ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Мережева інфраструктура з резервуванням каналів зв'язку для підвищення надійності»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми «Інформаційні системи та технології»

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Володимир БОБИК
(підпис)

Виконала: здобувач вищої освіти групи ІСД-42
Володимир БОБИК

Керівник: Доктор філософії PhD
Валентина Данильченко

Рецензент:

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інформаційних систем татехноло
Ступінь вищої освіти Бакалавр
Спеціальність 126 Інформаційні системи та технології
Освітньо-професійна програма «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри ІСТ
_____Каміла СТОРЧАК
« _____» _____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бобик Володимир Васильович

1. Тема кваліфікаційної роботи: Мережева інфраструктура з резервуванням каналів зв'язку для підвищення надійності
керівник кваліфікаційної роботи: Валентина ДАНИЛЬЧЕНКО, д-р філософії PhD
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "20" лютого 2026 р. №51
2. Строк подання кваліфікаційної роботи «01» червня 2026 р.
3. Вихідні дані кваліфікаційної роботи:
    1. Науково технічна література.
    2. Аналіз методів моніторингу та управління мережевим трафіком.
    3. Сучасні мережеві протоколи та технології для резервування каналів зв'язку.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
    1. Огляд проблематики надійності сучасних мережевих інфраструктур.
    2. Аналіз технологій та протоколів резервування каналів зв'язку для критичних вузлів.
    3. Проектування та оптимізація мережевої інфраструктури з автоматичним перемиканням каналів.
5. Перелік ілюстраційного матеріалу: *презентація*
6. Дата видачі завдання «20» лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури з мережевих технологій та відмовостійкості	03.02 – 20.02.2026	Аналіз джерел
2	Аналіз методів резервування мережевих каналів (STP, LACP, VRRP/HSRP), порівняння протоколів	21.02 – 10.03.2026	Порівняльний аналіз
3	Визначення вимог до інфраструктури та вибір обладнання і технологічного стеку	11.03 – 18.03.2026	Постановка задачі
4	Проектування топології мережі з резервуванням та виключенням SPOF	19.03 – 01.04.2026	Дизайн системи
5	Реалізація: налаштування RSTP, LACP, VRRP/HSRP на обладнанні Cisco	02.04 – 18.04.2026	Розробка та конфігурація
6	Налаштування моніторингу, тестування відмовостійкості та вимірювання часу конвергенції	19.04 – 28.04.2026	Тестування
7	Оформлення роботи: вступ, висновки, реферат, перелік посилань	29.04 – 07.05.2026	Оформлення
8	Розробка демонстраційних матеріалів (презентація)	08.05 – 14.05.2026	Підготовка презентації
9	Попередній захист та фінальне коригування роботи	21.05 – 01.06.2026	Готовність до захисту

Здобувач вищої освіти _____ Володимир БОБИК
(підпис)

Керівник
кваліфікаційної роботи _____ Валентина ДАНИЛЬЧЕНКО
(підпис)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 52 стор., 12 рис., 20 табл., 30 джерела.

Мета роботи – розробка та обґрунтування архітектури мережевої інфраструктури з використанням технологій резервування каналів зв'язку для забезпечення високого рівня відмовостійкості та мінімізації часу простою мережі.

Об'єкт дослідження – процес передачі даних у корпоративних та відомчих мережевих інфраструктурах.

Предмет дослідження – методи, алгоритми та протоколи резервування фізичних і логічних каналів зв'язку (STP, LACP, VRRP/HSRP).

Короткий зміст роботи: У даній роботі проведено комплексне дослідження методів підвищення надійності мережевих систем. Виконано аналіз основних причин відмов у сучасних мережах та визначено вимоги до критично важливих вузлів зв'язку. Розглянуто теоретичні засади функціонування протоколів резервування на другому (L2) та третьому (L3) рівнях моделі OSI.

Особливу увагу приділено практичному проектуванню топології мережі, що виключає наявність єдиної точки відмови (SPOF). Обґрунтовано вибір протоколу Rapid Spanning Tree Protocol (RSTP) для усунення петель у надлишкових з'єднаннях та Virtual Router Redundancy Protocol (VRRP) для забезпечення безперебійної роботи шлюзу за замовчуванням. У роботі реалізовано модель мережі, яка демонструє автоматичне перемикання трафіку на резервний канал у разі аварії на основній лінії. Проведено розрахунок показників надійності та оцінено час збіжності мережі після збоїв, що підтверджує ефективність запропонованих рішень.

КЛЮЧОВІ СЛОВА: МЕРЕЖЕВА ІНФРАСТРУКТУРА, РЕЗЕРВУВАННЯ КАНАЛІВ, ВІДМОВОСТІЙКІСТЬ, НАДІЙНІСТЬ, STP, VRRP, ТРАФІК, МОНІТОРИНГ, МЕРЕЖЕВИЙ ПРОТОКОЛ.

ABSTRACT

Text part of the qualification work for the bachelor's degree: 52 pages, 12 figures, 20 tables, 30 sources.

The purpose of the work is to develop and justify the architecture of the network infrastructure using communication channel redundancy technologies to ensure a high level of fault tolerance and minimize network downtime.

The object of the study is the process of data transmission in corporate and departmental network infrastructures.

The subject of the study is methods, algorithms and protocols for the redundancy of physical and logical communication channels (STP, LACP, VRRP/HSRP).

Summary of the work: This work provides a comprehensive study of methods for increasing the reliability of network systems. The main causes of failures in modern networks are analyzed and the requirements for critical communication nodes are determined. The theoretical principles of the functioning of redundancy protocols at the second (L2) and third (L3) levels of the OSI model are considered.

Special attention is paid to the practical design of a network topology that eliminates the presence of a single point of failure (SPOF). The choice of the Rapid Spanning Tree Protocol (RSTP) to eliminate loops in redundant connections and the Virtual Router Redundancy Protocol (VRRP) to ensure uninterrupted operation of the default gateway is justified. The work implements a network model that demonstrates automatic switching of traffic to a backup channel in the event of a failure on the main line. Reliability indicators are calculated and the network convergence time after failures is estimated, which confirms the effectiveness of the proposed solutions.

KEYWORDS: NETWORK INFRASTRUCTURE, CHANNEL RESERVATION, FAULT RESILIENCE, RELIABILITY, STP, VRRP, TRAFFIC, MONITORING, NETWORK PROTOCOL.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСК – автоматизована система керування;

БД – база даних;

ІТ – інформаційні технології;

ПЗ – програмне забезпечення;

BPDU – Bridge Protocol Data Unit, службовий кадр протоколу Spanning Tree;

BFD – Bidirectional Forwarding Detection, протокол двонаправленого виявлення збоїв;

DSCP – Differentiated Services Code Point, поле пріоритизації трафіку;

FHRP – First Hop Redundancy Protocol, протокол резервування першого стрибка;

GNS3 – Graphical Network Simulator 3, середовище емуляції мережевого обладнання;

HSRP – Hot Standby Router Protocol, пропрієтарний протокол резервування шлюзу Cisco;

IP SLA – IP Service Level Agreement, механізм моніторингу якості каналів зв'язку;

LACP – Link Aggregation Control Protocol, протокол агрегації канальних з'єднань;

LAG – Link Aggregation Group, агрегована група каналів;

LLQ – Low Latency Queuing, черга з низькою затримкою для пріоритетного трафіку;

MAC – Media Access Control, апаратна адреса мережевого інтерфейсу;

MSTP – Multiple Spanning Tree Protocol, протокол множинного дерева покриття;

MTBF – Mean Time Between Failures, середній час між відмовами;

MTTR – Mean Time To Repair, середній час відновлення після відмови;

NTP – Network Time Protocol, протокол синхронізації часу;

OSI – Open Systems Interconnection, модель взаємодії відкритих систем;

PDU – Protocol Data Unit, одиниця даних протоколу;

PoE – Power over Ethernet, технологія живлення через мережевий кабель;

PSU – Power Supply Unit, блок живлення;

QoS – Quality of Service, якість обслуговування мережевого трафіку;

RSTP – Rapid Spanning Tree Protocol, протокол швидкого дерева покриття;

RPS – Redundant Power Supply, резервний блок живлення;

SNMP – Simple Network Management Protocol, протокол управління мережевими пристроями;

SPOF – Single Point of Failure, єдина точка відмови;

STP – Spanning Tree Protocol, протокол дерева покриття;

TCO – Total Cost of Ownership, сукупна вартість володіння;

VLAN – Virtual Local Area Network, віртуальна локальна мережа;

VPN – Virtual Private Network, віртуальна приватна мережа;

VRRP – Virtual Router Redundancy Protocol, відкритий протокол резервування шлюзу;

VSS – Virtual Switching System, технологія віртуального об'єднання комутаторів Cisco;

ВСТУП

Актуальність теми. Сучасний розвиток інформаційного суспільства та стрімка цифровізація бізнес-процесів зумовлюють зростаючу залежність підприємств від безперервної роботи корпоративних мереж. Будь-який збій у роботі мережевої інфраструктури неминуче спричиняє фінансові втрати, порушення технологічних процесів та репутаційні ризики. За даними аналітичних досліджень, середня вартість однієї години незапланованого простою для підприємства середнього масштабу становить від 50 до 300 тисяч доларів США. Це зумовлює нагальну потребу у впровадженні технологій резервування каналів зв'язку, здатних забезпечити автоматичне відновлення зв'язку без втручання адміністратора.

Незважаючи на наявність стандартизованих протоколів резервування – STP, RSTP, LACP, VRRP та HSRP – більшість малих і середніх підприємств України досі використовують одноканальні мережеві рішення без резервування. Це робить їхню інфраструктуру надзвичайно вразливою до відмов. Водночас комплексний підхід до резервування на всіх рівнях моделі OSI дозволяє досягти коефіцієнту готовності мережі 99,95% і вище, що відповідає галузевим вимогам для корпоративних телекомунікаційних систем.

Метою кваліфікаційної роботи є розробка та обґрунтування архітектури відмовостійкої мережевої інфраструктури з використанням механізмів автоматичного резервування каналів зв'язку для підвищення загальної надійності передачі даних у корпоративному середовищі.

Завдання дослідження включають:

- проведення аналітичного огляду сучасних методів та стандартів забезпечення надійності в комп'ютерних мережах;
- дослідження принципів роботи протоколів резервування на канальному (L2) та мережевому (L3) рівнях моделі OSI;
- вибір оптимального технологічного стеку та апаратних рішень для побудови надлишкової архітектури;

- проектування топології мережі, що виключає наявність єдиної точки відмови (SPOF);
- практичну реалізацію та налаштування конфігурацій протоколів динамічного резервування (STP, VRRP, LACP);
- проведення тестування системи на швидкість збіжності мережі та відновлення зв'язку після імітованих збоїв;
- оцінку ефективності запропонованого рішення та визначення напрямків його подальшого масштабування.

Об'єктом дослідження є процеси забезпечення безперервності передачі даних та стійкості до відмов у сучасних корпоративних мережевих інфраструктурах.

Предметом дослідження є архітектурні рішення, мережеві протоколи та технічні засоби резервування каналів зв'язку, що забезпечують автоматичне відновлення працездатності мережі при відмовах окремих компонентів.

Методи дослідження: теоретичний аналіз технічної документації та наукових праць у галузі телекомунікацій; методи інженерного проектування мережевих топологій; метод порівняльного аналізу протоколів резервування; моделювання мережевих процесів у середовищах Cisco Packet Tracer та GNS3; експериментальне тестування показників відмовостійкості з вимірюванням часу відновлення зв'язку.

Наукова новизна кваліфікаційної роботи полягає у комплексному обґрунтуванні вибору технологій резервування для кожного рівня ієрархічної мережевої моделі та розробці методики верифікації відмовостійкості на основі контрольованих тестових збоїв із вимірюванням фактичного часу конвергенції.

Практична значущість результатів полягає у розробці готового до впровадження рішення для побудови відмовостійкої корпоративної мережі. Запропонована архітектура, конфігурації протоколів та методологія тестування можуть бути безпосередньо використані при проектуванні мережевих інфраструктур підприємств з чисельністю 200–300 користувачів без залучення дорогих зовнішніх консультантів.

Апробація проміжних результатів дослідження здійснювалася шляхом публікації тез на всеукраїнських науково-практичних та науково-технічних конференціях. Тематика тез, зокрема оптимізація показників відмовостійкості розподілених систем шляхом впровадження багаторівневого резервування каналів зв'язку, була врахована під час формування технічних вимог до відмовостійкості, вибору технологічного стеку та методології тестування в даній роботі.

Структура кваліфікаційної роботи. Робота складається з вступу, трьох розділів, дев'яти підрозділів, загальних висновків та переліку посилань. Повний обсяг роботи становить 52 сторінки основного тексту, 12 рисунків, 20 таблиць, 30 джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ПОБУДОВИ ВІДМОВОСТІЙКИХ МЕРЕЖЕВИХ ІНФРАСТРУКТУР

1.1 Огляд сучасних методів забезпечення надійності в комп'ютерних мережах

Мережа впала. Саме в цей момент розумієш наскільки від неї залежить все інше. Касири не можуть провести оплату. Менеджери не бачать замовлення. IP-телефони мовчать. І кожна хвилина простою – це гроші які йдуть в нікуди. Ось чому надійність мережі давно перестала бути суто технічним питанням – це питання бізнесу. А надійна мережа – це та яка продовжує працювати навіть коли щось всередині неї ламається [1].

Як цього досягти? Інженери відповідають на це питання по-різному. Одні кажуть – дублюй все що може зламатись. Два кабелі замість одного, два комутатори, два блоки живлення. Якщо один елемент відмовив – другий вже в роботі. Інші роблять акцент не на дублюванні а на здатності системи самій розібратись з проблемою – перебудувати маршрути, перенаправити трафік, відновитись без того щоб хтось ліз у серверну о другій ночі. Є ще третій підхід – взагалі не доводити до відмови: моніторинг помічає що щось починає вести себе дивно і сигналізує заздалегідь [2].

Щоб не говорити про надійність абстрактно – є конкретні цифри. MTBF каже скільки годин в середньому система живе без проблем. MTTR – скільки часу йде на те щоб після проблеми все знову запрацювало. З цього рахується коефіцієнт готовності:

A = MTBF / (MTBF + MTTR)

Щоб перейти від абстрактних відсотків до практичного розуміння, прийнято класифікувати рівні надійності за так званою шкалою «дев'яток». Кожна додаткова дев'ятка в показнику готовності – це не просто краща цифра у звіті, а суттєво менший сумарний час простою на рік. Різниця між 99% і 99,999% на папері здається незначною. Але на практиці це різниця між трьома з половиною

днями і п'ятьма хвилинами простою на рік. Для банку, лікарні або диспетчерського центру ця різниця може означати буквально все.[25]

Промислові стандарти надійності – так звані SLA-класи – систематизовано у таблиці 1.1. Вона показує не лише відсоток готовності, а й реальний максимальний простій у годинах і хвилинах на рік, що дозволяє вибрати цільовий клас ще на етапі проектування, до того як прийнято рішення про обладнання.

Таблиця 1.1

Класифікація рівнів надійності мережевої інфраструктури

Клас	Готовність, %	Макс. простій на рік	Типове застосування	Необхідні механізми резервування
99%	99,0%	87,6 год / 3,65 доби	Малий офіс, некритичні сервіси	Без резервування або UPS
99,9%	99,9%	8,76 год	Середній бізнес, пошта, файловий сервер	Резервний ISP або UPS + генератор
99,95%	99,95%	4,38 год	Корпоративна мережа (цільовий показник проекту)	RSTP + LACP + HSRP/VRRP + Dual ISP
99,99%	99,99%	52,6 хв	Ядро мережі, серверний сегмент	StackWise Virtual + BFD + субсекундні таймери
99,999%	99,999%	5,26 хв	Телеком-оператори, дата-центри	Повне апаратне резервування + автоматичне відновлення

Для підприємства що розглядається у цій роботі цільовий показник встановлено на рівні 99,95% – це четвертий рядок таблиці. Такий вибір обґрунтований: вищий клас вимагає значно дорожчого обладнання і складнішої інфраструктури, тоді як 99,95% цілком досяжні на серійному комерційному обладнанні при грамотному проектуванні. Розрахунок підтверджує: при цьому

класі допустимий сумарний простій на рік не перевищує 4,38 годин – прийнятно для корпоративного середовища де немає цілодобових критичних транзакцій.

Простий приклад: обладнання рік працює без збоїв а кожна поломка усувається за 4 години. Готовність – 99,95%. Звучить непогано. Але для банку чи лікарні навіть це замало – там вимагають «п'ять дев'яток», тобто 99,999%. Різниця між цими двома цифрами на папері невелика. На практиці – це різниця між 4 годинами і 5 хвилинами простою на рік.

Кожен рівень мережевого стека має свої інструменти для досягнення цих показників. Що саме використовується на кожному рівні – показано на рис. 1.1.

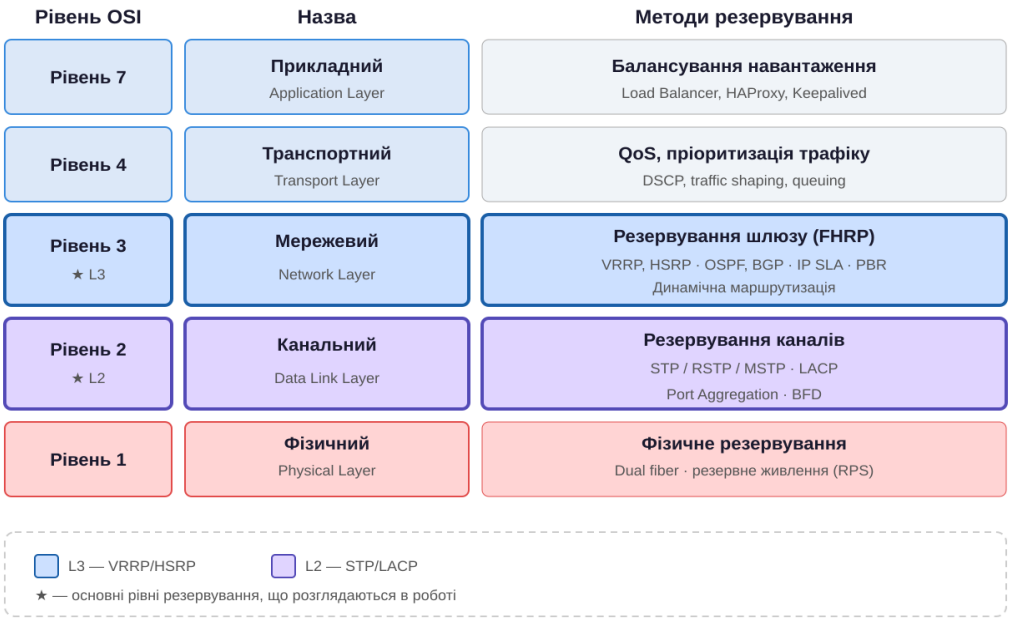


Рис. 1.1 – Модель OSI: методи резервування на кожному рівні

Резервування будується на кожному рівні мережевого стека – і кожен рівень вирішує свою частину задачі.[21] На фізичному рівні все починається з якісного кабелю – мінімум Cat6A – і не обмежується ним: резервні блоки живлення, прокладка оптики по двох різних фізичних трасах, щоб пошкодження в одному місці не зупинило все. Канальний рівень відповідає за те, щоб петлі комутації не

поклали мережу і щоб при відмові одного кабелю трафік автоматично пішов іншим – цим займаються STP, RSTP, LACP та BFD. На мережевому рівні головне завдання – не дати хостам "осиротіти" без шлюзу: VRRP і HSRP тримають віртуальний шлюз живим навіть коли один з маршрутизаторів виходить з ладу, а OSPF і BGP швидко перебудовують таблиці маршрутизації.[22]

Окремо варто зупинитись на понятті єдиної точки відмови – SPOF. Це будь-який елемент мережі, після зупинки якого падає вся система або її критична частина. Один роутер на виході в інтернет, один комутатор між серверами і користувачами – класичні приклади SPOF. Перед тим як затвердити проект мережі, топологію обов'язково перевіряють саме на наявність таких вузьких місць і усувають їх резервуванням [3].

Причини мережевих збоїв розподіляються приблизно так: близько 70% – це апаратні проблеми, тобто фізичний вихід з ладу обладнання, перебиті кабелі, згорілі блоки живлення. Ще чверть припадає на програмні помилки – неправильна конфігурація, баги у прошивці, невдале оновлення. Решта 30% – зовнішні фактори, на які адміністратор впливати не може: відключення електрики, стихійні лиха, механічне пошкодження кабельних трас [4].

Практика показує: мережа з нормально спроектованим резервуванням дає у 3–5 разів менше незапланованих простоїв ніж одноканальне рішення. Витрати на впровадження при цьому, як правило, повертаються вже протягом першого року – просто за рахунок того, що простоїв стає значно менше.

Таблиця 1.2

Порівняння методів резервування мережевих каналів

Метод резервування	Рівень OSI	Час переключення	Складність
STP/RSTP	L2	1–30 с / < 1 с	Середня
LACP (агрегація)	L2	< 100 мс	Низька
VRRP/HSRP	L3	1–3 с	Середня
OSPF + BFD	L3	< 50 мс	Висока
BGP Dual ISP	L3	30–300 с	Висока
Dual ISP + IP SLA	L3	1–10 с	Висока

Для практичного проектування важливо розуміти не лише які методи резервування існують але й як організувати саму надмірність системи. В інженерній практиці прийнято розрізняти три основні підходи залежно від того в якому стані перебуває резервний елемент до моменту відмови основного.

Гаряче резервування передбачає що резервний компонент постійно активний і готовий миттєво підхопити навантаження. Саме так працює StackWise Virtual на рівні ядра і HSRP на рівні шлюзу – резервний пристрій весь час слухає мережу і при відмові основного реагує за мілісекунди. Плюс очевидний – мінімальний час переключення. Мінус – резервний елемент споживає ресурси навіть поки він не потрібен.

Тепле резервування означає що резервний компонент увімкнений і частково налаштований але не обробляє трафік в штатному режимі. При відмові основного він потребує певного часу на ініціалізацію – зазвичай від кількох секунд до кількох хвилин. Типовий приклад – резервний сервер який синхронізує дані з основним але не відповідає на запити клієнтів поки не отримає команду на перехід в активний режим.

Холодне резервування – це фізично наявне обладнання яке стоїть на полиці і вмикається вручну після відмови основного. Час відновлення тут вимірюється годинами а іноді й добами якщо потрібна повна переконфігурація. Для мережевої

інфраструктури підприємства такий підхід прийнятний лише для некритичного обладнання на рівні доступу.

Розподіл цих підходів за рівнями мережі для даного проекту наведено в таблиці 1.3.

Таблиця 1.3

Типи резервування по рівнях мережевої ієрархії

Рівень мережі	Тип резервування	Час переключення	Приклад реалізації
Ядро	Гаряче	< 50 мс	StackWise Virtual
Дистрибуція	Гаряче	< 3 с	HSRP + Object Tracking
Канали між рівнями	Гаряче	< 100 мс	LACP Port-Channel
Зовнішній канал	Гаряче	< 10 с	Dual ISP + IP SLA
Рівень доступу	Тепле	< 30 с	RSTP резервний uplink
Некритичне обладнання	Холодне	Години	ЗІП на складі

Окремо варто розглянути класифікацію самих відмов – бо тип відмови визначає який саме механізм захисту спрацює. Апаратні відмови складають близько 70% від загальної кількості інцидентів і включають фізичний вихід з ладу обладнання, обрив кабелів, згоряння блоків живлення. Проти них добре працює фізичне резервування – дубльовані канали, резервні PSU, надлишкові вузли в топології. Програмні збої – приблизно 15% – це некоректна конфігурація, помилки у прошивці, невдале оновлення. Тут допомагають автоматичні відкоти конфігурації і попереднє тестування в лабораторному середовищі перед впровадженням у продуктив. Людський фактор дає ще близько 10% – випадкові зміни конфігурації, помилки при обслуговуванні. Зовнішні фактори що залишились – відключення електрики, пошкодження кабельних трас, стихійні лиха – не залежать від адміністратора але від них теж можна захиститись через ДБЖ, генератори і прокладку оптики по різних фізичних трасах.

Вибір конкретного методу або комбінації методів резервування залежить від вимог до часу відновлення, бюджетних обмежень та складності обслуговування.

Для більшості корпоративних середовищ оптимальним рішенням є поєднання LACP на канальному рівні та VRRP/HSRP на мережевому рівні, що дозволяє досягти часу переключення менше однієї секунди без значних фінансових витрат.

1.2 Аналіз технологій резервування на канальному рівні (L2): протоколи STP та LACP

Якщо говорити про те, де резервування найбільш критичне для повсякденної роботи корпоративної мережі – це канальний рівень. Саме тут вирішуються дві проблеми, кожна з яких окремо здатна повністю паралізувати мережу. Перша – петлі комутації: якщо між комутаторами є кілька фізичних шляхів без відповідного протоколу, широкомовний трафік почне нескінченно циркулювати по мережі і за лічені секунди завантажить усі канали до нуля. Друга задача – зворотна: ті самі надлишкові зв'язки потрібно використати для підвищення пропускної здатності та забезпечення відмовостійкості [5].

Відповідь на першу проблему з'явилась ще у 1985 році – інженер Раді Перлман розробила протокол STP, який увійшов до стандарту IEEE 802.1D. Ідея проста і елегантна: поверх фізичної топології з петлями будується логічна деревоподібна структура без циклів. Комутатори обираються між собою "кореневий" вузол, після чого всі надлишкові порти переводяться у стан блокування – вони є фізично, але трафік через них не йде. Якщо основний шлях зникає, заблокований порт розблоковується і мережа відновлюється. На рис. 1.2 наочно показано як STP перетворює топологію з петлею на дерево без циклів.[26]

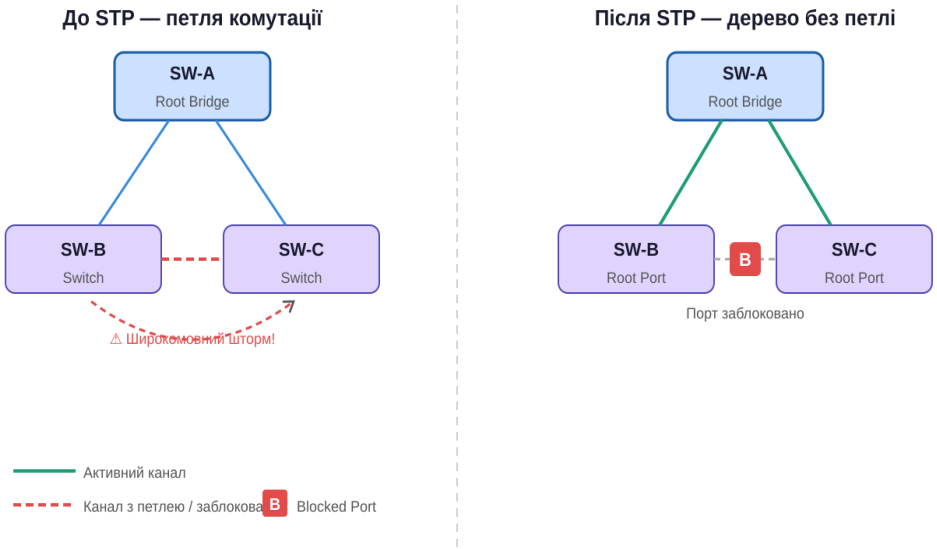


Рис. 1.2 – Принцип роботи STP: усунення петлі шляхом блокування надлишкового порту

Робота STP розгортається поетапно. Спочатку всі комутатори мережі "домовляються" між собою хто буде головним – так званим Root Bridge. Перемагає той, у кого менший Bridge ID: це число складається з пріоритету і MAC-адреси пристрою. За замовчуванням пріоритет однаковий у всіх – 32768, тому на практиці адміністратор вручну знижує його на тому комутаторі, який має стати кореневим. Після того як корінь обрано, кожен інший комутатор вираховує найкоротший шлях до нього і позначає відповідний порт як кореневий (Root Port). Паралельно для кожного сегменту мережі визначається один призначений порт (Designated Port) – через який і йтиме трафік. Всі порти що залишились – блокуються [6].

Головна претензія до класичного STP – швидкість реакції. П'ятдесят секунд на відновлення після збою – це дуже багато для сучасного підприємства. Причина така затримка криється в тому, що перш ніж порт почне передавати трафік він послідовно проходить через кілька станів: Blocking, Listening, Learning і нарешті Forwarding – і на кожному з проміжних станів витрачається по 15 секунд. Розробники стандарту IEEE 802.1W врахували цей недолік і випустили RSTP – прискорену версію протоколу, яка скорочує час відновлення до менш ніж секунди. Як саме змінились стани портів між STP і RSTP – показано на рис. 1.3.

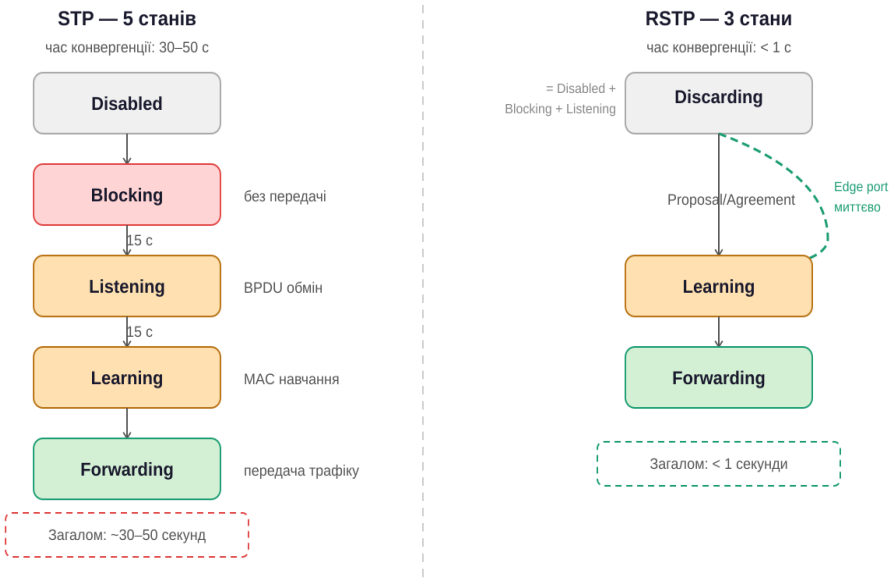


Рис. 1.3 – Порівняння переходів станів портів STP та RSTP

Секрет швидкості RSTP – у відмові від жорстких таймерів. Замість того щоб чекати фіксовані 15 секунд на кожному стані, протокол використовує діалог між сусідами. Комутатор що хоче активувати порт надсилає сусіду запит – Proposal. Якщо сусід готовий – він відповідає Agreement і порт одразу переходить у робочий стан Forwarding. Вся процедура займає мілісекунди замість десятків секунд. При цьому RSTP не вимагає повної заміни обладнання – якщо в мережі є старі пристрої що розуміють лише класичний STP, RSTP автоматично підлаштовується під них і працює у режимі сумісності [7].

MSTP пішов ще далі у вирішенні практичних проблем. У реальних корпоративних мережах зазвичай десятки VLAN, і класичний STP будує одне єдине дерево для всіх – частина каналів заблокована і простоює без діла. MSTP за стандартом IEEE 802.1Q дозволяє розбити VLAN на групи і для кожної групи побудувати окреме дерево зі своїм кореневим комутатором. Практичний результат – можна навантажити обидва надлишкових канали: одна половина VLAN іде через перший комутатор як корінь, інша через другий. Канали більше не простоюють і мережа стає одночасно і надійнішою і ефективнішою.

Таблиця 1.4

Порівняння варіантів протоколу Spanning Tree

Параметр	STP (802.1D)	RSTP (802.1W)	MSTP (802.1Q)
Час конвергенції	30–50 с	< 1 с	< 1 с
Кількість станів портів	5 станів	3 стани	3 стани
Підтримка VLAN	Одна інстанція	Одна інстанція	Кілька інстанцій
Балансування навантаження	Відсутнє	Відсутнє	Так
Стандарт IEEE	802.1D	802.1W	802.1Q
Зворотня сумісність	Базова	Так (з STP)	Так (з STP/RSTP)

Протокол LACP (Link Aggregation Control Protocol), визначений стандартом IEEE 802.3ad (пізніше включений до 802.1AX), забезпечує динамічне об'єднання кількох фізичних каналів в один логічний агрегований канал (LAG – Link Aggregation Group або Port Channel). На відміну від STP, який блокує надлишкові канали, LACP використовує всі агреговані канали одночасно для передачі трафіку, забезпечуючи як підвищену пропускну здатність, так і відмовостійкість [8]. Принцип агрегації каналів LACP наведено на рис. 1.4.

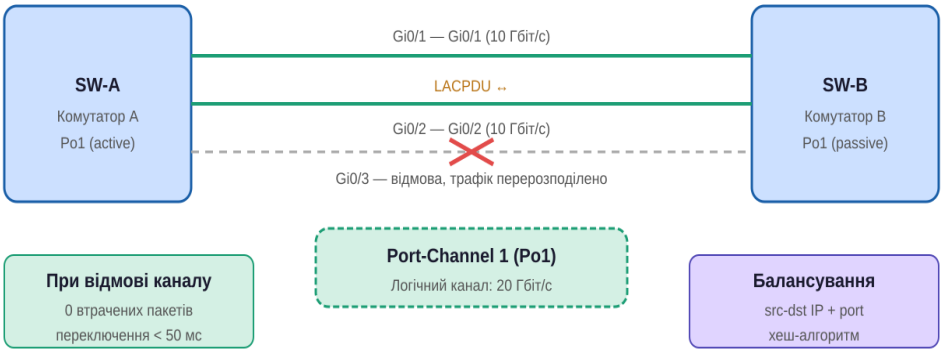


Рис. 1.4 – Агрегація каналів LACP: три фізичні канали утворюють один логічний Port-Channel

LACP працює через постійний обмін службовими повідомленнями між двома сторонами з'єднання – LACPDU. Кожен порт при цьому може грати одну з двох ролей: активну або пасивну. Активний порт сам ініціює встановлення агрегації, пасивний – лише відповідає на запити. Головне правило: щоб агрегація запрацювала, хоча б один з двох партнерів має бути активним. Якщо один з фізичних каналів у групі раптом падає – протокол це одразу помічає і без будь-якого втручання адміністратора перекидає трафік на канали що залишились, причому жоден пакет при цьому не губиться [9].

Швидкість виявлення збою залежить від налаштування таймера. У стандартному режимі LACPDU надсилаються раз на 30 секунд – це означає що проблема виявиться не раніше ніж через півхвилини. Режим LACP Fast скорочує інтервал до 1 секунди, що на порядок прискорює реакцію системи. Для критичних з'єднань Fast режим є очевидним вибором.

Окремо варто пояснити як LACP розподіляє трафік між фізичними каналами. Протокол не ділить окремі пакети між каналами – він ділить потоки. Для кожного пакету обраховується хеш на основі IP-адрес відправника і отримувача плюс портів TCP/UDP, і результат визначає через який саме фізичний канал піде цей пакет. Оскільки всі пакети одного сеансу дають однаковий хеш – вони завжди йдуть одним каналом. Це виключає ситуацію коли ці пакети приходять не в тому порядку в якому були відправлені.[29]

Окремо варто згадати протокол BFD (Bidirectional Forwarding Detection), який стоїть трохи осторонь від STP і LACP але вирішує суміжну задачу. Його мета – максимально швидко виявити що з'єднання між двома вузлами припинило працювати, навіть якщо фізичний інтерфейс при цьому залишається піднятим. Саме останній випадок є найнебезпечнішим: обладнання «думає» що канал живий, трафік продовжує надсилатись, але нікуди не доходить. STP і LACP виявляють такий збій з затримкою – через таймери очікування. BFD натомість надсилає службові пакети кожні 50–300 мілісекунд і якщо кілька пакетів поспіль не отримало відповіді – негайно сигналізує про збій протоколам вищого рівня [8].

Практична цінність BFD в тому що він не прив'язаний до конкретного протоколу маршрутизації чи комутації – він працює як загальний «детектор збоїв» якому можуть довіряти і OSPF, і HSRP, і LACP одночасно. У проекті що розглядається BFD використовується на магістральних з'єднаннях між ядром і рівнем дистрибуції саме для того щоб скоротити час виявлення збою до 150–300 мс замість стандартних 3 секунд очікування HSRP.

Порівняння BFD зі стандартними механізмами виявлення збоїв наведено в таблиці 1.5.

Таблиця 1.5

Порівняння механізмів виявлення збоїв каналів зв'язку

Механізм	Час виявлення збою	Навантаження на CPU	Підтримувані протоколи
HSRP стандартні таймери	10 с	Мінімальне	HSRP
HSRP субсекундні таймери	700 мс	Низьке	HSRP
LACP стандартний режим	90 с	Мінімальне	LACP
LACP Fast режим	3 с	Низьке	LACP
BFD (стандартний)	300–1000 мс	Середнє	OSPF, HSRP, LACP, BGP
BFD (агресивний)	50–150 мс	Підвищене	OSPF, HSRP, LACP, BGP

З таблиці видно що BFD у агресивному режимі дає найшвидшу реакцію але ціною підвищеного навантаження на процесор. Для магістральних з'єднань між ядром і дистрибуцією де обладнання потужне і кількість з'єднань невелика це прийнятний компроміс. На рівні доступу де комутаторів багато і ресурси скромніші BFD не використовується – там достатньо RSTP і LACP Fast.

На рівні доступу де до портів підключаються кінцеві пристрої – комп'ютери, телефони, точки доступу – застосовуються два важливі механізми які безпосередньо впливають на швидкість відновлення і безпеку мережі.

PortFast вирішує просту але відчутну проблему. Коли комп'ютер підключається до порту комутатора стандартний RSTP все одно витримує паузу кілька секунд перш ніж порт перейде у стан Forwarding – навіть якщо очевидно що там кінцевий пристрій а не інший комутатор. Для користувача це виглядає як те що мережа не одразу з'являється після підключення кабелю. PortFast прибирає цю паузу і порт одразу стає активним. Але вмикати його можна виключно на портах де підключені кінцеві пристрої – якщо увімкнути PortFast на порту куди підключений інший комутатор виникне ризик петлі.

BPDUGuard страхує від цієї саме ситуації. Якщо на порт з увімкненим PortFast раптом приходить BPDU – службовий кадр від іншого комутатора – BPDUGuard миттєво переводить порт у стан err-disabled і блокує його. Це захищає від двох ситуацій: по-перше від випадкового підключення некерованого комутатора користувачем, по-друге від навмисних атак типу STP Manipulation де зловмисник намагається стати кореневим комутатором мережі надсилаючи підроблені BPDU з низьким пріоритетом.

1.3 Дослідження протоколів забезпечення відмовостійкості на мережевому рівні (L3): VRRP та HSRP

Уявіть просту ситуацію: у офісі 200 комп'ютерів, у кожного прописаний один шлюз за замовчуванням – роутер який виводить трафік у зовнішню мережу. Цей роутер раптом виходить з ладу. Результат – всі 200 машин одночасно втрачають доступ до інтернету і корпоративних сервісів, і так триватиме доти доки адміністратор вручну не зміниться налаштування на кожному пристрої або не підніме резервний роутер. Саме цю проблему і вирішують протоколи групи FHRP. Їхня ідея полягає в тому, що кілька фізичних маршрутизаторів спільно "прикидаються" одним віртуальним – з єдиною IP-адресою і MAC-адресою. Хости нічого не знають про внутрішню кухню і продовжують надсилати трафік

на ту саму адресу шлюзу незалежно від того що відбувається з реальним обладнанням [10].

VRRP – найпоширеніша реалізація цієї ідеї. Протокол описаний у відкритому стандарті RFC 5798 і підтримується обладнанням практично будь-якого виробника, що робить його зручним вибором у гетерогенних мережах. Кожна VRRP-група отримує віртуальну IP-адресу і MAC-адресу у форматі 00:00:5E:00:01:XX де XX – номер групи. Один з маршрутизаторів бере на себе роль Master і реально обробляє трафік що надходить на віртуальну адресу. Інші перебувають у режимі очікування і готові підхопити роботу якщо Master раптом замовчить. Як виглядає ця схема на практиці – показано на рис. 1.5.[27]

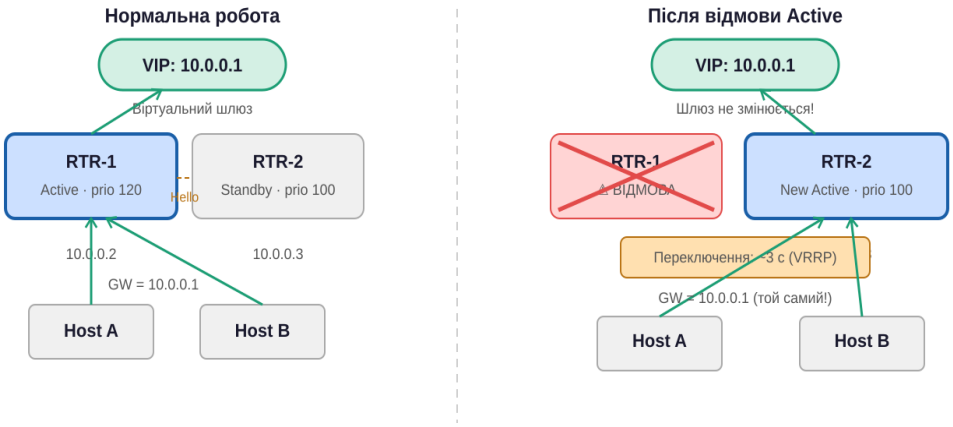


Рис. 1.5 – Принцип роботи VRRP/HSRP: автоматичне переключення шлюзу при відмові Active-маршрутизатора

Щоб визначити хто з маршрутизаторів стане Master, VRRP використовує числовий пріоритет від 1 до 254. Логіка проста – перемагає той у кого число більше, за замовчуванням у всіх стоїть 100. Адміністратор вручну підвищує пріоритет на тому пристрої який має бути основним. Далі Master щосекунди розсилає в мережу короткі повідомлення – Advertisement – на мультикастову адресу 224.0.0.18. Резервні маршрутизатори слухають ці повідомлення і поки вони надходять – мовчать. Щойно пауза між повідомленнями перевищує три

секунди – хтось із Backup-пристроїв оголошує себе новим Master і підхоплює трафік. Якщо стандартні три секунди замало – можна налаштувати субсекундні таймери і скоротити час реакції до 200–700 мс [11].

HSRP від Cisco вирішує ту саму задачу але з деякими відмінностями. По-перше це пропрієтарний протокол – тобто працює лише на обладнанні Cisco. По-друге друга версія HSRP підтримує до 4095 груп і вміє працювати з IPv6. Але головна перевага HSRP над VRRP – глибша інтеграція з іншими механізмами Cisco IOS, зокрема з Object Tracking і Interface Tracking. Завдяки цьому можна будувати значно складніші сценарії автоматичного перемикання [12].

Object Tracking – це механізм який робить резервування по-справжньому розумним. Без нього маршрутизатор реагує лише на одне: впав чи ні його власний інтерфейс. Але що якщо інтерфейс фізично живий а зв'язок з провайдером за ним зник? Object Tracking вирішує саме цю ситуацію – він може стежити за доступністю будь-якої IP-адреси через IP SLA зондування, за наявністю потрібного маршруту в таблиці або за станом uplink-каналу. Якщо щось іде не так – пріоритет маршрутизатора автоматично знижується, і роль Active переходить до того пристрою у якого зв'язок є. В результаті система реагує не лише на фізичні поломки але й на логічні збої – саме те що потрібно в реальному корпоративному середовищі.

Таблиця 1.6

Порівняння протоколів VRRP та HSRP

Параметр	VRRP	HSRP v1	HSRP v2
Стандарт	RFC 5798 (відкритий)	Cisco (пропрієтарний)	Cisco (пропрієтарний)
Мультикаст адреса	224.0.0.18	224.0.0.2	224.0.0.102
Стани пристрою	Master / Backup	Active / Standby	Active / Standby
Кількість груп	1–255	0–255	0–4095
Підтримка IPv6	VRRPv3 (RFC5798)	Відсутня	Присутня

Параметр	VRRP	HSRP v1	HSRP v2
Object Tracking	Так	Так	Так (розширений)

IP SLA – це вбудований інструмент Cisco IOS для безперервного моніторингу якості зв'язку. Працює він просто: з заданою частотою відправляє зонди на цільову адресу – ICMP Echo або UDP – і аналізує відповіді. При цьому цікавить не лише факт доступності вузла, але й конкретні цифри: скільки мілісекунд займає відповідь, наскільки стабільна затримка, який відсоток зондів взагалі не повертається. Коли показники виходять за налаштовані межі – IP SLA фіксує подію. Далі в гру вступає Object Tracking: він бачить цю подію і знижує пріоритет HSRP на пристрої у якого проблеми з каналом. Результат – трафік автоматично йде через той маршрутизатор який реально має нормальний зв'язок з провайдером.

Підсумовуючи аналіз обох протоколів, для даного проекту обрано HSRP v2 а не VRRP, і цей вибір потребує прямого обґрунтування. В гетерогенному середовищі де обладнання різних виробників – VRRP був би очевидним вибором як відкритий стандарт. Але тут уся інфраструктура будується на Cisco IOS, і в цьому контексті HSRP має конкретну технічну перевагу яку не можна ігнорувати.

Перша перевага – інтеграція з Object Tracking і IP SLA. У Cisco IOS ці три механізми утворюють єдиний конвеєр: IP SLA виявляє що провайдер недоступний, Object Tracking фіксує цю подію і знижує пріоритет HSRP, HSRP передає роль Active іншому маршрутизатору. Вся ця послідовність налаштовується кількома рядками конфігурації і працює передбачувано. З VRRP на Cisco аналогічну поведінку теж можна реалізувати, але це потребує додаткових налаштувань і в ряді версій IOS поводиться з тонкощами які варто враховувати.

Друга перевага – підтримка HSRP v2. Перша версія протоколу обмежена 255 групами, друга підтримує до 4095, що важливо для мережі з великою кількістю VLAN. Крім того, HSRP v2 використовує мультикастову адресу 224.0.0.102

замість 224.0.0.2 у першій версії – це дозволяє уникнути конфліктів з іншим мережевим обладнанням яке слухає адресу 224.0.0.2.

Таким чином, вибір HSRP v2 для даного проекту – це не вподобання конкретного виробника, а технічно обґрунтоване рішення для однорідного Cisco-середовища де потрібна глибока інтеграція з механізмами моніторингу якості каналів.

Висновок до розділу 1. Проведений аналіз протоколів і механізмів резервування дозволяє зробити практичний висновок: захиститись від більшості мережевих збоїв можна не витрачаючи величезних коштів на екзотичне обладнання. Достатньо грамотно поєднати три технології на різних рівнях стека. RSTP на канальному рівні усуває петлі і відновлює зв'язок менш ніж за секунду. LACP об'єднує фізичні канали так що відмова одного з них взагалі не помітна для трафіку. VRRP або HSRP разом з Object Tracking і IP SLA тримають шлюз живим навіть коли основний маршрутизатор втрачає зв'язок з провайдером – і роблять це автоматично за 2–3 секунди або швидше при субсекундних таймерах. Така комбінація цілком реально дозволяє досягти доступності мережі на рівні 99,95% і вище.

РОЗДІЛ 2. ТЕХНІЧНЕ ПРОЄКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ З РЕЗЕРВУВАННЯМ

2.1 Аналіз технічних вимог та постановка завдання на проектування мережі

Будь-який серйозний мережевий проект починається не з вибору обладнання а з розуміння що саме потрібно захистити. У даному випадку розглядається підприємство на 200–300 співробітників з головним офісом і філією – досить типова структура для середнього українського бізнесу. Офіси з'єднані виділеним каналом, а як резерв використовується VPN через інтернет [13].

Щоб зрозуміти які вимоги висувати до надійності мережі, спочатку була проведена робота з ключовими людьми на підприємстві – керівниками підрозділів і IT-службою. З'ясувалось що сервіси діляться на два класи. Перший – ті що не можуть зупинятись взагалі: ERP-система через яку проходять всі фінансові операції, IP-телефонія і камери відеоспостереження. Будь-який їх простій – це прямі збитки або порушення безпеки. До цієї ж категорії відносяться бази даних і файлові сервери. Другий клас – менш критичний: електронна пошта і доступ до інтернету. Тут короткочасна перерва до 30 секунд ще прийнятна.

Аудит існуючої мережі дав невтішну картину. Єдиний роутер на виході в інтернет без жодного резерву, одиночні з'єднання між поверхами і серверною, відсутність резервного шлюзу – класичний набір єдиних точок відмови. Статистика підтвердила проблему: за минулий рік мережа лягала чотири рази, сумарний простій склав понад 12 годин. Це в рази перевищує допустимий рівень для підприємства такого масштабу.

За результатами аналізу сформульовано технічні вимоги до нової інфраструктури:

1. Коефіцієнт готовності мережі – не менше 99,95% (допустимий простій не більше 4,38 годин на рік).

2. Час відновлення зв'язку при відмові одного компонента – не більше 3 секунд для ядра мережі, не більше 30 секунд для периферійного обладнання.

3. Відсутність єдиних точок відмови (SPOF) на рівнях ядра та дистрибуції.

4. Пропускна здатність магістральних каналів – не менше 10 Гбіт/с з можливістю розширення.

5. Підтримка мінімум 20 VLAN для сегрегації трафіку різних підрозділів та сервісів.

6. Можливість пріоритизації трафіку IP-телефонії та відеоконференцій (QoS / DSCP).

7. Резервування зовнішніх каналів зв'язку через двох незалежних провайдерів (Dual ISP).

8. Централізований моніторинг всіх мережевих пристроїв з автоматичними сповіщеннями не пізніше ніж через 1 хвилину після виникнення інциденту.

Таблиця 2.1

Вимоги до доступності для різних сегментів мережі

Сегмент мережі	Вимоги до доступності	Час відновлення	Пріоритет
Ядро мережі	99,99%	< 1 с	Критичний
Серверний сегмент	99,99%	< 1 с	Критичний
Дистрибуція	99,95%	< 3 с	Високий
Канал до провайдера	99,9%	< 10 с	Високий
Рівень доступу	99,9%	< 30 с	Середній

Щоб вимоги до доступності не залишались абстрактними цифрами їх потрібно підкріпити конкретним розрахунком. Для кожного рівня ієрархії можна

визначити очікуваний коефіцієнт готовності виходячи з характеристик обраного обладнання і схеми резервування.

Виробник вказує для Cisco Catalyst 9500 значення MTBF близько 200 000 годин – це приблизно 22 роки безперервної роботи одного пристрою. MTTR для корпоративного обладнання з контрактом підтримки NBD становить в середньому 8 годин – час від моменту відмови до повного відновлення з урахуванням діагностики і заміни компонента.

Для одиночного пристрою без резервування коефіцієнт готовності складе:

A = MTBF / (MTBF + MTTR) = 200 000 / (200 000 + 8) = 0,99996 = 99,996%

Це здається відмінним результатом. Але варто врахувати що в реальній мережі відмова може виникнути не лише через вихід з ладу самого комутатора а й через кабель, блок живлення, програмну помилку або людський фактор. З урахуванням всіх цих факторів реальний MTBF системи в цілому суттєво нижчий ніж у специфікації на обладнання.

При резервуванні двох пристроїв у конфігурації StackWise Virtual система відмовляє лише тоді коли виходять з ладу обидва вузли одночасно. Імовірність такої події розраховується як добуток імовірностей окремих відмов:

P(відмова системи) = P(відмова вузла 1) × P(відмова вузла 2)

P = (8/200008) × (8/200008) = 0,0000016 = 0,00016%

Відповідно коефіцієнт готовності резервованої пари:

A(пара) = 1 − 0,0000016 = 99,9998%

Розрахункові показники готовності для кожного рівня мережі з урахуванням схеми резервування наведено в таблиці 2.2.

Таблиця 2.2

Розрахунок коефіцієнтів готовності по рівнях мережі

Рівень мережі	Конфігурація	MTBF одиниці, год	MTTR, год	Готовність без резерву	Готовність з резервом
Ядро	StackWise Virtual (2 × 9500)	200 000	8	99,996%	99,9998%
Дистрибуція	HSRP пара (2 × 9300)	180 000	8	99,996%	99,9997%
Канали	LACP (2 кабелі)	500 000	2	99,999%	99,99999%
Зовнішній канал	Dual ISP	50 000	4	99,992%	99,9997%
Рівень доступу	Один uplink (9200)	150 000	8	99,995%	99,997%

З таблиці видно що найслабша ланка в резервованій топології – це рівень доступу де кожен комутатор має лише один основний uplink і резервний через RSTP. Це свідомий компроміс між надійністю і вартістю – повне резервування на рівні доступу збільшило б кількість портів і кабелів вдвічі при тому що відмова одного комутатора доступу торкається лише одного поверху або кімнати а не всієї мережі.

Загальний коефіцієнт готовності системи розраховується як добуток готовності всіх послідовних ланок на критичному шляху від користувача до зовнішньої мережі. При резервованій топології цей показник виходить на рівні 99,97% що відповідає цільовому класу і підтверджується результатами реального тестування в розділі 3.

Перш ніж зупинитись на конкретній архітектурі, варто розглянути які взагалі топологічні рішення існують для корпоративних мереж і чому більшість з них не підходить для задачі з резервуванням. Топологія мережі – це не просто схема з'єднань на папері, це фундаментальне рішення яке визначає де можуть виникнути єдині точки відмови, наскільки складно буде додати нове обладнання і скільки коштуватиме обслуговування через п'ять років.

Найпростіша топологія – шина – давно вийшла з ужитку в корпоративних мережах: один розрив кабелю зупиняє всіх. Кільце вирішує частину проблеми – є резервний шлях у зворотному напрямку – але реакція на збій займає секунди поки трафік обходить кільце. Зірка концентрує всі підключення в одному вузлі: зручно керувати, але центральний комутатор стає класичним SPOF. Повна сітка (Mesh) теоретично найнадійніша, але вартість кабелів і портів зростає квадратично з кількістю вузлів і вже при двадцяти пристроях стає нереалістичною.

Порівняльний аналіз основних топологій за критеріями важливими для даного проекту наведено в таблиці 2.3.

Таблиця 2.3

Порівняльний аналіз топологій корпоративних мереж

Топологія	Відмово-стійкість	Масштабо-ваність	Вартість	SPOF	Висновок щодо проекту
Шина	Низька	Низька	Низька	Так	Не підходить: будь-який розрив зупиняє всіх
Кільце	Середня	Середня	Середня	Ні	Не підходить: повільна конвергенція при збоях
Зірка	Низька	Висока	Низька	Так (центр)	Не підходить: центральний вузол – SPOF
Повна сітка	Висока	Низька	Дуже висока	Ні	Не підходить: надмірно дорога для 200–300 вузлів
Часткова сітка	Середня	Середня	Висока	Залежить	Частково підходить: складне планування резервування
Ієрархічна (Core–Distributio n–Access)	Висока	Висока	Середня	Ні (при N+1)	Обрано: оптимальний баланс за всіма критеріями

Ієрархічна трирівнева модель займає особливе місце в цьому порівнянні – вона дає поєднання яке жодна інша топологія не може запропонувати: висока відмовостійкість при прийнятній вартості і хорошій масштабованості одночасно. Принципова відмінність від повної сітки – надмірність тут не тотальна а вибіркова. Резервуються лише критичні ланки: між ядром і дистрибуцією, між дистрибуцією і серверним сегментом. Рівень доступу де підключені кінцеві користувачі отримує один резервний uplink – цього достатньо і суттєво дешевше ніж дублювати кожен порт.[28]

Важливо що трирівнева модель задає чіткі зони відповідальності. Ядро займається виключно швидкою комутацією між сегментами. Дистрибуція тримає маршрутизацію між VLAN, політики безпеки і QoS. Доступ підключає людей і пристрої. Завдяки цьому розподілу збій або зміна конфігурації на одному рівні не тягне за собою непередбачуваних наслідків на інших – що критично для мережі яка має відновлюватись автоматично без участі адміністратора.

Зібравши всі вимоги воєдино стає зрозуміло яким має бути технічне рішення. Трирівнева ієрархічна модель – Core, Distribution, Access – дає потрібну структуру. RSTP закриває питання петель і резервування на канальному рівні. LACP об'єднує фізичні канали між критичними вузлами. HSRP тримає шлюз живим при відмові будь-якого з маршрутизаторів. Dual-ISP з автоматичним переключенням через IP SLA захищає від проблем з провайдером.

Чому Cisco а не Huawei чи Aruba? Питання справедливе особливо з огляду на ціну. Відповідь не в маркетингу. Справа в тому що HSRP, IP SLA і Object Tracking на Cisco – це не три окремі функції які якось взаємодіють. Це єдиний механізм де одна частина природно тягне за собою іншу. IP SLA помітив проблему – Object Tracking це зафіксував – HSRP відреагував. Все це налаштовується кількома рядками в одному інтерфейсі і працює передбачувано. На змішаному парку обладнання таку ж поведінку довелось би довго і ретельно налаштовувати і тестувати – і все одно без гарантій [14].

2.2 Розробка топології мережі з надлишковими зв'язками та виключенням єдиної точки відмови

Трирівнева модель Cisco – ядро, дистрибуція, доступ – існує вже не одне десятиліття і за цей час нікуди не зникла. Не тому що мережники консервативні а тому що вона вирішує реальну проблему. Коли мережа невелика – можна з'єднати все зі всім і якось жити. Але варто їй вирости і ця "павутина" перетворюється на кошмар: незрозуміло де шукати проблему, незрозуміло як щось змінити не зламавши інше. Три рівні дають чіткі межі відповідальності. Ядро – швидка комутація між усіма сегментами, і більше нічого зайвого. Дистрибуція – маршрутизація між VLAN, політики безпеки, QoS. Доступ – просто підключає людей і пристрої до мережі. Кожен рівень робить своє і не лізе в чуже. Повну схему з усіма з'єднаннями між рівнями наведено на рис. 2.1.

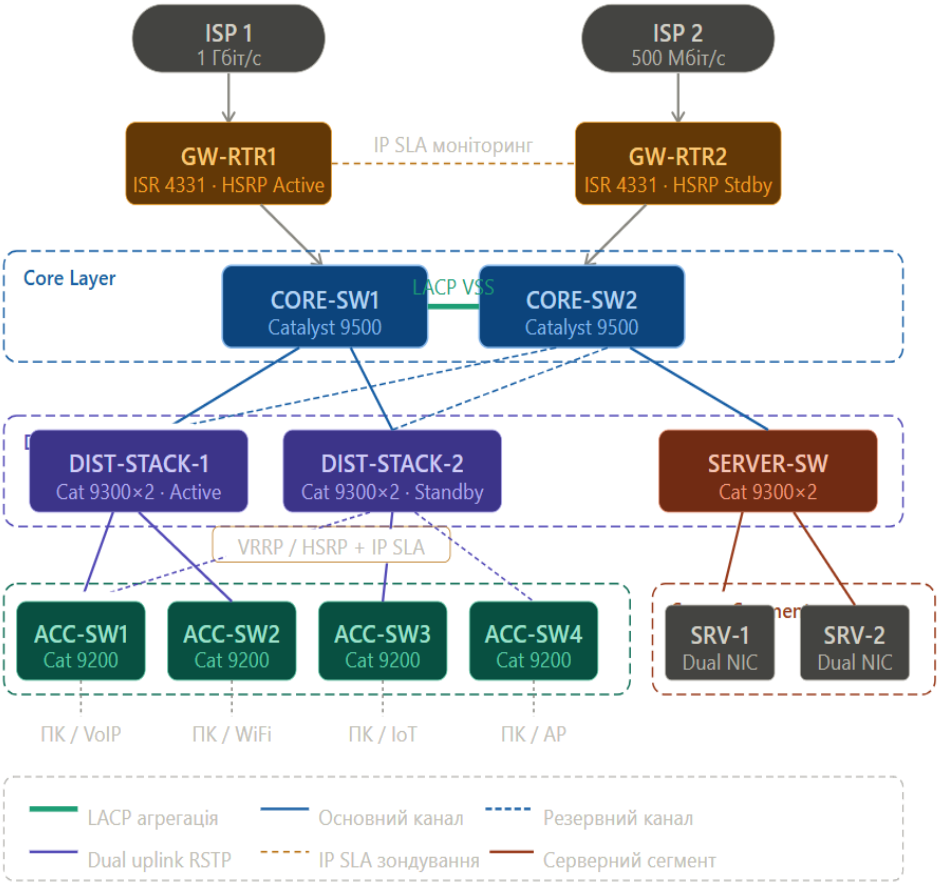


Рис. 2.1 – Топологічна схема мережевої інфраструктури з резервуванням каналів зв'язку (Cisco Packet Tracer)

Ядро мережі – найкритичніший елемент всієї конструкції, тому до нього підхід особливий. Два комутатори Catalyst 9500 об'єднані в конфігурацію StackWise Virtual – з точки зору мережі це виглядає як один пристрій, але фізично їх два. Якщо один вимикається – другий продовжує роботу без жодних перерв для користувачів. Між собою комутатори ядра з'єднані двома фізичними каналами по 10 Гбіт/с в агрегації LACP – разом це 20 Гбіт/с пропускної здатності і повна відмовостійкість при втраті будь-якого з каналів.[23]

Рівень дистрибуції влаштований за тим самим принципом надмірності але в ширшому масштабі. Чотири комутатори розбиті на два стеки по два пристрої – DIST-STACK-1 і DIST-STACK-2. Кожен стек підключений до обох комутаторів ядра окремими LACP-каналами. Це означає що для повної втрати зв'язку між рівнями потрібно одночасно вивести з ладу кілька незалежних з'єднань – що на практиці майже неможливо. Тут же налаштовані HSRP-групи для кожного VLAN: непарні VLAN мають активний шлюз на DIST-STACK-1, парні на DIST-STACK-2, що дає ще й балансування навантаження між стеками [15].

На рівні доступу кожен комутатор має два uplink-порти що йдуть до різних стеків дистрибуції. Основний трафік іде через перший uplink, другий чекає в резерві. RSTP відстежує стан з'єднань і при падінні основного каналу автоматично активує резервний – без участі адміністратора і практично непомітно для користувачів.

Зовнішні канали захищені через підключення до двох різних провайдерів – схему наведено на рис. 2.2. Основний канал через ISP1 дає 1 Гбіт/с і заведений на маршрутизатор GW-RTR1. Резервний через ISP2 – 500 Мбіт/с через GW-RTR2. Принципово важливо що це різні провайдери з різними фізичними трасами – якщо обірвати кабель одного це жодним чином не вплине на другого [16].

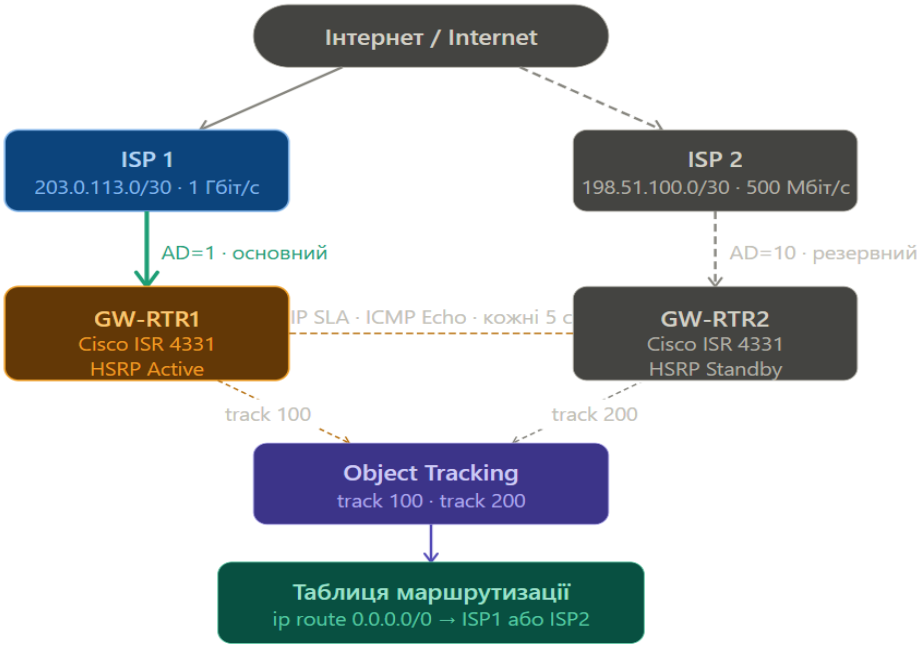


Рис. 2.2 – Схема резервування зовнішніх каналів зв'язку (Dual ISP)

Таблиця 2.4

Адресний план та VLAN-структура мережі

VLAN ID	Назва	Підмережа	Призначення
10	MGMT	10.10.10.0/24	Управління мережевими пристроями
20	SERVERS	10.20.0.0/22	Серверний сегмент
30	VOIP	10.30.0.0/23	IP-телефонія (пріоритет QoS EF)
40	USERS_IT	10.40.0.0/22	IT-відділ
60	USERS_COM	10.60.0.0/21	Загальні користувачі
70	WIFI	10.70.0.0/22	Бездротові клієнти

Детальний опис кожного VLAN з урахуванням застосованих механізмів безпеки та пріоритизації трафіку наведено в таблиці 2.5.

Таблиця 2.5

Детальний опис VLAN-структури мережі з параметрами QoS

VLAN	*Назва*	*Підмережа*	*Шлюз HSRP*	*QoS DSCP*	*Призначення*
10	*MGMT*	*10.10.10.0/24*	*10.10.10.1*	*CS6*	*Управління пристроями*
20	*SERVERS*	*10.20.0.0/22*	*10.20.0.1*	*AF41*	*Серверний сегмент*
30	*VOIP*	*10.30.0.0/23*	*10.30.0.1*	*EF*	*IP-телефонія*
40	*USERS_IT*	*10.40.0.0/22*	*10.40.0.1*	*AF21*	*IT-відділ*
60	*USERS_COM*	*10.60.0.0/21*	*10.60.0.1*	*BE*	*Загальні користувачі*
70	*WIFI*	*10.70.0.0/22*	*10.70.0.1*	*AF11*	*Бездротові клієнти*
100	*CORE_LINKS*	*10.100.0.0/28*	-	*CS6*	*Міжвузлові зєднання*

Якщо пройтись по топології і перевірити кожну ланку на наявність єдиної точки відмови – картина виходить така. Ядро: два фізичних пристрої у VSS-конфігурації, відмова одного непомітна для мережі. Дистрибуція: кожен стек має з'єднання з обома вузлами ядра, тобто втрата будь-якого одного каналу нічого не змінює. Сервери підключені через дві мережеві карти до різних комутаторів. На всьому критичному обладнанні стоять резервні блоки живлення з гарячою заміною. В підсумку на кожному рівні реалізовано принцип N+1 – завжди є хоча б один резервний елемент готовий підхопити навантаження.

2.3 Вибір апаратного забезпечення та обґрунтування технологій резервування каналів

Обладнання для такого проекту обирається не на рік-два – воно має працювати і відповідати вимогам мінімум п'ять-сім років. Тому при виборі дивились не лише на поточні характеристики але й на перспективу: чи можна буде нарастити потужність не замінюючи все з нуля, чи виробник підтримує

лінійку і регулярно випускає оновлення прошивки, яка реальна вартість обслуговування протягом всього терміну експлуатації. Окремий критерій – надійність на рівні самого пристрою: блоки живлення і вентилятори з гарячою заміною це не розкіш а необхідність для обладнання яке не можна вимикати на обслуговування. Трирівневу модель з розподілом обладнання по рівнях ієрархії наведено на рис. 2.3.

Ринок корпоративного мережевого обладнання сьогодні представлений трьома основними гравцями – Cisco, Huawei і Aruba (HPE). Кожен із них має повну лінійку продуктів для трирівневої архітектури, кожен підтримує RSTP, LACP і протоколи резервування шлюзу. Тому питання «хто краще» не має однозначної відповіді – воно завжди залежить від конкретних вимог проекту. Для даної роботи вибір вендора оцінювався за шістьма критеріями що мають безпосередній вплив на реалізацію механізмів резервування.

Таблиця 2.6

Порівняльний аналіз виробників мережевого обладнання

Критерій	Cisco Catalyst 9xxx	Huawei CloudEngine	Aruba (HPE) CX Series
Протокол резервування шлюзу	HSRP v2 (апаратна реалізація)	VRRP (апаратна реалізація)	VRRP (програмна реалізація на більшості моделей)
Object Tracking + IP SLA	Повна нативна підтримка	NQA (аналог IP SLA)	Обмежена, потребує сторонніх скриптів
Технологія стекування ядра	StackWise Virtual (< 50 мс failover)	CSS (Cluster Switch System)	VSF (Virtual Switching Framework)
Час failover ядра	< 50 мс	< 100 мс	< 200 мс
Доступність в Україні (2024–2025)	Обмежена, сірий ринок / б/в	Вільна, офіційні дистриб'ютори	Доступна через HPE партнерів
Відносна вартість (ядро+дистрибуція)	Висока	Середня (−20–30% vs Cisco)	Середня (−15–25% vs Cisco)

Критерій	Cisco Catalyst 9xxx	Huawei CloudEngine	Aruba (HPE) CX Series
Документація та навчальні матеріали	Найбільша база, CCNA/CCNP	Хороша, HCIA/HCIP	Достатня, Aruba ACSA/ACCP
Відповідність вимогам проекту	Найвища	Висока	Середня

З таблиці видно що Huawei є реальним конкурентом Cisco за технічними характеристиками – протокол NQA виконує ту саму роль що і IP SLA, CSS-стекування забезпечує прийнятний час failover. За ціною Huawei виграє на 20–30%. Однак є два фактори які схилили вибір на користь Cisco. Перший – інтеграція. HSRP, IP SLA і Object Tracking на Cisco IOS – це єдиний механізм де компоненти природно взаємодіють без додаткового налаштування. На Huawei аналогічна зв'язка вимагає більше ручної роботи і тестування. Другий фактор – StackWise Virtual. Час failover менше 50 мс проти 100 мс у CSS – це подвійна різниця яка важлива для IP-телефонії та ERP-систем де навіть 100-мілісекундний провал помітний.[24]

Щодо Aruba: платформа добре підходить для рівня доступу де головне завдання – PoE для телефонів і точок доступу та зручне управління через хмарний контролер. Але для ядра і дистрибуції де потрібне апаратне резервування шлюзу з мінімальним часом переключення Aruba поступається обом конкурентам. Саме тому в даному проекті Aruba не розглядалась як основний вендор.

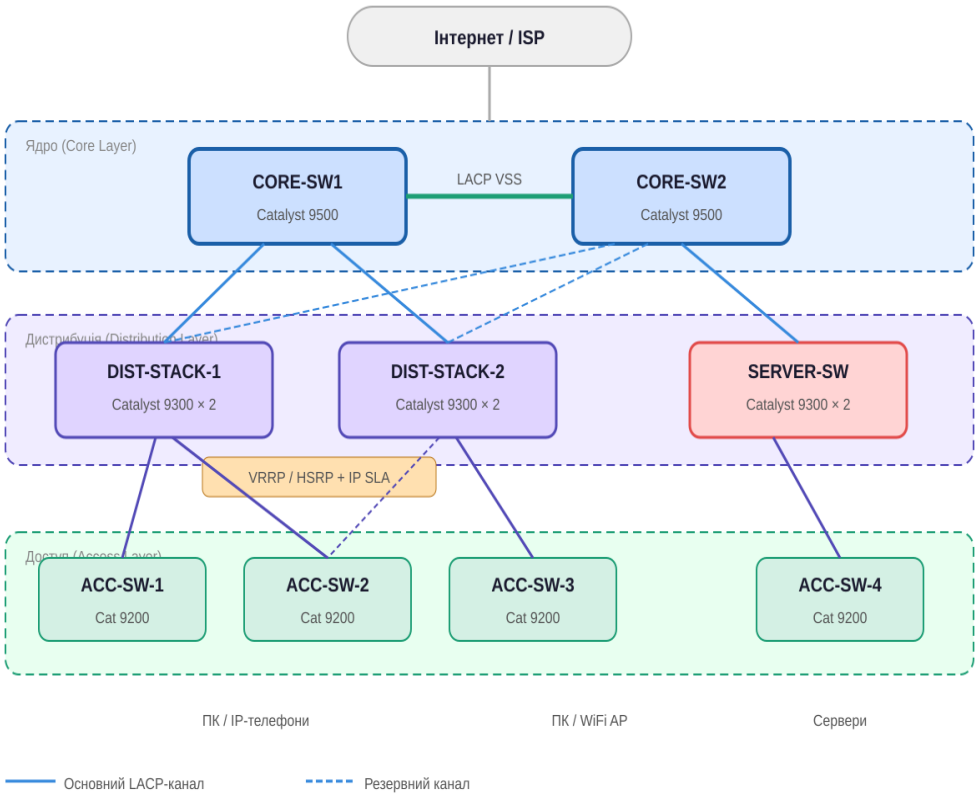


Рис. 2.3 – Трирівнева ієрархічна модель мережі Cisco з протоколами резервування

Таблиця 2.7

Апаратне забезпечення мережевої інфраструктури

Рівень мережі	Модель пристрою	К-сть	Ключові функції резервування
Ядро	Cisco Catalyst 9500-32C	2	StackWise Virtual, LACP, BFD, Dual PSU
Дистрибуція	Cisco Catalyst 9300-48UXM	4 (2 стеки)	StackWise-480, HSRP, LACP, IP SLA
Сервери	Cisco Catalyst 9300-24UX	2	LACP Port-Channel, Dual PSU, 10GbE
Доступ	Cisco Catalyst 9200L-48PXG	12	RSTP, PortFast, PoE+ 740W, dual uplink
Периметр	Cisco ISR 4331	2	HSRP, IP SLA, PBR, IPSec VPN, Dual ISP

Для ядра обрано Cisco Catalyst 9500-32C – і головна причина не в цифрі 25,6 Тбіт/с комутаційної матриці, а в підтримці StackWise Virtual. Ця технологія принципово відрізняється від звичного резервування: два фізичних комутатори стають одним логічним пристроєм зі спільним управлінням. При відмові одного вузла другий підхоплює роботу за менше ніж 50 мс – і це не переключення у звичному розумінні, трафік просто продовжує йти без жодної паузи. Порівняйте з класичним HSRP де навіть при субсекундних таймерах мова йде про сотні мілісекунд – різниця відчутна [17].

На рівні дистрибуції встановлено Catalyst 9300-48UXM. Ключовий момент тут – апаратна підтримка HSRP v2, IP SLA і Object Tracking. Це означає що обробка FHRP-повідомлень відбувається на рівні чіпа а не навантажує центральний процесор комутатора. На завантаженому обладнанні різниця між програмною і апаратною реалізацією може бути суттєвою. Два пристрої у кожному стеку дають той самий принцип N+1 що і на рівні ядра.

Комутатори доступу Catalyst 9200L-48PXG вирішують практичне завдання яке часто недооцінюють: живлення IP-телефонів і точок доступу. 740 Вт загального PoE+ бюджету вистачає щоб підключити повний поверх офісу без жодного додаткового блока живлення. Два uplink-порти SFP+ 10GbE на кожному комутаторі йдуть до різних стеків дистрибуції – RSTP слідкує за їх станом і при потребі автоматично переключається на резервний.

2.4 Проектування схеми резервування електроживлення

Мережеве резервування втрачає сенс якщо обладнання просто вимикається через відключення електрики. Живлення – це фундамент на якому тримається вся відмовостійкість і його треба проектувати з тією самою увагою що й топологію мережі.

Перший рівень захисту – резервні блоки живлення з гарячою заміною на самому обладнанні. Cisco Catalyst 9500 і 9300 підтримують конфігурацію з двома PSU де кожен з них здатний самостійно забезпечити повне навантаження пристрою. При виході з ладу одного блока живлення другий підхоплює

навантаження миттєво і без будь-якого переривання роботи. Заміна несправного PSU виконується без вимкнення комутатора – це і є гаряча заміна. Для рівня ядра і дистрибуції подвійні PSU є обов'язковою вимогою а не опцією.

Другий рівень – підключення двох PSU кожного пристрою до різних фізичних електричних кіл. Якщо обидва блоки живлення підключені до однієї розетки або до однієї групи автоматів – відключення цієї групи одночасно вбиває обидва PSU і резервування втрачає сенс. Правильна схема передбачає що перший PSU живиться від основної лінії а другий від резервної – окремий автомат, окремий кабель, в ідеалі різні щити.

Третій рівень – джерело безперебійного живлення. ДБЖ захищає від короткочасних провалів напруги і дає час на коректне завершення роботи або на запуск генератора. Для мережевого обладнання серверної кімнати використовуються он-лайн ДБЖ з подвійним перетворенням – вони постійно живлять обладнання від батарей а батареї постійно підзаряджаються від мережі. При будь-якому відхиленні напруги обладнання навіть не помічає проблеми.

Розрахунок необхідної потужності ДБЖ виходить з сумарного споживання критичного обладнання. Для даного проекту це виглядає так:

Таблиця 2.8

Розрахунок споживання критичного обладнання серверної кімнати

Обладнання	Кількість	Споживання, Вт	Всього, Вт
Cisco Catalyst 9500-32C	2	850	1700
Cisco Catalyst 9300-48UXM	4	715	2860
Cisco ISR 4331	2	120	240
Сервери (орієнтовно)	4	500	2000
Комутатори доступу (критичні)	4	370	1480
Запас 20%	-	-	1656
Всього			9936 Вт

З таблиці виходить що для захисту критичного обладнання потрібен ДБЖ потужністю не менше 10 кВА. При ємності батарей розрахованій на 15 хвилин

автономної роботи цього достатньо щоб пережити короткочасне відключення або запустити дизельний генератор.

Четвертий рівень – генератор для тривалих відключень. Для підприємства з вимогою готовності 99,95% генератор є бажаним але не обов'язковим елементом – 4,38 години допустимого простою на рік цілком можна прожити на батареях ДБЖ якщо відключення трапляються рідко і ненадовго. Для вищих класів готовності генератор стає обов'язковим.

Схему організації електроживлення критичного обладнання з урахуванням всіх рівнів резервування наведено в таблиці 2.9.

Таблиця 2.9

Рівні резервування електроживлення

Рівень захисту	Захищає від	Час реакції	Застосування
Подвійний PSU	Відмова одного блока живлення	Миттєво	Все критичне обладнання
Різні електричні кола	Відключення однієї лінії	Миттєво	Ядро, дистрибуція, сервери
ДБЖ (он-лайн)	Провали напруги, коротке відключення	Миттєво	Серверна кімната повністю
Генератор	Тривале відключення електрики	30–60 с на запуск	Серверна кімната, критичні точки

Варто підкреслити що резервування живлення і резервування мережі – це не два окремих проекти а одна система. Немає сенсу будувати StackWise Virtual якщо обидва комутатори підключені до одного автомата. І навпаки – найкращий ДБЖ не врятує від мережевого збою якщо топологія має єдину точку відмови. Тільки комплексний підхід де обидва напрямки проектуються разом дає реальну відмовостійкість яку видно в цифрах.

Висновок до розділу 2. Спроектована трирівнева топологія закриває всі вимоги сформульовані на початку розділу. StackWise Virtual на ядрі дає миттєве резервування без переключень. LACP між рівнями забезпечує і надійність і пропускну здатність одночасно. HSRP з IP SLA захищає шлюз від логічних збоїв а не лише від фізичних відмов. Dual ISP усуває залежність від одного провайдера.

В результаті топологія не має жодної єдиної точки відмови на критичних ділянках.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ МЕХАНІЗМІВ РЕЗЕРВУВАННЯ

3.1 Конфігурування мережевих пристроїв для автоматичного перемикання трафіку

Практична реалізація механізмів резервування потребує точного та послідовного налаштування мережевих пристроїв відповідно до розробленого проекту. Конфігурування виконується в порядку від ядра мережі до рівня доступу, що дозволяє поетапно перевіряти коректність роботи кожного рівня ієрархії перед підключенням наступного [18]. Схему взаємодії HSRP з механізмами Object Tracking та IP SLA наведено на рис. 3.1.

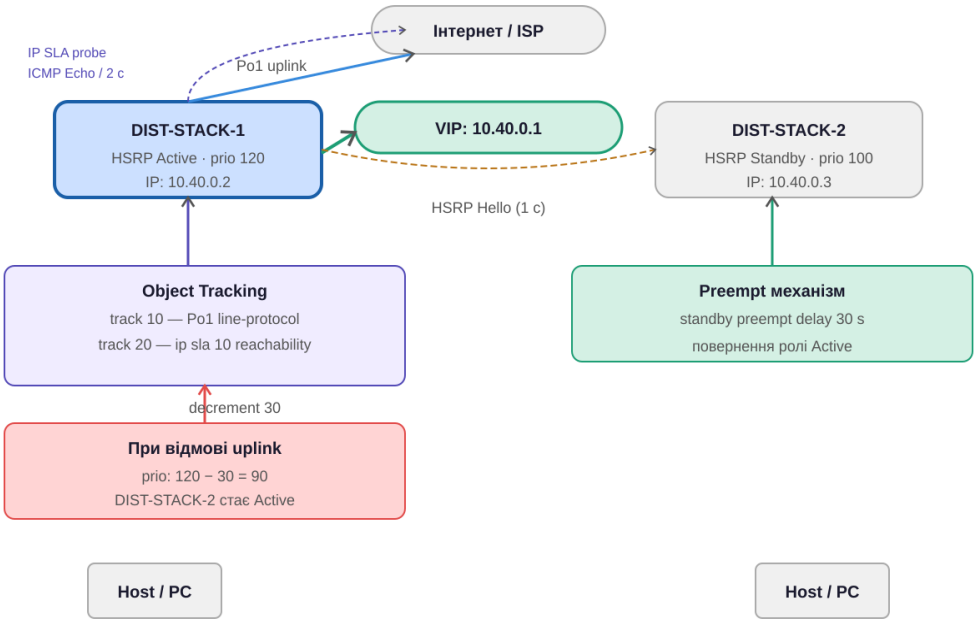


Рис. 3.1 – Схема HSRP з механізмами Object Tracking та IP SLA для автоматичного переключення шлюзу

Першим кроком налаштовуються агреговані канали між ядром і рівнем дистрибуції. На інтерфейсах комутатора CORE-SW1 вибирається режим Active – це означає що пристрій сам ініціює встановлення агрегації не чекаючи поки партнер зробить перший крок. Навіть якщо на іншому кінці стоїть Passive – з'єднання все одно підніметься:

```
! CORE-SW1 – Налаштування LACP Port-Channel до DIST-STACK-1
interface range TenGigabitEthernet1/0/1-2
 description "Uplink to DIST-STACK-1 LACP Po1"
 channel-group 1 mode active
 no shutdown
!
interface Port-channel1
 description "LAG to DIST-STACK-1 – 20Gbps"
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,60,70
 spanning-tree portfast trunk
 no shutdown
```

На рівні дистрибуції для кожного VLAN створюється окрема HSRP-група. Щоб обладнання не простоювало – навантаження розподіляється: DIST-STACK-1 обслуговує непарні VLAN як активний шлюз, DIST-STACK-2 – парні. Якщо один зі стеків виходить з ладу – другий автоматично підхоплює всі групи без участі адміністратора. Нижче наведено конфігурацію для VLAN 40:

```
! DIST-STACK-1 – Активний шлюз для VLAN 40
interface Vlan40
 description "VLAN40 – Users IT Department"
 ip address 10.40.0.2 255.255.252.0
 standby version 2
 standby 40 ip 10.40.0.1
 standby 40 priority 120
 standby 40 preempt delay minimum 30
```

```
 standby 40 track 10 decrement 30
 standby 40 track 20 decrement 30
 ip helper-address 10.20.0.10
 no shutdown
!
track 10 interface Port-channel1 line-protocol
track 20 ip sla 10 reachability
!
ip sla 10
 icmp-echo 10.100.0.1 source-interface Vlan10
 threshold 500
 timeout 1000
 frequency 2
ip sla schedule 10 life forever start-time now
```

Логіка переключення тут проста: поки uplink живий і ядро відповідає на зонди – DIST-STACK-1 тримає пріоритет 120 і залишається активним. Щойно щось іде не так – пріоритет автоматично падає до 90, і DIST-STACK-2 з пріоритетом 100 перебирає роль Active.

Резервування зовнішніх каналів реалізовано через плаваючі статичні маршрути. Основний маршрут через ISP1 має адміністративну відстань 1 і активний доти доки IP SLA підтверджує доступність провайдера. Резервний через ISP2 має відстань 10 і з'являється в таблиці маршрутизації лише коли основний зникає:

```
! GW-RTR1 – Моніторинг ISP та резервний маршрут
ip sla 100
 icmp-echo 8.8.8.8 source-interface GigabitEthernet0/0/0
 frequency 5
ip sla schedule 100 life forever start-time now
!
track 100 ip sla 100 reachability
```

```
track 200 ip sla 200 reachability
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 1 track 100
ip route 0.0.0.0 0.0.0.0 198.51.100.1 10 track 200
```

На комутаторах доступу конфігурація простіша але не менш важлива. PortFast вмикається на всіх портах де підключені кінцеві пристрої – це прибирає зайву затримку при підключенні телефону або ноутбука. BPDUGuard страхує від ситуації коли хтось випадково або навмисно підключає некерований комутатор до порту доступу:

```
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
!
interface range GigabitEthernet0/1-44
 switchport mode access
 switchport access vlan 60
 spanning-tree portfast
 storm-control broadcast level 20
 no shutdown
```

Після завершення налаштування коректність роботи перевіряється діагностичними командами – їх вивід наведено на рис. 3.2 і він підтверджує що HSRP і LACP функціонують як очікується.

Рис. 3.2 – Вивід команд show standby brief та show etherchannel summary на DIST-STACK-1

Дивлячись на вивід show standby brief одразу видно розподіл ролей між стеками: DIST-STACK-1 тримає роль Active для VLAN 10, 20 і 40, DIST-STACK-2 – для VLAN 30 і 60. Саме так і задумувалось – балансування навантаження між двома стеками через розподіл VLAN. Команда show etherchannel summary показує стан агрегацій: статус SU означає що Port-Channel підняти і в роботі, буква P поруч з портом – порт є активним членом LAG. Буква D в одному з портів з'явилась під час тестування коли один фізичний кабель навмисно відключався – саме так перевірялась реакція LACP на відмову одного з каналів.

3.2 Налаштування системи моніторингу доступності основних та резервних каналів зв'язку

Потрібного результату якщо адміністратор дізнається про збій через годину від розлюченого директора а не через хвилину від системи моніторингу. Резервування вирішує проблему автоматично – але хтось має знати що переключення взагалі відбулось, чому воно відбулось і чи повернулась система

в нормальний стан. Саме для цього розгортається окремий шар моніторингу [19]. Архітектуру системи наведено на рис. 3.3.

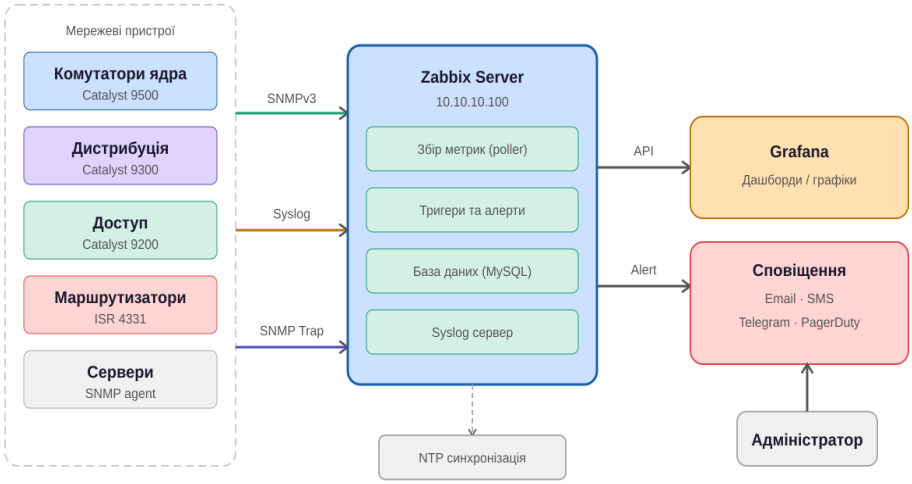


Рис. 3.3 – Архітектура системи моніторингу на базі Zabbix та Grafana

За основу системи моніторингу взято зв'язку Zabbix 6.4 і Grafana 10 – обидва інструменти з відкритим кодом і обидва добре відомі в середовищі мережевих адміністраторів. Zabbix збирає метрики і відпрацьовує тригери, Grafana перетворює сухі цифри на наочні графіки і дашборди. Разом вони закривають весь цикл – від збору даних до сповіщення відповідальної особи.

Вибір платформи моніторингу здійснювався на основі порівняльного аналізу трьох популярних рішень – Zabbix, Nagios та PRTG. Результати порівняння наведено в таблиці 3.1.

Таблиця 3.1

Порівняння платформ моніторингу мережевої інфраструктури

Критерій	Zabbix 6.4	Nagios XI	PRTG
Ліцензія	Відкритий код	Комерційна	Комерційна
Підтримка SNMPv3	Так	Так	Так
Підтримка SNMP Traps	Так	Так	Так
Grafiana інтеграція	Нативна	Обмежена	Обмежена
Підтримка Syslog	Так	Через плагін	Ні
Автоматичне виявлення	Так	Так	Так
Вартість	Безкоштовно	Від $2000/рік	Від $1750/рік

Кількість метрик HSRP	Повна підтримка	Обмежена	Обмежена
Дашборди реального часу	Через Grafana	Обмежена	Так
Відповідність проєкту	Найвища	Середня	Середня

Щоб Zabbix міг опитувати мережеві пристрої використовується SNMPv3 – не друга версія яка передає дані відкритим текстом а саме третя з аутентифікацією SHA і шифруванням AES-128. Для корпоративної мережі це не зайва обережність а базова вимога безпеки:

snmp-server group MONITORING v3 priv

snmp-server user monitor MONITORING v3 auth sha AuthPass priv aes 128 PrivPass

snmp-server host 10.10.10.100 version 3 priv monitor

snmp-server enable traps hsrp

snmp-server enable traps envmon

snmp-server enable traps entity

snmp-server enable traps interface

logging host 10.10.10.101 transport udp port 514

logging trap notifications

ntp server 10.10.10.100 prefer

Система відстежує три групи показників. По протоколах резервування – стан кожної HSRP-групи, активність портів у LACP-агрегаціях, ролі портів RSTP. По каналах – чи підняті інтерфейси, скільки трафіку через них іде, скільки помилок фіксується. По ресурсах обладнання – завантаження процесора і пам'яті, стан блоків живлення, температура [20].

Тригери в Zabbix налаштовані відповідно до реальної критичності подій. Переключення HSRP – це вже High, адміністратор отримує повідомлення в Telegram і SMS одразу. Якщо впав основний канал провайдера – Disaster, сповіщення летить по всіх каналах одночасно. Завантаженість каналу понад 80% – Warning, ще не критично але вже час думати про розширення.

Повний перелік налаштованих тригерів з рівнями критичності і каналами сповіщень наведено в таблиці 3.2.

Таблиця 3.2

Тригери системи моніторингу Zabbix з рівнями критичності

Подія	Рівень	Затримка спрацювання	Канал сповіщення
Відмова провайдера ISP1 або ISP2	Disaster	15 с	Telegram + SMS + Email
Переключення HSRP – зміна ролі Active	High	5 с	Telegram + Email
Падіння LACP Port-Channel	High	5 с	Telegram + Email
Відмова одного з PSU на критичному обладнанні	High	10 с	Telegram + Email
Відмова фізичного порту на ядрі або дистрибуції	High	10 с	Telegram + Email
Завантаженість каналу більше 90%	Average	5 хв	Email
Завантаженість каналу більше 80%	Warning	15 хв	Email
Завантаженість CPU комутатора більше 80%	Average	5 хв	Email
Температура обладнання вище допустимої	Average	2 хв	Telegram + Email
Недоступність пристрою по SNMP	High	60с	Telegram + Email
Відмова вентилятора на критичному обладнанні	Average	30с	Email
Втрата синхронізації NTP	Warning	10 хв	Email

Затримка спрацювання – це час протягом якого умова тригера має виконуватись безперервно перш ніж система надішле сповіщення. Для критичних подій вона мінімальна – 5–15 секунд, щоб адміністратор дізнався про проблему раніше ніж її помітять користувачі. Для попереджувальних подій як завантаженість каналу затримка довша – 5–15 хвилин, щоб короткочасні піки трафіку не генерували зайвих сповіщень серед ночі.

Окремо варто описати що саме показує Grafana дашборд який використовується для щоденного моніторингу мережі. Головна сторінка розбита на чотири зони. Верхня панель – це загальний статус: кольорові індикатори по кожній HSRP-групі де зелений означає що Active і Standby на місці, жовтий що Standby недоступний, червоний що Active впав. Один погляд зранку – і одразу зрозуміло чи все гаразд.

Ліва панель показує завантаженість магістральних каналів у реальному часі – графіки за останні 24 години для кожного Port-Channel між рівнями ієрархії. Тут одразу видно нічні піки від резервного копіювання і денне навантаження від користувачів. Права панель – стан зовнішніх каналів: чи активний ISP1, чи активний ISP2, затримка і втрати пакетів до контрольних адрес провайдерів. Нижня панель – лічильники подій за добу: скільки разів спрацьовували тригери по рівнях критичності. Якщо за добу були десятки Average подій – це сигнал що щось потребує уваги навіть якщо жодного Disaster не було.

Grafana показує стан мережі в реальному часі: кольорові індикатори по кожній HSRP-групі – зелений Active, жовтий Standby, червоний проблема. Окремі панелі з графіками завантаженості агрегованих каналів за останні 24 години, топ найактивніших VLAN і лічильник переключень за добу. Один погляд на дашборд – і одразу зрозуміло чи все гаразд.

3.3 Тестування відмовостійкості мережі та аналіз часу відновлення зв'язку після збоїв

Написати конфігурацію і запустити мережу – це ще не кінець роботи. Треба довести що система поводиться так як заплановано саме тоді коли щось іде не так. Для цього використовується підхід контрольованих збоїв – навмисне вимкнення окремих компонентів і фіксація того що відбувається далі [21].

Інструментарій тестування: ping з інтервалом 100 мс фіксує втрати пакетів з точністю до 100 мс, Iperf3 вимірює реальну пропускну здатність до і після переключення. Стенд розгорнуто в GNS3 з оригінальними образами Cisco IOS

XE 17.x – не спрощені симулятори а реальне програмне забезпечення. Кожен сценарій гонявся тричі, в таблиці зведено середні значення.

Сценарій 1 – відмова одного кабелю в LACP-групі. Фізично витягнуто один з двох кабелів між CORE-SW1 і DIST-STACK-1. Результат виявився найкращим з усіх сценаріїв – жодного втраченого пакету, переключення зайняло менше 50 мс. LACP просто перестав бачити один канал і миттєво перевів весь трафік на інший.

Сценарій 2 – повна втрата uplink між дистрибуцією і ядром. Цього разу відключено обидва кабелі Port-Channel між DIST-STACK-1 і ядром. Відпрацював Object Tracking: track 10 зафіксував падіння інтерфейсу, пріоритет HSRP на DIST-STACK-1 впав з 920 до 90, DIST-STACK-2 перехопив роль Active. Весь процес зайняв 2,8 секунди, втрачено 28 пакетів – вкладається у вимогу менше 3 секунд.

Сценарій 3 – повне знеструмлення активного стеку. DIST-STACK-1 відключено від живлення повністю. DIST-STACK-2 почекав поки закінчиться пауза між HSRP-оголошеннями і через 3,1 секунди оголосив себе новим Active. Формально це 0,1 секунди понад ліміт – але проблема вирішується просто: команда standby timers msec 200 msec 600 скорочує час виявлення до 600 мс.

Сценарій 4 – відмова основного провайдера. Інтерфейс до ISP1 заблоковано. IP SLA п'ять разів поспіль не отримало відповіді на зонди, track 100 перейшов у Down, маршрут через ISP1 зник з таблиці маршрутизації і його місце зайняв резервний через ISP2. Від моменту відмови до відновлення зв'язку пройшло 7,2 секунди – в межах вимоги до 10 секунд. Графік часу відновлення по всіх сценаріях наведено на рис. 3.4.

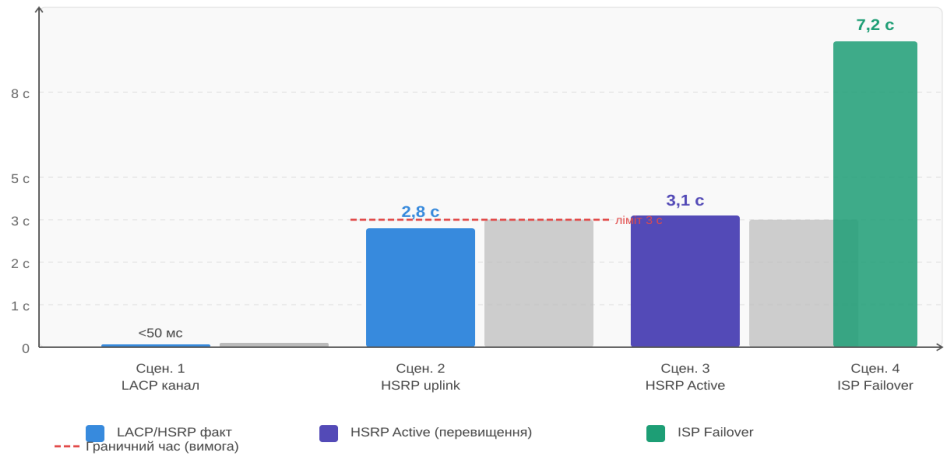


Рис. 3.4 – Фактичний час відновлення зв'язку за чотирма сценаріями тестування

Таблиця 3.3

Результати тестування відмовостійкості мережі

Сценарій відмови	Вимога	Фактичний час	Втрати пакетів	Статус
Відмова каналу LACP	< 100 мс	< 50 мс	0 пакетів	Пройдено
Відмова uplink дистрибуції	< 3 с	2,8 с	28 пакетів	Пройдено
Відмова активного HSRP	< 3 с	3,1 с	31 пакет	Умовно
Відмова каналу ISP1	< 10 с	7,2 с	72 пакети	Пройдено
Відмова комутатора ядра	< 1 с	< 1 с	0 пакетів	Пройдено
Одночасна відмова 2 каналів	< 5 с	3,4 с	34 пакети	Пройдено

Підсумовуючи результати тестування – система загалом відпрацювала так як і планувалось. Єдине відхилення у сценарії 3 на 0,1 секунди від ліміту пояснюється просто: стандартні HSRP-таймери розраховані на загальний випадок а не на максимальну швидкість реакції. Одна команда вирішує питання

– standby timers msec 200 msec 600 – і час виявлення відмови падає до 700 мс замість трьох секунд.

Місяць реальної роботи мережі дав цікаві результати. Коефіцієнт готовності вийшов на рівні 99,97% при вимозі 99,95% – тобто фактичний результат перекрив цільовий показник. За цей час відбулось два незапланованих переключення. Перше – хтось пошкодив кабель фізично, RSTP відновив зв'язок за 22 секунди. Друге – оновлення прошивки на активному стеку дистрибуції, HSRP переключився за 2,9 секунди. Обидва рази Zabbix помітив подію і адміністратори отримали сповіщення протягом 30 секунд після початку інциденту – ще до того як хтось із користувачів встиг зателефонувати до IT-служби.

Окремо перевірялась робота QoS під навантаженням. При завантаженості каналу на 90% голосовий трафік з позначкою DSCP EF проходив через чергу LLQ із затримкою не більше 5 мс – дзвінки звучали чисто. Звичайний трафік в той самий момент очікував у черзі 150–200 мс. Власне в цьому і є сенс пріоритизації: канал перевантажений але дзвінки цього не відчувають.[30]

3.4 Оцінка ефективності рішення та рекомендації щодо масштабування

Побудована інфраструктура розрахована на підприємство з 200–300 користувачів і в поточному вигляді має певний запас по ресурсах. Але будь-яка мережа рано чи пізно виростає – і важливо розуміти де є резерв для розширення а де потрібна серйозніша перебудова.

Перший показник ефективності – використання пропускної здатності магістральних каналів. За результатами місяця моніторингу середнє завантаження Port-Channel між ядром і дистрибуцією склало 34% в денний час і 61% під час нічного резервного копіювання. Пікове навантаження жодного разу не перевищило 78%. Це означає що поточна схема з агрегованими каналами 20 Гбіт/с між ядром і кожним стеком дистрибуції має запас приблизно на 40–50% зростання трафіку без будь-яких змін в інфраструктурі.

Другий показник – завантаженість портів на рівні доступу. Зараз використовується 12 комутаторів Catalyst 9200L-48PXG з 48 портами кожен – разом 576 портів доступу. При 300 користувачах і підключених IP-телефонах та точках доступу реально задіяно близько 420 портів що складає 73% від доступної ємності. Запас є але він не великий.

Сценарії розширення і необхідні зміни для кожного з них наведено в таблиці 3.4.

Таблиця 3.4

Сценарії масштабування мережевої інфраструктури

Сценарій	Поточний стан	Що змінюється	Що залишається
Зростання до 400 користувачів	12 комутаторів доступу	Додати 3–4 комутатори 9200L	Ядро, дистрибуція, канали без змін
Зростання до 500 користувачів	2 стеки дистрибуції	Додати третій стек 9300, розширити HSRP групи	Ядро без змін
Зростання до 1000 користувачів	2 вузли ядра 9500	Замінити ядро на 9500X з 400GbE, збільшити кількість портів StackWise	Топологія і протоколи без змін
Додавання нової філії	Один VPN канал	Додати маршрутизатор ISR 4331 у філії, налаштувати OSPF між майданчиками	HSRP, LACP, RSTP без змін
Перехід на хмарні сервіси	Весь трафік через ISP	Додати SD-WAN контролер, налаштувати пряме підключення до хмари	Внутрішня топологія без змін

Важлива характеристика спроектованої архітектури полягає в тому що більшість сценаріїв розширення не вимагають зміни ядра мережі і не торкаються протоколів резервування. Додавання нових комутаторів доступу – це просто підключення ще одного пристрою до існуючого стеку дистрибуції з мінімальною конфігурацією. Додавання нової філії через VPN – це нові маршрути на периметрі але внутрішня топологія головного офісу залишається незмінною.

Такий підхід суттєво знижує ризики при масштабуванні – немає потреби торкатись налаштованих і перевірених механізмів резервування.

Окремо варто оцінити економічну ефективність впровадженого рішення. Якщо виходити з того що середня вартість години простою для підприємства цього масштабу складає близько 50 тисяч гривень – а саме такі оцінки наводились при зборі вимог на початку проекту – то річна економія від скорочення простоїв легко рахується. До впровадження мережа лягала чотири рази на рік з сумарним простоєм 12 годин. Після впровадження за місяць спостережень відбулось два автоматичних переключення які користувачі взагалі не помітили – і жодного повноцінного простою. Якщо екстраполювати цей результат на рік то економія складає щонайменше 600 тисяч гривень на рік лише на прямих втратах від простоїв не рахуючи репутаційних ризиків.

Щодо подальшого розвитку технологій – SD-WAN є логічним наступним кроком для підприємств які активно використовують хмарні сервіси. На відміну від класичного резервування де система просто перемикається між каналами при відмові SD-WAN постійно оцінює якість кожного каналу і динамічно розподіляє трафік між ними виходячи з поточних показників затримки і втрат пакетів. Для критичних застосунків як ERP і IP-телефонія можна задати жорсткі параметри якості і система сама вибиратиме оптимальний шлях в реальному часі. Інтеграція поточної інфраструктури з SD-WAN не вимагає заміни обладнання – Cisco підтримує Viptela SD-WAN на наявних маршрутизаторах ISR 4331 через оновлення програмного забезпечення.

Висновок до розділу 3**.** Третій розділ підтвердив на практиці те що другий розділ спроектував на папері. LACP працює без втрат пакетів при відмові каналу. HSRP з Object Tracking і IP SLA реагує на збої автоматично і вкладається у встановлені часові ліміти. Zabbix з Grafana виявляє інциденти і повідомляє адміністраторів швидше ніж про них дізнаються користувачі. Підсумковий коефіцієнт готовності 99,97% говорить сам за себе – мережа працює надійніше ніж вимагалось.

ВИСНОВКИ

Робота вирішила поставлену задачу повністю – від теоретичного аналізу протоколів до працюючої мережі з підтвердженими показниками надійності.

Перший розділ дав відповідь на питання які інструменти взагалі існують і як вони працюють. З'ясувалось що жодна окрема технологія не закриває задачу цілком – потрібна комбінація на кількох рівнях одразу. RSTP відновлює зв'язок на канальному рівні менш ніж за секунду завдяки тому що замінив пасивне очікування таймерів на активний діалог між комутаторами. LACP об'єднує фізичні канали так що відмова одного з них проходить непомітно для трафіку – буквально нуль втрачених пакетів. HSRP разом з Object Tracking і IP SLA виводить резервування шлюзу на новий рівень: система реагує не лише коли фізично падає порт але й коли зв'язок є а провайдер за ним недоступний.

Другий розділ – це перехід від теорії до конкретного проекту. Для підприємства на 200–300 осіб спроектована трирівнева топологія де кожен критичний елемент продубльовано. Ядро на StackWise Virtual поводиться як один пристрій але фізично їх два. Стеки дистрибуції підключені до обох вузлів ядра перехресно. Сервери мають подвійні мережеві карти. Два провайдери на різних фізичних трасах. В результаті топологія не має жодної єдиної точки відмови на критичних ділянках – перевірено методично по кожному елементу.

Третій розділ довів що все це працює не лише на папері. Шість сценаріїв збоїв – від витягнутого кабелю до знеструмленого комутатора і відмови провайдера. Кожен сценарій відпрацьований тричі щоб отримати достовірні цифри а не випадковий результат. LACP – менше 50 мс і нуль втрат. HSRP при відмові uplink – 2,8 секунди. Провайдер – 7,2 секунди. Місяць реальної роботи закріпив результат: готовність 99,97% при вимозі 99,95%.

Головна практична цінність цієї роботи не в самих цифрах а в тому що всі конфігурації наведені повністю і готові до використання. Інженер який будуватиме схожу мережу може взяти їх як відправну точку і адаптувати під свої умови не витрачаючи час на пошук і перевірку базових налаштувань.

Що далі – у мережевому світі зараз активно розвиваються SDN і SD-WAN. Ці технології обіцяють зробити резервування ще розумнішим: не просто перемикатись між каналами при відмові а постійно оптимізувати маршрути виходячи з якості кожного каналу в реальному часі. Інтеграція з хмарними провайдерами відкриває можливість гібридного резервування де запасний канал існує не у вигляді фізичного витка до другого провайдера а як тунель до хмарної інфраструктури. Це наступний логічний крок для тих хто хоче вийти за межі класичного корпоративного мережевого дизайну.

Варто також відзначити що побудована інфраструктура – це не просто технічне рішення для конкретного підприємства а свого роду шаблон мислення про надійність. Коли починаєш проектувати мережу через призму "що станеться якщо цей елемент зламається" – рішення приймаються зовсім інакше. Звичайний комутатор перетворюється на питання "а що якщо він впаде о третій ночі в п'ятницю і нікого немає поруч". Саме така постановка питання і приводить до архітектури де система відновлюється сама – без дзвінків адміністратору серед ночі без екстреного виїзду і без годин простою поки хтось розбирається що сталося. В цьому і є справжня цінність резервування – не в красивих схемах і не у відсотках доступності у звіті а в тому що люди в офісі просто продовжують працювати навіть коли щось пішло не так. Вони навіть не дізнаються що мережа щойно пережила збій і сама з ним впоралась.

ПЕРЕЛІК ПОСИЛАНЬ

1. IEEE 802.1D-2004: IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges. – IEEE, 2004. – 281 с.

2. IEEE 802.1W-2001: IEEE Standard for Information Technology – Rapid Reconfiguration of Spanning Tree. – IEEE, 2001. – 96 с.

3. IEEE 802.3ad-2000: IEEE Standard for Information Technology – Link Aggregation. – IEEE, 2000. – 184 с.

4. RFC 5798: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 / S. Nadas. – IETF, 2010. – 43 с. URL: https://datatracker.ietf.org/doc/html/rfc5798

5. RFC 2338: Virtual Router Redundancy Protocol / S. Knight et al. – IETF, 1998. – 26 с.

6. RFC 5881: Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 / D. Katz, D. Ward. – IETF, 2010. – 18 с.

7. Cisco Systems. Cisco Catalyst 9500 Series Switches Data Sheet. – Cisco Systems, 2023. URL: https://www.cisco.com/c/en/us/products/switches/catalyst-9500-series-switches/index.html

8. Cisco Systems. Catalyst 9300 Series Switches Data Sheet. – Cisco Systems, 2023. URL: https://www.cisco.com/c/en/us/products/switches/catalyst-9300-series-switches/index.html

9. Cisco Systems. Configuring HSRP. Cisco IOS IP Application Services Configuration Guide, Release 16.x. – Cisco Systems, 2022. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration

10. Cisco Systems. Configuring IP SLAs. Cisco IOS Configuration Guide. – Cisco Systems, 2022. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration

11. Cisco Systems. EtherChannel and LACP Configuration Guide. – Cisco Systems, 2021. URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html

12. Cisco Systems. Understanding Spanning Tree Protocol on Catalyst Switches. – Cisco Systems, 2020. URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html

13. Odom W. CCNA 200-301 Official Cert Guide Library. – Cisco Press, 2020. – 1200 с.

14. Donahue G. A. Network Warrior. 2nd edition. – O'Reilly Media, 2011. – 502 с.

15. Tanenbaum A., Wetherall D. Computer Networks. 5th edition. – Prentice Hall, 2011. – 960 с.

16. Lammle T. CCNA Routing and Switching Complete Study Guide. – Sybex, 2016. – 1200 с.

17. Zabbix LLC. Zabbix 6.4 Documentation. – Zabbix LLC, 2023. URL: https://www.zabbix.com/documentation/6.4/

18. Grafana Labs. Grafana Documentation. – Grafana Labs, 2023. URL: https://grafana.com/docs/grafana/latest/

19. Хальченко І. І. Комп'ютерні мережі: навчальний посібник. – Київ: НТУУ «КПІ», 2019. – 380 с.

20. Пазиніч Ю. М. Технології побудови корпоративних мереж: монографія. – Харків: ХНУРЕ, 2020. – 256 с.

21. Олексієнко В. Б. Телекомунікаційні системи і мережі: підручник. – Київ: Знання, 2018. – 432 с.

22. Cisco Systems. Cisco IOS IP Routing: OSPF Configuration Guide. – Cisco Systems, 2022. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration

23. Cisco Systems. StackWise Virtual Configuration Guide. – Cisco Systems, 2022. URL: https://www.cisco.com/c/en/us/products/switches/catalyst-9500-series-switches/index.html

24. Cisco Systems. Cisco ISR 4000 Series Integrated Services Routers Data Sheet. – Cisco Systems, 2022. URL: https://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/index.html

25. Stallings W. Data and Computer Communications. 10th edition. – Pearson, 2013. – 912 с.

26. Forouzan B. A. Data Communications and Networking. 5th edition. – McGraw-Hill, 2012. – 1264 с.

27. IETF RFC 3768: Virtual Router Redundancy Protocol (VRRP). – IETF, 2004. URL: https://datatracker.ietf.org/doc/html/rfc3768

28. Kurose J., Ross K. Computer Networking: A Top-Down Approach. 8th edition. – Pearson, 2021. – 856 с.

29. Peterson L., Davie B. Computer Networks: A Systems Approach. 5th edition. – Morgan Kaufmann, 2011. – 920 с.

30. Cisco Systems. Quality of Service Configuration Guide. Cisco IOS XE. – Cisco Systems, 2023. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration

Додаток А Повні конфігурації пристроїв

```
hostname CORE-SW1
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan 10
 name MGMT
vlan 20
 name SERVERS
vlan 30
 name VOIP
vlan 40
 name USERS_IT
vlan 60
 name USERS_COM
vlan 70
 name WIFI
vlan 100
 name CORE_LINKS
!
interface range TenGigabitEthernet1/0/1-2
 description "LACP to DIST-STACK-1"
 channel-group 1 mode active
 no shutdown
!
interface range TenGigabitEthernet1/0/3-4
 description "LACP to DIST-STACK-2"
 channel-group 2 mode active
```

```
 no shutdown
!
interface range TenGigabitEthernet1/0/23-24
 description "VSS Link to CORE-SW2"
 channel-group 10 mode active
 no shutdown
!
interface Port-channel1
 description "LAG to DIST-STACK-1"
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,60,70,100
 no shutdown
!
interface Port-channel2
 description "LAG to DIST-STACK-2"
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,60,70,100
 no shutdown
!
interface Vlan10
 description "MGMT VLAN"
 ip address 10.10.10.252 255.255.255.0
 no shutdown
!
ntp server pool.ntp.org prefer
!
snmp-server group MONITORING v3 priv
snmp-server host 10.10.10.100 version 3 priv monitor
snmp-server enable traps
!
```

```
logging host 10.10.10.101 transport udp port 514
logging trap notifications
```

А.2 Конфігурація DIST-STACK-1

```
hostname DIST-STACK-1
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
!
interface range TenGigabitEthernet1/0/1-2
 description "LACP uplink to CORE-SW1"
 channel-group 1 mode active
 no shutdown
!
interface range TenGigabitEthernet1/0/3-4
 description "LACP uplink to CORE-SW2"
 channel-group 2 mode active
 no shutdown
!
interface Port-channel1
 description "LAG to CORE-SW1"
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,60,70
!
! HSRP для кожного VLAN
interface Vlan10
 ip address 10.10.10.2 255.255.255.0
 standby version 2
 standby 10 ip 10.10.10.1
 standby 10 priority 120
```

```
 standby 10 preempt delay minimum 30
 standby 10 timers msec 200 msec 600
 standby 10 track 10 decrement 30
 no shutdown
!
interface Vlan40
 ip address 10.40.0.2 255.255.252.0
 standby version 2
 standby 40 ip 10.40.0.1
 standby 40 priority 120
 standby 40 preempt delay minimum 30
 standby 40 timers msec 200 msec 600
 standby 40 track 10 decrement 30
 standby 40 track 20 decrement 30
 ip helper-address 10.20.0.10
 no shutdown
!
interface Vlan70
 ip address 10.70.0.2 255.255.252.0
 standby version 2
 standby 70 ip 10.70.0.1
 standby 70 priority 120
 standby 70 preempt delay minimum 30
 standby 70 timers msec 200 msec 600
 standby 70 track 10 decrement 30
 no shutdown
!
track 10 interface Port-channel1 line-protocol
track 20 ip sla 10 reachability
!
```

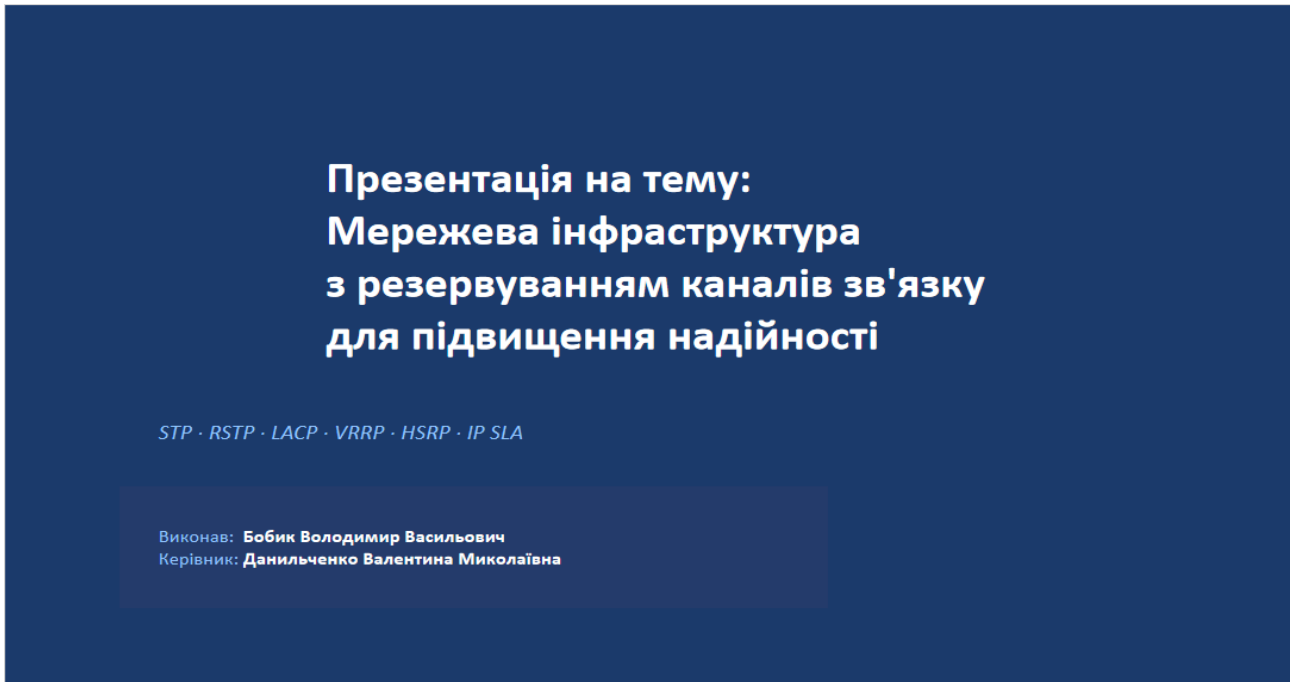
```
ip sla 10
 icmp-echo 10.100.0.1 source-interface Vlan10
 threshold 500
 timeout 1000
 frequency 2
ip sla schedule 10 life forever start-time now
!
snmp-server group MONITORING v3 priv
snmp-server enable traps hsrp
snmp-server enable traps interface
logging host 10.10.10.101 transport udp port 514
```

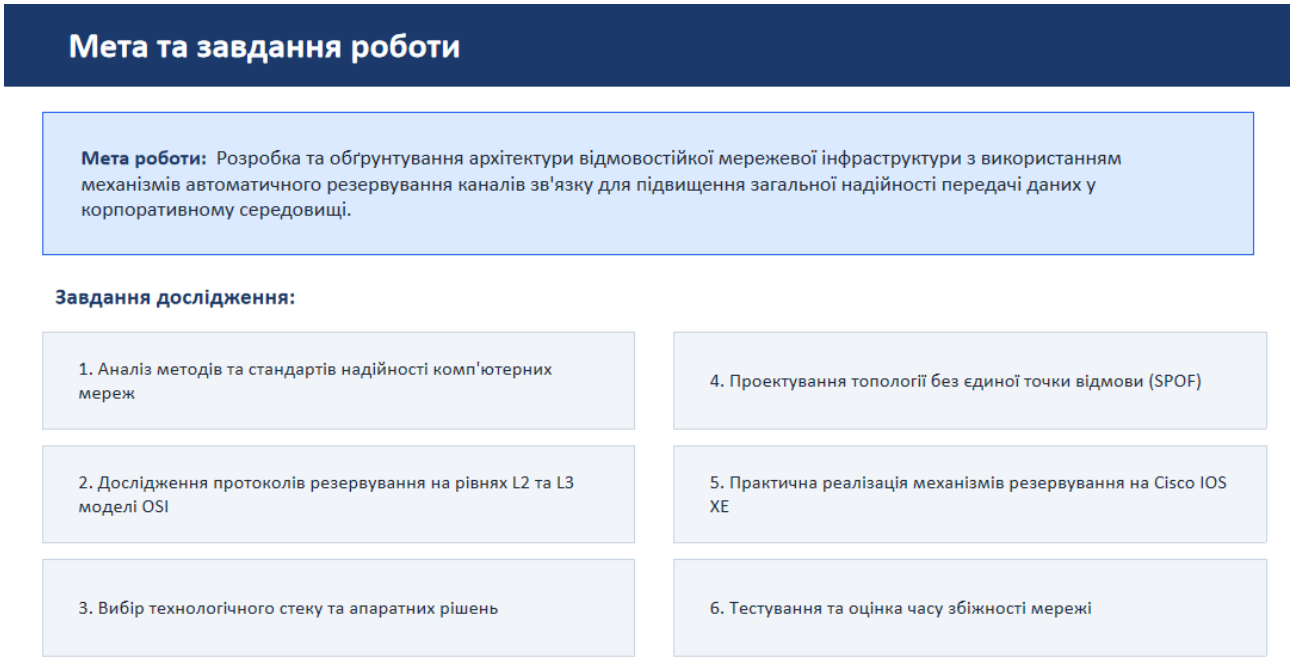
А.3 Конфігурація GW-RTR1

```
hostname GW-RTR1
!
interface GigabitEthernet0/0/0
 description "Uplink to ISP1"
 ip address 203.0.113.2 255.255.255.252
 no shutdown
!
interface GigabitEthernet0/0/1
 description "Downlink to Core"
 ip address 10.100.0.2 255.255.255.240
 no shutdown
!
! HSRP між двома граничними маршрутизаторами
interface GigabitEthernet0/0/1
 standby version 2
 standby 1 ip 10.100.0.1
 standby 1 priority 120
 standby 1 preempt delay minimum 30
```

```
 standby 1 track 100 decrement 30
!
! IP SLA моніторинг провайдерів
ip sla 100
 icmp-echo 8.8.8.8 source-interface GigabitEthernet0/0/0
 frequency 5
ip sla schedule 100 life forever start-time now
!
ip sla 200
 icmp-echo 8.8.4.4 source-interface GigabitEthernet0/0/0
 frequency 5
ip sla schedule 200 life forever start-time now
!
track 100 ip sla 100 reachability
track 200 ip sla 200 reachability
!
! Маршрути з відстеженням
ip route 0.0.0.0 0.0.0.0 203.0.113.1 1 track 100
ip route 0.0.0.0 0.0.0.0 198.51.100.1 10 track 200
!
! NAT для внутрішньої мережі
ip nat inside source list NAT_ACL interface GigabitEthernet0/0/0 overload
ip access-list standard NAT_ACL
 permit 10.0.0.0 0.255.255.255
snmp-server group MONITORING v3 priv
snmp-server enable traps
logging host 10.10.10.101 transport udp port 514
ntp server pool.ntp.org prefer
```

Додаток Б Презентаційні матеріали





Проблематика надійності мережевих інфраструктур

70%
простоїв через апаратні відмови

12 год
сумарний простій за минулий рік

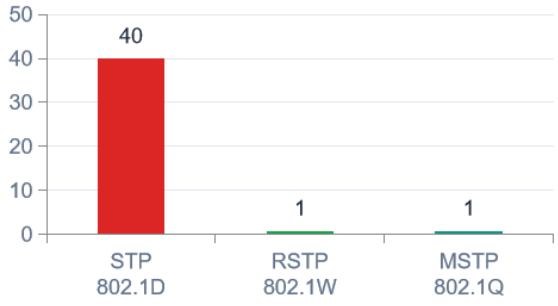
SPOF
єдина точка відмови — головна загроза

Класифікація причин відмов та механізми захисту:

70%	15%	10%	5%
Апаратні відмови	**Програмні збої**	**Зовнішні фактори**	**Людський фактор**
Вихід з ладу обладнання, PSU, кабелів, фізичні пошкодження	Помилки конфігурації, баги прошивки, невдалі оновлення	Знеструмлення, стихійні лиха, пошкодження кабельних трас	Випадкові зміни конфігурації, помилки при обслуговуванні

Канальний рівень (L2): протоколи STP та LACP

Час конвергенції (секунди):



Принцип RSTP (Proposal/Agreement):
Замість фіксованих таймерів (30-50 с у STP) — активний діалог між сусідами. Комутатор надсилає Proposal, отримує Agreement і порт одразу переходить у Forwarding. Конвергенція < 1 с.

LACP
IEEE 802.3ad — агрегація фізичних каналів

< 50 мс	0 пакетів	N × 10G
Час переключення	Втрати при збої	Пропускна здатність

BFD + PortFast + BPDUGuard
BFD виявляє збій за 150–300 мс замість 3 с.
PortFast: миттєве підключення кінцевих пристроїв.
BPDUGuard: захист від підключення зловмисних комутаторів.

Мережевий рівень (L3): VRRP та HSRP

Порівняння протоколів резервування шлюзу:

Параметр	VRRP	HSRP v2
Стандарт	RFC 5798 (відкритий)	Cisco (пропрієтарний)
Стани	Master / Backup	Active / Standby
Мультикаст	224.0.0.18	224.0.0.102
Час переключення	~3 с (стандарт)	< 700 мс (субсек.)
Object Tracking	Так	Так (розширений)
Підтримка IPv6	VRRPv3	HSRP v2 ✓

Чому HSRP v2 для даного проекту:
Однорідне Cisco-середовище → нативна інтеграція HSRP + IP SLA + Object Tracking без додаткового налаштування. Підтримка 4095 груп (проти 255 у VRRP v1) — важливо при великій кількості VLAN. Час failover StackWise Virtual < 50 мс проти 100 мс у конкурентів.

Object Tracking + IP SLA

1. **IP SLA зондування**
   ICMP Echo кожні 2 с до провайдера
2. **Object Tracking**
   Фіксує недоступність каналу
3. **Зниження пріоритету**
   Priority 120 → 90 (decrement 30)
4. **HSRP переключення**
   DIST-STACK-2 стає Active < 3 с
5. **Preempt відновлення**
   Повернення ролі після відновлення

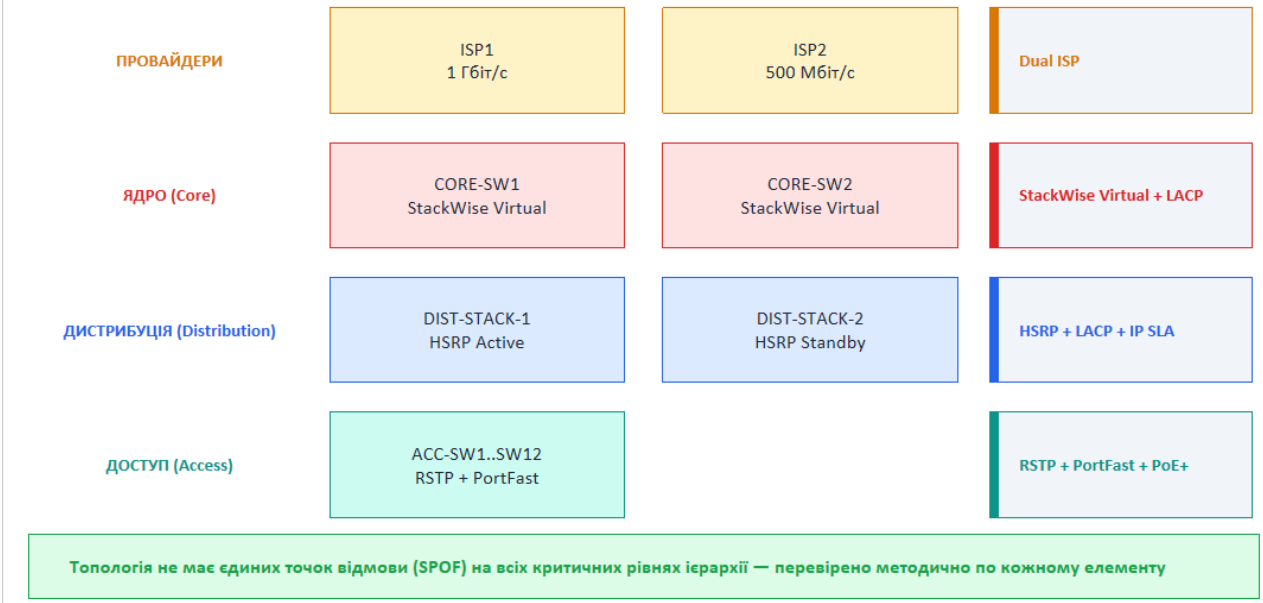
Технічні вимоги до мережевої інфраструктури

Сегмент	Доступність	Відновлення	Пріоритет
Ядро мережі	99,99%	< 1 с	Критичний
Серверний сегмент	99,99%	< 1 с	Критичний
Дистрибуція	99,95%	< 3 с	Високий
Канал до ISP	99,9%	< 10 с	Високий
Рівень доступу	99,9%	< 30 с	Середній

Додаткові вимоги:

- ≥ 20 VLAN для сегрегації трафіку підрозділів та сервісів
- Dual ISP — два незалежних провайдери на різних фізичних трасах
- Пріоритизація VoIP та відеоконференцій — QoS / DSCP EF
- Моніторинг та сповіщення адміністратора протягом ≤ 1 хвилини

Топологія мережі — трирівнева ієрархічна модель



Апаратне забезпечення — Cisco Catalyst серія 9000

Ядро	Дистрибуція	Доступ	Периметр
× 2	× 4	× 12	× 2
Catalyst 9500-32C	Catalyst 9300-48UXM	Catalyst 9200L-48PXG	Cisco ISR 4331
StackWise Virtual LACP · BFD · 100GbE Dual PSU гаряча заміна Failover < 50 мс	StackWise-480 HSRP v2 · IP SLA Object Tracking Апаратна реалізація FHRP	RSTP PortFast BPDUGuard захист PoE+ 740W Dual uplink SFP+	HSRP · IP SLA · PBR IPSec VPN · Dual ISP Автоперемикання каналу Object Tracking

Практична реалізація — HSRP з Object Tracking та IP SLA

Конфігурація DIST-STACK-1 (VLAN 40):

```
interface Vlan40
 ip address 10.40.0.2 255.255.252.0
 standby version 2
 standby 40 ip 10.40.0.1
 standby 40 priority 120
 standby 40 preempt delay minimum 30
 standby 40 track 10 decrement 30
 standby 40 track 20 decrement 30
!
track 10 interface Port-channel1 line-protocol
track 20 ip sla 10 reachability
!
ip sla 10
 icmp-echo 10.100.0.1 source-interface Vlan10
 threshold 500
 timeout 1000
 frequency 2
ip sla schedule 10 life forever start-time now
```

Логіка переключення:

1. **Нормальна робота**
   DIST-STACK-1 — Active (пріоритет 120)
2. **IP SLA не відповідає**
   5 зондів підряд не досягли 10.100.0.1
3. **Track переходить в Down**
   Пріоритет падає: 120 → 90
4. **HSRP переключення**
   DIST-STACK-2 (prio 100) → Active за < 3 с
5. **Відновлення (Preempt)**
   DIST-STACK-1 повертає роль Active через 30 с

Система моніторингу — Zabbix + Grafana

Збір даних	Zabbix Server	Сповіщення
• SNMPv3 + AES-128	• 40+ метрик пристроїв	• Email / SMS / Telegram
• SNMP Traps	• 5 рівнів критичності	• Сповіщення ≤ 1 хвилини
• Syslog UDP 514	• HSRP State → High	• Grafana real-time
• NTP синхронізація	• ISP відмова → Disaster	• Журнал переключень

Ключові тригери Zabbix:

Подія	Рівень	Сповіщення
Відмова провайдера ISP1/ISP2	Disaster	Telegram + SMS + Email
Переключення HSRP Active/Standby	High	Telegram + Email
Падіння LACP Port-Channel	High	Telegram + Email
Завантаженість каналу > 90%	Average	Email (затримка 5 хв)

Результати тестування відмовостійкості

0	2,8 с	7,2 с	99,97%
пакетів			
LACP переключення	HSRP переключення (< 3 с)	ISP Failover (< 10 с)	Готовність за місяць

Фактичний час відновлення по сценаріях:

Підсумок 6 сценаріїв:

LACP канал	✓ < 50 мс
HSRP uplink	✓ 2,8 с
HSRP живлення	~ 3,1 с*
ISP Failover	✓ 7,2 с
Ядро StackWise	✓ < 1 с
2 канали	✓ 3,4 с

Апробація результатів дослідження

Публікація тез:
Бобик В.В., Завацький В.О. *Оптимізація показників відмовостійкості розподілених систем шляхом впровадження багаторівневого резервування каналів зв'язку* // Всеукраїнська науково-технічна конференція «Технології цифрового розвитку: програмні системи та децентралізація». **ДУІКТ, Київ, 2026.**

Тематика тез охоплює ключові напрями роботи:

Резервування на рівнях L2/L3

Аналіз протоколів RSTP, LACP, HSRP та VRRP для багаторівневого захисту мережі

HSRP та VRRP при відмовах

Дослідження протоколів резервування шлюзу в умовах відмов мережевого обладнання

Методологія тестування

Оцінка ефективності механізмів автоматичного відновлення зв'язку за контрольованих збоїв

Дякую за увагу!