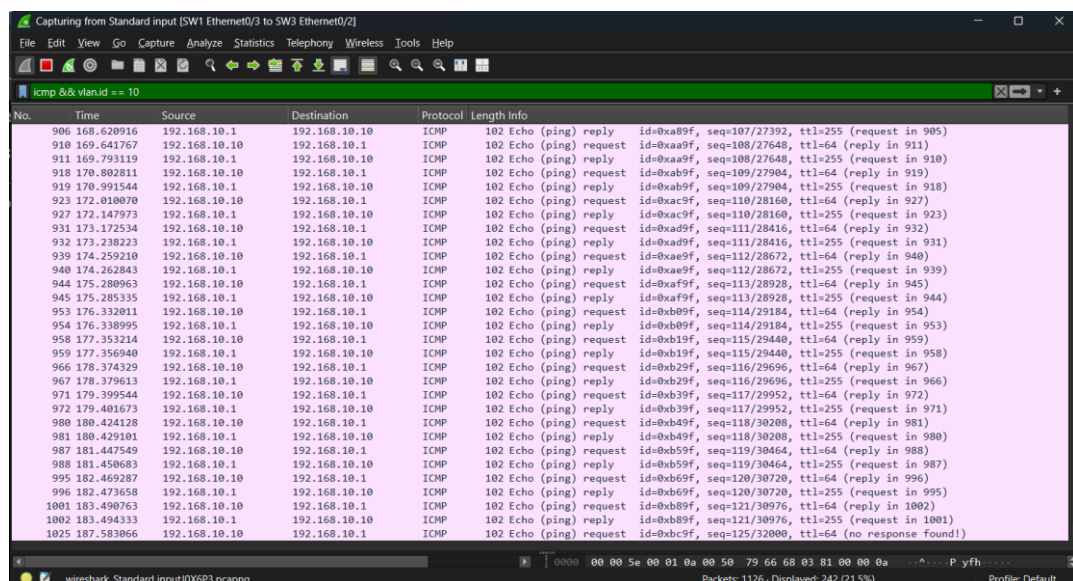


Рис. 3.3 — Припинення проходження трафіку через основний канал SW3–SW1 після створення експериментальної аварії (eth0/2)

No.	Time	Source	Destination	Protocol	Length	Info
894	201.450281	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xcb9f, seq=140/35840, ttl=255
901	202.471882	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xcc9f, seq=141/36096, ttl=64
902	202.476141	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xcc9f, seq=141/36096, ttl=255
907	203.494135	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xcd9f, seq=142/36352, ttl=64
908	203.498497	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xcd9f, seq=142/36352, ttl=255
916	204.515731	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xce9f, seq=143/36608, ttl=64
917	204.519178	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xce9f, seq=143/36608, ttl=255
921	205.537265	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xcf9f, seq=144/36864, ttl=64
922	205.540279	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xcf9f, seq=144/36864, ttl=255
929	206.558878	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd09f, seq=145/37120, ttl=64
930	206.563948	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd09f, seq=145/37120, ttl=255
934	207.580960	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd19f, seq=146/37376, ttl=64
935	207.583932	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd19f, seq=146/37376, ttl=255
942	208.602734	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd29f, seq=147/37632, ttl=64
944	208.618523	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd29f, seq=147/37632, ttl=255
948	209.640690	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd39f, seq=148/37888, ttl=64
949	209.647112	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd39f, seq=148/37888, ttl=255
958	210.664578	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd49f, seq=149/38144, ttl=64
959	210.671460	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd49f, seq=149/38144, ttl=255
963	211.685524	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd59f, seq=150/38400, ttl=64
964	211.690259	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd59f, seq=150/38400, ttl=255
971	212.709679	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd69f, seq=151/38656, ttl=64
972	212.712628	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd69f, seq=151/38656, ttl=255
977	213.728706	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd79f, seq=152/38912, ttl=64
978	213.732461	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd79f, seq=152/38912, ttl=255
985	214.749731	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd89f, seq=153/39168, ttl=64
986	214.755337	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd89f, seq=153/39168, ttl=255
990	215.773121	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xd99f, seq=154/39424, ttl=64
991	215.777349	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xd99f, seq=154/39424, ttl=255

Рис. 3.4 — Проходження трафіку через резервний канал SW3–SW2 після перебудови Rapid-PVST/RSTP внаслідок експериментальної аварії (eth0/3)

Окремо було перевірено стан SW2, оскільки після аварії саме через нього почав проходити резервний шлях від SW3 до SW1. На SW2 порт Ethernet0/3 у напрямку SW3 перебуває у стані Designated Forwarding, а Port-channel1 виконує роль Root Port у напрямку SW1. Це означає, що SW2 після аварії виконує роль транзитного комутатора між SW3 і root bridge.

Стан SW2 після перебудови Rapid-PVST/RSTP:

```
SW2#show spanning-tree vlan 10
```

```
VLAN0010
```

```
Spanning tree enabled protocol rstp
```

```
Root ID    Priority    4106
```

```
Address    aabb.cc00.0100
```

```
Cost       56
```

```
Port       65 (Port-channel1)
```

```
Interface    Role Sts    Cost    Prio.Nbr Type
```

```

-----
Et0/0      Desg FWD 100 128.1 P2p
Et0/3      Desg FWD 100 128.4 P2p
Po1        Root FWD 56 128.65 P2p

```

Аналогічний стан було зафіксовано для VLAN 20 і VLAN 99. Це підтверджує, що SW2 не став новим root bridge, а лише забезпечив транзитний шлях до SW1. Така поведінка відповідає очікуваній логіці резервування: root bridge залишається незмінним, а змінюється лише активний шлях від комутатора доступу до кореневого комутатора.

Для перевірки доступності під час аварії з PC1 було запущено тривалу ICMP-перевірку віртуального шлюзу VLAN 10:

```

PC1> ping 192.168.10.1 -c 1000
84 bytes from 192.168.10.1 icmp_seq=144 ttl=255 time=13.929 ms
84 bytes from 192.168.10.1 icmp_seq=145 ttl=255 time=5.060 ms
84 bytes from 192.168.10.1 icmp_seq=146 ttl=255 time=6.718 ms
84 bytes from 192.168.10.1 icmp_seq=147 ttl=255 time=9.976 ms
84 bytes from 192.168.10.1 icmp_seq=148 ttl=255 time=3.725 ms

```

У збереженому фрагменті ICMP-перевірки втрати пакетів не зафіксовано: відсутні пропуски icmp_seq і повідомлення timeout. Проте цей результат не слід трактувати як нульовий час збіжності або повну відсутність короткочасної перерви. Звичайний ping має обмежену точність, оскільки ICMP-запити надсилаються з певним інтервалом. Якщо перебудова дерева відбулася між двома ICMP-запитами, короткочасне порушення зв'язності могло не відобразитися у збереженому виводі.

Отже, Rapid-PVST/RSTP у досліджуваній топології коректно відреагував на відмову основного uplink-з'єднання SW3–SW1. Порт Ethernet0/3, який до аварії був резервним, перейшов у стан Root/Forwarding і забезпечив новий шлях до root bridge через SW2.

На відміну від Rapid-PVST/RSTP, де для кожної VLAN формується окремий екземпляр Spanning Tree, MSTP дозволяє об'єднати кілька VLAN в один MST-

instance. MST-instance у цьому контексті – це окреме логічне дерево Spanning Tree для певної групи VLAN.

У тестовій топології VLAN 10, VLAN 20 і VLAN 99 були об'єднані в MST1. Додатково до топології були додані PC4 та PC5, прив'язані до VLAN 30 і VLAN 40 відповідно, які були об'єднані в MST2. Для демонстрації практичної відмінності MSTP було задано різні Root Bridge: SW1 для MST1 і SW2 для MST2. Це дозволило отримати різні активні uplink-шляхи для різних груп VLAN, що показано на рисунку 3.5.

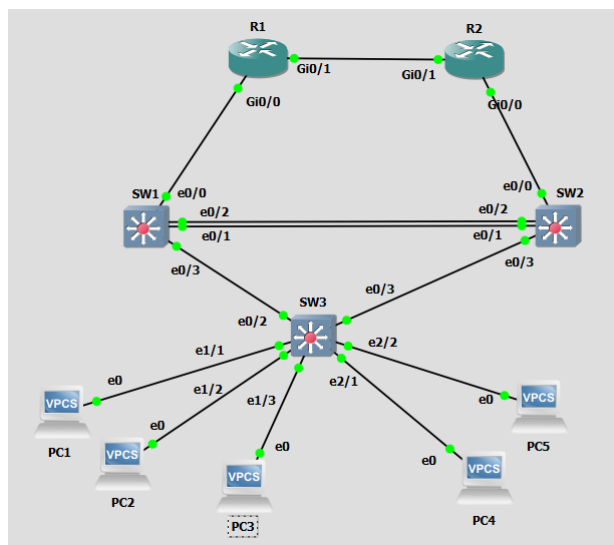


Рис. 3.5 — Оновлена схема для тестування MSTP в середовищі GNS3

Фрагмент MSTP-конфігурації SW3:

```
spanning-tree mode mst
spanning-tree mst configuration
name GNS3-MST
revision 1
instance 1 vlan 10,20,99
instance 2 vlan 30,40
exit
```

Початковий стан MSTP на SW3 підтверджує, що MST1 і MST2 використовують різні активні шляхи. Для MST1 порт Ethernet0/2 має роль Root і

перебуває у стані Forwarding, тоді як Ethernet0/3 є Alternate/Blocking. Для MST2 ситуація протилежна: Ethernet0/3 є Root/Forwarding, а Ethernet0/2 – Alternate/Blocking.

```
SW3#show spanning-tree mst 1
```

```
##### MST1   vlans mapped:  10,20,99
```

```
Root      address aabb.cc00.0100 priority 4097
          port   Et0/2      cost 2000000
```

```
Interface  Role Sts Cost
```

```
-----
```

```
Et0/2      Root FWD 2000000
```

```
Et0/3      Altn BLK 2000000
```

```
SW3#show spanning-tree mst 2
```

```
##### MST2   vlans mapped:  30,40
```

```
Root      address aabb.cc00.0300 priority 4098
          port   Et0/3      cost 2000000
```

```
Interface  Role Sts Cost
```

```
-----
```

```
Et0/2      Altn BLK 2000000
```

```
Et0/3      Root FWD 2000000
```

Команда *show interfaces trunk* підтвердила, що у forwarding state для Ethernet0/2 перебували VLAN 10, 20 і 99, а для Ethernet0/3 – VLAN 30 і 40.

Розподіл VLAN між trunk-портами SW3 до аварії MSTP:

```
SW3#show interfaces trunk
```

```
Port      Vlans in spanning tree forwarding state and not pruned
```

```
Et0/2      10,20,99
```

```
Et0/3      30,40
```

Wireshark Capture додатково підтвердив цей стан: ICMP-трафік VLAN 10 проходив через інтерфейс SW3–SW1, що показано на рисунку 3.6, а ICMP-трафік VLAN 30 – через інтерфейс SW3–SW2, що підтверджено на рисунку 3.7.

No.	Time	Source	Destination	Protocol	Length	Info
761	101.177668	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x1c84, seq=77/19712, ttl=255 (request in 760)
768	102.204638	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x1d84, seq=78/19968, ttl=64 (reply in 769)
769	102.205964	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x1d84, seq=78/19968, ttl=255 (request in 768)
776	103.225677	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x1e84, seq=79/20224, ttl=64 (reply in 777)
777	103.230768	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x1e84, seq=79/20224, ttl=255 (request in 776)
784	104.242343	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x1f84, seq=80/20480, ttl=64 (reply in 785)
785	104.255614	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x1f84, seq=80/20480, ttl=255 (request in 784)
792	105.266803	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2084, seq=81/20736, ttl=64 (reply in 793)
793	105.278447	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2084, seq=81/20736, ttl=255 (request in 792)
800	106.286308	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2184, seq=82/20992, ttl=64 (reply in 801)
801	106.293337	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2184, seq=82/20992, ttl=255 (request in 800)
807	107.301888	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2284, seq=83/21248, ttl=64 (reply in 808)
808	107.305548	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2284, seq=83/21248, ttl=255 (request in 807)
815	108.321007	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2384, seq=84/21504, ttl=64 (reply in 816)
816	108.325489	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2384, seq=84/21504, ttl=255 (request in 815)
822	109.341137	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2484, seq=85/21760, ttl=64 (reply in 824)
824	109.352455	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2484, seq=85/21760, ttl=255 (request in 822)
832	110.360353	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2584, seq=86/22016, ttl=64 (reply in 833)
833	110.366145	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2584, seq=86/22016, ttl=255 (request in 832)
839	111.381501	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2684, seq=87/22272, ttl=64 (reply in 840)
840	111.385997	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2684, seq=87/22272, ttl=255 (request in 839)
848	112.398132	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2784, seq=88/22528, ttl=64 (reply in 849)
849	112.403350	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2784, seq=88/22528, ttl=255 (request in 848)
855	113.415271	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2884, seq=89/22784, ttl=64 (reply in 856)
856	113.418978	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2884, seq=89/22784, ttl=255 (request in 855)
865	114.434907	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2984, seq=90/23040, ttl=64 (reply in 866)
866	114.442497	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2984, seq=90/23040, ttl=255 (request in 865)
872	115.455872	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2a84, seq=91/23296, ttl=64 (reply in 873)
873	115.465259	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2a84, seq=91/23296, ttl=255 (request in 872)
880	116.471012	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2b84, seq=92/23552, ttl=64 (reply in 881)
881	116.480911	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2b84, seq=92/23552, ttl=255 (request in 880)
887	117.491091	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2c84, seq=93/23808, ttl=64 (reply in 888)
888	117.494041	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2c84, seq=93/23808, ttl=255 (request in 887)
895	118.513535	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2d84, seq=94/24064, ttl=64 (reply in 896)
896	118.523182	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2d84, seq=94/24064, ttl=255 (request in 895)
903	119.534367	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x2f84, seq=95/24320, ttl=64 (reply in 904)
904	119.544465	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x2f84, seq=95/24320, ttl=255 (request in 903)

Рис. 3.6 — ICMP-трафік VLAN 10 на інтерфейсі SW3–SW1 до аварії MSTP

No.	Time	Source	Destination	Protocol	Length	Info
76	11.964095	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xd183, seq=1/256, ttl=64 (reply in 77)
77	11.967713	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xd183, seq=1/256, ttl=255 (request in 76)
83	12.984799	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xd283, seq=2/512, ttl=64 (reply in 84)
84	12.988931	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xd283, seq=2/512, ttl=255 (request in 83)
92	14.009273	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xd383, seq=3/768, ttl=64 (reply in 93)
93	14.012567	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xd383, seq=3/768, ttl=255 (request in 92)
100	15.031741	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xd483, seq=4/1024, ttl=64 (reply in 101)
101	15.034610	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xd483, seq=4/1024, ttl=255 (request in 100)
108	16.052835	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xd583, seq=5/1280, ttl=64 (reply in 109)
109	16.055918	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xd583, seq=5/1280, ttl=255 (request in 108)
115	17.071950	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xd683, seq=6/1536, ttl=64 (reply in 116)
116	17.078390	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xd683, seq=6/1536, ttl=255 (request in 115)
123	18.090704	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xd783, seq=7/1792, ttl=64 (reply in 124)
124	18.093531	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xd783, seq=7/1792, ttl=255 (request in 123)
133	19.108627	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xd883, seq=8/2048, ttl=64 (reply in 134)
134	19.113080	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xd883, seq=8/2048, ttl=255 (request in 133)
141	20.128476	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xd983, seq=9/2304, ttl=64 (reply in 142)
142	20.130796	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xd983, seq=9/2304, ttl=255 (request in 141)
149	21.148773	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xda83, seq=10/2560, ttl=64 (reply in 149)
149	21.151684	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xda83, seq=10/2560, ttl=255 (request in 148)
157	22.166851	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xdb83, seq=11/2816, ttl=64 (reply in 158)
158	22.174188	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xdb83, seq=11/2816, ttl=255 (request in 157)
164	23.191074	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xdc83, seq=12/3072, ttl=64 (reply in 165)
165	23.195930	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xdc83, seq=12/3072, ttl=255 (request in 164)
174	24.211982	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xdd83, seq=13/3328, ttl=64 (reply in 175)
175	24.214770	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xdd83, seq=13/3328, ttl=255 (request in 174)
182	25.230332	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xde83, seq=14/3584, ttl=64 (reply in 183)
183	25.233977	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xde83, seq=14/3584, ttl=255 (request in 182)
190	26.247479	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xdf83, seq=15/3840, ttl=64 (reply in 191)
191	26.250927	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xdf83, seq=15/3840, ttl=255 (request in 190)
197	27.265488	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xe083, seq=16/4096, ttl=64 (reply in 198)
198	27.267852	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xe083, seq=16/4096, ttl=255 (request in 197)
205	28.285460	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xe183, seq=17/4352, ttl=64 (reply in 206)
206	28.290181	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xe183, seq=17/4352, ttl=255 (request in 205)
212	29.307067	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xe283, seq=18/4608, ttl=64 (reply in 213)
213	29.310151	192.168.30.1	192.168.30.10	ICMP	102	Echo (ping) reply id=0xe283, seq=18/4608, ttl=255 (request in 212)
220	30.325544	192.168.30.10	192.168.30.1	ICMP	102	Echo (ping) request id=0xe383, seq=19/4864, ttl=64 (reply in 221)

Рис. 3.7 — ICMP-трафік VLAN 30 на інтерфейсі SW3–SW2 до аварії MSTP

Для перевірки реакції MSTP було змодельовано відмову активного uplink-з'єднання для MST1. Оскільки до аварії MST1 використовував Ethernet0/2 на SW3 як Root Port у напрямку SW1, саме цей інтерфейс було адміністративно вимкнено:

```

conf t
interface Ethernet0/2
shutdown
end

```

Після вимкнення Ethernet0/2, MST1 instance перебудував активний шлях: порт Ethernet0/3 на SW3 став Root/Forwarding для VLAN 10, VLAN 20 і VLAN 99. Вартість шляху до root bridge SW1 збільшилася до 3000000, оскільки новий шлях проходить через SW2 та Port-channel1. MST2 при цьому не потребував суттєвої перебудови, оскільки до аварії вже використовував Ethernet0/3 як активний шлях до root bridge SW2.

```
SW3#show spanning-tree mst 1
```

```
##### MST1   vlans mapped:  10,20,99
```

```
Root      address aabb.cc00.0100 priority 4097
          port   Et0/3      cost 3000000
```

Interface	Role	Sts	Cost
Et0/3	Root	FWD	2000000

```
SW3#show spanning-tree mst 2
```

```
##### MST2   vlans mapped:  30,40
```

```
Root      address aabb.cc00.0300 priority 4098
          port   Et0/3      cost 2000000
```

Interface	Role	Sts	Cost
Et0/3	Root	FWD	2000000

Після аварії команда `show interfaces trunk` показала, що всі досліджувані VLAN перейшли у forwarding state через Ethernet0/3.

```
SW3#show interfaces trunk
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Et0/3     10,20,30,40,99
```

Після відмови Ethernet0/2 Wireshark Capture показав перехід ICMP-трафіку VLAN 10 на інтерфейс SW3–SW2, що наведено на рисунку 3.8. Тобто VLAN 10 з MST1 почав використовувати той самий фізичний uplink, який VLAN 30 з MST2 використовував ще до аварії.

No.	Time	Source	Destination	Protocol	Length	Info
830	107.289007	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3184, seq=97/24832, ttl=64 (reply in 831)
831	107.292419	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3184, seq=97/24832, ttl=255 (request in 830)
842	108.311427	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3284, seq=98/25088, ttl=64 (reply in 843)
843	108.313625	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3284, seq=98/25088, ttl=255 (request in 842)
854	109.332563	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3384, seq=99/25344, ttl=64 (reply in 855)
855	109.338870	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3384, seq=99/25344, ttl=255 (request in 854)
866	110.351189	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3484, seq=100/25600, ttl=64 (reply in 867)
867	110.358758	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3484, seq=100/25600, ttl=255 (request in 866)
875	111.368253	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3584, seq=101/25856, ttl=64 (reply in 876)
876	111.372423	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3584, seq=101/25856, ttl=255 (request in 875)
885	112.391298	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3684, seq=102/26112, ttl=64 (reply in 886)
886	112.394721	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3684, seq=102/26112, ttl=255 (request in 885)
894	113.414239	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3784, seq=103/26368, ttl=64 (reply in 895)
895	113.418831	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3784, seq=103/26368, ttl=255 (request in 894)
904	114.433073	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3884, seq=104/26624, ttl=64 (reply in 905)
905	114.435825	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3884, seq=104/26624, ttl=255 (request in 904)
914	115.453455	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3984, seq=105/26880, ttl=64 (reply in 915)
915	115.457779	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3984, seq=105/26880, ttl=255 (request in 914)
924	116.471249	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3a84, seq=106/27136, ttl=64 (reply in 925)
925	116.474574	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3a84, seq=106/27136, ttl=255 (request in 924)
933	117.487963	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3b84, seq=107/27392, ttl=64 (reply in 934)
934	117.498409	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3b84, seq=107/27392, ttl=255 (request in 933)
944	118.510794	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3c84, seq=108/27648, ttl=64 (reply in 945)
945	118.517656	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3c84, seq=108/27648, ttl=255 (request in 944)
954	119.541524	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3d84, seq=109/27904, ttl=64 (reply in 955)
955	119.550466	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3d84, seq=109/27904, ttl=255 (request in 954)
965	120.560918	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3e84, seq=110/28160, ttl=64 (reply in 966)
966	120.564545	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3e84, seq=110/28160, ttl=255 (request in 965)
975	121.581290	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x3f84, seq=111/28416, ttl=64 (reply in 976)
976	121.588149	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x3f84, seq=111/28416, ttl=255 (request in 975)
985	122.601512	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x4084, seq=112/28672, ttl=64 (reply in 986)
986	122.607228	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x4084, seq=112/28672, ttl=255 (request in 985)
994	123.621392	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x4184, seq=113/28928, ttl=64 (reply in 995)
995	123.624141	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x4184, seq=113/28928, ttl=255 (request in 994)
1004	124.652895	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x4284, seq=114/29184, ttl=64 (reply in 1005)
1005	124.658433	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x4284, seq=114/29184, ttl=255 (request in 1004)
1014	125.668719	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x4384, seq=115/29440, ttl=64 (reply in 1015)

Рис. 3.8 — Перехід ICMP-трафіку VLAN 10 на інтерфейс SW3–SW2 після відмови Ethernet0/2 у MSTP

У збережених фрагментах ICMP-перевірки з PC1 і PC4 не зафіксовано повідомлень timeout або пропусків послідовності icmp_seq. Це свідчить, що в межах використаного методу перевірки аварія uplink-з'єднання не проявилася як втрата ICMP-пакетів. Водночас, як і в попередньому експерименті, стандартний ping не дозволяє точно виміряти короткочасні перерви між ICMP-запитами.

Порівняння результатів Rapid-PVST/RSTP і MSTP показує різницю між цими підходами. У тесті Rapid-PVST/RSTP VLAN 10, VLAN 20 і VLAN 99 мали однакову логіку проходження: до аварії через SW3–SW1, після аварії через SW3–SW2. У тесті MSTP VLAN були поділені на дві групи: MST1 використовував активний шлях через SW1, а MST2 – через SW2. Після відмови Ethernet0/2 перебудовувався шлях для MST1, тоді як MST2 продовжував використовувати Ethernet0/3.

За результатами проведених тестів зміна стандартних таймерів Rapid-PVST/RSTP або MSTP для цієї топології не є необхідною. У конфігурації використовувалися базові значення Hello Time – 2 с, Max Age – 20 с, Forward Delay – 15 с. У сценаріях прямого вимкнення активного uplink-порту комутатори реагували на зміну фізичного стану інтерфейсу, тому в межах збережених ICMP-фрагментів втрати пакетів не зафіксовано. Більш доцільним способом підвищення

передбачуваності роботи L2-домену є правильне призначення root bridge, узгодження trunk-з'єднань, контроль allowed VLAN і перевірка фактичного шляху трафіку за допомогою Wireshark Capture.

Таким чином, Rapid-PVST/RSTP у досліджуваній топології забезпечив переведення VLAN 10, VLAN 20 і VLAN 99 на резервний uplink після відмови основного шляху. MSTP додатково показав можливість групування VLAN в окремі MST- instance та використання різних активних шляхів ще до аварії. Це робить MSTP доцільним для мереж із кількома групами VLAN, де потрібно не лише резервування, а й більш керований розподіл L2-трафіку між trunk-з'єднаннями.

3.3 Дослідження роботи LACP при відмові фізичного каналу зв'язку

У цьому підрозділі досліджується робота LACP/EtherChannel при відмові одного фізичного каналу між комутаторами SW1 і SW2. На відміну від STP/RSTP/MSTP, які можуть блокувати резервні L2-шляхи для запобігання петлям, LACP об'єднує кілька фізичних інтерфейсів в один логічний канал Port-channel. Тому метою експерименту є перевірка того, чи залишиться логічний інтерфейс Port-channel1 активним після адміністративного вимкнення одного з його фізичних учасників.

У тестовій топології GNS3 агрегований канал було налаштовано між комутаторами SW1 та SW2. До складу логічного інтерфейсу Port-channel1 входять два фізичні з'єднання:

SW1 Ethernet0/1 — SW2 Ethernet0/1

SW1 Ethernet0/2 — SW2 Ethernet0/2

На обох комутаторах фізичні інтерфейси працюють у режимі LACP active. Логічний інтерфейс Port-channel1 налаштований як trunk-з'єднання і в межах цього експерименту передає VLAN 10, VLAN 20 і VLAN 99.

Перед створенням аварії було перевірено початковий стан EtherChannel на SW1 і SW2 за допомогою команд:

```
show etherchannel summary
show interfaces port-channel 1
show interfaces trunk
show lacp neighbor
```

Фрагмент виводу команди `show etherchannel summary` на SW1 до аварії мав такий вигляд:

Group	Port-channel	Protocol	Ports
1	Po1(SU)	LACP	Et0/1(P) Et0/2(P)

Позначення Po1(SU) означає, що Port-channel1 є L2-агрегованим каналом і використовується в роботі. Символ (P) біля Et0/1 та Et0/2 показує, що обидва фізичні порти успішно включені до складу агрегованого каналу.

Команда `show interfaces port-channel 1` додатково підтвердила, що логічний інтерфейс перебуває у стані up/up, а його членами є два фізичні інтерфейси:

```
Port-channel1 is up, line protocol is up (connected)
Members in this channel: Et0/1 Et0/2
BW 20000 Kbit/sec
```

Аналогічний стан було зафіксовано і на SW2:

Group	Port-channel	Protocol	Ports
1	Po1(SU)	LACP	Et0/1(P) Et0/2(P)

Також було перевірено trunk-режим роботи Port-channel1. Команда `show interfaces trunk` підтвердила, що Po1 працює як trunk-з'єднання та пропускає VLAN 10, VLAN 20 і VLAN 99:

Port	Mode	Encapsulation	Status	Native vlan
Po1	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Po1	10,20,99			
Port	Vlans allowed and active in management domain			
Po1	10,20,99			

Port Vlans in spanning tree forwarding state and not pruned
Po1 10,20,99

Для додаткового підтвердження роботи LACP було використано Wireshark Capture на фізичних каналах між SW1 і SW2. У фільтрі `lasp || icmp` відображалися службові LACPDU-кадри та ICMP-трафік, який використовувався для перевірки доступності. До аварії у захопленні були присутні LACP / Slow Protocols, а також ICMP Echo Request та Echo Reply між PC1 192.168.10.10 і маршрутизатором 192.168.10.3, що показано на рисунку 3.1.

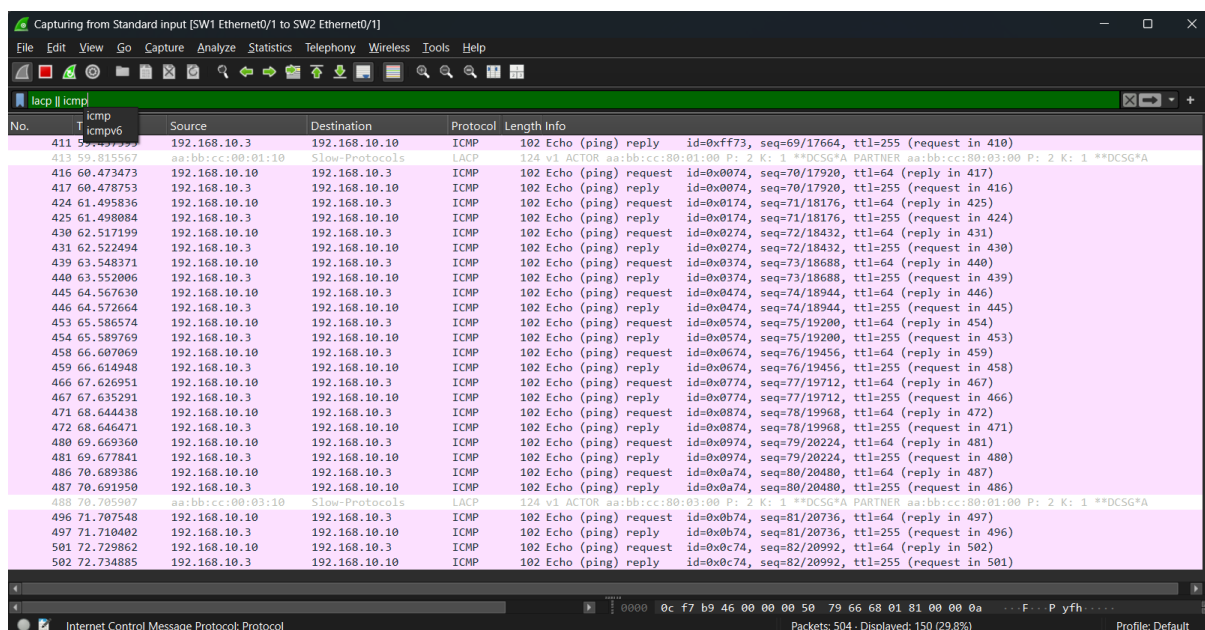


Рис. 3.1 — Захоплення LACPDU та ICMP-трафіку на інтерфейсі між SW1 і SW2 до аварії

Окремо було зафіксовано службові LACPDU-кадри з фільтром `lasp` на інтерфейсі `ethernet0/2`. Їх наявність підтверджує, що комутатори SW1 і SW2 обмінюються службовими повідомленнями LACP для узгодження стану фізичних учасників агрегованого каналу. Результат захоплення наведено на рисунку 3.2.

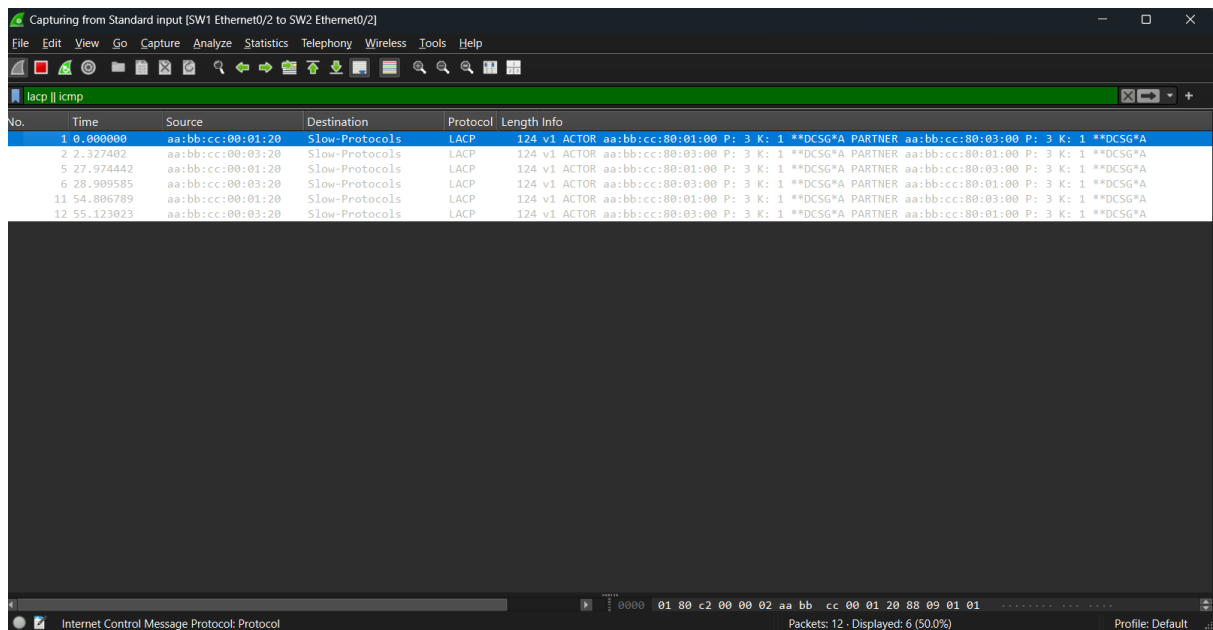


Рис. 3.2 — Службові LACPDU-кадри між SW1 і SW2 у Wireshark через порт eth0/2

Для створення аварійного сценарію на SW1 було адміністративно вимкнено один фізичний інтерфейс, який входив до складу Port-channel1:

```
conf t
```

```
interface Ethernet0/1
```

```
shutdown
```

```
end
```

Після вимкнення Ethernet0/1 було повторно перевірено стан EtherChannel. На SW1 команда `show etherchannel summary` показала, що Port-channel1 залишився активним, але Ethernet0/1 більше не бере участі в роботі агрегованого каналу:

```
SW1#show etherchannel summary
```

```
Group Port-channel Protocol Ports
```

```
-----+-----+-----+-----+
1          Po1(SU)    LACP    Et0/1(D)    Et0/2(P)
```

Позначення (D) біля Et0/1 показує, що цей фізичний порт перебуває у стані down. Водночас Et0/2(P) залишився активним учасником Port-channel1.

Команда `show interfaces port-channel 1` підтвердила, що логічний інтерфейс не перейшов у стан down:

```
SW1#show interfaces port-channel 1
```

```
Port-channel1 is up, line protocol is up (connected)
```

```
Members in this channel: Et0/2
```

```
BW 10000 Kbit/sec
```

Порівняно з початковим станом кількість активних фізичних членів Port-channel1 зменшилася з двох до одного. Відображена пропускна здатність також зменшилася з BW 20000 Kbit/sec до BW 10000 Kbit/sec. Це означає, що відбулася не повна відмова міжкомутаторного каналу, а його часткова деградація.

На SW2 після аварії було зафіксовано аналогічний стан:

```
Group Port-channel Protocol Ports
```

```
-----+-----+-----+-----+
1      Po1(SU)    LACP    Et0/1(s)    Et0/2(P)
```

У цьому випадку Et0/1(s) показує, що порт більше не бере активної участі у роботі агрегованого каналу, тоді як Et0/2(P) залишається активним учасником. Команда show interfaces port-channel 1 на SW2 також підтвердила, що Port-channel1 залишився у стані up/up, а його єдиним активним членом став Et0/2:

```
SW2#show interfaces port-channel 1
```

```
Port-channel1 is up, line protocol is up (connected)
```

```
Members in this channel: Et0/2
```

```
BW 10000 Kbit/sec
```

Додатково було перевірено trunk-режим роботи Po1 після аварії. Команда show interfaces trunk на SW1 і SW2 показала, що Port-channel1 залишився trunk-з'єднанням і продовжив пропускати VLAN 10, VLAN 20 і VLAN 99:

Port	Mode	Encapsulation	Status	Native vlan
Po1	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Po1	10,20,99			
Port	Vlans allowed and active in management domain			
Po1	10,20,99			

Port Vlans in spanning tree forwarding state and not pruned
Po1 10,20,99

Отже, за консольними виводами було підтверджено, що після відмови одного фізичного каналу агрегований канал Port-channel1 не перейшов у стан down. Передавання VLAN 10, 20 і 99 через логічний trunk-інтерфейс збереглося.

Після створення аварійної ситуації захоплення трафіку було повторено на другому фізичному інтерфейсі Ethernet0/2, який залишився активним у складі Port-channel1. Результат наведено на рисунку 3.3.

No.	Time	Source	Destination	Protocol	Length	Info
194	111.083477	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x3a74, seq=112/28672, ttl=64 (no response found!)
200	111.842791	aa:bb:cc:00:01:20	Slow-Protocols	LACP	124	v1 ACTOR aa:bb:cc:00:01:00 P: 3 K: 1 **DCSG*A PARTNER aa:bb:cc:00:03:00 P: 3 K: 1 **DCSG*A
205	113.082312	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x3c74, seq=113/28928, ttl=64 (no response found!)
215	115.079242	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x3e74, seq=114/29184, ttl=64 (no response found!)
225	117.079242	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x4074, seq=115/29440, ttl=64 (no response found!)
235	119.080689	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x4274, seq=116/29696, ttl=64 (no response found!)
246	121.080686	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x4474, seq=117/29952, ttl=64 (no response found!)
258	123.092384	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x4674, seq=118/30208, ttl=64 (no response found!)
268	125.089944	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x4874, seq=119/30464, ttl=64 (no response found!)
280	127.086623	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x4a74, seq=120/30720, ttl=64 (no response found!)
290	129.089335	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x4c74, seq=121/30976, ttl=64 (no response found!)
301	131.136781	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x4e74, seq=122/31232, ttl=64 (no response found!)
312	133.222538	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x5074, seq=123/31488, ttl=64 (no response found!)
323	135.237327	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x5274, seq=124/31744, ttl=64 (reply in 324)
324	135.242875	192.168.10.3	192.168.10.10	ICMP	102	Echo (ping) reply id=0x5374, seq=124/31744, ttl=255 (request in 323)
331	136.257387	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x5474, seq=125/32000, ttl=64 (reply in 332)
332	136.261775	192.168.10.3	192.168.10.10	ICMP	102	Echo (ping) reply id=0x5474, seq=125/32000, ttl=255 (request in 331)
336	137.278953	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x5574, seq=126/32256, ttl=64 (reply in 337)
337	137.281475	192.168.10.3	192.168.10.10	ICMP	102	Echo (ping) reply id=0x5574, seq=126/32256, ttl=255 (request in 336)
342	137.756935	aa:bb:cc:00:03:20	Slow-Protocols	LACP	124	v1 ACTOR aa:bb:cc:00:03:00 P: 3 K: 1 **DCSG*A PARTNER aa:bb:cc:00:01:00 P: 3 K: 1 **DCSG*A
345	138.297393	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x5674, seq=127/32512, ttl=64 (reply in 346)
346	138.301600	192.168.10.3	192.168.10.10	ICMP	102	Echo (ping) reply id=0x5674, seq=127/32512, ttl=255 (request in 345)
350	138.846487	aa:bb:cc:00:01:20	Slow-Protocols	LACP	124	v1 ACTOR aa:bb:cc:00:01:00 P: 3 K: 1 **DCSG*A PARTNER aa:bb:cc:00:03:00 P: 3 K: 1 **DCSG*A
352	139.315503	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x5774, seq=128/32768, ttl=64 (reply in 353)
353	139.319418	192.168.10.3	192.168.10.10	ICMP	102	Echo (ping) reply id=0x5774, seq=128/32768, ttl=255 (request in 352)
361	140.335865	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x5874, seq=129/33024, ttl=64 (reply in 362)
362	140.339738	192.168.10.3	192.168.10.10	ICMP	102	Echo (ping) reply id=0x5874, seq=129/33024, ttl=255 (request in 361)
367	141.355768	192.168.10.10	192.168.10.3	ICMP	102	Echo (ping) request id=0x5974, seq=130/33280, ttl=64 (reply in 368)
368	141.361305	192.168.10.3	192.168.10.10	ICMP	102	Echo (ping) reply id=0x5974, seq=130/33280, ttl=255 (request in 367)

Рис. 3.3 — Передавання ICMP-трафіку через активний фізичний канал після відмови одного учасника Port-channel1

З рисунка 3.3 видно, що після відмови одного фізичного каналу ICMP-трафік між 192.168.10.10 та 192.168.10.3 продовжує передаватися через активний фізичний канал. Це підтверджує, що після перебудови складу EtherChannel логічний інтерфейс Port-channel1 не був повністю втрачений, а трафік продовжив передаватися через другий фізичний інтерфейс. Також на рисунку видно, що після завершення перебудови агрегованого каналу ICMP Echo Request та Echo Reply між 192.168.10.10 і 192.168.10.3 знову проходять через міжкомутаторну ділянку мережі. Отриманий результат показує, що в момент зміни складу Port-channel1

можлива короткочасна втрата ICMP-відповідей, однак після виключення несправного фізичного інтерфейсу з агрегованого каналу зв'язність відновлюється через інший активний фізичний інтерфейс.

Для перевірки доступності після створення аварії було використано довготривалу ICMP-перевірку з PC1 до адреси 192.168.10.3. Під час тесту було зафіксовано, що до моменту аварії ICMP-відповіді надходили стабільно. Після вимкнення одного фізичного інтерфейсу з'явилася короткочасна серія втрат:

192.168.10.3 icmp_seq=96 timeout

192.168.10.3 icmp_seq=97 timeout

...

192.168.10.3 icmp_seq=123 timeout

Після цього доступність вузла відновилося:

84 bytes from 192.168.10.3 icmp_seq=124 ttl=255 time=7.332 ms

84 bytes from 192.168.10.3 icmp_seq=125 ttl=255 time=5.559 ms

84 bytes from 192.168.10.3 icmp_seq=126 ttl=255 time=4.653 ms

Таким чином, LACP не гарантує повної відсутності втрат пакетів у момент аварійної події, але дозволяє зберегти логічну зв'язність між SW1 і SW2 після завершення перебудови EtherChannel. Порівняння стану EtherChannel до і після аварії наведено в таблиці 3.1.

Таблиця 3.1 — Порівняння стану EtherChannel до і після аварії

Параметр	До аварії	Після відмови одного фізичного каналу
Port-channel1	up/up, trunking	up/up, trunking
Ethernet0/1	active member, (P)	down / suspended, неактивний учасник
Ethernet0/2	active member, (P)	active member, (P)
VLAN 10/20/99	allowed / active / forwarding	allowed / active / forwarding
Кількість активних фізичних каналів	2	1

Продовження таблиці 3.1

Відображена пропускна здатність	BW 20000 Kbit/sec	BW 10000 Kbit/sec
ICMP-доступність	є	короткочасні втрати, потім відновлення
Характер відмови	немає	часткова деградація каналу

Для коректної роботи EtherChannel важливо, щоб фізичні інтерфейси мали однакові параметри на обох комутаторах: режим LACP, належність до однієї channel-group, trunk-режим, дозволені VLAN, швидкість і duplex-режим. У межах експерименту було підтверджено, що Port-channel1 працює через LACP, фізичні порти Ethernet0/1 та Ethernet0/2 входять до channel-group 1, а логічний інтерфейс Po1 зберігає trunk-режим до і після аварії.

Проведений експеримент показав, що після відмови одного фізичного учасника агрегований інтерфейс Port-channel1 залишився активним за рахунок другого фізичного каналу. Це підтверджено станом Po1(SU), наявністю активного учасника Et0/2(P), збереженням trunk-режиму та відновленням ICMP-доступності. Водночас відмова одного фізичного каналу зменшила сумарну доступну пропускну здатність агрегованого каналу з BW 20000 Kbit/sec до BW 10000 Kbit/sec. Отже, LACP забезпечив не миттєве або безвтратне перемикавання, а збереження логічної зв'язності між SW1 і SW2 за умови, що в Port-channel залишився хоча б один активний фізичний учасник.

3.4 Дослідження роботи VRRP при відмові основного шлюзу

У цьому підрозділі досліджується робота VRRP під час відмови основного шлюзу за замовчуванням. На відміну від протоколів канального рівня, які забезпечують резервування L2-шляхів або агрегованих каналів, VRRP використовується для резервування шлюзу на мережевому рівні. У практичній частині досліджено саме VRRP як відкритий стандартний механізм FHRP. HSRP і GLBP були розглянуті в аналітичному розділі 2, але окремо в GNS3 не

моделювалися.

У тестовій топології маршрутизатори R1 і R2 виконують роль резервованої пари шлюзів для VLAN 10, VLAN 20 і VLAN 99. Кінцеві вузли використовують не фізичні IP-адреси маршрутизаторів, а віртуальні адреси шлюзів: для VLAN 10 – 192.168.10.1, для VLAN 20 – 192.168.20.1, для VLAN 99 – 192.168.99.1. У штатному режимі R1 має VRRP priority 110 і виконує роль Master, а R2 з priority 100 перебуває у стані Backup.

R1#show vrrp brief

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Gi0/0.10	10	110	3570	Y	Master	192.168.10.2	192.168.10.1	
Gi0/0.20	20	110	3570	Y	Master	192.168.20.2	192.168.20.1	
Gi0/0.99	99	110	3570	Y	Master	192.168.99.2	192.168.99.1	

R2#show vrrp brief

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Gi0/0.10	10	100	3609	Y	Backup	192.168.10.2	192.168.10.1	
Gi0/0.20	20	100	3609	Y	Backup	192.168.20.2	192.168.20.1	
Gi0/0.99	99	100	3609	Y	Backup	192.168.99.2	192.168.99.1	

З наведеного виводу видно, що до аварії R1 обслуговує віртуальні шлюзи для VLAN 10, VLAN 20 і VLAN 99. R2 бачить R1 як активний маршрутизатор і перебуває у стані Backup. Це відповідає початковій логіці резервування: основний gateway працює на R1, а R2 готовий перебрати його роль у разі відмови.

Для створення аварійного сценарію на R1 було адміністративно вимкнено інтерфейс GigabitEthernet0/0, який використовується як trunk-підключення R1 до комутованої частини топології, тому його вимкнення імітує втрату основного шлюзу для VLAN 10, VLAN 20 і VLAN 99.

Створення аварії на R1

R1#conf t

R1(config)#interface GigabitEthernet0/0

```
R1(config-if)#shutdown
```

```
R1(config-if)#end
```

Після виконання команди *shutdown* у журналі R1 було зафіксовано перехід VRRP-груп зі стану Master у стан Init, а також зміну стану інтерфейсу GigabitEthernet0/0 на administratively down. Це означає, що R1 більше не може виконувати роль активного шлюзу для відповідних VLAN.

Стан VRRP після аварії підтверджує, що R1 втратив активну роль, а R2 став Master для всіх трьох груп.

Стан VRRP після аварії

```
R1#show vrrp brief
```

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Gi0/0.10	10	110	3570	Y	Init	0.0.0.0	192.168.10.1	
Gi0/0.20	20	110	3570	Y	Init	0.0.0.0	192.168.20.1	
Gi0/0.99	99	110	3570	Y	Init	0.0.0.0	192.168.99.1	

```
R2#show vrrp brief
```

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Gi0/0.10	10	100	3609	Y	Master	192.168.10.3	192.168.10.1	
Gi0/0.20	20	100	3609	Y	Master	192.168.20.3	192.168.20.1	
Gi0/0.99	99	100	3609	Y	Master	192.168.99.3	192.168.99.1	

Після аварії фізичний маршрутизатор, який обслуговує gateway, змінився з R1 на R2. При цьому віртуальні IP-адреси шлюзів для кінцевих вузлів залишилися незмінними: 192.168.10.1, 192.168.20.1 і 192.168.99.1. Це є основною перевагою VRRP для клієнтських пристроїв, оскільки їхні налаштування gateway не потребують зміни.

Для перевірки доступності було використано ICMP-перевірку з кінцевого вузла PC3 до віртуального шлюзу VLAN 99 – 192.168.99.1. Ping було запущено до аварії та залишено активним під час перемикання.

Фрагмент ICMP-перевірки під час перемикання VRRP

```
84 bytes from 192.168.99.1 icmp_seq=100 ttl=255 time=9.419 ms
```

```
84 bytes from 192.168.99.1 icmp_seq=101 ttl=255 time=10.714 ms
```

84 bytes from 192.168.99.1 icmp_seq=102 ttl=255 time=9.053 ms

192.168.99.1 icmp_seq=103 timeout

84 bytes from 192.168.99.1 icmp_seq=104 ttl=255 time=41.233 ms

84 bytes from 192.168.99.1 icmp_seq=105 ttl=255 time=10.463 ms

84 bytes from 192.168.99.1 icmp_seq=106 ttl=255 time=5.205 ms

У збереженому фрагменті ICMP-перевірки зафіксовано короточасну втрату одного ICMP-пакета на icmp_seq=103. Після цього відповіді від віртуального шлюзу відновилися, починаючи з icmp_seq=104. Такий результат підтверджує, що VRRP забезпечив відновлення доступності gateway після переходу ролі Master на R2. Водночас цей результат не слід трактувати як точний вимір часу перемикання, оскільки стандартний ping не є інструментом високоточного вимірювання збіжності протоколу.

Додатково поведінку VRRP було перевірено за допомогою Wireshark Capture. До аварії на інтерфейсі R1–SW1 фіксувалися VRRP Announcement від адрес маршрутизатора R1 для VLAN 10, VLAN 20 і VLAN 99, що показано на рисунку 3.1. Після аварії на інтерфейсі R2–SW2 були зафіксовані VRRP Announcement уже від адрес маршрутизатора R2. Також після переходу ролі Master у захопленні було видно Gratuitous ARP для віртуальних шлюзів, що наведено на рисунку 3.2. Це підтверджує оновлення інформації про активний віртуальний gateway у L2-домени.

No.	Time	Source	Destination	Protocol	Length	Info
676	128.592238	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x59c0, seq=11/2816, ttl=255 (request in 675)
677	128.715511	192.168.10.2	224.0.0.18	VRRP	64	Announcement (v2)
678	128.798018	192.168.20.2	224.0.0.18	VRRP	64	Announcement (v2)
679	128.803362	192.168.99.2	224.0.0.18	VRRP	64	Announcement (v2)
683	129.587698	192.168.10.2	224.0.0.18	VRRP	64	Announcement (v2)
684	129.615991	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x5ac0, seq=12/3072, ttl=64 (reply in 685)
685	129.619870	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x5ac0, seq=12/3072, ttl=255 (request in 684)
686	129.737502	192.168.20.2	224.0.0.18	VRRP	64	Announcement (v2)
687	129.835517	192.168.99.2	224.0.0.18	VRRP	64	Announcement (v2)
688	130.510572	192.168.10.2	224.0.0.18	VRRP	64	Announcement (v2)
689	130.588421	192.168.20.2	224.0.0.18	VRRP	64	Announcement (v2)
690	130.681575	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x5bc0, seq=13/3328, ttl=64 (reply in 691)
691	130.685037	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x5bc0, seq=13/3328, ttl=255 (request in 690)
692	130.812356	192.168.99.2	224.0.0.18	VRRP	64	Announcement (v2)
696	131.640699	192.168.20.2	224.0.0.18	VRRP	64	Announcement (v2)
697	131.660526	192.168.10.2	224.0.0.18	VRRP	64	Announcement (v2)
698	131.701867	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x5cc0, seq=14/3584, ttl=64 (reply in 699)
699	131.705284	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x5cc0, seq=14/3584, ttl=255 (request in 698)
700	131.829137	192.168.99.2	224.0.0.18	VRRP	64	Announcement (v2)
701	132.669456	192.168.10.2	224.0.0.18	VRRP	64	Announcement (v2)
702	132.674838	192.168.20.2	224.0.0.18	VRRP	64	Announcement (v2)
703	132.722203	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x5dc0, seq=15/3840, ttl=64 (reply in 704)
704	132.724590	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x5dc0, seq=15/3840, ttl=255 (request in 703)
705	132.733964	192.168.99.2	224.0.0.18	VRRP	64	Announcement (v2)
709	133.579325	192.168.10.2	224.0.0.18	VRRP	64	Announcement (v2)
710	133.639107	192.168.99.2	224.0.0.18	VRRP	64	Announcement (v2)
711	133.655968	192.168.20.2	224.0.0.18	VRRP	64	Announcement (v2)
712	133.739188	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x5ec0, seq=16/4096, ttl=64 (reply in 713)
713	133.741252	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x5ec0, seq=16/4096, ttl=255 (request in 712)

Рис. 3.1 — VRRP Announcement до аварії від маршрутизатора R1

No.	Time	Source	Destination	Protocol	Length	Info
938	171.688522	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x88c0, seq=57/14592, ttl=64 (reply in 939)
939	171.691001	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x88c0, seq=57/14592, ttl=255 (request in 938)
940	171.851987	192.168.99.3	224.0.0.18	VRRP	64	Announcement (v2)
941	172.072090	192.168.10.3	224.0.0.18	VRRP	64	Announcement (v2)
945	172.627952	192.168.20.3	224.0.0.18	VRRP	64	Announcement (v2)
946	172.710994	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x89c0, seq=58/14848, ttl=64 (reply in 947)
947	172.715144	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x89c0, seq=58/14848, ttl=255 (request in 946)
948	172.734872	192.168.99.3	224.0.0.18	VRRP	64	Announcement (v2)
949	173.149823	192.168.10.3	224.0.0.18	VRRP	64	Announcement (v2)
950	173.565851	192.168.20.3	224.0.0.18	VRRP	64	Announcement (v2)
951	173.684365	192.168.99.3	224.0.0.18	VRRP	64	Announcement (v2)
952	173.746898	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x8ac0, seq=59/15104, ttl=64 (reply in 953)
953	173.751727	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x8ac0, seq=59/15104, ttl=255 (request in 952)
954	174.207059	192.168.10.3	224.0.0.18	VRRP	64	Announcement (v2)
955	174.494343	192.168.20.3	224.0.0.18	VRRP	64	Announcement (v2)
959	174.772569	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x8bc0, seq=60/15360, ttl=64 (reply in 961)
960	174.776982	192.168.99.3	224.0.0.18	VRRP	64	Announcement (v2)
961	174.785621	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x8bc0, seq=60/15360, ttl=255 (request in 959)
963	175.133629	192.168.10.3	224.0.0.18	VRRP	64	Announcement (v2)
964	175.400231	192.168.20.3	224.0.0.18	VRRP	64	Announcement (v2)
965	175.807399	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x8cc0, seq=61/15616, ttl=64 (reply in 966)
966	175.811295	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x8cc0, seq=61/15616, ttl=255 (request in 965)
967	175.842729	192.168.99.3	224.0.0.18	VRRP	64	Announcement (v2)
968	176.125969	192.168.10.3	224.0.0.18	VRRP	64	Announcement (v2)
969	176.493905	192.168.20.3	224.0.0.18	VRRP	64	Announcement (v2)
973	176.836089	192.168.99.50	192.168.99.1	ICMP	102	Echo (ping) request id=0x8dc0, seq=62/15872, ttl=64 (reply in 974)
974	176.841413	192.168.99.1	192.168.99.50	ICMP	102	Echo (ping) reply id=0x8dc0, seq=62/15872, ttl=255 (request in 973)
975	176.892666	192.168.99.3	224.0.0.18	VRRP	64	Announcement (v2)
976	177.216338	192.168.10.3	224.0.0.18	VRRP	64	Announcement (v2)

Рис. 3.2 — VRRP Announcement та Gratuitous ARP після переходу ролі Master на R2

Після завершення аварійного тесту було виконано відновлення основного маршрутизатора R1. Для цього інтерфейс GigabitEthernet0/0 було знову увімкнено командою *no shutdown*.

Після відновлення інтерфейсу R1 спочатку перейшов зі стану Init у Backup, а потім повернув собі роль Master для всіх трьох VRRP-груп. Це підтверджується системними повідомленнями та виводом *show vrrp brief*:

R1#show vrrp brief

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Gi0/0.10	10	110	3570	Y	Master		192.168.10.2	192.168.10.1
Gi0/0.20	20	110	3570	Y	Master		192.168.20.2	192.168.20.1
Gi0/0.99	99	110	3570	Y	Master		192.168.99.2	192.168.99.1

R2#show vrrp brief

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Gi0/0.10	10	100	3609	Y	Backup		192.168.10.2	192.168.10.1
Gi0/0.20	20	100	3609	Y	Backup		192.168.20.2	192.168.20.1
Gi0/0.99	99	100	3609	Y	Backup		192.168.99.2	192.168.99.1

Повернення ролі Master на R1 пояснюється тим, що R1 має вищий VRRP-пріоритет – 110, тоді як R2 використовує пріоритет 100. У виводі *show vrrp brief* також видно параметр Pre зі значенням Y, що вказує на можливість повернення активної ролі маршрутизатору з вищим пріоритетом після його відновлення.

Проведений експеримент показав, що VRRP забезпечує автоматичне перенесення ролі активного шлюзу на резервний маршрутизатор. При цьому кінцеві вузли не потребують зміни параметрів gateway, оскільки продовжують використовувати ту саму віртуальну IP-адресу. У разі відмови R1 роль Master для VLAN 10, VLAN 20 і VLAN 99 перейшла до R2, а після відновлення R1 активна роль повернулася на основний маршрутизатор. VRRP не усуває фізичну причину аварії, а лише зменшує її вплив на доступність шлюзу за замовчуванням. Зафіксована втрата одного ICMP-пакета показує, що під час перемикання можливе короткочасне порушення доступності. Крім того, коректна робота VRRP залежить від працездатності L2-топології, trunk-з'єднань, allowed VLAN і правильності адресації підінтерфейсів.

Отже, експеримент підтвердив працездатність VRRP як механізму резервування шлюзу за замовчуванням. До аварії R1 виконував роль Master, після

вимкнення основного інтерфейсу R1 резервний маршрутизатор R2 перейшов у стан Master, а після відновлення R1 активна роль повернулася на основний маршрутизатор. Це підтверджує доцільність використання VRRP у мережах електронних комунікацій для зменшення впливу відмови основного gateway на доступність користувацьких сервісів.

Висновки до розділу 3

Під час дослідження Rapid-PVST/RSTP було підтверджено перебудову L2-топології після відмови основного uplink-з'єднання SW3: після вимкнення Ethernet0/2 активним шляхом став Ethernet0/3 у напрямку SW2. MSTP додатково показав можливість групування VLAN у MST-instance та використання різних активних trunk-шляхів. Wireshark Capture підтвердив фактичну зміну напрямку трафіку, однак результати ping не слід трактувати як точний вимір часу збіжності.

У дослідженні LACP/EtherChannel встановлено, що після відмови одного фізичного учасника Port-channel1 між SW1 і SW2 логічний канал залишився працездатним за рахунок другого активного каналу. Це підтверджує здатність LACP підтримувати міжкомутаторну зв'язність при частковій відмові, хоча сумарна доступна пропускна здатність агрегованого каналу при цьому зменшується.

Під час перевірки VRRP було підтверджено резервування шлюзу за замовчуванням для VLAN 10, VLAN 20 і VLAN 99. Після вимкнення R1 його VRRP-групи перейшли у стан Init, а R2 став Master для тих самих віртуальних шлюзів. У збереженому фрагменті ICMP-перевірки зафіксовано короточасну втрату одного пакета з подальшим відновленням доступності. Після повторного ввімкнення R1 роль Master повернулася на основний маршрутизатор, а R2 знову перейшов у Backup.

Отже, практичне моделювання показало, що Rapid-PVST/RSTP і MSTP забезпечують перебудову L2-топології, LACP підтримує працездатність агрегованого каналу при відмові одного каналу, а VRRP резервує шлюз за

замовчуванням. Найкращий результат досягається завдяки поєднанню кількох механізмів, які працюють на різних рівнях мережевої інфраструктури.

ВИСНОВКИ

У дипломній роботі проаналізовано протоколи забезпечення відмовостійкості в мережах електронних комунікацій та виконано експериментальне дослідження їхньої поведінки в середовищі GNS3 на прикладі механізмів STP/RSTP, MSTP, LACP, VRRP та BFD. У роботі показано, що відмовостійкість мережі не може забезпечуватися одним окремим протоколом, оскільки різні механізми працюють на різних рівнях мережевої архітектури й вирішують різні задачі: запобігання петлям, резервування фізичних каналів, резервування шлюзу за замовчуванням і швидке виявлення втрати зв'язності.

У першому розділі було розглянуто теоретичні основи відмовостійкості мереж електронних комунікацій. Проаналізовано поняття відмови, простою, MTBF, MTTR і коефіцієнта готовності. Визначено, що зменшення часу простою залежить не тільки від надійності обладнання, а й від швидкості виявлення інциденту, діагностики, перемикання на резервний шлях і перевірки відновлення роботи. Тому підвищення готовності мережі потребує поєднання архітектурного резервування, коректного налаштування протоколів і механізмів швидкого виявлення відмов.

У другому розділі проаналізовано особливості протоколів, які забезпечують відмовостійкість на каналному та мережевому рівнях. STP запобігає петлям у надлишкових L2-топологіях, але має повільнішу збіжність через залежність від таймерів. RSTP/Rapid-PVST швидше реагує на зміну топології завдяки ролям портів і швидшому переходу резервного шляху в активний стан. MSTP дозволяє групувати VLAN у MST-інстанси та ефективніше використовувати резервні uplink-з'єднання. Установлено, що в практичних мережах важливіше правильно призначати Root Bridge, контролювати path cost, port priority, trunk-з'єднання та VLAN-параметри, ніж без потреби агресивно зменшувати STP-таймери.

Окремо розглянуто EtherChannel і LACP як механізми агрегації фізичних каналів. На відміну від STP, який блокує надлишкові шляхи для запобігання петлям, LACP об'єднує кілька фізичних лінків в один логічний Port-channel. Це

дозволяє підвищити сумарну пропускну здатність і зберегти зв'язність при відмові одного фізичного каналу. Водночас LACP не гарантує повної відсутності втрат пакетів у момент аварії та не замінює ні протоколи Spanning Tree, ні протоколи резервування шлюзу за замовчуванням.

Для резервування шлюзу за замовчуванням у роботі проаналізовано VRRP, HSRP і GLBP. VRRP є відкритим стандартним механізмом, який створює virtual router із virtual IP і virtual MAC, а вибір активного маршрутизатора виконується через ролі Master/Backup і параметр priority. HSRP виконує подібну функцію в Cisco-середовищі через ролі Active/Standby. GLBP додатково підтримує балансування навантаження між кількома шлюзами, що дозволяє не лише забезпечити резервування, а й ефективніше використовувати ресурси маршрутизаторів. Отже, FHRP-протоколи вирішують задачу, яку не можуть вирішити L2-механізми: збереження доступності gateway для кінцевих пристроїв.

Також у роботі розглянуто BFD, keepalive і timer-based failover як механізми швидкого виявлення відмов. BFD скорочує час виявлення втрати двонаправленої зв'язності та може прискорювати реакцію протоколів маршрутизації, зокрема OSPF. Keepalive і timer-based failover є простішими механізмами контролю доступності, але зазвичай менш гнучкі й повільніші за BFD. Водночас надто агресивне зменшення таймерів може спричиняти хибні спрацювання, особливо при короткочасних затримках, нестабільності каналу або перевантаженні обладнання.

У третьому розділі побудовано тестову топологію в середовищі GNS3 та перевірено поведінку протоколів у типових аварійних ситуаціях. Було досліджено роботу Rapid-PVST/RSTP і MSTP при зміні топології мережі, роботу LACP при відмові фізичного учасника агрегованого каналу, роботу VRRP при відмові основного шлюзу, а також роль BFD у швидкому виявленні втрати зв'язності. За результатами моделювання встановлено, що досліджені протоколи виконують різні, але взаємопов'язані функції: STP/RSTP/MSTP забезпечують L2-безпетльовість і резервні шляхи, LACP підтримує працездатність агрегованого

каналу, VRRP забезпечує перемикання шлюзу, а BFD прискорює виявлення аварії для подальшої реакції протоколів маршрутизації.

За результатами роботи сформовано практичні рекомендації щодо побудови відмовостійких мереж. Для L2-топологій доцільно заздалегідь визначати Root Bridge, контролювати ролі портів, trunk-з'єднання, allowed VLAN і native VLAN. Для міжкомутаторних з'єднань, де потрібно одночасно використовувати кілька фізичних каналів, доцільно застосовувати LACP замість незалежних паралельних лінків. Для збереження доступності шлюзу за замовчуванням необхідно використовувати FHRP-протоколи, зокрема VRRP, HSRP або GLBP залежно від середовища. Для критичних маршрутів, де важливий малий час виявлення відмови, доцільно застосовувати BFD. При цьому змінювати таймери протоколів потрібно лише за наявності технічного обґрунтування, оскільки надмірне їх зменшення може погіршити стабільність мережі.

Отримані результати можуть бути використані для навчального моделювання, попереднього тестування мережевих конфігурацій, обґрунтування вибору протоколів резервування та підготовки практичних рекомендацій для корпоративних і телекомунікаційних мереж. Перспективами подальших досліджень є перевірка розглянутих протоколів у більших топологіях, порівняння результатів моделювання з поведінкою реального обладнання, аналіз впливу різних значень таймерів на стабільність мережі та дослідження поєднання протоколів відмовостійкості з системами моніторингу й телеметрії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. European Union Agency for Cybersecurity (ENISA). Telecom Security Incidents 2024. ENISA Reports. 2025. URL:
<https://www.enisa.europa.eu/publications/telecom-security-incidents-2024> (дата звернення: 21.04.2026).
2. Donnellan D., Lawrence A., Weinschenk R. Annual outage analysis 2025: the causes and impacts of IT and data center outages. Uptime Intelligence report. May 2025. URL:
https://uptimeinstitute.com/uptime_assets/d7c049ef5b02a6e0a15540a3e5cb8fbf742c7fa54a1af6caaaaab32b7c15d443-GA-2025-05-annual-outage-analysis.pdf (дата звернення: 21.04.2026).
3. Opengear. The many costs of downtime: why minimizing outages must become a higher business priority. Research Commentary. 2022. URL:
<https://opengear.com/wp-content/uploads/2022/09/RC-TheManyCostsOfDowntime-GP-EN-092622.pdf> (дата звернення: 21.04.2026).
4. ITIC 2024 Hourly Cost of Downtime Survey Results by Laura DiDio -
<https://www.calyptix.com/wp-content/uploads/ITIC-2024-Hourly-Cost-of-Downtime-Survey-Results-Part-2.pdf> (дата звернення: 24.04.2026).
5. Out-of-Band Management: What It Is and Why You Need It. URL:
<https://zpesystems.com/defining-oob-network-and-oob-management/> (дата звернення: 24.04.2026).
6. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. Київ: Держстандарт України, 1994. URL: https://dnaop.com/html/2273/doc-%D0%94%D0%A1%D0%A2%D0%A3_2860-94 (дата звернення: 24.04.2026).
7. Erwood K. The True Costs of Downtime in 2025: A Deep Dive by Business Size and Industry. Erwood Group. 2025. URL:
<https://www.erwoodgroup.com/blog/the-true-costs-of-downtime-in-2025-a-deep-dive-by-business-size-and-industry/> (дата звернення: 24.04.2026).

8. National Security Agency. Performing Out-of-Band Network Management. Cybersecurity Information. September 2020. URL:
https://media.defense.gov/2020/Sep/17/2002499616/-1/-1/0/PERFORMING_OUT_OF_BAND_NETWORK_MANAGEMENT20200911.PDF (дата звернення: 26.04.2026).
9. IEEE 802.1Q-2022. IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks. IEEE, 2022. URL:
<https://standards.ieee.org/ieee/802.1Q/10323/> (дата звернення: 26.04.2026).
10. Juniper Networks. Aggregated Ethernet LACP for Switches. Junos OS Documentation. URL:
<https://www.juniper.net/documentation/us/en/software/junos/interfaces-ethernet-switches/topics/topic-map/aggregated-ethernet-lacp-switches.html> (дата звернення: 27.04.2026).
11. Cisco Systems. Understand EtherChannel Load Balance and Redundancy on Catalyst Switches. Document ID: 12023. Updated: November 30, 2023. URL:
<https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html> (дата звернення: 28.04.2026).
12. IEEE Standards Association. IEEE 802.1Q-2022. IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks. IEEE, 2022. URL:
<https://standards.ieee.org/ieee/802.1Q/10323/> (дата звернення: 29.04.2026).
13. RFC Editor. Information on RFC 9568: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. 2024. URL: <https://www.rfc-editor.org/info/rfc9568/> (дата звернення: 30.04.2026).
14. Katz D., Ward D. Bidirectional Forwarding Detection (BFD): RFC 5880. IETF, 2010. DOI: <https://doi.org/10.17487/RFC5880>. URL: <https://www.rfc-editor.org/rfc/rfc5880.html> (дата звернення: 30.04.2026).
15. Katz D., Ward D. Generic Application of Bidirectional Forwarding Detection (BFD): RFC 5882. IETF, 2010. DOI: <https://doi.org/10.17487/RFC5882>. URL: <https://www.rfc-editor.org/rfc/rfc5882> (дата звернення: 01.05.2026).
16. National Institute of Standards and Technology. Security Requirements. URL:

- <https://www.nist.gov/document/2005092920ahgvvsg2draft4doc> (дата звернення: 25.04.2026).
17. International Telecommunication Union. Recommendation ITU-T E.800 (09/2008): Definitions of terms related to quality of service. Geneva: ITU, 2008. URL: https://www.itu.int/rec/dologin_pub.asp?id=T-REC-E.800-200809-I%21%21PDF-E&lang=e&type=items (дата звернення: 26.04.2026).
 18. Lindem A., Dobra A. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6: RFC 9568. IETF, 2024. DOI: <https://doi.org/10.17487/RFC9568>. URL: <https://www.rfc-editor.org/info/rfc9568/> (дата звернення: 30.04.2026).
 19. Moy J. OSPF Version 2: RFC 2328. IETF, 1998. DOI: <https://doi.org/10.17487/RFC2328>. URL: <https://www.rfc-editor.org/info/rfc2328/> (дата звернення: 12.05.2026).
 20. Rekhter Y., Li T., Hares S. A Border Gateway Protocol 4 (BGP-4): RFC 4271. IETF, 2006. DOI: <https://doi.org/10.17487/RFC4271>. URL: <https://www.rfc-editor.org/info/rfc4271/> (дата звернення: 03.05.2026).
 21. International Telecommunication Union. ITU-T Recommendation E.800: Definitions of terms related to quality of service. Geneva: ITU, 2008. URL: <http://rfc.nor.hu/itu7/E/E0800e.pdf> (дата звернення: 26.04.2026).
 22. Technical Guide on Mean Time Between Failure (MTBF) Measuring Reliability. URL: https://smeda.org/files/Industry%20Support%20Cell/Productivity%20Improvement/Technical_Guide_on_Mean_Time_Between_Failure_MTBF_Measuring_Reliability.pdf (дата звернення: 22.04.2026).
 23. Alavian P. та ін. The (α, β) -Precise Estimates of MTBF and MTTR: Definitions, Calculations, and Induced Effect on Machine Efficiency Evaluation. URL: https://ocw.mit.edu/courses/2-611-marine-power-and-propulsion-fall-2006/8fd4b50ef794af75294c44aa555196c3_23reliability.pdf (дата звернення: 23.04.2026).
 24. MIT OpenCourseWare. Reliability and Availability. URL: <https://ocw.mit.edu/courses/2-611-marine-power-and-propulsion-fall->

- 2006/8fd4b50ef794af75294c44aa555196c3_23reliability.pdf (дата звернення: 24.04.2026).
- 25.Pro-face. ConneXium TCSESB Basic Managed Switch Redundancy Configuration / Rapid Spanning Tree. URL:
<https://www.proface.com/media/47822> (дата звернення: 11.05.2026).
- 26.Menčík J. Reliability of Systems. IntechOpen, 2016. DOI: 10.5772/62358. URL:
<https://www.intechopen.com/chapters/50094> (дата звернення: 25.04.2026).
- 27.Cisco Systems. Bidirectional Forwarding Detection for OSPF. Cisco White Paper. URL:
https://www.cisco.com/en/US/technologies/tk648/tk365/tk480/technologies_white_paper0900aecd80244005.html (дата звернення: 15.05.2026).
- 28.Cisco Systems. Understand and Tune Spanning Tree Protocol Timers. Cisco Support Documentation. Updated: February 2, 2023. URL:
<https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/19120-122.html> (дата звернення: 11.05.2026).
- 29.Cisco Systems. Understand Rapid Spanning Tree Protocol (802.1w). Cisco Support Documentation. Updated: February 9, 2023. URL:
<https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html> (дата звернення: 12.05.2026).
- 30.Cisco Systems. Understand Spanning Tree PortFast and BPDU Guard Features. Cisco Support Documentation. URL:
<https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10586-65.html> (дата звернення: 13.05.2026).
- 31.Cisco Systems. Enhance STP with Root Guard. Cisco Support Documentation. Updated: December 2, 2025. URL:
<https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html> (дата звернення: 14.05.2026).
- 32.IEEE Std 802.1AX-2020. IEEE Standard for Local and Metropolitan Area Networks — Link Aggregation. IEEE, 2020. URL:

https://standards.ieee.org/standard/802_1AX-2020.html (дата звернення: 29.04.2026).

33. Cisco Systems. Use Standby Preempt and Standby Track Commands. Cisco Support Documentation. URL:

<https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/13780-6.html> (дата звернення: 02.05.2026).

34. Cisco Systems. GLBP — Gateway Load Balancing Protocol. Cisco IOS Feature Guide. URL:

https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glb.html (дата звернення: 03.05.2026).