МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

Порівняльний аналіз протоколів маршрутизації в комп'ютерних мережах OSPF, EIGRP та BGP

Виконав: студент групи 1К-21
Спеціальності 123 Комп’ютерна інженерія
Ростислав ХЛІВЕНКО
Керівник:
Павло РАТАЙЧУК

Черкаси 2025

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп'ютерної інженерії та інформаційних технологій
(повна назва випускової кафедри)

Спеціальність 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

Освітня програма «Комп'ютерна інженерія»
(назва освітньої програми)

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії та
інформаційних технологій
(назва кафедри)
Хотунов В.І.
(підпис) (ПІБ)
«_____» _____ 2025 р.

З А В Д А Н Н Я

НА ВИПУСКНУ РОБОТУ СТУДЕНТУ

Хлівенку Ростиславу Андрійовичу
(прізвище, ім'я, по батькові студента)

1. Тема випускної роботи Порівняльний аналіз протоколів маршрутизації в комп'ютерних мережах OSPF, EIGRP та BGP
2. Науковий керівник роботи
   Ратайчук Павло Єгорович, викладач методист
   (прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від ―" 7 " жовтня 2024 року № 68У.

3. Строк подання студентом випускної роботи 02.06.2025
4. Вихідні дані до випускної роботи Здійснити порівняльний аналіз протоколів маршрутизації OSPF, EIGRP та BGP на основі їхньої продуктивності, масштабованості, ефективності використання ресурсів і адаптивності до змін у мережі.
5. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити) Вивчити теоретичні основи маршрутизації та класифікацію протоколів, розглянути принципи роботи OSPF, EIGRP та BGP, проаналізувати ключові параметри порівняння: алгоритми маршрутизації, конвергенція, масштабованість, надійність та відмовостійкість, використання ресурсів, Провести моделювання мережі з використанням кожного з протоколів (у Cisco Packet Tracer, GNS3 або EVE-NG). Оцінити ефективність роботи протоколів у різних умовах (динамічна зміна топології, затримки тощо), надати рекомендації щодо вибору протоколу в залежності від типу мережі.
6. Дата видачі завдання 16.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання з підписами керівника і студента
1	Вступ	14.10.2024	
2	Розділ 1 (ТЕОРЕТИЧНІ ОСНОВИ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ)	9.12.2024	
3	Розділ 2 (ОГЛЯД ПРОТОКОЛІВ OSPF, EIGRP, BGP)	10.03.2025	
4	Розділ 3 (ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ OSPF, EIGRP ТА BGP)	28.04.2025	
5	Висновки	12.05.2025	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2025	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2025	
8	Подання кваліфікаційної роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	10.06.2025	

Студент _____ Хлівенко Р.А.
(підпис) (прізвище та ініціали)

Науковий керівник роботи _____ Ратайчук П.Є.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

З розвитком інформаційних технологій та зростанням складності мережевих інфраструктур виникає необхідність у використанні ефективних механізмів маршрутизації, які забезпечують стабільну та безпечну передачу даних. У даній роботі здійснено детальний аналіз трьох основних протоколів маршрутизації: OSPF, EIGRP і BGP, які відіграють ключову роль у функціонуванні сучасних комп'ютерних мереж.

Досліджено архітектуру, принципи роботи та алгоритми кожного з цих протоколів, а також їхні особливості у різних мережевих середовищах. Проведено порівняння за основними параметрами, такими як швидкість конвергенції, масштабованість, використання ресурсів, безпека та відмовостійкість. Окремо розглянуто питання продуктивності та оптимізації маршрутизації залежно від мережевих вимог та навантаження.

У роботі також досліджено практичні аспекти впровадження та налаштування кожного з протоколів, їхню сумісність з існуючими мережевими технологіями та перспективи розвитку. Проведено аналіз типових сценаріїв використання OSPF, EIGRP та BGP у локальних, корпоративних і глобальних мережах.

На основі отриманих результатів сформульовано рекомендації щодо вибору оптимального протоколу маршрутизації відповідно до конкретних потреб організацій, їхніх технічних можливостей та вимог до продуктивності мережі.

ABSTRACT

With the advancement of information technologies and the increasing complexity of network infrastructures, the need for effective routing mechanisms that ensure stable and secure data transmission has become more critical. This study conducts a detailed analysis of three fundamental routing protocols: OSPF, EIGRP, and BGP, which play a crucial role in the functioning of modern computer networks.

The research explores the architecture, operational principles, and algorithms of each of these protocols, as well as their distinct characteristics in various network environments. A comparative analysis is performed based on key parameters such as convergence speed, scalability, resource utilization, security, and fault tolerance. Special attention is given to performance-related aspects and the optimization of routing processes depending on network requirements and traffic load.

Furthermore, this study examines the practical aspects of implementing and configuring each protocol, their compatibility with existing networking technologies, and their future prospects. An in-depth analysis of common use cases for OSPF, EIGRP, and BGP is provided, covering their application in local, corporate, and global networks.

Based on the findings of this research, recommendations are developed for selecting the most suitable routing protocol according to the specific needs of organizations, their technical capabilities, and network performance requirements.

ЗМІСТ

ВСТУП

Актуальність обраної теми. У сучасному світі, де обсяг трафіку в комп'ютерних мережах стрімко зростає, ефективність маршрутизації відіграє ключову роль у забезпеченні стабільного та безперебійного функціонування мережевих інфраструктур. Вибір оптимального протоколу маршрутизації має значний вплив на продуктивність, безпеку та масштабованість мережі. OSPF, EIGRP та BGP є найбільш поширеними протоколами, кожен із яких має свої особливості, переваги та сфери застосування. Аналіз їхньої ефективності допоможе визначити найкращий варіант для конкретних мережевих середовищ.

Об’єкт дослідження. Центральним елементом дослідження є процес маршрутизації в комп'ютерних мережах, а саме робота та взаємодія протоколів OSPF, EIGRP і BGP. Вивчається їхня ефективність у різних типах мереж, а також їхній вплив на продуктивність і стабільність мережевого середовища.

Предмет дослідження. Робота зосереджена на методах та підходах до використання OSPF, EIGRP і BGP у сучасних мережах. Досліджуються їхні основні алгоритми роботи, особливості впровадження, продуктивність, переваги та недоліки, а також доцільність застосування в локальних, корпоративних та глобальних мережах.

Мета дослідження. Метою роботи є аналіз та порівняння протоколів маршрутизації OSPF, EIGRP і BGP з урахуванням таких параметрів, як швидкість

конвергенції, масштабованість, використання ресурсів, рівень безпеки та стійкість до збоїв. На основі цього аналізу буде розроблено рекомендації щодо вибору оптимального протоколу залежно від потреб і технічних можливостей мережевої інфраструктури.

Завдання дослідження. Для досягнення поставленої мети необхідно вирішити такі завдання:

провести огляд сучасних досліджень, особливостей та принципів роботи протоколів OSPF, EIGRP і BGP;

визначити ключові параметри, за якими слід оцінювати ефективність протоколів маршрутизації;

проаналізувати їхню продуктивність у різних мережевих умовах;

розглянути переваги та недоліки кожного протоколу в контексті локальних, корпоративних та глобальних мереж;

сформулювати рекомендації щодо вибору та впровадження оптимального протоколу маршрутизації відповідно до конкретних мережевих потреб.

РОЗДІЛ І
ОСНОВИ МАРШРУТИЗАЦІЇ ТА АНАЛІЗ ПРОТОКОЛІВ

1.1 Основні поняття та принципи маршрутизації

Маршрутизація – це фундаментальний процес у комп'ютерних мережах, що забезпечує передавання даних між пристроями через проміжні вузли. Вона визначає найефективніший шлях для пакета даних, враховуючи різні характеристики мережі, такі як затримка, пропускна здатність, завантаженість каналів та відмовостійкість. Без маршрутизації ефективна передача даних у великих, складних мережах була б неможливою, оскільки пристрої не змогли б коректно взаємодіяти між собою, а трафік не знаходив би свого призначення. Маршрутизація є основою для функціонування Інтернету та будь-якої іншої глобальної чи корпоративної мережі. Вона є невід'ємною частиною мережевого рівня (Layer 3) моделі OSI та забезпечує логічну адресацію та пересилання даних.

Основні принципи маршрутизації, які забезпечують її функціональність, включають:

Адресація – кожен пристрій у мережі має унікальну IP-адресу, яка використовується для ідентифікації джерела та отримувача даних. Це дозволяє забезпечити точність і коректність маршрутизації, оскільки маршрутизатор знає, куди саме потрібно доставити пакет. IP-адреси є основою для побудови таблиць маршрутизації та визначення шляху, що дозволяє унікально ідентифікувати кожен вузол у мережі.

Обмін маршрутною інформацією – маршрутизатори взаємодіють між собою, обмінюючись інформацією про доступні маршрути та оновлюючи свої таблиці маршрутизації. Цей процес відбувається за допомогою спеціальних протоколів маршрутизації, які дозволяють мережі залишатися динамічною і оперативно адаптуватися до змін, таких як додавання нових пристроїв, відмова зв'язків або зміна параметрів мережі. Постійний обмін

інформацією забезпечує актуальність даних про топологію мережі та дозволяє маршрутизаторам мати повне уявлення про доступні шляхи до різних мережевих сегментів.

Прийняття рішень – на основі зібраної маршрутної інформації, що міститься в таблиці маршрутизації, маршрутизатор обирає оптимальний шлях для передачі пакета. Це рішення приймається за допомогою складних алгоритмів, які можуть враховувати різні метрики, такі як кількість переходів (хопів), затримка, пропускна здатність, вартість з'єднання або навіть політичні уподобання адміністратора. Метою є вибір найкоротшого, найшвидшого або найменш завантаженого шляху для ефективної доставки даних. Цей процес є центральним для функціонування маршрутизації.

Пересилання пакетів – після визначення оптимального маршруту дані передаються через відповідні вихідні інтерфейси маршрутизатора до наступного вузла на шляху до пункту призначення. Цей процес відбувається на мережевому рівні (рівень 3 моделі OSI) і дозволяє ефективно керувати потоком інформації через мережу, забезпечуючи її доставку до кінцевого адресата. Пересилання пакетів включає інкапсуляцію даних у фрейми канального рівня та направлення їх до відповідного фізичного інтерфейсу.

Конвергенція – це критично важлива здатність мережі адаптуватися до змін у топології (наприклад, збою лінії зв'язку або додавання нового маршрутизатора), автоматично оновлюючи маршрути та забезпечуючи безперебійне з'єднання. Час конвергенції є ключовим фактором у забезпеченні стабільної роботи мережі, оскільки чим швидше мережа конвергується, тим менший час простою та переривання сервісів. Це особливо важливо для додатків, чутливих до затримок, таких як VoIP та відеоконференції.

Балансування навантаження – це стратегія рівномірного розподілу трафіку між декількома можливими маршрутами до одного пункту призначення. Це дозволяє підвищити ефективність використання доступних мережевих ресурсів, розподіляючи навантаження між різними каналами або

маршрутизаторами, що особливо важливо для великих корпоративних мереж, де висока пропускна здатність є пріоритетом. Балансування навантаження може бути реалізовано як по рівновеликих, так і по нерівновеликих шляхах, залежно від можливостей протоколу маршрутизації.

Крім зазначених принципів, важливим аспектом маршрутизації є також надійність. Мережа повинна бути здатною функціонувати навіть у разі відмови окремих вузлів, таких як маршрутизатори, або каналів зв'язку. Це досягається за рахунок надмірності маршрутів (наявності альтернативних шляхів) та механізмів швидкого перемикання на ці альтернативні шляхи у разі збою основного. Ще одним ключовим аспектом є безпека маршрутизації. Несанкціоноване втручання в маршрутну інформацію може призвести до серйозних наслідків, таких як перехоплення даних, відмова в обслуговуванні (DoS-атаки), створення маршрутних петель, які паралізують мережу, або перенаправлення трафіку на шкідливі ресурси. Тому протоколи маршрутизації повинні мати вбудовані механізми автентифікації, шифрування та захисту даних, щоб забезпечити цілісність та конфіденційність маршрутної інформації.

1.2 Класифікація протоколів маршрутизації

Протоколи маршрутизації класифікуються за кількома основними критеріями, що дозволяє краще зрозуміти їхні особливості та сфери застосування.

За способом конфігурування:

Статична маршрутизація – це метод, при якому маршрути задаються адміністратором вручну і не змінюються автоматично. Цей підхід підходить для невеликих, стабільних мереж з простою топологією, де зміни відбуваються рідко. Переваги статичної маршрутизації включають простоту реалізації та низьке споживання ресурсів, оскільки маршрутизаторам не потрібно обмінюватися маршрутною інформацією. Проте, її головним

недоліком є відсутність адаптивності до змін у мережі – будь-який збій або зміна вимагає ручної переконфігурації, що може бути надзвичайно трудомістким у великих мережах і призвести до тривалого простою.

Динамічна маршрутизація – це підхід, при якому маршрутизатори автоматично обмінюються маршрутною інформацією один з одним, дозволяючи мережі адаптуватися до змін у топології в режимі реального часу. Цей метод широко використовується у великих та складних мережах для забезпечення швидкої адаптації до відмов обладнання, додавання нових сегментів або зміни завантаженості каналів. Динамічна маршрутизація значно більш гнучка і масштабована порівняно зі статичною, але вимагає більших обчислювальних ресурсів маршрутизаторів для обробки маршрутної інформації та може бути складнішою в налаштуванні та усуненні несправностей. Протоколи динамічної маршрутизації здатні самостійно виявляти маршрути та оновлювати їх у разі зміни мережевих умов.

За областю дії:

Внутрішні протоколи (IGP – Interior Gateway Protocols) – це протоколи, які працюють у межах однієї автономної системи (AS). Автономна система – це група маршрутизаторів, що знаходяться під єдиним адміністративним контролем (наприклад, мережа компанії або інтернет-провайдера). IGP відповідають за обмін маршрутною інформацією між маршрутизаторами, що належать до однієї адміністративної доменної області, дозволяючи оптимізувати внутрішню маршрутизацію та забезпечувати ефективне доставлення трафіку в межах AS. Прикладами IGP є OSPF, EIGRP, RIP. Вони призначені для швидкої конвергенції та ефективного використання внутрішніх мережевих ресурсів.

Зовнішні протоколи (EGP – Exterior Gateway Protocols) – це протоколи, які використовуються для обміну маршрутами між різними автономними системами. EGP є ключовим компонентом Інтернету, оскільки вони забезпечують зв'язок між незалежними мережами та провайдерами Інтернету по всьому світу. Найвідомішим та фактично єдиним широко

використовуваним EGP є BGP. EGP орієнтовані на політики маршрутизації та стабільність, а не на швидкість конвергенції, оскільки вони працюють у глобальному масштабі.

За алгоритмом роботи:

Протоколи з вектором відстані (Distance-Vector Protocols) – ці протоколи обмінюються інформацією про маршрути на основі "вектора відстані", який зазвичай представляє собою кількість проміжних вузлів (хопів) до цільової мережі. Кожен маршрутизатор повідомляє своїм сусідам про маршрути, які йому відомі, та їхні відстані. Сусідні маршрутизатори, у свою чергу, додають власну "відстань" (наприклад, один хоп) до отриманої інформації та передають її далі. Прикладом є EIGRP (хоча він має гібридні властивості) та RIP. Такі протоколи використовують простий підхід, але можуть мати проблеми з масштабованістю, утворенням маршрутних петель (особливо в умовах повільної конвергенції) та повільною конвергенцією у великих мережах, що може призвести до "рахунку до нескінченності" (count-to-infinity problem).

Протоколи стану каналу (Link-State Protocols) – ці протоколи працюють за іншим принципом. Кожен маршрутизатор у мережі, що використовує протокол стану каналу, створює "базу даних стану каналів" (Link State Database, LSDB), яка є повною топологічною картою мережі. Маршрутизатори обмінюються інформацією про свої безпосередні з'єднання (стан каналу), а не про повні маршрути. Отримавши інформацію від усіх сусідів, кожен маршрутизатор може самостійно побудувати повну картину топології мережі і за допомогою алгоритму Дейкстри (SPF - Shortest Path First) розрахувати найкоротші шляхи до всіх пунктів призначення. Ці протоколи забезпечують більш точне визначення оптимального маршруту, швидку конвергенцію та кращу масштабованість, оскільки кожен маршрутизатор має повну картину топології мережі і може швидко адаптуватися до змін, що є їхньою значною перевагою над протоколами вектора відстані.

1.3 Загальна характеристика OSPF, EIGRP та BGP

Детальний розгляд основних характеристик трьох найбільш поширених протоколів маршрутизації допоможе краще зрозуміти їхнє місце у мережевій архітектурі.

OSPF (Open Shortest Path First) – це стандартний протокол стану каналу (link-state), який використовує алгоритм Дейкстри для динамічного визначення найкоротшого шляху. OSPF підтримує багатозонну маршрутизацію (multi-area routing), що дозволяє розділяти великі мережі на менші, керовані області, значно підвищуючи його масштабованість та ефективність використання ресурсів. Протокол швидко адаптується до змін у мережі, оскільки маршрутизатори оперативно обмінюються інформацією про зміни стану каналів (LSA - Link State Advertisements) і перераховують маршрути, мінімізуючи обсяг трафіку оновлення маршрутної інформації. OSPF широко використовується у великих корпоративних мережах та мережах провайдерів завдяки своїй надійності, масштабованості та відкритому стандарту. Це означає, що він сумісний з обладнанням різних виробників, що сприяє його широкому розповсюдженню та інтеграції в гетерогенні мережі.

EIGRP (Enhanced Interior Gateway Routing Protocol) – це вдосконалений гібридний протокол, який поєднує переваги протоколів з вектором відстані та протоколів стану каналу. Він використовує унікальний алгоритм DUAL (Diffusing Update Algorithm) для швидкої конвергенції та забезпечення гарантованої відсутності маршрутних петель. EIGRP відомий своєю ефективністю використання ресурсів та мінімізує навантаження на процесор маршрутизатора, оскільки він надсилає лише часткові оновлення маршрутної інформації. Це робить його дуже популярним у великих організаціях, які використовують обладнання Cisco. Важливо зазначити, що EIGRP є

власницьким протоколом Cisco, хоча згодом Cisco відкрила його специфікацію, що дозволило з'явитися деяким відкритим реалізаціям. Він підтримує маршрутизацію без класів (CIDR - Classless Inter-Domain Routing) та автоматичне узагальнення маршрутів, що сприяє зменшенню розміру таблиць маршрутизації та більш ефективному використанню IP-адресного простору.

BGP (Border Gateway Protocol) – це основний протокол глобальної Інтернет-маршрутизації (EGP), що дозволяє автономним системам (AS) обмінюватися маршрутною інформацією та управляти міжмережевими маршрутами. Він підтримує складні політики маршрутизації, що дозволяє адміністраторам мережі контролювати потік трафіку на основі різних атрибутів маршрутів, таких як AS-шлях, локальні уподобання або метрики. Це забезпечує високу гнучкість конфігурації, але водночас робить його досить складним у налаштуванні та підтримці. BGP використовується провайдерами Інтернету та великими корпораціями, які мають прямі підключення до декількох ISP. BGP є протоколом векторної відстані за шляхом (path-vector protocol), що означає, що він обмінюється інформацією не тільки про відстань до цільової мережі, але й про повний шлях (послідовність автономних систем), яким пройшов маршрут. Це є ключовим для запобігання маршрутним петлям у міждоменній маршрутизації та забезпечення стабільності глобального Інтернету.

1.4 Особливості вибору протоколу залежно від типу мережі

Вибір оптимального протоколу маршрутизації є одним з найважливіших рішень при проектуванні мережевої інфраструктури, і він залежить від масштабів мережі, її архітектури, вимог до продуктивності, безпеки, масштабованості та наявних ресурсів.

Локальні мережі (LAN) – для локальних мереж, особливо середнього та великого розміру, зазвичай використовують OSPF або EIGRP через їхню

гнучкість, швидкість конвергенції та ефективне управління ресурсами. Ці протоколи добре підходять для мереж, де важливо забезпечити швидке реагування на зміни топології (наприклад, додавання або видалення пристроїв, збої кабелів) та ефективне використання пропускної здатності. Для дуже малих і простих мереж, де топологія рідко змінюється, також може бути використана статична маршрутизація, оскільки вона не вимагає додаткових обчислювальних ресурсів для обміну маршрутною інформацією. Однак, статична маршрутизація вимагає значних ручних зусиль для підтримки та не здатна автоматично адаптуватися до змін, що робить її менш гнучкою.

Корпоративні мережі (WAN) – у корпоративних мережах, що охоплюють географічно розподілені офіси та філії, OSPF є часто оптимальним вибором завдяки його здатності працювати з великими та складними топологіями та підтримці багаторівневої маршрутизації. Це дозволяє створювати ієрархічні структури (за допомогою областей), що спрощує управління та масштабування великих мереж. EIGRP також може бути використаний у корпоративних мережах, особливо якщо компанія вже має значну інфраструктуру на обладнанні Cisco, оскільки EIGRP є власницьким протоколом Cisco, і його повна функціональність та продуктивність найкраще реалізуються в цьому середовищі. Для мереж з високими вимогами до безпеки та конфіденційності даних у WAN може бути розглянута імплементація VPN (Virtual Private Network) поверх існуючої маршрутизації для забезпечення шифрованих тунелів та додаткового рівня захисту.

Глобальні мережі (Internet, міжмережеве з'єднання) – для маршрутизації між різними автономними системами, тобто для обміну маршрутами в глобальній мережі Інтернет, BGP є основним і практично єдиним використовуваним протоколом. Він забезпечує ефективну маршрутизацію між незалежними мережами, дозволяючи провайдерам та великим корпораціям керувати політикою маршрутизації, контролювати

трафік та забезпечувати зв'язок з усім світом. При виборі BGP важливим є ретельне планування та конфігурація політик маршрутизації для оптимізації трафіку, забезпечення стабільності з'єднань та захисту від маршрутних атак. Його гнучкість у застосуванні політик є ключовою для складних сценаріїв маршрутизації, таких як багатодомовість (multihoming) та інженерія трафіку.

Змішані середовища – у багатьох реальних мережевих архітектурах часто використовують комбінацію різних протоколів маршрутизації, відому як перерозподіл маршрутів (route redistribution). Наприклад, дуже поширений підхід – використовувати OSPF для внутрішньої маршрутизації в межах автономної системи (IGP) та BGP для зовнішніх з’єднань з іншими AS (EGP). Такий підхід дозволяє оптимізувати внутрішній трафік за допомогою швидких та ефективних IGP, а зовнішній – за допомогою потужного та гнучкого EGP. У таких випадках критично важливо правильно налаштувати перерозподіл маршрутів між протоколами, щоб уникнути маршрутних петель, неоптимальних шляхів та інших проблем, які можуть виникнути при некоректній конфігурації. Це вимагає глибокого розуміння роботи обох протоколів та їх взаємодії.

Розуміння принципів маршрутизації та вибір оптимального протоколу є важливими факторами для забезпечення ефективної роботи мережевих систем. Коректний вибір маршрутизаційного протоколу дозволяє досягти високої продуктивності, стабільності та безпеки мережевого середовища, що відповідає сучасним вимогам бізнесу та користувачів. Також варто враховувати, що постійний моніторинг та оптимізація маршрутизації є невід'ємною частиною підтримки здорової, адаптивної та ефективної мережевої інфраструктури, що дозволяє оперативно реагувати на зміни та виклики.

РОЗДІЛ ІІ
АНАЛІЗ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ OSPF, EIGRP ТА BGP

2.1 Загальні принципи маршрутизації в комп’ютерних мережах

Комп’ютерна мережа — це сукупність взаємопов’язаних пристроїв, які можуть обмінюватися даними. Для передавання інформації між цими пристроями необхідно забезпечити правильне визначення шляху, яким має рухатися пакет. Цей процес називається маршрутизацією. Він виконується автоматично за допомогою спеціальних алгоритмів і протоколів, вбудованих у маршрутизатори. Маршрутизація є ключовим компонентом архітектури будь-якої комп'ютерної мережі, від локальних до глобальних, оскільки без неї пакети даних не змогли б знайти свій шлях до призначення.

Протоколи маршрутизації виконують дві ключові функції: Автоматичне виявлення топології мережі; Обчислення оптимального маршруту для кожного пакету даних.

Ці функції дозволяють маршрутизаторам динамічно адаптуватися до змін у мережі, таких як відмова обладнання, додавання нових пристроїв або зміни в конфігурації.

Усі протоколи маршрутизації можна умовно розділити на: Статичні, де маршрути задаються вручну адміністратором; Динамічні, де маршрутизатори автоматично будують таблиці маршрутів на основі отриманої інформації.

Статична маршрутизація, хоч і проста в налаштуванні для невеликих мереж з незмінною топологією, має суттєвий недолік – відсутність адаптивності до змін. При відмові каналу чи вузла, адміністратору доведеться вручну змінювати маршрути, що є неефективним у великих або динамічних мережах. Це може призвести до значних простоїв і вимагає постійного втручання.

Динамічна маршрутизація, навпаки, забезпечує автоматичне оновлення маршрутних таблиць, дозволяючи мережі самостійно адаптуватися до змін.

Це значно підвищує відмовостійкість та масштабованість мережі. Динамічні протоколи дозволяють мережі швидко відновлюватися після збоїв та оптимізувати трафік у реальному часі.

У свою чергу динамічні маршрутизаційні протоколи поділяються на внутрішньомережеві (IGP — Interior Gateway Protocols), що функціонують у межах однієї автономної системи, та зовнішньомережеві (EGP — Exterior Gateway Protocols), що обслуговують зв’язки між різними автономними системами. До IGP належать OSPF і EIGRP, а до EGP — протокол BGP.

2.2 Протокол OSPF (Open Shortest Path First)

OSPF — це відкритий протокол маршрутизації, розроблений у межах стандарту IETF (Internet Engineering Task Force), що належить до класу протоколів із підтримкою стану каналу (link-state). Протокол використовує алгоритм SPF (Shortest Path First), також відомий як алгоритм Дейкстри, який дозволяє розрахувати найкоротший шлях до кожного вузла в мережі. OSPF підтримує ієрархічну побудову, що дозволяє логічно поділяти мережу на області (areas). Це значно покращує масштабованість мережі та зменшує обсяг маршрутної інформації, що передається між маршрутизаторами.

Ключові переваги OSPF: Ієрархічна побудова: OSPF підтримує логічне поділення мережі на області (areas), що дає змогу масштабувати мережу та зменшити обсяг маршрутної інформації. Кожна область може бути налаштована незалежно, що спрощує управління великими мережами. Швидке оновлення маршрутів: Завдяки використанню LSA (Link State Advertisements) оновлення маршруту здійснюється тільки в разі зміни топології. Це забезпечує швидку конвергенцію мережі при виникненні збоїв, мінімізуючи час простою. Незалежність від вендора: Протокол підтримується всіма провідними виробниками мережевого обладнання, що робить його універсальним рішенням для різнорідних мережевих середовищ. Це дозволяє компаніям не бути прив'язаними до обладнання одного виробника.

Можливість автентифікації: Підтримує кілька методів захисту обміну маршрутною інформацією, що підвищує безпеку мережі та запобігає несанкціонованим змінам маршрутів.

Слід зазначити, що OSPF підтримує поділ на зону ядра (Area 0) та вторинні області, які мають підключатися до ядра. Цей поділ покращує керованість і стабільність протоколу в мережах великого масштабу. Кожна область має свою топологічну базу даних, що зменшує навантаження на обчислювальні ресурси маршрутизаторів, оскільки їм не потрібно знати всю топологію мережі. Крім того, OSPF підтримує балансування навантаження через рівновартісні шляхи, що дозволяє ефективно використовувати доступні мережеві ресурси.

2.3 Протокол EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP — це вдосконалений внутрішній протокол маршрутизації, створений компанією Cisco як заміна класичного протоколу IGRP. Він поєднує переваги протоколів дистанційно-векторного типу та протоколів стану каналу, утворюючи гібридний тип. Протокол використовує алгоритм DUAL (Diffusing Update Algorithm), що дозволяє гарантувати безпетльову маршрутизацію та вибір резервних маршрутів ще до виникнення збоїв у мережі. Це значно скорочує час перебудови маршрутної таблиці в разі змін у топології, що є критично важливим для мереж з високими вимогами до доступності та мінімальним часом простою.

Серед переваг EIGRP: Низьке навантаження на мережу завдяки частковим оновленням. EIGRP надсилає оновлення лише тоді, коли відбуваються зміни в мережі, а не періодично, що зменшує обсяг трафіку, який генерується протоколом. Висока швидкість збіжності, що робить його одним із найшвидших серед IGP. Завдяки алгоритму DUAL EIGRP швидко адаптується до змін у топології мережі, забезпечуючи мінімальний час простою. Підтримка VLSM (Variable Length Subnet Masking), що дозволяє

ефективно використовувати адресний простір IP-адрес і спрощує проектування мереж. Автоматичне резервування маршрутів через feasible successors. Це означає, що маршрутизатор заздалегідь розраховує альтернативні шляхи, які можуть бути використані в разі збою основного маршруту без необхідності повторного обчислення.

Попри те, що EIGRP тривалий час був закритим протоколом, у 2013 році Cisco опублікувала специфікацію, що дозволила розширити його використання за межами обладнання Cisco. Однак, він досі залишається найефективнішим саме в мережах із Cisco-інфраструктурою через оптимізацію під їхнє обладнання та підтримку специфічних функцій.

2.4 Протокол BGP (Border Gateway Protocol)

BGP — це основний зовнішній протокол маршрутизації, який забезпечує обмін маршрутною інформацією між автономними системами (AS) в Інтернеті. Він має принципово інший підхід до маршрутизації: замість найкоротшого шляху, BGP враховує політики маршрутизації, що задаються адміністратором. Це дозволяє провайдерам та великим корпораціям контролювати, як трафік проходить через їхні мережі та як вони взаємодіють з іншими автономними системами, що є критично важливим для глобальної маршрутизації та реалізації бізнес-домовленостей.

Особливості BGP: Підтримка атрибутів маршруту, таких як AS_PATH, NEXT_HOP, LOCAL_PREF тощо. Ці атрибути використовуються для реалізації складних політик маршрутизації, дозволяючи маршрутизаторам приймати рішення не лише на основі метрики, а й на основі встановлених правил. Маршрутизація за політиками, а не лише за метрикою. Це дозволяє адміністраторам задавати пріоритети маршрутів на основі бізнес-логіки, а не тільки технічних показників, що забезпечує більший контроль над потоком даних. Масштабованість, що дозволяє підтримувати сотні тисяч маршрутів. BGP є єдиним протоколом, здатним впоратися з величезною кількістю

маршрутів, які існують в Інтернеті, що робить його незамінним для глобальної маршрутизації. Надійність, що є критично важливим для глобальної мережі Інтернет. BGP розроблений для забезпечення стабільності та відмовостійкості маршрутизації на міждоменному рівні, що є життєво необхідним для функціонування Інтернету.

Оскільки BGP працює у відкритому середовищі, він має вбудовані механізми безпеки та перевірки цілісності маршрутної інформації. Однак його складність у налаштуванні та повільніша збіжність роблять його менш придатним для локальних мереж. Налаштування BGP вимагає глибокого розуміння принципів маршрутизації та політик безпеки, що робить його одним із найскладніших протоколів для конфігурації.

Існує дві версії BGP: External BGP (eBGP), що використовується для обміну маршрутами між різними автономними системами, та Internal BGP (iBGP), який застосовується всередині однієї AS для узгодження маршрутної інформації між внутрішніми маршрутизаторами. BGP працює поверх TCP (порт 179), що забезпечує надійність доставки маршрутних повідомлень. У сучасних мережах активно впроваджуються розширення до BGP, такі як BGP Route Reflectors**,** Confederations, а також BGP-LS (Link-State) для інтеграції з SDN-рішеннями. Для покращення безпеки використовуються механізми, як-от RPKI (Resource Public Key Infrastructure), що дозволяє верифікувати авторитетність джерел маршруту та запобігати атакам типу «prefix hijacking». Таким чином, BGP є критичним компонентом сучасного Інтернету, що дозволяє ефективно керувати маршрутизацією на глобальному рівні, зберігаючи гнучкість, масштабованість та контроль над потоками трафіку.

2.5 Порівняльний аналіз OSPF, EIGRP та BGP

Для кращого розуміння відмінностей та переваг кожного протоколу, нижче представлена порівняльна таблиця, яка узагальнює їхні ключові характеристики:

Таблиця 2.1 – Порівняльний аналіз протоколів

Параметр	**OSPF**	**EIGRP**	**BGP**
Тип протоколу	Link-state	Hybrid (distance-vector)	Path-vector
Сфера використаня	Внутрішньомережевий (IGP)	Внутрішньомережевий (IGP)	Зовнішньомережевий (EGP)
Алгоритм маршрутизаії	SPF (Дейкстра)	DUAL	Вибір за політиками
Швидкість збіжності	Висока	Дуже висока	Повільна
Підтримка резервних маршрутів	Обмежена	Є (feasible successors)	Залежить від політики
Масштабованість	Середня	Висока	Дуже висока
Складність налаштуваня	Середня	Низька	Висока
Незалежність від виробника	Так	Обмежена (в основному Cisco)	Так
Гнучкість маршрутизаії	Висока	Середня	Дуже висока

Ця таблиця наочно демонструє ключові відмінності між протоколами, що допомагає у виборі оптимального рішення для конкретних потреб мережі.

2.6 Висновки до розділу

У цьому розділі було проведено детальний аналіз трьох ключових протоколів маршрутизації — OSPF, EIGRP та BGP. Кожен з них реалізує власний підхід до обміну маршрутною інформацією та має свої сильні й слабкі сторони.

OSPF є загальновживаним відкритим протоколом для середніх і великих локальних мереж. Його ієрархічна структура та швидка конвергенція роблять його ідеальним для комплексних мереж, де потрібна гнучкість та надійність.

EIGRP забезпечує швидку та гнучку маршрутизацію, але залишається прив’язаним до інфраструктури Cisco. Це може бути перевагою для компаній, які повністю використовують обладнання Cisco, але обмежує його застосування в інших середовищах.

BGP, у свою чергу, є незамінним для глобальних мереж і забезпечує масштабовану маршрутизацію з використанням складних політик. Його роль у функціонуванні Інтернету є критичною, оскільки він дозволяє встановлювати зв'язки між різними автономними системами та керувати потоками трафіку на глобальному рівні.

Таким чином, вибір маршрутизаційного протоколу залежить від структури мережі, її розміру, наявного обладнання та цілей, які ставить перед собою мережевий адміністратор. У наступному розділі буде проведено моделювання комп’ютерної мережі з використанням зазначених протоколів з метою оцінки їх продуктивності на практиці.

2.7 Алгоритми маршрутизації, що лежать в основі протоколів

Розуміння роботи маршрутизаційних протоколів неможливе без глибшого аналізу алгоритмів, які лежать в їх основі. Саме ці алгоритми визначають принципи пошуку шляху, реакцію на зміни топології та швидкість збіжності.

Алгоритм SPF (Shortest Path First), що використовується в OSPF, заснований на методі Дейкстри. Він побудований на створенні повної карти мережі, після чого обчислюється найкоротший шлях до кожного вузла. Основною перевагою є точність і надійність, однак оновлення таблиці вимагає значних обчислювальних ресурсів. Це особливо відчутно у великих

мережах, де кожна зміна топології вимагає перерахунку всієї карти, що може займати певний час.

DUAL (Diffusing Update Algorithm) — інноваційний алгоритм, реалізований у EIGRP. Він дозволяє маршрутизатору мати запасні шляхи (feasible successors), що зменшує час простою при зміні топології. DUAL гарантує відсутність петель маршрутизації та підвищує швидкість адаптації. Завдяки цьому EIGRP є одним з найшвидших IGP протоколів, забезпечуючи майже миттєву реакцію на зміни в мережі.

Path-vector, як у BGP, відрізняється від інших тим, що основний акцент робиться не на довжині шляху, а на політиках і історії проходження маршруту (AS_PATH). Це дозволяє контролювати, через які автономні системи будуть передаватися пакети, навіть якщо шлях не є найкоротшим. Такий підхід є критично важливим для управління глобальним трафіком і реалізації бізнес-політик, оскільки провайдери можуть встановлювати власні правила для маршрутизації трафіку.

2.8 Практичні сценарії застосування протоколів

Кожен з протоколів має типові сценарії, в яких він демонструє найвищу ефективність: OSPF часто використовується в державних установах, навчальних закладах та корпоративних мережах великого масштабу. Його ієрархічна структура з областями дозволяє ефективно керувати великою кількістю пристроїв і мереж. Він забезпечує хорошу масштабованість та швидку конвергенцію, що робить його універсальним рішенням для мереж з різними потребами.

EIGRP ідеально підходить для корпоративних мереж, які базуються виключно на обладнанні Cisco. Завдяки високій швидкості збіжності та ефективному алгоритму DUAL, він забезпечує стабільну роботу критично важливих служб. Це робить його привабливим вибором для компаній, які вже інвестували в екосистему Cisco та прагнуть максимальної продуктивності.

BGP незамінний для провайдерів інтернет-послуг (ISP), транзитних операторів та великих дата-центрів. Він забезпечує обмін маршрутом між автономними системами, що дозволяє створювати стійкі та оптимізовані маршрути на глобальному рівні. BGP дозволяє гнучко управляти трафіком та реалізовувати складні політики маршрутизації, що є невід'ємною частиною сучасного Інтернету.

2.9 Питання безпеки у протоколах маршрутизації

У сучасних мережах безпека маршрутизаційних протоколів стає критично важливою. Неконтрольоване поширення фальшивої маршрутної інформації може призвести до перенаправлення трафіку (route hijacking), DDoS-атак, або порушення доступності сервісів. Ці загрози можуть мати серйозні наслідки для бізнесу та користувачів.

OSPF підтримує кілька механізмів аутентифікації, зокрема просту (plain-text) та криптографічну (MD5), що дозволяє перевіряти легітимність маршрутної інформації. Новіші версії OSPF також підтримують більш сильні методи аутентифікації, такі як HMAC-SHA, для підвищення рівня безпеки.

EIGRP також реалізує механізми перевірки автентичності сусідів, зокрема через використання key-chain та алгоритмів хешування. Це забезпечує захист від несанкціонованих оновлень маршрутів та допомагає підтримувати цілісність маршрутної таблиці.

BGP, попри складну природу, довгий час мав мінімальні засоби захисту, що зумовило розвиток нових стандартів, таких як BGP Prefix Filtering, TCP MD5 Signatures і RPKI (Resource Public Key Infrastructure). Останній дозволяє перевіряти легітимність оголошень маршрутів, що походять від певного автономного системного номера. Це значно підвищує довіру до маршрутної інформації в глобальній мережі та допомагає боротися з такими явищами, як перенаправлення префіксів.

Таким чином, сучасне налаштування будь-якого з розглянутих протоколів повинно враховувати не лише продуктивність і сумісність, а й аспекти безпеки, які мають не менш важливе значення. Забезпечення безпеки маршрутизації є ключовим для стабільності та надійності функціонування всієї мережевої інфраструктури в умовах зростаючих кіберзагроз.

РОЗДІЛ ІІІ
ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ OSPF, EIGRP ТА BGP

Порівняльний аналіз протоколів маршрутизації OSPF, EIGRP та BGP ґрунтується на комбінованому методі дослідження, що поєднує теоретичну оцінку характеристик кожного з протоколів та практичне моделювання їх роботи в симульованому середовищі. Основна мета полягає у виявленні переваг і недоліків кожного з протоколів на основі таких критеріїв, як швидкість конвергенції, масштабованість, ефективність використання ресурсів, стійкість до відмов, підтримка політик маршрутизації, рівень безпеки та сумісність із різними мережевими структурами. Цей розділ є критично важливим для розуміння того, як різні протоколи маршрутизації відповідають різним вимогам мережевих інфраструктур, від невеликих локальних мереж до глобальних інтернет-систем. Детальний розгляд архітектури, принципів роботи та механізмів кожного протоколу дозволить зробити обґрунтовані висновки щодо їхнього оптимального застосування.

3.1 Теоретичний аналіз протоколів маршрутизації

Теоретична частина дослідження ґрунтується на ретельному вивченні технічної документації, стандартів протоколів (RFC), а також аналізу результатів наукових публікацій та досліджень у галузі мережевих технологій. Цей етап включає опис базових принципів роботи, архітектурних особливостей, механізмів обміну маршрутною інформацією та ключових характеристик кожного протоколу.

Для кращого розуміння особливостей та застосування різних протоколів маршрутизації доцільно порівняти їх за ключовими характеристиками. У таблиці нижче наведено порівняння трьох популярних протоколів — OSPF, EIGRP та BGP.

Таблиця 3.1 – Порівняльна таблиця протоколів маршрутизації

Характеристика	OSPF	EIGRP	BGP
Тип протоколу	Внутрішній, протокол стану каналу (Link-State)	Внутрішній, гібридний (Distance Vector + LS)	Зовнішній, вектор шляху (Path Vector)
Стандартизація	Відкритий стандарт (IETF)	Власний (Cisco)	Відкритий стандарт (IETF)
Призначення	Внутрішньо-мережева маршрутизація (IGP)	Внутрішньо-мережева маршрутизація (IGP)	Міжмережева маршрутизація (EGP)
Алгоритм	Dijkstra (Shortest Path First)	DUAL (Diffusing Update Algorithm)	Best Path Selection Algorithm
Метрика	Вартість (Cost) — залежить від пропускної здатності	Комбінована: пропускна здатність, затримка, надійність, завантаженість	Кількість автономних систем (AS-path), інші атрибути
Конвергенція	Висока	Дуже висока	Низька (але стабільна)
Підтримка VLSM/CIDR	Так	Так	Так
Підтримка множинних шляхів	Так (ECMP)	Так (Feasible Successors)	Обмежено (може використовувати декілька шляхів)
Простота налаштування	Складна	Простіша (на Cisco)	Складна
Ресурсомісткість	Середня	Середня	Висока
Використання	Enterprise-мережі	Cisco-мережі малого/середнього масштабу	Mix AS в Інтернеті

3.1.1 Протокол OSPF (Open Shortest Path First)

OSPF належить до класу протоколів із підтримкою стану каналу (link-state), що означає, що кожен маршрутизатор у мережі OSPF підтримує повну базу даних стану каналів (Link State Database, LSDB), яка є топологічною картою мережі. Він використовує алгоритм SPF (Shortest Path First), заснований на методі Дейкстри, для обчислення найкоротших шляхів до всіх пунктів призначення в мережі з точки зору самого маршрутизатора. Це забезпечує високу точність маршрутизації, оскільки кожен маршрутизатор має повне уявлення про всю топологію, та дозволяє динамічно адаптуватися

до змін у мережі, таких як додавання нових з'єднань, відмова існуючих або зміна метрик.

Для кращого розуміння принципу роботи протоколу OSPF доцільно розглянути загальну послідовність його дій на маршрутизаторі. Схема нижче ілюструє основні етапи встановлення та функціонування OSPF -сесії, зокрема процеси обміну маршрутами, вибору оптимального шляху та оновлення маршрутної інформації.

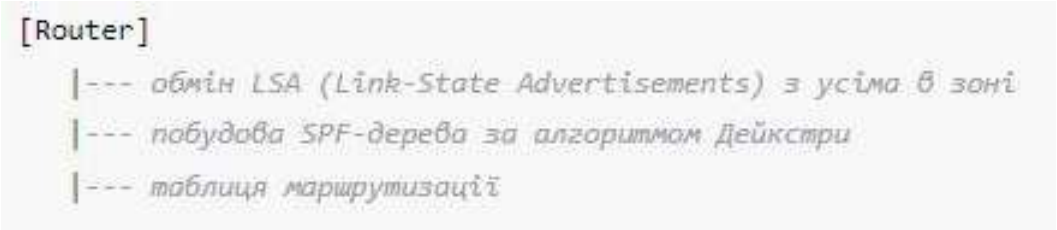

Рисунок 3.1 – принцип роботи протоколу OSPF

OSPF підтримує поділ на області (areas), що значно підвищує його масштабованість. Мережа OSPF розділяється на декілька областей, які пов'язані з нульовою областю (backbone area). Такий ієрархічний дизайн дозволяє зменшити розмір таблиць маршрутизації та обсяг службового трафіку (LSA – Link State Advertisement), оскільки LSA поширюються лише в межах своєї області. Це зменшує навантаження на процесори маршрутизаторів та обсяг пам'яті, необхідний для зберігання маршрутної інформації. Крім того, OSPF є протоколом, незалежним від виробника (vendor-neutral), та широко підтримується різними типами мережевого обладнання, що робить його універсальним рішенням для різноманітних та гетерогенних мережевих інфраструктур.

OSPF використовує багатоадресну розсилку (multicast) для обміну інформацією про стан каналів (LSA-пакети), що забезпечує ефективність передачі даних та швидке поширення змін топології. Кожен маршрутизатор, отримуючи LSA, оновлює свою LSDB, а потім запускає алгоритм SPF для перерахунку найкоротших шляхів. Це забезпечує швидку конвергенцію, хоча і вимагає деяких обчислювальних ресурсів. Протокол також підтримує різні

типи мереж, включаючи широкомовні (broadcast), точково-точкови (point-to-point) та неширокомовні багатоточкові (NBMA), що робить його гнучким для використання у різних фізичних топологіях.

3.1.2 Протокол EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP є гібридним протоколом, який поєднує риси протоколів із вектором відстані та протоколів стану каналу. Це дозволяє йому поєднувати простоту налаштування та легкість, характерні для протоколів вектора відстані, з високою швидкістю конвергенції та відсутністю маршрутних петель, властивими протоколам стану каналу. Його ключовою особливістю є використання алгоритму DUAL (Diffusing Update Algorithm), який забезпечує гарантовану відсутність маршрутних петель та дозволяє підтримувати декілька резервних маршрутів (feasible successors) до кожного пункту призначення. Ця наявність попередньо обчислених резервних шляхів забезпечує надзвичайно швидку конвергенцію у разі збою основного маршруту, що є критично важливим для додатків, чутливих до затримок, таких як VoIP, відеоконференції та потокові медіа.

Для кращого розуміння принципу роботи протоколу EIGRP доцільно розглянути загальну послідовність його дій на маршрутизаторі. Схема нижче ілюструє основні етапи встановлення та функціонування EIGRP -сесії, зокрема процеси обміну маршрутами, вибору оптимального шляху та оновлення маршрутної інформації.

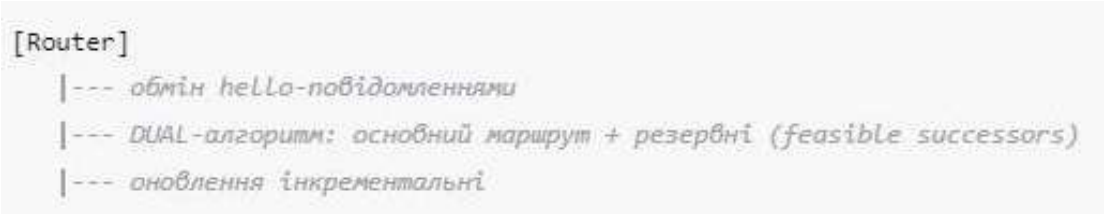

Рисунок 3.2 – принцип роботи протоколу EIGRP

EIGRP також відомий своєю винятковою ефективністю використання ресурсів, оскільки він надсилає лише часткові оновлення маршрутної

інформації (partial updates), і лише тоді, коли відбуваються зміни в мережі. Це значно зменшує обсяг службового трафіку порівняно з протоколами, які регулярно відправляють повні таблиці маршрутизації. Проте, його ефективність повною мірою реалізується здебільшого в інфраструктурах на базі обладнання Cisco, оскільки EIGRP є пропрієтарним протоколом Cisco. Хоча це обмежує його застосування в гетерогенних мережах з обладнанням різних виробників, у чистому середовищі Cisco EIGRP демонструє виняткову продуктивність, стабільність та гнучкість.

EIGRP використовує надійний транспортний протокол (RTP - Reliable Transport Protocol) для передачі оновлень, що забезпечує доставку інформації про маршрути та підтвердження її отримання, підвищуючи надійність протоколу. Крім того, EIGRP підтримує балансування навантаження по нерівних шляхах (unequal-cost load balancing), що дозволяє використовувати декілька маршрутів до одного призначення, навіть якщо їх метрики відрізняються, забезпечуючи більш ефективне використання мережевих ресурсів та підвищуючи пропускну здатність.

3.1.3 Протокол BGP (Border Gateway Protocol)

Протокол BGP відрізняється від OSPF та EIGRP своєю сферою застосування — він призначений для маршрутизації між автономними системами (AS) у глобальній мережі Інтернет. Це протокол зовнішнього шлюзу (External Gateway Protocol, EGP), на відміну від OSPF та EIGRP, які є протоколами внутрішнього шлюзу (Interior Gateway Protocols, IGPs). BGP використовує вектор шляху (path-vector), що означає, що він передає не лише інформацію про метрику (відстань), а й повний шлях (послідовність AS), яким пройшов маршрут до певного пункту призначення. Ця інформація про AS-шлях є критично важливою для запобігання маршрутним петлям у міждоменній маршрутизації та дозволяє операторам мережі приймати рішення на основі складної політики маршрутизації.

Для кращого розуміння принципу роботи протоколу BGP доцільно розглянути загальну послідовність його дій на маршрутизаторі. Схема нижче ілюструє основні етапи встановлення та функціонування BGP-сесії, зокрема процеси обміну маршрутами, вибору оптимального шляху та оновлення маршрутної інформації.

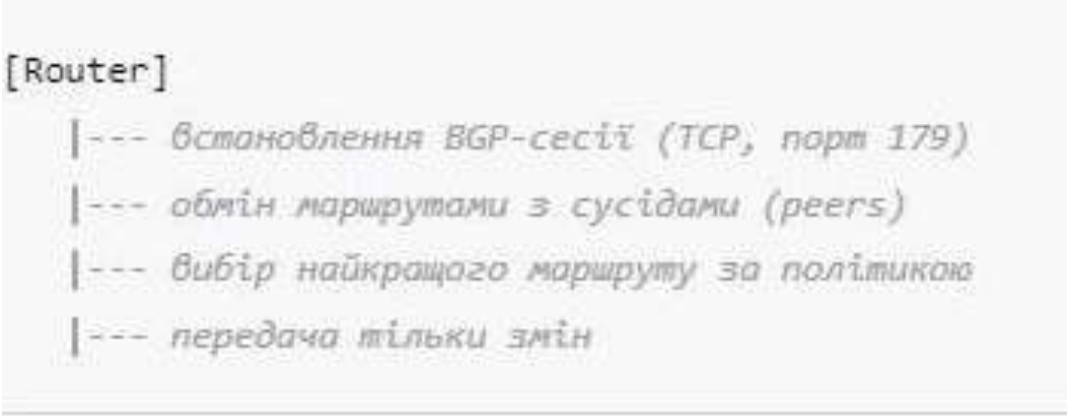

Рисунок 3.2 – принцип роботи протоколу BGP

BGP працює на основі політик, а не лише метрик, що забезпечує неперевершену гнучкість управління маршрутами. Це дозволяє адміністраторам мережі реалізовувати складні політики маршрутизації, такі як контроль доступу до певних маршрутів, балансування навантаження на основі атрибутів маршрутів, фільтрація трафіку, вибір оптимального маршруту на основі договірних відносин з іншими AS та багато іншого. Проте, це вимагає складної конфігурації, глибоких знань протоколу та високої кваліфікації персоналу, що робить BGP одним з найскладніших протоколів для налаштування та управління.

BGP менш придатний для використання в локальних мережах через свою повільну конвергенцію порівняно з OSPF та EIGRP. Його пріоритетом є стабільність глобальної маршрутизації та гнучкість управління потоками трафіку між AS, а не швидке реагування на внутрішні зміни топології. BGP обмінюється маршрутною інформацією за допомогою TCP-з'єднання (порт 179), що забезпечує надійну передачу даних. Він є основою маршрутизації в Інтернеті, забезпечуючи зв'язок між мільйонами мереж по всьому світу та

дозволяючи глобальним потокам даних знаходити свій шлях через різні автономні системи.

3.2 Практичний аналіз та моделювання

Практичний аналіз проводився за допомогою симуляційних інструментів Cisco Packet Tracer та GNS3, що дозволяє імітувати реальні мережеві середовища та тестувати поведінку протоколів маршрутизації без необхідності розгортання фізичного обладнання. Для забезпечення об'єктивності результатів, було створено три ідентичні мережеві топології з однаковою кількістю маршрутизаторів, кінцевих пристроїв (хостів) та підмереж. Кожна топологія була налаштована на використання одного з досліджуваних протоколів: OSPF, EIGRP та BGP. У ході моделювання здійснювалися різноманітні тестування, які включали: вимкнення вузлів для імітації відмов обладнання, імітацію втрати зв’язку на певних сегментах мережі, збільшення навантаження на маршрутизатори шляхом генерації значного обсягу трафіку та динамічну зміну топології (наприклад, додавання або видалення маршрутизаторів та з'єднань). Метою цих тестів було об'єктивне визначення ключових показників продуктивності, таких як час конвергенції, рівень завантаженості центрального процесора (CPU) маршрутизаторів, обсяг службового трафіку, який генерує кожен протокол, та загальна здатність протоколів до відновлення стабільної роботи після збоїв.

3.2.1 Швидкість конвергенції

Швидкість конвергенції є одним з найважливіших показників продуктивності протоколу маршрутизації, оскільки вона визначає, наскільки швидко мережа адаптується до змін у топології та відновлює повноцінне функціонування. Результати моделювання засвідчили, що EIGRP продемонстрував найвищу швидкість реакції на зміну топології. Це

обумовлено використанням алгоритму DUAL та наявністю попередньо обчислених резервних маршрутів (feasible successors). У випадку збою основного маршруту, EIGRP може миттєво переключитися на резервний шлях, не запускаючи повний процес переобчислення маршрутів. Конвергенція для EIGRP становила в середньому 1,5–2 секунди, навіть при значному навантаженні на мережу, що є винятковим показником для будь-якого протоколу маршрутизації. Це робить EIGRP ідеальним для мереж, де час простою повинен бути мінімальним, а швидке відновлення зв'язку є критично важливим, наприклад, для IP-телефонії або відеоспостереження.

OSPF забезпечував стабільну роботу з конвергенцією в межах 4–5 секунд. Хоча OSPF повільніший за EIGRP, його механізми швидкого перерахунку шляхів при отриманні нових LSA та ієрархічна структура дозволяють забезпечити стабільну та надійну роботу у масштабованих корпоративних мережах. Час конвергенції OSPF є цілком прийнятним для більшості додатків, що не вимагають мілісекундної реакції. Завдяки повній топологічній карті мережі, OSPF може знаходити оптимальні шляхи після змін у топології, забезпечуючи ефективне використання ресурсів.

Протокол BGP, як очікувалося, мав найповільнішу конвергенцію — до 10–15 секунд, а іноді й більше, залежно від масштабу таблиць маршрутизації та кількості BGP-пірів. Це пов'язано з його природою роботи, яка орієнтована на стабільність міждоменних з'єднань та використання складних політик, а не на миттєве реагування на внутрішні зміни топології. BGP розроблений для обробки величезних обсягів маршрутної інформації в глобальному масштабі, де швидкість конвергенції є вторинною порівняно зі стабільністю, гнучкістю та запобіганням маршрутним петлям. Проте, BGP забезпечив гнучке управління маршрутами і стабільність в умовах втрати зв’язків між автономними системами, що є його ключовою перевагою у глобальних мережах.

3.2.2 Ефективність використання ресурсів

Ефективність використання ресурсів маршрутизаторів (CPU, пам'ять) є важливим фактором при проектуванні мереж, особливо у великих і складних топологіях. Під час практичної симуляції було виявлено суттєві відмінності у споживанні ресурсів між протоколами. EIGRP навантажував центральний процесор маршрутизатора в межах 25–30 % при середньому навантаженні на мережу. Це свідчить про його високу ефективність використання обчислювальних потужностей, що дозволяє використовувати EIGRP на менш потужних пристроях або забезпечувати більшу кількість мережевих сервісів на тих самих маршрутизаторах без значного зниження продуктивності. Обсяг пам'яті, необхідний для EIGRP, також відносно невеликий, оскільки він зберігає лише інформацію про сусідів та їхні маршрути.

OSPF продемонстрував помірне навантаження — на рівні 40–50 % CPU. Це обумовлено необхідністю підтримувати повну базу даних стану каналів (LSDB) та регулярно запускати алгоритм SPF для перерахунку найкоротших шляхів. Однак, завдяки своїй ієрархічній структурі (поділ на області), OSPF дозволяє гнучко розподіляти обчислення між окремими областями мережі, що може зменшити загальне навантаження на окремі маршрутизатори у великих мережах. Кожен маршрутизатор зберігає повну топологічну карту лише для своєї області, а для інших областей зберігає лише зведену інформацію, що допомагає контролювати споживання пам'яті.

Найбільш ресурсомістким виявився BGP, який в умовах великої кількості маршрутів (понад 1000 префіксів IP-адрес) створював навантаження на рівні 70–80 % потужностей CPU. Це характерно для глобальних магістральних вузлів та інтернет-провайдерів, де BGP обробляє величезну кількість маршрутної інформації з усього світу, включаючи тисячі префіксів IP-адрес та сотні тисяч записів у таблицях маршрутизації. Високе споживання ресурсів BGP обумовлене необхідністю зберігання та обробки великих обсягів маршрутної інформації, підтримки складних політик, а

також підтримання TCP-з'єднань з BGP-пірами. Для ефективної роботи BGP потрібні потужні маршрутизатори з великим обсягом оперативної пам'яті та високопродуктивними процесорами.

3.2.3 Стійкість до відмов та відновлення роботи

Стійкість до відмов та здатність протоколу до швидкого відновлення роботи після збою є критично важливими для забезпечення неперервності функціонування мережі. Усі розглянуті протоколи показали стабільну роботу після відновлення з'єднань, що свідчить про їхню надійність. Проте, механізм миттєвого перемикання у EIGRP залишився найефективнішим з огляду на час реакції та простоту реалізації. Це обумовлено наявністю у DUAL алгоритмі готових "наступних найкращих" шляхів (feasible successors), які EIGRP вже обчислив і зберігає. У разі збою основного маршруту, маршрутизатор миттєво перемикається на feasible successor без необхідності запускати новий процес обчислення або розсилання запитів, що мінімізує час простою до мілісекунд.

OSPF також продемонстрував високу стійкість до відмов завдяки швидкому перерахунку найкоротших шляхів при отриманні нових LSA, які сигналізують про зміни в топології. Хоча це займає трохи більше часу, ніж миттєве перемикання EIGRP, OSPF швидко відновлює маршрутизацію, забезпечуючи стабільність мережі. Його ієрархічна структура допомагає локалізувати проблеми, запобігаючи їх поширенню на всю мережу.

BGP забезпечив високу стабільність в умовах втрати зв’язків між автономними системами, хоча і з повільнішою конвергенцією. Його стійкість забезпечується механізмами, такими як маршрутна агрегація, яка зменшує розмір таблиць маршрутизації, та гнучка фільтрація маршрутів, що допомагає зменшити вплив збоїв на глобальну маршрутизацію. Крім того, BGP сесії є стійкими до збоїв у зв'язку завдяки використанню TCP, який забезпечує надійну доставку пакетів. У разі розриву TCP-сесії BGP, протокол

спробує її відновити, а маршрути будуть зберігатися до відновлення зв'язку або до закінчення таймера.

3.3 Безпека протоколів маршрутизації

У сучасних мережах безпека маршрутної інформації є критично важливою, оскільки втручання у маршрутизаційний процес може призвести до серйозних порушень функціонування мережі, таких як перехоплення трафіку, відмова в обслуговуванні (DoS-атаки), створення маршрутних петель, або перенаправлення трафіку на зловмисні ресурси. Захист протоколів маршрутизації є фундаментальним для забезпечення цілісності, доступності та конфіденційності мережевих даних.

3.3.1 Засоби безпеки в OSPF

OSPF реалізує автентифікацію маршрутної інформації для захисту від несанкціонованих оновлень. Існують два основних типи автентифікації:

Проста автентифікація (Simple password authentication): Використовує простий текстовий пароль, який передається у відкритому вигляді. Цей метод не є безпечним і не рекомендується для використання в продакшн-середовищах через легкість перехоплення пароля.

Автентифікація MD5 (MD5 authentication): Використовує хешування MD5 для створення дайджесту повідомлення, який включається до OSPF-пакетів. Це дозволяє запобігти підробці LSA-повідомлень (Link State Advertisement) та інших OSPF-пакетів. Якщо маршрутизатор отримує пакет OSPF з невірним дайджестом, він ігнорує його, що захищає мережу від зловмисних або пошкоджених оновлень. Автентифікація гарантує, що лише довірені маршрутизатори, які знають секретний ключ, можуть брати участь у процесі маршрутизації OSPF, захищаючи мережу від несанкціонованих вузлів. Хоча MD5 вже не вважається криптографічно стійким для деяких

застосувань, для захисту OSPF-трафіку він все ще забезпечує прийнятний рівень захисту в багатьох корпоративних мережах.

3.3.2 Засоби безпеки в EIGRP

EIGRP також пропонує механізми автентифікації для захисту маршрутної інформації:

Автентифікація MD5 (MD5 authentication): Схожий на OSPF, EIGRP використовує MD5 для хешування пакета оновлення, що забезпечує цілісність даних та автентифікацію джерела. Маршрутизатори повинні використовувати один і той же ключ для автентифікації сусідства та обміну маршрутами.

Key-chain та обмеження дії ключів у часі: EIGRP підтримує використання key-chain, що дозволяє адміністраторам налаштовувати послідовність ключів (secret keys), які змінюються з часом. Це підвищує рівень безпеки, оскільки зловмисникам складніше перехопити та використати статичні ключі. Можливість задавати час дії для кожного ключа в key-chain дозволяє автоматично змінювати ключі автентифікації без ручного втручання та переривання роботи мережі. Це допомагає запобігти несанкціонованому доступу та втручанню в обмін маршрутною інформацією EIGRP, забезпечуючи цілісність даних та автентифікацію джерел, що є критично важливим для стабільності мережі.

3.3.3 Засоби безпеки в BGP

BGP, будучи протоколом, що працює у глобальному Інтернет-середовищі, має найрозвиненішу систему безпеки серед розглянутих протоколів. Це обумовлено високими ризиками маршрутних атак у міждоменному середовищі.

Автентифікація TCP MD5: BGP використовує TCP як транспортний протокол, і автентифікація TCP MD5 застосовується для захисту самого TCP-

з'єднання між BGP-пірами. Це запобігає несанкціонованому встановленню BGP-сесії та перехопленню маршрутних оновлень.

Префіксна фільтрація (Prefix filtering): Цей механізм дозволяє адміністраторам мережі суворо контролювати, які IP-префікси (маршрути) приймаються або анонсуються BGP-маршрутизатором. Це критично важливий інструмент для запобігання поширенню невірних або зловмисних маршрутів, таких як маршрутні підробки (route hijacks) або "чорні діри" (blackholing). Фільтрація може бути налаштована на основі AS-шляху, спільнот BGP або інших атрибутів.

Inbound/Outbound Route Filtering: Дозволяє фільтрувати маршрути, які отримуються (inbound) або анонсуються (outbound) BGP-маршрутизатором. Це дає змогу реалізовувати політики безпеки, запобігаючи анонсуванню приватних IP-адрес або маршрутів, які не належать даній AS.

Resource Public Key Infrastructure (RPKI): RPKI є сучасною інфраструктурою відкритих ключів, яка дозволяє перевіряти автентичність маршрутів на основі цифрових сертифікатів. RPKI забезпечує криптографічну перевірку того, що анонсований маршрут належить законному власнику префіксу IP-адреси. Це є потужним засобом боротьби з маршрутними підробками (route hijacks) та іншими видами атак на глобальну маршрутизацію, підвищуючи довіру до маршрутної інформації в Інтернеті. Такі механізми є абсолютно необхідними у глобальному Інтернет-середовищі, де маршрутизаційні помилки або зловмисні втручання можуть мати катастрофічні наслідки для мільйонів користувачів та всієї мережевої інфраструктури.

3.4 Рекомендації щодо застосування протоколів

З урахуванням проведеного комплексного теоретичного та практичного аналізу можна сформулювати наступні рекомендації, які допоможуть зробити обґрунтований вибір протоколу маршрутизації для конкретних

потреб та архітектури мережі. Оптимальний вибір залежить від багатьох факторів, включаючи розмір мережі, її топологію, вимоги до продуктивності, наявний бюджет, тип обладнання та кваліфікацію персоналу.

3.4.1 Застосування OSPF

Протокол OSPF доцільно застосовувати у великих та середніх корпоративних мережах, а також у мережах провайдерів послуг, де важливо забезпечити збалансовану продуктивність, високу масштабованість та відмовостійкість. Його незалежність від виробника та широка підтримка різними мережевими пристроями роблять його універсальним рішенням для гетерогенних мережевих інфраструктур. OSPF ідеально підходить для мереж, що потребують високої надійності та швидкого відновлення після збоїв, а також для мереж з частими змінами топології, оскільки він ефективно адаптується до таких змін.

Ключова перевага OSPF – його ієрархічна архітектура з поділом на області. Цей поділ дозволяє:

Зменшити розмір таблиць маршрутизації на маршрутизаторах всередині областей, оскільки вони зберігають детальну інформацію лише про свою область, а для інших областей – лише зведену інформацію.

Локалізувати проблеми: Збої в одній області не впливають на маршрутизацію в інших областях, що підвищує загальну стабільність мережі.

Зменшити обсяг службового трафіку: LSA-пакети поширюються лише в межах своєї області, що знижує навантаження на мережеві канали та процесори маршрутизаторів.

OSPF є чудовим вибором для мереж, де планується подальше масштабування, оскільки його модульна структура дозволяє легко додавати нові області без значного впливу на існуючу мережу.

3.4.2 Застосування EIGRP

Протокол EIGRP варто впроваджувати в інфраструктурах, побудованих переважно на обладнанні Cisco. Це обумовлено тим, що EIGRP є пропрієтарним протоколом Cisco, і хоча існують деякі реалізації для інших виробників, найкраща продуктивність та функціональність досягаються саме на обладнанні Cisco. EIGRP є оптимальним вибором для мереж, де критично важливими є мінімальні затримки, дуже швидке відновлення зв’язку та ефективне використання ресурсів.

EIGRP є відмінним вибором для мереж, що підтримують голосовий трафік (VoIP), відеоконференції або інші додатки, чутливі до затримок, завдяки своїй унікальній швидкості конвергенції. Його механізм DUAL дозволяє миттєво перемикатися на резервний маршрут у разі збою основного, мінімізуючи час простою та забезпечуючи безперебійну роботу критично важливих сервісів. Додаткові переваги EIGRP включають:

Балансування навантаження по нерівних шляхах: EIGRP може розподіляти трафік по декількох маршрутах, навіть якщо їх метрики відрізняються, що дозволяє більш ефективно використовувати наявну пропускну здатність.

Часткові оновлення: Надсилає лише зміни в маршрутній інформації, що зменшує обсяг службового трафіку та навантаження на маршрутизатори.

EIGRP є ідеальним рішенням для локальних мереж підприємств, де мережеве обладнання в основному складається з пристроїв Cisco, і потрібна висока продуктивність з мінімальним часом простою.

3.4.3 Застосування BGP

Протокол BGP, своєю чергою, є незамінним для організацій, що здійснюють обмін маршрутом із зовнішніми мережами, насамперед в умовах глобальної мережі Інтернет. Це стосується інтернет-провайдерів (ISP),

великих корпорацій, що мають прямі підключення до декількох ISP (multihoming), дата-центрів та транзитних вузлів. BGP забезпечує максимальну гнучкість маршрутизації, виняткову масштабованість і потужні засоби контролю доступу та застосування політик.

BGP є єдиним протоколом, призначеним для міждоменної маршрутизації, що дозволяє:

Управляти глобальними маршрутами: Обмінюватися інформацією про мільйони IP-префіксів з іншими автономними системами.

Реалізовувати складні політики маршрутизації: Визначати пріоритет маршрутів на основі різних атрибутів (AS-path, local preference, MED), контролювати вхідний та вихідний трафік, забезпечувати фільтрацію небажаних маршрутів.

Забезпечувати багатодомовість (multihoming): Підключатися до декількох інтернет-провайдерів одночасно, що підвищує відмовостійкість та дозволяє оптимізувати маршрутизацію трафіку.

Хоча BGP вимагає високої кваліфікації персоналу для правильного налаштування, його можливості політики маршрутизації є критично важливими для управління глобальним трафіком, забезпечення міждоменної зв'язності та захисту мережевої інфраструктури в умовах глобального Інтернету. Його повільна конвергенція є прийнятною, оскільки зміни у глобальній маршрутизації відбуваються не так часто, як у внутрішніх мережах, а пріоритетом є стабільність та контроль.

3.5 Висновки за розділом

У цьому розділі було здійснено глибокий порівняльний аналіз трьох ключових протоколів маршрутизації: OSPF, EIGRP та BGP. Аналіз включав як теоретичні аспекти, що стосуються їх архітектури, принципів роботи та механізмів, так і практичні аспекти, які базувалися на результатах моделювання у симульованих мережевих середовищах.

Основні висновки за розділом:

Відсутність універсального рішення: Аналіз підтвердив, що жоден із протоколів не може вважатися універсальним "найкращим" рішенням для всіх типів мережевих інфраструктур. Натомість, кожен із них має конкретну нішу застосування, де його переваги реалізуються найкраще.

OSPF – для масштабованих внутрішніх мереж: OSPF є ефективним інструментом для внутрішньої маршрутизації у великих та середніх корпоративних мережах, а також у мережах провайдерів послуг, завдяки своїй ієрархічній архітектурі, відмовостійкості та незалежності від виробника. Він забезпечує збалансовану продуктивність та масштабованість.

EIGRP – для швидкої конвергенції в Cisco-середовищах: EIGRP демонструє виняткову продуктивність і надзвичайно швидку адаптацію до змін у топології в однорідних середовищах, побудованих на обладнанні Cisco. Це робить його ідеальним для додатків, чутливих до затримок, таких як VoIP та відео, де час простою повинен бути мінімальним.

BGP – для глобальної міждоменної маршрутизації: BGP, хоч і складніший у налаштуванні та з повільною конвергенцією, забезпечує критично важливі функції у глобальних мережах. Він є незамінним елементом Інтернет-інфраструктури, надаючи неперевершену гнучкість у застосуванні політик маршрутизації та контролі трафіку між автономними системами.

Важливість обґрунтованого вибору: Обґрунтований вибір протоколу маршрутизації, що базується на детальному аналізі потреб конкретної мережі (розмір, топологія, вимоги до продуктивності, безпеки, масштабованості, наявне обладнання та кваліфікація персоналу), є запорукою побудови ефективної, надійної та безпечної мережевої інфраструктури, здатної відповідати сучасним та майбутнім вимогам до мережевої комунікації.

Таким чином, успішне проектування та експлуатація комп'ютерних мереж вимагають глибокого розуміння сильних і слабких сторін кожного

протоколу маршрутизації та вміння застосовувати їх відповідно до конкретних сценаріїв.

ВИСНОВКИ

У ході виконання дипломної роботи було здійснено детальний аналіз трьох основних протоколів маршрутизації: OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol) та BGP (Border Gateway Protocol), які відіграють ключову роль у функціонуванні сучасних комп'ютерних мереж. Дослідження показало, що кожен із протоколів має свої переваги та обмеження, і вибір конкретного рішення залежить від специфіки мережевого середовища, топології, вимог до масштабованості, надійності та швидкості реагування на зміни.

Протокол OSPF виявився найбільш ефективним для внутрішньої маршрутизації у великих організаційних мережах завдяки ієрархічній структурі, відкритості стандарту та використанню алгоритму SPF, що забезпечує швидку конвергенцію. EIGRP, хоча є частково пропрієтарним рішенням, продемонстрував високу гнучкість, ефективне використання ресурсу процесора і здатність до швидкої адаптації до змін у мережі, що робить його придатним для складних внутрішніх мереж Cisco-інфраструктури. Протокол BGP, як єдиний міждоменно орієнтований протокол, є незамінним у глобальній маршрутизації між автономними системами, забезпечуючи гнучкий механізм політик маршрутизації та високу масштабованість.

У результаті експериментального моделювання та порівняння характеристик (швидкість конвергенції, стабільність, навантаження на ресурси, гнучкість у керуванні маршрутами) було визначено доцільність використання кожного протоколу в залежності від поставлених завдань. Робота довела важливість комплексного підходу до проектування маршрутизованих мереж, де часто необхідно використовувати комбінацію кількох протоколів для досягнення оптимального результату.

Таким чином, результати дослідження можуть бути корисними для фахівців із мережевої інженерії під час побудови масштабованих,

продуктивних і безпечних мереж, а також слугувати основою для подальшого вивчення взаємодії маршрутизованих протоколів у мультипротокольних середовищах.

OSPF: ідеальний для великих корпоративних мереж з багатьма маршрутизаторами, що вимагають детального контролю.

EIGRP: добрий вибір для мереж Cisco; швидкий і ефективний, але обмежений лише пристроями Cisco (або з обмеженою підтримкою).

BGP: критичний для Інтернету; використовується між автономними системами (AS), має складну політику маршрутизації, але забезпечує гнучкість і масштабованість.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Таненбаум Е., Уезеролл Д. **Комп'ютерні мережі.** – К.: Діалектика, 2020. – 800 с.

2. Курган М., Романишин Я. **Мережеві технології TCP/IP.** – Львів: Видавництво ЛНУ, 2021. – 432 с.

3. RFC 2328 – OSPF Version 2. – https://tools.ietf.org/html/rfc2328

4. RFC 4271 – A Border Gateway Protocol 4 (BGP-4). – https://tools.ietf.org/html/rfc4271

5. Cisco Systems. **Introduction to EIGRP.** – Cisco Networking Academy, 2023. – https://www.cisco.com

6. Forouzan B. **Data Communications and Networking.** – McGraw-Hill, 2017. – 1264 p.

7. Stallings W. **Data and Computer Communications.** – Pearson, 2021. – 960 p.

8. Олійник О.В., Соловей О.М. **Мережеві протоколи та технології.** – Харків: ХНУРЕ, 2020. – 312 с.

9. White R. **Optimal Routing Design.** – Cisco Press, 2019. – 912 p.

10. Гуменюк В.С. **Проектування комп’ютерних мереж.** – Київ: КНЕУ, 2018. – 278 с.

11. Behrouz A. Forouzan. **TCP/IP Protocol Suite.** – McGraw-Hill, 2020. – 896 p.

12. Тарасов В.І. **Аналіз ефективності протоколів маршрутизації у корпоративних мережах.** // Вісник НТУУ «КПІ». – 2021. – №4. – С. 65–71.

13. Cisco Packet Tracer. **User Guide.** – Cisco Academy, 2023.

14. Медведєв А.І., Лисенко Н.П. **Дослідження протоколів маршрутизації з використанням емулятора GNS3.** // Сучасні інформаційні системи. – 2022. – №2(46). – С. 54–59.