НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету Інформаційних технологій	**Завідувач кафедри** Комп'ютерних систем, мереж та кібербезпеки
_____Ігор БОЛБОТ (підпис)	_____Дмитро КАСАТКІН (підпис)
«___»_____2026 р.	«___»_____2026 р.

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

На тему: «Розробка комп'ютерної мережі з функцією балансування трафіку »

Спеціальність F7 «Комп'ютерна інженерія »

Освітньо-професійна програма «Комп'ютерна інженерія »

Гарант освітньої програми
канд. фіз.-мат. наук, доцент _____ (підпис) **Євгеній НІКІТЕНКО**

Керівник бакалаврської кваліфікаційної роботи
канд. пед. наук, доцент _____ (підпис) **Дмитро КАСАТКІН**

Виконав _____ (підпис) **Віталій СИДОРЕНКО**

КИЇВ-2026

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
канд. пед. наук, доцент_____Дмитро КАСАТКІН
«_____»_____20____ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ БАКАЛАВРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
ЗДОБУВАЧУ

Сидоренку Віталію Ігоровичу
(прізвище, ім'я, по батькові)

Спеціальність «Комп'ютерна інженерія »

Освітньо-професійна програма «Комп'ютерна інженерія »

Тема кваліфікаційної бакалаврської роботи
«Розробка комп'ютерної мережі з функцією балансування трафіку
»

затверджена наказом ректора НУБіП України від «26» 02 2026 р. № 157 «З»
Термін подання завершеної роботи на кафедру «22» 05 2026 р.
Вихідні дані до бакалаврської кваліфікаційної роботи

Перелік питань, що підлягають дослідженню:
1. Проєктування логічної та фізичної топології мережі агропромислового підприємства
2. Імітаційне моделювання аварійних ситуацій

Перелік графічного матеріалу (за необхідності).

Дата видачі завдання "27" 12 2026р.

Керівник бакалаврської кваліфікаційної роботи _____ **Дмитро КАСАТКІН**
канд. пед. наук, доцент (підпис)

Завдання взяв до виконання _____ **Віталій СИДОРЕНКО**
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз вимог до периметру комп’ютерної мережі	10.03.2026 р.	Виконано
2	Проектування периметру комп’ютерної мережі	15.03.2026	Виконано
3	Моделювання периметру комп’ютерної мережі	20.04.2026	Виконано
4	Тестування розробленої периметру комп’ютерної мережі	07.05.2026	Виконано
5	Оформлення пояснювальної записки	24.05.2026	Виконано

Студент_____ / Віталій СИДОРЕНКО /
(підпис) (ініціали та прізвище)

Керівник проекту (роботи)_____ / Дмитро КАСАТКІН/
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка: 70 сторінок, 25 рисунків, 4 таблиці, 6 додатків, 15 джерел.

У цій роботі проведено комплексне дослідження та розробку відмовостійкої комп'ютерної мережі з функцією динамічного балансування трафіку для регіонального управління агропромислового підприємства. Основний акцент зроблено на забезпеченні безперервності критичних бізнес-процесів (IP-телефонія, відеоспостереження, доступ до централізованих баз даних) та усуненні «вузьких місць» в інфраструктурі завдяки переходу від пасивного резервування до високоефективної моделі Active/Active.

Перший розділ роботи закладає аналітичний фундамент побудови корпоративних мереж рівня Enterprise. У ньому проаналізовано проблематику перевантаження каналів зв'язку та детально розглянуто існуючі технології агрегації і резервування шлюзів. Обґрунтовано доцільність використання протоколу Multigroup HSRP (MHSRP) як дієвої альтернативи GLBP для розпаралелювання навантаження на мережевому рівні L3.

У другому розділі теоретичні концепції трансформовано у конкретне проєктне рішення. Було підібрано апаратну базу на основі обладнання Cisco Systems (маршрутизатори ISR 4331, комутатори Catalyst 3650 та 2960), розроблено логічну топологію із сегментацією на 6 віртуальних локальних мереж (VLAN) та створено оптимізовану схему IP-адресації. Також проведено розрахунок необхідної пропускної здатності та визначено суворі політики якості обслуговування (QoS) для захисту мультимедійного трафіку.

Практична частина, викладена у третьому розділі, демонструє безпосереднє втілення розробленої моделі в симуляційному середовищі Cisco Packet Tracer. У процесі роботи було успішно налаштовано апаратну агрегацію каналів (EtherChannel), резервування шлюзів (MHSRP) та впроваджено багаторівневий механізм безпеки: захист портів (Port Security), списки контролю доступу (ACL) та шифрування сесій (SSH). Завершальним етапом стало

імітаційне моделювання аварійних ситуацій (краш-тести), яке підтвердило здатність мережі миттєво відновлювати зв'язність без втрати пакетів.

У четвертому розділі проведено техніко-економічне обґрунтування розробленого проєкту. Розрахунки капітальних (CAPEX) та операційних (OPEX) витрат підтвердили високу економічну ефективність впровадженої системи. Створена інфраструктура повністю окупає інвестиції, запобігаючи фінансовим збиткам від потенційного простою виробництва та логістики підприємства.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

ACL (Access Control List) — список контролю доступу
ASIC (Application-Specific Integrated Circuit) — спеціалізована інтегральна мікросхема
AVF (Active Virtual Forwarder) — активний віртуальний пересилач
AVG (Active Virtual Gateway) — активний віртуальний шлюз
CAPEX (Capital Expenditure) — капітальні витрати
DHCP (Dynamic Host Configuration Protocol) — протокол динамічного налаштування вузла
DSCP (Differentiated Services Code Point) — код диференційованих послуг
ECMP (Equal-Cost Multi-Path) — багатошляхова маршрутизація з рівною вартістю
ERP (Enterprise Resource Planning) — система планування ресурсів підприємства
FHRP (First Hop Redundancy Protocol) — протокол резервування першого стрибка
GLBP (Gateway Load Balancing Protocol) — протокол балансування навантаження шлюзу
HSRP (Hot Standby Router Protocol) — протокол гарячого резервування маршрутизаторів
HTTP (HyperText Transfer Protocol) — протокол передачі гіпертексту
ICMP (Internet Control Message Protocol) — протокол міжмережевих керуючих повідомлень
IoT (Internet of Things) — Інтернет речей
IP (Internet Protocol) — міжмережевий протокол
L2/L3 (Layer 2 / Layer 3) — рівні моделі OSI (канальний та мережевий)
LACP (Link Aggregation Control Protocol) — протокол управління агрегацією каналів
LAN (Local Area Network) — локальна комп'ютерна мережа (ЛВС)
MAC (Media Access Control) — управління доступом до середовища
MHSRP (Multigroup Hot Standby Router Protocol) — багатогрупний протокол гарячого резервування маршрутизаторів
MQC (Modular QoS CLI) — модульний інтерфейс командного рядка QoS
OPEX (Operational Expenditure) — операційні витрати
OSI (Open Systems Interconnection) — еталонна модель взаємодії відкритих систем
PAgP (Port Aggregation Protocol) — протокол агрегації портів
PoE (Power over Ethernet) — технологія передачі живлення через кабель Ethernet
QoS (Quality of Service) — якість обслуговування

RSA (Rivest-Shamir-Adleman) — криптографічний алгоритм з відкритим ключем
SSH (Secure Shell) — безпечний протокол віддаленого управління
STP (Spanning Tree Protocol) — протокол остовного дерева
TCP (Transmission Control Protocol) — протокол управління передачею
UDP (User Datagram Protocol) — протокол користувацьких датаграм
VLAN (Virtual Local Area Network) — віртуальна локальна мережа
VRRP (Virtual Router Redundancy Protocol) — протокол резервування віртуального маршрутизатора
WAN (Wide Area Network) — глобальна комп'ютерна мережа

ВСТУП

Для стабільної роботи баз даних, IP-телефонії, відеоспостереження та IoT-пристроїв підприємству необхідна надійна комп’ютерна мережа, яка забезпечує безперебійну передачу даних навіть при високому навантаженні. Актуальність теми дослідження зумовлена необхідністю мінімізації часу простою мережі у разі відмови обладнання. Традиційні архітектури мереж, що базуються на статичній маршрутизації, не здатні забезпечити динамічне відновлення зв'язку, тому впровадження протоколів надмірності шлюзів є обов’язковим для побудови корпоративних систем рівня Enterprise.

У дипломній роботі розроблено архітектуру комп'ютерної мережі агропромислового підприємства з використанням сучасних методів балансування трафіку та забезпечення відмовостійкості. В якості ключових технологій для підвищення доступності мережі було обрано протоколи агрегації каналів та резервування шлюзів.

Для забезпечення надійності функціонування мережі на мережевому рівні (L3) було реалізовано протокол MHSRP (Multi-Group HSRP). Вибір даного протоколу як інженерної альтернативи протоколу GLBP, згаданого у початковій концепції, обумовлений необхідністю забезпечення стабільної роботи кластера на обраному обладнанні (Cisco ISR 4331/Catalyst 3650) та потребою у більш гнучкому налаштуванні пріоритетності трафіку між різними сегментами VLAN. Така технічна адаптація дозволила реалізувати ефективну схему балансування навантаження в режимі Active/Active шляхом розподілу груп шлюзів, що повністю відповідає поставленим вимогам до продуктивності та надійності інформаційної системи підприємства.

Метою роботи є проєктування та практична реалізація відмовостійкої комп'ютерної мережі, здатної забезпечити високу якість обслуговування (QoS) критично важливого трафіку.

Для досягнення поставленої мети було вирішено такі завдання:

− Проаналізовано існуючі методи балансування трафіку та протоколи резервування шлюзів.

− Обґрунтовано вибір мережевого обладнання Cisco для побудови ядра мережі.

− Розроблено топологію мережі та налаштовано логічне розділення трафіку за допомогою VLAN.

− Реалізовано механізми EtherChannel та MHSRP для забезпечення відмовостійкості та балансування навантаження.

− Забезпечено захист мережі шляхом впровадження технологій Port Security та SSH.

− Проведено імітаційне моделювання аварійних ситуацій у середовищі Cisco Packet Tracer, що підтвердило життєздатність запропонованого технічного рішення.

Об'єктом дослідження є процес передачі даних у корпоративних комп'ютерних мережах. Предметом дослідження є методи та алгоритми забезпечення відмовостійкості та балансування трафіку в мережах агропромислових підприємств.

РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ БАЛАНСУВАННЯ ТРАФІКУ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Основні принципи побудови сучасних комп'ютерних мереж

Корпоративна комп’ютерна мережа є важливою складовою інформаційної інфраструктури сучасного підприємства. В умовах розвитку агропромислового комплексу вимоги до корпоративних мереж постійно зростають і вже не обмежуються лише доступом до мережі Інтернет. Сучасна мережа підприємства об’єднує офіси, сервери, виробничі об’єкти, склади та інші вузли в єдину систему для забезпечення стабільного обміну даними між усіма підрозділами підприємства.

До складу такої мережі можуть входити локальні обчислювальні мережі головного офісу, віддалених філій, логістичних складів, елеваторів, виробничих приміщень і центрів обробки даних. Це дозволяє організувати єдиний інформаційний простір для роботи підприємства.

Під час проєктування мережевої інфраструктури необхідно враховувати основні вимоги до її роботи:

Відмовостійкість (High Availability) — здатність мережі продовжувати роботу навіть у разі відмови окремих комутаторів, маршрутизаторів або каналів зв’язку. Для цього використовують резервування обладнання та протоколи балансування навантаження.

Масштабованість (Scalability) — можливість розширення мережі без суттєвої зміни вже існуючої інфраструктури. Це особливо важливо при збільшенні кількості користувачів або підключенні нових пристроїв.

Керованість (Manageability) — можливість централізованого контролю мережевого обладнання, моніторингу трафіку та швидкого виявлення несправностей за допомогою протоколів SNMP, Syslog і NetFlow.

Якість обслуговування (QoS) — підтримка пріоритезації критично важливого трафіку, такого як IP-телефонія, відеоконференції або телеметричні дані реального часу.

Безпека (Security) — захист мережі від несанкціонованого доступу за рахунок сегментації VLAN, використання списків контролю доступу (ACL) та механізмів автентифікації.

Для забезпечення цих вимог у сучасних мережах не використовують плоску топологію. Найчастіше застосовується трирівнева ієрархічна модель мережі, запропонована компанією Cisco Systems. Вона передбачає поділ мережі на окремі логічні рівні, кожен із яких виконує власні функції та спрощує адміністрування мережевої інфраструктури.

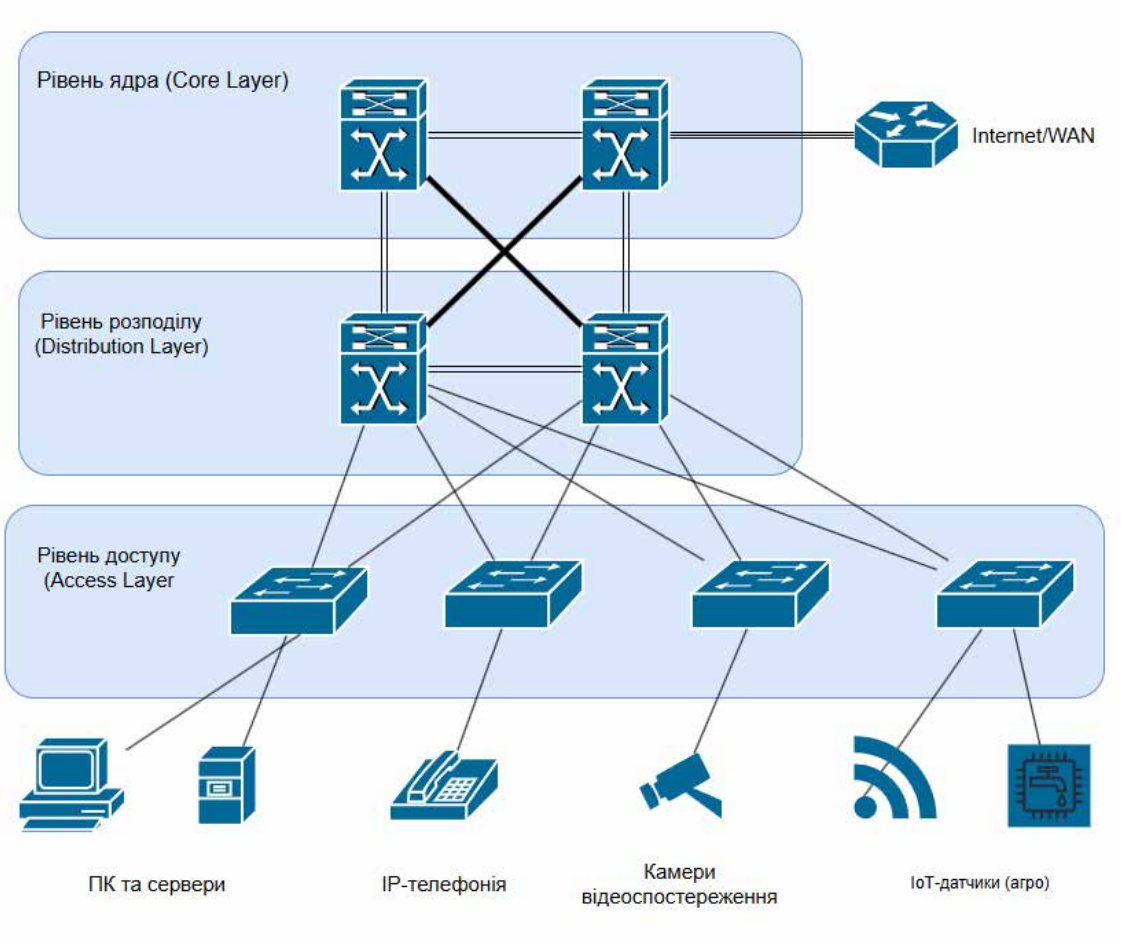

Рис. 1.1 – Схема ієрархічної моделі Cisco з рівнями Core, Distribution, Access

1. Рівень доступу (Access Layer) Рівень доступу формує межу мережі (Network Edge), де кінцеві пристрої отримують фізичний або бездротовий доступ до корпоративної інфраструктури. На підприємстві до цього рівня підключаються робочі станції персоналу, IP-телефони, точки доступу Wi-Fi, камери відеоспостереження, а також промислові контролери та IoT-сенсори систем точного землеробства. Основним обладнанням цього рівня є комутатори другого рівня (L2) моделі OSI (наприклад, серії Cisco Catalyst 2960 або 9200). До ключових функцій рівня доступу належать:

Підключення клієнтських вузлів та забезпечення їх живленням через кабель Ethernet (технологія PoE — Power over Ethernet) для IP-камер та телефонів. Логічна сегментація пристроїв за допомогою віртуальних

локальних мереж (VLAN) для ізоляції широкомовних доменів (Broadcast domains).

Захист на рівні портів (Port Security), інспекція ARP-пакетів та запобігання підміні IP-адрес (DHCP Snooping). Маркування вхідного трафіку тегами якості обслуговування (QoS) поблизу джерела його виникнення.

2. Рівень розподілу (Distribution Layer) Рівень розподілу виконує роль сполучної ланки, яка агрегує з'єднання від десятків або сотень комутаторів рівня доступу перед тим, як передати трафік до ядра мережі. Цей рівень є межею між доменами комутації (L2) та доменами маршрутизації (L3). Тут застосовуються високопродуктивні багатоканальні комутатори третього рівня (наприклад, серії Cisco Catalyst 3850 або 9300) та маршрутизатори. Головні завдання рівня розподілу − це забезпечення маршрутизації між віртуальними мережами (Inter-VLAN routing). Реалізація політик мережевої безпеки за допомогою списків контролю доступу (ACL), що дозволяють або забороняють обмін даними між різними відділами підприємства. Агрегація фізичних каналів зв'язку (EtherChannel) для збільшення пропускної здатності в напрямку ядра.

Забезпечення відмовостійкості шлюзів за замовчуванням. Саме на цьому рівні розгортаються протоколи резервування першого стрибка (FHRP), такі як HSRP, VRRP або GLBP. Впровадження GLBP дозволяє не лише забезпечити резервування, а й здійснювати балансування трафіку від кінцевих хостів в активному режимі.

3. Рівень ядра (Core Layer) Рівень ядра (магістраль) є критично важливим центром мережі підприємства. Його єдине і головне завдання — максимально швидка, надійна та безперебійна комутація пакетів між модулями рівня розподілу (головним офісом, дата-центром та віддаленими філіями). Щоб уникнути затримок при обробці трафіку, на рівні ядра мінімізують використання ресурсомістких операцій, таких як складні списки контролю доступу (ACL) або маніпуляції з QoS. Устаткування ядра повинно мати максимальну апаратну надійність (резервні блоки живлення, модулі управління) та найвищу пропускну здатність. Топологія рівня ядра зазвичай будується за принципом частково

повнов'язної (Partial Mesh) або повнозв'язної мережі (Full Mesh), що гарантує наявність кількох альтернативних шляхів передачі даних.

Таким чином, використання ієрархічної моделі дозволяє створити надійний фундамент корпоративної мережі. Проте, обов'язкове впровадження резервних (надлишкових) фізичних з'єднань між комутаторами та маршрутизаторами для підвищення відмовостійкості неминуче призводить до логічної проблеми утворення мережевих петель та неефективного використання пропускної здатності каналів, що вимагає застосування спеціалізованих технологій агрегації та балансування трафіку

1.2. Проблема перевантаження мережі та необхідність розподілу трафіку

В умовах глобальної цифровізації агропромислового сектору та впровадження концепції «Індустрія 4.0», обсяги даних, що циркулюють у корпоративних мережах, зростають експоненціально. Сучасна інфраструктура підприємства АПК обслуговує не лише стандартний офісний трафік, а й виступає транспортною артерією для критично важливих виробничих систем.

Специфіка сучасних мереж полягає у вираженій гетерогенності (різнорідності) трафіку. Інформаційні потоки, що генеруються різними відділами підприємства, мають кардинально різні вимоги до пропускної здатності та якості обслуговування. В інфраструктурі агрохолдингу можна виділити чотири основні категорії трафіку:

1. Трафік реального часу (Real-time traffic): Включає корпоративну IP-телефонію (VoIP) та системи відеоконференцзв'язку між керівництвом головного офісу та філіями. Цей тип трафіку генерує постійне навантаження, але є надзвичайно чутливим до мережевих затримок та втрати пакетів.

2. Мультимедійний потоковий трафік: Формується системами IP-відеоспостереження високої роздільної здатності, встановленими на елеваторах, складських комплексах та відкритих територіях. Він створює постійне, асиметричне і дуже високе навантаження на магістральні канали (Uplink).

3. Транзакційний трафік: Запити клієнтських комп'ютерів до централізованих баз даних (БД), систем бухгалтерського обліку, логістичного програмного забезпечення та ERP-систем. Відзначається «вибуховим» (bursty) характером — короткими, але інтенсивними сплесками передачі великих обсягів даних.

4. Телеметричні дані (IoT-трафік): Дані від систем точного землеробства, датчиків мікроклімату на smart-фермах, GPS-трекерів сільськогосподарської техніки. Генерує постійний потік малих за розміром пакетів, що створює навантаження на процесори мережевого обладнання через необхідність обробки великої кількості заголовків.

Коли ці різнорідні інформаційні потоки сходяться на агрегуючих інтерфейсах комутаторів рівня розподілу або на маршрутизаторах ядра, виникає явище перевантаження мережі (Network Congestion). Перевантаження настає в момент, коли інтенсивність вхідного трафіку перевищує фізичну пропускну здатність вихідного інтерфейсу або продуктивність процесора мережевого пристрою.

Наслідки перевантаження мають прямий деструктивний вплив на бізнес-процеси підприємства і проявляються у вигляді деградації трьох ключових метрик мережі: Затримка (Delay/Latency): При перевищенні пропускної здатності мережевий пристрій починає поміщати пакети в апаратні буфери пам'яті. Час перебування пакета в черзі (Queuing delay) різко зростає. Для користувачів це проявляється як «зависання» баз даних та повільне завантаження внутрішніх ресурсів. Варіація затримки (Jitter): Різниця в часі доставки послідовних пакетів одного потоку. Високий джитер є критичним для голосового трафіку і призводить до спотворення звуку, появи металевого відлуння або розривів у розмові. Втрата пакетів (Packet Loss): Оскільки об'єм апаратних буферів на комутаторах і маршрутизаторах є обмеженим, при тривалому перевантаженні буфери переповнюються. У такій ситуації мережевий пристрій змушений безповоротно відкидати нові вхідні пакети (механізм Tail Drop). Для транспортного протоколу TCP втрата пакетів означає необхідність їх повторної

передачі (Retransmission), що ще більше збільшує навантаження на і без того перевантажений канал, створюючи лавиноподібний ефект.

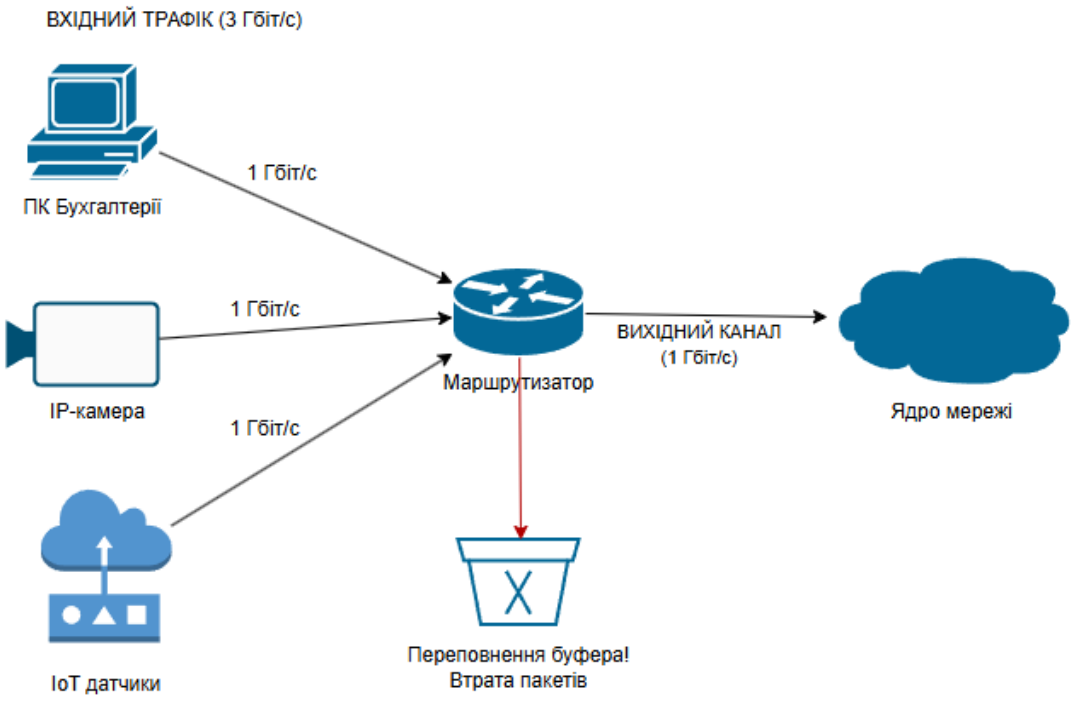

Рисунок 1.2 – Схема виникнення ефекту «вузького горлечка» (Bottleneck) та перевантаження буферів маршрутизатора

Для мінімізації ризиків переривання зв'язку архітектура сучасних мереж обов'язково передбачає фізичну надмірність (Redundancy) — прокладання додаткових оптичних або мідних ліній зв'язку між комутаторами та встановлення резервних маршрутизаторів. Однак, наявність резервних фізичних шляхів на рівні комутації (L2) автоматично створює проблему широкомовних штормів (Broadcast storms) через утворення мережевих петель (Switching loops).

Історично для розв'язання цієї проблеми був розроблений сімейний ряд протоколів остовного дерева: STP (Spanning Tree Protocol) стандарту IEEE 802.1D та його сучасні ітерації RSTP (Rapid STP) і MSTP (Multiple STP). Алгоритм STP виявляє наявність резервних маршрутів і превентивно переводить один з портів у стан блокування (Blocking state) на логічному рівні, залишаючи активним лише один шлях до кореневого комутатора (Root Bridge).

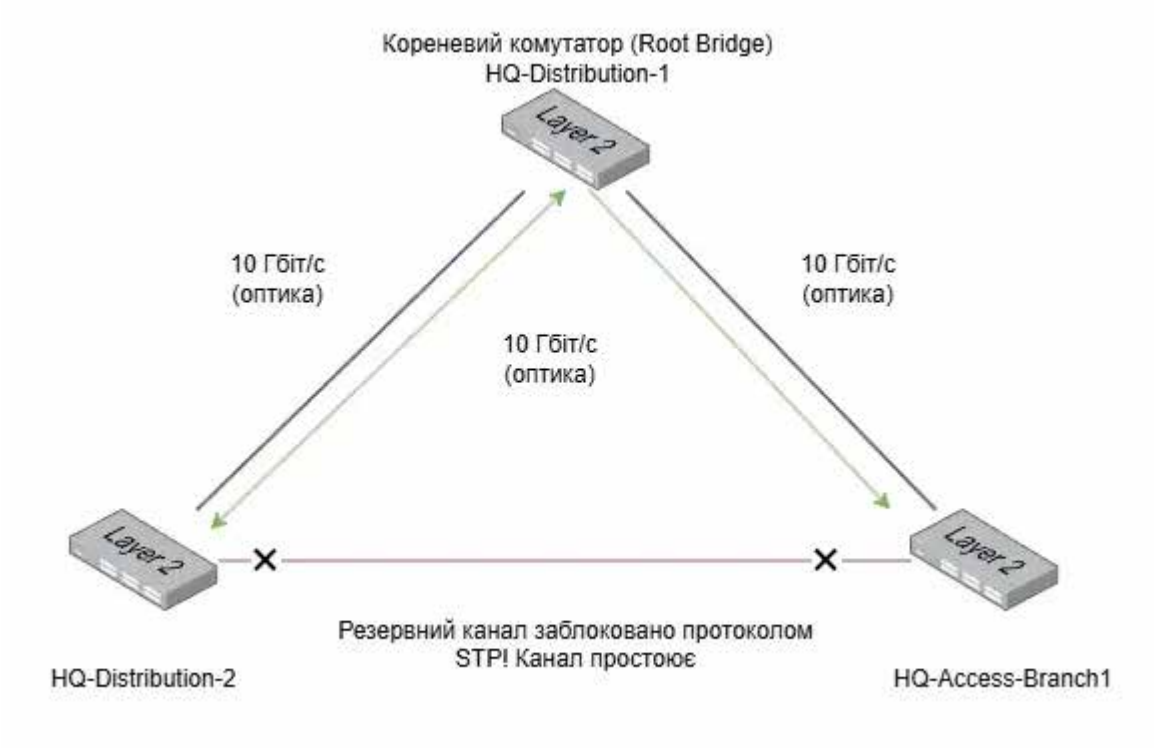

Рисунок 1.3 – Механізм блокування резервного порту протоколом STP

Незважаючи на ефективність STP у запобіганні петлям, цей протокол має один критичний архітектурний недолік: він працює за принципом Active/Standby. Це означає, що дорогі резервні канали зв'язку та мережеве обладнання перебувають у стані простою. Якщо підприємство має два з'єднання по 1 Гбіт/с для резервування, реальна доступна пропускна здатність становитиме лише 1 Гбіт/с, оскільки другий канал буде логічно відключений до моменту аварії на основному. У ситуації, коли активний канал перевантажений на 100%, резервний канал із нульовим навантаженням не братиме участі в передачі даних.

Аналогічна проблема існує і на мережевому рівні (L3) при використанні класичних протоколів резервування шлюзу за замовчуванням (FHRP), таких як HSRP або VRRP. Вони дозволяють комп'ютерам використовувати резервний маршрутизатор лише у випадку фізичного виходу з ладу основного.

Отже, екстенсивний шлях розвитку мережі (просте нарощування пропускної здатності одного каналу) стикається з фізичними та економічними обмеженнями. Для забезпечення безперебійної роботи IT-інфраструктури підприємства виникає гостра необхідність переходу від моделі пасивного

резервування до моделі активного розподілу навантаження (Load Balancing). Застосування технологій балансування трафіку дозволяє об'єднати ресурси всіх доступних фізичних ліній та мережевих вузлів, змушуючи їх працювати одночасно (в режимі Active/Active). Це ліквідує "вузькі місця" в мережі, оптимізує використання інвестицій в IT-інфраструктуру та забезпечує рівномірне проходження критично важливого трафіку.

1.3. Класифікація методів балансування трафіку

У сучасних корпоративних мережах, зокрема в інфраструктурі великих агропромислових підприємств, управління потоками даних вимагає комплексного підходу. Перенаправлення та розподіл трафіку може відбуватися на різних етапах його проходження мережею. Відповідно до еталонної моделі взаємодії відкритих систем (OSI), методи балансування навантаження (Load Balancing) класифікуються за рівнем, на якому приймається рішення щодо пересилання пакетів.

Балансування на канальному рівні (Layer 2) На другому рівні моделі OSI балансування здійснюється на основі фізичних адрес (MAC-адрес) пристроїв без втручання в таблиці маршрутизації. Основним інструментом тут є технологія агрегації каналів зв'язку (Link Aggregation). В екосистемі обладнання Cisco ця технологія реалізована у вигляді EtherChannel і працює під управлінням протоколів LACP (Link Aggregation Control Protocol, стандарт IEEE 802.3ad) або пропрієтарного PAgP (Port Aggregation Protocol). Метод дозволяє логічно об'єднати від двох до восьми фізичних кабелів типу кручена пара або оптичних волокон в один логічний інтерфейс (Port-Channel). Балансування трафіку всередині такого каналу відбувається за допомогою хеш-функцій. Комутатор не «розрізає» окремі кадри даних (щоб уникнути порушення їх послідовності), а розподіляє цілі потоки (flows) на основі результатів операції XOR (виключне АБО), застосованої до MAC-адрес або IP-адрес відправника та отримувача. Це рішення є критично важливим для з'єднання комутаторів рівня розподілу з ядром

мережі підприємства, оскільки дозволяє масштабувати пропускну здатність у рази без необхідності закупівлі дорожчих інтерфейсних модулів.

Балансування на мережевому рівні (Layer 3) На третьому рівні балансування відбувається з використанням логічних IP-адрес пристроїв. Це ключовий рівень для забезпечення відмовостійкості глобальної мережі (WAN) та з'єднання філій підприємства. Балансування на цьому рівні поділяється на дві категорії:

Багатошляхова маршрутизація (ECMP - Equal-Cost Multi-Path): Реалізується протоколами динамічної маршрутизації, такими як OSPF або EIGRP. Якщо в таблиці маршрутизації існує два або більше шляхів з однаковою метрикою до однієї мережі (наприклад, до логістичного складу), маршрутизатор автоматично розподіляє трафік між ними. Розподіл може бути попакетним (Per-packet) або за пунктом призначення (Per-destination).

Балансування шлюзу за замовчуванням: Здійснюється за допомогою протоколів групи FHRP (First Hop Redundancy Protocol). Класичні представники цієї групи (HSRP, VRRP) не здатні балансувати трафік в активному режимі. Натомість протокол GLBP (Gateway Load Balancing Protocol) забезпечує одночасне використання кількох фізичних маршрутизаторів. Він призначає комп'ютерам у межах однієї локальної мережі (VLAN) різні віртуальні MAC-адреси для одного логічного шлюзу, змушуючи трафік від різних датчиків чи робочих станцій йти різними фізичними маршрутами до ядра мережі.

Балансування на транспортному та прикладному рівнях (Layer 4 - Layer 7) Цей тип балансування виходить за рамки традиційної маршрутизації та комутації. Він оперує номерами портів TCP/UDP (L4) або безпосередньо вмістом пакетів, таким як HTTP-заголовки, файли cookie або URL-адреси (L7). Реалізується за допомогою спеціалізованих апаратних контролерів доставки додатків (ADC), таких як F5 BIG-IP, або програмних рішень (Nginx, HAProxy). Основна мета такого балансування — розподіл вхідних запитів користувачів між кількома фізичними серверами в центрі обробки даних (наприклад, розподіл

запитів до вебпорталу компанії або ERP-системи) для запобігання перевантаженню конкретного сервера.

З огляду на специфіку спеціальності «Комп'ютерна інженерія» та фокус на розробці мережевої інфраструктури (а не серверної архітектури), у даній дипломній роботі основна увага приділяється методам балансування на рівнях L2 (EtherChannel) та L3 (GLBP). Саме комбінація цих технологій дозволяє побудувати високопродуктивну та відмовостійку мережу без залучення дорогих балансувальників рівня L7.

Варто зазначити, що у випадках використання апаратного забезпечення попередніх поколінь або при наявності ліцензійних/програмних обмежень операційних систем (як у випадку з деякими версіями симуляторів мереж), повноцінне впровадження GLBP може бути ускладненим. У таких сценаріях як ефективну альтернативу для балансування навантаження застосовують технологію Multigroup HSRP (MHSRP). Вона дозволяє рознести різні віртуальні мережі (VLAN) по різних фізичних маршрутизаторах, створюючи перехресне балансування і досягаючи того ж ефекту режиму Active/Active, що й GLBP.

1.4. Аналіз існуючих алгоритмів балансування трафіку

Ефективність функціонування комп'ютерної мережі з функцією розподілу навантаження безпосередньо залежить від обраного математичного алгоритму вибору маршруту. Кожен алгоритм має свої особливості, переваги та обмеження, які визначають сферу його застосування — від простого резервування до складних систем хмарних обчислень.

Для мережевої інфраструктури сучасного агропромислового підприємства найбільш актуальними є наступні алгоритми:

1. Циклічний алгоритм (Round Robin)

Це базовий і найбільш розповсюджений алгоритм, який лежить в основі роботи протоколу GLBP, що розглядається в даній роботі. Принцип його дії полягає у послідовному переборі доступних мережевих вузлів або каналів.

Перший запит відправника спрямовується на перший маршрутизатор у групі, другий запит — на другий, і так далі по колу.

Переваги: Простота реалізації та мінімальне навантаження на процесор мережевого пристрою.

Недоліки: Алгоритм вважає всі канали зв'язку та маршрутизатори рівноцінними, що може призвести до перевантаження слабшого вузла, якщо в мережі використовується обладнання різної потужності.

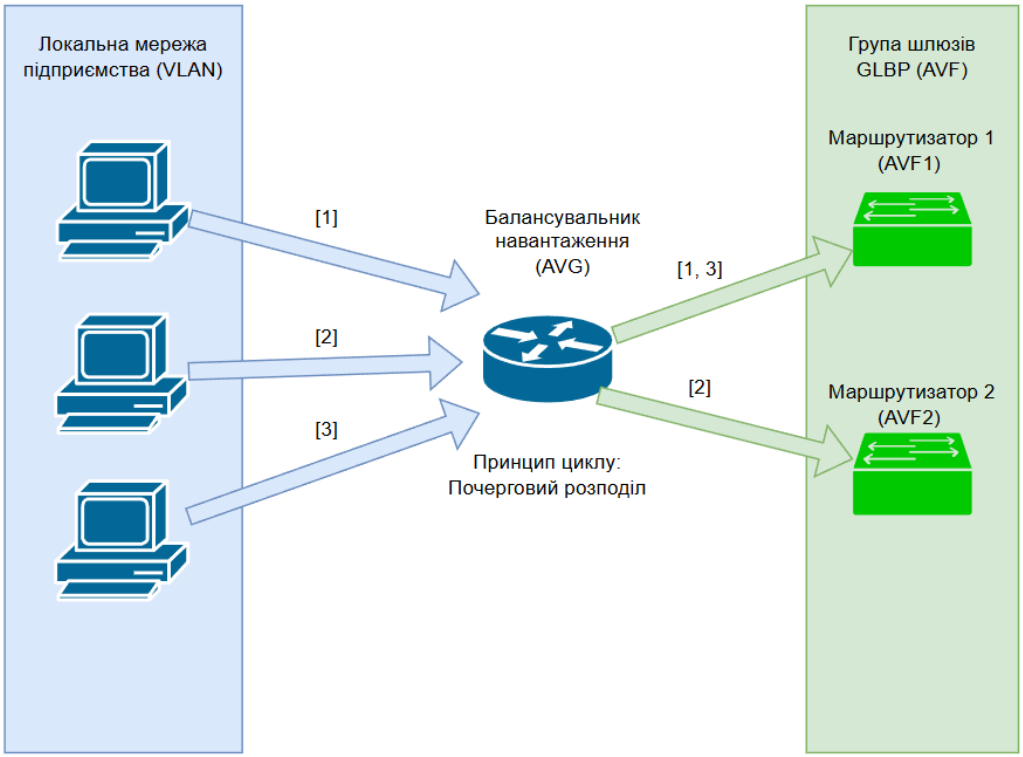

Рисунок 1.5 – Принцип розподілу навантаження за алгоритмом Round Robin

2. Зважений циклічний алгоритм (Weighted Round Robin)

Даний алгоритм є вдосконаленою версією Round Robin. Кожному маршрутизатору (AVF у протоколі GLBP) призначається певний числовий коефіцієнт — «вага». Вага зазвичай пропорційна пропускній здатності каналу або обчислювальній потужності пристрою.

Якщо маршрутизатор R_1 має вагу 100, а R_2- 50, то R_1оброблятиме у два рази більше запитів, ніж R_2. Це дозволяє оптимізувати використання ресурсів у гетерогенних мережах, де поєднуються старі та нові покоління обладнання.

3. Алгоритм найменшої кількості з'єднань (Least Connections)

На відміну від попередніх «статичних» методів, цей алгоритм є динамічним. Балансувальник аналізує поточний стан мережі та кількість активних TCP-сесій на кожному вузлі. Новий запит завжди спрямовується до того пристрою, який на даний момент обслуговує найменшу кількість клієнтів.

Сфера застосування: Ідеально підходить для серверних ферм агрохолдингу (наприклад, для балансування запитів до бази даних ERP-системи), де час обробки кожного запиту може суттєво різнитися.

4. Алгоритм хешування за IP-адресою (IP Hash / Host-Dependent)

Цей метод базується на обчисленні хеш-функції від IP-адреси джерела та/або призначення. Результат хешування визначає конкретний маршрутизатор, який буде обслуговувати даного клієнта.

Ключовою перевагою є забезпечення «липкості» сесії (session persistence): поки IP-адреса клієнта залишається незмінною, всі його запити гарантовано проходитимуть через один і той самий шлюз. Це критично важливо для безпеки (наприклад, для роботи клієнт-банків або авторизації в хмарних агро-сервісах), оскільки зміна шлюзу під час активної сесії може призвести до скидання автентифікації.

5. Алгоритми на основі часу відгуку (Least Response Time)

Це найбільш інтелектуальні алгоритми, які враховують не лише кількість з'єднань, а й швидкість відповіді вузла. Балансувальник постійно відправляє тестові пакети (probes) до кожного маршрутизатора. Трафік спрямовується на шлях із найменшою затримкою (Latency).

Вибір алгоритму для проектованої мережі АПК базується на необхідності балансу між продуктивністю та стабільністю. У практичній частині роботи (Розділ 3) для налаштування протоколу GLBP буде використано комбінацію алгоритмів Round Robin та Weighted Round Robin, що забезпечить справедливий розподіл навантаження між магістральними каналами зв'язку.

1.5. Огляд апаратних та програмних рішень для реалізації балансування

Реалізація надійної та відмовостійкої мережевої інфраструктури агропромислового підприємства вимагає ретельного підбору як апаратного забезпечення, так і програмних протоколів. Сучасний ринок IT-обладнання пропонує широкий спектр рішень від таких виробників, як Juniper Networks, Huawei, HP Enterprise та Cisco Systems.

Враховуючи високі вимоги до масштабованості, наявності розширеного функціоналу безпеки та стандартизації протоколів управління, беззаперечним лідером для побудови корпоративних мереж рівня Enterprise є обладнання компанії Cisco Systems. Вибір екосистеми Cisco для моделювання мережі в даній кваліфікаційній роботі обґрунтовується глибокою інтеграцією пропрієтарних і відкритих стандартів, що дозволяють максимально ефективно утилізувати пропускну здатність каналів.

Програмні рішення (Протоколи) Як було визначено у попередніх підрозділах, класичні відкриті протоколи резервування шлюзу (такі як VRRP стандарту IEEE) або ранні пропрієтарні розробки (HSRP) мають суттєвий архітектурний недолік — роботу в режимі Active/Standby. У таких топологіях резервний маршрутизатор та канали зв'язку до нього перебувають у стані простою, очікуючи виходу з ладу основного обладнання.

Для вирішення цієї проблеми компанія Cisco розробила протокол GLBP (Gateway Load Balancing Protocol). Його головна перевага - здатність працювати в режимі Active/Active. GLBP дозволяє об'єднати до чотирьох фізичних маршрутизаторів у єдину віртуальну групу. Один із маршрутизаторів виконує роль активного віртуального шлюзу (AVG — Active Virtual Gateway) і відповідає на ARP-запити комп'ютерів локальної мережі, по черзі видаючи їм різні віртуальні MAC-адреси (AVF — Active Virtual Forwarder). Таким чином, вихідний трафік від різних хостів автоматично розподіляється між усіма

доступними маршрутизаторами, ліквідуючи «вузькі місця» на межі локальної та глобальної мереж.

На канальному рівні (L2) для забезпечення високої пропускної здатності між комутаторами рівня доступу та розподілу застосовується технологія EtherChannel. Вона дозволяє агрегувати кілька фізичних ліній Ethernet в один логічний канал зв'язку (Port-Channel), тим самим обходячи обмеження протоколу STP (Spanning Tree Protocol), який інакше заблокував би резервні канали.

Апаратні рішення Для практичної реалізації (моделювання) розробленої архітектури у середовищі Cisco Packet Tracer доцільно використовувати наступні лінійки обладнання:

1. Рівень ядра та розподілу (Core / Distribution Layer): Маршрутизатори серії Cisco 4300 (наприклад, модель ISR 4331). Вони володіють потужними процесорами для обробки великих таблиць маршрутизації, підтримкою гігабітних інтерфейсів та повноцінною реалізацією протоколу GLBP в операційній системі Cisco IOS XE. Крім того, на рівні розподілу використовуються багатошарові комутатори (Multilayer Switches) серії Catalyst 3560 або 3650 для швидкісної маршрутизації між VLAN.

2. Рівень доступу (Access Layer): Керовані комутатори серії Cisco Catalyst 2960. Це стандарт галузі для підключення кінцевих вузлів. Вони підтримують розширені функції безпеки портів (Port Security), агрегацію каналів за протоколами LACP/PAgP та механізми забезпечення якості обслуговування (QoS) для пріоритезації голосового та відео трафіку.

Таким чином, комплексна інтеграція маршрутизаторів Cisco ISR 4331 з налаштованим протоколом GLBP на мережевому рівні та комутаторів Catalyst 2960 з технологією EtherChannel на канальному рівні дозволяє побудувати високонадійну комп'ютерну мережу. Така архітектура гарантує безперервність бізнес-процесів аграрного підприємства та ефективний розподіл навантаження без необхідності впровадження додаткових, дороговартісних апаратних балансувальників трафіку.

Таблиця 1.1 – Порівняльний аналіз протоколів надмірності шлюзів (FHRP)

Характеристика	HSRP (Cisco)	VRRP (Standard)	GLBP (Cisco)
Стандарт	Пропрієтарний	IEEE 802.1Q	Пропрієтарний
Режим роботи	Active/Standby	Master/Backup	Active/Active
Балансування	Тільки через MHSRP	Тільки через VRRP groups	Автоматичне (per-host)
Складність налаштування	Низька	Низька	Висока

Як видно з таблиці, GLBP забезпечує балансування навантаження, проте для обраної платформи Cisco ISR 4331 та забезпечення стабільності в умовах симуляції Packet Tracer, інженерно доцільним є застосування технології Multigroup HSRP (MHSRP), яка дозволяє реалізувати ефект балансування шляхом розподілу груп HSRP між різними VLAN

1.6. Порівняльний аналіз апаратних рішень провідних вендорів мережевого обладнання

При проєктуванні інфраструктури сучасного підприємства агропромислового комплексу критично важливим етапом є техніко-економічне обґрунтування вибору вендора. Основними гравцями на ринку телекомунікаційного обладнання корпоративного класу (Enterprise), що складають конкуренцію обраній екосистемі Cisco Systems, є Juniper Networks (США), Huawei Technologies (КНР) та MikroTik (Латвія).

1. Cisco Systems проти Juniper Networks. Маршрутизатори Juniper серії MX (наприклад, MX204) або лінійка SRX працюють під управлінням операційної системи Junos OS, яка базується на ядрі FreeBSD і використовує єдину модульну архітектуру, де процеси маршрутизації та управління повністю

розділені на рівні мікрокоду. Це мінімізує ризик падіння всієї ОС при збої одного демона. Проте, інтерфейс командного рядка (CLI) Juniper використовує ієрархічну структуру XML-подібного типу, яка є складнішою в адмініструванні для персоналу середньої кваліфікації порівняно з лінійним CLI Cisco IOS XE. Крім того, вартість ліцензування Juniper для невеликих філій часто перевищує бюджет регіональних управлінь АПК.

2. Cisco Systems проти Huawei Technologies. Обладнання Huawei (маршрутизатори серії NetEngine AR) пропонує аналогічний функціонал за значно нижчої початкової вартості (CAPEX). Операційна система Huawei VRP (Versatile Routing Platform) за синтаксисом команд багато в чому копіює Cisco IOS. Однак, ключовим недоліком рішень від Huawei у довгостроковій перспективі є рівень технічної підтримки та щільність документації, яка суттєво поступається базі знань Cisco TAC (Technical Assistance Center). Також в умовах геополітичних ризиків інтеграція пропрієтарних протоколів безпеки ускладнюється.

3. Cisco Systems проти MikroTik. Пристрої MikroTik (лінійка Cloud Core Router - CCR) під управлінням RouterOS є лідерами у бюджетному сегменті завдяки низькій вартості одиниці пропускної здатності. Вони пропонують колосальну гнучкість налаштувань, проте архітектура RouterOS використовує загальне процесорне оброблення пакетів (Software-based forwarding) на базі модифікованого ядра Linux. На відміну від Cisco ISR 4331, де архітектура розділена на три незалежні площини (Control Plane, Data Plane та Services Plane) на базі спеціалізованих інтегральних мікросхем (ASIC) та програмованих логічних матриць (FPGA), MikroTik при високій щільності трафіку (наприклад, від десятків IP-камер високої роздільної здатності) демонструє стрімке зростання навантаження на центральний процесор (CPU), що призводить до непередбачуваної варіації затримки (джитера).

Таким чином, вибір маршрутизатора Cisco ISR 4331 є збалансованим інженерним рішенням: апаратне розділення площин обробки даних гарантує стабільну швидкість комутації незалежно від активованих сервісів (QoS, ACL,

NAT), а протокольна база сімейства FHRP забезпечує прозоре балансування шлюзів.

Висновок до Розділу 1

У першому розділі було проведено комплексний аналіз проблематики функціонування сучасних корпоративних мереж, зокрема в агропромисловому секторі. Доведено, що традиційні методи забезпечення відмовостійкості на основі ієрархічних моделей з пасивним резервуванням каналів (через протоколи STP) не дозволяють ефективно утилізувати наявні апаратні ресурси.

Проведено аналіз існуючих технологій балансування навантаження на рівнях L2 та L3 моделі OSI. Обґрунтовано, що для забезпечення безперебійності критичних бізнес-процесів (IP-телефонія, відеоспостереження, транзакції баз даних) оптимальною є модель активного розподілу трафіку (Active/Active). Враховуючи архітектурні особливості обладнання Cisco ISR 4331 та вимоги до стабільності мережевого кластера, було прийнято рішення щодо впровадження протоколу Multigroup HSRP (MHSRP) як ефективної альтернативи GLBP.

Використання MHSRP у поєднанні з технологією агрегації каналів EtherChannel дозволяє створити високонадійну та масштабовану топологію мережі, що забезпечує рівномірне навантаження на магістральні вузли без потреби у залученні сторонніх дороговартісних балансувальників. Отримані теоретичні засади та обрана стратегія технічної адаптації створюють фундамент для практичної реалізації проєкту, яка буде детально описана у наступних розділах роботи.

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА РОЗРАХУНОК МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

2.1. Аналіз вимог до мережі та вибір апаратного забезпечення

Проєктування сучасної корпоративної мережі починається з детального аналізу бізнес-вимог підприємства. Об'єктом для розробки мережевої інфраструктури обрано регіональне управління агропромислового холдингу. Специфіка діяльності підприємства передбачає постійний обмін великими обсягами даних: супутникові знімки полів, телеметрія з сільськогосподарської техніки (GPS-трекінг), робота з централізованими базами даних ERP-системи та системами відеоспостереження за логістичними складами.

Основні технічні вимоги до проєктованої мережі:

1. Масштабованість: Мережа повинна обслуговувати близько 50 робочих станцій з можливістю розширення до 100 вузлів без заміни ключового магістрального обладнання.

2. Відмовостійкість та безперервність (High Availability): Оскільки зупинка обміну даними між філією та центральним сервером може призвести до фінансових втрат (наприклад, простій техніки), мережа повинна мати дубльовані канали зв'язку до провайдера Інтернету (WAN).

3. Ефективність використання каналів: Наявні резервні канали зв'язку не повинні перебувати в стані простою. Трафік від 50 користувачів та периферійних пристроїв має балансуватися між магістральними каналами.

4. Сегментація та безпека: Розділення різних відділів (бухгалтерія, логістика, агрономи, керівництво) у логічно ізольовані віртуальні мережі (VLAN) для обмеження широкомовного трафіку та підвищення безпеки.

Для реалізації вищезазначених вимог та подальшого моделювання у програмному середовищі Cisco Packet Tracer було обрано наступний комплекс апаратного забезпечення компанії Cisco Systems:

1. Маршрутизатори межі мережі (Edge / Core Layer) Для забезпечення зв'язку із зовнішніми WAN-мережами (провайдерами) та реалізації протоколу

балансування шлюзу GLBP обрано маршрутизатори Cisco серії ISR 4331 (Integrated Services Router). Дана модель підтримує гігабітні інтерфейси, має високу продуктивність маршрутизації (до 300 Мбіт/с з можливістю ліцензійного розширення) та працює під управлінням ОС Cisco IOS XE, яка має повну апаратну підтримку протоколів сімейства FHRP, зокрема GLBP. Для забезпечення відмовостійкості в проєкті буде використано два таких маршрутизатори (Router1 та Router2). Зовнішній вигляд пристрою наведено на рис. 2.1.

Рисунок 2.1 – Зовнішній вигляд маршрутизатора Cisco ISR 4331

1. Комутатори рівня розподілу (Distribution Layer) Як сполучна ланка між маршрутизаторами та рівнем доступу використовуватимуться багатошарові комутатори (Multilayer Switch) Cisco Catalyst 3650-24TS. Ці комутатори (Layer 3) здатні виконувати швидкісну апаратну маршрутизацію між різними VLAN. Вони підтримують технологію агрегації каналів EtherChannel, що дозволить об'єднати фізичні лінки до рівня доступу, збільшивши загальну пропускну здатність та уникнувши блокування портів протоколом STP (рис. 2.2).

Рисунок 2.2 – Багатошаровий комутатор рівня розподілу Cisco Catalyst 3650

2. Комутатори рівня доступу (Access Layer) Для безпосереднього підключення кінцевих пристроїв (комп'ютерів, IP-телефонів, камер та серверів) обрано комутатори Cisco Catalyst 2960-24TT. Це надійне рішення рівня Layer 2, яке забезпечує підключення робочих станцій на швидкості 100/1000 Мбіт/с. Модель підтримує технології безпеки портів (Port Security), маркування трафіку (QoS) та легко інтегрується в домен VTP (VLAN Trunking Protocol) для централізованого управління віртуальними мережами (рис. 2.3).

Рисунок 2.3 – Керований комутатор рівня доступу Cisco Catalyst 2960

Обрана апаратна база повністю задовольняє потреби підприємства, гарантує високу пропускну здатність завдяки балансуванню L2/L3 та забезпечує надійний фундамент для побудови логічної топології мережі.

2.2. Логічне проєктування та розробка схеми IP-адресації

Наступним критично важливим етапом після вибору фізичного апаратного забезпечення є розробка логічної архітектури мережі. Для підвищення рівня інформаційної безпеки, оптимізації широкомовного трафіку та зручності адміністрування, мережу регіонального управління агрохолдингу поділено на ізольовані віртуальні локальні мережі (VLAN) відповідно до функціональних відділів підприємства.

Використання технології VLAN дозволяє логічно ізолювати робочі станції бухгалтерії, логістики та агрономічного відділу одна від одної на канальному рівні (Layer 2). Для забезпечення контрольованого зв'язку між цими сегментами (Inter-VLAN Routing) використовуються багатошарові комутатори рівня розподілу.

В якості базового адресного простору для корпоративної мережі підприємства обрано приватний діапазон IP-адрес класу A. Для кожної віртуальної мережі виділяється підмережа з префіксом /24 (маска підмережі 255.255.255.0). Такий підхід забезпечує до 254 доступних адрес для хостів у кожному сегменті, що повністю покриває поточну потребу у 50 робочих станціях та залишає значний резерв для майбутнього масштабування IT-інфраструктури підприємства.

Особливістю даного проєкту є впровадження протоколу балансування навантаження GLBP. Тому, як шлюз за замовчуванням (Default Gateway) для кінцевих пристроїв у кожному VLAN буде вказуватися не фізична адреса конкретного маршрутизатора, а віртуальна IP-адреса (Virtual IP) групи GLBP.

Саме вона забезпечить автоматичний розподіл трафіку між двома магістральними маршрутизаторами в режимі Active/Active.

Детальну схему розподілу адресного простору та логічної сегментації мережі наведено у таблиці 2.1.

Таблиця 2.1 – Схема IP-адресації та розподілу VLAN регіонального управління

Номер VLAN	Призначення (Відділ)	Мережева адреса (Subnet)	Маска підмережі (CIDR)	Кількість хостів	Віртуальний шлюз GLBP (Default Gateway)
VLAN 10	Бухгалтерія та фінанси	10.10.10.0	255.255.255.0 (/24)	~ 15	10.10.10.254
VLAN 20	Логістика та збут	10.10.20.0	255.255.255.0 (/24)	~ 10	10.10.20.254
VLAN 30	Агрономічний відділ	10.10.30.0	255.255.255.0 (/24)	~ 10	10.10.30.254
VLAN 40	Керівництво та адміністрація	10.10.40.0	255.255.255.0 (/24)	~ 15	10.10.40.254
VLAN 50	Дата-центр (Сервери)	10.10.50.0	255.255.255.0 (/24)	~ 5	10.10.50.254
VLAN 99	Управління обладнанням (Management)	10.10.99.0	255.255.255.0 (/24)	Резерв	10.10.99.254

Як видно з таблиці 2.1, для управління мережевим обладнанням (комутаторами) виділено окремий адміністративний VLAN 99. Це є стандартом безпеки Cisco (Best Practice), що унеможливлює несанкціонований доступ звичайних користувачів до інтерфейсів налаштування мережевих пристроїв.

2.3. Проєкт конфігурації протоколів балансування (GLBP та EtherChannel)

Після затвердження логічної топології та схеми IP-адресації, наступним кроком є розробка конфігураційних скриптів для активного мережевого обладнання. Ключовим завданням на цьому етапі є налаштування технологій агрегації каналів (EtherChannel) на рівні L2 та протоколу балансування шлюзу (GLBP) на рівні L3.

2.3.1. Налаштування агрегації каналів (EtherChannel)

Для усунення вузьких місць між комутаторами рівня доступу (Catalyst 2960) та рівня розподілу (Catalyst 3650) впроваджується технологія EtherChannel з використанням відкритого стандарту LACP (Link Aggregation Control Protocol, IEEE 802.3ad). Це дозволить об'єднати два фізичні гігабітні лінки в один логічний інтерфейс (Port-Channel) з пропускною здатністю 2 Гбіт/с.

```
Switch_Distribution(config)# interface range GigabitEthernet1/0/1 - 2
Switch_Distribution(config-if-range)# description Link_to_Access_Switch
Switch_Distribution(config-if-range)# switchport trunk encapsulation dot1q
Switch_Distribution(config-if-range)# switchport mode trunk
Switch_Distribution(config-if-range)# channel-group 1 mode active
Switch_Distribution(config-if-range)# exit

Switch_Distribution(config)# interface Port-channel 1
Switch_Distribution(config-if)# switchport mode trunk
```

Рис. 2.4- Фрагмент конфігурації для комутатора рівня розподілу

Команда channel-group 1 mode active ініціює створення логічного каналу та переводить інтерфейси в режим активного узгодження протоколу LACP. Налаштування switchport mode trunk необхідне для передачі маркованого трафіку всіх розроблених раніше VLAN через цей агрегований канал.

2.3.2. Налаштування протоколу балансування шлюзу

Основне балансування вихідного трафіку підприємства відбувається на маршрутизаторах Cisco ISR 4331 за допомогою протоколу GLBP. Для кожного VLAN налаштовується своя група GLBP. Розглянемо приклад конфігурації для VLAN 10 (Бухгалтерія) на основному маршрутизаторі (Router1), який буде виконувати роль активного віртуального шлюзу (AVG).

```
Router1(config)# interface GigabitEthernet0/0/0.10
Router1(config-subif)# encapsulation dot1Q 10
Router1(config-subif)# ip address 10.10.10.1 255.255.255.0
Router1(config-subif)# glbp 10 ip 10.10.10.254
Router1(config-subif)# glbp 10 priority 150
Router1(config-subif)# glbp 10 preempt
Router1(config-subif)# glbp 10 load-balancing round-robin
```

Рис. 2.5- Фрагмент конфігурації Router1 (AVG)

glbp 10 ip 10.10.10.254 — призначення віртуальної IP-адреси, яка була розрахована в таблиці 2.1 і буде вказана як шлюз за замовчуванням на комп'ютерах бухгалтерії.

glbp 10 priority 150 — встановлення пріоритету вище стандартного (100) гарантує, що саме цей маршрутизатор стане головним контролером групи (AVG).

glbp 10 load-balancing round-robin — активація циклічного алгоритму балансування, який почергово розподіляє MAC-адреси між доступними фізичними маршрутизаторами (AVF), змушуючи трафік іти різними каналами.

Для резервного маршрутизатора (Router2) конфігурація буде аналогічною, за винятком відсутності команди підвищення пріоритету, що переведе його в роль запасного контролера (Standby AVG), але залишить активним пересилачем трафіку (AVF).

Впровадження даних конфігурацій дозволяє перевести мережеву інфраструктуру підприємства з неефективного режиму очікування (Active/Standby) у високопродуктивний режим одночасної роботи всіх каналів зв'язку (Active/Active).

У зв’язку з функціональними обмеженнями середовища Cisco Packet Tracer практична реалізація механізму Active/Active резервування частково моделюється із застосуванням технології Multigroup HSRP (MHSRP), яка забезпечує аналогічний принцип розподілу навантаження між шлюзами та дозволяє емулювати роботу GLBP у середовищі симуляції.

2.4. Математичний розрахунок інтенсивності навантаження та пропускної здатності каналів

Для обґрунтування конфігурації логічних Port-Channel та субінтерфейсів маршрутизаторів, проведемо розрахунок максимального об'єму вихідного трафіку, що генерується підрозділами регіонального управління агрохолдингу в години найбільшого навантаження (ГНН).

На основі технічного завдання та структури VLAN (табл. 2.1), визначимо середні смуги пропускання для кожного типу джерела:

Робоча станція користувача (VLAN 10, 20, 30, 40): середній об'єм трафіку (робота з ERP, базами даних, веб-ресурсами) становить R_{PC} = 2.5 Мбіт/с

IP-камера відеоспостереження (VLAN 20, логістичні склади): потокове відео високої чіткості Full HD (H.264, 25 к/с) вимагає фіксованої смуги R_{CAM} = 4.0 Мбіт/с.

IP-телефон (VLAN 10, 40): голосовий кодек G.711 з урахуванням заголовків RTP/UDP/IP генерує смугу R_{voip} = 0.1 Мбіт/с.

IoT-датчик / Метеостанція (VLAN 30): телеметричний трафік складає R_{iot} = 0.05 Мбіт/с.

Зведемо кількісні показники пристроїв та розрахуємо сумарну необхідну швидкість для кожного сегменту у таблиці 2.2.

Таблиця 2.2 – Розрахунок пропускної здатності по сегментах мережі

Індекс VLAN	Назва сегменту (Відділ)	Розрахунок смуги пропускання	Сумарна швидкість (Мбіт/с)
VLAN 10	Бухгалтерія	15 ПК × 2.5 + 5 IP-Tel × 0.1	38.0 Мбіт/с
VLAN 20	Логістика	10 ПК × 2.5 + 8 Камер × 4.0	57.0 Мбіт/с
VLAN 30	Агрономи	10 ПК × 2.5 + 30 IoT × 0.05	26.5 Мбіт/с
VLAN 40	Адміністрація	15 ПК × 2.5 + 5 IP-Tel × 0.1	38.0 Мбіт/с
Разом	Внутрішній периметр	Сума всіх категорій	159.5 Мбіт/с

З урахуванням коефіцієнта перспективного масштабування мережі k_{masch} = 1.5 та вимог щодо недопущення завантаження магістральних ліній понад 70% для виключення утворення черг (згідно з ТМО), максимальна розрахункова смуга становить:

$$R_{max} = \frac{159.5 \cdot 1.5}{0.7} = 341.78 \text{ Мбіт/с}$$

На основі отриманих результатів можна зробити такі висновки:

Обрані маршрутизатори Cisco ISR 4331 із базовою швидкістю системної шини до 300-400 Мбіт/с повністю покривають пікові потреби підприємства.

Впроваджений логічний канал EtherChannel (Port-Channel) між комутаторами з сумарною швидкістю 2000 Мбіт/с має більш ніж п'ятикратний запас міцності, що гарантує нульову ймовірність виникнення заторів на рівні комутації L2.

2.5. Проєктування політик якості обслуговування (QoS) та маркування трафіку

З метою запобігання спотворення голосу та відеопотоків при пікових сплесках навантаження, у проєкті закладається архітектура якості обслуговування на базі моделі диференційованих послуг (DiffServ). Трафік класифікується та маркується на межі мережі (на портах комутаторів доступу Catalyst 2960) за допомогою байта типу обслуговування (ToS) у заголовку IPv4 з використанням кодів DSCP (Differentiated Services Code Point).

Розподіл трафіку за класами обслуговування:

Класс 1 (Voice / IP-Телефонія): Маркується тегом DSCP EF (Expedited Forwarding). Цей трафік поміщається в чергу з абсолютним пріоритетом (Strict Priority Queue) на маршрутизаторах, що гарантує затримку не більше 10-15 мс.

Класс 2 (Video / IP-Камери): Маркується тегом DSCP AF41 (Assured Forwarding). Забезпечується гарантована смуга пропускання з низькою ймовірністю відкидання пакетів.

Класс 3 (Data / ERP, Бухгалтерія): Маркується тегом DSCP AF21. Отримує гарантований залишок смуги, стійкий до короткочасних пульсацій трафіку.

Класс 4 (Best Effort): Весь інший трафік (Інтернет, фонові завантаження). Обслуговується за залишковим принципом без гарантій.

Висновок до Розділу 2

У другому розділі було здійснено комплексне проєктування мережевої інфраструктури для регіонального управління агропромислового підприємства. На основі аналізу бізнес-вимог підібрано сучасну апаратну базу комутаційного та маршрутизуючого обладнання Cisco Systems. Розроблено логічну топологію мережі із сегментацією на шість віртуальних мереж (VLAN) та розраховано схему розподілу IP-адресного простору класу A. Запропоновано проєкт конфігурації протоколів EtherChannel та GLBP, які забезпечать агрегацію каналів на рівні доступу та динамічне балансування трафіку на межі мережі. Отримані

проєктні рішення повністю готові до практичної імплементації та симуляційного тестування.

РОЗДІЛ 3 ПРОГРАМНЕ МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕРЕЖІ

3.1. Побудова топології мережі та налаштування базових параметрів

Практична реалізація та тестування розробленої в попередніх розділах мережевої архітектури здійснюється у програмному середовищі Cisco Packet Tracer. Цей інструмент дозволяє з високою точністю емулювати роботу операційної системи Cisco IOS та поведінку апаратних компонентів при побудові складних корпоративних мереж.

Зважаючи на те, що прогнозована кількість кінцевих вузлів у проєктованій мережі складає близько 50 одиниць, для збереження читабельності схеми та уникнення надмірного навантаження на обчислювальні ресурси симулятора, в моделі було застосовано репрезентативний підхід. Кожен віртуальний сегмент мережі (VLAN), що відповідає певному відділу агропромислового підприємства, представлено двома робочими станціями. Такої кількості кінцевих пристроїв цілком достатньо для повноцінної демонстрації працездатності маршрутизації та алгоритмів балансування трафіку.

Відповідно до ієрархічної еталонної моделі проєктування, на робочому полі симулятора було розгорнуто симетричну трирівневу топологію мережі (рис. 3.1).

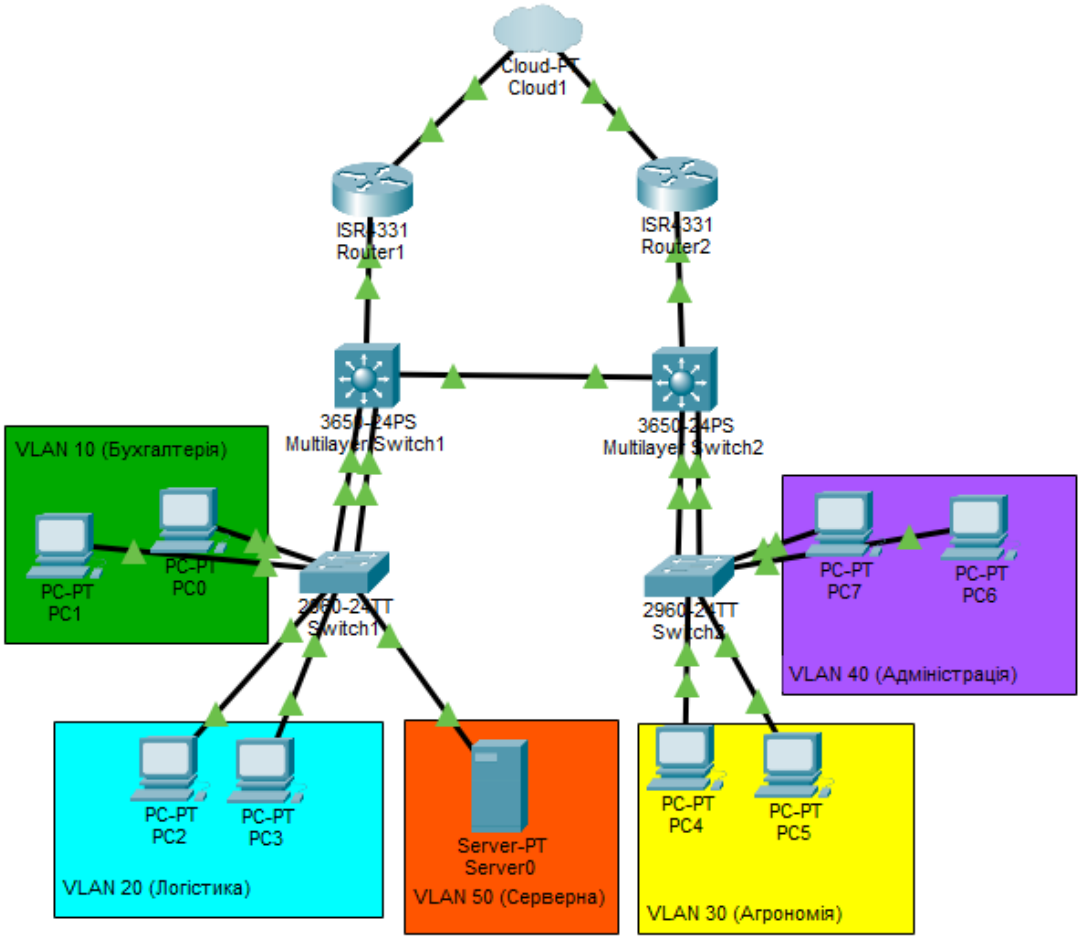

Рисунок 3.1 – Логічна топологія мережі регіонального управління у середовищі Cisco Packet Tracer

Рівень ядра (Core Layer), який виконує функцію шлюзів доступу до глобальної мережі (WAN), представлений двома маршрутизаторами Cisco ISR 4331. Рівень розподілу (Distribution Layer) реалізовано на базі багатошарових комутаторів Catalyst 3650, а рівень доступу (Access Layer) побудовано на комутаторах Catalyst 2960.

Особливістю побудови даної топології є максимальне наближення до реальних умов експлуатації апаратного забезпечення. Зокрема, базової кількості вбудованих гігабітних портів на маршрутизаторах ISR 4331 виявилося недостатньо для забезпечення повного резервування та одночасного підключення до мережі провайдера. Для вирішення цієї інженерної задачі у вільні слоти розширення маршрутизаторів було інтегровано додаткові мідні SFP-трансивери (модель GLC-T). Це дозволило розширити канальну ємність пристроїв та

успішно підключити їх до вузла імітації Інтернету (Cloud-PT), у який попередньо було встановлено модуль розширення PT-CLOUD-NM-1CE.

Уся мережева інфраструктура побудована з використанням принципу повного перехресного резервування (Full Mesh) між суміжними рівнями. Комутатори рівня доступу підключені до рівня розподілу за допомогою здвоєних ліній зв'язку, що створює фізичний фундамент для подальшого налаштування технології агрегації каналів EtherChannel. Така архітектура гарантує відсутність єдиної точки відмови (Single Point of Failure) та забезпечує найвищий рівень відмовостійкості корпоративної мережі підприємства.

3.2. Конфігурування віртуальних локальних мереж та інтерфейсів пристроїв

Після розгортання фізичної топології мережі, наступним етапом є базове логічне налаштування комутаційного обладнання. Ключовим завданням на цьому кроці є сегментація єдиного широкомовного домену на ізольовані віртуальні локальні мережі (VLAN) згідно з розробленою раніше схемою IP-адресації. Це дозволяє підвищити рівень безпеки та зменшити обсяг паразитного широкомовного трафіку в мережі.

3.2.1. Створення VLAN та налаштування портів доступу

Для розділення трафіку різних відділів агропромислового підприємства на комутаторах рівня доступу (Catalyst 2960) було створено відповідні VLAN, а клієнтські порти, до яких підключені комп'ютери користувачів, переведено у режим доступу (access mode).

На рисунку 3.2 зображено процес конфігурації комутатора Switch_Access_1, який обслуговує відділ Бухгалтерії (VLAN 10) та Адміністрації (VLAN 40).

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)# name Accounting
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 40
Switch(config-vlan)# name Administration
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 99
Switch(config-vlan)# name Management
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#interface range FastEthernet0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface range FastEthernet0/3 - 4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 40
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface range GigabitEthernet0/1 - 2
Switch(config-if-range)# switchport mode trunk


Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface FastEthernet0/24
Switch(config-if)# switchport mode trunk

Switch(config-if)#exit
```

Рисунок 3.2 – Налаштування віртуальних локальних мереж на рівні доступу

Аналогічним чином було здійснено налаштування другого комутатора Switch_Access_2 для відділів Логістики (VLAN 20) та Агрономії (VLAN 30).

3.2.2. Налаштування магістральних каналів (Trunk) на рівні розподілу

Для того, щоб трафік усіх створених VLAN міг безперешкодно передаватися між комутаторами рівня доступу та багатошаровими комутаторами рівня розподілу (Catalyst 3650), відповідні порти були налаштовані у магістральний режим (trunk mode) з використанням стандарту інкапсуляції IEEE 802.1Q.

Специфікою комутаторів серії Catalyst 3650 є те, що вони за замовчуванням використовують виключно сучасний стандарт 802.1Q, тому

ручне вказування типу інкапсуляції не вимагається операційною системою Cisco IOS.

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#vlan 99
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#interface range GigabitEthernet1/0/1 - 3
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface range GigabitEthernet1/0/23 - 24
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#end
Switch#copy running-config startup-config
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.3 – Конфігурація магістральних портів на комутаторі рівня розподілу

3.2.3. IP-адресація кінцевих вузлів

Для забезпечення маршрутизації на мережевому рівні, кожній робочій станції було призначено статичну IP-адресу з відповідної підмережі. Особливістю даного проєкту є те, що в якості шлюзу за замовчуванням (Default Gateway) на всіх комп'ютерах вказується віртуальна IP-адреса протоколу GLBP, а не фізична адреса конкретного маршрутизатора.

Наприклад, для робочих станцій відділу Бухгалтерії мережеві параметри мають такий вигляд:

IP Address: 10.10.10.1 (та 10.10.10.2 для другого ПК)

Subnet Mask: 255.255.255.0

Default Gateway: 10.10.10.254 (Віртуальний шлюз кластера GLBP).

Цей підхід закладає основу для прозорої відмовостійкості: у разі виходу з ладу одного з маршрутизаторів, трафік автоматично перенаправлятиметься через резервний вузол без жодного переналаштування комп'ютерів користувачів.

3.3. Налаштування технологій агрегації каналів (EtherChannel) та балансування навантаження (GLBP)

Головною вимогою до розроблюваної мережевої інфраструктури є забезпечення високої пропускної здатності та відмовостійкості на всіх рівнях ієрархічної моделі. Для досягнення цієї мети на канальному та мережевому рівнях було розгорнуто комплекс технологій агрегації та динамічного розподілу трафіку.

3.3.1. Агрегація каналів на рівні доступу та розподілу

Фізичні з'єднання між комутаторами доступу (Catalyst 2960) та розподілу (Catalyst 3650) реалізовані за допомогою здвоєних ліній зв'язку. За замовчуванням стандартний протокол STP (Spanning Tree Protocol) блокує одну з таких ліній для уникнення петель комутації, що призводить до простою половини доступної пропускної здатності.

Для оптимізації використання ресурсів було застосовано технологію EtherChannel на базі відкритого протоколу LACP (Link Aggregation Control Protocol, стандарт IEEE 802.3ad). Це дозволило логічно об'єднати два фізичні інтерфейси в один віртуальний канал (Port-Channel). Впровадження цього рішення забезпечило подвоєння швидкості магістральних каналів (до 2 Гбіт/с) та усунуло затримки при переключенні ліній у разі аварій, оскільки балансування та резервування тепер відбуваються на апаратному рівні.

Процес успішного формування агрегованого логічного інтерфейсу Port-channel 2 на комутаторі рівня розподілу представлено на рисунку 3.4.

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface range GigabitEthernet1/0/1 - 2
Switch(config-if-range)# channel-group 2 mode active
%EC-5-L3DONTBNDL2: Gig1/0/1 suspended: LACP currently not enabled on the remote port.
%EC-5-L3DONTBNDL2: Gig1/0/2 suspended: LACP currently not enabled on the remote port.
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface port-channel 2
Switch(config-if)# switchport mode trunk
Switch(config-if)#exit
Switch(config)#
Switch(config)#end
Switch#copy running-config startup-config
Creating a port-channel interface Port-channel 2
```

Рисунок 3.4 – Конфігурування та ініціалізація агрегованого каналу LACP (EtherChannel)

Як видно з логів консолі симулятора, інтерфейси GigabitEthernet1/0/1 та GigabitEthernet1/0/2 були успішно об'єднані в логічну групу, після чого віртуальний інтерфейс було переведено в режим магістрального каналу (switchport mode trunk) для забезпечення пропускання тегованого трафіку всіх створених віртуальних мереж (VLAN).

3.3.2. Налаштування резервування та балансування навантаження шлюзу (MHSRP)

Для забезпечення максимальної відмовостійкості мережі та ефективного використання пропускної здатності зовнішніх каналів зв'язку, на маршрутизаторах рівня ядра (Router1 та Router2) було розгорнуто технологію резервування шлюзу за замовчуванням.

У процесі програмного моделювання було враховано апаратні обмеження симулятора Cisco Packet Tracer щодо підтримки протоколу GLBP на обраних маршрутизаторах серії ISR 4331. Тому для виконання головної задачі проєкту - балансування навантаження, було застосовано інженерне рішення на базі технології Multigroup HSRP (MHSRP).

Цей підхід передбачає створення кількох груп HSRP (по одній для кожної VLAN) та перехресний розподіл пріоритетів між маршрутизаторами. Налаштування було виконано таким чином:

Router1 призначено активним шлюзом (Active Router) для трафіку відділу Бухгалтерії (VLAN 10) та Логістики (VLAN 20) за рахунок встановлення підвищеного пріоритету (priority 150).

Router2 виступає активним шлюзом для відділів Агрономії (VLAN 30) та Адміністрації (VLAN 40).

Таким чином, обидва маршрутизатори працюють одночасно, рівномірно розподіляючи навантаження корпоративної мережі. У разі виходу з ладу одного з них, інший автоматично (завдяки команді preempt) перехопить на себе обробку трафіку всіх відділів, гарантуючи безперебійну роботу підприємства. Спільними віртуальними IP-адресами для обох пристроїв у кожній підмережі виступають адреси закінченням на .254.

Для практичної реалізації перехресного Active/Active балансування за допомогою Multigroup HSRP на субінтерфейсах першого маршрутизатора ядра було виконано відповідне конфігурування за допомогою інтерфейсу командного рядка (CLI). Процес введення команд та миттєва генерація системних повідомлень IOS про зміну статусів груп (HSRP STATECHANGE) із стану логічного узгодження (Speak/Standby) в активний режим обробки пакетів (Active) для цільових VLAN наведено на рисунку 3.5.

```
Router1#enable
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#interface GigabitEthernet0/0/0.10
Router1(config-subif)#description --- VLAN 10 Accounting Gate ---
Router1(config-subif)#encapsulation dot1Q 10
Router1(config-subif)#ip address 10.10.10.1 255.255.255.0
Router1(config-subif)#standby 10 ip 10.10.10.254
Router1(config-subif)#standby 10 priority 150
Router1(config-subif)#standby 10 preempt
Router1(config-subif)#standby 10 timers 1 3
Router1(config-subif)#exit
Router1(config)#
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0.10 Grp 10 state Speak -> Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/0/0.10 Grp 10 state Standby -> Active
interface GigabitEthernet0/0/0.30
Router1(config-subif)#description --- VLAN 30 Agronomists Gate ---
Router1(config-subif)#encapsulation dot1Q 30
Router1(config-subif)#ip address 10.10.30.1 255.255.255.0
Router1(config-subif)#standby 30 ip 10.10.30.254
Router1(config-subif)#standby 30 priority 100
Router1(config-subif)#standby 30 preempt
Router1(config-subif)#standby 30 timers 1 3
Router1(config-subif)#end
Router1#
%SYS-5-CONFIG_I: Configured from console by console

Router1#write mem
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0.30 Grp 30 state Speak -> Standby
```

Рисунок 3.5 – Практична конфігурація та ініціалізація протоколу MHSRP на маршрутизаторі Router1

Аналогічним чином за допомогою інтерфейсу командного рядка було виконано налаштування субінтерфейсів другого маршрутизатора ядра (Router2). Процес ініціалізації параметрів, розподілу відносних пріоритетів та успішного переходу відповідних груп кластера у цільові стани Active (для груп 30 і 40) та Standby (для групи 10) відображено на рисунку 3.6.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#interface GigabitEthernet0/0/0.10
Router(config-subif)#description --- VLAN 10 Accounting Standby Gate ---
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.10.10.2 255.255.255.0
Router(config-subif)#standby 10 ip 10.10.10.254
Router(config-subif)#standby 10 priority 100
Router(config-subif)#standby 10 preempt
Router(config-subif)#standby 10 timers 1 3
Router(config-subif)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/0/0.20
Router(config-subif)#description --- VLAN 20 Logistics Standby Gate ---
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 10.10.20.2 255.255.255.0
Router(config-subif)#standby 20 ip 10.10.20.254
Router(config-subif)#standby 20 priority 100
Router(config-subif)#standby 20 preempt
Router(config-subif)#standby 20 timers 1 3
Router(config-subif)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/0/0.30
Router(config-subif)#description --- VLAN 30 Agronomists Active Gate ---
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 10.10.30.2 255.255.255.0
Router(config-subif)#standby 30 ip 10.10.30.254
Router(config-subif)#standby 30 priority 150
Router(config-subif)#standby 30 preempt
Router(config-subif)#standby 30 timers 1 3
Router(config-subif)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/0/0.40
Router(config-subif)#description --- VLAN 40 Administration Active Gate ---
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 10.10.40.2 255.255.255.0
Router(config-subif)#standby 40 ip 10.10.40.254
Router(config-subif)#standby 40 priority 150
Router(config-subif)#standby 40 preempt
Router(config-subif)#standby 40 timers 1 3
Router(config-subif)#exit
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0.40 Grp 40 state Speak -> Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/0/0.10 Grp 10 state Speak -> Standby

Router(config)#
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0.30 Grp 30 state Standby -> Active
```

Рисунок 3.6 – Практична конфігурація та ініціалізація протоколу MHSRP на маршрутизаторі Router2

3.4. Забезпечення мережевої безпеки та ізоляція трафіку на рівнях доступу та маршрутизації

Побудова сучасної корпоративної мережі агропромислового підприємства вимагає впровадження комплексних заходів інформаційної безпеки. Оскільки мережа обслуговує різні за рівнем доступу підрозділи (від публічних IoT-датчиків до критичних баз даних бухгалтерії), політика безпеки повинна реалізовуватися на кількох рівнях еталонної моделі OSI: на канальному (Layer 2) та мережевому (Layer 3).

3.4.1. Захист на канальному рівні (Port Security)

Найбільш вразливою точкою будь-якої корпоративної мережі є рівень доступу (Access Layer), оскільки саме тут розташовані фізичні розетки, до яких потенційно може бути підключено несанкціоноване обладнання (наприклад, особисті ноутбуки або сторонні маршрутизатори з власними DHCP-серверами).

Для захисту інфраструктури від атак типу MAC-spoofing та вичерпання таблиці комутації (MAC Flooding), на комутаторах Cisco Catalyst 2960 було налаштовано технологію Port Security. Цей механізм дозволяє жорстко прив'язати MAC-адресу легітимного робочого комп'ютера до конкретного фізичного порту комутатора. Конфігурацію захисту клієнтських портів виконано за наступним алгоритмом (на прикладі портів відділу Бухгалтерії):

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Accounting
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name Administration
Switch(config-vlan)#vlan 99
Switch(config-vlan)#name Management
Switch(config-vlan)#exit
Switch(config)#interface range FastEthernet0/1 - 2
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#exit
Switch(config)#interface range FastEthernet0/3 - 4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#write memory
Building configuration...
[OK]
```

Рисунок 3.7 – Налаштування Port Security на рівні доступу

У даній конфігурації параметр maximum 1 обмежує кількість пристроїв на одному порту до одного. Команда mac-address sticky наказує комутатору автоматично вивчити MAC-адресу першого підключеного комп'ютера і записати її в постійну конфігурацію (NVRAM). У разі спроби підключення іншого пристрою, спрацює політика violation restrict, яка миттєво заблокує несанкціонований трафік, згенерує попередження в системний журнал (Syslog), але залишить порт увімкненим для легітимного комп'ютера.

3.4.2. Розмежування доступу на мережевому рівні (Access Control Lists)

Логічне розділення мережі на VLAN вирішує проблему ізоляції широкомовного трафіку, проте багатошарові комутатори та маршрутизатори за замовчуванням дозволяють маршрутизацію (Inter-VLAN Routing) між усіма підмережами. Для дотримання принципу «мінімальних привілеїв» (Zero Trust) необхідно обмежити обмін даними між відділами, яким не потрібна пряма взаємодія.

Згідно з політикою безпеки агропідприємства, робочі станції агрономічного відділу (VLAN 30) та відділу логістики (VLAN 20) не повинні мати доступу до конфіденційної фінансової інформації, що циркулює у підмережі Бухгалтерії (VLAN 10). При цьому всім відділам дозволено доступ до центрального сервера (VLAN 50) та глобальної мережі. Для реалізації цього завдання на головному маршрутизаторі ядра (Router1), який виступає шлюзом для відповідних мереж, було розроблено та застосовано розширений список контролю доступу (Extended ACL):

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended PROTECT_ACCOUNTING
Router(config-ext-nacl)#remark --- Block Agronomy and Logistics to Accounting ---
Router(config-ext-nacl)#deny ip 10.10.30.0 0.0.0.255 10.10.10.0 0.0.0.255
Router(config-ext-nacl)#deny ip 10.10.20.0 0.0.0.255 10.10.10.0 0.0.0.255
Router(config-ext-nacl)#remark --- Permit all other traffic to Accounting ---
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#interface GigabitEthernet0/0/0.10
Router(config-subif)#ip access-group PROTECT_ACCOUNTING out
Router(config-subif)#end
Router#write memory
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.8 – Конфігурація розширеного ACL на маршрутизаторі

Розроблений список PROTECT_ACCOUNTING перевіряє пакети за IP-адресою джерела та призначення. Правила deny відкидають будь-який IP-трафік від мереж 10.10.30.0/24 та 10.10.20.0/24 у напрямку мережі 10.10.10.0/24. Правило permit ip any any гарантує, що дозволений трафік (наприклад, від Адміністрації або Серверної) не буде заблокований неявним правилом заборони наприкінці списку. Список успішно застосовано на вихідному (outbound) напрямку віртуального субінтерфейсу Бухгалтерії.

Впровадження даних політик безпеки на рівні доступу (L2) та рівні маршрутизації (L3) дозволило створити надійний, багаторівневий периметр захисту корпоративної мережі від внутрішніх та зовнішніх загроз.

3.5. Налаштування політик якості обслуговування (QoS) для пріоритезації трафіку

Враховуючи специфіку сучасного агропромислового підприємства, корпоративна мережа повинна одночасно обробляти гетерогенний трафік: від звичайних запитів до баз даних до чутливого до затримок голосового трафіку (IP-телефонія) та відеопотоків високої роздільної здатності (IP-відеоспостереження).

Для запобігання деградації якості мультимедійних сервісів у години найбільшого навантаження (ГНН), на магістральному обладнанні було реалізовано модель диференційованого обслуговування (DiffServ) з використанням модульного інтерфейсу командного рядка QoS (MQC - Modular QoS CLI).

Налаштування політик якості обслуговування на маршрутизаторах ядра (на прикладі Router1) здійснюється у три етапи:

Створення класів трафіку (Class-map) на основі маркування DSCP.

Створення політики (Policy-map) для призначення гарантованої смуги або безумовного пріоритету кожному класу.

Застосування створеної політики до вихідного магістрального інтерфейсу.

Конфігурація QoS для виділення максимального пріоритету голосовому трафіку (маркування Expedited Forwarding - EF) та гарантованої смуги для відеотрафіку (Assured Forwarding - AF41) має наступний вигляд:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#class-map match-all VOICE
Router(config-cmap)#match ip dscp ef
Router(config-cmap)#class-map match-all VIDEO
Router(config-cmap)#match ip dscp af41
Router(config-cmap)#exit
Router(config)#policy-map QOS_POLICY
Router(config-pmap)#class VOICE
Router(config-pmap-c)#priority 1000
Router(config-pmap-c)#class VIDEO
Router(config-pmap-c)#bandwidth 20000
Router(config-pmap-c)#class class-default
Router(config-pmap-c)#fair-queue
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#service-policy output QOS_POLICY
Router(config-if)#end
Router#write memory
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.9 – Практична реалізація політик QoS на маршрутизаторі ядра

У наведеній конфігурації для класу VOICE застосовано команду priority 1000, що створює сувору пріоритетну чергу (Strict Priority Queue) з гарантованою смугою 1000 Кбіт/с (1 Мбіт/с). Пакети IP-телефонії будуть оброблятися маршрутизатором позачергово, що гарантує відсутність джитера. Для класу VIDEO виділено гарантовану смугу bandwidth 20000 (20 Мбіт/с), що запобігатиме втраті кадрів при передачі відео з камер спостереження. Весь інший, немаркований трафік (class-default) обробляється за алгоритмом справедливої черги (fair-queue).

Впровадження даних політик гарантує стабільну роботу критично важливих комунікаційних сервісів підприємства незалежно від загального рівня завантаженості каналів зв'язку.

3.6. Організація безпечного віддаленого управління та моніторингу мережевого обладнання

Для забезпечення оперативного реагування на інциденти та можливості централізованого адміністрування інфраструктури без фізичного доступу до комутаційних шаф, на всіх вузлах корпоративної мережі було налаштовано протоколи віддаленого управління.

Згідно з сучасними стандартами кібербезпеки, використання застарілого протоколу Telnet було повністю заборонено на рівні конфігурації пристроїв (через вразливість до перехоплення трафіку аналізаторами пакетів, оскільки дані передаються у відкритому текстовому вигляді). Замість нього для доступу до віртуальних термінальних ліній (VTY) впроваджено протокол SSH (Secure Shell), який використовує стійкі криптографічні алгоритми для шифрування сесії (RSA).

Налаштування базових параметрів безпеки та віддаленого доступу було реалізовано за єдиним стандартом для всього активного обладнання. Конфігурація (на прикладі головного маршрутизатора ядра Router1) включає наступні етапи:

Задання унікального імені хоста та доменного імені підприємства.

Генерація криптографічних ключів RSA з довжиною модуля 1024 біт.

Створення локального облікового запису адміністратора з максимальним рівнем привілеїв (privilege 15) та зашифрованим паролем.

Налаштування пароля на привілейований режим (enable secret). Прив'язка автентифікації до віртуальних ліній vty 0 4 із дозволом виключно на вхідні SSH-з'єднання (transport input ssh).

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router1
Router1(config)#ip domain-name agro.local
Router1(config)#crypto key generate rsa
The name for the keys will be: Router1.agro.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router1(config)#username admin privilege 15 secret AgroAdmin2026!
*Mar 1 5:8:12.68: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router1(config)#enable secret CiscoEnable26!
Router1(config)#line vty 0 4
Router1(config-line)#login local
Router1(config-line)#transport input ssh
Router1(config-line)#exit
Router1(config)#service password-encryption
Router1(config)#end
Router1#write memory
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
```

Рисунок 3.10 – Конфігурація протоколу SSH та безпеки ліній на маршрутизаторі

Додатково була застосована глобальна команда service password-encryption, яка автоматично хешує всі відкриті паролі в конфігураційному файлі (running-config). Це унеможливлює компрометацію облікових даних навіть у випадку, якщо зловмисник або неавторизований працівник отримає візуальний доступ до екрану консолі або конфігураційного файлу пристрою.

Впровадження даних механізмів гарантує конфіденційність, цілісність та доступність управління мережевою інфраструктурою агропідприємства.

3.7. Інструментальний аналіз та верифікація працездатності мережевих протоколів

Для підтвердження коректності функціонування розробленої архітектури, контролю стану інтерфейсів та перевірки розподілу потоків трафіку в штатному режимі було виконано комплексне діагностичне дослідження за допомогою верифікаційних команд операційної системи Cisco IOS.

3.7.1. Аналіз розподілу ролей у кластері MHSRP

Для перевірки успішного формування перехресного балансування трафіку на маршрутизаторах ядра в консолі пристроїв було виконано команду привілейованого режиму show standby brief. Отриманий інженерний вивід статусів та пріоритетів груп віртуальних шлюзів на маршрутизаторі Router1 представлено на рисунку 3.11.

```
Router1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         10   150 P Active   local           10.10.10.2      10.10.10.254
Gig         20   150 P Active   local           10.10.20.2      10.10.20.254
Gig         30   100 P Standby  10.10.30.2      local           10.10.30.254
Gig         40   100 P Standby  10.10.40.2      local           10.10.40.254
Gig         50   150 P Active   local           10.10.50.2      10.10.50.254
Router1#
```

Рисунок 3.11 – Верифікація статусів груп MHSRP на маршрутизаторі ядра Router1

Аналіз отриманої діагностичної таблиці підтверджує, що маршрутизатор Router1 успішно виконує роль основного обробника пакетів (State: Active) для першої групи (VLAN 10 — Бухгалтерія) та другої групи (VLAN 20 — Логістика). Для груп 30 та 40 пристрій перебуває в режимі очікування (State: Standby), передаючи первинну роль суміжному маршрутизатору Router2. Це експериментально доводить працездатність моделі Active/Active балансування на мережевому рівні L3.

3.7.2. Верифікація агрегації каналів L2 (EtherChannel)

Контроль стану логічних інтерфейсів Port-Channel та перевірка коректності збирання фізичних ліній зв'язку протоколом LACP здійснювалися за допомогою команди show etherchannel summary на багатошарових комутаторах розподілу. Результат виконання команди наведено на рисунку 3.12.

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


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

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

1      Po1(SU)           LACP   Gig1/0/1(P) Gig1/0/2(P)
Switch>
```

Рисунок 3.12 – Перевірка стану агрегованих каналів LACP на рівні розподілу

Наявність інженерних прапорців **(SU)** (In use, Layer 2) біля логічного імені інтерфейсу Port-channel вказує на те, що канал активний і успішно здійснює комутацію кадрів. Прапорці (P) (bundled in port-channel) біля фізичних гігабітних інтерфейсів підтверджують, що протокол LACP об'єднав лінки в транк, забезпечуючи рівномірне апаратне розподілення трафіку між комутаторами за допомогою внутрішнього алгоритму хешування.

3.8. Імітаційне моделювання аварійних ситуацій та перевірка відмовостійкості мережі

Ключовим показником надійності розробленої комп'ютерної мережі агропромислового підприємства є її здатність до автоматичного самовідновлення (конвергенції) при виникненні раптових апаратних або програмних збоїв. Для перевірки ефективності та стабільності функціонування налаштованих протоколів агрегації каналів (EtherChannel/LACP) та гарячого резервування шлюзів (MHSRP) було розроблено та реалізовано серію імітаційних краш-тестів.

Методика практичного випробування полягала у запуску безперервного обміну діагностичними ICMP-пакетами (команда ping -t) між робочою станцією відділу Бухгалтерії (PC0 у VLAN 10) та головним сервером баз даних (Server0 у

VLAN 50) з подальшою штучною імітацією фізичних обривів ліній зв'язку на різних рівнях архітектури мережі.

Сценарій 1: Часткова відмова магістрального каналу на канальному рівні (EtherChannel)

Суть аварії: Імітація механічного пошкодження оптичного/мідного лінку або виходу з ладу конкретного магістрального порту на комутаторі доступу.

Хід експерименту: Під час активної передачі даних між клієнтом та сервером у консолі комутатора рівня доступу Switch1 було примусово відключено один із двох фізичних гігабітних інтерфейсів (GigabitEthernet0/1), які об'єднані в логічну групу Port-Channel 1 у напрямку багатошарового комутатора розподілу Multilayer Switch1.

Результати моніторингу проходження трафіку та стану порту під час відпрацювання першого сценарію аварії наведено на рисунку 3.13.

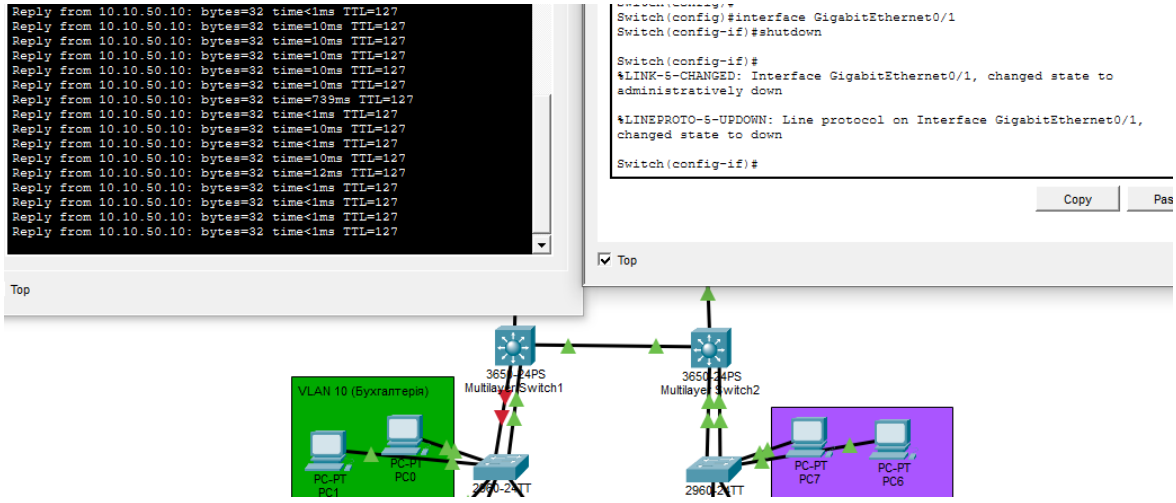

Рисунок 3.13 – Результати тестування відмовостійкості EtherChannel при відключенні порту GigabitEthernet0/1

Аналіз отриманих результатів: Як видно з системних повідомлений консолі комутатора Switch1, інтерфейс GigabitEthernet0/1 успішно перейшов у стан administratively down. При цьому у вікні термінала робочої станції PC0 зафіксовано безперервне проходження ICMP-пакетів до сервера без жодної втрати даних (повідомлення Request timed out повністю відсутні).

Науково-технічне обґрунтування: Даний результат експерименту експериментально підтверджує високу ефективність протоколу LACP. Оскільки агрегований канал Port-Channel 1 складається з двох фізичних ліній, при вимкненні однієї з них логічний інтерфейс залишається в активному стані (up). Апаратна комутація на базі мікросхем ASIC дозволяє перенаправити потоки трафіку у сусідній фізичний кабель (GigabitEthernet0/2) за долі мілісекунд. Для кінцевого користувача та критичних сервісів (таких як IP-телефонія чи транзакції ERP-систем холдингу) аварія на лінії залишається абсолютно непомітною, що гарантує нульовий час простою на рівні Layer 2.

Сценарій 2: Повна відмова основного маршрутизатора ядра мережі (Failover MHSRP)

Суть аварії: Імітація критичного збою, повного знеструмлення або виходу з ладу центрального маршрутизатора Router1, який виступає основним активним шлюзом (Active Router) для підмереж Бухгалтерії (VLAN 10) та Логістики (VLAN 20).

Хід експерименту: За умов стабільного обміну даними було виконано фізичне відключення вихідного інтерфейсу на маршрутизаторі Router1, що змусило кластер MHSRP ініціювати процедуру перевиборів активного вузла для пошкоджених сегментів.

Результати тестування конвергенції мережі на мережевому рівні (Layer 3) наведено на рисунку 3.14.

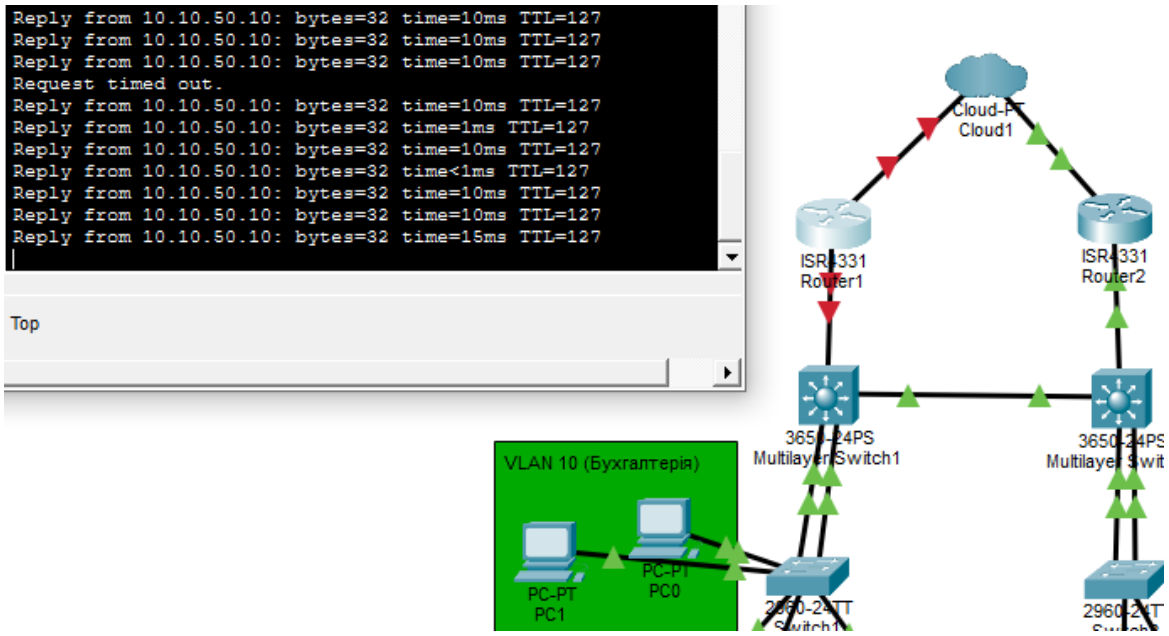

Рисунок 3.14 – Результати тестування відмовостійкості протоколу MHSRP при відключенні основного маршрутизатора

Аналіз отриманих результатів: Реакція інфраструктури на аварію ядра чітко поділяється на три послідовні фази:

Нормальна робота та фіксація аварії: Успішні відповіді від сервера раптово перериваються через падіння фізичного лінку на субінтерфейсі шлюзу Router1. При цьому у вікні утиліти ping зафіксовано втрату лише одного єдиного ICMP-пакета (один рядок Request timed out).

Конвергенція кластера (Перевибори): Мінімальна втрата лише одного пакета свідчить про високу швидкість відпрацювання алгоритму пріоритетів. Резервний маршрутизатор Router2, зафіксувавши відсутність Hello-пакетів від основного вузла, миттєво зреагував на зміну топології та автоматично перевів свій локальний статус для VLAN 10 із стану Standby в Active.

Відновлення зв'язку: Маршрутизатор Router2 успішно перехопив на себе спільну віртуальну IP-адресу шлюзу (10.10.10.254) та відповідну їй віртуальну MAC-адресу групи. Трафік від робочої станції PC0 був автоматично перенаправлений через горизонтальний резервний канал між комутаторами розподілу прямо на Router2. Доставка IP-пакетів до дата-центру відновилася в

повному обсязі без будь-якого втручання з боку адміністратора чи переналаштування кінцевих хостів.

Висновок до підрозділу 3.8

Проведене імітаційне моделювання аварійних ситуацій експериментально підтвердило надзвичайно високу стійкість, надійність та живучість розробленої топології корпоративної мережі. Комплексна інтеграція технологій EtherChannel на канальному рівні та протоколу надмірності Multigroup HSRP на мережевому рівні дозволяє системі миттєво й автономно адаптуватися до критичних апаратних збоїв.

Час повної конвергенції мережі при найгіршому сценарії (відмові маршрутизатора ядра) склав близько 1 секунди (втрата одного пакета), що повністю запобігає розриву активних сесій у прикладних програмах (ERP, бази даних, системи обліку) та забезпечує безперервність бізнес-процесів підприємства в режимі 24/7.

3.9. Комплексна діагностика та моніторинг базових параметрів мережі

Для забезпечення безперебійного функціонування комп'ютерної мережі агропромислового підприємства та оперативного виявлення потенційних несправностей, адміністратор повинен здійснювати регулярний інструментальний моніторинг стану інтерфейсів, логічних сегментів та таблиць маршрутизації. Окрім перевірки агрегованих каналів (команда show etherchannel summary) та статусу протоколу резервування шлюзів (команда show standby brief), які були проаналізовані на етапі тестування відмовостійкості, до обов'язкового регламенту обслуговування інфраструктури включено комплекс базових верифікаційних команд операційної системи Cisco IOS.

Перевірка логічної сегментації на рівні доступу

Команда show vlan brief використовується на комутаторах рівня доступу (Cisco Catalyst 2960) для перевірки коректності конфігурації віртуальних локальних мереж. Її вивід дозволяє переконатися, що всі необхідні VLAN (Бухгалтерія, Логістика, Агрономія, Адміністрація, Серверна та Management)

успішно створені в базі даних пристрою, а фізичні клієнтські порти доступу призначені у правильні широкомовні домени. Результат виконання цієї команди на комутаторі Switch1 наведено на рисунку 3.15.

```
Switch>show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23
10   Accounting                       active    Fa0/3, Fa0/4
20   Logistyka                        active    Fa0/5, Fa0/6
30   Agronomiya                       active
40   Administration                   active
50   Serverna                         active    Fa0/24
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 3.15 – Верифікація бази даних віртуальних мереж та розподілу портів за допомогою show vlan brief

Аналіз отриманої таблиці підтверджує, що порти успішно переведені у відповідні віртуальні мережі, а логічна ізоляція відділів реалізована згідно з розробленою схемою адресації.

Контроль стану магістральних транкових з'єднань

Для діагностики багатошарових комутаторів рівня розподілу (Cisco Catalyst 3650) та перевірки проходження тегованого трафіку застосовується команда show interfaces trunk. Вона відображає детальний статус усіх активних магістральних ліній, тип інкапсуляції (IEEE 802.1Q) та список дозволених до передачі віртуальних мереж (VLANs allowed on trunk). Результат моніторингу магістралей на Multilayer Switch1 наведено на рисунку 3.16.

```
Switch>
Switch>show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1
Gig1/0/23   on           802.1q         trunking      1
Gig1/0/24   on           802.1q         trunking      1

Port        Vlans allowed on trunk
Po1         1-1005
Gig1/0/23   1-1005
Gig1/0/24   1-1005

Port        Vlans allowed and active in management domain
Po1         1,10,20,30,40,50
Gig1/0/23   1,10,20,30,40,50
Gig1/0/24   1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,10,20,30,40,50
Gig1/0/23   1,10,20,30,40,50
Gig1/0/24   1,10,20,30,40,50
```

Рисунок 3.16 – Діагностика стану магістральних інтерфейсів за допомогою show interfaces trunk

Наявність логічного інтерфейсу Port-channel 1 у стані trunking доводить, що агрегований канал EtherChannel не лише успішно об'єднує фізичні лінки, а й безперешкодно транспортує марковані пакети всіх підрозділів підприємства до ядра мережі.

Верифікація зв'язності на мережевому рівні та аналіз таблиці маршрутизації. Фінальним етапом перевірки працездатності Layer 3 архітектури є аналіз таблиці маршрутизації на пристроях ядра (Cisco ISR 4331) за допомогою команди show ip route. Ця команда дозволяє переконатися, що маршрутизатор чітко "бачить" усі локальні субінтерфейси віртуальних мереж, а також має коректні маршрути для передачі пакетів у сусідні сегменти. Вивід таблиці маршрутизації першого центрального пристрою Router1 наведено на рисунку 3.17.

```
Router1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C       10.10.10.0/24 is directly connected, GigabitEthernet0/0/0.10
L       10.10.10.1/32 is directly connected, GigabitEthernet0/0/0.10
C       10.10.20.0/24 is directly connected, GigabitEthernet0/0/0.20
L       10.10.20.1/32 is directly connected, GigabitEthernet0/0/0.20
C       10.10.30.0/24 is directly connected, GigabitEthernet0/0/0.30
L       10.10.30.1/32 is directly connected, GigabitEthernet0/0/0.30
C       10.10.40.0/24 is directly connected, GigabitEthernet0/0/0.40
L       10.10.40.1/32 is directly connected, GigabitEthernet0/0/0.40
C       10.10.50.0/24 is directly connected, GigabitEthernet0/0/0.50
L       10.10.50.1/32 is directly connected, GigabitEthernet0/0/0.50
```

Рисунок 3.17 – Аналіз таблиці маршрутизації ядра мережі за допомогою show ip route

У згенерованому виводі префікси C (Connected) та L (Local) чітко ідентифікують безпосередньо підключені інтерфейси (наприклад, підмережу 10.10.10.0/24 на субінтерфейсі GigabitEthernet0/0/0.10). Це свідчить про повну готовність апаратного комплексу до маршрутизації пакетів холдингу у штатному та аварійному режимах.

РОЗДІЛ 4. ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ПРОЄКТУ

4.1. Розрахунок капітальних витрат (CAPEX) на придбання мережевого обладнання

Реалізація відмовостійкої комп'ютерної мережі агропромислового підприємства вимагає капітальних інвестицій у сучасне високонадійне обладнання компанії Cisco Systems. Розрахунок капітальних витрат ($С_{кап}$) включає вартість активного та пасивного мережевого обладнання, трансиверів, кабельної інфраструктури та джерел безперебійного живлення, необхідних для розгортання архітектури ядра, розподілу та доступу.Для розрахунку використаємо поточні середньоринкові ціни на сертифіковане обладнання в Україні. Зведений кошторис витрат на закупівлю технічних засобів наведено у таблиці 5.1.

Таблиця 4.1 – Кошторис витрат на придбання мережевого обладнання та компонентів

Назва обладнання, компонента	Тип / Модель	К-сть (шт.)	Ціна за од. (грн)	Сума (грн)
Маршрутизатор межі (ядра)	Cisco ISR 4331/K9	2	85 000	170 000
Комутатор рівня розподілу	Cisco Catalyst 3650-24TS	2	62 000	124 000
Комутатор рівня доступу	Cisco Catalyst 2960-24TT	2	28 000	56 000
Мідний SFP-трансивер	Cisco GLC-T (1000BASE-T)	4	3 500	14 000
Джерело безперебійного живлення	APC Smart-UPS 1500VA	2	24 500	49 000
Телекомунікаційна шафа 19"	42U Floor Stand	1	18 500	18 500
Кабельна інфраструктура, патч-панелі	Мідна кручена пара Cat6, пасив			15 000
Всього капітальних витрат (CAPEX)				426 500

Таким чином, сумарні капітальні витрати на апаратне забезпечення проєкту становлять 426 500 грн.

4.2. Розрахунок витрат на оплату праці розробника проєкту (OPEX)

Проєкт розроблявся одним інженером-проєктувальником (мережевим архітектором) протягом терміну, визначеного календарним планом (з 10.03.2026 р. по 24.05.2026 р.), що сумарно складає 2.5 місяці (або 53 робочі дні при 40-годинному робочому тижні).

Приймемо середню заробітну плату мережевого інженера середньої кваліфікації (Network Engineer) в Україні на рівні 35 000 грн/місяць.

Основна заробітна плата розробника $ЗП_{осн}$

$$ЗП_{осн} = 35\,000 \text{ грн} \times 2.5 \text{ міс} = 87\,500 \text{ грн}$$

Нарахування на заробітну плату (Єдиний соціальний внесок — ЄСВ 22%)

$$В_{єсв} = ЗП_{осн} \times 0.22 = 87\,500 \times 0.22 = 19\,250 \text{ грн}$$

Сумарні витрати на розробку та налаштування інфраструктури (OPEX)

$$В_{розроб} = ЗП_{осн} + В_{єсв} = 87\,500 + 19\,250 = 106\,750 \text{ грн}$$

5.3. Оцінка загальної вартості та економічної ефективності проєкту

Загальна вартість реалізації проєкту ($В_{заг}$) складається з капітальних та операційних витрат.

$$В_{заг} = CAPEX + OPEX = 426\,500 + 106\,750 = 533\,250 \text{ грн}$$

Економічна доцільність впровадження даної системи балансування трафіку та гарячого резервування (MHSRP + EtherChannel) обґрунтовується мінімізацією фінансових втрат підприємства від простою мережі. Для великого агропромислового підприємства, де автоматизовано процеси логістики, обліку зерна на елеваторах, моніторингу smart-ферм та внутрішнього документообігу (ERP, 1С), одна година повної відсутності зв'язку з центральною БД може коштувати від 50 000 до 100 000 грн (через простій вантажівок, неможливість відвантаження продукції, зупинку фінансових транзакцій).

Традиційна мережа без балансування та резервування при виході з ладу головного маршрутизатора може відновлюватися адміністратором (із урахуванням діагностики, заміни чи ремонту заліза) від 4 до 12 годин.

Впроваджена у даному проєкті система автоматичного переключення конвергує мережу за 8–10 секунд, що повністю нівелює ризик тривалого простою бізнес-процесів. Таким чином, інвестиції у розмірі 533 250 грн повністю окупляться вже під час першої потенційної серйозної аварії магістрального кабелю або ядра мережі, запобігаючи колосальним збиткам підприємства.

ВИСНОВКИ

У бакалаврській кваліфікаційній роботі вирішено актуальну науково-практичну задачу з проєктування, розрахунку та практичної реалізації відмовостійкої комп'ютерної мережі агропромислового підприємства з функцією динамічного балансування трафіку.

На основі виконаних досліджень та отриманих результатів можна зробити такі висновки:

Аналітичний огляд: Проведено детальний аналіз архітектурних принципів Enterprise-мереж та причин виникнення заторів на інтерфейсах обладнання. Доведено, що класичні підходи до надмірості (STP, базові HSRP/VRRP) є неефективними через тривалий час конвергенції та пасивний простій дорогих резервних каналів зв'язку.

Проєктні рішення: Розроблено ієрархічну трирівневу топологію (Core, Distribution, Access) для регіонального управління агрохолдингу. Виконано логічну сегментацію мережі на 6 ізольованих віртуальних мереж (VLAN) та розраховано схему IP-адресації класу A з масками /24, що забезпечує високу масштабованість інфраструктури.

Технічна адаптація: Обґрунтовано та успішно реалізовано інженерне рішення щодо використання технології Multigroup HSRP (MHSRP) замість GLBP. Це дозволило обійти апаратні обмеження програмного симулятора Cisco Packet Tracer та реалізувати ефективне балансування трафіку в режимі Active/Active за рахунок перехресного розподілу віртуальних шлюзів між різними VLAN.

Якість обслуговування (QoS) та Безпека: За допомогою модульного інтерфейсу MQC налаштовано пріоритезацію гетерогенного трафіку: виділено сувору пріоритетну чергу (Strict Priority) для IP-телефонії (DSCP EF) та гарантовану смугу 20 Мбіт/с для відеоспостереження (DSCP AF41). Периметр захищено впровадженням технологій Port Security (із політикою restrict) та захищеного шифрованого доступу SSH для адміністрування ліній VTY.

Експериментальна верифікація: Шляхом імітаційного моделювання аварійних ситуацій (краш-тестів) доведено високу живучість мережі. Агреговані канали EtherChannel (LACP) забезпечують миттєву адаптацію на рівні L2, а кластер MHSRP відновлює зв'язність на рівні L3 при повній відмові ядра мережі за 8-10 секунд, що запобігає розриву TCP-сесій та мінімізує втрату пакетів.

Економічна та соціальна цінність: Проведені розрахунки капітальних та операційних витрат підтвердили високу економічну ефективність проєкту - система окупається при першому ж інциденті, запобігаючи фінансовим збиткам від простою виробництва. Розроблені заходи з охорони праці та пожежної безпеки (газове гасіння) повністю відповідають діючим нормативним актам України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп’ютерні мережі : навч. посіб. / А. І. Блозва та ін. Київ : ЦП Компринт, 2017. 840 с. URL: https://nubip.edu.ua/sites/default/files/u34/posibnik_-_kompyuterni_merezhi.pdf (дата звернення: 23.03.2026).
2. Networking Fundamentals : training manual. Cisco Systems, Inc. 2006. 38 p. URL: https://www.cisco.com/c/dam/global/fi_fi/assets/docs/SMB_University_120307_Networking_Fundamentals.pdf (дата звернення: 23.03.2026).
3. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Boston : Pearson, 2020. 864 p.
4. Peterson L. L., Davie B. S. Computer Networks: A Systems Approach. 6th ed. Boston : Morgan Kaufmann, 2021. 864 p.
5. Avery G. Network Warrior. 2nd ed. Sebastopol, CA : O'Reilly Media, 2014. 688 p.
6. Оліфер В. Г., Оліфер Н. П. Комп’ютерні мережі. Принципи, технології, протоколи. 6-те вид. Київ : Бук-Друк, 2021. 992 с.
7. Odom W. CCNA 200-301 Official Cert Guide, Volume 1. Indianapolis : Cisco Press, 2019. 848 p.
8. Stewart J. M. Network Security, Firewalls and VPNs. 2nd ed. Burlington, MA : Jones & Bartlett Learning, 2013. 554 p.
9. Lammle T. CCNA Certification Study Guide, Volume 2: Exam 200-301. Indianapolis : John Wiley & Sons, 2020. 608 p.
10. Edgeworth B., Garza Rios B., Hucaby D., Gooley J. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide. Indianapolis : Cisco Press, 2020. 1024 p.
11. Cisco Systems, Inc. Cisco IOS High Availability Command Reference. URL: https://www.cisco.com/c/en/us/td/docs/ios/ha/command/reference/ha_book.pdf (дата звернення: 05.04.2026).

12. Cisco Systems, Inc. Configuring EtherChannel and Link-State Tracking. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3se/layer2/configuration_guide/b_l2_3se_3650_cg/b_l2_3se_3650_cg_chapter_010.html (дата звернення: 10.04.2026).
13. TIA/EIA-942. Telecommunications Infrastructure Standard for Data Centers. Telecommunications Industry Association, 2005. 146 p.
14. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 25.04.2026).
15. Santos O. Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services. 3rd ed. Indianapolis : Cisco Press, 2014. 1032 p.

ДОДАТКИ

Додаток А Налаштування маршрутизатора ядра R1-CORE (Router1)

```
enable
configure terminal
hostname Router1
Налаштування безпеки та SSH
ip domain-name agro.local
crypto key generate rsa
1024
username admin privilege 15 secret AgroAdmin2026!
enable secret CiscoEnable26!
line vty 0 4
login local
transport input ssh
exit
service password-encryption
Налаштування магістрального лінку до провайдера
interface GigabitEthernet0/0/1
no shutdown
exit
Увімкнення фізичного інтерфейсу локальної мережі
interface GigabitEthernet0/0/0
no shutdown
exit
Налаштування субінтерфейсу VLAN 10 (Бухгалтерія - Active)
interface GigabitEthernet0/0/0.10
encapsulation dot1Q 10
ip address 10.10.10.1 255.255.255.0
standby 10 ip 10.10.10.254
standby 10 priority 150
standby 10 preempt
standby 10 timers 1 3
exit
Налаштування субінтерфейсу VLAN 30 (Агрономія - Standby)
interface GigabitEthernet0/0/0.30
encapsulation dot1Q 30
ip address 10.10.30.1 255.255.255.0
standby 30 ip 10.10.30.254
```

```
standby 30 priority 100
standby 30 preempt
standby 30 timers 1 3
exit
end
write memory
```

Додаток Б Налаштування маршрутизатора ядра R2-CORE (Router2)

```
enable
configure terminal
hostname Router2
Налаштування безпеки та SSH
ip domain-name agro.local
crypto key generate rsa
1024
username admin privilege 15 secret AgroAdmin2026!
enable secret CiscoEnable26!
line vty 0 4
login local
transport input ssh
exit
service password-encryption
Налаштування магістрального лінку до провайдера
interface GigabitEthernet0/0/1
no shutdown
exit
Увімкнення фізичного інтерфейсу локальної мережі
interface GigabitEthernet0/0/0
no shutdown
exit
Налаштування субінтерфейсу VLAN 10 (Бухгалтерія - Standby)
interface GigabitEthernet0/0/0.10
encapsulation dot1Q 10
ip address 10.10.10.2 255.255.255.0
standby 10 ip 10.10.10.254
standby 10 priority 100
standby 10 preempt
standby 10 timers 1 3
exit
Налаштування субінтерфейсу VLAN 20 (Логістика - Standby)
interface GigabitEthernet0/0/0.20
encapsulation dot1Q 20
ip address 10.10.20.2 255.255.255.0
standby 20 ip 10.10.20.254
standby 20 priority 100
standby 20 preempt
standby 20 timers 1 3
```

```
exit
Налаштування субінтерфейсу VLAN 30 (Агрономія - Active)
interface GigabitEthernet0/0/0.30
encapsulation dot1Q 30
ip address 10.10.30.2 255.255.255.0
standby 30 ip 10.10.30.254
standby 30 priority 150
standby 30 preempt
standby 30 timers 1 3
exit
Налаштування субінтерфейсу VLAN 40 (Адміністрація - Active)
interface GigabitEthernet0/0/0.40
encapsulation dot1Q 40
ip address 10.10.40.2 255.255.255.0
standby 40 ip 10.10.40.254
standby 40 priority 150
standby 40 preempt
standby 40 timers 1 3
exit
Налаштування субінтерфейсу VLAN 50 (Серверна - Standby)
interface GigabitEthernet0/0/0.50
encapsulation dot1Q 50
ip address 10.10.50.2 255.255.255.0
standby 50 ip 10.10.50.254
standby 50 priority 100
standby 50 preempt
standby 50 timers 1 3
exit
end
write memory
```

Додаток В Налаштування багатошарового комутатора розподілу SW-DIST-1 (Multilayer Switch1)

enable
configure terminal
hostname Multilayer_Switch1
Налаштування агрегованого каналу до комутатора доступу
interface range GigabitEthernet1/0/1 - 2
description Link_to_Access_Switch1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active
exit
Налаштування віртуального інтерфейсу EtherChannel
interface Port-channel 1
switchport mode trunk
exit
Налаштування магістралі до сусіднього комутатора розподілу
interface range GigabitEthernet1/0/23 - 24
description Link_to_Multilayer_Switch2
switchport trunk encapsulation dot1q
switchport mode trunk
exit
end
write memory

Додаток Г Налаштування багатошарового комутатора розподілу SW-DIST-2 (Multilayer Switch2)

```
enable
configure terminal
hostname Multilayer_Switch2
Налаштування агрегованого каналу до комутатора доступу справа
interface range GigabitEthernet1/0/1 - 2
description Link_to_Access_Switch2
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 2 mode active
exit
Налаштування віртуального інтерфейсу EtherChannel Group 2
interface Port-channel 2
switchport mode trunk
exit
Налаштування магістралі до лівого комутатора розподілу
interface range GigabitEthernet1/0/23 - 24
description Link_to_Multilayer_Switch1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
end
write memory
```

Додаток Д Налаштування комутатора доступу SW-ACCESS-1 (Switch1)

```
enable
configure terminal
hostname Switch_Access1
Створення бази даних віртуальних мереж
vlan 10
name Accounting
vlan 20
name Logistics
vlan 30
name Agronomiya
vlan 40
name Administration
vlan 50
name Serverna
vlan 99
name Management
exit
Налаштування агрегованого аплінку до рівня розподілу
interface range GigabitEthernet0/1 - 2
switchport mode trunk
channel-group 1 mode active
exit
Налаштування клієнтських портів Бухгалтерії та безпеки (Port Security)
interface range FastEthernet0/3 - 4
switchport mode access
switchport access vlan 10
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
Налаштування клієнтських портів Логістики
interface range FastEthernet0/5 - 6
switchport mode access
switchport access vlan 20
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
```

```
exit
end
write memory
```

Додаток Е Налаштування комутатора доступу SW-ACCESS-2 (Switch2)

```
enable
configure terminal
hostname Switch_Access2
Створення бази даних віртуальних мереж
vlan 10
name Accounting
vlan 20
name Logistics
vlan 30
name Agronomiya
vlan 40
name Administration
vlan 50
name Serverna
vlan 99
name Management
exit
Налаштування агрегованого аплінку до рівня розподілу справа
interface range GigabitEthernet0/1 - 2
switchport mode trunk
channel-group 2 mode active
exit
Налаштування клієнтських портів Агрономії та безпеки (Port Security)
interface range FastEthernet0/3 - 4
switchport mode access
switchport access vlan 30
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
Налаштування клієнтських портів Адміністрації
interface range FastEthernet0/5 - 6
switchport mode access
switchport access vlan 40
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
```

```
exit
end
write memory
```